# Cisco Community Live event

## Seguridad en BGP – Mejores Prácticas

Alejandro Acosta– Coordinador de I+D en LACNC
Ignacio Magaña – Senior TCE XR SP, CCIE SP #53583
Hector Carranza – Technical Leader SP XR, CCIE Enterprise #42717

Septiembre 27, 2022

# Novedades & Eventos próximos

# Ask Me Anything- Sesión del evento

Hasta el Viernes 7 Septiembre, 2022

Con
Alejandro, Hector e Ignacio

https://bit.ly/ama-seguridad_bgp

# Entrevista con los Expertos

Conozca más de un evangelizador global de la tecnología e Ipv6

Con
Alejandro
Acosta


https://bit.ly/entrevista-acosta

# Califique el contenido de la Comunidad de Cisco en Español

¡Califique “Discusiones, Documentos y Videos!



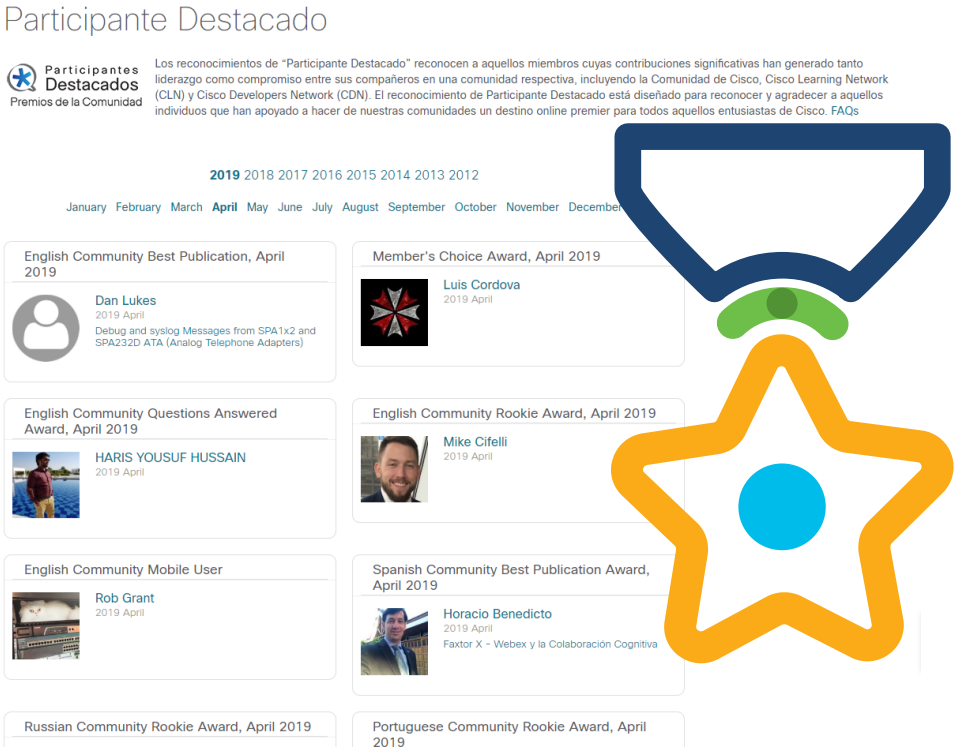
Ayúdenos a identificar el contenido de calidad y a reconocer el esfuerzo de los integrantes de la Comunidad

# Reconocimientos en la Comunidad

**Participante Destacado**

Reconocimiento mensual

Diseñado para reconocer y agradecer a quienes colaboran en la comunidad: publicando contenido o participando en discusiones



# Gracias por su asistencia el día de hoy

La presentación incluirá algunas preguntas a la audiencia.
Le invitamos cordialmente a participar activamente en las preguntas que le haremos durante la sesión



¡Resuelva su dudas y comparta opiniones!

# Expertos de la Comunidad de Cisco

Alejandro Acosta
Coordinador de I+D en LACNC

Hector Carranza
Technical Leader
CCIE #42717

Ignacio Magaña
Sr. Technical Customer Experience
CCIE #53583

# ¡Gracias por estar con nosotros hoy día!

https://bit.ly/slides-sep27

# ¡Haga sus preguntas al Panel de Expertos!

Use  el panel de preguntas y (**P&R / Q&A**) para preguntar a los expertos.

