**Reglas de Operación que establece el Consorcio para el Intercambio de Tráfico de Internet, A.C. (CITI) para llevar a cabo el intercambio de tráfico entre los participantes del Punto de Intercambio de Tráfico de Internet de la Ciudad de Querétaro (en adelante IXP.QRO).**

**Estas reglas fueron aprobadas por el Consejo Directivo del CITI en su sesión celebrada el 24 de septiembre de 2019.**

CONSIDERANDO

Que el objetivo de CITI es promover el intercambio de tráfico de Internet a través de una matriz de conmutación en capas que ofrece puertos de acceso Ethernet y que utilizan el Protocolo de Internet (IP), con neutralidad y transparencia.

Que un Punto de Intercambio de Tráfico o Internet Exchange Point (IXP), es una solución de red compuesta típicamente de switches y enrutadores que usan el Protocolo de Internet (IP) en sus versiones 4 y 6, y funcionan en la capa 2 y 3 del modelo ISO / OSI, que ofrece servicios para la interconexión de Sistemas Autónomos (AS, por sus siglas en inglés) de las entidades participantes.

Que todos los puertos de equipos de red participantes conectados al **IXP.QRO** deben usar el protocolo BGP-4, que es el protocolo Capa-3 predeterminado utilizado por los Sistemas Autónomos en Internet para informar y obtener de sus pares los prefijos de red de otros conectados a él, en una conexión conocida como sesión BGP. Es a través de este intercambio de información, que Internet se puede ver como una sola red, o una red de redes. Cada participante deberá anunciar prefijos con máscara de un máximo de 24 bits.

Que en un IXP no es necesario que el equipo de red del participante establezca sesiones BGP con todos los demás participantes. En su lugar se utilizan route servers para que ahí se anuncien los prefijos de cada participante. Esto permite que, a través de una única sesión BGP establecida con el route server, el equipo de red del participante obtenga los prefijos anunciados por todos los demás participantes, promoviendo una economía general de recursos.

Que en el **IXP.QRO** se tienen al menos un route-servers.

Para asegurar que la infraestructura del **IXP.QRO** funcione eficientemente se emiten las siguientes:

**Reglas de Operación para llevar a cabo el intercambio de tráfico entre los participantes del IXP.QRO**

1. El participante es responsable de asegurarse que su información cumpla con las disposiciones legales aplicables y con las Reglas que establezca el **IXP.QRO**.
2. El **IXP.QRO** con la validación del Consejo Técnico de Querétaro y aprobación del Consejo Directivo de Querétaro, podrá modificar las presentes Reglas en cualquier momento y sin previo aviso, haciendo disponible la versión actualizada en el sitio web: www.ixp.mx.
3. El participante está obligado a asignar un contacto técnico titular y su suplente, a cargo de todas las cuestiones técnicas de su participación.
4. El participante está obligado a asignar un contacto administrativo titular y su suplente, a cargo de todas las cuestiones administrativas y financieras derivadas de su participación en el **IXP.QRO**
5. El participante deberá proporcionar la siguiente información:

|  |  |
| --- | --- |
| Nombre de la empresa |  |
| Dirección |  |
| Código postal |  |
| Ciudad |  |
| País |  |
| Fecha |  |
| Firma |  |
| Persona autorizada a firmar |  |
| Puesto |  |
| Correo electrónico |  |
| Número de teléfono |  |
| Nombre del contacto técnico titular |  |
| Puesto |  |
| Correo electrónico |  |
| Número de teléfono |  |
| Nombre del contacto técnico suplente |  |
| Puesto |  |
| Correo electrónico |  |
| Número de teléfono |  |
| Nombre del contacto administrativo titular |  |
| Puesto |  |
| Correo electrónico |  |
| Número de teléfono |  |
| Nombre del contacto administrativo suplente |  |
| Puesto |  |
| Correo electrónico |  |
| Número de teléfono |  |

