socium

Fortaleciendo la Infraestructura de Internet

IDMX MEETING

BGP ROUTING AND PEERING

# De los fundamentos del ruteo a la operación segura de peering

Taller técnico integrado para operadores de red

Fundamentos de BGP · Peering e interconexión · Seguridad de ruteo · Configuración y operación

AGENDA DEL TALLER

# Cinco bloques, de la teoría a la práctica

01

## Fundamentos de BGP

Sistemas autónomos, atributos, mensajes y estados del protocolo

02

## Peering e interconexión

Qué es el peering, tipos de acuerdo y la ruta de implementación

03

## Seguridad y buenas prácticas

Hijacking, route leaks, spoofing

04

## Configuración y operación

Comandos, verificación, incidencias comunes y laboratorio

05

## Cierre y recursos

Resumen, referencias y siguientes pasos

SECCIÓN 1

# Fundamentos de BGP

Antes de hablar de peering, necesitamos un lenguaje común: qué es un sistema autónomo, qué es BGP y cómo toma decisiones.

- Sistema Autónomo (AS) y ASN
- Qué es BGP y cuándo se usa: iBGP vs. eBGP
- Atributos, mensajes y estados del protocolo

# Sistema Autónomo (AS)

**Un Sistema Autónomo (AS)** es un conjunto de redes que comparten una misma política de enrutamiento y que se administran bajo un solo control técnico.

Cada AS tiene un identificador único: el **ASN** (Autonomous System Number). Es el "número de placa" que usan los routers para reconocerse entre sí en Internet.

*Un WISP, un ISP, una universidad o un IXP: todos son, técnicamente, sistemas autónomos.*

### Rangos de numeración de ASN

| Rango | Uso |
|---|---|
| 0 y 65,535 | Reservados |
| 1 – 64,495 | Internet pública (16 bits) |
| 64,496 – 64,511 | Documentación (RFC 5737) |
| 64,512 – 65,534 | Uso privado |
| 65,536 – 65,551 | Documentación 32 bits (RFC 5398) |
| 65,552 – 4,294,967,295 | Internet pública (32 bits) |

# ¿Qué es BGP?

**BGP (Border Gateway Protocol)** es el protocolo de enrutamiento que intercambia información de alcance de red entre routers de diferentes sistemas autónomos.

## RFC 1163

Descrito originalmente como protocolo de gateway exterior (EGP).

## Puerto TCP 179

BGP usa TCP como transporte, garantizando entrega confiable de los anuncios de rutas.

## Borde externo e interno

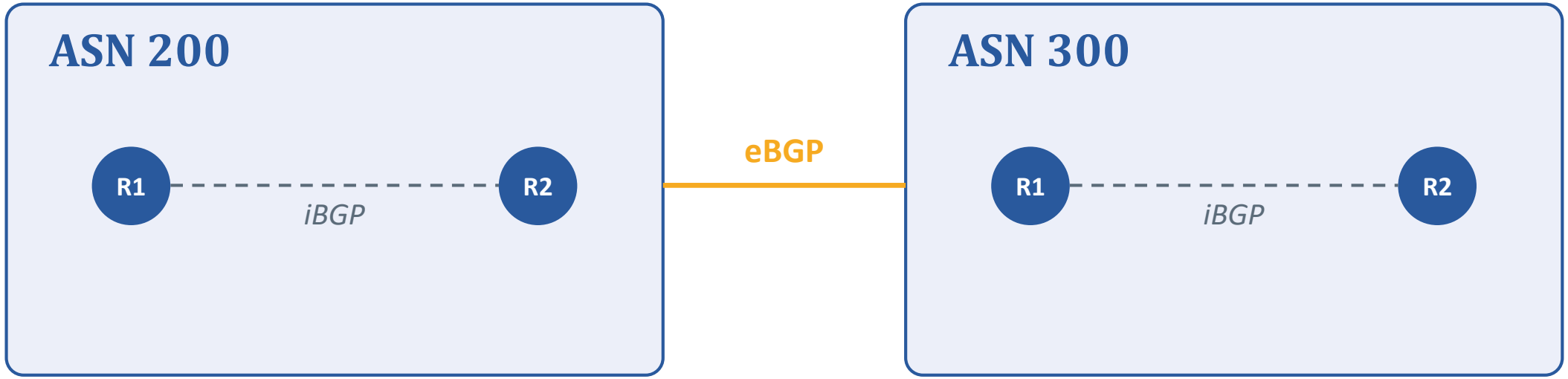
Aporta estabilidad actuando como protocolo entre AS (eBGP) y dentro de un AS (iBGP).

