MANRS

Normas Mutuamente Acordadas para el Enrutamiento Seguro en Internet

Acción 1 - Filtrado

Agenda Sesion 1

- Bienvenida
- Repaso de MANRS
- Acción 1 – Filtrado
- Caso de Operador de Red de México
- Preguntas y Respuestas

MANRS

Normas Mutuamente Acordadas para Enrutamiento Seguro en Internet

Las Normas comúnmente acordadas para la seguridad del enrutamiento (MANRS) es una iniciativa comunitaria organizada por Internet Society, que tiene como objetivo mejorar la seguridad y la resiliencia del sistema de enrutamiento global.

Es una colaboración entre operadores implementando mejores prácticas que permiten un enrutamiento más seguro y confiable para todos.

ANUIES ANUIES - TIC cudi Corporación Universitaria para el Desarrollo de Internet A.C. Internet 2 - México Red CLARA Internet Society lacnic NIC MÉXICO

MANRS

Normas Mutuamente Acordadas para Enrutamiento Seguro en Internet

El taller consta de **6 sesiones; 5 virtuales y uno presencial**

Sesión 1: Jueves 11 y 25 de abril – Introducción a MANRS

Sesión 2: Jueves 23 de mayo – MANRS: Acción 1 – Filtrado

Sesión 3: Jueves 13 de junio – MANRS: Acción 2 – Anti-Spoofing

Sesión 4: Jueves 11 de julio – MANRS: Acción 3 – Coordinación

Sesión 5: Jueves 22 de agosto – MANRS: Acción 4 – Validación Global

La conclusión será con **una sesión presencial** en el marco de los eventos:

- Encuentro TICAL 2019, 2 – 4 de septiembre de 2019 en Cancún, México.
- Encuentro ANUIES-TIC 2019, 2 de octubre de 2019 en la UANL, Nuevo León, México.

ANUIES · ANUIES - TIC · cudi Corporación Universitaria para el Desarrollo de Internet A.C. Internet 2 - México · Red CLARA · Internet Society · lacnic · NIC MÉXICO

Silvia Nora Chávez Morones
(CUDI, México)

Ingeniera en Sistemas Computacionales con posgrado en Redes de Computadoras, egresada de la Universidad Tecnológica de México.
Desde hace 15 años se ha desarrollado como Operador e Ingeniero de Red dentro del Centro de Operación de la Red CUDI.
Encargada del buen funcionamiento en el NOC para el monitoreo, detección y solución de fallas dentro del backbone, así como de las mejoras en la configuración de cada uno de los equipos que a este lo constituyen.
Participa en la toma de decisiones para promover, desarrollar e implementar las conexiones de diversas universidades e institutos de investigación que se conectan a Red CUDI, dando de igual manera el soporte debido a estos enlaces.
Colaboró dentro del NOC de la Red del Caribe (C@ribNET - CKLN) y ha participado también en diversos proyectos para lograr la interconexión entre la Red CUDI y RedNIBA (SCT), así como con las diferentes NRENs internacionales.
Ha colaborado en LACNIC y MEXNOG apoyando el buen uso de BGP en las redes académicas.
Actualmente también forma parte del NOC de Red CLARA y gestionará dentro del NOC para la red NICTÉ (SCT).

Carmen Denis Polanco
(Yucatán, México)

Cuenta con 25 años de experiencia en tecnologías para la interconexión de redes e Internet.

Ha coordinado proyectos de Conectividad de Redes LAN, MAN y WAN, Internet, IPv6 y MANRS en la Universidad Autónoma de Yucatán, México.

Actualmente colabora en el proyecto MANRS para Operadores de Red de Universidades con asociaciones académicas de México y de Latinoamérica: ANUIES, CUDI y Red Clara, en colaboración ISOC, LACNIC y NICMX; embajadora de RIPE Atlas para el despliegue en Universidades de México.

Colabora con ANUIES, CUDI y NIC México para impulsar IPv6 en Universidades del Sureste de México.

MANRS

MANRS
Breve repaso de la sesión 1

MANRS

El taller consta de **6 sesiones: 5 virtuales y uno presencial.** **OBJETIVOS**

- Despertar conciencia e impulsar acciones para mejorar la seguridad y la coordinación en el ruteo global de Internet reduciendo los problemas que afectan a la estabilidad y resiliencia del servicio.
- Proveer un marco para que los operadores de red de universidades entiendan y se ocupen de los temas relativos a la resiliencia y seguridad del sistema de enrutamiento global de Internet.
- Promover una cultura de responsabilidad colectiva para la resiliencia y seguridad del sistema de ruteo global de Internet.
- Guiar a los operadores de red de universidades en la utilización de RPKI, filtrados y otras técnicas que ayudan a prevenir problemas de ruteo.
- Demostrar la capacidad de los operadores de red de universidades para resolver los problemas de seguridad y resiliencia de Internet.

MANRS

Antecedentes

Todos los que operan una red son corresponsables de la estabilidad del ruteo global: es una responsabilidad compartida.

Los Operadores de Red de las Universidades no quedamos excentos de esa responsabilidad.

Una mala configuración de una red no solo afecta el servicio para sus usuarios, sino que puede afectar a otros operadores en cualquier parte del mundo.

MANRS BGP basado en la confianza

Internet, con cerca de 35 años de edad, se ha convertido en un servicio crítico y para su operación conserva el protocolo BGP (Border Gateway Protocol) para la interconexión de redes.

BGP se basa totalmente en la confianza entre redes.

BGP: es uno de los protocolos fundamentales que tienen el potencial de afectar la estabilidad y seguridad del Core de Internet.

MANRS

Incremento en los incidentes de enrutamiento

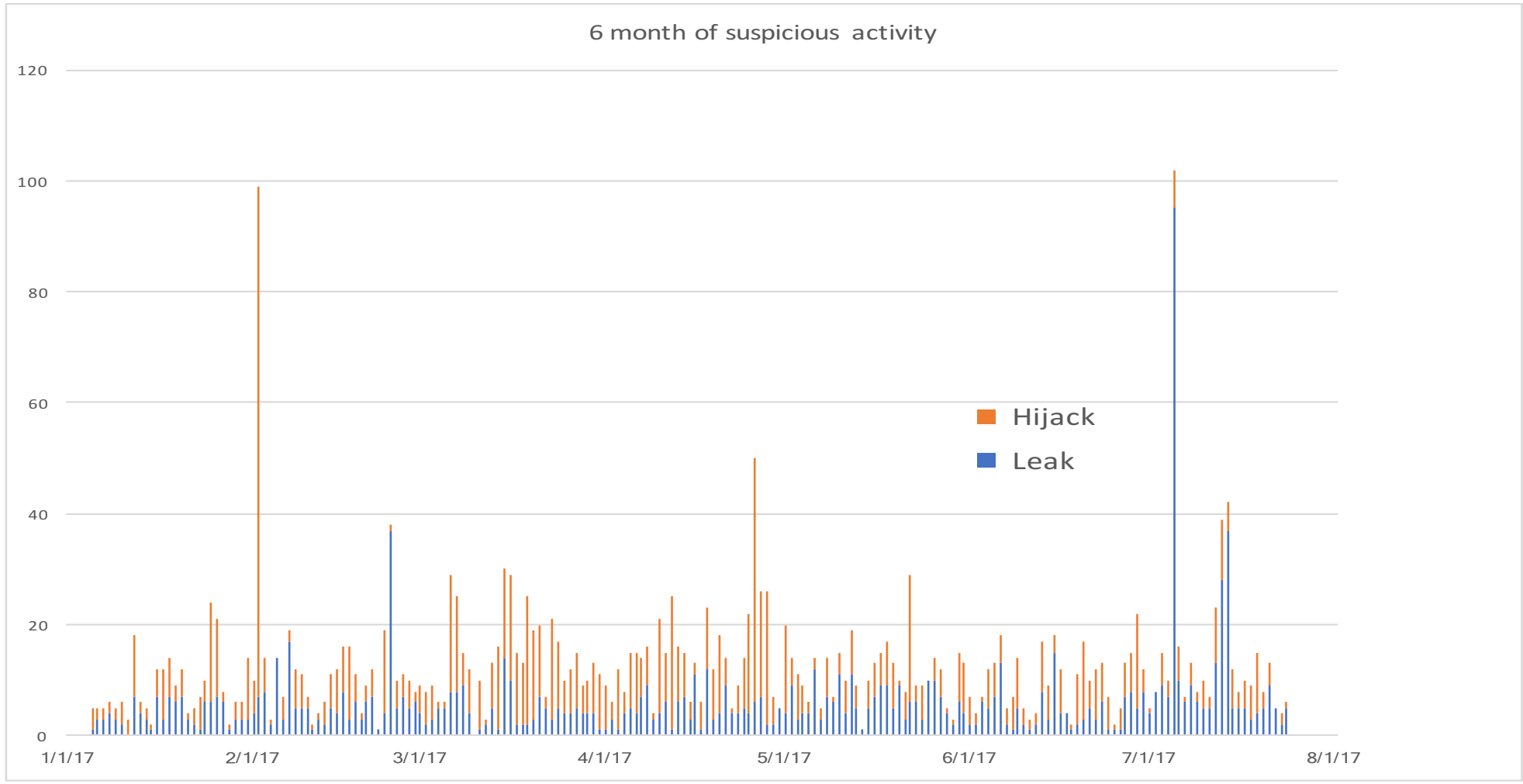
El enrutamiento inseguro es uno de las caminos más comunes para las amenazas maliciosas.

