GLOBAL CYBER ALLIANCE

IDMX MEETING

# MANRS

## Seguridad en el Core de Internet

MANRS

GLOBAL CYBER ALLIANCE

IDMX MEETING

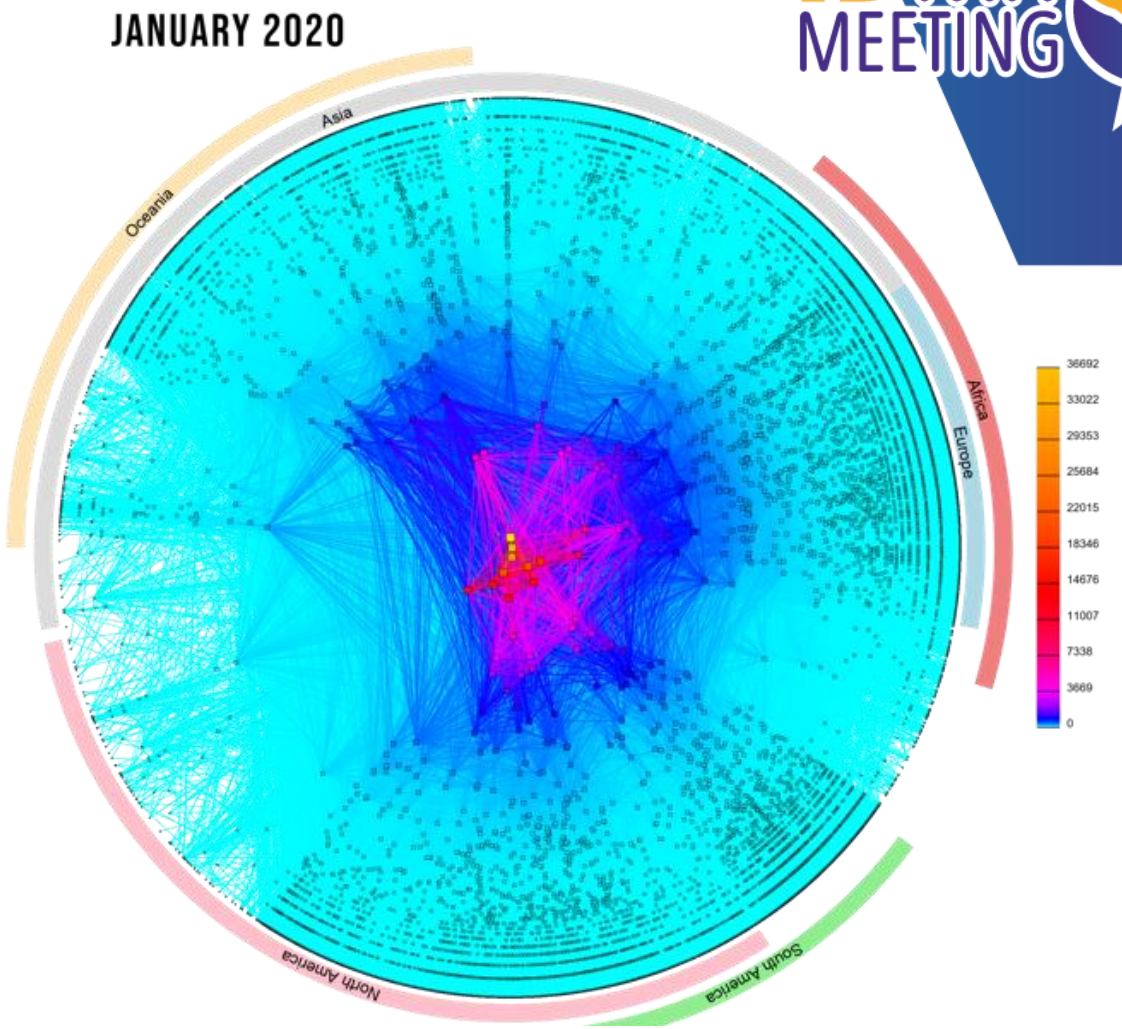
# El sistema actual de enrutamiento de Internet

**+78K** Sistemas Autónomos (AS) conforman juntos el Internet.

Cada AS construye su propio camino o ruta de Internet utilizando un lenguaje llamado **Border Gateway Protocol, o BGP.**

