Medidas o Acciones para la Gestión de Tráfico y Administración de la Red

Servicios de Banda Ancha Fija y Banda Ancha Satelital

Medidas o Acciones para la Gestión de Tráfico y Administración de la Red

Servicios de Banda Ancha Fija y Banda Ancha Satelital

A continuación se detallan las medidas de Gestión de Tráfico y Administración de la Red que Movistar realiza o podría realizar sobre sus planes de Banda Ancha Fija y planes de Banda Ancha Satelital.

Para cada una de las medidas se indica en qué consiste aquella, las razones técnicas o comerciales por las cuales se realiza y el impacto que tendría eliminar dicha práctica. Se hace presente que si bien no se hace explícito en cada medida, la eliminación de cualquiera de ellas tiene impacto directo en la percepción de calidad o "experiencia de usuario" de la mayoría de los clientes, así como impacto en los costos de proveer el servicio y, por lo tanto, en el precio del servicio.

Las medidas de Gestión de Tráfico y Administración de la Red se realizan a nivel de red y no por plan, y en su mayoría no afectan la velocidad de navegación del cliente.

1. Gestión del Ancho de Banda

Movistar actualmente no aplica medidas de gestión del ancho de banda para el servicio de banda ancha fija ni para el servicio de banda ancha satelital en todo el país.

¿En qué consiste?

Consiste en administrar la capacidad de la red, debido a que ésta tiene un límite máximo de ancho de banda que pueden ocupar los clientes, tanto en la subida de datos como en la bajada. Esta restricción se podría presentar sólo en algunas partes de la red. Cuando el ancho de banda total que ocupan todos los clientes se acerca al máximo que permite esa parte de la red, se podría establecer que las comunicaciones del tipo "tiempo real" (tales como Telefonía IP o juegos on-line) hagan uso del ancho de banda que demandan, en desmedro de las comunicaciones del tipo "Intercambio de Archivos" (File Sharing). Estas últimas son aquellas en que el cliente puede esperar o dejar descargando archivos, como por ejemplo, las descargas del tipo Peer to Peer (P2P) (aplicaciones como uTorrent o Vuze son muy comunes para las descargas tipo P2P) o descarga directa de archivos, tales como Rapidshare, Mediafire u otras aplicaciones similares.

Si el ancho de banda total usado por las comunicaciones del tipo tiempo real llega al máximo que permite esa parte de la red, a las comunicaciones del tipo "Intercambio de Archivos" se les podría asignar una menor prioridad. Cuando el consumo total está por debajo del máximo que permite esa parte de la red, los protocolos tipo "Intercambio de Archivos" no se restringen.

Estas medidas de gestión del ancho de banda se podrían aplicar, por ejemplo, cuando los recursos de transmisión son limitados.

¿Por qué lo hacemos?

Se podría hacer para administrar el uso compartido entre todos los usuarios del recurso escaso que representa la capacidad limitada de alguna parte específica de la red y evitar que, ante una demanda excesiva de ancho de banda, se afecten todos los tipos de comunicaciones que estén realizando los clientes y perjudique las aplicaciones que son más sensibles a la congestión, como lo son las aplicaciones de "tiempo real".

Cabe señalar que los enlaces de microondas tienen un ancho de banda muy limitado y, la gestión de tráfico permitiría un suministro más eficiente del servicio, ya que mejora la experiencia de utilización de Internet por parte de los clientes.

¿Qué pasa si lo dejamos de hacer?

- Bajaría la experiencia de navegación de todos los clientes, ya que "todas" las comunicaciones, y no solo las del tipo "Intercambio de Archivos" se verían afectadas en los momentos en que el tráfico de los clientes ocupe la capacidad máxima de la red.
- Se produciría una lentitud generalizada del servicio de acceso a Internet, lo que se traduciría en un aumento de reclamos.

2. Almacenamiento Temporal de Contenidos o "Content Delivery Network" (CDN)

¿En qué consiste?

Consiste en almacenar temporalmente, lo más cerca del usuario y en servidores del propio proveedor del contenido o del ISP, los contenidos más vistos, con el objeto de descargarlos sólo una vez desde el sitio central, que por lo general está en otro país. El Content Delivery Network (CDN) se basa en que el 80% de los usuarios bajan el 20% de los contenidos, lo que se da en especial a nivel de videos. Con esto se logran ahorros de ancho de banda internacional y una mejor velocidad de respuesta, lo que se traduce en una mejor calidad de navegación del usuario.