Los ataques pueden tomar desde horas hasta meses para reconocerlos.

Los errores involuntarios pueden llevar a países enteros fuera de línea, mientras que los atacantes pueden robar los datos de un individuo o mantener a la red como rehén de una organización.

Solo en 2017, 14,000 interrupciones o ataques de enrutamiento, como secuestro, filtraciones y suplantación de identidad.

No hay día sin un incidente de enrutamiento



http://bgpstream.com/

La Solución: Mutually Agreed Norms for Routing Security (MANRS)

Normas Mutuamente Acordadas para el Enrutamiento Seguro en Internet

Mutually Agreed Norms for Routing Security

MANRS es una iniciativa comunitaria organizada por Internet Society, que tiene como objetivo mejorar la seguridad y la estabilidad del sistema del enrutamiento global. Es una forma en que los operadores de red trabajen juntos para crear un nuevo estándar de un enrutamiento más seguro y resistente.

MANRS

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

Actualmente más de 150 operadores de red se han suscrito el manifiesto.

MANRS define cuatro acciones concretas que los Operadores de Red deben implementar:

Filtrado: evita la propagación de información del enrutamiento incorrecto

Asegure la corrección de sus propios anuncios y anuncios de sus clientes a redes adyacentes con prefijo y granularidad AS-PATH

Anti-spoofing: prevención del tráfico con direcciones IP de origen falsificadas

Habilite la validación de la dirección de origen para al menos las redes de clientes, sus propios usuarios finales e infraestructura

Coordinación: facilitar la comunicación y coordinación operativa global entre los operadores de red

Mantenga la información de contacto actualizada a nivel mundial en bases de datos de enrutamiento comunes

Validación global: facilitar la validación de la información del enrutamiento a nivel mundial

Publica tus datos para que otros puedan validar.

¿Porqué MANRS?
Redes de Educación e Investigación

- Mostrar liderazgo técnico y diferenciarse de los ISPs comerciales.
- Para ayudar a resolver los problemas de la red global. Las Redes Nacionales de Educación e Investigación (RNEI) son a menudo los primeros en adoptar nuevos desarrollos.
- Liderar con el ejemplo y mejorar la seguridad de enrutamiento para todos.
- Promover el cumplimiento de MANRS a clientes y proveedores centrados en la seguridad.

https://www.manrs.org/isps/participants/

Network Operator Participants

Network operators across the globe have already committed to the MANRS initiative and implemented the Actions defined in the MANRS document.

Search Participants

SEARCH

COPY CSV PRINT Show 10 entries

Organization Name	Areas Served	ASNs	Action 1 - Filtering	Action 2 - Anti-Spoofing	Action 3 - Coordination	Action 4 - Global Validation
.pt	PT	199993	✔	✔	✔	✔
1&1 IONOS	EU US	8560	✔	✔	✔	✔
AARNet Pty Ltd	AU	7575	✔	✔	✔	✔
Adam	ES	15699	✔	✔	✔	✔
Algar Telecom	BR	16735 53006 27664	✔		✔	✔
Altibox	NO	29695	✔	✔	✔	✔
Amsio BV	NL	8315	✔	✔	✔	✔
Andorra Telecom	AD	6752	✔	✔	✔	✔
Anura	AR	52275	✔	✔	✔	
Anycast.io	DE NL GB	34868	✔	✔	✔	✔
Organization	Areas	ASNs	Action 1 - Filtering	Action 2 - Anti-Spoofing	Action 3 - Coordination	Action 4 - Global Validation

Showing 1 to 10 of 155 entries

Previous 1 2 3 4 5 ... 16 Next

INDIANA UNIVERSITY
FULFILLING the PROMISE

Testimonial from Indiana University

Indiana University is committed to following and promoting the principles of the MANRS initiative. The security and stability of Internet routing is a responsibility shared by all organizations. We hope to lead by example and encourage a commitment to these principles.

Seth Garrett
Principal Network Engineer, Indiana University

RedIRIS

Testimonial from RedIRIS

Since its beginnings, RedIRIS has striven to maintain a secure and resilient network, deploying the most updated best practices and, as a National R&E Network, disseminating them to its customers in order to get from them a commitment of deploying these best practices in their networks as well. Adhering to MANRS initiative reinforces this position.

Maribel Cosin
Senior Network Engineer, RedIRIS

MANRS
@RoutingMANRS

A very warm welcome to our new #MANRS member Universidad Autónoma de Yucatán @uady_mx. ¡Bienvenido a bordo! Thanks for supporting #Routing #Security ow.ly/xt1z50jDqdu

12:29pm · 9 Nov 2018 · Hootsuite Inc.

MANRS
@RoutingMANRS

Hello @Google :)

Translate Tweet

> **Donald Clark** @donaldsclark
> @Google is now a @RoutingMANRS member - manrs.org/isps/participa...
>
> "From 2019-Q2 we will be applying route filters to all our BGP sessions."

1:59am · 27 Feb 2019 · TweetDeck

Network Operator Participants

Network operators across the globe have already committed to the MANRS initiative and implemented the Actions defined in the MANRS document.

← Go back

Google LLC

Google LLC Website

https://www.google.com

Areas Served: US

ASNs

15169

https://www.manrs.org/isps/participants/entry/659/

MANRS
@RoutingMANRS

#Microsoft joins the #MANRS initiative that takes meaningful action to keep the #Internet safe for everyone by improving the #routing resiliency of the Internet manrs.org/2019/05/micros...

Translate Tweet

7:05am · 22 May 2019 · Hootsuite Inc.

https://www.manrs.org/isps/participants/entry/698/

MANRS

Enfrentemos en conjunto …

- Los operadores de red tienen la responsabilidad de garantizar una infraestructura de enrutamiento segura y robusta a nivel mundial.
- La seguridad de la red depende de una infraestructura de enrutamiento que elimine a los malos actores: configuraciones erróneas y accidentales que puedan causar estragos en Internet.
- Cuantos más operadores de red trabajen juntos, menos incidentes habrá y menos daño podrán hacer.

lacnic

Internet Society

lacnog

NIC MÉXICO

Red CLARA

ANUIES

ANUIES - TIC

cudi
Corporación Universitaria para el Desarrollo de Internet A.C.
Internet 2 - México

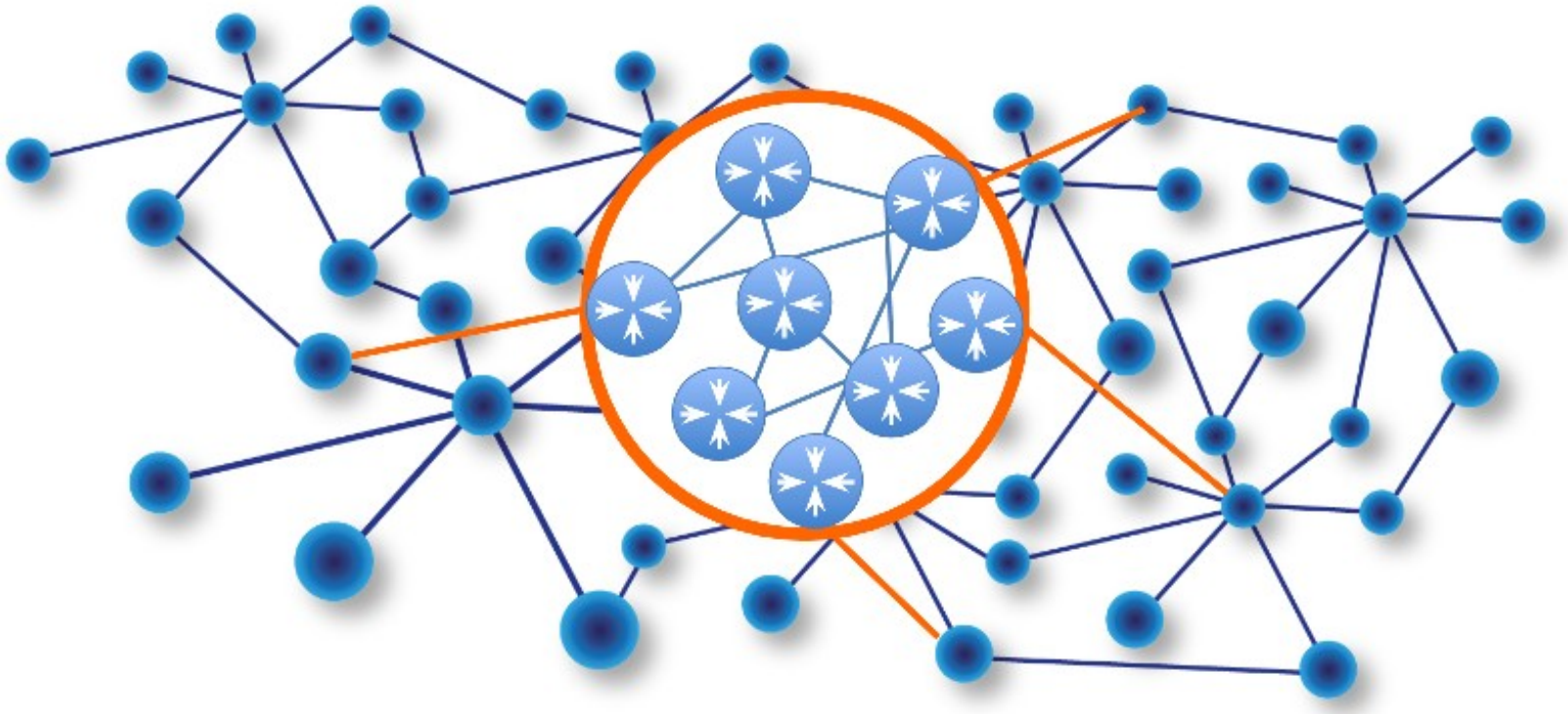
MANRS

Action 1. Filtering

Evitar la propagación de información de enrutamiento incorrecta.

