Solución Integral de Red

para ISPs en Crecimiento por **Auben Networks**

(WhitePaper)

Introducción

Los ISP que se dedican a dar acceso a internet a poblaciones intermedias y pequeñas, al igual que proveedores de servicios de banda ancha rural, enfrentan diferentes retos únicos relacionados con la sostenibilidad del modelo de negocio, por lo que deben generar soluciones innovadoras para crear condiciones favorables, por ejemplo:

Asunto	Desafíos	Soluciones
Costos de infraestructura	Construir y mantener la infraestructura de banda ancha en áreas apartadas es costoso debido a la necesidad de redes extensas de fibra óptica, torres celulares y tecnología satelital.	Asociaciones con tendido eléctrico y redes codesarrolladas con las comunidades
Condiciones geográficas	Terrenos difíciles, como montañas, bosques y grandes distancias, que dificultan la colocación de cables o la configuración de puntos de acceso inalámbrico.	Apalancarse en tendidos de red eléctrica o servicios satelitales
Base de clientes limitada	La densidad de población más baja significa menos clientes potenciales.	Usar al límite las especificaciones de concurrencia y/o uso de frecuencias
Regulaciones y permisos	El panorama regulatorio para obtener los permisos necesarios para el despliegue de banda ancha puede ser complejo y lento.	Acogerse a programas de gobiernos para disminución de la brecha digital
Apoyo financiero	Acceder a financiamiento y apoyo financiero de programas federales y estatales puede ser un desafío.	Suscribir acuerdos locales con gobiernos provinciales.
Factores ambientales	Las condiciones meteorológicas adversas, como lluvias intensas, nieve y fuertes vientos, pueden dañar la infraestructura y causar interrupciones frecuentes en el servicio.	Acogerse a los términos de la infraestructura eléctrica
Asequibilidad y accesibilidad	Incluso cuando la infraestructura está disponible, los altos costos de los servicios de internet pueden dificultar que los residentes los puedan pagar.	Suscribir acuerdos locales con gobiernos provinciales. Entrar en cadena de valor de CDN.
Brecha digital	La brecha entre las grandes áreas urbanas y provincia en términos de acceso a internet puede tener implicaciones significativas para el desarrollo económico, la educación, la atención médica y la calidad de vida en general de las comunidades rurales.	Proveer el acceso a internet a oficinas de gobierno, escuelas, centros de salud y en general servicios a la comunidad hace la diferencia.
Calidad percibida del streaming (garantizar el transporte)	Entregar al usuario servicios de streaming sin cortes o “buffering”	Tecnologías de “caching” y CDN. Aplicar técnicas de QoS
Bloqueo (Baneo) de direcciones IP públicas	Una o varias IP públicas o servicios se niegan como consecuencia de tráfico sospechoso o botnets	CG-NAT con protección DDoS y reasignación automática de prefijos/usuarios

Desde el punto de vista tecnológico, los retos tienen que ver con simplicidad y eficiencia. Tradicionalmente las funciones de administración de usuarios y terminales se asocian a las funciones contables en un sistema de gestión integral.
El presente documento plantea una aproximación a mejorar la experiencia de usuario (UX) a partir de una arquitectura simplificada con funciones de red específicas que ofrece escalabilidad, crecimiento y confiabilidad para los proveedores de servicios de conexión a internet.

Mitos y realidades

Mito #1: *CGN es para operadores grandes!*
Realidad: CGN o - "Carrier Grade" NAT- se refiere, desde el punto de vista funcional, a una serie de características especiales que permiten persistencia y trazabilidad de las sesiones para que el usuario no se vea actado por cortes o reinicios, características de especial utilidad para comunicaciones Peer-toPeer (P2P) en tiempo real (video llamadas), streaming y gaming. Por otro lado, LSN (Large Scale NAT) o NAT a gran escala sí que aplica para grandes cantidades de usuarios, léase ISP grandes.
Mito #2: *Los micro-cortes no se notan.*
Realidad: Los usuarios SI perciben los micro-cortes que se reflejan en interrupciones de la comunicación y/o "buffering" que degrada la calidad de la experiencia.
¡El gran sueño del usuario es tener una conexión estable y sin interrupciones, el sueño del ISP es ofrecerla!
Mito #3: *La Experiencia de Usuario (UX) no es tan importante en sitios remotos o comunidades pequeñas...*
Realidad: El creciente número de usuarios remotos y nómadas digitales demanda un servicio impecable. ¿Estamos dejando guita sobre la mesa?

Mito #4: *La atención al cliente es un mal necesario.*
Realidad: 66% de usuarios que cambian de operador por el mal servicio al cliente. Tener habilitados diferentes canales de atención (teléfono, Chat, Redes sociales, e-mail, WhatsApp) ayudan a tener tiempos de respuesta rápidos y dar respuestas concretas. Y si, la competencia son los que entregan servicios satelitales.
Mito #5: *Un ataque DoS/DDoS solo le pasa a los grandes.*
Realidad: Es muy fácil ser parte de un botnet, sólo con un click a un spam... Afortunadamente CG-NAT ayuda a mitigar alertando para mover los usuarios de las IP penalizadas antes de aplicarles "blackhole" (DDoS IP protection)
Mito #6: *Monitoreo con herramientas open source es todo lo que necesito...*
Realidad: Observabilidad... Una herramienta especializada permite no solamente monitorear estados sino ir más allá, permite determinar tendencias y tomar acción de manera proactiva, así como generar reportes ejecutivos que hacen la vida fácil al operador.