## Multiprotocolo (MBGP)

Las extensiones MP-BGP permiten que BGP soporte IPv6 además de IPv4.

# ¿Cuándo se usa BGP? - iBGP y eBGP

BGP se usa tanto para enrutar información dentro de un AS como entre distintos AS. La diferencia depende de si los routers que forman el par (peers) están en el mismo sistema autónomo o no.



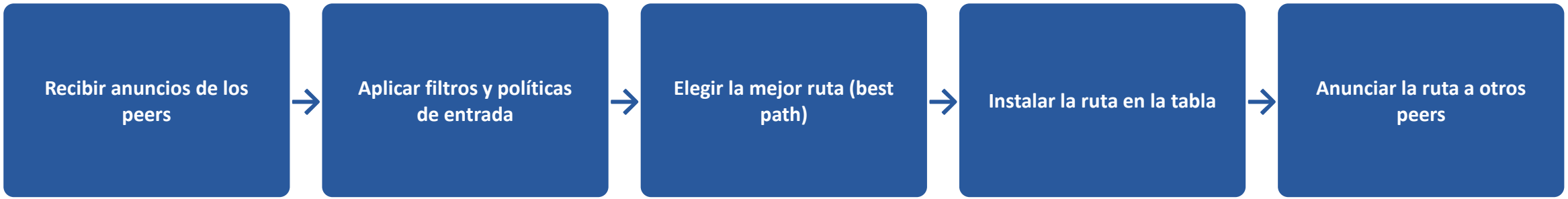

- eBGP se establece entre routers de distinto AS; requiere conexión física (directa o vía IXP).
- iBGP se establece entre routers del mismo AS; no necesitan estar directamente conectados, solo alcanzar el puerto 179/TCP.
- Ambos garantizan mayor estabilidad al basar sus decisiones en políticas definidas por el operador de red.

# iBGP y eBGP: comparación directa

| Característica | iBGP | eBGP |
|---|---|---|
| **Se ejecuta entre...** | Routers del mismo AS | Routers de AS diferentes |
| **Conexión física** | No requiere adyacencia directa | Los routers sí deben estar físicamente conectados |
| **Topología** | Independiente de la topología (usa TCP/179) | Depende del enlace directo o del IXP |
| **Propósito típico** | Sincronizar rutas entre routers de borde de un mismo operador | Intercambiar rutas con otro operador (tránsito o peering) |
| **Ejemplo** | R1 y R2 dentro de ASN 200 | ASN 200 ↔ ASN 300 |

# ¿Cómo funciona BGP?

Un sistema BGP comparte información de accesibilidad de red con sistemas BGP adyacentes, conocidos como **vecinos** o **peers**. Cada router mantiene una tabla de ruteo BGP (RIB) que usa para decidir por dónde enviar cada paquete.




*Este ciclo se repite constantemente: BGP es un protocolo de vector de ruta que converge de forma incremental, no periódica.*

# Atributos de BGP: cómo se elige la mejor ruta

BGP determina la mejor ruta evaluando, en orden, los atributos de cada ruta candidata en la tabla de ruteo:

## ORIGIN

Indica cómo se aprendió la ruta: IGP (i), EGP (e) o incompleto (?).

## AS-PATH

Lista de AS atravesados. BGP prefiere el camino más corto; se puede alargar (prepending) para desalentar una entrada.

## NEXT HOP

La dirección IP del siguiente salto necesario para alcanzar el destino.

## LOCAL PREFERENCE

Costo interno de un destino; garantiza coherencia de salida en todo el AS.

## MED

Discriminador de salidas múltiples: sugiere a un AS vecino qué entrada preferir entre varias conexiones.

## COMUNIDADES

Etiquetas genéricas que señalizan políticas administrativas entre routers BGP.

# Tipos de mensajes BGP

## OPEN

Inicia el intercambio de información de una sesión BGP entre dos peers.