BGP Repaso

BGP (Border Gateway Protocol)



MANRS

Interconexión de Sistemas Autónomos

MANRS

BGP - Selección del mejor camino

1. Evaluación del NH

   El NH es alcanzable?

   SÍ → Evalúa synchronization

   NO → Ruta se descarta

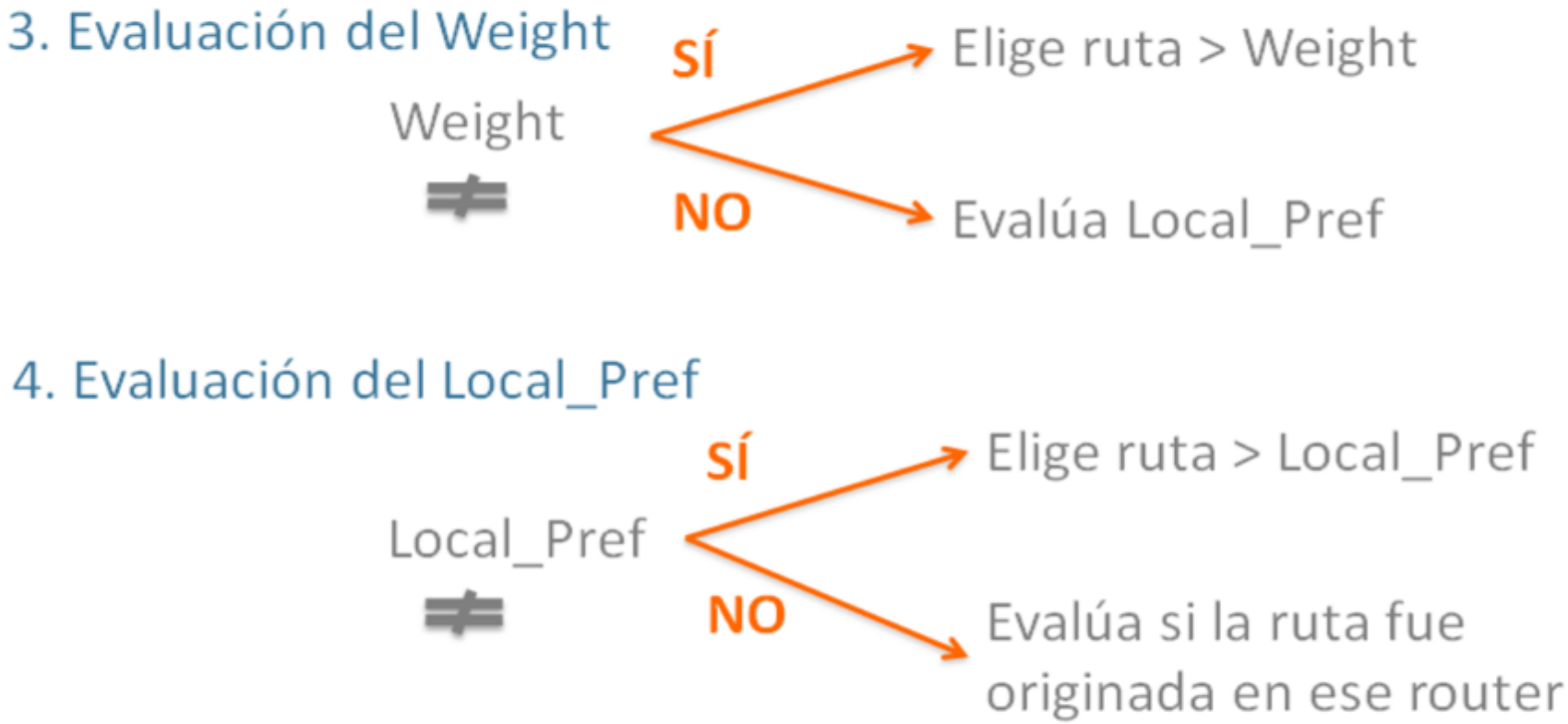
2. Evaluación de synchronization

- iBGP
- Synch habilitado
- No hay entrada en la tabla de ruteo

   SÍ → Ruta se descarta

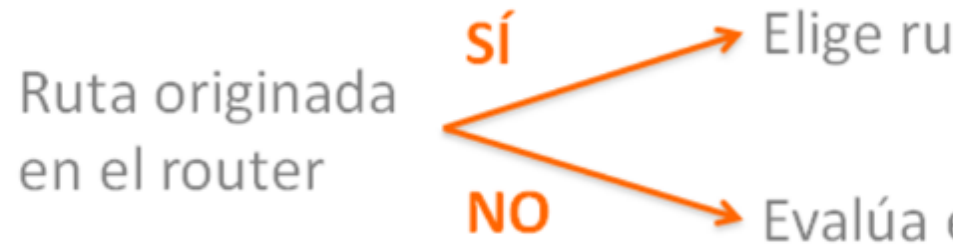
   NO → Continúa el proceso de evaluación

BGP - Selección del mejor camino



BGP - Selección del mejor camino

5. Origin de la ruta



6. Evaluación del AS_Path

BGP - Selección del mejor camino

7. Evaluación de Origin

Origin ≠

SÍ → Elige ruta < origin (i < e < ?)