Sus preguntas serán respondidas eventualmente

The bridge to possible

# Seguridad en BGP

## Mejores Prácticas

Alejandro Acosta– Coordinador de I+D en LACNC

Ignacio Magaña – Senior TCE XR SP, CCIE SP #53583

Hector Carranza – Technical Leader SP XR, CCIE Enterprise #42717

Septiembre 27, 2022

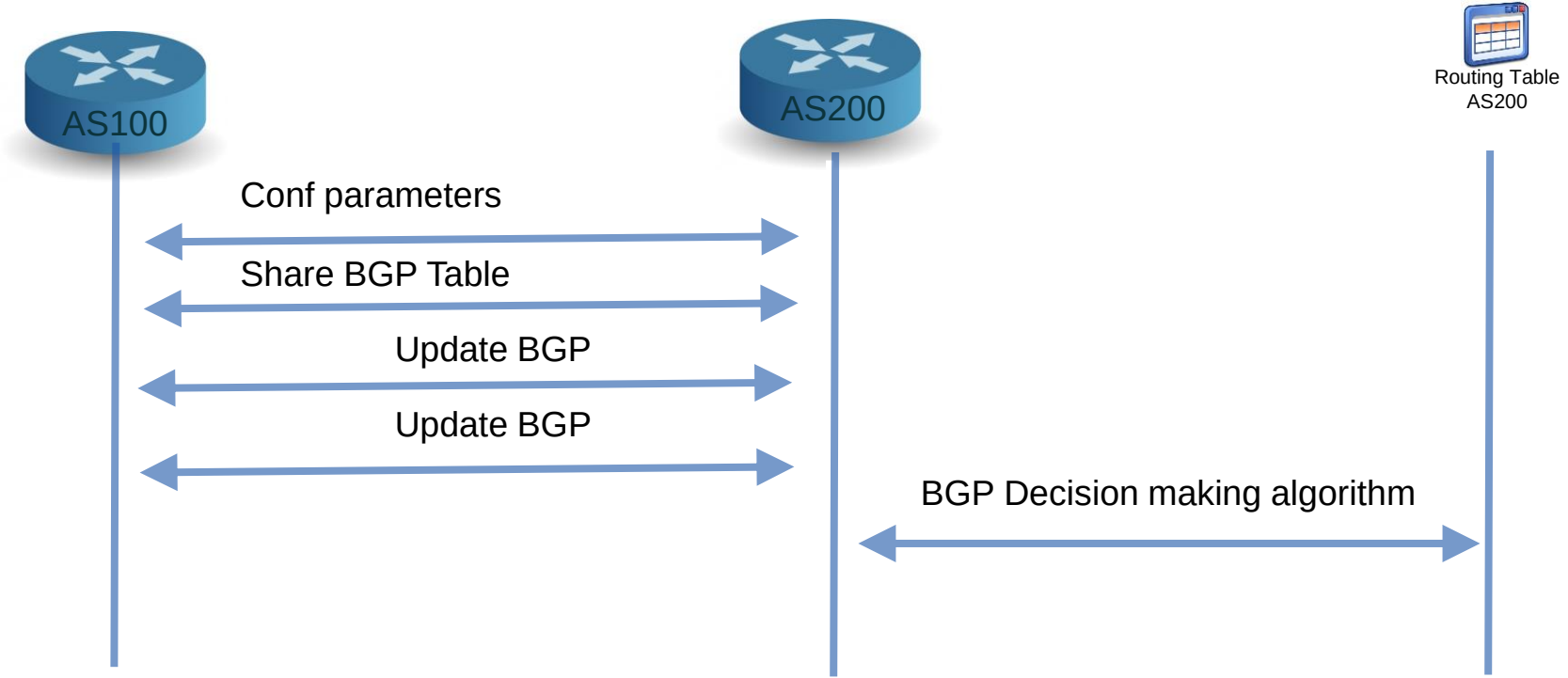
# Agenda

- ¿Qué es BGP?
- Importancia de la Seguridad en BGP
- Mejores prácticas en las vecindades
- Filtrado de prefijos
- Demostración