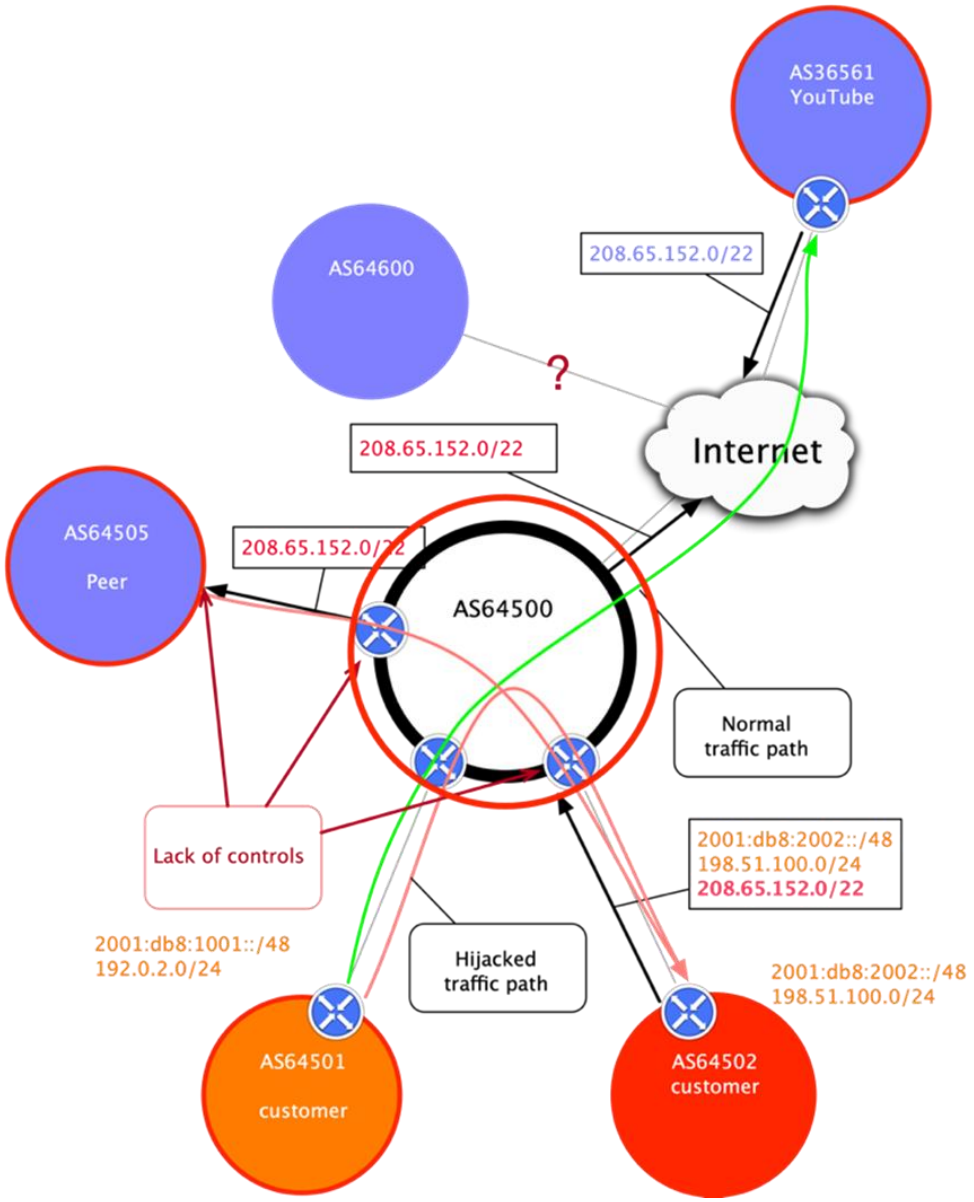
Hay más de 1,3 millones* de prefijos IP anunciados (rutas).

