UNIVERSIDAD NACIONAL DE INGENIERÍA

Facultad de Ingeniería Eléctrica y Electrónica

TRABAJO DE SUFICIENCIA PROFESIONAL

Ingeniería de una red de banda ancha para brindar acceso a internet e intranet a instituciones educativas rurales de la región Puno

Para obtener el Título Profesional de Ingeniero de Telecomunicaciones

Elaborado por

César Eduardo Colorado Monja

0009-0008-8062-2008

Asesor

M. Sc. Ing. Alfredo Efraín Rodríguez Gutiérrez

0000-0001-6246-049X

LIMA – PERÚ

2025

Citar/How to cite	Colorado Monja [1]
Referencia/Reference Estilo/Style: IEEE (2020)	[1] C. Colorado Monja, "*Ingeniería de una red de banda ancha para brindar acceso a internet e intranet a instituciones educativas rurales de la región Puno*" [Trabajo de suficiencia profesional]. Lima (Perú): Universidad Nacional de Ingeniería, 2025.

Citar/How to cite	(Colorado, 2025)
Referencia/Reference Estilo/Style: APA (7ma ed.)	Colorado, C. (2025). *Ingeniería de una red de banda ancha para brindar acceso a internet e intranet a instituciones educativas rurales de la región Puno*. [Trabajo de suficiencia profesional, Universidad Nacional de Ingeniería]. Repositorio institucional Cybertesis UNI.

Dedicatoria:

A mis padres por el apoyo y cariño continuo,

aconsejarme e impulsarme a cumplir con mis objetivos.

Resumen

El presente trabajo de suficiencia profesional se enmarca en los proyectos regionales impulsados por el gobierno, con el propósito de mejorar la infraestructura de telecomunicaciones en la red de acceso y beneficiar a sectores clave como la educación. Se centra en la ingeniería de una red de banda ancha para brindar acceso a internet e intranet a 581 instituciones educativas en la región Puno y, de esta manera, mejorar el acceso a estos servicios. Se realiza la implementación de una red de banda ancha con *Broadband Remote Access Server* (B-RAS) o también conocido como *Broadband Network Gateway* (BNG) para la administración de suscriptores y planes, que considera el número de suscriptores (instituciones educativas), los planes de velocidad carga y descarga de internet e intranet. Se muestra el proceso de autenticación de los suscriptores, así como la asignación del plan correspondiente, y se realizan las pruebas de velocidad de acceso a internet e intranet desde una institución educativa. Finalmente, se concluye que la implementación propuesta mejora significativamente el acceso a servicios de internet e intranet en las instituciones educativas de la región Puno, cumpliendo con los objetivos establecidos por los proyectos regionales. La red de banda ancha implementada es capaz de gestionar eficientemente el tráfico de datos y de asignar los recursos de manera adecuada. Además, el uso del B-RAS/BNG permite una gestión flexible y escalable de suscriptores, lo que facilita futuras expansiones de la red sin comprometer el rendimiento. Palabras clave – Broadband Network Gateway (BNG), acceso a internet, proyectos regionales.

Abstract

This professional proficiency project is framed within the regional projects promoted by the government, with the purpose of improving the telecommunications infrastructure in the access network and benefiting key sectors such as education. It focuses on the design of a broadband network to provide internet and intranet access to 581 educational institutions in the Puno region, thereby improving access to these services. The design of a broadband network is carried out using a Broadband Remote Access Server (B-RAS) or also known as a Broadband Network Gateway (BNG) for subscriber and plan management, taking into account the number of subscribers (educational institutions) and the upload and download speed plans for internet and intranet. The process of subscriber authentication is shown, as well as the assignment of the corresponding plan, and speed tests for internet and intranet access from an educational institution are conducted. Finally, it is concluded that the implementation of the proposed design significantly improves access to internet and intranet services in educational institutions in the Puno region, meeting the objectives established by the regional projects. The designed broadband network is capable of efficiently managing data traffic and allocating resources appropriately. Furthermore, the use of B-RAS/BNG allows for flexible and scalable subscriber management, facilitating future broadband network expansions without compromising performance.

Keywords –Broadband Network Gateway (BNG), internet access, regional projects.

Tabla de Contenido

Pág.

Lista de tablas

Lista de figuras

Introducción

El presente trabajo se centra en la implementación de una red de banda ancha para brindar acceso a internet e intranet a quinientos ochenta y una (581) instituciones educativas. Se muestra el proceso de la definición de dicha cantidad de suscriptores, se definen tres (03) planes de carga y descarga de internet e intranet, el proceso de autenticación, el flujo de funcionamiento y el resultado de las pruebas de velocidad de uno de los planes (plan de 8 Mbps). Asimismo, se muestra el proceso de autenticación y asignación del plan para los suscriptores, el flujo de datos para la conectividad a internet e intranet. En ese sentido, se divide en cuatro capítulos.