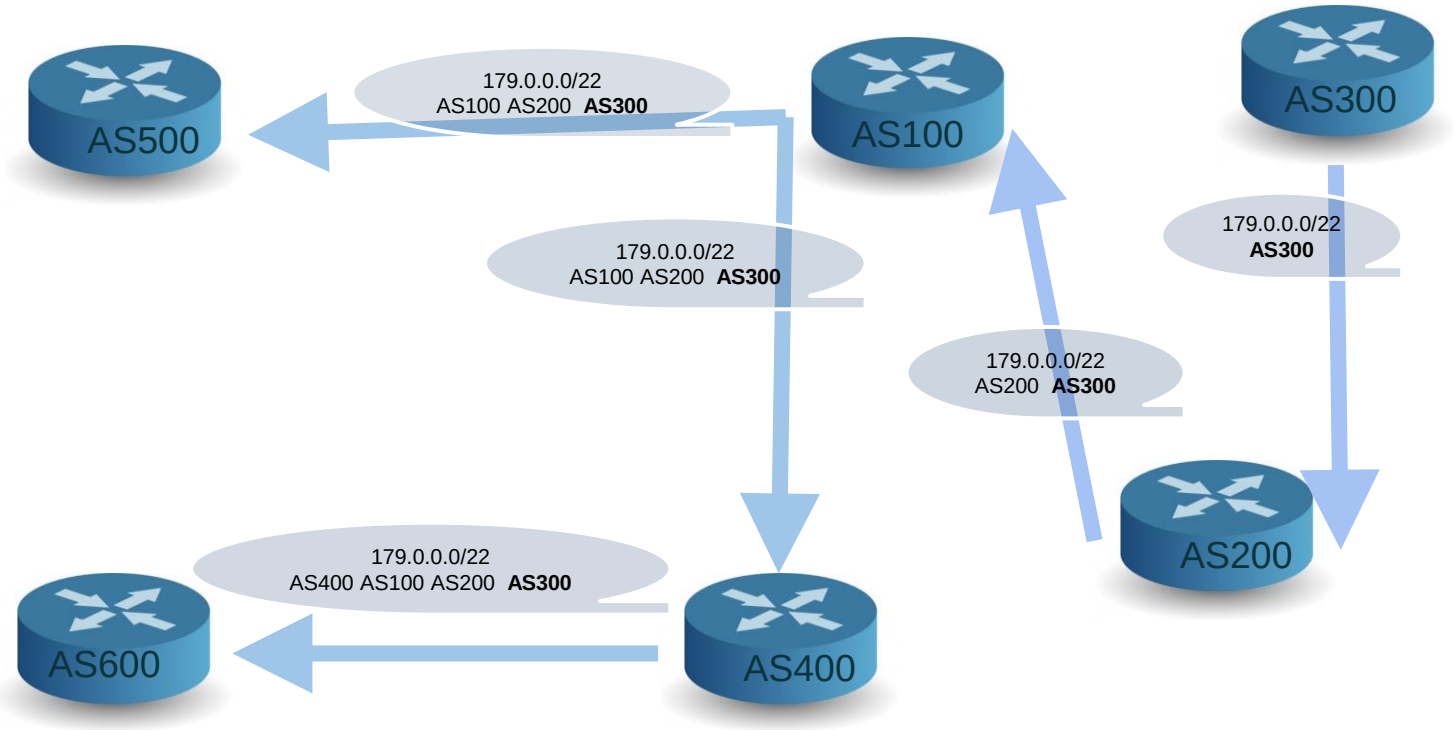
# Introducción - ¿Qué es BGP?

- Protocolo de enrutamiento utilizado principalmente para interconectar routers en diferentes Sistemas Autónomos e ISPs para permitir el intercambio de trafico entre AS, mediante el anuncio de prefijos
- Protocolo definido en el RFC 1654 típicamente conocido como el protocolo del Internet.
- Base de la comunicación y la red para la conexión a Internet.
- Principal propósito es el anuncio de prefijos que los paquetes utilizaran para alcanzar el destino final, pero no garantiza el envío seguro de la información.
- Nuevas funcionalidades y capacidades fueron introducidas con el RFC 2858 (MP-BGP)
- Dos tipos de BGP, eBGP e iBGP

# Cómo funciona Internet/ BGP Session and Routing Table



# Actualizar BGP




¿Quién origino l 179/22?

AS 300

¿Quienes son los vecinos de AS100?

AS 200, AS 400, AS 500

¿Quién más anuncia prefijos?

AS 200, AS 100, AS 400

¿Quién aprendió los prefijos?

TODOS

# Polling Question 1

Mantener buenas prácticas de seguridad al usar BGP es algo que...

A. Siempre consideramos
B. Ocasionalmente consideramos
C. Nunca lo habíamos pensado
D. No consideramos

# ¿Por qué asegurar BGP?

## El principal problema:

- BGP es basado en la confianza entre los operadores y administradores de  los AS.
- No existen mecanismos de validación de identidad o criptográficos en las vecindades.