## KEEPALIVE

Mensajes periódicos que confirman los OPEN e informan que la sesión debe mantenerse activa.

## UPDATE

Transmite información sobre rutas nuevas o modificadas.

## NOTIFICATION

Se usa para eliminar rutas o abortar una sesión cuando no llega un KEEPALIVE esperado.

# Estados de BGP (máquina de estados finitos)

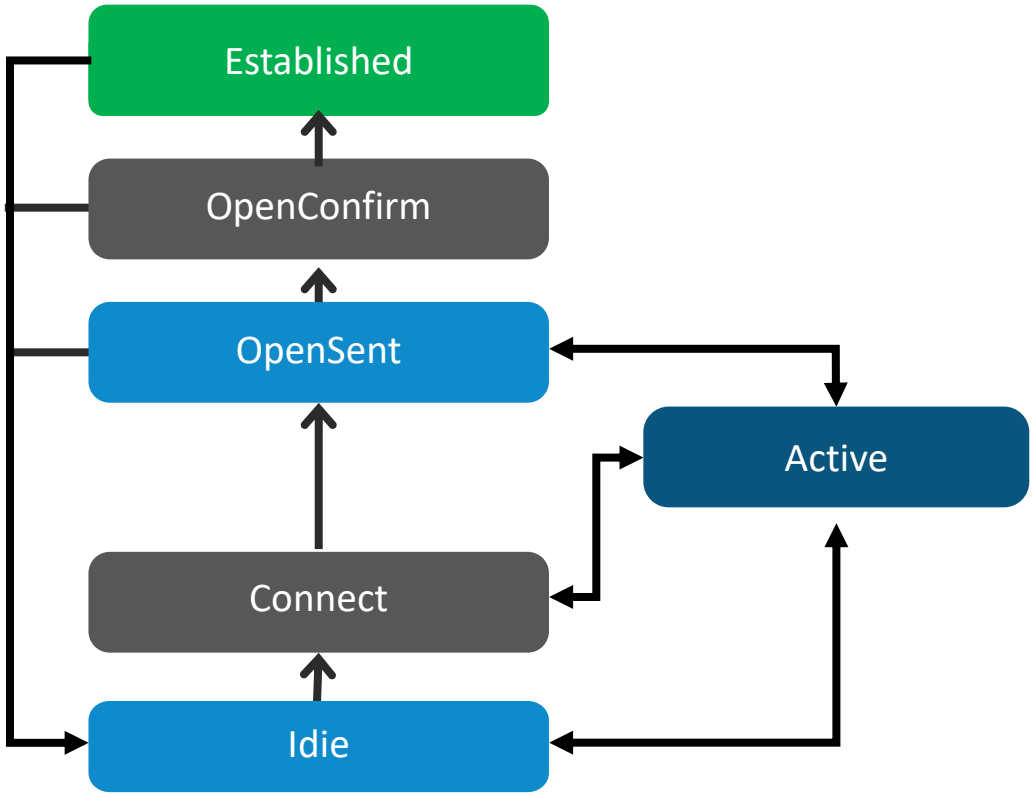
La sesión BGP está activa: los peers ya intercambian mensajes UPDATE.

El router espera un mensaje KEEPALIVE o NOTIFICATION.

Se envió el mensaje OPEN; el router espera el OPEN de respuesta.

BGP espera que se complete la conexión TCP de transporte.

Estado inicial: el router no está intentando establecer la sesión.