El capítulo I, Parte introductoria del trabajo, muestra la importancia del acceso a internet, la problemática de las instituciones educativas de la región Puno y la necesidad de desplegar una red de banda ancha para el acceso a internet e intranet dentro de la red de acceso de dicha región.

El capítulo II, Marco teórico y conceptual, aborda las definiciones de términos y funcionamiento de protocolos y arquitecturas de redes de telecomunicaciones.

El capítulo III, Desarrollo del trabajo de investigación, muestra los pasos para consideración de la cantidad de los suscriptores, la definición de los planes, el proceso de autenticación, el flujo de datos, funcionamiento general de la solución y el resultado de la prueba de velocidad.

En el capítulo IV, Análisis y discusión de resultados, se analizan y justifican los resultados obtenidos, se comparan y se comentan en tablas y gráficos.

Capítulo I. Parte introductoria del trabajo

1.1 Generalidades

En la actualidad, el acceso a internet es indispensable, porque permite a las personas estar conectadas con el mundo, acceder a una amplia variedad de información, realizar transacciones bancarias, compras en línea, promover el desarrollo, entre otros. Por estas razones, es importante su promoción en nuestro país, especialmente en las áreas rurales.

Como describe el MTC (Ministerio de Transportes y Comunicaciones, 2013) en la Exposición de Motivos del Decreto Supremo N°014-2013-MTC:

> La banda ancha es un elemento importante en el desarrollo social y económico, además que amplía los derechos fundamentales como acceso a salud y educación, libertad de expresión, comercio, entre otros (…). Por otro lado, el IDB (Banco Interamericano de Desarrollo) señaló, como resultado de un estudio, que esto trae un incremento en el PBI (Producto Bruto Interno), productividad y puestos de trabajo. Además, la CEPAL (Comisión Económica para América Latina) advirtió la brecha digital como un tema urgente para la competitividad y la inclusión social de un país. (MTC, 2013, p.1)

En ese contexto, se aprobó la Ley N° 29904, publicada en julio de 2012, mediante la cual se estableció la promoción del desarrollo de una red de banda ancha en el territorio peruano. La Secretaría Técnica del FITEL (Fondo de Inversión en Telecomunicaciones), hoy Pronatel (Programa Nacional de Telecomunicaciones) como persona jurídica, promovió la ejecución del Proyecto de la Red Dorsal Nacional de Fibra Óptica y 21 proyectos regionales de ‘Instalación de Banda Ancha para la conectividad y desarrollo social’.

El presente informe desarrolla parte del proyecto ‘Instalación de banda ancha para la conectividad y desarrollo social’ en la Región Puno. Se enfoca en la

implementación de una red de acceso de banda ancha con Broadband Network Gateway (BNG) para brindar el acceso a internet e intranet a instituciones educativas. Se espera que también sea una referencia para futuros trabajos acerca del tema.

La solución con BNG es ampliamente empleada por los proveedores de servicios de internet en la actualidad y es proporcionada por los proveedores líderes en equipos de redes, como Nokia, Cisco, Juniper, Huawei, entre otros. Estas empresas se basan en los estándares de la industria de telecomunicaciones, así como en investigaciones y desarrollos propios.

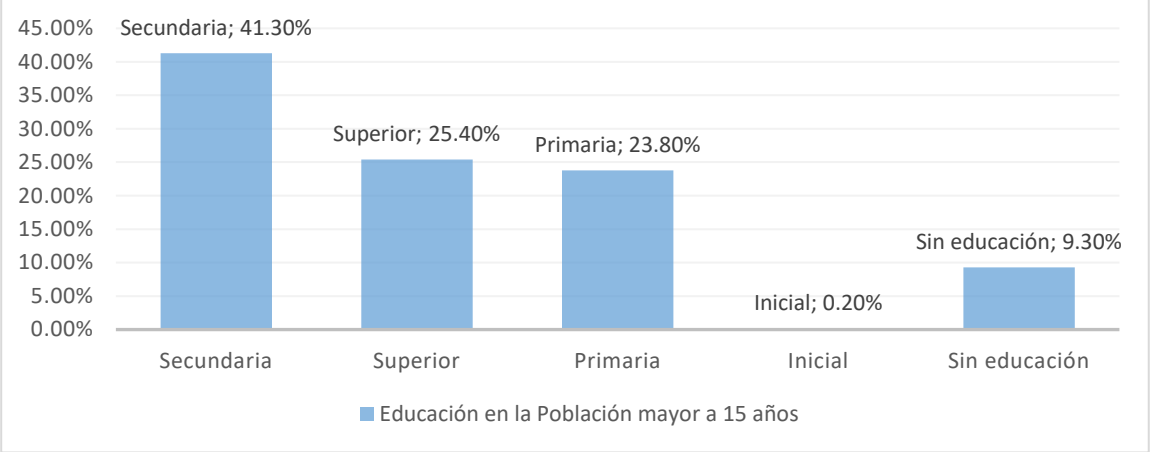
1.2 Descripción del problema de investigación