La experiencia de Usuario (User Experience, UX)

En el contexto de un ISP la ***Experiencia de Usuario*** (UX, por sus siglas en inglés) puede definirse como: "El conjunto de percepciones, emociones e interacciones que los clientes tienen con los servicios, productos y soporte ofrecidos por el ISP. Esto incluye aspectos como la facilidad de instalación, calidad de la conexión, rapidez en la resolución de problemas, claridad en la facturación, interfaz de las plataformas digitales (como apps o portales web), y atención al cliente."
Es decir, que tan satisfecho queda el usuario al usar el servicio.

En este contexto específico, se deben considerar elementos clave que impactan la experiencia de usuario, como:

- **Estabilidad de la conexión:** Conexiones “sin parpadeos” o sin caídas del Wi-Fi que permitan tranquilidad al usuario.
- **Calidad del servicio:** Velocidad estable, mínimo tiempo de latencia y sin interrupciones.
- **Facilidad de uso:** Procesos simples para la activación de servicios y uso de aplicaciones.
- **Atención al cliente:** Respuesta rápida, amabilidad y soluciones eficientes en soporte técnico.
- **Transparencia:** Claridad en los planes, precios y políticas sin costos ocultos.
- **Personalización:** Opciones adaptadas a las necesidades del cliente, como paquetes de canales o velocidades de internet ajustables.

El objetivo principal es proporcionar a los usuarios una interacción fluida, satisfactoria y libre de frustraciones en cada etapa, desde la contratación hasta el uso diario de los servicios.

Importancia del NAT robusto (CGNAT)

CGNAT, o *Carrier Grade Network Address Translation*, es una técnica que permite que varios dispositivos utilicen la misma dirección IP pública para acceder a Internet. Se implementa para gestionar más eficientemente las direcciones IP disponibles y facilitar la conexión de más usuarios a la red. Tradicionalmente se usa el prefijo 100.64.0.0/10 (100.64.0.0-100.95.255.255), definido por la IETF en la RFC 6598 (**https://tools.ietf.org/html/rfc6598**) Destinado para ayudar a mitigar la escasez de direcciones IPv4 y ayudar en la transición a IPv6.

La simple y llana traducción de origen (Source-NAT) puede acarrear errores de *persistencia* de sesiones que se reflejan como problemas en la estabilidad de tráfico Peer-to-peer (P2P) en gaming (Xbox, Play Station, etc), conferencias multimedia en tiempo real (Zoom, G-Meet, Teams, etc) o streaming (Spotify, Disney+, Netflix, Prime Video, etc.). En temas de seguridad una gran diferencia es *DDoS selectivo* para mover los usuarios de las IP penalizadas antes de aplicarles “blackhole” (DDoS IP protection).

Diferencias principales de CGNAT con el NAT Tradicional (S-NAT):

Característica	NAT tradicional	CGNAT (Carrier Grade NAT)
Lugar de implementación	En el router o gateway del usuario final	En la red del proveedor de servicios (ISP)
Escala	Pequeña escala: hogares, oficinas pequeñas	Gran escala: miles o millones de usuarios
Uso de IP pública	Normalmente una IP pública por red privada	Una sola IP pública compartida por muchos clientes
Asignación de puertos	Sin limitaciones relevantes para cada usuario	Puertos limitados por usuario (PBA, NAT Determinístico)
Privacidad y trazabilidad	No se hace necesaria	Identifica usuarios para trazabilidad y auditoría
Impacto en aplicaciones	Funciona bien con la mayoría de aplicaciones	Pueden causar problemas con juegos online, P2P,

		servidores y servicios que requieren acceso entrante
Seguridad	Proporciona cierto aislamiento de la red interna	Añade una capa de seguridad al impedir conexiones directas, pero puede complicar la gestión de incidentes
Complejidad	Configuración sencilla y local	Configuración compleja y centralizada, requiere equipos especializados
Transición a IPv6	Pueden retrasar la adopción de IPv6	Prolonga la vida útil de IPv4, pero también ayuda con la migración a IPv6 (NAT64/DNS64)

Ventajas de CGNAT

- **Ahorro de costos**: Al reducir la cantidad de direcciones IP públicas necesarias, los operadores disminuyen los gastos asociados a la compra y gestión de direcciones IP.
- **Flexibilidad en la administración de tráfico:** Permite la conversión y gestión de puertos TCP/UDP y el mapeo independiente de puntos finales, lo que ayuda a optimizar el uso de recursos de red.
- **Mejora de la seguridad:** CGNAT puede actuar como una barrera de seguridad, dificultando el acceso no autorizado a dispositivos que están detrás de servicio CGNAT.
- **Eliminación de límites en servicios que requieren conexión directa:** Técnicas como Port Forwarding ayudan a habilitar el uso de aplicaciones que requieran abrir puertos específicos, como servidores de juegos, domótica (o dispositivos IoT), FTP, NAS o VPN, ya que CGNAT se permite el reenvío y re-mapeo de puertos desde la IP pública.
- En conjunto con las funciones de BNG (Broadband Network Gateway = Manejo de suscriptores) **permite hacer QoS a usuarios diferenciados como premium**.
- **Técnicas de mitigación al bloqueo de IP** (baneo) re-asignando los usuarios a otras IP Públicas minimizando el impacto.