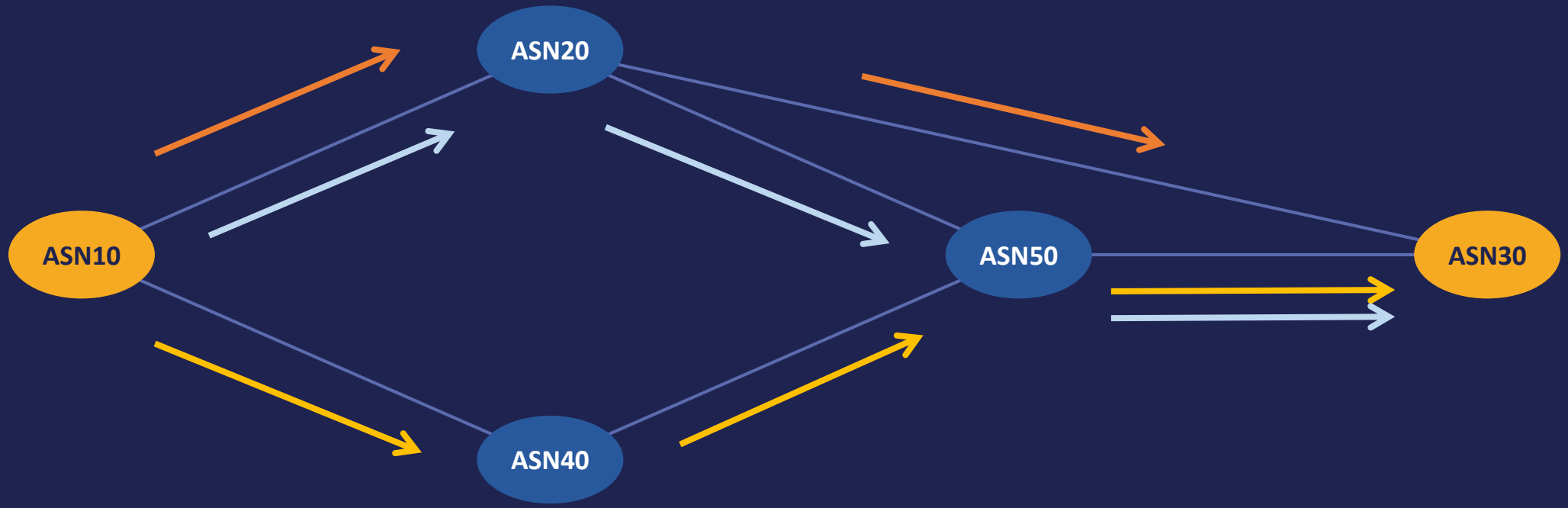



BGP intenta activamente establecer la conexión TCP con el peer.

*Cuando BGP no logra establecer la conexión en Connect, Active u OpenSent, regresa a Idle y reintenta.*

# ¿Por qué necesito BGP en mi red?

Sin BGP, cada operador dependería de una única ruta fija hacia el resto de Internet. Con BGP, cada AS puede elegir entre múltiples caminos posibles.




*¿Cuál es el camino para llegar de ASN 10 a ASN 30? BGP evalúa varias rutas posibles y selecciona la mejor según sus atributos.*

SECCIÓN 1 · CIERRE

# De sistemas autónomos a rutas inteligentes

## En esta sección vimos:

- Un AS es una red bajo una política común, identificada por su ASN.
- BGP intercambia información de alcanzabilidad entre AS (eBGP) y dentro de un AS (iBGP).
- Los atributos (AS-PATH, LOCAL_PREF, MED, comunidades) son las palancas que controlan qué ruta se usa.
- Los mensajes OPEN/KEEPALIVE/UPDATE/NOTIFICATION y los seis estados del FSM describen el ciclo de vida de una sesión BGP.

*Con estos fundamentos ya podemos hablar de peering: la decisión de a quién conectarnos directamente para mejorar esas rutas.*

SECCIÓN 2

# Peering e Interconexión

Ahora que entendemos cómo decide BGP, veamos cómo un operador pasa de depender solo de tránsito a construir sus propias rutas directas.

- Qué es el peering y qué tipos de interconexión existen
- Tipos de acuerdo de peering: bilateral, pagado y multilateral
- La ruta de implementación: seis pasos concretos

# ¿Qué es el peering?

**El peering** es una conexión entre dos redes IP que permite intercambiar información de enrutamiento, de modo que el tráfico fluye desde orígenes en cualquiera de las redes hacia destinos en la otra. Es un acuerdo entre las partes para compartir tráfico entre sus AS.

### AS

Cada red que participa mantiene su propio sistema autónomo con su ASN.

### Sesión eBGP

El intercambio de rutas se realiza mediante una sesión eBGP entre los routers de borde.