1. Ningún servicio, sistema o estructura de red de **IXP.QRO** podrá usarse para fines ilegales, deshonestos o que violen cualquier disposición legal local, estatal, nacional o internacional aplicable.
2. El participante no divulgará a terceros no autorizados información que pueda ayudarlos a comprometer la operación del **IXP.QRO**, incluida la información confidencial privilegiada proporcionada a los participantes, así como información sobre el **IXP.QRO** que no sea de dominio público y pueda ser utilizada por terceros no autorizados.
3. El participante se abstendrá de comprometer de cualquier forma los sistemas y la seguridad de la operación del **IXP.QRO** y sus participantes.
4. El **IXP.QRO** ayudará a resolver incidentes de seguridad y cooperará con las investigaciones realizadas por las autoridades. Para ello el consejo podrá emitir las políticas y procedimientos correspondientes.
5. El **IXP.QRO** se reserva el derecho de desconectar todos los puertos involucrados en actividades maliciosas y/o escaneo de puertos.
6. El participante está obligado a anunciar todas las rutas de sus clientes a los demás participantes y a aceptar las rutas anunciadas por los demás participantes y así como las rutas de sus clientes.
7. El participante está obligado a intercambiar tráfico entre sus propios clientes y todos los clientes de todos los demás participantes, a través del **IXP.QRO**.
8. El participante es responsable de que el tráfico que se intercambie en el **IXP.QRO** no sea filtrado, manipulado o examinado.
9. La infraestructura de intercambio de tráfico se basa en el estándar Ethernet II (IEEE 802.3) o DIX Ethernet.
10. El intercambio de rutas se realizará utilizando BGP4. Todos los puertos de equipos de red participantes conectados a los canales de acceso deben usar el protocolo BGP-4 (Border Gateway Protocol 4 - RFC4271).
11. El participante acepta usar un número de Sistema Autónomo (AS), asignado por un Registro Regional de Internet, del que sea titular para sus comunicaciones de intercambio de ruta.
12. El participante acepta que los prefijos de ruta (bloques de espacio de direcciones IP) anunciados tendrán una longitud máxima de máscara de prefijo de 24 bits.
13. El participante acepta que solo asignará las rutas para las direcciones IP que tiene asignadas por un Registro Regional de Internet de él o sus clientes.
14. El participante no podrá utilizar al **IXP.QRO** como "ruta de default", ni utilizar a cualquier otro participante del **IXP.QRO** como “ruta de default”, sin un muto acuerdo previo.
15. No está permitido el uso del proxy-ARP en equipos en red conectados a puertos físicos o virtuales del **IXP.QRO**.
16. No deben habilitarse protocolos de descubrimiento de vecindad, tales como CDP, MNDP, o similares.
17. Se deberá deshabilitar el anuncio de enrutador (RA) en IPv6.
18. No se permite enviar paquetes de difusión o multidifusión IPv4 o IPv6, excepto los paquetes ICMPv6 ND.
19. No se debe anunciar el direccionamiento utilizado en los puertos del IXP a otras redes. Esto implica el uso de la funcionalidad next-hop-self para el anuncio interno de rutas recibidas a través del **IXP.QRO**.
20. El equipo y los circuitos utilizados por un participante conectado al **IXP.QRO** deben ser capaces de operar con una unidad de transferencia máxima (MTU) de 1500 bytes.
21. La unidad de transferencia máxima (MTU) en los switches del **IXP.QRO** será de 1523 bytes.
22. El número máximo de MAC addresses por VLAN será de 2048.
23. La política de enrutamiento se ajustará a las futuras recomendaciones del Internet Engineering Task Force (IETF).
24. El participante deberá mantener suficiente ancho de banda hacia el **IXP.QRO** para mantener sus conexiones al Servicio de enrutamiento del **IXP.QRO** sin congestión. Al llegar al 80% de capacidad de los puertos existentes deberá añadir capacidad adicional.

Cuando la utilización llegue al 80% de la capacidad nominal de un puerto compartido en el IXP, no serán provisionadas nuevas VLANs y será necesario proporcionar una mayor capacidad adicional de puertos Ethernet al **IXP.QRO**.

