Medidas o Acciones para la Gestión de Tráfico y Administración de la Red
Servicios de Banda Ancha Fija

A continuación, se detallan las medidas de Gestión de Tráfico y Administración de la Red que SUMERTEL COMUNICACIONES S.A.S realiza o podría realizar sobre sus planes de Banda Ancha.

Para cada una de las medidas se indica en qué consiste, 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

¿En qué consiste?
Consiste en la administración de la capacidad del tráfico de red que se puede enviar o recibir a través de una conexión en un determinado tiempo, debido a que ésta tiene un límite máximo de ancho de banda que pueden ocupar los clientes, tanto en carga como en descarga de datos. Esta restricción se podría presentar sólo en algunas partes de la red.

Cuando se trate de planes residenciales o clientes adscritos a planes con reusó, con el fin de garantizar la mejor experiencia de navegación a todos los usuarios de la red fija y atendida la naturaleza del servicio ofrecido, se les podría reducir la velocidad máxima de navegación, dicha variación está sujeta al reusó del plan en horarios y lugares de congestión, en el evento que el cliente dé un uso indebido de su servicio (lo explote con fines comerciales, lo revenda o realice redistribución a terceros), según los términos indicados en las Condiciones Comerciales del respectivo plan que haya contratado, las cuales están publicadas en el sitio web de SUMERTEL COMUNICACIONES S.A.S se limitara el número de conexiones o de hilos.

¿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. 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 de los equipos de borde, 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 restablecer 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).

3. Gestión del Equipamiento Terminal del Lado Usuario

¿En qué consiste?
Consiste en que el ISP gestione técnicamente el equipamiento del lado cliente provisto por SUMERTEL COMUNICACIONES S.A.S 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 dentro de su red Lan, 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 de valor agregado, adicionales al acceso a Internet (Telefonía IP, IPTV).

4. Administración de las Direcciones IP

¿En qué consiste?

Consiste en que el SUMERTEL COMUNICACIONES S.A.S administra 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 SUMERTEL COMUNICACIONES S.A.S por los organismos internacionales administradores de las direcciones IP), bajo las modalidades de asignación “fija “o “Dinámica”. Otro tipo de asignación que se puede realizar es por medio de 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 router o Ont inalámbrico (WiFi), o un dispositivo 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 del protocolo IP versión 6 (IPv6), en reemplazo del protocolo IP versión 4 (IPv4) que actualmente aún se encuentra en uso, hay suficiente disponibilidad de direcciones IP y no será hace necesario efectuar la Administración de las Direcciones IP que se ha indicado.

¿Por qué lo hacemos?

Es necesario usar eficientemente las direcciones IP, especialmente los direccionamientos que pertenecen a la versión 4 de la misma, ya que hoy en día son un recurso escaso en Internet, por tanto, no se puede asignar una IP fija a cada cliente.

SUMERTEL COMUNICACIONES S.A.S tiene la libertad para administrar las direcciones IP que le asigna al usuario, públicas o privadas, y debe cuenta con la facultad de ocupar NAT, para hacer más eficiente su uso. Vale la pena resaltar que dentro del proceso de asignación de recursos Ipv4 público a un cliente se encuentran vinculadas ciertas políticas y responsabilidades uso que se le asigna al cliente.

¿Qué pasa si lo dejamos de hacer?
• Habría una ocupación innecesaria de un recurso escaso en Internet, como lo son las direcciones IPv4 públicas.

5. 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, o para evitar el acceso a los puertos que SUMERTEL COMUNICACIONES S.A.S utiliza para la gestión y administración de los dispositivos que instala en el domicilio de sus clientes, ya que dicho acceso posibilitaría modificar las configuraciones y adulterar el servicio de SUMERTEL COMUNICACIONES S.A.S 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 SUMERTEL COMUNICACIONES S.A.S

El bloqueo se aplica en el "borde" de la red de SUMERTEL COMUNICACIONES S.A.S, con lo cual se protege a los usuarios de ataques externos a la red, pero éste no afecta al tráfico interno a la red (tráfico entre clientes de SUMERTEL COMUNICACIONES S.A.S). 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 SUMERTEL COMUNICACIONES S.A.S de no tomar las medidas necesarias para evitar la propagación de virus, excepto las direcciones Ip publicas asignadas directamente a los clientes, dichas medidas deben ser implementadas dentro de la red Lan del cliente.
• Se podrían bloquear en el extranjero los servicios de correo de los clientes, producto de que las direcciones IP de SUMERTEL COMUNICACIONES S.A.S aparecerían en las "listas negras" de Spam.

6. Filtro de Servicios y/o Aplicaciones Ilegales

¿En qué consiste?
Consiste en filtrar páginas web que contengan pornografía infantil, respondiendo a un requerimiento consignado en la Ley 679 de 2001, y bajo solicitud del Ministerio de las tecnologías de información y las comunicaciones (MINTIC) entidad 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 SUMERTEL COMUNICACIONES S.A.S, 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 SUMERTEL COMUNICACIONES S.A.S, 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.

7. Protección ante Acciones Maliciosas

SUMERTEL COMUNICACIONES S.A.S *usa actualmente esta medida sobre el direccionamiento IP que intenta realizar escaneo sospechoso y/o ataques de usuarios mal intencionados hacia dispositivos de nuestra red.*

¿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 SUMERTEL COMUNICACIONES S.A.S, 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.

ANEXO 1
Puertos a los que se les aplica Bloqueo
Filtraje de puertos generales para la Banda Ancha Fija:

Puerto	Protocolo	Acción
53	TCP/UDP	Drop
25	TCP	Filtered out
110	TCP	Filtered out
143	TCP	Filtered out
995	TCP	Filtered out
465	TCP	Filtered out

ANEXO 2
Filtros a nivel de Servidores de Dominio (DNS)
Sitios filtrados por concepto de Phishing:
• Actualmente no se cuenta con filtro.

Sitios filtrados por orden judicial:
• preload-nxdomain " www.s0lc.net";
• Deny { 198.255.56.18};

Sitios filtrados por concepto de ataques:
• Actualmente no se cuenta con filtro.