

# Implementando validación de origen (ROV) en Cisco IOS

Carlos Martínez, LACNIC, @CagnazzoEng



# Checklist

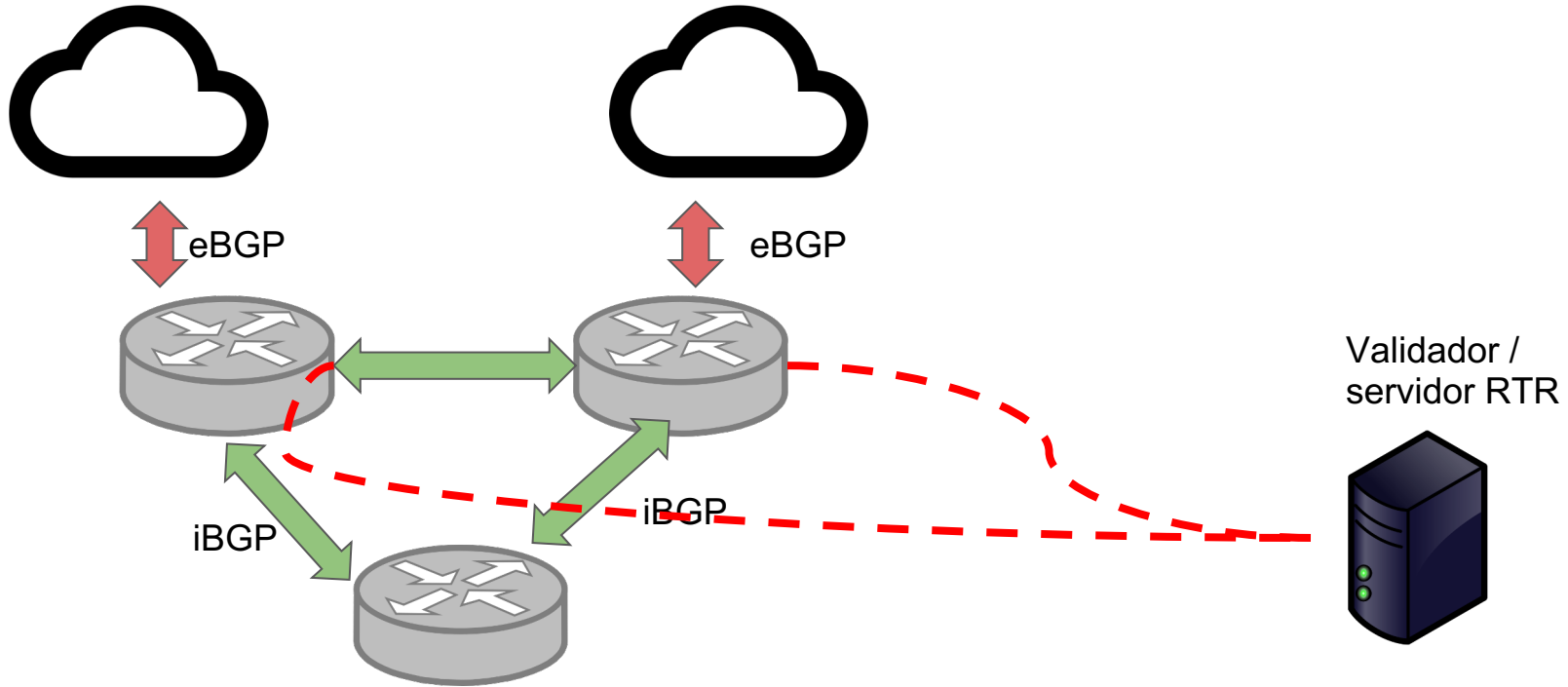
¿Que necesitamos saber antes de empezar?

- Las **direcciones IP** de nuestros servidores RTR (validadores)
- Nuestro **sistema autónomo**
- Tener acceso **enable** a nuestros routers

¿Qué pasos vamos a seguir?

- Habilitar las sesiones RTR en los routers
- Habilitar la validación de origen en cada “address family” del proceso BGP
- Verificar la correcta operación del ROV

# Nuestra red, donde vamos a trabajar



# Habilitar RPKI en IOS XE

Referencia: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_bgp/configuration/xe-3s/irg-xe-3s-book/bgp-origin-as-validation.html?referring\\_site=RE&pos=1&page=https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k\\_r4-2/routing/configuration/guide/b\\_routing\\_cg42xr12k/b\\_routing\\_cg42xr12k\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-xe-3s-book/bgp-origin-as-validation.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r4-2/routing/configuration/guide/b_routing_cg42xr12k/b_routing_cg42xr12k_chapter_01.html)

## Pasos:

### 1. Habilitar el servidor RTR

- a. En el proceso bgp: `bgp rpki server tcp {ipv4-address | ipv6-address} port port-number refresh seconds`
- b. Conviene tener más de uno (redundancia, diversidad de código)
- c. Vamos a usar estos servidores RTR:
  - i. 179.0.156.123 port 8323
  - ii. 168.121.185.105 por 8323

# Habilitar RPKI en IOS XE (ii)

Pasos:

2. Habilitar / deshabilitar validación de origen por address-family

```
address-family ipv4 unicast
```

```
    bgp bestpath prefix-validate disable
```

```
address-family ipv6 unicast
```

```
    bgp bestpath prefix-validate allow-invalid
```

# Habilitar RPKI en IOS XE (iii)

Pasos:

2. (Opcional, dependiendo del escenario) Permitir prefijos inválidos en la tabla

```
address-family ipv4 unicast
```

```
    bgp bestpath prefix-validate allow-invalid
```

```
address-family ipv6 unicast
```

```
    bgp bestpath prefix-validate allow-invalid
```

# Verificar la operación de RPKI

## 3. Verificar que el servidor RTR esté respondiendo

```
# sh bgp ipv4 unicast rpki table
```

```
119339 BGP sovc record entries using 3818848 bytes of memory
```

| Network    | Maxlen | Origin-AS | Source | Neighbor           |
|------------|--------|-----------|--------|--------------------|
| 1.0.0.0/24 | 24     | 13335     | 0      | 179.0.156.123/8323 |
| 1.1.1.0/24 | 24     | 13335     | 0      | 179.0.156.123/8323 |

# Verificar la operación correcta de RPKI

Verificar que las rutas aprendidas por BGP tienen un estado de validación asignado:

```
# sh bgp ipv4 unicast
```

```
BGP table version is 375420, local router ID is 200.7.84.35
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,  
               x best-external, a additional-path, c RIB-compressed,  
               t secondary path,
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

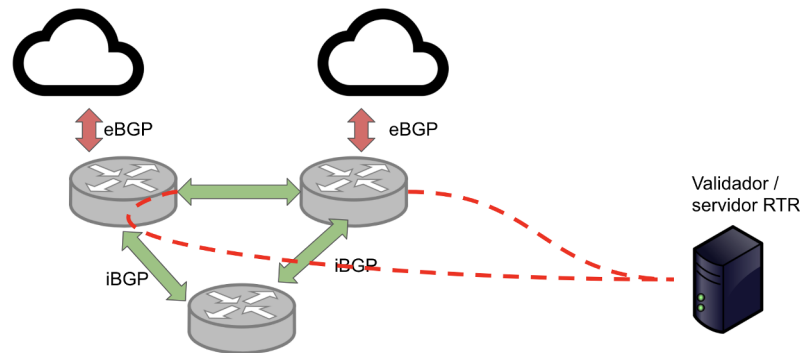
```
RPKI validation codes: V valid, I invalid, N Not found
```

|      | Network       | Next Hop       | Metric | LocPrf | Weight | Path      |
|------|---------------|----------------|--------|--------|--------|-----------|
| N*   | 0.0.0.0       | 200.58.128.245 |        |        |        | 0 19422 i |
| V*>i |               | 200.7.84.34    | 0      | 250    | 0      | 6057 i    |
| V*>i | 2.18.64.0/24  | 200.40.98.29   | 0      | 100    | 0      | 6057 i    |
| V*>i | 2.19.251.0/24 | 200.40.98.29   | 0      | 100    | 0      | 6057 i    |



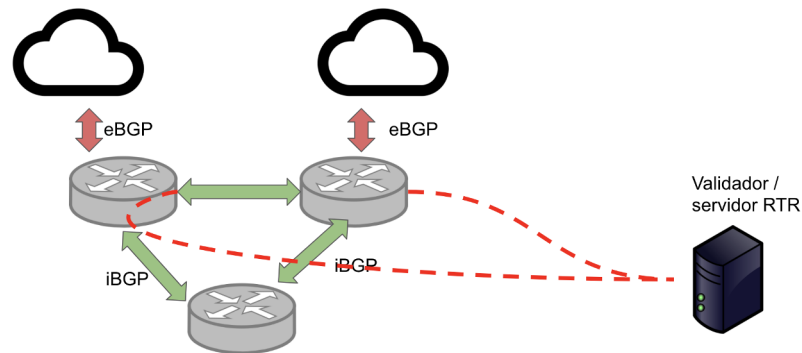
# ¿Qué pasa con las sesiones iBGP?

- En Cisco **todo lo que un router aprende por iBGP es marcado como válido por defecto**
- Esto puede tener algunas consecuencias inesperadas
  - Rutas por defecto “menos” óptimas
  - R1 aprende una default “not found” (¡naturalmente!) por eBGP pero ve com “valid” la que aprende por iBGP



# ¿Qué pasa con las sesiones iBGP?

- En IOS XE tenemos disponible la posibilidad de enviar el **estado de validez** de un prefijo como una **comunidad extendida**



```
router bgp 65000

  neighbor 10.10.10.10 remote-as 65000

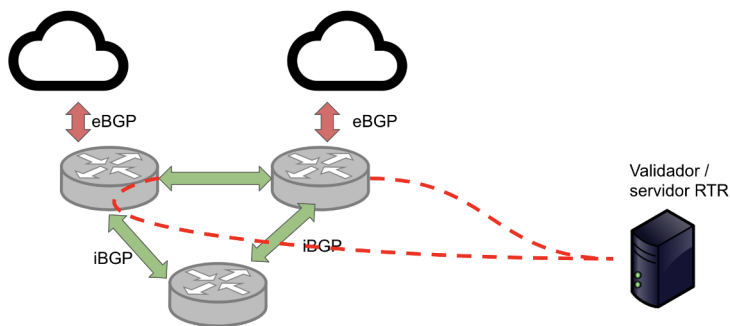
  address-family ipv4 unicast

  neighbor 10.10.10.10 send-community extended

  neighbor 10.10.10.10 announce rpki state
```

# Configurando política usando el estado de validez

En route-maps:



```
router bgp 65000
```

```
neighbor 10.10.10.10 remote-as 65000
```

```
address-family ipv4 unicast
```

```
neighbor 10.10.10.10 send-community extended
```

```
neighbor 10.10.10.10 announce rpki state
```

¡Muchas gracias!