Si el tráfico en cualquier dirección excede el 95% de la capacidad nominal del puerto, el IXP NOC puede deshabilitar uno o más puertos virtuales del participante, a su discreción, para llevar la saturación por debajo del 80% de la capacidad nominal.

La capacidad se considerará capacidad sin redundancia. Por ejemplo, si un participante tiene 6 puertos agregados de 10Gbps, con dos conexiones ópticas redundantes de 30 Gbps, se considera que la capacidad nominal es 30 Gbps, no 60 Gbps.

1. El participante será responsable de que la pérdida de paquetes sea inferior al 20% en cualquiera de sus conexiones.
2. El participante tiene la responsabilidad de garantizar que su equipo de red esté disponible para todos los demás participantes, lo que significa que todos los participantes tendrán acceso a través de todo el ancho de banda disponible en su puerto para el tráfico útil, sin obstáculos por ningún acto, accidental o deliberado.

En caso de tener una eventualidad que cause una degradación, el participante podrá temporalmente deshabilitar su puerto en su equipo. Una vez corregida la eventualidad deberá habilitar nuevamente su puerto. En todo momento deberá notificar al NOC del IXP sobre las medidas adoptadas durante la eventualidad.

1. El participante tomará todas las medidas, incluidas las propuestas del **IXP.QRO**, para garantizar el funcionamiento adecuado del Punto de Intercambio de Tráfico de Internet, incluyendo la gestión del tráfico de Internet de una manera proactiva en sus propias redes, independientemente de quién generó el tráfico de Internet.
2. El participante es responsable de monitorear adecuadamente sus redes las 24 horas del día, los 7 días de la semana, para garantizar que su uso del **IXP.QRO** no se utilice para causar inundaciones o ataques de denegación de servicio.
3. El participante tomará las medidas necesarias para evitar el acceso no autorizado o intentos maliciosos que puedan comprometer la operación del **IXP.QRO**
4. El participante utilizará la base de datos de Peering DB para reflejar su política de enrutamiento, la cual deberá mantenerse actualizada.
5. El participante deberá pagar sus cuotas aprobadas por el Consejo Directivo y sus conexiones al **IXP.QRO**.
6. El **IXP.QRO** informará a los participantes cada vez que se incorpore un nuevo participante. La activación de nuevos miembros se agendará con anticipación, se notificará a todos los miembros y se realizará de bajo tráfico para minimizar el impacto de posibles fallas o degradaciones.
7. El participante tiene prohibido:

* Comprometer o manipular los recursos del sistema o de la infraestructura del **IXP.QRO**
* El uso o distribución de herramientas diseñadas para comprometer la seguridad. Ejemplos de tales herramientas son programas para descifrar contraseñas, herramientas de intrusión o sondas;
* Acceso o uso no autorizado de datos de sistemas o redes. Esto incluye cualquier intento de sondear, escanear o probar las vulnerabilidades del sistema, la red o la seguridad;
* Monitoreo no autorizado de datos o tráfico en cualquier red o sistema sin el permiso expreso del sistema o del propietario de la red;
* Falsificar cualquier paquete TCP / IP o encabezado de paquete o cualquier parte de la información de encabezados

1. El participante deberá aplicar los filtros BGP necesarios de entrada y salida de prefijos y AS para garantizar un ruteo seguro, tales como:

* No enviar ni recibir los prefijos definidos en el RFC 1918
* No aceptar ni enviar prefijos mayores de /24

1. El participante deberá aplicar técnicas de Anti-Spoofing tales como: implementaciones de BCP 38, tales como:

* Implementar BCP 38 (RFCs 2827 y 3704)
* Access List Control (ACL)
* Unicast Reverse Path Filter

1. El participante deberá tener certificados sus recursos de internet a través de un IRR o RPKI.
2. Para efectos de las presentes Reglas se utilizará el siguiente

Glosario de Términos

**Anti-Spoofing.** Es una técnica utilizada para evitar que los paquetes salgan de la red del participante hacia el resto de Internet con una dirección de origen IP falsificada.