Desventajas de CGNAT

- **Aumento de la latencia:** Puede haber un leve aumento en la latencia que afecta a usuarios de juegos en línea o aplicaciones que requieren una respuesta rápida. Requeriría aplicar QoS.
- **Introduce una capa adicional de procesamiento**, lo que puede afectar negativamente la experiencia en juegos online, videollamadas y streaming en tiempo real.
- **Problemas de bloqueo de IP:** Si un usuario que comparte su dirección IP es baneado de un servicio, otros usuarios con la misma IP pueden verse afectados, aunque no hayan cometido ninguna infracción.

Principales atributos de CGNAT

- **Optimización del uso de direcciones IPv4 públicas:** CGNAT (Carrier Grade Network Address Translation) permite que múltiples usuarios compartan una sola dirección IP pública, lo que ayuda a los proveedores de servicios de Internet (ISP) a gestionar la escasez de direcciones IPv4 disponibles.

- **Escalabilidad:** Puede gestionar miles o incluso millones de conexiones simultáneas, lo que lo hace adecuado para grandes redes de operadores y facilita la transición gradual hacia IPv6.
- **Registro avanzado y trazabilidad:** Los sistemas CGNAT mantienen registros (logs) detallados de las conexiones, lo que permite identificar qué usuario utilizó cada puerto en cada momento, facilitando la gestión y el cumplimiento de normativas (Regulaciones contra crimen cibernético).
- **Compatibilidad con tecnologías de transición:** CGNAT puede integrarse con soluciones como NAT64/DNS64 y soportar múltiples plataformas de capa de aplicación (FTP, SIP, DNS, etc.), ayudando en la coexistencia de IPv4 e IPv6

Seguridad contra DDoS en CGNAT (A10)

Los ataques de negación de servicio *(Denial-Of-Service: DoS y Distributed-DoS: DDoS)* pueden ser defendidos y/o mitigados por la solución de CGN, ofreciendo diferentes características según donde se detecte el ataque:

- **Ataques gestionado por el CGN:** Ataques identificados por el CGN y que las acciones son tomadas por este elemento
- **Ataques gestionados por la red (Solución externa):** Ataques identificador por una tercera herramienta e informados mediante BGP (*BGP Flow-Spec*) que activan el vaciado de trafico en el equipo.

Ataques gestionados por el CGN

Cuando una dirección IP pública recibe un volumen de conexiones no solicitadas que excede el umbral de tasa configurado (rate-limit), se activa un mecanismo automático de mitigación. Este proceso genera las siguientes acciones:

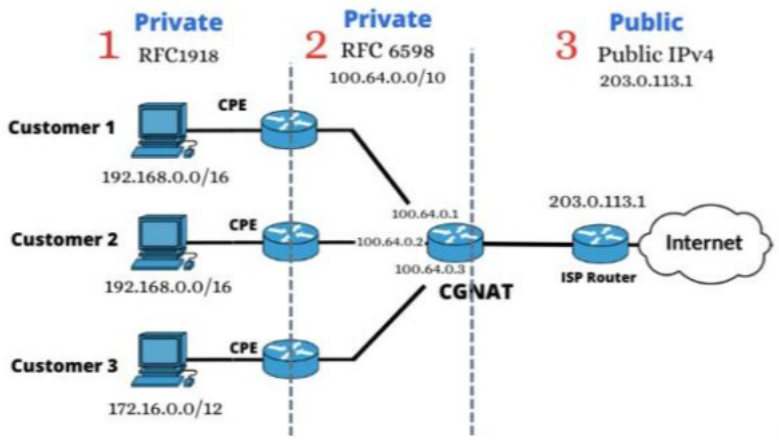
1. **Registro de Evento:** Se genera una entrada de registro (log) exportada a través de Syslog, indicando que la IP ha sido incluida en la lista negra (blacklist) debido a actividad sospechosa.
2. **Limpieza de Sesiones:** Todas las sesiones activas asociadas a la IP atacante son inmediatamente finalizadas. Cuando los usuarios afectados intentan reconectarse, se les asignarán nuevas direcciones IP del pool disponible, garantizando así la continuidad de su servicio.
3. **Cuarentena Temporal:** La IP infractora entra en un período de cuarentena con un tiempo de expiración definido. Durante este tiempo, la IP no se utilizará para nuevas conexiones.
4. **Anuncio BGP para Blackholing Remoto (RTBH):** Inmediatamente después de entrar en cuarentena, la IP es anunciada a través del protocolo BGP con una comunidad específica configurada para Blackholing Remoto (RTBH).
5. **Descarte en el Router de Frontera:** El router de frontera, configurado para actuar como receptor de RTBH, recibe el anuncio BGP y comienza a descartar todo el tráfico destinado a la IP en cuarentena, impidiendo que las conexiones no deseadas lleguen al Carrier-Grade NAT (CGN).
6. **Monitoreo y Reactivación de Cuarentena:** Al expirar el período de cuarentena, el CGN deja de anunciar la ruta BGP para RTBH, permitiendo que el tráfico legítimo pueda alcanzar el CGN. Sin embargo, si el tráfico de ataque persiste, el período de cuarentena se reactiva inmediatamente, repitiendo los pasos 4 y 5.

