Medidas de gestión de tráfico y administración de red

a. Gestión del Ancho de Banda

La red de datos de DIRECTV tiene una capacidad finita que es compartida por todos los subscriptores, cuando la ocupación de la red se acerca a su límite máximo se vuelve necesario gestionar el ancho de banda para asegurar una mejor experiencia de usuario. Por esta razón DIRECTV podría utilizar técnicas de Calidad de Servicio (QoS) que durante escenarios de congestión permiten controlar y administrar los recursos de red por medio del etiquetado de los diferentes tipos de tráfico (video, audio, archivos, etc.) a solicitud del cliente y aplicable únicamente en su servicio, permitiendo, por ejemplo, priorizar las comunicaciones del tipo "tiempo real" (como telefonía IP) sobre comunicaciones menos sensibles a la latencia como el intercambio de archivos. Cuando la utilización de la red vuelve a niveles normales el tráfico vuelve a ser tratado de manera regular.

- **Los principales beneficios son:**

Optimización de los recursos de la red permitiendo que en escenarios de congestión las comunicaciones sensibles al retardo sean priorizadas sobre comunicaciones menos sensibles.

- **Impacto en caso de eliminar la medida:**

Degradación generalizada de la experiencia de usuario en escenarios de congestión en los que todo el tráfico se vería afectado pues se atendería con la misma prioridad.

b. Gestión del Equipamiento Terminal del Lado Usuario

Mantener la configuración personalizada en los perfiles de los abonados, y de esa forma garantizar la asignación de ancho de banda a cada usuario y prioridad en la calidad de acuerdo con los paquetes contratados por los usuarios, garantizando la comunicación activa con el sistema administrativo de suscritores para la perfecta administración automatizada, y garantizar toda la gestión correcta evitando actividades manuales que pongan el peligro el flujo adecuado de una administración correctamente centralizada.

DIRECTV no limita el derecho de los usuarios del servicio de acceso a Internet a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos que se conecten a su red, siempre y cuando éstos se encuentren homologados, tomando en cuenta que no todos los dispositivos existentes en el mercado cuentan con las caracterizarías técnicas para poder ser conectados a su red.

c. Administración de las Direcciones IP

Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local; es un identificador que permite el intercambio de información en Internet. Las direcciones IP son asignadas por el organismo internacional, Internet Assigned Numbers Authority, quien administra dichas direcciones de manera eficiente para permitir el acceso a Internet de todos los usuarios a nivel global de manera equitativa. Toda vez que se trata de insumos finitos, la administración de direcciones IP, se realiza de la siguiente manera:

Asignación dinámica y compartida de las direcciones IP "públicas" de los tipos:

- IPv4 a través de Carrier Grade NAT, lo que implica que una misma direcicón IPv4 pública puede ser compartida por una multiplicidad de direcciones IPv4 privadas
- IPv6 con asignación pública directamente sobre el CPE en sitio del cliente
- Asignación dinámica de direcciones IPv4 privadas serán las que se asignen directamente en el CPE en sitio del cliente
- La navegación en Internet genera lo que se conoce comúnmente como sesiones, las cuales emplean las direcciones IP privadas; el Proveedor podrá gestionar la cantidad de direcciones simultáneas disponibles al usuario.

La implementación de lo anterior generará:

- Ocupación adecuada de las direcciones IPv4 públicas
- Disponibilidad de las direcciones IPv4 públicas.

d. Filtro de Puertos y/o de Correo Spam

El bloqueo es la técnica que impide el acceso de los usuarios finales a un sitio web determinado o la utilización de un tipo de contenido o servicio particular, ya sea de manera temporal o permanente.

Política de bloqueo de puerto 25 SMTP:

Causa: Por existir riesgo a la integridad de la red y a las comunicaciones legítimas de los usuarios finales. Debido a la prevalencia de máquinas que tienen gusanos, virus u otro software malintencionado que genere grandes cantidades de correo electrónico no deseado.