NO → Evalúa MED

8. Evaluación del MED

MED ≠

SÍ → Elige ruta < MED

NO → Evalúa cómo fue aprendida la ruta

BGP - Selección del mejor camino

9. Evaluación de cómo fue aprendida la ruta

10. Evaluación de la métrica del NH

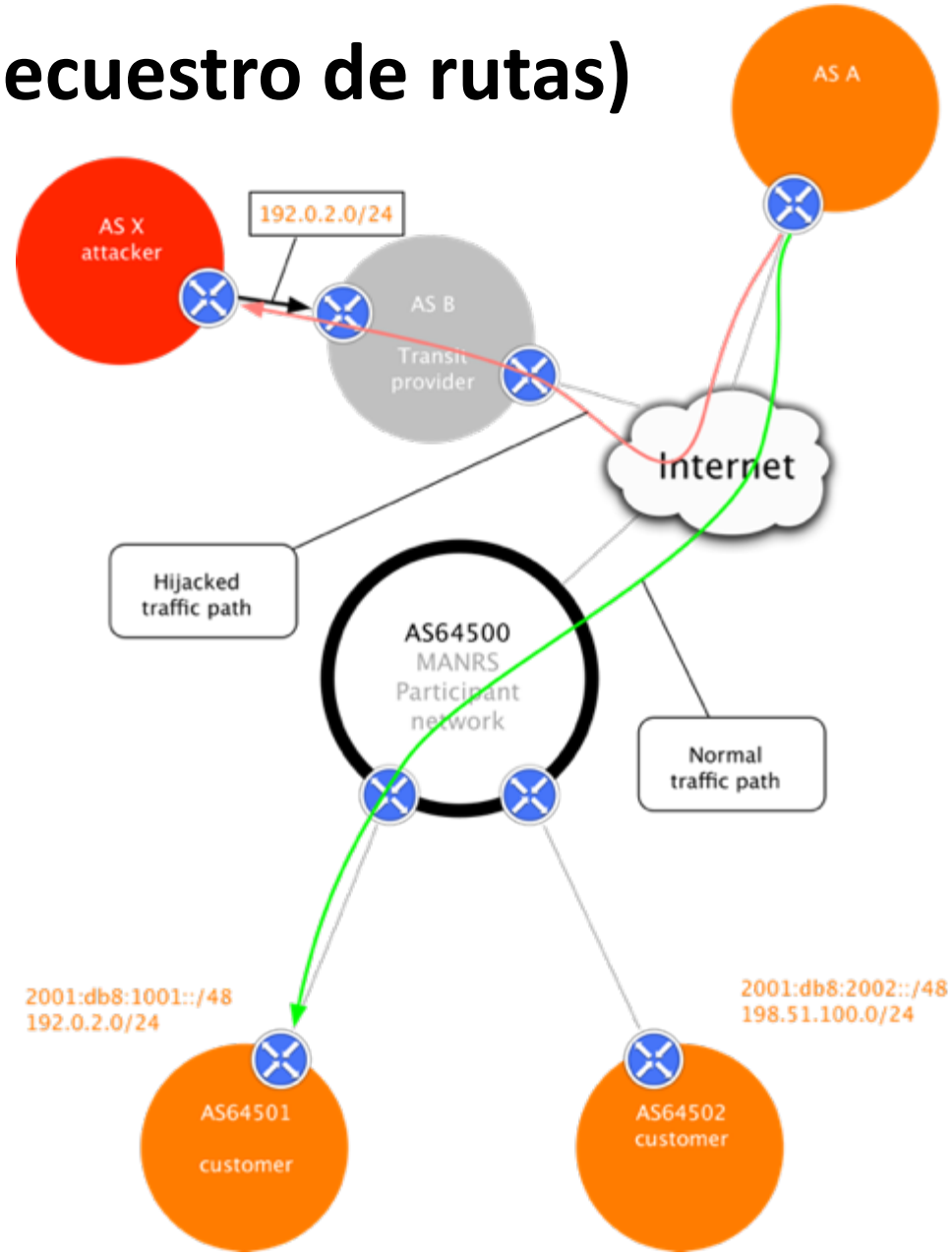
MANRS

BGP Problems

- El Secuestro de BGP o el BGP Hijacking, ocurre cuando de manera malintencionada, se anuncian prefijos de otras redes hacia los equipos vecinos, esto con el fin de disfrazar y engañar a los sistemas para redirigir el tráfico hacia él. Esto impacta de manera crítica a los sistemas autónomos (AS) ya que, si esta información falsa es aceptada, pueden comprometer el RoadMap del protocolo pues este puede ir propagándose a través de la red.

Las amenazas: **Prefix/Route Hijacking (secuestro de rutas)**

Evento	Prefix/Route Hijacking (secuestro de rutas)
Descripción	Un operador de red o atacante se hace pasar por otro operador de red, simulando que un servidor o una red es su cliente.
Repercusión	Los paquetes se reenvían al lugar equivocado y pueden provocar ataques de denegación de servicio (DoS) o intercepción de tráfico.
Solución	Políticas de filtrado más fuertes.

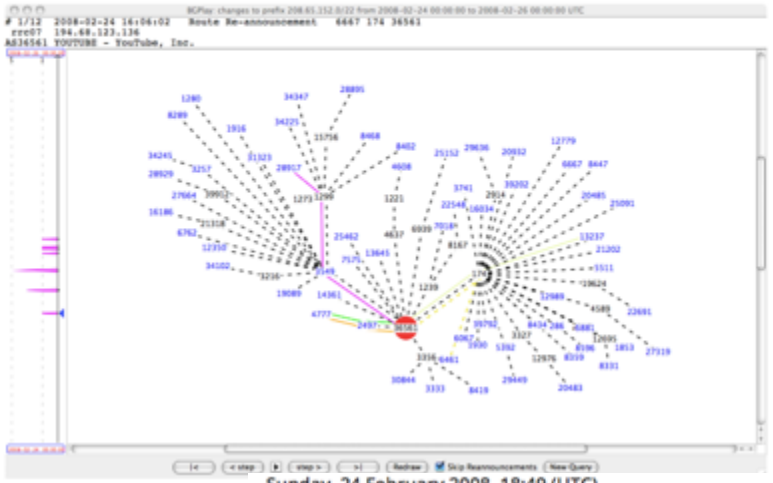


Example: *The 2008 YouTube hijack; an attempt to block Youtube through route hijacking led to much of the traffic to Youtube being dropped around the world (https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)*

YouTube Hijacking: A RIPE NCC RIS case study

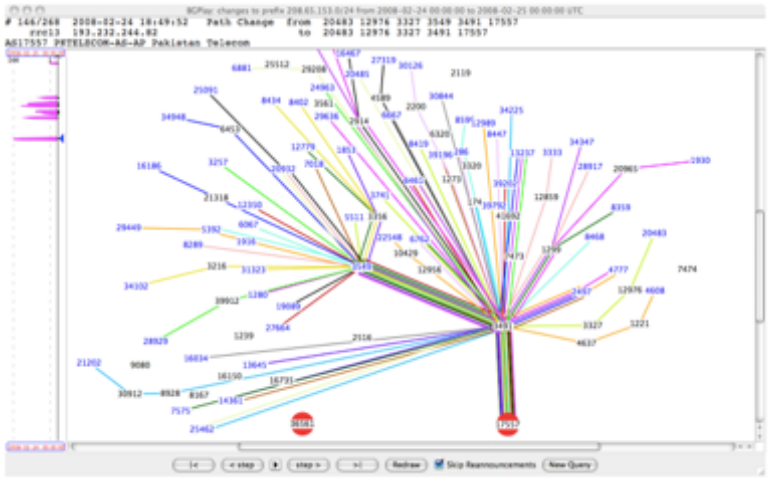
Before, during and after Sunday, 24 February 2008

AS36561 (YouTube) announces 208.65.152.0/22. Note that its connectivity almost doesn't change during the period of the hijacking.



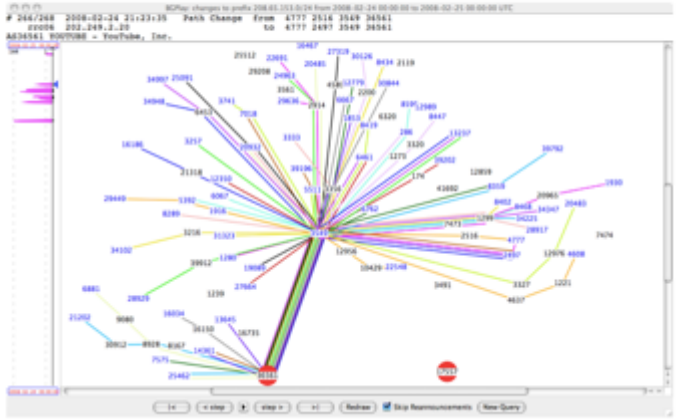
Sunday, 24 February 2008, 18:49 (UTC)

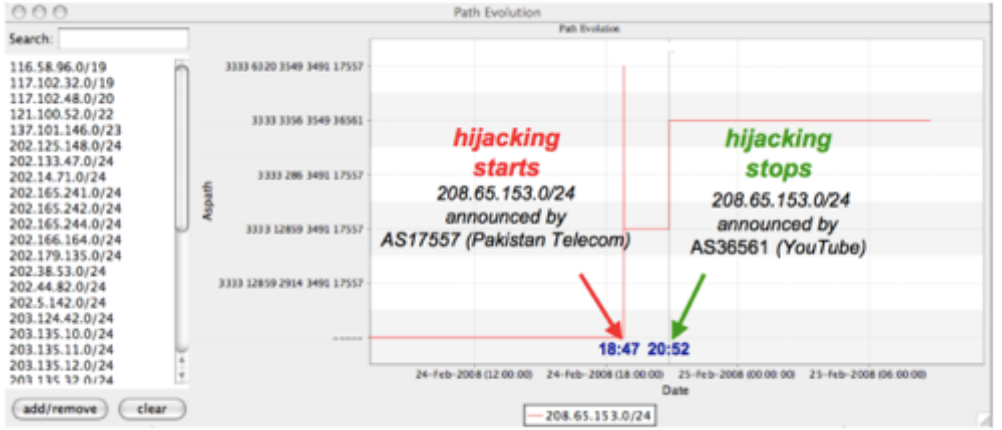
AS17557 (Pakistan Telecom) has been announcing 208.65.153.0/24 for the past two minutes. RIS peers around the world have received the route update, and YouTube traffic is being redirected to Pakistan.



Sunday, 24 February 2008, 21:23 (UTC)

AS36561 (YouTube) has been announcing 208.65.153.0/24 since 20:07 (UTC). The bogus announcement from AS17557 (Pakistan Telecom) has been withdrawn, and RIS peers now only have routes to YouTube's AS36561