**BGP** es una base fundamental de Internet.




MANRS

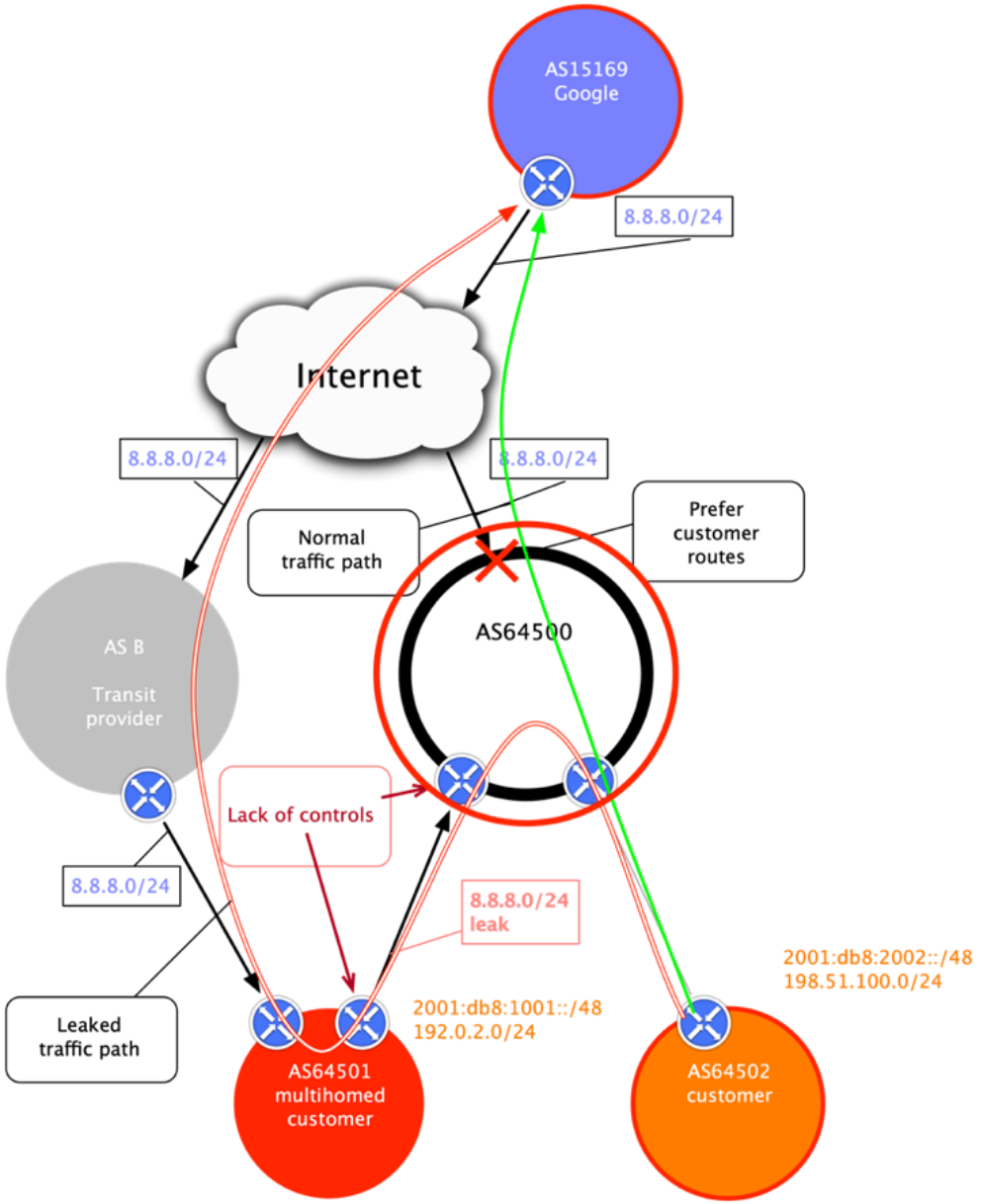
# Prefix/Route Hijacking




**Ejemplo:** El 2008 YouTube hijack; un intento de bloquear YouTube mediante el secuestro de rutas provocó que gran parte del tráfico de YouTube se cayera en todo el mundo.

**Solución:** Políticas de filtrado sólidas (las redes adyacentes deben fortalecer sus políticas de filtrado para evitar anuncios falsos).