7. **Periodo de Estabilización (Remove-Wait):** Si el tráfico de ataque cesa durante el período de cuarentena, se inicia un período de "Remove-Wait" para asegurar la estabilidad de la IP.
8. **Rehabilitación de la IP:** Una vez que el período de "Remove-Wait" finaliza, la IP se considera sana y puede volver a utilizarse para alojar nuevas sesiones. El tráfico legítimo puede fluir nuevamente hacia esta IP.

Ataques gestionados por la red

Cuando una dirección IP pública es objeto de un ataque y las técnicas de mitigación selectiva no logran contenerlo, se implementa el Blackholing Remoto (RTBH). Para ello, se ejecutan las siguientes acciones:

1. **Bloqueo en el Router de Frontera**: Inicialmente, el router de frontera de la red bloquea el tráfico destinado a la IP atacada para evitar que el flujo malicioso impacte la infraestructura principal.
2. **Anuncio BGP al Router de Descarte:** El router de descarte anuncia la IP afectada a través del protocolo BGP, utilizando una comunidad BGP predefinida y específica para la señalización de blackholing.
3. **Propagación del Anuncio BGP al CGN:** Un peer BGP, establecido con el CGN a través de una sesión BGP dedicada para este propósito, debe propagar el anuncio de la IP afectada. Se pueden emplear comunidades BGP para automatizar este anuncio.
4. **Activación de Protección DDoS en el CGN:** El CGN recibe el anuncio BGP de la IP afectada a través del peer dedicado. Mediante una funcionalidad específica del sistema operativo ACOS, la IP es identificada e ingresa a una zona de protección contra ataques DDoS.
5. **Identificación del Pool de IP:** El CGN localiza la IP atacada y determina el pool de direcciones IP al que pertenece.
6. **Aislamiento y Limpieza de Sesiones:** El CGN mueve la IP a una lista de bloqueo (banlist) y finaliza todas las sesiones activas asociadas a ella, impidiendo que los usuarios continúen utilizando la dirección IP comprometida.
7. **Registro de Evento:** Se genera una entrada de registro (log) exportada a través de Syslog, indicando que la IP ha sido incluida en la lista negra (blacklist) debido a actividad sospechosa.
8. **Retorno a Estado Activo:** Una vez que el anuncio BGP de la IP afectada deja de propagarse (indicando que el blackholing ha sido retirado), el CGN automáticamente retorna la IP a su estado activo, permitiendo el establecimiento de nuevas conexiones.



Resumen

CGNAT es una solución clave para los ISP ante la escasez de direcciones IPv4, permitiendo compartir direcciones públicas entre muchos usuarios, ahorrar costos, mejorar la seguridad y facilitar la transición a IPv6; Es la mejor alternativa de estabilidad para usuarios de P2P. Además, ofrece escalabilidad y herramientas avanzadas de registro y administración del tráfico, adaptándose a las necesidades de las redes modernas.

Acompañar el NAT de una buena herramienta de visibilidad y correlación puede hacer la gran diferencia entre usuarios satisfechos y campañas de descuento tarifario.

CDN y Experiencia de Usuario

Un CDN *(Content Delivery Network)* es una red de servidores distribuidos geográficamente que trabajan juntos para entregar contenido de manera más rápida y eficiente a los usuarios. El objetivo principal de un CDN es reducir la latencia, mejorar la velocidad de entrega de contenido, y optimizar la experiencia del usuario al acceder a sitios web, videos, aplicaciones, etc.

Ejemplo Netflix:

Netflix utiliza CDNs para transmitir contenido como películas y series de televisión. Su plataforma emplea una arquitectura llamada Open Connect, que es su propia CDN personalizada. Netflix almacena copias de su contenido más popular en servidores locales cercanos a los usuarios, conocidos como "caches". Cuando un usuario reproduce una película, esta se transmite desde el servidor más cercano, reduciendo la carga en la red central y asegurando una transmisión fluida, incluso en horas pico.

Ejemplo Akamai:

Akamai es uno de los proveedores de CDN más conocidos del mundo. Empresas como Spotify, Airbnb, y grandes compañías de comercio electrónico utilizan Akamai para distribuir contenido web y garantizar que este esté accesible sin importar la ubicación del usuario. En el caso de servicios de streaming o páginas web de alto tráfico, Akamai ayuda a optimizar el rendimiento, evitar interrupciones y proteger contra ataques DDoS.

Los CDNs son herramientas fundamentales para garantizar que el contenido digital sea accesible de manera rápida y confiable, especialmente en un mundo donde la demanda de servicios en línea sigue creciendo exponencialmente.