**ARP.** Cada interfaz de red tiene tanto una dirección IP como una dirección física MAC. En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas). Para realizar esta conversión, el nivel de enlace utiliza las tablas ARP. ARP está documentado en el RFC 826. El protocolo de resolución de direcciones inverso (RARP) realiza, obviamente, la operación inversa y se encuentra descrito en el RFC 903.

**AS**. Sistema Autónomo (Autonomous System). Identificador para un grupo de redes de direcciones IP que son gestionadas por uno o más operadores de red que poseen una clara y única política de enrutamiento.

**BCP 38.** Las actuales mejores prácticas de filtrando para el ingreso a la red están documentadas por la IETF en los documentos BCP 38 y BCP 84, los cuales están definidos por las RFCs 2827 y 3704, respectivamente.

**BGP**. Border Gateway Protocol. Es el protocolo de Puerta de Enlace de Frontera del Sistema Autónomo mediante el cual se intercambia la información de enrutamiento entre sistemas autónomos (AS). El protocolo utiliza el puerto 179 de TCP para el intercambio de información de enrutamiento. Al utilizar TCP, la comunicación en una misma sesión solo es entre un par de routers a los cuales se dice que están haciendo una comunicación entre pares (Peering). BGP utiliza varios atributos para el cálculo de las mejores rutas.

**Ethernet.** Estándar de redes de área local para computadoras, por sus siglas en inglés de Acceso Múltiple con Escucha de Portadora y Detección de Colisiones (CSMA/CD). Ethernet es la base para el estándar internacional de IEEE 802.3.

**IETF Internet Engineering Task Force** (en español, Grupo de Trabajo de Ingeniería de Internet). Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, enrutamiento, y seguridad. Se creó en los Estados Unidos, en 1986 y es mundialmente conocido porque se trata de la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.

**ICMPv6 ND.** Es un protocolo de IPv6, equivalente al protocolo de “Address Resolution Protocol” (ARP) en IPv4, aunque se distingue por incorporar funcionalidades de ICMP (Internet Control Message Protocol). Consiste en un mecanismo con el cual un nodo que se acaba de conectar a la red descubre la presencia de otros nodos en el mismo enlace, además de ver sus direcciones IP. Descrito en el RFC 4861 (neighbor discovery protocol).

**IPv4.** El Protocolo de Internet versión 4 (en inglés, Internet Protocol versión 4, IPv4), es la cuarta versión del Internet Protocol (IP). Está definido en el RFC 791 IPv4 y usa direcciones de 32 bit.

**IPv6.** El Protocolo de Internet versión 6 (en inglés, Internet Protocol versión 6, IPv6), es una versión del Internet Protocol (IP). Está definido en el RFC 2460 y en lugar de usar direcciones de 32 bits, usa direcciones de 128 bits.

**IRR.** Internet Routing Registry es una base de datos regional de objetos de ruteo para la determinación, compartición de rutas y de información relativa a ellas. Con esta base de datos usada para la configuración de routers se evitan problemas típicos de errores de configuración en el intercambio de información de enrutamiento entre proveedores de servicio de Internet.

**IXP.** Internet Exchange Point es un Punto de Intercambio de tráfico de Internet, consistente en una infraestructura física a través de la cual los participantes poseedores de un sistema autónomo (AS) intercambian el tráfico de Internet entre sus redes.

**LAG (802.3ad).** Es un esquema que permite hacer la agregación de enlaces físicos de gigabit Ethernet en un solo enlace lógico que permite la agregación del ancho de banda de todos los enlaces físicos agrupados.

**LLC/SNAP (802.2).** Logical Link Control está definido como un estándar de la IEEE usado para la comunicación en redes 802.3 (Ethernet) y otras redes.

**MAC address o dirección MAC.** Es un identificador único de 48 bits (6 bloques de dos caracteres hexadecimal [4bit]) que corresponde de forma única a una tarjeta o dispositivo de red. También se conoce como dirección física o de hardware, y es única para cada dispositivo. Está determinada y configurada por la IEEE.