# Route Leak



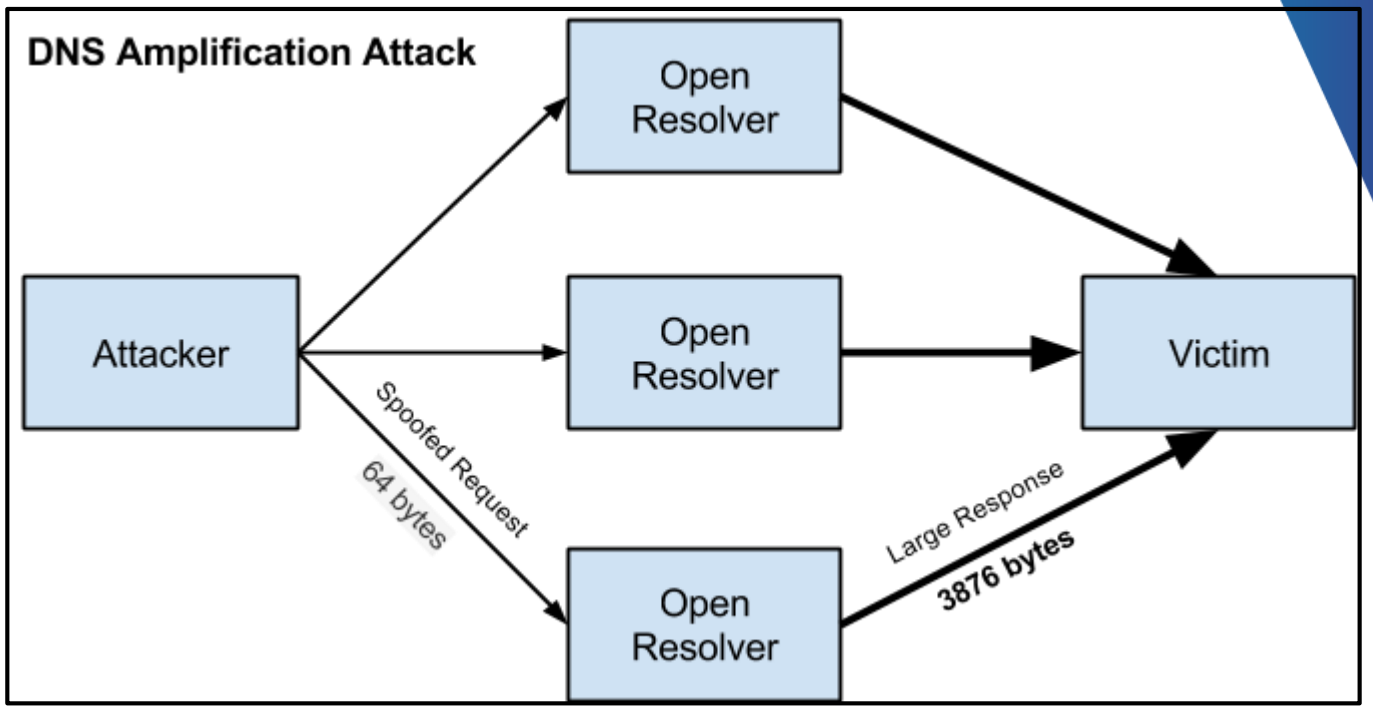

**Ejemplo:** 2015, Malaysia Telecom y Level 3, un importante proveedor de backbone. Malaysia Telecom dijo a una de las redes de Level 3 que era capaz de enviar tráfico a cualquier lugar de Internet.

Una vez que Level 3 decidió que la ruta a través de Malaysia Telecom parecía la mejor opción, desvió una gran cantidad de tráfico a Malaysia Telecom.

# IP Address Spoofing

**Ejemplo:** Ataque de amplificación de DNS. Al enviar múltiples solicitudes falsificadas a diferentes resolutores de DNS, un atacante puede solicitar que se envíen muchas respuestas del resolutor de DNS a un objetivo, mientras que solo usa un Sistema para atacar.

**Solución:** Validación de la dirección de origen: los sistemas para validación de la dirección de origen pueden ayudar a determinar si los usuarios finales y las redes de los clientes tienen direcciones IP de origen correctas (combinadas con el filtrado)



# MANRS: La solución existe

- **MANRS** = Mutually Agreed Norms for Routing Security
  - Normas Mutuamente Acordadas para la Seguridad del Enrutamiento
- **Misión:** "Hacer de Internet un lugar más seguro y confiable"
- **Enfoque:** "Comunidad global + Mejores prácticas técnicas“

Mejora la seguridad y confiabilidad del sistema global de enrutamiento de Internet, basado en la colaboración entre los participantes y la responsabilidad compartida de la infraestructura de Internet.