Las CDN más populares se muestran en la siguiente tabla:

Resumen de las CDN más populares (2025)

CDN	Características destacadas
Cloudflare	Seguridad, plan gratuito, cobertura global
Akamai	Red masiva, alto rendimiento, líder histórico
Amazon CloudFront	Integración AWS, escalabilidad, global
Google Cloud CDN	Integración Google, baja latencia, global
Microsoft Azure	Integración Microsoft, rendimiento global
Bunny CDN	Funciona bien con la mayoría de aplicaciones
KeyCDN	Precios asequibles, integración WordPress
Gcore	Fuerte en Europa del Este, planes accesibles
Fastly	Entrega dinámica, alto rendimiento
CDN77	Fiabilidad, precios competitivos
CDNSun	Latencia baja, seguridad
Beluga CDN	Alternativa asequible, buen soporte
MediaNova	Streaming, mercados emergentes
Sucuri	Seguridad avanzada, protección web
CacheFly	Red global, precios flexibles

Elegir un CDN adecuado puede tener un impacto significativo en la velocidad, la seguridad y la experiencia general de tus usuarios.
Algunos factores clave a considerar incluyen:

- **Ubicación de los servidores:** Asegúrate de que la red del CDN tenga servidores en las regiones donde se encuentra la mayoría de tus usuarios. Esto ayudará a minimizar la latencia.
- **Tipo de contenido:** Algunos CDNs están optimizados para ciertos tipos de contenido, como streaming de video, páginas web, aplicaciones móviles o archivos grandes.
- **Escalabilidad:** Considera si el CDN puede manejar el crecimiento de tu negocio y los picos de tráfico sin afectar el rendimiento.
- **Integración:** Comprueba que el CDN sea compatible con tu infraestructura actual (por ejemplo, plataforma de nube, sistema de gestión de contenido, etc.).
- **Seguridad:** Busca funciones como protección contra ataques DDoS, cifrado HTTPS, y controles avanzados de acceso.
- **Análisis y monitoreo:** Un buen CDN debe ofrecer herramientas para rastrear el rendimiento, las métricas de tráfico, y los problemas potenciales.
- **Costo:** Los CDNs varían en precio, desde soluciones económicas hasta servicios premium. Compara los costos en función de tus necesidades y presupuesto.
- **Reputación y soporte técnico:** Investiga la confiabilidad del proveedor y la calidad de su soporte técnico. Esto puede ser crucial para resolver problemas rápidamente.

Cada ISP tiene necesidades únicas, así que el mejor CDN dependerá de los objetivos específicos o tipo de tráfico de mayor consumo. Una abuena herramienta de observabilidad puede ayudar!

Beneficios para el usuario

Impacto de la descongestión de tráfico en la experiencia del usuario para un pequeño ISP:

- **Mejora** de la velocidad y reducción de la latencia.
- **Disminución** de interrupciones y caídas del servicio
- **Mejor** calidad en aplicaciones sensibles al tiempo
- **Mayor** satisfacción y fidelización del cliente
- **Optimización** de la infraestructura existente
- **Reducción** de costos y cumplimiento de SLA por regulación.

En conclusión, la descongestión de tráfico es fundamental para que un pequeño ISP pueda ofrecer una experiencia de usuario rápida, estable y satisfactoria, lo que se traduce en mayor competitividad y sostenibilidad del negocio.

Beneficios de los CDN para ISP pequeños y rurales

- **Mejora de la experiencia del usuario:** Las CDN reducen significativamente los tiempos de descarga y la latencia. Esto es especialmente valioso donde la infraestructura de red suele ser más limitada y las conexiones internacionales pueden ser costosas o lentas
- **Reducción del consumo de ancho de banda internacional:** Al almacenar en caché los contenidos más populares localmente se disminuyen la cantidad de tráfico que debe salir hacia Internet internacional, lo que reduce los costos operativos para el ISP.Un gran porcentaje, dependiendo los patrones de tráfico, puede ser cacheado localmente.
- **Optimización de recursos y escalabilidad:** Al descargar la red principal y los servidores de origen, los CDN permiten que los ISP atiendan a más usuarios finales con el mismo ancho de banda, manteniendo la calidad del servicio. Esto es crucial para maximizar su cobertura y eficiencia.
- **Mejora de la seguridad:** Las CDN modernas ofrecen protección contra ataques DDoS y otras amenazas de seguridad, filtrando el tráfico malicioso antes de que llegue a la red del ISP. Esto ayuda a mantener la estabilidad y disponibilidad del servicio, algo esencial para operadores pequeños que pueden no contar con equipos de seguridad avanzados.
- **Reducción de la congestión y mayor disponibilidad:** Al responder a las solicitudes de contenido desde servidores cercanos, se reduce la congestión en la red principal y se mejora la disponibilidad del contenido, incluso en situaciones de alta demanda o fallos en la red internacional.

Desafíos específicos para pequeños ISP y rurales

A pesar de estos beneficios, los grandes proveedores de contenido suelen priorizar la instalación de CDN en operadores de gran tamaño, ya que el tráfico de los pequeños ISP no siempre justifica la inversión. Por ello, los pequeños ISP y WISP (Wireless ISP) suelen quedar fuera de estos acuerdos y no pueden aprovechar plenamente las ventajas del caché local, lo que los coloca en desventaja frente a los grandes operadores. Sin embargo, existen iniciativas y asociaciones de pequeños ISP que buscan negociar colectivamente con los grandes generadores de contenido para acceder a estas tecnologías y reducir la brecha digital en zonas rurales.

Resumen de beneficios principales

Beneficio	Descripción
Reducción de costos de ancho de banda	Menos tráfico internacional, menor gasto en enlaces y mayor eficiencia de red.
Mejor experiencia de usuario	Menor latencia, cargas más rápidas y menos quejas por interrupciones o lentitud.
Mayor seguridad	Protección contra DDoS y filtrado de amenazas.