YouTube, por ejemplo, emplea esta metodología para acceder a sus videos más populares en los distintos países.

¿Por qué lo hacemos?

Esta acción tiene por objetivo acercar los contenidos al cliente, logrando una mejor experiencia de navegación (mayor rapidez en la descarga) y evitar inversiones y gastos en ancho de banda internacional y transporte nacional.

¿Qué pasa si lo dejamos de hacer?

- Bajaría la experiencia de navegación de los usuarios.

- Dificultad de implementar servicios futuros.
- Aumentaría el nivel de reclamos por lentitud de la navegación.

3. Gestión de la Conexión del Usuario

¿En qué consiste?

Consiste en suspender temporalmente la conexión del cliente en el caso en que su conexión esté generando, hacia la red, una cantidad muy elevada de requerimientos "anormales" o "perturbaciones" (requerimientos desviados del promedio, miles de veces más que los de un cliente normal), afectando con ello a equipos de la red o bien a otros usuarios.

Desde la conexión del cliente se pueden introducir a la red de ISP, ya sea en forma voluntaria o involuntaria, una serie de "perturbaciones", las que se pueden producir por diversos motivos, tales como el mal funcionamiento del modem, equipos contaminados con virus troyano (spynet), u otros motivos. Si bien la red del ISP se diseña considerando que existe un cierto nivel de "perturbaciones", cuando ellas son excesivas se pone en riesgo la estabilidad de la red, o pueden perjudicar la calidad de servicio, afectando a miles de clientes.

En el caso que se le suspenda temporalmente la conexión a un cliente, se toma contacto con dicho cliente, se le informa lo que está ocurriendo y se lo apoya para que solucione su problema, con el fin de reponerle su conexión.

¿Por qué lo hacemos?

El ISP tiene la necesidad de proteger la red mediante acciones de efecto inmediato frente a circunstancias que puedan dañar la red, la seguridad de la misma y la calidad de servicio de todos los usuarios.

¿Qué pasa si lo dejamos de hacer?

- Se podría dañar la red y la seguridad de la misma.
- No contaríamos con herramientas para la mitigación de los problemas de operación.
- Podría haber inestabilidad de la red o saturación de algunos servicios "críticos", como por ejemplo, el servidor de nombres de dominio (DNS).

4. Duración Máxima de la Sesión del Usuario

¿En qué consiste?

Consiste en desconectar la sesión de un cliente si ésta se mantiene activa por más de un cierto tiempo (29 horas, aproximadamente), por lo que el usuario tendrá que reiniciar su conexión.

¿Por qué lo hacemos?

Si la sesión de un usuario se extiende por un tiempo demasiado prolongado se dificulta o se pierde el registro entre el "inicio" y el "fin" de la sesión, lo que imposibilita la "identificación" de la sesión del cliente, lo cual es requerido en ocasiones para responder a los juzgados que solicitan identificar a determinados usuarios que cometen ilícitos.

¿Qué pasa si lo dejamos de hacer?

- Habría un incumplimiento de exigencias legales, en cuanto a atender los requerimientos de los juzgados que realizan investigaciones, ya que no se podría identificar la sesión del cliente.

5. Gestión del Equipamiento Terminal del Lado Usuario

¿En qué consiste?

Consiste en que el ISP gestione técnicamente el equipamiento del lado cliente provisto por Movistar e instalado en el domicilio del usuario, habida cuenta que es en este equipamiento donde se define parte de la configuración del servicio y que son estos dispositivos los que permiten evaluar remotamente el correcto funcionamiento del servicio. El equipamiento terminal instalado en el domicilio del cliente marca el punto de terminación de la red del ISP, definiendo el límite del ámbito de responsabilidad del ISP.

La evolución tecnológica de los servicios y la convergencia hacia IP, hacen que el equipamiento terminal del lado cliente se convierta en dispositivos que gestionarán múltiples servicios, o Gateway Residencial (RGW, por sus siglas en inglés), desde el cual se atenderán todo tipo de servicios (voz, datos, video y otros).