1.2.1 Situación problemática

En la región Puno, se identificó un problema significativo. Los indicadores estadísticos de esta región revelan una situación socioeconómica y educativa preocupante, que podría estar estrechamente relacionada con la falta de acceso a internet en las escuelas. En la figura 1, se muestran los datos estadísticos de la formación académica de la población mayor a 15 años. Se observa que 9.3% no cuenta con ninguna formación, 0.2% solo cuenta con educación inicial, 23.8% cuenta con educación primaria, 41.3% cuenta con nivel secundaria y solo 25.40% logra una formación superior siendo de este último en su mayoría de la zona urbana (INEI, 2017).

Figura 1

Porcentaje de nivel de educación en la región Puno

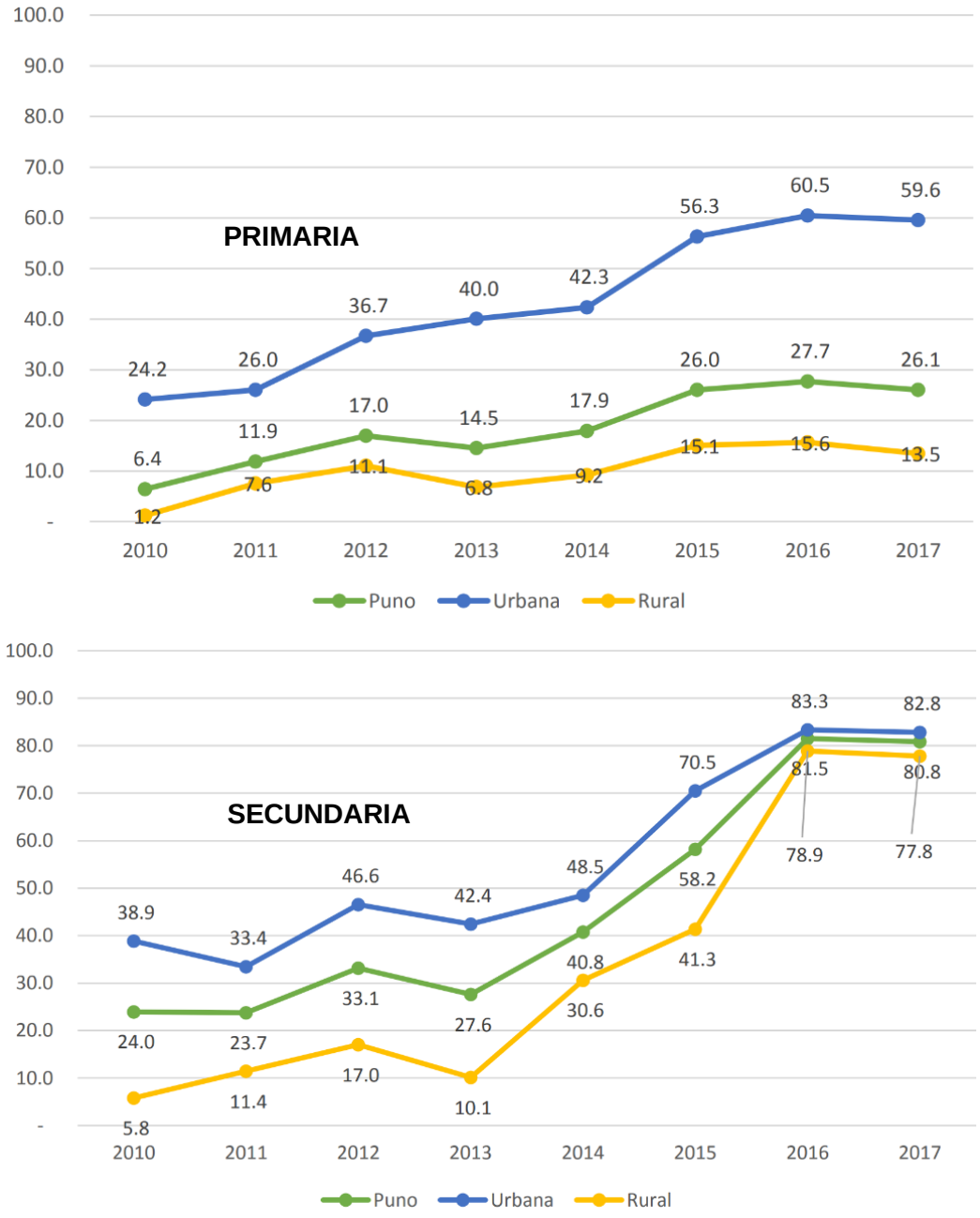


Nota: diagrama de barras en porcentaje de la población nivel de educación: secundaria, superior, primaria, inicial y sin ninguna de las anteriores. Adaptado de Censos INEI (2017)