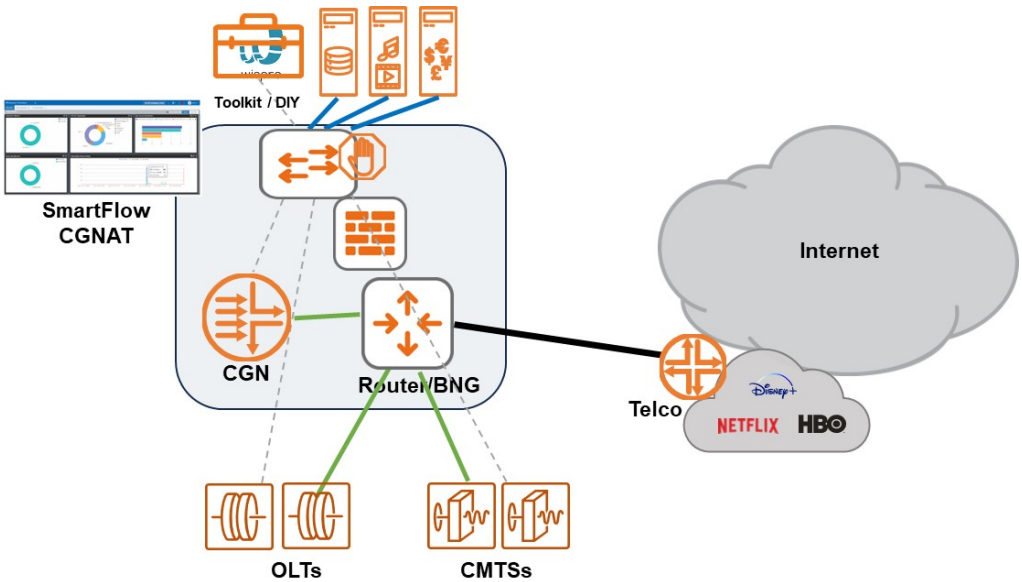
Escalabilidad y eficiencia operativa	Permite atender a más usuarios con los mismos recursos.
Menor congestión y mayor disponibilidad	Contenido accesible incluso en picos de demanda o fallos externos.

Consideraciones finales

Para los ISP pequeños y rurales, el acceso a CDN representa una oportunidad clave para mejorar la experiencia de usuario (UX) al percibir mayor calidad del servicio, reducir costos y competir en mejores condiciones. Sin embargo, la viabilidad depende de acuerdos con proveedores de contenido y, en muchos casos, de la colaboración sectorial para lograr que los grandes generadores de contenido desplieguen cachés en sus redes locales o puntos de interconexión.
Herramientas como ADN SmartFlow ayudan a identificar los patrones de tráfico con exactitud para justificar nodos de los CDN documentando uso específico.

Una aproximación a la Arquitectura de la red

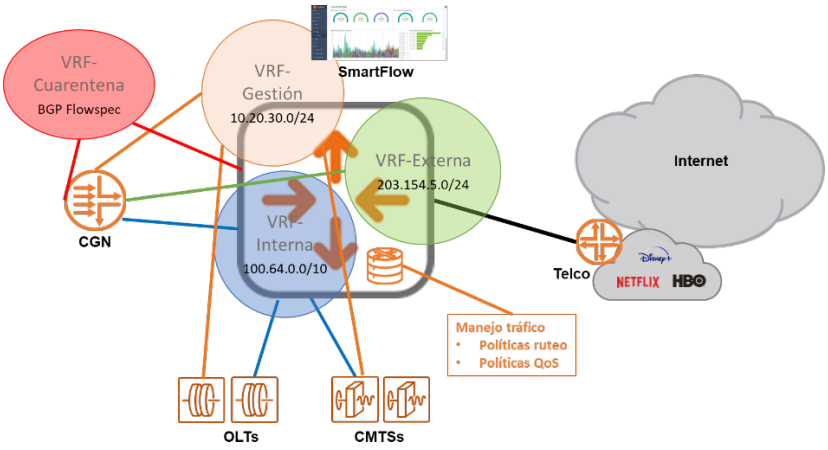
Una arquitectura de red ordenada ayuda a simplificar el despliegue, operación, definición de procesos, documentación y troubleshooting (resolución de problemas). Los elementos funcionales se alinean como las fichas de un juego de bloques de construcción y se convierten en módulos que pueden ajustarse a las necesidades cambiantes del negocio.



Los elementos y funciones de red se definen a continuación:

Router de Borde:

Encargado de funciones de enrutamiento como **BGP Peering, separación y control de tráfico (VRF y Políticas de ruteo)** así como también aplicar las políticas de QoS o diferenciación del tráfico para manejo de la congestión.