https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

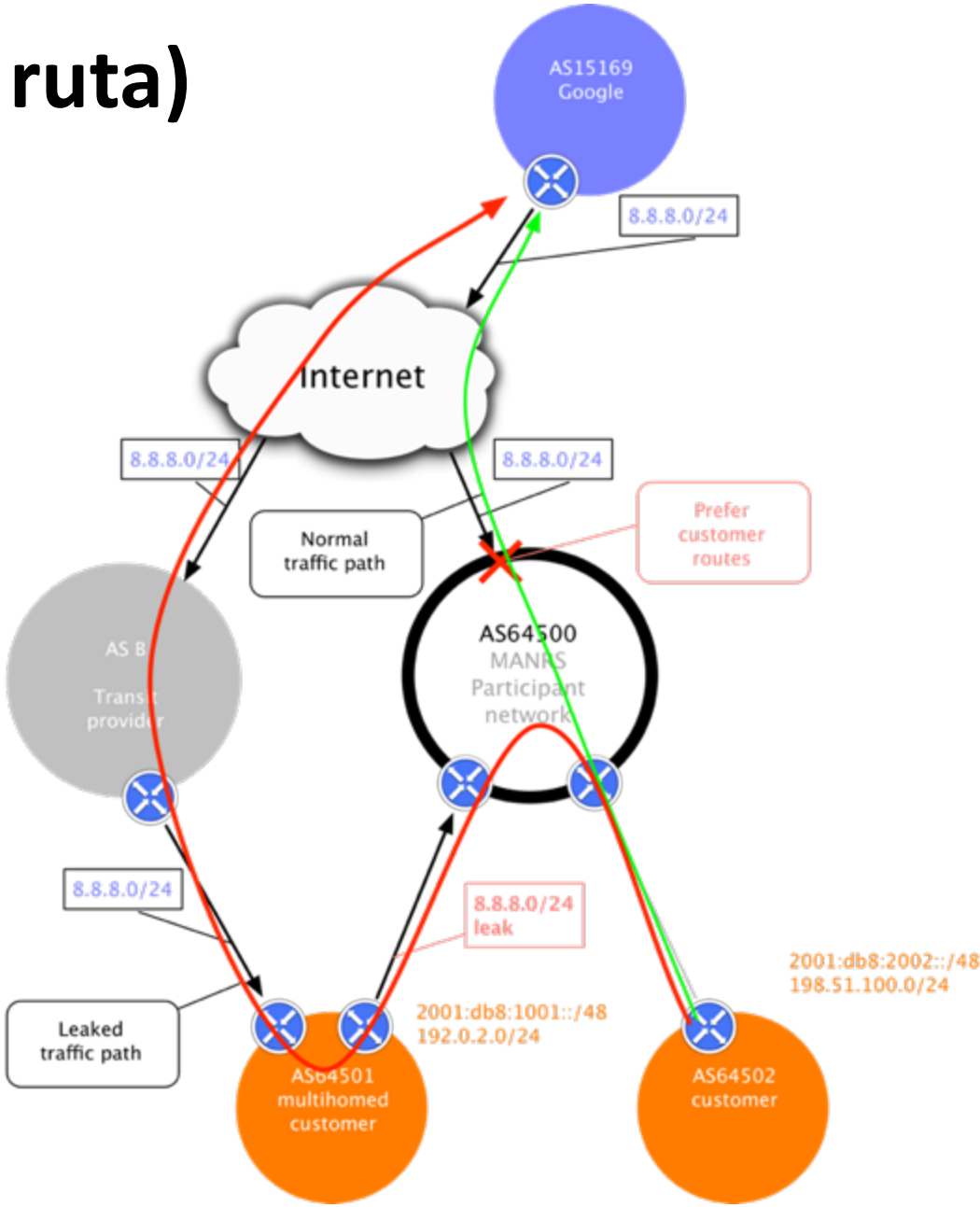
MANRS

- La Fuga de Rutas (Route Leak), se presenta cuando un operador de red anuncia, ya sea de manera accidental o no, hacia sus proveedores que tiene una ruta de destino hacia otros ISP, esto implica un flujo de datos continuo a través del AS innecesario, o de manera intencional, para el espionaje y análisis de tráfico de paquetes.

Algunas de las consecuencias del secuestro de BGP o de la fuga de rutas, pueden ser la Denegación de Servicios, Spoofing, Sobrecargas, Agujeros Negros, Pérdida de datos como cuentas bancarias, transacciones, bases de datos, etc.

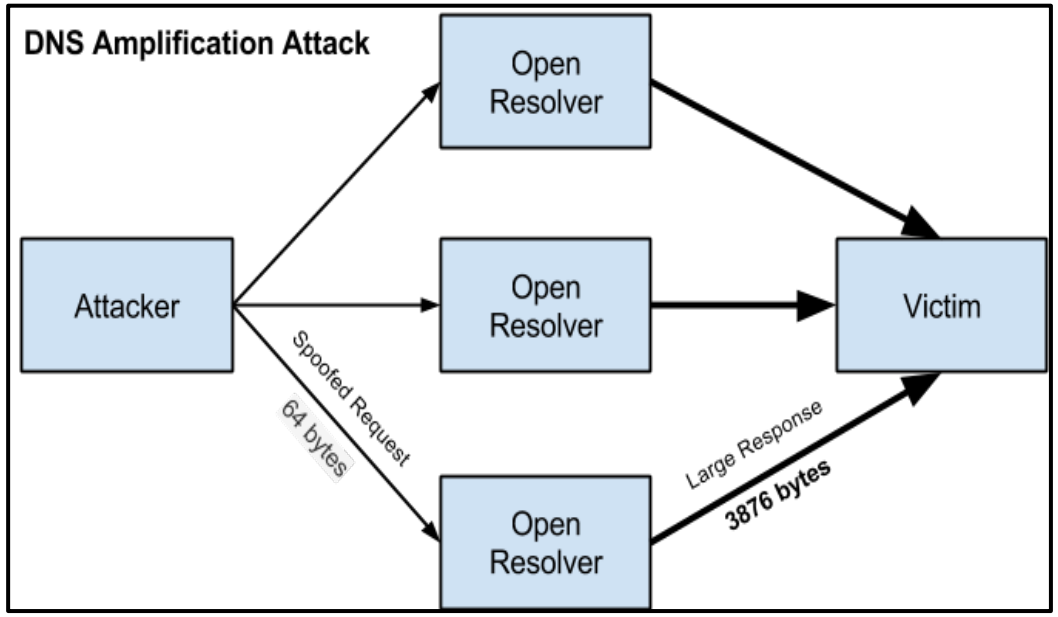
Las amenazas: **Route Leak (fuga de ruta)**

Evento	Route Leak
Descripción	Un operador de red con múltiples proveedores anuncia a un proveedor ascendente (a menudo debido a una mala configuración accidental) que tiene una ruta a un destino a través del otro proveedor ascendente.
Repercusión	Puede ser utilizado para la inspección de tráfico y reconocimiento.
Solución	Políticas de filtrado más fuertes.



Las amenazas: **IP Address Spoofing (Falsificación IP Address)**

Evento	IP Address Spoofing
Descripción	Alguien crea paquetes IP con una dirección IP de origen falsa para ocultar la identidad del remitente o hacerse pasar por otro sistema informático.
Repercusión	Causa raíz de los ataques DDoS.
Solución	Validación de la dirección de origen.



Acción 2 MANRS – Anti-spoofing (13 de junio)

MANRS

¿Qué podemos hacer?

- Por lo general se tienen diferentes maneras de atacar la alta inseguridad a través del internet, una de ellas es el AS PATH Filtering, este consiste básicamente en filtrar los prefijos de las redes vecinas, acotándolas dependiendo de las necesidades del operador de red, como, por ejemplo: Aceptar solo prefijos de AS conectados directamente, aceptar solo prefijos de AS conectados directamente y con un AS detrás del primero, negar ciertos AS de tránsito, etc.

MANRS

- También es posible validar los datos RPKI globales, políticas de ruteo, etc. mediante herramientas como RPKI validator, IRR toolset, IRRPT, BGPQ3 para la toma de decisiones BGP, así como en la configuración de sus routers.

- En el año 2017, La IETF (Internet Engineering Taks Force) lanzó un protocolo de seguridad denominado BGPsec el cual consiste en una extensión del BGP que proporciona confianza y seguridad a los AS mediante el envío de mensajes BGP UPDATE, estos mensajes contienen firmas digitales de seguridad haciendo más confiable las rutas a través de los AS.

Filtering: https://www.manrs.org/isps/guide/filtering/

MANRS en lo referente a Filtrado, que tiene como objetivo evitar la propagación de información de enrutamiento incorrecta, espera de los Operadores de Red 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 a redes adyacentes con prefijo y granularidad de ruta 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.

Lo más importante es asegurar los anuncios de enrutamiento entrante, particularmente desde las redes de clientes, mediante el uso de filtros explícitos de nivel de prefijo o mecanismos equivalentes.

MANRS Actions
https://www.manrs.org/isps/join/

- El operador de red define una política de enrutamiento clara e implementa un sistema que garantiza la corrección de sus propios anuncios y anuncios de sus clientes a redes adyacentes con prefijos y granularidad de ruta AS.
- El operador de red puede comunicar a sus redes adyacentes qué anuncios son correctos.
- El operador de red aplica la debida diligencia al verificar la exactitud de los anuncios de sus clientes, específicamente que el cliente posee legítimamente el ASN y el espacio de direcciones que anuncia.

- Lo más importante es asegurar los anuncios de enrutamiento entrante, particularmente desde las redes de clientes, mediante el uso de filtros explícitos de nivel de prefijo (prefix-list) o mecanismos equivalentes.

- En segundo lugar, los filtros de ruta por AS (as-path), que se pueden usar para exigir que las redes del cliente o del ISP sean explícitas acerca de qué Sistemas Autónomos (AS) están más debajo de ellos.

MANRS

- Tenga en cuenta que un error común es un error tipográfico en las direcciones IP anunciadas, lo que hace que las direcciones incorrectas se anuncien desde un ASN permitido. Por lo tanto, el filtrado de los anuncios BGP de los clientes por los filtros As-path solo es insuficiente para evitar problemas de enrutamiento catastróficos a nivel sistémico

MANRS

- Antes de crear filtros, es importante aplicar las acciones debidas y verificar si la información proporcionada por el cliente sobre su identidad y recursos es correcta.