- ✓ En qué consiste: Bloqueo del puerto 25 (SMTP) del protocolo de transporte TCP.
- ✓ En qué casos y para qué se utiliza: Se establece este filtrado en la entrega inicial del servicio de acceso a Internet en todos los casos.
- ✓ Impacto en la experiencia del usuario final: Al intentar utilizar este puerto no obtendrá conexión. El usuario final puede solicitar la apertura de este filtro para efectos de soportar el servicio en el puerto 25.
- ✓ Afectaciones del usuario final en caso de que no fuera implementada: Afectación al servicio de los clientes que legítimamente usan este puerto, al ser potencialmente incluido en listas negras de correo.

e. Filtro de Servicios y/o Aplicaciones Ilegales

DIRECTV podrá bloquear el acceso a determinados contenidos, aplicaciones o servicios con el fin de preservar la privacidad de sus usuarios, la seguridad de la red, así como para prevenir la comisión de delitos. Asimismo, DIRECTV podrá bloquear el acceso a contenidos, aplicaciones o servicios ofrecidos en Internet.

Los casos en los que se aplicaría esta técnica serían los siguientes:

- ✓ A petición expresa y consentida del usuario final. En este supuesto, su utilización radicaría más a intereses propios del usuario final quien señalará de manera específica el contenido que desea restringir al proveedor del servicio de internet;

- ✓ Cuando cierto contenido, aplicación o servicio dentro de internet sea un riesgo técnicamente comprobable y pueda repercutir a la integridad y seguridad de la red, así como la privacidad e inviolabilidad de las comunicaciones de los usuarios finales. Se utilizaría con la finalidad de garantizar la continuidad del funcionamiento de la red así de la seguridad de los usuarios finales y sus equipos.

- ✓ Contenido, aplicación o servicio determinado como ilícitos por la autoridad competente por medio de ordenamiento jurídico aplicable y obligatorio para el proveedor del servicio de internet.

IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL

- ✓ No tendrá acceso al contenido, aplicación o servicio bloqueado dentro del plazo que persista el supuesto que lo originó o de forma indefinida.

POSIBLES AFECTACIONES EN CASO DE NO APLICARSE

- ✓ A LA RED: De no bloquearse contenido que afecten la integridad y seguridad de la red o que sean señalados como ilícitos, se perturbaría y se comprometería el tráfico que exista dentro de la misma red, infectándose de posibles virus o amenazas de terceros. En el caso de bloqueo de contenido a petición del usuario final, no tendría afectación alguna en la red.

- ✓ AL USUARIO FINAL O EN SU SUS COMUNICACIONES. De no bloquearse contenido que afecten la integridad y seguridad de la red o que sean señalados como ilícitos, existe una gran posibilidad de fuga de datos privados de los usuarios finales así de una evidente interceptación de las comunicaciones por parte de terceros.

f. Protección ante Acciones Maliciosas que Directv podría aplicar:

Consiste en la protección e implementación de técnicas informáticas para la seguridad e integridad de la red del proveedor del servicio de internet. Dicha protección puede ser implementada mediante la aplicación de políticas/reglas en el firewall (cortafuegos), esto con la finalidad de aislar a clientes dentro de la red de ataques externos e internos.

- ✓ CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZARÍA.
  Se aplica en casos donde existen ataques de agentes externos e internos que buscan alterar, degradar, perturbar o corromper el funcionamiento eficiente y correcto de la red (virus, malware, spyware y ransomware). Para estos casos, la implementación de técnicas informáticas por parte del proveedor del servicio de internet hará todo lo posible por anular, atacar y desaparecer el ataque

- ✓ IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.
  Puede que la velocidad de navegación del usuario final baje o no tenga acceso a contenido, aplicación o servicio por causas originadas del ataque. El proveedor del servicio de internet se comprometerá en realizar todas las acciones posibles que tenga a su alcance para que el tiempo de impacto sea mínimo.

- ✓ POSIBLES AFECTACIONES EN CASO DE NO APLICARSE A LA RED
  Puede comprometerse el tráfico de datos que se encuentre en la red, infectándose de posibles virus y en consecuencia dañando la estabilidad del servicio de internet.
- ✓ AL USUARIO FINAL O EN SU SUS COMUNICACIONES. Posible afectación en la velocidad de navegación además de acceso no autorizado a terceros causantes del ataque a datos privados además de las comunicaciones del usuario final

Servicios Especiales de Acceso a Internet y Priorización de Tráfico

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.

Servicios Diferenciados Sobre Ancho de Banda Adicional

Directv podría 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. Por ejemplo, servicios de televisión IP (IPTV)

Gestión de la Conexión del Usuario

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.