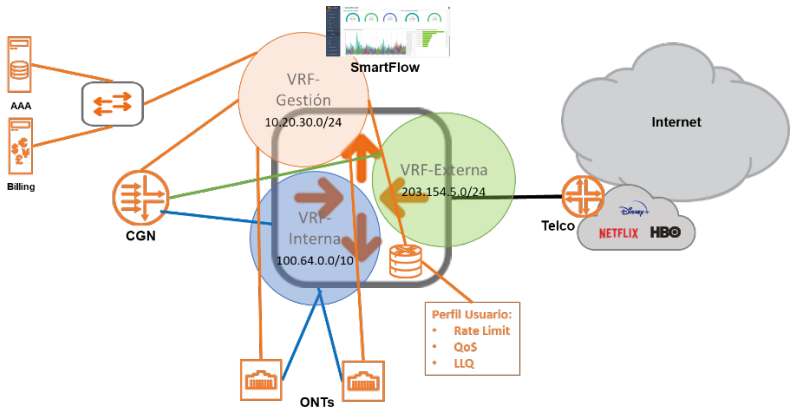
En la figura se observa que el enrutador separa al menos 4 VRF o router virtuales:

- **VRF Externa** o de peering, para conectar a los proveedores de internet (y CDN según el caso)
- **VRF interna** o de direccionamiento privado para comunicación con los elementos de red de servicio a suscriptores (OLTs, CMTSs, etc.) y por supuesto el CGNAT.
- **VRF de Gestión**, para comunicarse con redes OOO y los elementos para monitoreo.
- **VRF de Cuarentena**, opcionalmente para poner los prefijos o IP públicas que han sido bloqueadas (baneadas).

BNG/BRAS:

(Broadband Network Gateway (BNG) / Broadband Remote Access Server (BRAS) es un tipo especial de router de red que agrega el tráfico de sesión del suscriptor desde las redes de acceso realizando las siguientes tareas para los suscriptores además de las funciones de enrutamiento:

- **Manejo de la sesión:** Autenticación, monitoreo y terminación.
- **Aplicar diferentes políticas al tráfico del suscriptor como son:** rate limiting, traffic shaping, QoS y políticas de seguridad.
- **Interface con el software de facturación**.

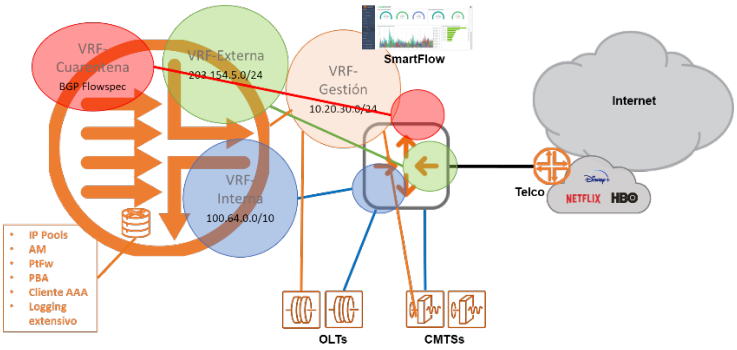


En los últimos años se ha impuesto el modelo de **"Desagregado" DBNG, vBNG ó BNG-CUPS (Control Plane – User Plane Separation)** que permite virtualizar y distribuir funciones más cerca de los usuarios. El Plano de Control Desagregado maneja funciones incluyendo:

- **Terminación de sesiones del suscriptor**.
- **Terminación de sesiones de CPE:** PPPoE o IPoE (DHCPv4/DHCPv6/SLAAC)
- **Autenticación.**
- **Cliente AAA para completar Autenticación contra Servidor** AAA (RADIUS, TACACS, etc) por mensajes PPPoE o DHCP.
- **IPAM**
- **Envío de reglas al Plano de Usuario**
- **Accounting**
- **Envío de información de uso** a servidores asociados y herramientas de Observabilidad.
- **PEP** (Policy Enforcement Point)

CGN

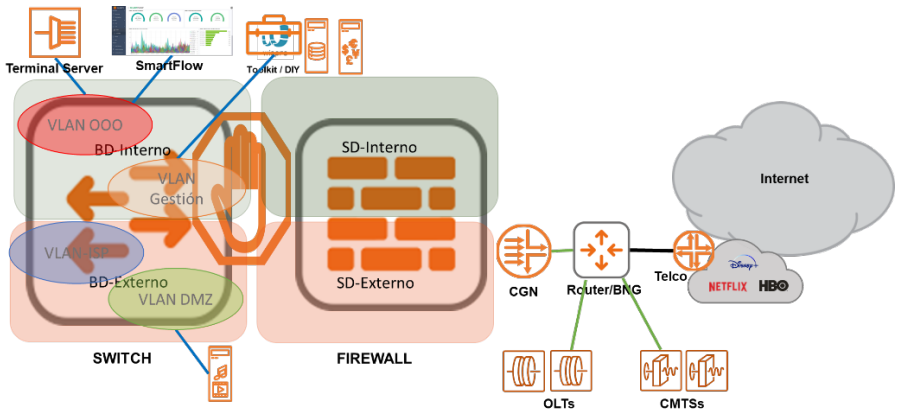
Manejo de direccionamiento y funcionalidades CGNAT (vs. LSN)



Participa de las mismas VRF del Router de borde, por su funcionalidad, además de administrar los pool de IPs, manejo de direcciones, funciones de ***Port Forwarding y Port Block Allocation (PBA)*** para el manejo de persistencia en P2P y trazabilidad de los usuarios, por cumplimiento de normas de las autoridades contra los crímenes informáticos. Provee además un logging extensivo para alimentar las herramientas de Monitoreo, Observabilidad y Analítica.

LAN Administración Nodo

La Red LAN interna debe presentar características de seguridad y privacidad en el acceso a los recursos internos y gestión de los elementos de red y servicios.



Los componentes y sus características son:

Switch:

Manejo y separación de redes internas por **VLANs** y entregar troncales a Firewall y enrutadores.