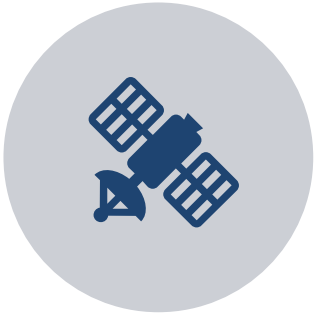
## Mayores riesgos

- Robo de identidad del router
- Reseteo de las sesiones de BGP
  - Vulnerable a ataques TCP/IP
  - BGP Hijacks
  - BGP Route leaks

# Mejores practicas en Vecinos (Neighbors)

| | | |
|---|---|---|
| Utilice el cifrado TCP MD5 para el establecimiento de la sesión | Limite la cantidad de prefijos máximos aceptados de pares | Use el valor TTL para limitar el alcance de los paquetes de control |
| Filtrado basado en el número de AS y los prefijos asignados a los pares | Eliminación de AS privada | Filtrar martians* o rutas falsas |

# Autenticación MD5



MÉTODO SIMPLE DE AUTENTICACIÓN ENTRE VECINOS DE BGP

SE SOPORTA HMAC-MD5 (MESSAGE DIGEST)

OPCIONALMENTE SE PUEDEN OCUPAR "KEY-CHAINS" LO QUE PERMITE ESTABLACER TIEMPOS DE VIDA DE CADA LLAVE.

# Autenticación MD5

```
router bgp 65001
 bgp router-id 100.100.2.1
 address-family ipv4 unicast
 !
 neighbor 100.100.3.1
  remote-as 65001
  password encrypted 1423373838340B1817
  update-source Loopback0
  address-family ipv4 unicast
```

```
router bgp 65001
 bgp router-id 100.100.3.1
 address-family ipv4 unicast
 !
 neighbor 100.100.2.1
  remote-as 65001
  password encrypted 03307E38323F007F7D
  update-source Loopback0
  address-family ipv4 unicast
```

# Filtro de prefijo máximo

- Limita el número de prefijos que se pueden recibir de un vecino.
- En caso de superar el límite una de las siguientes acciones aplica:
  - La opción por defecto es tirar la sesión
  - Descartar los prefijos adicionales, no causa caída de sesión
  - Mostrar un log con la notificación únicamente

** Por defecto la sesión de BGP no se recuperar automáticamente.

** Apoya para prevenir ataques tipo DDoS

# Configuración de filtro de prefijo máximo

IOS XR

```
router bgp 200
  neighbor 100.20.30.1
    address-family ipv4 unicast
     maximum-prefix 1000 90 discard-extra-paths

  neighbor 100.20.30.3
    address-family ipv4 unicast
     maximum-prefix 1000 75 warning-only

 neighbor 20.30.30.30
    address-family ipv4 unicast
      maximum-prefix 1000 90 restart 2
```

IOS / IOS XE

```
router bgp 300
  address-family ipv4
  aggregate-address 30.0.0.0 255.0.0.0 summary-
  only
  neighbor 30.10.10.10 activate
   neighbor 30.10.10.10 next-hop-self

   neighbor 100.20.30.1 activate
   neighbor 100.20.30.1 maximum-prefix 1000 90
  restart 2

   neighbor 100.20.30.2 activate
   neighbor 100.20.30.2 maximum-prefix 1000
  warning-only
```

# Seguridad TTL

- Disponible solo para sesiones eBGP
- El comportamiento es poco diferente de IOS/IOS XE a IOS XR
- Para XR se validará que el TTL de los paquetes sea mayor o igual al máximo valor de TTL disponible.
- Modo ligero de prevenir ataques de DDoS

```
router bgp 200
  neighbor 100.20.30.1
   remote-as 100
  ttl-security
    address-family ipv4 unicast

neighbor 100.20.30.3
   remote-as 300
   ttl-security
    address-family ipv4 unicastg-only
```

```
router bgp 300
  bgp router-id 30.40.40.40
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 100.20.30.1 remote-as 100
  neighbor 100.20.30.1 ttl-security hops 1
  neighbor 100.20.30.2 remote-as 200
```

# AS Filtrado basado en rutas

- Permite aceptar únicamente prefijos de los sistemas autónomos que consideramos válidos.
- Generalmente aceptar prefijos del AS directamente conectado.
- Evitar los AS de tránsito.
- Se requieren expresiones regulares.
- Filtrar los prefijos únicamente del ISP al que estamos conectados.