- Existen otras herramientas para la ayuda en la validación de los datos, como RPKI validator, IRR toolset, IRRPT, BGPQ3 para la toma de decisiones BGP.

MANRS

- Utilice los registros de enrutamiento de Internet (IRR) y solicite a los clientes que registren los objetos de la ruta.

- Utilice la infraestructura de clave pública de recursos (RPKI) y solicite a los clientes que creen autorizaciones de origen de ruta (ROA)

- Utilice una base de datos interna con la información proporcionada como parte del proceso de aprovisionamiento

MANRS

Additional reading

- IRR Power Tools (IRRPT) https://github.com/6connect/irrpt
- Internet Routing Registry Toolset (IRRToolset) https://github.com/irrtoolset/irrtoolset
- BGPQ3 https://github.com/snar/bgpq3
- Ansible http://www.ansible.com/
- Cisco Network Services Orchestrator http://www.cisco.com/go/nso
- IRR Explorer http://irrexplorer.nlnog.net/
- RPKIhttps://www.lacnic.net/980/1/lacnic/certificacion-de-recursos-rpki

BGP Filtrado de rutas

- 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 la rutas no se incluyen en nuestra tabla de ruteo.
  - **Filtrado de salida:** se aplica a rutas previamente a ser anunciadas a un vecino.
    - Entonces las rutas no se incluirán en las tablas de ruteo remotas.
- **Razones?**
  - Económicas – Ej: Transit ISP vs peering
  - Seguridad – Ej: sólo rutas asignadas a nuestros clientes
  - Técnicas – Ej: problemas de memoria

BGP Filtrado de rutas

MANRS

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 access-list 101 permit ip 203.0.113.0 0.0.0.255 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 ip prefix-list Entrada seq 10 deny 203.0.113.0/24 le 32 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

MANRS

Filtros con prefix-list - Ejemplo

Prefix-list

```
router bgp 64496
  neighbor 203.0.113.100 remote-as 65551   neighbor
  203.0.113.100 prefix-list PEER-IN in
  neighbor 203.0.113.100 prefix-list PEER-OUT out
!
ip prefix-list PEER-IN deny 198.51.100.0/24
ip prefix-list PEER-IN permit 0.0.0.0/0 le 32
ip prefix-list PEER-OUT permit 192.0.2.0/24
```

MANRS

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 access-list **<nro_filtro>** permit | deny <regexp>

  2. Aplicar el filtro

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

MANRS

Filtros con AS-PATH- Ejemplo

```
...
 neighbor 198.51.100.22 filter-list 11 out
...


ip as-path access-list 11 deny 64496$
ip as-path access-list 11 deny ^645
ip as-path access-list 11 permit _64497_64498_
...
```

MANRS

Expresiones Regulares

Caracter	Función
^	empieza con
$	termina con
.	cualquier caracter
_	cualquier delimitador (espacio, comienzo, fin, coma)
[0-9]	rango del 0 al 9
[123]	1, 2 ó 3
( )	asocia
|	ó
*	cero o más veces
?	cero o una vez
+	una o más veces
\#	llama a la expresión ubicada en la posición # del regexp

MANRS Filtrado de rutas – Route-maps

- Los route-map son similares a las sentencias de un lenguaje de programación,
  - “if ……. then ……”
- Cada instancia del route-map tiene un número de secuencia.
- Son ejecutados en orden desde la sentencia con menor número de secuencia hasta el más alto. Es posible editarlos o modificarlos utilizando este número de secuencia.
- Si en un route-map, una sentencia con un determinado criterio de coincidencia resulta verdadera, la ejecución del route-map se detiene.
- Se puede utilizar route-map para permitir o denegar según el criterio encontrado por la sentencia ***match***.

MANRS

Filtrado de rutas - Route-maps

- Si no existiera una sentencia *match* dentro de una instancia de un route- map, todas las rutas resultan con criterio verdadero. Las sentencias *set* son aplicadas a todas las rutas*.
- Si no existiera una lista de acceso para la sentencia *match* dentro de la instancia del route-map, todas las rutas resultan con criterio verdadero. Las sentencias *set* se aplican a todas las rutas.
- Tal como con las listas de acceso, una denegación implícita es incluida al final del route-map.
- Si múltiples sentencias *match* son utilizadas dentro de una instancia de un mapa de ruteo, todas las sentencias *match* deben resultar verdaderas para que de la instancia surja un resultado verdadero

* o paquetes

MANRS

Route-map - Ejemplo con prefix-list

```
router bgp 64496
  neighbor 203.0.113.10 route-map infilter in
!
route-map infilter permit 10
  match ip address prefix-list HIGH-PREF
  set local-preference 120
!
route-map infilter permit 20
  match ip address prefix-list LOW-PREF
  set local-preference 80
!
route-map infilter permit 30
!
ip prefix-list HIGH-PREF permit 192.0.2.0/25
ip prefix-list LOW-PREF permit 192.0.2.128/25
```

MANRS

Route-map - Ejemplo con As-path

```
router bgp 64496
  neighbor 203.0.113.10 route-map filter-on-as-path in
!
route-map filter-on-as-path permit 10
  match as-path 1
  set local-preference 80
  set weight 200
  set metric 127
  set next-hop 192.0.2.10
!
route-map filter-on-as-path permit 20
  match as-path 2
  set local-preference 200
  set weight 500
  set metric 327
  set next-hop 192.0.2.100
!
route-map filter-on-as-path permit 30
!
ip as-path access-list 1 permit _64505$
ip as-path access-list 2 permit _64510_
```

MANRS

BGP
Buenas prácticas

- Es importante que los prefijos que enviamos hacia afuera de nuestro AS deben estar sumarizados.

- Que anuncios no debería recibir
  - No recibir los prefijos definidos en el RFC1918
  - No aceptar mis propios prefijos
  - No aceptar el default (a menos que se requiera)
  - No aceptar prefijos mayores de /24

MANRS

- Que prefijos no debería recibir:

```
router bgp 64496
 network 192.0.2.0 mask  255.255.255.0
 neighbor 203.0.113.100  remote-as 64505
 neighbor 203.0.113.100  prefix-list in-filter in
!
ip  prefix-list in-filter  deny 0.0.0.0/0        ! Block default
ip  prefix-list in-filter  deny 0.0.0.0/8 le 32
ip  prefix-list in-filter  deny 10.0.0.0/8 le 32
ip  prefix-list in-filter  deny 101.10.0.0/19 le 32    ! Block local prefix
ip  prefix-list in-filter  deny 127.0.0.0/8 le 32
ip  prefix-list in-filter  deny 169.254.0.0/16 le 32
ip  prefix-list in-filter  deny 172.16.0.0/12 le 32
ip  prefix-list in-filter  deny 192.0.2.0/24 le 32
ip  prefix-list in-filter  deny 192.168.0.0/16 le 32
ip  prefix-list in-filter  deny 224.0.0.0/3 le 32      ! Block multicast
ip  prefix-list in-filter  deny 0.0.0.0/0 ge 25        ! Block prefixes >/24
ip prefix-list  in-filter
                           permit 0.0.0.0/0 le 32
```

Procedimiento MANRS

Existe un procedimiento para poder formar parte como miembro oficial del Proyecto MANRS, el primero de ellos es cumplir con requisitos de autoevaluación:

- El primero es estar de acuerdo con las acciones y principios de MANRS, los cuales pueden ser visualizados en la siguiente liga:

https://www.manrs.org/wp-content/uploads/sites/14/2018/03/MANRS-BCOP-20170125.pdf

- Dentro de las acciones se deben realizar algunas pruebas para diagnosticar el ASN que desea incorporarse:
  - **Filtrado**: El objetivo del filtrado es evitar la propagación de información de ruteo erróneo.
    - Comprobar que el ASN no anuncia bogons(direccionamiento falso), para esto se puede utilizar informe CIDR:
      https://www.cidr-report.org/as2.0/
    - Comprobar que el ASN no estuvo implicado en incidentes recientes:
      https://bgpstream.com/

MANRS

- **Antispoofing**: El objetivo del Antispoofing es evitar el tráfico con direcciones IP de origen falsificadas.
  - Comprobar que el ASN no aparezca en la base de datos de spoofer CAIDA: https://spoofer.caida.org/provider.php?asn=[ASN], https://spoofer.caida.org/as.php?asn=[ASN]
  - Si no hay pruebas recientes, ejecute Spoofer https://spoofer.caida.org/as.php?asn=[ASN]

MANRS

- **Coordinación:** El objetivo es facilitar la comunicación operativa global y la coordinación entre operadores de red.
  - Comprobar que los contactos están en el whois.
    whois -h whois.lacnic.net prefijo
  - Verificar que la información de contacto esté registrada en el PeeringDB:
    https://www.peeringdb.com/asn/[ASN]