**Modelo de referencia ISO / OSI** El modelo de interconexión de sistemas abiertos (ISO/IEC 7498), más conocido como “modelo OSI”, (en inglés, Open System Interconnection) es un modelo de referencia para los protocolos de la red, adoptado por la Unión Internacional de Telecomunicaciones (UIT) y, por la Organización Internacional de Normalización (ISO).

**MTU.** Unidad Máxima de Transferencia (Maximum Transmission Unit), un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede usarse utilizando un protocolo de comunicaciones.

**Next-hop-self.** Esta funcionalidad, dentro del protocolo BGP, es utilizada para modificar el atributo de siguiente salto (next-hop) y utilizar el identificador del router en vez de enviar la dirección IP del router externo al sistema autónomo.

**Peering DB.** Es una base de datos de redes de libre acceso, mantenida por los usuarios para facilitar la interconexión global de redes en puntos de intercambio de Internet (IXP), centros de datos y otras instalaciones de interconexión.

**Protocolo CDP.** (Cisco Discovery Protocol) es un protocolo propietario de Cisco de la capa 2 del modelo OSI, que permite que los dispositivos marca Cisco se comuniquen sin importar el estado de la conectividad de capa 3. Se utiliza para comunicar la información sobre las propiedades del puerto, conexión, y/o dispositivo.

**Protocolo MNDP.** Por sus siglas en inglés MikroTik Neighbor Discovery Protocol. Es un Protocolo de descubrimiento de equipos vecinos de marca MikroTik. Se utiliza para comunicar la información sobre las propiedades del puerto, conexión, y/o dispositivo, y así facilita la configuración y administración de la red al permitir que cada enrutador MikroTik descubra otros enrutadores MikroTik conectados.

**Proxy-ARP.** Es una técnica en la cual un router contesta requisiciones de ARP (Address Resolution Protocol) dirigidas a otro equipo, aceptando la responsabilidad de reenviarlos a su destino correcto.

**RA (Router Advertisement) IPv6**. El Router Advertisement se utiliza para la configuración automática y el enrutamiento de IPv6. Cuando está habilitado, el enrutador envía mensajes periódicamente y en respuesta a solicitudes. Un dispositivo utiliza la información para aprender los prefijos y parámetros para la red local.

**RFC.** Los “Request for Comments”, más conocidos por sus siglas RFC, son una serie de publicaciones del IETF que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre éstos.

**RFC 1918.** Espacio de direcciones para uso privado. La "Autoridad de Números Asignados en Internet", Internet Assigned Numbers Authority (IANA), ha reservado los tres siguientes bloques de direcciones IP para el uso privado:

10.0.0.0 - 10.255.255.255 (prefijo 10/8)

172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)

192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)

**RPKI**. Resource Public Key Infrastructure. Es un es sistema de certificación de recursos numéricos asignados globalmente y en Latinoamérica es operado por LACNIC.

**Route-server.** Es un equipo con software de enrutamiento que dirige la información de enrutamiento entre los routers que utilizan BGP y que generalmente están ubicados en nodos de acceso a la red de internet (IXP) donde se ubican múltiples routers.

**Ruta de default.** Es una ruta estática predeterminada, que se utiliza como último recurso cuando no se conoce una ruta hasta un destino determinado, o cuando no es posible almacenar en la tabla de enrutamiento de los routers la información relativa a todas las rutas posibles.

**TCP.** Transport Control Protocol es un protocolo de Internet definido en el RFC 793 que garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron y además proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

**Unicast Reverse Path Filter.** Esta característica de seguridad permite que un router verifique la accesibilidad de la dirección IP de origen en los paquetes que se reenvían. Esta capacidad permite limitar la aparición de direcciones falsificadas en una red, descartando el paquete cuando la dirección IP de origen no es válida.

**VLAN.** (Virtual Local Area Network). Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único switch físico o en una única red física.

Las VLANs se pueden extender entre varios Switches o Routers con interfaces Ethernet, usando técnicas de etiquetado de paquetes (802.1q, Vlan tagging), pudiendo entonces crear circuitos lógicos.