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

Servicio WiFi Móvil (Internet Móvil), Planes Multimedia, Planes de Datos y Planes de Internet en el Tablet [*]

[*] Los planes de Internet en el Tablet ya no se comercializan.

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

Servicio de WiFi Móvil (Internet Móvil), Planes Multimedia, Planes de Datos y Planes de Internet en el Tablet[1]

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 Internet Móvil y Planes Multimedia (planes para Smartphones).

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. Optimización del Tráfico

Movistar actualmente no aplica medidas de optimización del tráfico para el servicio de Internet móvil (WiFi Móvil) ni para los planes multimedia, con la excepción en este último caso del Plan Plus Libre en que se aplica esta medida en relación a la descarga de videos. Lo anterior se aplica en todo el país.

¿En qué consiste?

Consiste en reducir el tamaño de las páginas web, imágenes y videos que se descargan a través de la red móvil, con el objeto de reducir el volumen de datos y acelerar las descargas. De esta forma, la descarga de páginas web se optimiza eliminando información que no es útil para el usuario, comprimiendo además la información de los videos e imágenes para que puedan ser vistos sin retardo adicional.

Estas técnicas de optimización, en general, no son perceptibles por el usuario, pero sí son de gran utilidad para que la experiencia de la navegación sea de mayor calidad. Además, tiene la ventaja de disminuir el volumen de datos descargados, considerando que los planes de acceso a Internet móvil por lo general están afectos a límites de descarga.

[1] Los planes de Internet en el Tablet ya no se comercializan.

¿Por qué lo hacemos?

Todas estas medidas son necesarias para mantener una velocidad de descarga y lograr un uso más eficiente de la red, sobre la base que los datos viajan por medios inalámbricos compartidos, permitiendo así acelerar la navegación del cliente.

¿Qué pasa si lo dejamos de hacer?

- Se incrementaría el tráfico especialmente en las horas de alto tráfico, afectando la calidad de la navegación de todos los usuarios.
- El usuario percibiría lentitud de navegación y descarga.

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.
- Aumentaría el costo operacional por concepto de enlaces internacionales.
- Dificultad de implementar servicios futuros
- Aumentaría el nivel de reclamos por lentitud de la navegación.

3. 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".

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.
- Habría un aumento de inversiones y de costos de operación, por ampliaciones de red y de las plataformas.

4. 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.

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

Los clientes del servicio móvil sin saldo no tienen acceso a la técnica DNS tunneling.

¿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 la empresa 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 la empresa aparecerían en las "listas negras" de Spam.
- Pérdida de imagen de la compañía, al ser clasificado como fuente de Spam a nivel mundial.

5. 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 una pérdida de clientes institucionales (Bancos) y reclamos de los usuarios por no haberles advertido del riesgo de estafa, debido al Phishing.

6. 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.
- Habría un impacto en la imagen de la empresa y un aumento de los reclamos.

7. Límite del Máximo de Sesiones por Usuario

¿En qué consiste?

Consiste en limitar la cantidad de conexiones simultáneas que establece el navegador o las APP que usa el usuario. Cada vez que el usuario abre una nueva página web (aun cuando sea dentro del mismo navegador), utiliza una aplicación, o bien establece una comunicación en línea (como Chat o MSN), se abre una conexión distinta para mantener el orden en la navegación y la descarga de información.

Estas conexiones se limitan a un máximo de 2.048 por usuario, número que se considera lo suficientemente elevado como para no interferir en las actividades de navegación o de comunicaciones que usualmente se realizan en Internet.

¿Por qué lo hacemos?

Se hace con el objeto de no saturar los equipos que le prestan el servicio al usuario, los que podrían quedar vulnerables a actos malintencionados, afectando la seguridad de la red y de los usuarios, considerando que cada una de las "conexiones simultáneas" del usuario son registradas y tratadas por separado en los equipos y plataformas técnicas de la red, además de poder registrar la dirección IP asignada al cliente cada vez que se conecta a Internet, información que es requerida por la autoridad judicial correspondiente.

¿Qué pasa si lo dejamos de hacer?

- Podríamos no cumplir con la información de trazabilidad que solicita la autoridad judicial.

8. Bloqueo de Tráfico Entrante no Iniciado por el Usuario (Control de Polución de Internet)

¿En qué consiste?

Consiste en bloquear el tráfico que se origina "desde la red Internet hacia el usuario", sin que el usuario lo haya solicitado expresamente, con el objeto de mejorar la experiencia de navegación del cliente y evitar así que aumente el volumen de datos que consume el cliente.

¿Por qué lo hacemos?

Para evitar ataques y tráficos no requeridos por el usuario, que afecten el consumo de datos, especialmente a los clientes sensibles a los volúmenes de tráfico cursados.

Además, dada la naturaleza de la red Móvil (una red de acceso compartida), es necesario bloquear este tráfico para mantener la integridad de las redes.

¿Qué pasa si lo dejamos de hacer?

- Se cargaría a la cuota de tráfico de los clientes, aquellos tráficos que no han sido generados o solicitados por ellos, con la probabilidad de alcanzar la cuota de tráfico o generar costos adicionales.

9. Gestión de Capacidad para la Calidad de Servicio en Episodios de Congestión

¿En qué consiste?

Con el objeto de garantizar lo más posible a los usuarios alcanzar la mayor velocidad contratada, en situaciones de congestión, se gestiona el acceso a capacidad de los usuarios de forma que los clientes que no hayan superado su umbral de navegación lograrán mayor velocidad de acceso, a diferencia de aquellos clientes que hayan cumplido su cuota de descarga, los que podrán ver reducida su velocidad dentro de su ciclo de facturación.

De la misma forma, a los usuarios de planes libres se les podría reducir la velocidad máxima de navegación de bajada hasta una calidad de 3G, en horario y/o lugares de congestión, en el evento de que su consumo de datos haya sobrepasado los 130 GB en el tráfico total.

Se podrá aplicar como medida de Administración de Red, a los usuarios que estén dentro del 5% con mayor tráfico de datos de su plan, una disminución de la velocidad máxima de navegación de bajada hasta 256 Kbps.

Para el caso de planes WiFi Móvil, una vez consumida dentro del período de facturación respectivo la capacidad de cada plan contratado, los clientes podrán continuar navegando a una velocidad máxima de hasta 64 Kbps.

¿Por qué lo hacemos?

Para propiciar un uso de la red adecuado a las condiciones comerciales contratadas por los clientes, disminuir la congestión y permitir una mejor experiencia de servicio para los clientes.

¿Qué pasa si lo dejamos de hacer?

- Se pone en riesgo el cumplimiento de las condiciones ofertadas al cliente
- Ineficiencia en el acceso a los recursos de red de los usuarios.

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

Movistar actualmente no provee servicios especiales de acceso a Internet ni efectúa priorización de tráfico en la red de móvil en todo el país.

¿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.

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 no provee servicios diferenciados sobre ancho de banda adicional en la red móvil. Esta medida de Gestión de Tráfico no afecta el servicio de Internet móvil ni los planes Multimedia del usuario, por cuanto se refiere a servicios que se podrían prestar 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 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 del cliente, 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 al cliente, para prestarle a través de esta nueva conexión los servicios diferenciados de valor agregado.

12. Gestión del Ancho de Banda

Movistar actualmente no aplica medidas de gestión del ancho de banda para el servicio de Internet móvil ni para los planes Multimedia 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.

ANEXO 1

Puertos a los que se les aplica Bloqueo

Filtraje de puertos generales para Internet Móvil:

- 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";