Digital Academy

# Acerca de MANRS

- Iniciativa liderada por la industria con 1300+ redes participantes para implementar las mejores prácticas y colaborar hacia una visión compartida de una infraestructura de enrutamiento segura.
- MANRS ofrece acciones concretas para operadores de red, IXPs, proveedores de CDN/nube y proveedores de equipos para reducir o eliminar las amenazas más comunes al enrutamiento.
- No hay cuotas para unirse a MANRS.
- MANRS cuenta con el apoyo de la ***Global Cyber Alliance.***

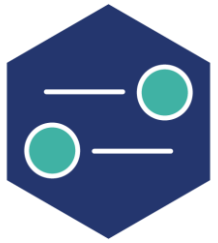
# Programas de MANRS

- MANRS para Operadores de Red
- MANRS para IXPs
- MANRS para CDNs y Proveedores de Nube
- MANRS para vendedores de equipos.

# Matrix de Acciones de MANRS

## Filtrado

*Asegúrate de la corrección de tus propios anuncios y de los anuncios de tus clientes a redes adyacentes con granularidad de prefijo y ruta AS*



## Anti-spoofing

*Activa la validación de direcciones fuente para al menos redes de clientes stub de homing único, tus propios usuarios finales e infraestructura*

## Coordinación

*Mantener información de contacto actualizada y accesible a nivel mundial*

## Información de enrutamiento

*Publica tu información para que otros puedan validar la información de rutas a escala global*

## Herramientas

*Proporcionar herramientas de monitorización y depuración para ayudar a otros*

## Promoción

*Fomentar activamente la adopción de MANRS entre compañeros, clientes y socios*

GLOBAL CYBER ALLIANCE

IDMX MEETING

# ¿Por qué te debe importar?

## Para ISPs

- Reducción de hijacks incidentales.
- Mejor comportamiento de peers.
- Mejora de reputación y confianza.
- Facilita resolución de incidentes.

## Para IXPs

- Infraestructura más estable.
- Aumento del valor del peering.
- Mejora en gestión de miembros.

## Para Ingenieros

- Cumplimiento operativo.
- Menos incidentes NOC.
- Validación profesional (MANRS, certificaciones técnicas).

MANRS

# Acción 2 Filtrado

## Prevención de la propagación de información de enrutamiento incorrecta

GLOBAL CYBER ALLIANCE

IDMX MEETING

MANRS, en lo referente a Filtrado, tiene como objetivo el evitar la propagación de enrutamiento incorrecto, se espera que los Operadores de Red realicen las siguientes acciones relevantes:

- Definir una política de enrutamiento clara.
- Implementar un sistema que garantice la corrección de sus propios anuncios y los anuncios de sus clientes adyacentes con prefijo y granularidad de ruta de AS.
- Verificar la exactitud de los anuncios de sus clientes.
- Verificar específicamente que el cliente posee legítimamente el ASN y el espacio de direcciones que anuncia.

MANRS

# Filtrado de rutas BGP

Es un proceso muy importante a fin de garantizar la estabilidad de nuestro AS y los AS vecinos.

- **Filtrado de Entrada:** es aplicado a rutas aprendidas.
  - Entonces las rutas no se incluyen en nuestra tabla de ruteo.
- **Filtrado de Salida:**
  - Las rutas no se incluyen en las tablas de ruteo remotas.

Razones:

- **Económicas** – Ejem: Transit IPS vs peering.
- **Seguridad** – Ejem: sólo rutas asignadas a nuestros clientes.
- **Técnicas** – Ejem: problemas de memoria

# Filtrado de rutas BGP

- Existen dos grandes tipos de filtros en BGP

# Filtros con Prefix-list

| Access-list (ACL) | Prefix-list |
| --- | --- |
| access-list <nro_access-list> permit\|deny ip <prefijo> <máscara de wildcard> | ip prefix-list <nombre_prefix-list> <nro_seq> permit\|deny <red/prefijo> [**ge** length \| **le** length ] |
| access-list 101 permit ip 10.0.0.0 0.255.255.255<br>access-list 101 permit ip 203.0.113.0 0.0.0.255<br>access-list 101 permit ip 192.0.2.0 0.0.0.255 | ip prefix-list Entrada seq 5 deny 10.0.0.0/8 le 32<br>ip prefix-list Entrada seq 10 deny 203.0.113.0/24 le 32<br>ip prefix-list Entrada seq 15 permit 0.0.0.0/0 le 32 |

Cómo se aplica el prefix-list a la sesión BGP?