En consideración a lo anterior, el equipamiento del lado cliente no debería ser de propiedad del cliente ni de terceros. Esto no imposibilita que el cliente instale diversos equipos aguas abajo del equipamiento terminal, los cuales no deben afectar la integridad de los servicios prestados ni la estabilidad de la red. A este respecto, el ISP no se puede responsabilizar de la velocidad y disponibilidad de la conexión a Internet si el usuario instala equipos por su cuenta, por ejemplo, routers inalámbricos (WiFi).

¿Por qué lo hacemos?

Porque la gestión del equipamiento del lado cliente es parte integral de la red y servicios del ISP.

¿Qué pasa si lo dejamos de hacer?

- El cliente podría tener una mala calidad de servicio o una mala experiencia de navegación, ya que el ISP no podría controlar los servicios que le provee.
- El ISP se vería imposibilitado de prestar nuevos servicios, adicionales al acceso a Internet, tales como Telefonía IP, IPTV, u otros de similar naturaleza.

6. Administración de las Direcciones IP

¿En qué consiste?

Consiste en que el ISP administre la forma cómo le entrega el "número" que identifica al cliente mientras navega en Internet (las llamadas "Direcciones IP"), pudiendo asignar direcciones IP "públicas" (direcciones correspondientes a los rangos asignados a Movistar por los organismos internacionales administradores de las direcciones IP), bajo las modalidades de asignación "fija" (el cliente navega siempre con la misma dirección IP) o "dinámica" (en cada sesión se le asigna una dirección IP para que el cliente navegue); o bien que el ISP le asigne direcciones IP "privadas" (direcciones que son de rangos definidos por organismos internacionales para el uso interno de las operadoras y empresas), bajo las modalidades de asignación "fija" o "dinámica".

Además, en las conexiones de banda ancha fija que emplean un modem/router inalámbrico (WiFi), o un modem/router que opera con una única dirección IP fija o dinámica, se hace uso de un mecanismo denominado "Traducción de Direcciones de Red" (Network Address Translation, o NAT), que consiste en utilizar direcciones IP privadas "al interior" de la red local (o LAN) del cliente, las cuales se "traducen" a una única dirección IP pública para acceder a Internet. Este mecanismo puede ocasionar problemas para que operen algunas aplicaciones de los clientes (tales como programas Peer to Peer, juegos online, u otros) y, además, hace más complejo (o podría llegar a impedir) que un cliente implemente servidores web, servidores de correo, servidores de juego, u otros desde su domicilio. Para salvar los problemas de la Traducción de Direcciones de Red existen varios mecanismos, siendo los más populares que en el router del domicilio del cliente se haga un "Mapeo de Puertos" (Port Mapping), mediante el cual se le asigna a cada equipo de la red local (o LAN) del cliente un determinado "Puerto", permitiendo de esta forma su identificación inequívoca, lo cual permite que las aplicaciones operen sin problemas, o bien que las propias aplicaciones adopten técnicas (denominadas "Traversal NAT") que les permiten operar en un ambiente con "Traducción de Direcciones de Red".

Con la implementación a futuro del protocolo IP versión 6 (IPv6), en reemplazo del protocolo IP versión 4 (IPv4) que se utiliza actualmente, habrá suficiente disponibilidad de direcciones IP y no será necesario efectuar la Administración de las Direcciones IP que se ha indicado. El ISP debe tener la facultad de planificar e implementar la transición de IPv4 a IPv6.

¿Por qué lo hacemos?

Es necesario usar eficientemente las direcciones IP, puesto que hoy en día son un recurso escaso en Internet (no se puede asignar una IP fija a cada cliente porque a nivel de Internet no hay suficientes direcciones IPv4).

El ISP debe tener libertad para administrar las direcciones IP que le asigna al usuario, públicas o privadas, y debe tener la facultad de ocupar NAT, para hacer más eficiente su uso.

¿Qué pasa si lo dejamos de hacer?

- Habría una ocupación innecesaria de un recurso escaso en Internet, como lo son las direcciones IPv4 públicas.

7. Filtro de Puertos y/o de Correo Spam

¿En qué consiste?