# AS Filtrado basado en rutas

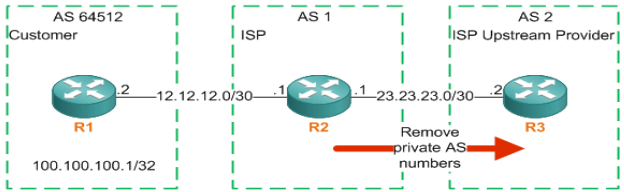
```
ip as-path access-list 1 permit ^200$
ip as-path access-list 1 permit ^100$
ip as-path access-list 1 permit ^500

ip as-path access-list 2 permit ^$

route-map AS_PATH_FILTER_OUT permit 10
match as-path 2

route-map AS_PATH_FILTER_IN permit 10
match as-path 1

router bgp 300
  address-family ipv4
    neighbor 100.20.30.2 route-map AS_PATH_FILTER_IN in
    neighbor 100.20.30.2 route-map AS_PATH_FILTER_OUT out
```

```
as-path-set AS_IN
  neighbor-is '300',
  ios-regex '^100$',
  ios-regex '^500'
end-set

as-path-set AS_OUT
  ios-regex '^$'
end-set

route-policy BGP_AS_FILTER_IN
  if as-path in AS_IN then
    pass
  else
    drop
  endif
end-policy

route-policy BGP_AS_FILTER_OUT
  if as-path in AS_OUT then
    pass
  else
    drop
  endif
end-policy

router bgp 200
neighbor 100.20.30.1
   address-family ipv4 unicast
   route-policy BGP_AS_FILTER_IN in
   route-policy BGP_AS_FILTER_OUT out
  !
!
neighbor 100.20.30.3
   address-family ipv4 unicast
   route-policy BGP_AS_FILTER_IN in
   route-policy BGP_AS_FILTER_OUT out
```

# Sistemas Autónomos Privados

- Rango de 64512 to 65534 para formato de 2-bytes.
- Al igual que las IPs privadas, estos no deben de ser anunciados en Internet.
- Responsabilidad de cada ISP o Enterprise de removerlos.

```
router bgp 200
 neighbor 100.20.30.1
  address-family ipv4 unicast
   remove-private-AS
  !
 !
 neighbor 100.20.30.3
  address-family ipv4 unicast
   remove-private-AS
```




```
router bgp 300
 address-family ipv4
  neighbor 100.20.30.2 activate
  neighbor 100.20.30.2 remove-private-as
  neighbor 100.20.30.2 route-map AS_PATH_FILTER_IN in
  neighbor 100.20.30.2 route-map AS_PATH_FILTER_OUT out
  neighbor 100.20.30.2 maximum-prefix 1000 warning-only
 exit-address-family
```

# Redes "Martians"

Redes privadas o que no están pensadas en ser ruteadas a nivel global.

https://ipgeolocation.io/resources/bogon.html

Se muestra un listado de las redes IPv4 e IPv6 que no deben de ser ruteadas.

Se pueden filtrar ocupando ACLs en conjunto con route-maps, filter-list o en el caso de XR con route-policy y prefix-set

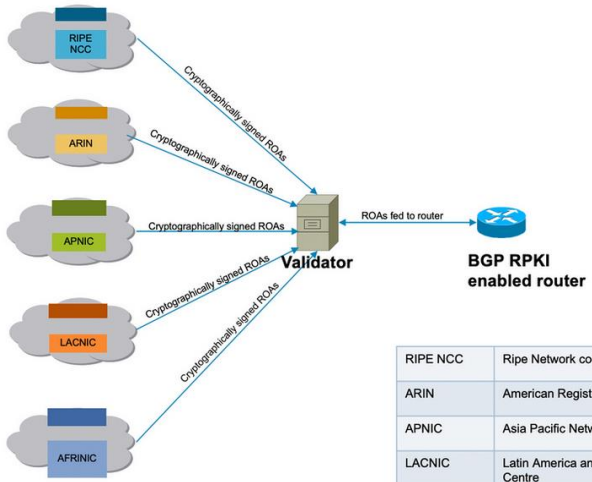
# Comportamiento eBGP IOS Vs. IOS-XR

- Por default, IOS es "inseguro" hablando de una vecindad eBGP.
- El OS IOS permitirá y enviará todos los prefijos a los vecinos eBGP sin que sea necesario aplicar filtrado a la salida o entrada de la vecindad con el AS remoto. Esto puede considerarse peligroso e inseguro.
- IOS-XR tiene con comportamiento que se apega mas a los estándares actuales de seguridad. IOS-XR requiere tener aplicado un RPL de entrada o salida permitiendo rutas específicas para aceptar o anunciar prefijos.