- **Validación Global:** El objetivo es validar que la información de enrutamiento a escala global sea correcta y veraz.
  - Verificar que la información de enrutamiento esté registrada en un IRR y tenga ROA

    http://localcert.ripe.net:8088/bgp-preview

    https://milacnic.lacnic.net/lacnic/rpki/state

MANRS

Video

BGP - MANRS: Acción 1 - Filtrado

https://www.youtube.com/watch?v=eUSjVqj5ib4

Caso de un Operador de Red en México: MANRS en una Universidad Pública

Caso Operador de Red de una Universidad Pública de México

Organización: Universidad Autónoma de Yucatán

País: México

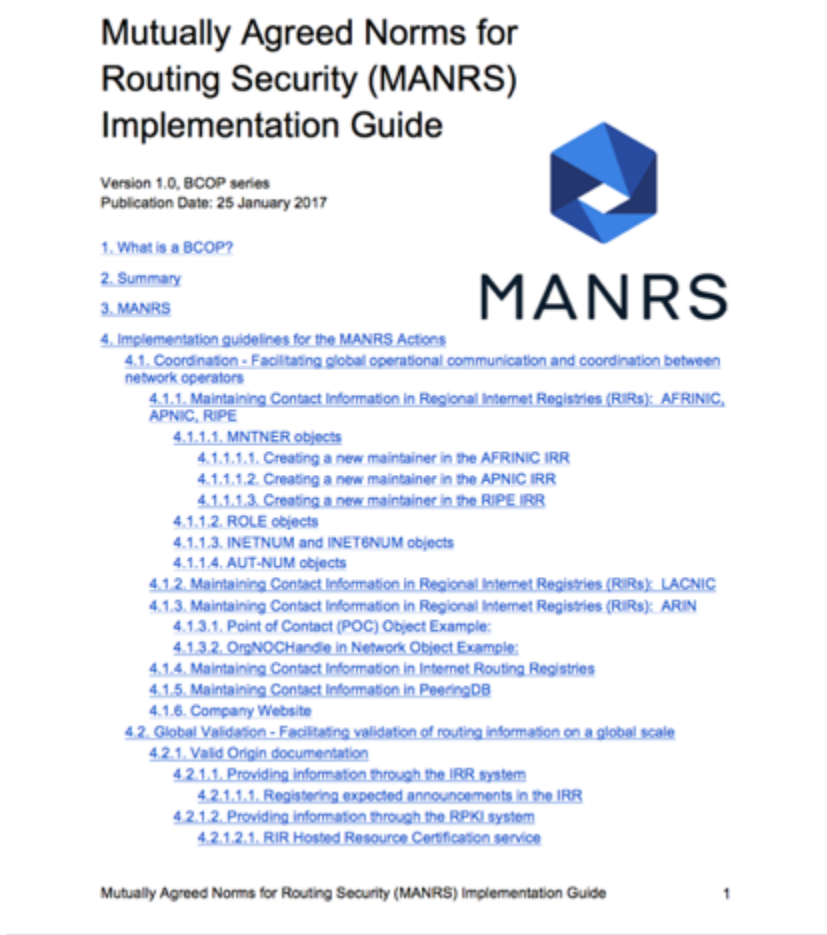
RIR: LACNIC

Recursos de Internet:

ASN 22122, 148.209.0.0/16, 2801:c4:19::/48

Estrategia de Apoyo:

- Webinars MANRS
- https://www.manrs.org/tutorials
- https://www.manrs.org/bcop/



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

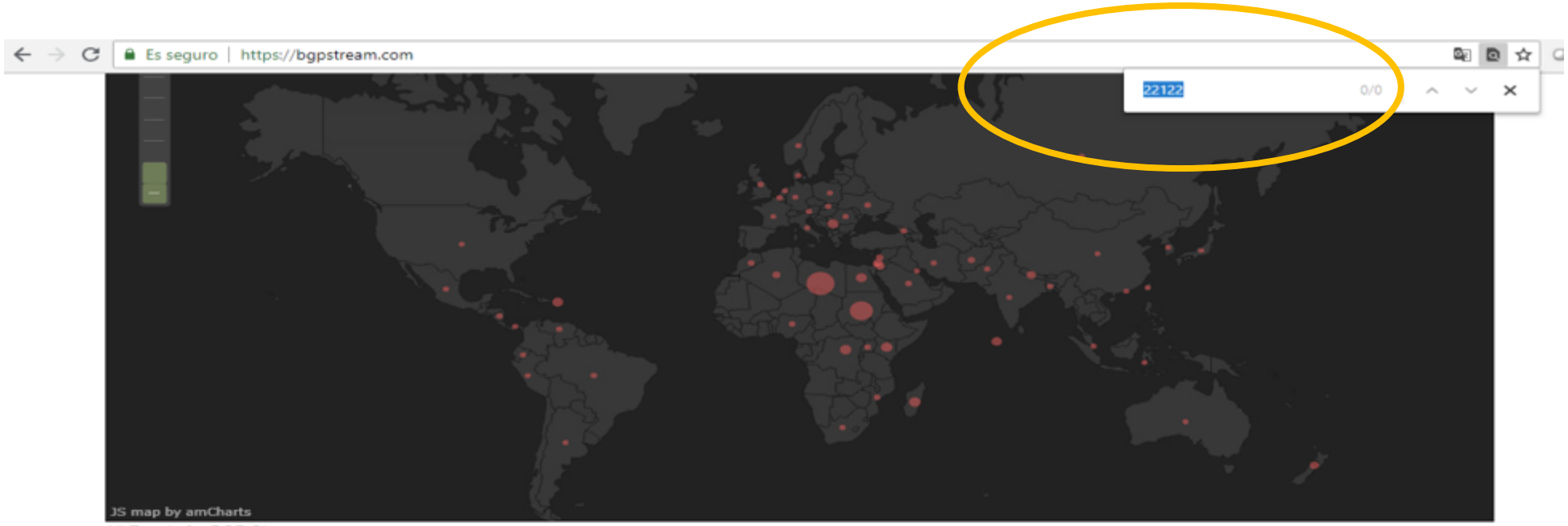
Proceso para la Acción 1: Filtrado

1. Autoevaluación:

- Comprobar que la ASN no anuncia bogons. Utilizar informe CIDR: https://www.cidr-report.org/as2.0/
- Compruebe que el ASN no haya estado implicado en incidentes recientes: https://bgpstream.com/

2. Implementación de las medidas necesarias en BGP: verificación de los propios anuncios y actualización de la configuración de Prefix-list.

Autoevaluación: Se comprobó que la ASN no anuncia bogons (direccionamiento falso), utilizando el informe CIDR: https://www.cidr-report.org/as2.0/



All Events for BGP Stream.

Event type	Country	ASN	Start time (UTC)	End time (UTC)	More info
Outage		BELL- (AS 37126)	2018-08-21 15:56:00		More detail
Outage		Gigatel Networks Private Limited (AS 135193)	2018-08-21 15:55:00	2018-08-21 15:58:00	More detail
Outage		EDUARDO LIMA E SILVA NETTO - ME (AS 266566)	2018-08-21 14:45:00		More detail

Se comprobó que el ASN no haya estado implicado en incidentes recientes: https://bgpstream.com/

5141	5202	AS8151	Uninet S.A. de C.V., MX
4620	4696	AS12479	UNI2-AS, ES
4557	4684	AS4538	ERX-CERNET-BKB China Education and Research Network Center, CN
4286	4418	AS7545	TPG-INTERNET-AP TPG Telecom Limited, AU
3775	3778	AS39891	ALJAWWALSTC-AS, SA
3488	3488	AS10620	Telmex Colombia S.A., CO
3390	3439	AS6327	SHAW - Shaw Communications Inc., CA
3163	3237	AS22773	ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc., US
3150	3152	AS11492	CABLEONE - CABLE ONE, INC., US
3110	3115	AS8551	BEZEQ-INTERNATIONAL-AS Bezeqint Internet Backbone, IL
2936	2945	AS7552	VIETEL-AS-AP Viettel Group, VN
2736	2825	AS4766	KIXS-AS-KR Korea Telecom, KR
2710	2729	AS45899	VNPT-AS-VN VNPT Corp, VN
2647	2658	AS11830	Instituto Costarricense de Electricidad y Telecom., CR
2527	2546	AS9394	CTTNET China TieTong Telecommunications Corporation, CN
2525	2553	AS20940	AKAMAI-ASN1, US
2250	2261	AS17974	TELKOMNET-AS2-AP PT Telekomunikasi Indonesia, ID
2223	2252	AS9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN
2213	2255	AS16509	AMAZON-02 - Amazon.com, Inc., US
2160	2816	AS9829	BSNL-NIB National Internet Backbone, IN

Report: ASes ordered by number of more specific prefixes
Report: More Specific prefix list (by AS)
Report: More Specific prefix list (ordered by prefix)

Possible Bogus Routes and AS Announcements

Possible Bogus Routes

Prefix	Origin AS	AS Description	Unallocated block
27.100.7.0/24	AS56096		27.100.4.0 - 27.100.7.255
41.76.136.0/22	AS37500	-Reserved AS-, ZZ	41.76.136.0 - 41.76.143.255
41.76.136.0/24	AS37500	-Reserved AS-, ZZ	41.76.136.0 - 41.76.143.255
41.76.138.0/24	AS37500	-Reserved AS-, ZZ	41.76.136.0 - 41.76.143.255