neighbor <ip-address|peer-group> prefix-list <nombre_prefix-list> in|out

# Ejemplos: Creando filtrado Bogons IPv4

```
ip prefix-list BOGONS_v4 deny 0.0.0.0/8 le 32
ip prefix-list BOGONS_v4 deny 10.0.0.0/8 le 32
ip prefix-list BOGONS_v4 deny 100.64.0.0/10 le 32
ip prefix-list BOGONS_v4 deny 127.0.0.0/8 le 32
ip prefix-list BOGONS_v4 deny 169.254.0.0/16 le 32
ip prefix-list BOGONS_v4 deny 172.16.0.0/12 le 32
ip prefix-list BOGONS_v4 deny 192.0.2.0/24 le 32
ip prefix-list BOGONS_v4 deny 192.88.99.0/24 le 32
ip prefix-list BOGONS_v4 deny 192.168.0.0/16 le 32
ip prefix-list BOGONS_v4 deny 198.18.0.0/15 le 32
ip prefix-list BOGONS_v4 deny 198.51.100.0/24 le 32
ip prefix-list BOGONS_v4 deny 203.0.113.0/24 le 32
ip prefix-list BOGONS_v4 deny 224.0.0.0/4 le 32
ip prefix-list BOGONS_v4 deny 240.0.0.0/4 le 32
```

# Ejemplos: Creando filtrado Bogons IPv6

- ipv6 prefix-list BOGONS_v6 deny ::/8 le 128
- ipv6 prefix-list BOGONS_v6 deny 100::/64 le 128
- ipv6 prefix-list BOGONS_v6 deny 2001:2::/48 le 128
- ipv6 prefix-list BOGONS_v6 deny 2001:10::/28 le 128
- ipv6 prefix-list BOGONS_v6 deny 2001:db8::/32 le 128
- ipv6 prefix-list BOGONS_v6 deny 2002::/16 le 128
- ipv6 prefix-list BOGONS_v6 deny 3ffe::/16 le 128
- ipv6 prefix-list BOGONS_v6 deny fc00::/7 le 128
- ipv6 prefix-list BOGONS_v6 deny fe80::/10 le 128
- ipv6 prefix-list BOGONS_v6 deny fec0::/10 le 128
- ipv6 prefix-list BOGONS_v6 deny ff00::/8 le 128

# Aplicando el prefix-list

```
router bgp 64500
 no synchronization
 neighbor 203.0.113.255 remote-as 64501
 neighbor 203.0.113.255 prefix-list BOGONS_v4 in
 neighbor 203.0.113.255 prefix-list BOGONS_v4 out
 no auto-summary
 !
 neighbor 2001:db8:1000:FFFE::B prefix-list
BOGONS_v6 in
  neighbor 2001:db8:1000:FFFE::B prefix-list
BOGONS_v6 out
```

```
router bgp 64500
 address-family ipv4
  neighbor 203.0.113.251 prefix-list BOGONS_v4 in
  neighbor 203.0.113.251 prefix-list BOGONS_v4 out
 !
 address-family ipv6
  neighbor 2001:db8:1000:FFFD::B prefix-list
BOGONS_v6 in
  neighbor 2001:db8:1000:FFFD::B prefix-list
BOGONS_v6 out
```

# Filtros por AS-PATH

El filtro actúa según el **camino** hecho por los prefijos

**Dos Pasos:**

1. Crear sentencia con expresión regular.

   *ip as-path acces-list* **<nro_filtro>** *permit | deny* **<regexp>**

2. Aplicar filtro

   *Neighbor* **<IP_neighbor>** *filter-list* **<nro_filtro>** ***in | out***

# Ejemplos: Filtrado Bogons con ASN (AS-PATH)

- bgp as-path access-list bogon-asns deny 23456
- bgp as-path access-list bogon-asns deny 64496-131071
- bgp as-path access-list bogon-asns deny 4200000000-4294967295