Consiste en bloquear algunas puertas de entrada lógicas desde Internet al PC del cliente (los denominados "Puertos") que normalmente los ocupan los hackers para transmitir virus, alterar la información en los computadores de los clientes y/o enviar correo Spam. El bloqueo se realiza tanto en el sentido de subida como en el de bajada. Esta medida se enmarca dentro de las acciones para preservar la seguridad de la red y de los usuarios.

En el ANEXO 1 se indican los Puertos a los que se les aplica bloqueo en la banda ancha fija de Movistar.

El bloqueo se aplica en el "borde" de la red de Movistar, con lo cual se protege a los usuarios de ataques externos a la red de Movistar, pero éste no afecta al tráfico interno a la red (tráfico entre clientes de Movistar). El bloqueo es general y no es factible aplicarlo en forma selectiva cliente a cliente.

¿Por qué lo hacemos?

El filtraje de puertos tiene por objeto evitar ataques maliciosos o propagación de virus, tanto a los clientes como a la propia infraestructura del ISP.

En el caso del Spam, se busca evitar que las direcciones IP del ISP se incluyan en las "listas negras" de Spam que elaboran algunos organismos internacionales, en cuyo caso se bloquea en el extranjero todo el rango de direcciones IP del ISP, afectando a una gran cantidad de clientes para enviar correos.

¿Qué pasa si lo dejamos de hacer?

- Habría un aumento de fallas en los equipos de los clientes, producto de que serían infectados por virus por parte de los hackers.
- Habría un impacto en la imagen del ISP, por baja en la calidad y lentitud de navegación en los PC infectados, con el consecuente aumento de reclamos.
- Los clientes podrían culpar a Movistar de no tomar las medidas necesarias para evitar la propagación de virus.
- Se podrían bloquear en el extranjero los servicios de correo de los clientes, producto de que las direcciones IP de Movistar aparecerían en las "listas negras" de Spam.

8. Filtro de Servicios y/o Aplicaciones Ilegales

¿En qué consiste?

Consiste en filtrar páginas web que contengan pornografía infantil, respondiendo a un compromiso corporativo del Grupo Telefónica, en conjunto con la "Internet Watch Foundation (IWF)", entidad internacional que vela por la erradicación de este tipo de contenidos en Internet.

Además, se aplican algunos filtros a pedido, para evitar otro tipo de acciones maliciosas, como por ejemplo la "suplantación de identidad" de alguna entidad, típicamente la dirección web de un banco para cometer estafas bancarias (esta práctica es denominada "Phishing").

El filtraje se efectúa, centralizadamente, en los "Servidores de Dominios" (DNS) que atienden a los clientes de Movistar, de modo que los clientes no puedan acceder a las direcciones IP que son filtradas. En el caso que los clientes utilicen un Servidor de Dominios diferente al de Movistar, o que digiten directamente la dirección IP del sitio requerido, el filtro no actuará.

Este filtro es sin perjuicio de dar cumplimiento a las resoluciones judiciales dictadas sobre filtro o bloqueo de contenidos ilegales.

La normativa de Neutralidad de Red excluye expresamente los contenidos, aplicaciones y servicios ilegales, por lo que no se debiera prohibir filtrar (sin esperar una orden judicial) contenidos, aplicaciones o servicios ilegales (como la pornografía infantil), en la medida que con el filtro aplicado no se afecte a contenidos legales que puedan estar alojados en el mismo sitio u operar con la misma dirección IP del contenido ilegal.

En el ANEXO 2 se indican los filtros que actualmente se aplican a nivel de DNS.

¿Por qué lo hacemos?

Se requiere evitar la instrumentalización de Internet como medio para cometer ilícitos, por medio de evitar la proliferación de contenidos, aplicaciones o servicios ilegales, que puedan ser filtrados sobre la base de información provista por organizaciones mundiales que entregan herramientas para ello (como por ejemplo la IWF) o bien por organismos nacionales de reconocido prestigio como la Superintendencia de Bancos e Instituciones Financieras o la Asociación de Bancos en el caso del Phishing.

¿Qué pasa si lo dejamos de hacer?

- Habría un impacto en la imagen de responsabilidad social de la empresa, en el caso de los sitios con pornografía infantil.
- Podría haber reclamos de clientes institucionales (Bancos) y de los usuarios por no haberles advertido del riesgo de estafa, debido al Phishing.