MANRS Actions
https://www.manrs.org/isps/join/

1. Filtering
Evitar la propagación de información de enrutamiento incorrecta.

2. Anti-spoofing
Evitar el tráfico con direcciones IP de origen falsificadas.

3. Coordination
Facilitar la comunicación operativa global y la coordinación entre operadores de redes.

4. Global Validation
Facilitar la validación de la información de enrutamiento a escala global.

MANRS

https://www.manrs.org/participants/

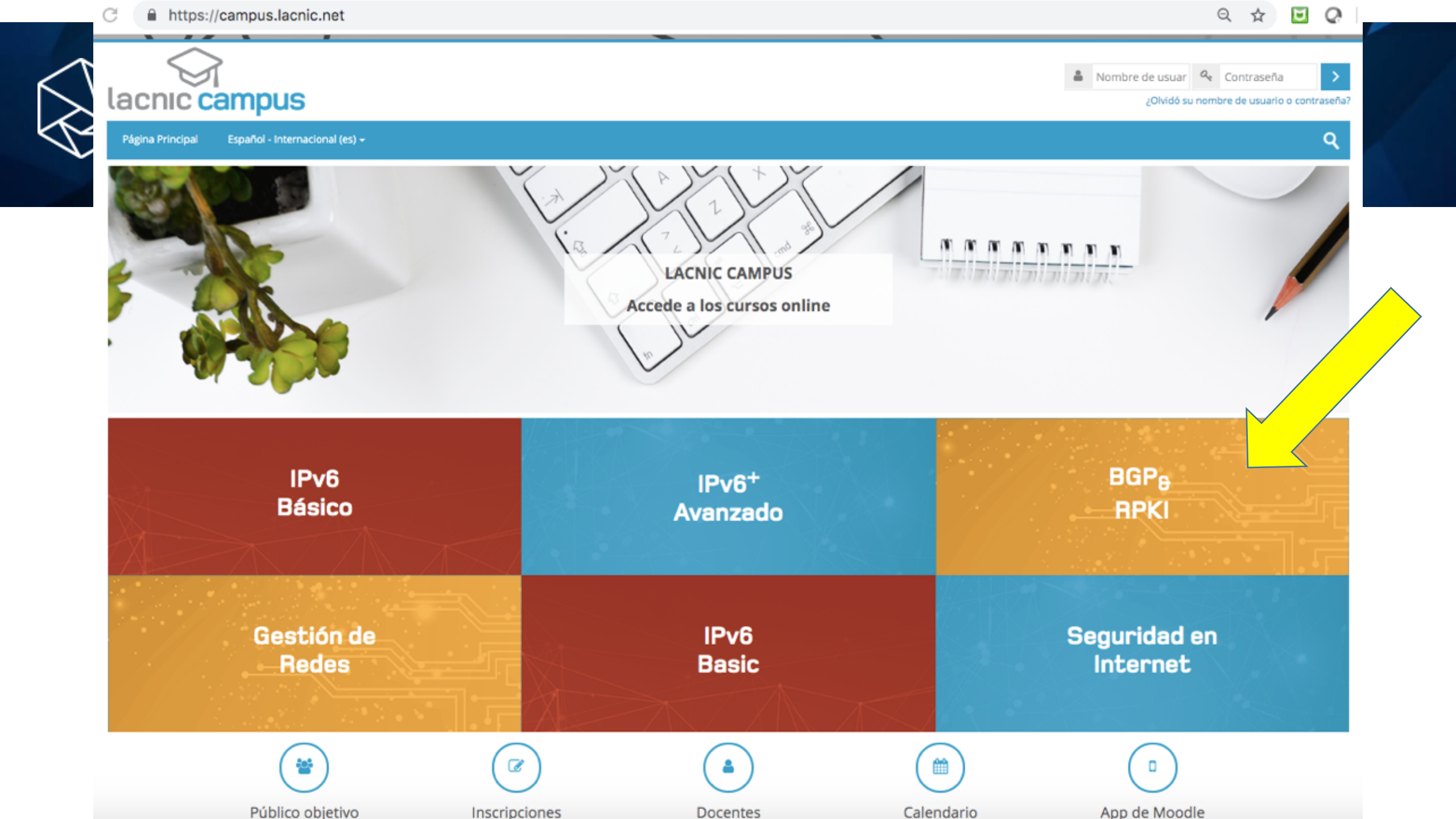
Displaying 51 - 75 of 92

« 1 2 3 4 »

Organization	Country	ASNs	Action 1 - Filtering	Action 2 - Anti-Spoofing	Action 3 - Coordination	Action 4 - Global Validation
Universidad Autónoma de Yucatán	MX	22122	✔	✔	✔	✔
GEANT	NL GB	21320 20965	✔	✔	✔	✔
BIT BV	NL		✔	✔	✔	✔
KPN	NL	1136 5615 8737	✔	✔	✔	✔

MANRS

Recomendaciones


https://campus.lacnic.net
lacnic campus
Nombre de usuar
Contraseña
¿Olvidó su nombre de usuario o contraseña?
Página Principal
Español - Internacional (es)
LACNIC CAMPUS
Accede a los cursos online
IPv6 Básico
IPv6+ Avanzado
BGP6 RPKI
Gestión de Redes
IPv6 Basic
Seguridad en Internet
Público objetivo
Inscripciones
Docentes
Calendario
App de Moodle

lacnic campus

Página Principal Español - Internacional (es)

Fundamentos de BGP e Introducción a RPKI

Objetivos del curso:

•Comprender el concepto de Sistema Autónomo, y las diferencias entre el ruteo interno y externo.

•Comprender cómo trabaja BGP y para lo que fue concebido.

•Comprender la importancia de contar con una política de ruteo propia en la organización.

•Aprender a configurar BGP en forma básica.

•Identificar y analizar los datos que aporta BGP, mediante el uso de atributos y comandos útiles.

•Conocer la importancia y alcances de los filtros en BGP.

•Conocer acerca de la confiabilidad del ruteo en Internet y qué medidas existen para evitar el secuestro de rutas.

•Conocer cómo trabaja el sistema de certificación de recursos RPKI.

•Identificar y resolver problemas básicos de BGP.

•Conocer e implementar las mejores prácticas recomendadas para el ruteo en Internet.

- Regístrese desde: https://eventos.lacnic.net/ev4/detail?id=bgp-rpki-3ra-edicion-2019
- Costo: USD 179
- Instituciones miembros de LACNIC: Sin costo

Autoevaluación: Acción 1 Filtrado

- Comprobar que la ASN no anuncia bogons. Utilizar informe CIDR: https://www.cidr-report.org/as2.0/

- Compruebe que el ASN no haya estado implicado en incidentes recientes: https://bgpstream.com/

MANRS

Bibliografía

https://www.manrs.org/

https://www.manrs.org/wp-content/uploads/sites/14/2018/03/MANRS-BCOP-20170125.pdf

https://www.internetsociety.org/es/issues/manrs-es/

https://www.internetsociety.org/es/blog/2018/08/tech-companies-endorse-manrs-routing-security-actions/

https://www.lacnic.net/innovaportal/file/3512/1/bgp_buenas_practicas_2019a.pdf

https://www.lacnic.net/innovaportal/file/3512/1/20190510_marns_universidades_tutorial_peeringlacnic31.pdf

https://www.lacnic.net/innovaportal/file/3139/1/bgp-rosario-lacnic30.pdf

https://www.youtube.com/watch?v=eUSjVqj5ib4

MANRS

Additional reading

- IRR Power Tools (IRRPT) https://github.com/6connect/irrpt
- Internet Routing Registry Toolset (IRRToolset) https://github.com/irrtoolset/irrtoolset
- BGPQ3 https://github.com/snar/bgpq3
- Ansible http://www.ansible.com/
- Cisco Network Services Orchestrator http://www.cisco.com/go/nso
- IRR Explorer http://irrexplorer.nlnog.net/
- RPKIhttps://www.lacnic.net/980/1/lacnic/certificacion-de-recursos-rpki

MANRS

Preguntas

Próxima sesión: Acción 2 – Anti-spoofing

El taller consta de **6 sesiones; 5 virtuales y uno presencial**

Sesión 1: Jueves 11 y 25 de abril – Introducción a MANRS

Sesión 2: Jueves 23 de mayo – MANRS: Acción 1 – Filtrado

Sesión 3: Jueves 13 de junio – MANRS: Acción 2 – Anti-Spoofing

Sesión 4: Jueves 11 de julio – MANRS: Acción 3 – Coordinación

Sesión 5: Jueves 22 de agosto – MANRS: Acción 4 – Validación Global

La conclusión será con **una sesión presencial** en el marco de los eventos:

- Encuentro TICAL 2019, 2 – 4 de septiembre de 2019 en Cancún, México.
- Encuentro ANUIES-TIC 2019, 2 de octubre de 2019 en la UANL, Nuevo León, México.

MANRS

ANUIES

ANUIES - TIC

cudi
Corporación Universitaria para el Desarrollo de Internet A.C.
Internet 2 - México

Red CLARA
Cooperación Latino Americana de Redes Avanzadas

Internet Society

lacnic

NIC MÉXICO

Gracias