- ip as-path regex-mode asn

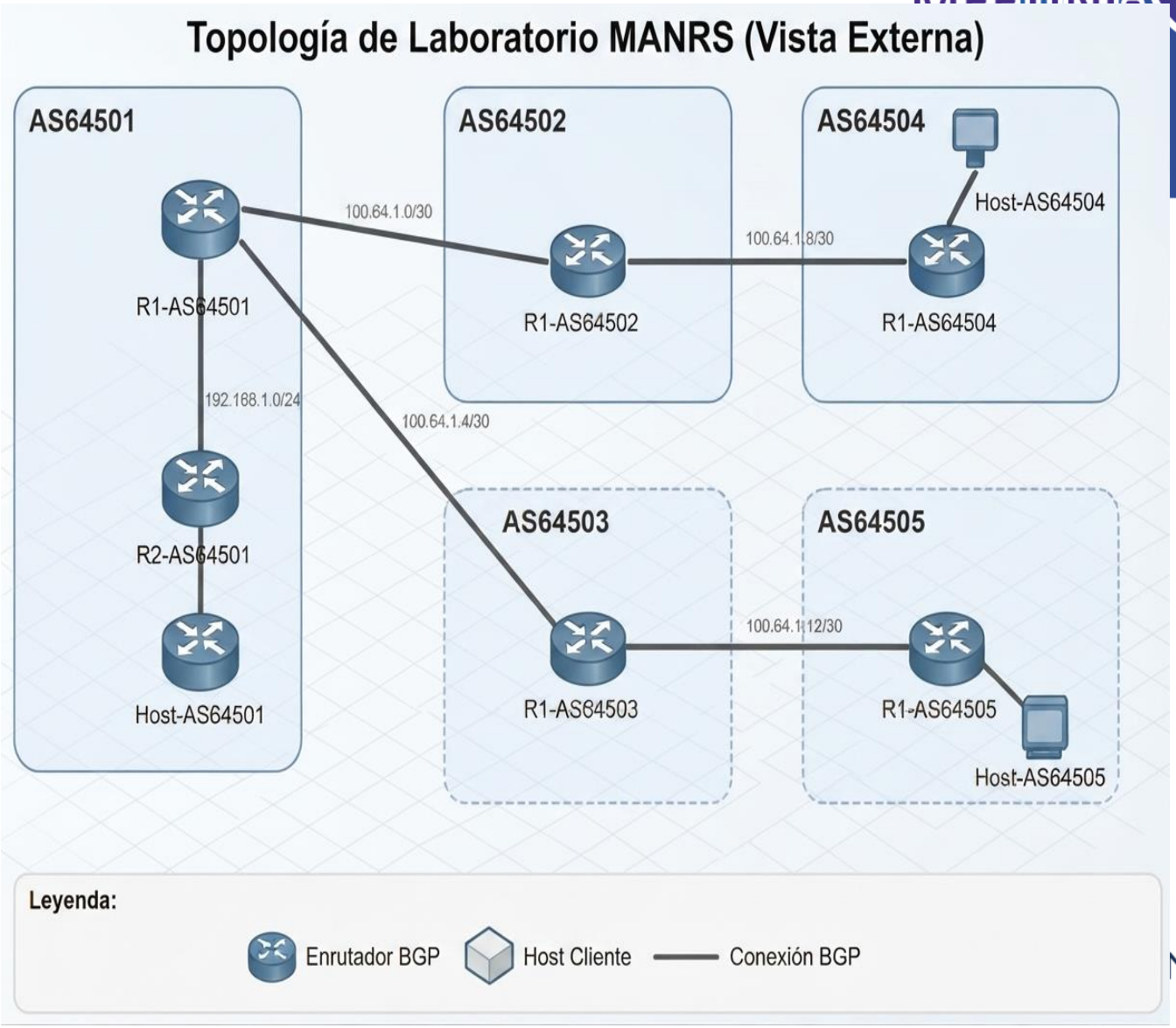
- ip as-path access-list bogon-asns permit _0_ any
- ip as-path access-list bogon-asns permit _23456_ any
- ip as-path access-list bogon-asns permit _[64496-64511]_ any
- ip as-path access-list bogon-asns permit _[65536-65551]_ any
- ip as-path access-list bogon-asns permit _[64512-65534]_ any
- ip as-path access-list bogon-asns permit _[4200000000-4294967294]_ any
- ip as-path access-list bogon-asns permit _65535_ any
- ip as-path access-list bogon-asns permit _4294967295_ any
- ip as-path access-list bogon-asns permit _[65552-131071]_ any

- route-map Import-Peer deny 7
- match as-path bogon-asns
- !

# MANRS LAB

Prácticas de laboratorio diseñadas para implementar las acciones recomendadas por MANRS (Mutually Agreed Norms for Routing Security).

MANRS_LAB



GLOBAL CYBER ALLIANCE

IDMX MEETING

- LEARN MORE: https://www.manrs.org
- FOLLOW US:
- /RoutingMANRS

- Siguenos @lacdigitalacademy
- **LAC Digital Academy**

MANRS

# Gracias.

Emmanuel Serrano

Email:

emmanuel.serrano@lacdigitalacademy.net

manrs.org

Digital Academy