# Seguridad Avanzada en BGP

## Validación del AS de Origen

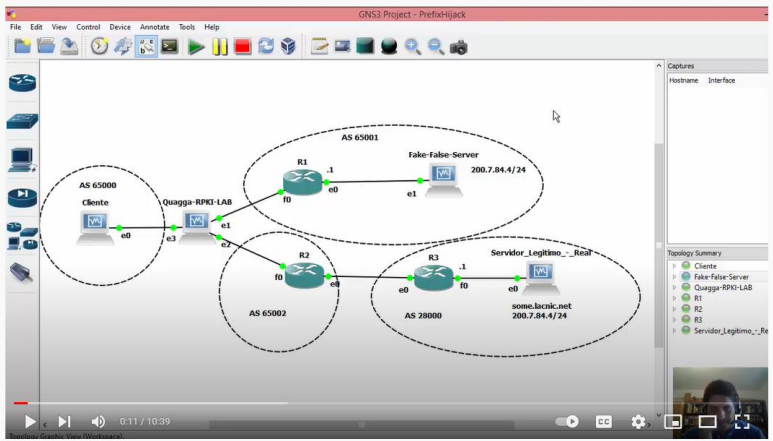
- Ocupa una infraestructura con un servidor RPKI (Resource Public Key Infrastructure)
- El servidor mantiene una relación de prefijos / AS válidos para el anuncio de rutas
- Actualmente los repositorios mantenidos con información de los certificados son: RIPE NCE, ARIN, APNIC, LACNIC y AFRINIC




| | |
|---|---|
| RIPE NCC | Ripe Network coordination center |
| ARIN | American Registry for Internet Numbers |
| APNIC | Asia Pacific Network Information Centre |
| LACNIC | Latin America and Caribbean Network Information Centre |
| AFRINIC | African Network Information Centre |

# Secuestro de Prefijos - RPKI - BGP

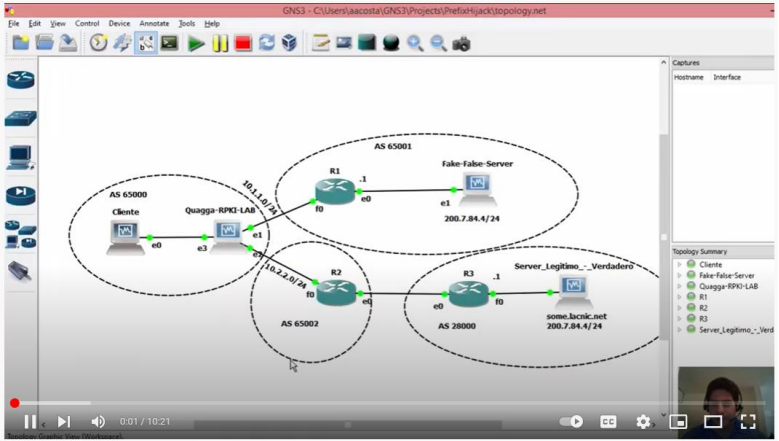
## Parte I




Demostracion de Secuestro de Prefijos - RPKI - BGP (parte 1/2)

[Link del video]