### Tráfico propio

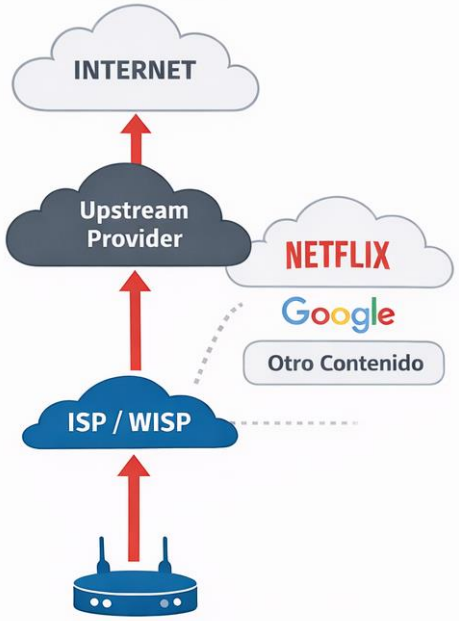
Solo se intercambia tráfico que se origina o termina en las redes de las partes — no es tránsito.

# De un solo camino a rutas locales

## Modelo dependiente (solo tránsito)

- Red destino
- ↑
- **Proveedor de tránsito**
- ↑
- Cliente WISP

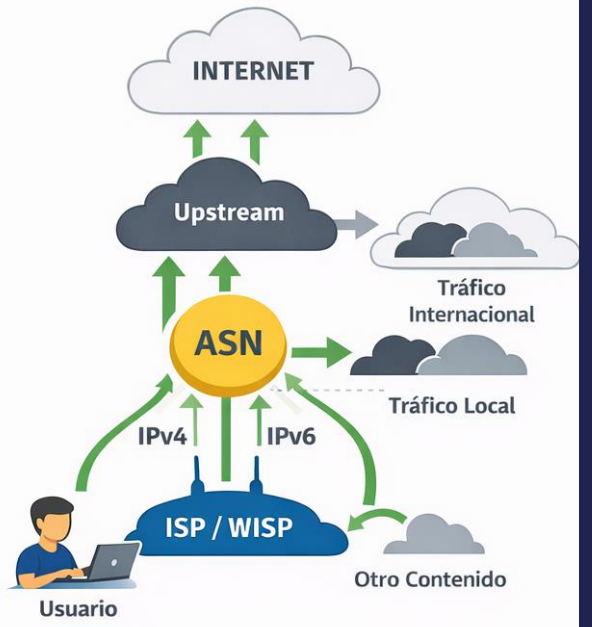
**ANTES**




**Dependencia total del Upstream**

- Sin ASN propio
- Sin direcciones IP propias

**DESPUÉS**




**Autonomía y control de rutas**

- ASN propio
- Direcciones IP propias (IPv4 / IPv6)

## Modelo con peering

- **AS destino local**
- ↑
- **IXP / PNI** | **Tránsito**
- ↖ ↗
- **Cliente WISP → AS propio**

*El tráfico local toma rutas locales; el tránsito queda para lo que realmente lo necesita.*

# Tipos de interconexión

## IXP (Punto de Intercambio)

INTERCONEXIÓN PÚBLICA

Se realiza a través de un IXP, donde una red puede conectarse con muchas otras mediante una sola conexión física.

## PNI (Private Network Interconnect)

INTERCONEXIÓN PRIVADA

Dos o más redes acuerdan intercambiar tráfico en una instalación privada, con un enlace dedicado entre ambas.

## No es peering

TRÁNSITO (REFERENCIA)

Una red provee a otra la capacidad de llegar a toda Internet, típicamente a cambio de una tarifa por volumen.

# Tres formas de acordar el peering

## Bilateral libre de costo

SETTLEMENT-FREE

Dos AS de tamaño y tráfico comparables acuerdan intercambiar sin pago mutuo.

## Peering pagado

PAID PEERING

Una parte paga por el acceso directo cuando el tráfico es muy asimétrico entre ambas redes.

## Multilateral (recomendado para empezar)

ROUTE SERVER

Una sola sesión BGP con el route server del IXP abre acceso a muchos miembros a la vez.