Esto puede indicar dificultades para acceder a programas educativos y recursos en línea en las escuelas rurales. Como prueba de esto, en la figura 2 se presentan las estadísticas de acceso a internet en instituciones educativas ubicadas en áreas rurales (línea amarilla). En el año 2010, el acceso a internet en escuelas primarias rurales alcanzó el 1.2%, mientras que en escuelas secundarias fue ligeramente superior, llegó al 5.8%. Para el año 2017, estos valores aumentaron a un 13.5% de acceso en primaria y 77.8% en secundaria en zonas rurales. Al comparar estos datos con el acceso en las zonas urbanas (línea azul), se evidencia una seria brecha a nivel primaria. Como se observa en 2010, el acceso a internet en escuelas primarias urbanas fue del 24.2%, mientras que en secundarias alcanzó el 38.9% para el mismo año. En el 2017, los porcentajes de la zona urbana aumentaron considerablemente a 59.6% en primaria y hasta 82.8% en secundaria. Es importante destacar que hay mejoras en las instituciones secundarias rurales, pero el acceso en escuelas primarias, donde se establecen las bases para las habilidades digitales, aún se encuentra rezagado (13.5% de acceso) en comparación con las áreas urbanas (59.6% de acceso).

Figura 2

Histograma de instituciones educativas con acceso a internet en Puno entre 2010 – 2017



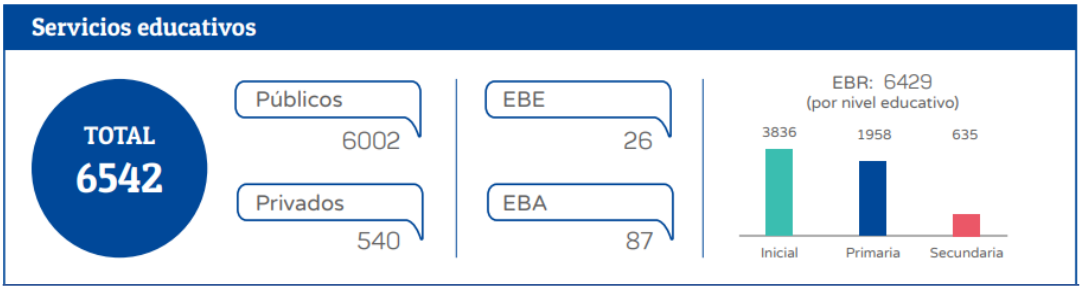
Nota: histograma de acceso a internet en primaria (imagen superior) y secundaria (imagen inferior). La línea amarilla representa el porcentaje considerando solo la zona rural, la línea azul considera la zona urbana y de color verde un promedio general para la región Puno. Minedu (2017)

Como se mostró, hubo un incremento del porcentaje de acceso a internet en las instituciones educativas secundarias rurales; sin embargo, también se debe considerar que la mayor cantidad de instituciones educativas son de grado inicial (3844) y primaria (1964) como se muestra en la figura 3. Es decir que el 77.8% de acceso a internet en secundaria

rural equivale a 140 instituciones educativas de nivel secundaria sin internet y el 13.5% de acceso, en primaria, representa 1703 instituciones educativas de nivel primaria sin internet.

Figura 3

Servicios educativos en Puno

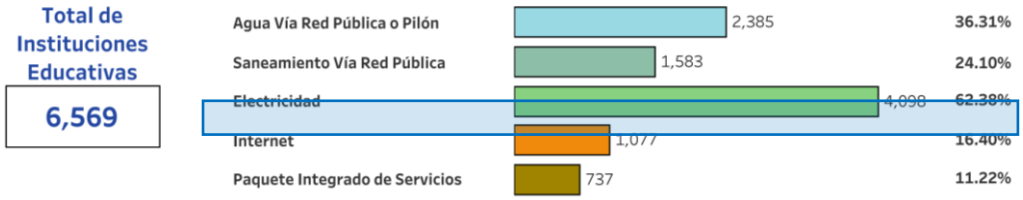


Nota: servicios educativos del 2022 en la región Puno. A la derecha se tiene la cantidad de instituciones educativas de Educación Básica Regular por tipo de nivel educativo. Minedu (2022)

Por esta razón, como se muestra en la figura 4, el resultado general del Censo Escolar 2020 realizado por el Minedu con relación al acceso a internet (considerando el total de instituciones educativas) fue solo del 16.4%. Esto muestra el déficit de acceso a internet en instituciones educativas en esta región (Midis, 2023, p.3).

Figura 4

Acceso a servicios en instituciones educativas en Puno



Nota: la cantidad de instituciones educativas con internet se muestra en el recuadro azul, los resultados que muestra el MIDIS son basados en el Censo Escolar en Puno del año 2020. Midis (2023).

1.2.2 Problema a resolver

Falta de una red de telecomunicaciones de banda ancha que brinde el acceso a internet e intranet en las instituciones educativas rurales de la región Puno.