- **Bridge Domain (BD)** al menos 2 para evitar MAC Spoofing
- **VLAN conectividad servidores**
- **VLAN conectividad equipos de red**
- **VLAN gestión fuera de banda (OOO)**
- Si se está usando Virtualización o Contenedores en servidores y aplicaciones debería poder soportar VTEP.

Firewall:

Encargado de implementar separación de Security Domains, implementar Políticas de seguridad **inter-VLAN** y garantizar explícitamente **ZTNA (Zero Trust Network Access).**

Terminal Server: (Opcional) para conectar los puertos seriales de consola de los equipos (RS232 o USB).

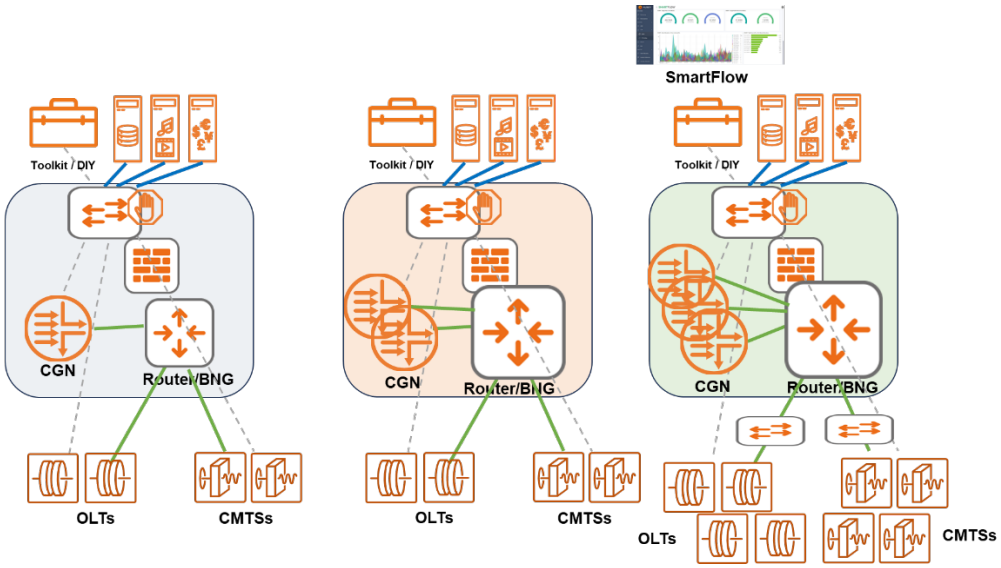
Herramientas observabilidad y analítica

Las herramientas para visualizar lo que sucede en las redes toman la información directamente de los dispositivos (Routers, Switches, Firewalls, Servidores, etc.) con protocolos y formatos propios de cada plataforma (Syslog, NetFlow, gRPC, SNMP, etc). Una vez recolectados se enriquecen para dar sentido (Correlacionar), visualizar gráficamente y poder hacer reportes.

Más allá del monitoreo de Tráfico las herramientas como **SmartFlow** permiten Identificar los patrones y flujos de información permitiendo acortar el tiempo de encontrar causa raíz en un problema presentando los hechos de manera que se hacen accionables.

Escalabilidad de la Arquitectura

Los módulos de la arquitectura o elementos de red pueden crecer por scale-out, es decir agregar elementos funcionales a manera de Cluster dando flexibilidad para crecer en escenarios de aumento de suscriptores y de ancho de banda hacia internet y hacia los usuarios (planes diferenciados).



Consideraciones adicionales

Definir y documentar procesos es de vital importancia para mantener una operación eficiente y que de espacio a una gran experiencia de usuario. Cosas a tener en cuenta:

- **Crecer de forma ordenada**: Una operación ordenada reduce el MTTR y sube la disponibilidad.
- **Monitoreo de recursos y cumplimiento de seguridad**.
- **Normalización:** Estandarización de configuraciones y construcción de políticas (Rutas, QoS, filtros y ACL)
- **Filtros/Seguridad** para el plano de control (Hardening)
- **IPAM:** Asignación de IPs uniforme (ejemplo DHCP - CMTS)
- **Control y gestión de inventario**
- **Documentar el Control de cambios**
- **Automatización** de tareas repetitivas y susceptibles al error humano.

Conclusiones

Gracias por llegar hasta acá, para cerrar un resumen de las ideas mencionadas durante la lectura.

- **Existen retos únicos para ISPs regionales** ¡Pero se pueden afrontar!, los más relevantes se pueden categorizar en: Costos, tamaño de la base de usuarios, alcance geográfico y acceso a la tecnología.
- **Se deben desbancar los mitos** que limitan la capacidad de mejorar la experiencia del usuario.
- **CGNAT es una alternativa alcanzable** para mejorar el manejo del ISP y la experiencia del usuario (estabilidad, seguridad, ahorro y transición a IPv6)
- **Las CDN y Cachés** son una excelente alternativa para mejorar UX y ahorrar con una mejor utilización de los enlaces.
- **Una Arquitectura de red ordenada** hace la diferencia en la operación del ISP y una gran experiencia de Usuario.
- **La implementación de metodologías y políticas de gestión** de la red y uso adecuado de herramientas de Observabilidad hacen amable la vida del operador.
- **SmartFlow** – Es una gran herramienta de Observabilidad y analítica para apoyar la operación.

AUBEN networking **for people**