*Un WISP que inicia peering casi siempre debe empezar por el route server multilateral y evaluar PNI o peering bilateral dedicado sólo cuando un par concreto lo justifique.*

# ¿Qué se necesita para empezar?

| Dimensión | Mínimo para iniciar | Siguiente nivel |
|---|---|---|
| **Identidad** | ASN, prefijos y contactos | PeeringDB, IRR, ROAs y política pública |
| **Conectividad** | Un puerto IXP y backhaul estable | Dos sitios o rutas diversas |
| **BGP** | Router con eBGP IPv4/IPv6 y filtros | Dos routers, BFD, automatización y comunidades |
| **Seguridad** | Filtros, max-prefix y ROAs | ROV estricto, anti-spoofing y monitoreo de leaks |
| **Operación** | Responsable NOC y procedimiento de cambios | NOC 24×7, runbooks y pruebas de contingencia |
| **Economía** | Presupuesto de puerto, transporte y equipo | Modelo de ahorro por Mbps y crecimiento |

# Beneficios del peering que sí se pueden medir

## Menor costo

El tráfico intercambiado localmente deja de consumir capacidad facturable de tránsito.

## Menor latencia

Las rutas locales evitan trayectos innecesariamente largos.

## Control de tráfico

BGP permite seleccionar rutas mediante políticas, atributos y comunidades.

## Resiliencia

Múltiples caminos reducen el impacto de fallas de un solo proveedor upstream.

## Escalabilidad

El crecimiento del tráfico no depende linealmente de un solo proveedor.

SECCIÓN 2 · CIERRE

# De la teoría del protocolo a una red interconectada

## En esta sección vimos:

- El peering es un acuerdo para intercambiar tráfico propio directamente entre dos AS, sin pasar por tránsito.
- Puede ser público (vía IXP) o privado (PNI); y bilateral, pagado o multilateral según el acuerdo comercial.
- La ruta de seis pasos lleva de la identidad (ASN) a la validación operativa, pasando siempre por seguridad de routing.
- Los beneficios (costo, latencia, control, resiliencia, escalabilidad) son medibles, no solo teóricos.

*Pero cada uno de estos pasos —sobre todo la seguridad de routing— existe porque BGP, sin controles, es vulnerable. Veamos qué puede salir mal y cómo prevenirlo.*

SECCIÓN 3

# Seguridad y Buenas Prácticas en BGP

BGP fue diseñado asumiendo confianza entre operadores. Esa confianza se puede abusar, por error o intencionalmente.

- Route/prefix hijacking y route leaks: qué son y cómo han ocurrido en la vida real
- IP address spoofing y ataques de amplificación
- Filtrado, ACLs y anti-spoofing: las defensas prácticas

# Tres incidentes que todo operador debe conocer

## Route / Prefix Hijacking

Un operador (por error o ataque) anuncia un prefijo que no le pertenece, desviando tráfico ajeno hacia sí mismo.

## Route Leak

Un operador con varios proveedores upstream reenvía accidentalmente rutas de uno hacia el otro, actuando como tránsito no autorizado.

## IP Address Spoofing

Se falsea la dirección IP de origen de un paquete para ocultar identidad o amplificar un ataque.

SECCIÓN 4

# Configuración y Operación de BGP

Llevemos todo lo anterior a la práctica: cómo se configura, se verifica y se resuelven problemas en una sesión BGP real.

- Pasos y comandos para configurar una sesión BGP (IOS Cisco)
- Comandos de verificación en IPv4 e IPv6
- Incidencias comunes y actividad de laboratorio

# Pasos para configurar una sesión BGP

1

## Activar el protocolo

Activar BGP y asignar el ASN propio del router

2

## Configurar el peer

Definir la sesión con el neighbor: su IP y su ASN remoto

3

## Describir el peer

Agregar una descripción clara para identificar al vecino

4

## Activar la sesión

Activar la sesión de peer con el neighbor (mensaje OPEN)

5

## Anunciar prefijos

Anunciar los prefijos deseados mediante mensajes UPDATE

6

## Verificar Established

Confirmar que el estado del vecino llegó a Established

# Comandos de configuración BGP (IOS Cisco)

## Configuración base

```
router bgp <ASN>

neighbor <IPv4/IPv6_Address> remote-as <ASN-Remoto>

neighbor <IPv4/IPv6_Address> activate

address-family ipv4 / ipv6

network <IPv4/IPv6_Address> <prefix_mask>
```

# Comandos de verificación BGP (IOS Cisco)

| Propósito | IPv4 | IPv6 |
|---|---|---|
| Resumen de sesiones | show ip bgp summary | show bgp ipv6 unicast summary |
| Detalle de un vecino | show ip bgp neighbor | show ipv6 bgp neighbor |
| Tabla de ruteo | show ip route | show ipv6 route |

# Incidencias comunes y resolución

## Falla en Router ID

Verificar que el Router ID esté configurado explícitamente y no dependa de una interfaz que puede caer.