El proyecto ‘Instalación de banda ancha para la conectividad y desarrollo social’ en la región Puno, que se desarrolla bajo las bases del proyecto de Pronatel, tiene entre sus

alcances brindar el acceso a internet e intranet a 581 instituciones educativas. El presente informe tiene como objetivo resolver este problema.

Para enfocar el documento, en este objetivo se considera la existencia de la infraestructura y conexiones necesarias de una ‘Red de transporte’ y una ‘Red de acceso’, cuyas especificaciones técnicas se describen en el anexo 8-A y 8-B del contrato de financiamiento (MTC, 2024), respectivamente. A continuación, una breve descripción de la infraestructura de la red regional de Puno:

Análisis de la situación preliminar de red regional de Puno. La red regional de Puno está conformada por dos redes independientes (diferentes sistemas autónomos), una red IP/MPLS con enlaces de fibra óptica entre los equipos enrutadores, la Red de transporte, una red IP/MPLS compuesta por sectores aislados denominados ‘clústeres’ y un *Core*, la Red de acceso. Ambas redes se integran entre sí a través de Inter-AS Opción C estableciendo de sesiones BGP LU para IPv4 (RFC 3107) en una arquitectura conocida como MPLS sin interrupciones (*Seamless* MPLS).

Análisis de la arquitectura física y lógica de la red de acceso. La Red de acceso, una pieza fundamental en la infraestructura de conectividad regional, está compuesta por clústeres y el *Core* de la Red de acceso. Los clústeres a su vez están compuestos por nodos terminales, intermedios, distritales, y desempeñan una función importante en la distribución local de la señal, mientras que el *Core* de la Red de acceso coordina la gestión de toda la red.

En este contexto, el ‘Nodo terminal’ emerge con la función de ‘Punto de presencia’ (PoP), actúa como el punto de acceso primario para los usuarios finales. Este nodo desempeña un papel fundamental en la distribución local de la señal y en la entrega de servicios a los usuarios en áreas específicas. A partir del Nodo terminal, la señal se transmite a través de una serie de nodos intermedios, cada uno actuando como un punto de retransmisión para ampliar la cobertura de la red. Estos nodos intermedios facilitan la conectividad entre los nodos terminales y los nodos distritales, que aseguran una cobertura amplia y eficiente en toda la región. Los nodos distritales representan puntos de

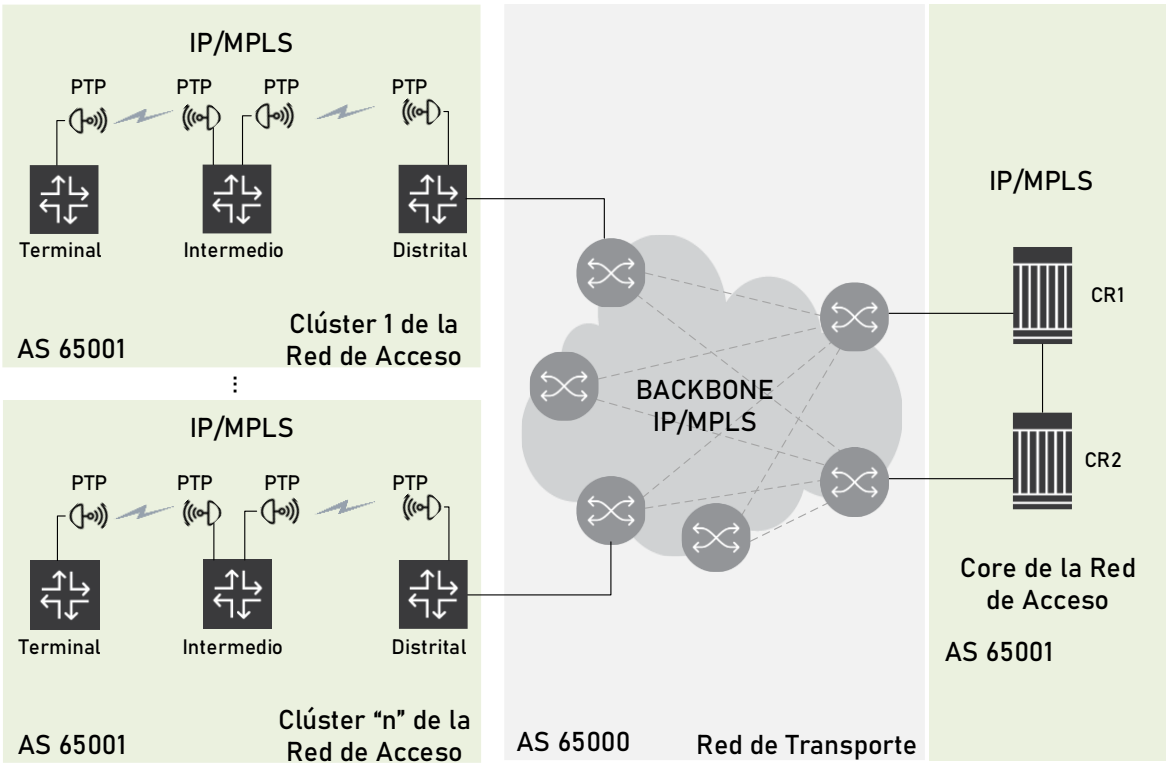
interconexión entre la Red de acceso y la Red de transporte. Estos nodos son vitales para la integración de la red local con una infraestructura más amplia, permiten el acceso a servicios externos y la comunicación a través de la Red de transporte.