9. Protección ante Acciones Maliciosas

Movistar actualmente no aplica esta medida, pero en caso de contingencia, como ataques de usuarios mal intencionados, la podría aplicar.

¿En qué consiste?

Consiste en bloquear los tráficos de salida y/o de entrada de quienes hayan sido identificados como hackers, por el hecho que estén atacando a equipos de Movistar, o atacando a terceros a través de nuestra red, sin esperar la orden judicial para proceder.

Estas acciones de defensa de red se realizan en forma incremental, en su severidad, y pueden llagar al bloqueo completo del tráfico y/o servicios del hacker. La idea es bloquear el origen del ataque o eliminar el objetivo del ataque de forma que no tenga sentido seguir con el ataque.

En el ANEXO 2 se indican los filtros que actualmente se aplican a nivel de DNS.

¿Por qué lo hacemos?

Los operadores de red deben contar con herramientas que le permitan mitigar y/o eliminar los ataques de los hackers, mediante acciones de efecto inmediato, por cuanto existe la necesidad de proteger la red ante ataques maliciosos. En Internet los hackers están constantemente sondeando la red (equipos, plataformas, servidores, etc.) en busca de vulnerabilidades a fin de tomar control de dichos equipos o bien dejarlos fuera de operación. Estos ataques pueden durar desde minutos hasta días.

¿Qué pasa si lo dejamos de hacer?

- Podría haber pérdida de servicios, debido a la caída de equipos de la red producto de los ataques.
- Los ataques podrían producir lentitud en la navegación de los usuarios.

10. Servicios Especiales de Acceso a Internet y Priorización de Tráfico

Si el cliente tiene contratado el Servicio Público Telefónico de Movistar, con tecnología IP, dicho servicio ocupa parte del ancho de banda de la conexión de banda ancha fija del cliente, en los momentos en que se cursan llamadas telefónicas.

¿En qué consiste?

Consiste en que el ISP pueda prestar servicios de acceso a Internet con características técnicas especiales, como es el caso de aquellos que requieren un retardo mínimo de respuesta, tales como la Telefonía IP, los juegos en línea y, muy pronto, servicios de Telemetría (por ejemplo, medición remota de procesos industriales), Telemedicina (por ejemplo, supervisión remota de cirugías de alta especialidad o complejidad), y Video conferencia de alta calidad, entre otros. En otras palabras, que

los servicios de acceso a Internet que presten los ISP no sólo se diferencien por la velocidad de la conexión, como lo es hoy en día, sino también por la respuesta inmediata y la calidad de la imagen cuando ello se requiera.

La priorización de tráfico consiste en dar preferencia a cierto tipo de comunicaciones por sobre el resto de las comunicaciones de la red, cuando se requiere que determinados servicios no sufran retardos o interrupciones.

Actualmente Movistar provee servicio público telefónico, con tecnología IP, a través de las conexiones de banda ancha, y este servicio ocupa parte del ancho de banda de la conexión de banda ancha del cliente, en los momentos en que cursan llamadas telefónicas.

Los nuevos servicios de acceso a Internet con características técnicas "especiales" serán ofrecidos mediante ofertas no discriminatorias a todos los clientes. Asimismo, se les podrán ofrecer condiciones especiales a los proveedores de contenido que deseen diferenciarse de su competencia mejorando la velocidad de descarga de sus contenidos a los clientes, por ejemplo, un proveedor de videos de alta definición por Internet.

Cabe destacar que la priorización de tráficos se requiere sólo en la medida en que el cliente tenga contratado, simultáneamente con el servicio de acceso a Internet, algún servicio que requiera de dicha priorización.

¿Por qué lo hacemos?

Se realiza con el objeto de dar al usuario la posibilidad de contratar un servicio que tenga las características técnicas que más se ajusten a sus necesidades de uso, respetando la libertad de comercialización de los operadores, como expresión de la libertad de emprender.

También tiene por objeto no inhibir la innovación y desarrollo de servicios más especializados que los actuales, los cuales serán factibles de proveer en la medida que existan redes más modernas.