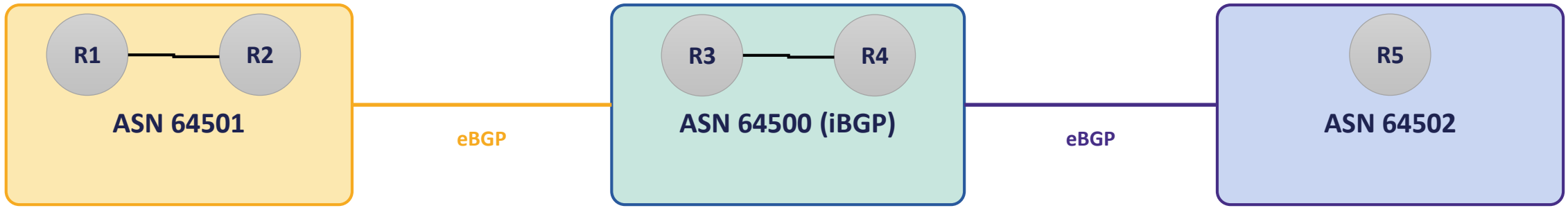
## Falla al establecer sesión

Revisar conectividad TCP/179, remote-as correcto y que 'activate' esté aplicado en el address-family.

## Prefijos no anunciados

Confirmar el comando 'network' con la máscara exacta y que el prefijo exista en la tabla de ruteo local.

# Actividad práctica: configura tu primera sesión BGP




**Actividades:**

1. Configurar la sesión BGP del ASN 64500 entre los routers R3 y R4 (iBGP).
2. Configurar la sesión BGP del ASN 64502 (R5) hacia ASN 64500.
3. Configurar el proceso BGP del ASN 64501 (R1) hacia ASN 64500.

*El facilitador compartirá la guía en PDF y el acceso al laboratorio virtual al inicio de esta actividad.*

Qr Laboratorio

Qr PDF Guía

# De la configuración a la operación confiable

## En esta sección vimos:

- Configurar BGP sigue una secuencia clara: activar el protocolo, definir el peer, activarlo y anunciar prefijos.
- Los comandos 'show ... summary' y 'show ... neighbor' son la primera línea de verificación.
- La mayoría de incidencias iniciales se deben a 'activate' faltante, remote-as incorrecto o máscaras mal definidas.
- El laboratorio replica un escenario realista con iBGP y eBGP combinados, igual que en producción.

*Con los fundamentos, el peering, la seguridad y la práctica cubiertos, cerramos el taller con un resumen y los recursos para seguir aprendiendo.*

SECCIÓN 5

# Cierre y Recursos

Lo que aprendimos hoy, y hacia dónde seguir.

# Recursos y referencias

## RFC 1163

Especificación original de BGP como protocolo de gateway exterior.

*datatracker.ietf.org/doc/html/rfc1163*

## Cisco — Casos prácticos BGP

Documentación técnica con ejemplos de configuración y troubleshooting.

*cisco.com — BGP support docs*

## Cisco — Resolución de problemas comunes de BGP

Guía de diagnóstico para incidencias frecuentes en sesiones BGP.

*cisco.com — BGP troubleshooting*

## LACNIC

Administración de recursos de numeración (ASN, IPv4, IPv6) para la región.

*lacnic.net*

## MANRS

Marco de buenas prácticas de seguridad de ruteo entre operadores.

*manrs.org*

## PeeringDB

Directorio global de redes, IXPs y políticas de peering.

*peeringdb.com*

socium
Fortaleciendo la Infraestructura de Internet

IDMX MEETING

# ¡GRACIAS!

BGP Routing and Peering

**Emmanuel Serrano**
emmanuel@socium.cr

*Preguntas, dudas o seguimiento: con gusto seguimos la conversación después del taller.*