Como pieza más importante dentro de la Red de acceso, se encuentran los equipos enrutadores del *Core* de la Red de acceso, el enrutador de Core Acceso 1 (CR1) y el Enrutador de Core de Acceso 2 (CR2). Estos equipos desempeñan un papel crucial en el enrutamiento del tráfico de datos y de gestión dentro de la red.

La interconexión de los equipos en los nodos terminales, intermedios y distritales se realiza mediante radioenlaces punto a punto (PTP), que garantizan una comunicación confiable y de alta velocidad. Por otro lado, la conexión entre los enrutadores del *Core* de la Red de acceso (CR1 y CR2) se lleva a cabo mediante enlaces de fibra óptica, que aseguran una conexión estable y de alta capacidad entre los nodos centrales de la red. Además, la conexión del enrutador distrital con los CR1 y CR2 con la Red de transporte, como se aprecia en la figura 5, se realiza a través de enlaces de fibra óptica, que permiten una conexión robusta y de alto rendimiento con la infraestructura de la Red de transporte.

Figura 5

Diagrama físico de la red de acceso y transporte

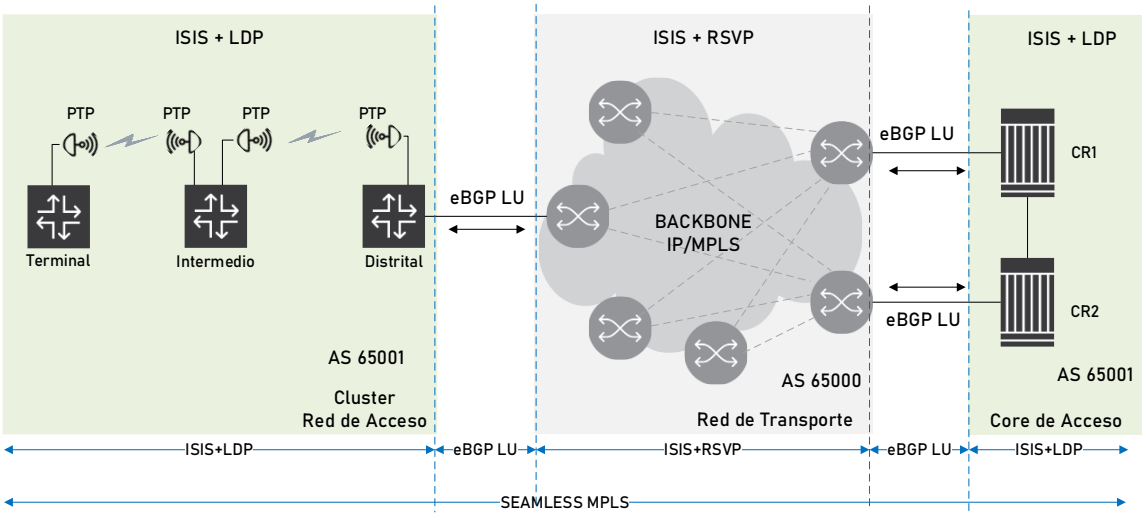


Nota: para simplificar se muestra el enrutador distrital con una conexión a un solo enrutador intermedio; sin embargo, se puede tener más ramificaciones o incluso radio enlaces directos entre distrital y terminal.

Por otro lado, como se puede apreciar en la figura 6, cada uno de los clústeres de la Red de acceso son redes IP/MPLS (IS-IS con LDP). El enrutador distrital utiliza BGP LU para anunciar su IP de servicio (*loopback*) junto a una etiqueta MPLS hacia la Red de transporte. Estos datos NLRI (*Network Layer Reachability Information*) se propagan internamente en la Red de transporte a través de BGP y se anuncian, finalmente, a los enrutadores del Core de la Red de Acceso (CR1 y CR2) ubicados a la derecha de la imagen. Este proceso también se realiza en sentido inverso, donde el CR1 y CR2 anuncian su IP de servicio (*loopback*) y etiqueta MPLS por BGP hacia la Red de transporte, que luego las propagará y la anunciará a los enrutadores distritales. Con esto cada enrutador distrital de la Red de acceso puede establecer un túnel MPLS sin interrupciones (*Seamless* MPLS) con cada enrutador del Core de la Red de acceso y viceversa.