Con estas medidas se busca garantizar que los requerimientos técnicos de transmisión que requieren algunos servicios sean los adecuados (por ejemplo, mínima demora para tráficos sensibles al retardo, como lo son los servicios de tiempo real, tales como voz o video, los que requieren para su adecuado funcionamiento un mínimo retardo en la transmisión). En particular, la priorización del tráfico es crítica y necesaria en los momentos de plena utilización de la red.

¿Qué pasa si lo dejamos de hacer?

- Habría problemas para desarrollar nuevos servicios diferenciados.
- Tendría impacto en la calidad de los servicios sensibles al retardo.
- Habría dificultad para asegurar condiciones contractuales, con lo que bajaría la satisfacción del cliente por una menor calidad de los servicios sensibles al retardo.
- Se restringiría el desarrollo de nuevos servicios sobre Internet, tales como la Telemetría, Telemedicina, Video conferencia, y otros.

11. Servicios Diferenciados Sobre Ancho de Banda Adicional

Actualmente Movistar provee su servicio de televisión IP (IPTV) sobre ancho de banda adicional a la banda ancha fija. Esta medida de Gestión de Tráfico no afecta el servicio de banda ancha fija del usuario, por cuanto se refiere a servicios que se prestan fuera de su conexión a Internet.

¿En qué consiste?

Consiste en prestar "otros servicios" on-line, distintos del "servicio de acceso a Internet", utilizando para ello ancho de banda adicional al ancho de banda de la conexión de banda ancha del cliente que se emplea para dar acceso a Internet. Actualmente en estas condiciones se prestan servicios de televisión IP (IPTV) y, a futuro, se desarrollarán otros servicios, como por ejemplo podría ser una conexión de Red Privada Virtual (o VPN por su sigla en inglés), que una empresa pueda contratar para que sus empleados realicen teletrabajo.

La prestación de estos "otros servicios" no puede afectar la velocidad contratada originalmente por el cliente.

¿Por qué lo hacemos?

Se debe permitir el desarrollo de nuevas aplicaciones y servicios innovadores sobre la conexión de banda ancha, distintos del servicio de acceso a Internet, no coartando el desarrollo de las redes y tecnologías y los nuevos modelos de inversión y financiamiento que de ello provengan.

¿Qué pasa si lo dejamos de hacer?

- Sería un freno para el desarrollo de nuevos servicios (distintos del acceso a Internet) y de servicios de valor agregado.
- Habría un impacto en la calidad de aquellos servicios diferenciados que sean sensibles al ancho de banda de la conexión, dificultando asegurar las condiciones contractuales.
- Habría que habilitar una segunda conexión de banda ancha al cliente, para prestarle a través de esta nueva conexión los servicios diferenciados de valor agregado.

ANEXO 1

Puertos a los que se les aplica Bloqueo

Filtraje de puertos generales para la Banda Ancha Fija:

- deny ipv4 127.0.0.0 0.255.255.255 any
- deny tcp any any eq 445
- deny tcp any any eq 135
- deny udp any any eq 135
- deny tcp any any eq 137
- deny udp any any eq netbios-ns
- deny tcp any any eq 138
- deny udp any any eq netbios-dgm
- deny tcp any any eq 139
- deny udp any any eq netbios-ss
- deny udp any any eq 1900
- deny tcp any any eq 7547
- deny tcp any any eq 4567
- deny tcp any any eq 51005
- deny tcp any any eq 53
- deny udp any any eq 53

ANEXO 2

Filtros a nivel de Servidores de Dominio (DNS)

Sitios filtrados por concepto de Phishing:

- preload-nxdomain "bankochile.com";
- preload-nxdomain "security-bancochile.com";
- preload-nxdomain "bcibanco.com";
- preload-nxdomain "verynx.cn";
- forward "verynx.cn" only { 200.28.34.169; 200.28.34.170; };

Sitios filtrados por orden judicial:

- preload-nxdomain "verdaderasidentidades.com";
- forward "verdaderasidentidades.com" only { 200.28.34.169; 200.28.34.170; };

Sitios filtrados por concepto de ataques:

- preload-nxdomain "boughtem.nowslate1703.info";
- preload-nxdomain "newircd.slateit1703.info";
- preload-nxdomain "boughtemm.nowsmirror.info";
- preload-nxdomain "rapidkeys.com";
- preload-nxdomain "santandersantiago.cl.rapidkeys.com";
- preload-nxdomain "l.ocalhost.host";