## Parte II

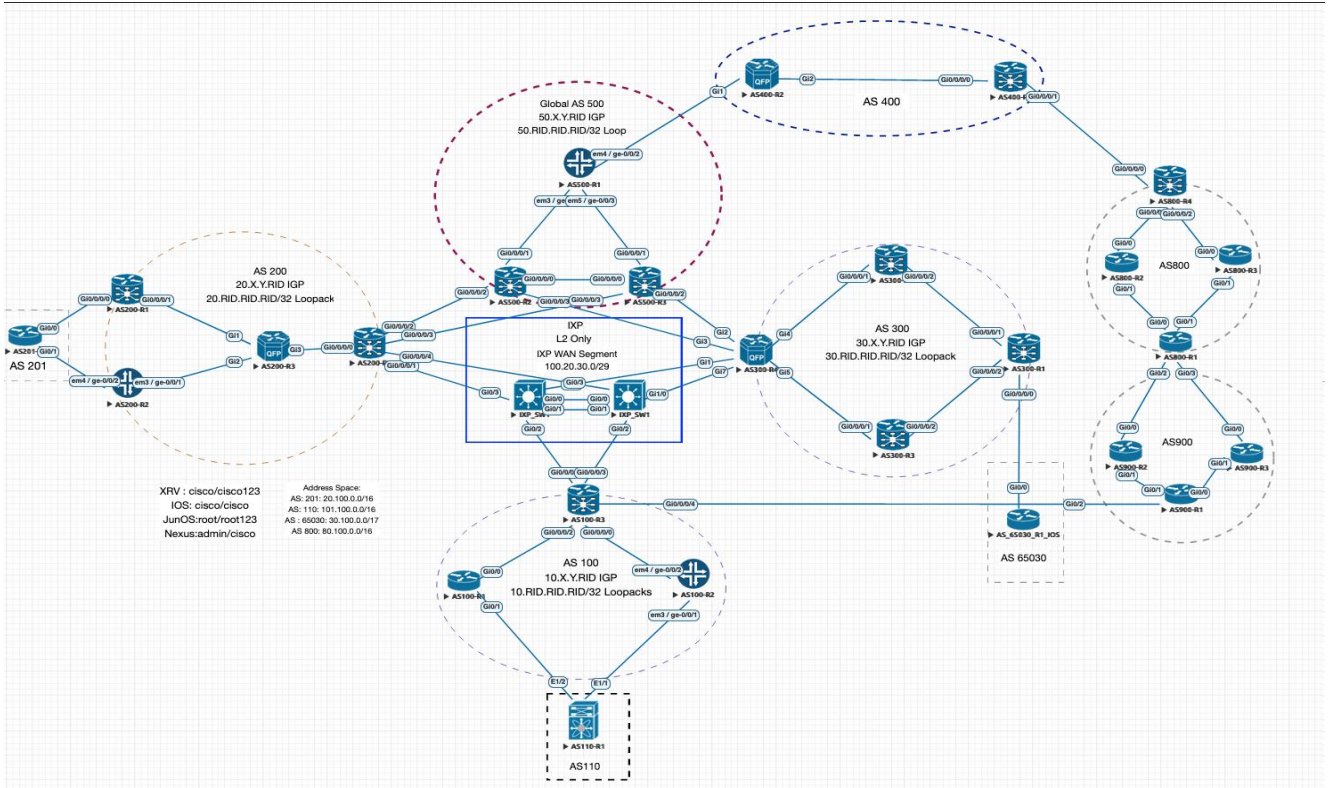



Demostracion de Secuestro de Prefijos - RPKI - BGP (parte 2/2).

[Link del video]

Entonces ¿debemos considerar la seguridad?

# Topología



# Descripción del Laboratorio

El Laboratorio consiste en X Sistemas autónomos utilizando diferentes plataformas incluidas IOS, IOS-XE, IOS-XR,  NxOs de Cisco y Junos VMx de Juniper para demostrar compatibilidad entre vendors. El layout del direccionamiento se encuentra en el diagrama topológico.

Descripción:

IXP conformado por los ASes 100,200,300. L2 IXP con redundancia nivel VLAN. No se permite trafico de transito entre estos ASes
AS 500 Representa unISP Tier2 conectado al backbone de internet.
ASes > 500 representan la red de global internet.
AS201 Cliente del AS200, tiene acceso a partial routing table+default route
AS301 Cliente del AS300, proveedor local tiene acceso a Internet mediate default route.
AS101 Cliente del AS100, utiliza mecanismos de TTL sec.
ASes 100,200,300, configurados con mecanismo de Maximum prefix para prevenir resource attack.

Todas las sesiones de EBGP tienen configurada Autenticación para efectos de Seguridad.

La Topología, archivo de simulación y configuraciones pueden ser descargadas en el siguiente link:

https://drive.google.com/drive/folders/1lPaXScc2kiH1ApCieplaWLsbuFK98aQo?usp=sharing

# Recursos de la sesión en la nube

Más información:
https://1drv.ms/f/s!Ajacm8dDgObUdF9r3JPHjzVCptI

Por favor espere un momento al terminar la session para encontrarles

# Polling Question 2

¿Le gustaría que hiciéramos más sesiones con LACNIC?