Figura 6

Diagrama lógico de la red de acceso y transporte



Nota: los túneles MPLS posteriormente se usarán construir servicios L2 VPN desde el enrutador distrital hasta los enrutadores del *Core* de la red de acceso (CR1 y CR2).

Análisis de los componentes fundamentales en el *Core* de la Red de acceso. Como se mencionó previamente, en el Core de la Red de acceso, se encuentran dos equipos enrutadores, CR1 y CR2, que desempeñan un papel fundamental en el enrutamiento del tráfico de datos y de gestión dentro de la red. Estos enrutadores están interconectados con una serie y dispositivos esenciales para la operación y el mantenimiento de la infraestructura de red como lo son el servidor AAA, el servidor DHCP**,** cortafuegos (*firewalls*), un enrutador parte de la solución SDN (llamado *Underlay Border Router*), servidor de intranet y la conexión al ISP que enrutará el tráfico hacia internet.

A continuación, se da una breve descripción de los dispositivos mencionados:

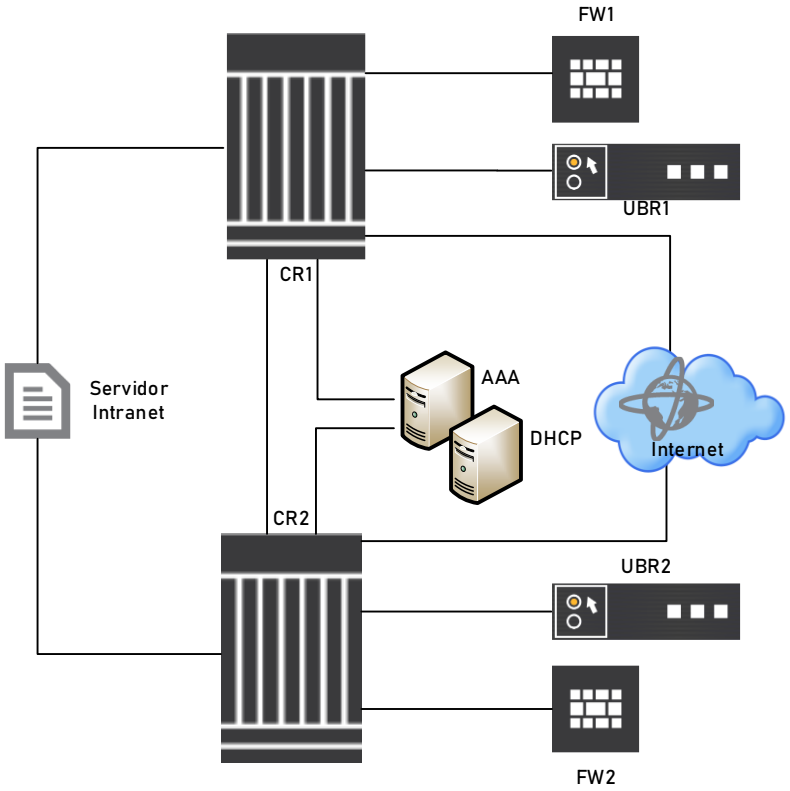
- **Cortafuegos o *firewall*.** El Core de la Red de acceso cuenta con dos (02) firewalls funcionando en alta disponibilidad (HA o *High Availability*). Estos equipos redundantes tienen la capacidad de filtrar páginas web no permitidas en la Red de acceso. A nivel lógico se puede dividir en instancias virtuales con las que se puede mejorar el análisis y generar estadísticas de los flujos de datos en internet e intranet por separado.

- ***Underlay Border Router* (UBR).** Es un equipo parte de la tecnología SDN implementada en la Red de acceso. Existen dos (02) equipos cada uno conectado a cada CR. En este equipo terminan los túneles VXLAN creados desde los equipos CPE.
- **Servidor AAA.** En este proyecto es un servidor virtualizado (*FreeRadius*). Se encarga de autenticar a los CPE. Para ello tiene declarada la lista de CPE permitidos y demás permisos para acceder a los recursos de la Red de acceso, como el plan de navegación de internet e intranet.
- **Servidor DHCP.** En este proyecto, se consideró el uso de una funcionalidad de los enrutadores de *Core* de acceso (CR1 y CR2) para brindar una IP de manera automática a los CPE. Se configura un pool de segmentos privados para la asignación de IP a cada CPE. Está representado como un servidor externo.
- **Servidor de intranet.** Es un servidor que podrá ser accedido por los usuarios finales para uso de almacenamiento. Solo se podrá tener acceso a este servidor a través de los *firewalls*.
- **Internet.** El *Core* de la Red de acceso tiene una conexión con un proveedor de servicio de internet de la región. Este está conectado a los enrutadores del Core de acceso.
- **Enrutadores de *Core* de acceso.** Los enrutadores del Core de acceso se encargan de concentrar el tráfico de datos y de gestión dentro de la red. Son redundantes, funcionando activo (CR1) y espera (CR2).