A. Sí, hagan la de RPKI
B. Sí, realicen muchas más
C. No es esencial
D. Otros temas o comentarios:____

# Resuelva sus dudas

Utilice el panel de Q&A o P&R para realizar sus preguntas

# Ask Me Anything- Sesión del evento

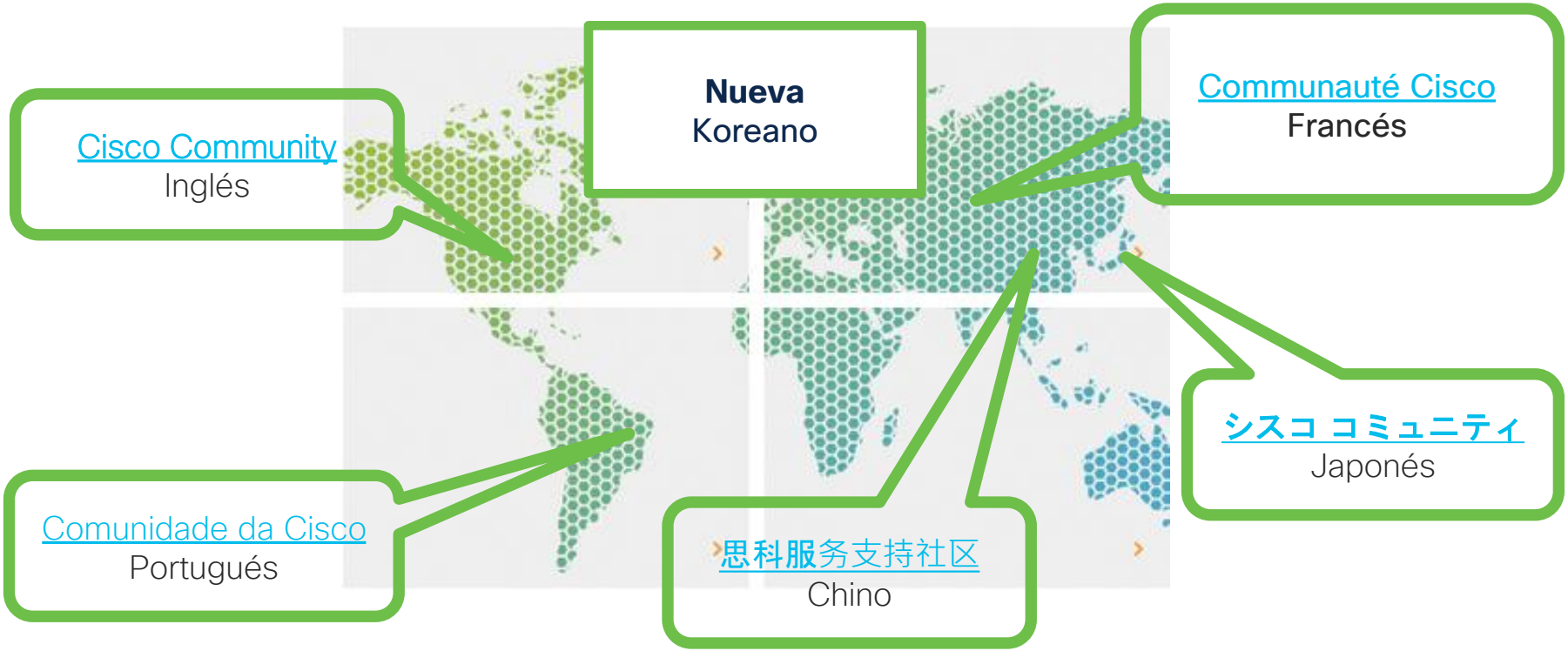
Hasta el Viernes 7 Septiembre, 2022

Con
Alejandro, Hector e Ignacio

https://bit.ly/ama-seguridad_bgp

# La Comunidad de soporte tiene otros Idiomas

Si habla Portugués, Japonés, Ruso, Chino o Inglés lo invitamos a participar en otro idioma.



# Lo invitamos a nuestros próximos eventos en Redes Sociales

## Twitter

- @CiscoTSLatam
- @cisco_spain
- @cisco_support
- @Cisco_LA

## Facebook

- Cisco TS- Latam
- Cisco España
- Cisco Latinoamérica
- CiscoCommunity

# Lo invitamos a nuestros próximos eventos en Redes Sociales

## YouTube

- CiscoLatam
- ciscocommunity

## App

- Cisco Technical Support

## LinkedIn

- Cisco Community

# ¡Nos interesa su opinión!

Por favor complete la encuesta,
aparecerá en la pantalla de su buscador



*¡Gracias por acompañarnos !*


CISCO