Con el fin de brindar una representación visual clara de la interconexión física de los dispositivos ubicados en el Core de la Red de acceso. A continuación, se presenta un esquema detallado de la infraestructura.

Figura 7

Diagrama físico en el Core de la red de acceso



Nota: los dispositivos de la imagen son los involucrados con la estructura de *Broadband Network Gateway* (BNG) que se desarrollará más adelante en el capítulo 3.

En resumen, este informe se enfoca en resolver el problema de brindar el acceso a internet e intranet a 581 instituciones educativas consideradas en el proyecto 'Instalación de banda ancha para la conectividad y desarrollo social' en la región Puno considerando el despliegue mencionado de la infraestructura física de la red.

1.3 Objetivos de estudio

1.3.1 Objetivo general

Implementar una red de banda ancha con funcionalidad *Broadband Network Gateway* (BNG) para brindar acceso a internet e intranet a 581 instituciones educativas rurales consideradas en el proyecto 'Instalación de banda ancha para la conectividad y desarrollo social' en la región Puno.

1.3.2 Objetivos específicos

- Determinar los requerimientos para la implementación de la solución de una red de banda ancha con *Broadband Network Gateway* (BNG) en la red de acceso de la región Puno.
- Implementar la red de banda ancha con BNG en la red de acceso de la región Puno.
- Realizar las pruebas de funcionamiento de la red de banda ancha con BNG en la red de acceso de la región.

1.3.3 Indicadores de logro de los objetivos

Para medir el éxito en estos objetivos, se establecerán indicadores de logro específicos que permitan evaluar el cumplimiento de las metas establecidas. Estos indicadores proporcionarán una visión clara del progreso de la implementación y la eficacia de la solución BNG, garantizando así su alineación con los objetivos estratégicos del proyecto.

Tabla 1

Indicadores de logro

Objetivo específico	Indicador de logro	Métrica
Determinar los requerimientos para la implementación de la solución de una red de banda ancha con BNG en la red de acceso de la región Puno.	Cantidad de suscriptores	Numérico
	Ancho de banda de descarga	Mbps
	Ancho de banda de carga	Mbps
Implementar la Red de Banda Ancha con BNG en la red de acceso de la región Puno	Máxima cantidad de suscriptores	Numérico
	Ancho de banda de descarga	Mbps
	Ancho de banda de carga	Mbps
Realizar las pruebas de funcionamiento de la red de banda ancha con BNG en la red de acceso de la región.	Cantidad de suscriptores	Numérico
	Ancho de banda de descarga	Mbps
	Ancho de banda de carga	Mbps

1.4 Antecedentes investigativos

Se han realizado trabajos de investigación relacionados con la implementación de una red de banda ancha para proveer el servicio internet como los descritos a continuación.

A. Diseño de una red de telecomunicaciones para brindar el servicio de acceso a internet como factor de desarrollo social y económica de la región Pasco (Campos, 2020). Este informe aborda los desafíos en la región Pasco, centrándose en la infraestructura necesaria para conectar a los usuarios finales con el Centro de Operaciones de la Red (NOC), donde se encuentra el Core de la Red de acceso. Se propone la construcción de una red de transporte basada en fibra óptica, complementada con una red inalámbrica en la zona de acceso, con el objetivo de extender la conectividad en la región Pasco brindando internet a la población e instituciones públicas de la región.

B. Instalación de internet de banda ancha para la conectividad integral y desarrollo social de la región Cajamarca (Auris, 2020)**.** Este informe se enfoca en la implementación de infraestructura de red para interconectar las instituciones públicas de diversas localidades en la región de Cajamarca con el fin de proporcionar acceso a intranet e internet de banda ancha en instituciones clave como centros educativos, centros de salud y entidades de seguridad pública.

C. Diseño de un sistema para la prestación de *Triple Play* basado en Protocolo Internet para el concesionario de audio y video por suscripción Cayambe Visión (Monteros, 2009). Este informe, realizado en Ecuador, desarrolla la provisión sobre un mismo medio de los servicios IPTV, Telefonía e Internet basados en IP con el objetivo de prestar servicios Triple Play orientándose al dimensionamiento a nivel de capacidades de los recursos de red y la regulación vigente en su país.

Los informes mencionados ofrecen una perspectiva centrada en la implementación de la infraestructura física necesaria para establecer una conexión de extremo a extremo desde el usuario final hasta el núcleo de la red de acceso; sin embargo, se observa una falta de enfoque en los protocolos de redes utilizados. Este informe se enfoca en el aspecto lógico, ya que es común que los proveedores de servicio de Internet (ISP) utilicen soluciones similares con BNG para proporcionar servicios de internet fija a sus abonados.

A continuación, se muestra la visión que algunos proveedores de enrutadores tienen sobre sus productos y servicios ofrecidos, lo que muestra la capacidad de la solución BNG.

Soluciones de *Broadband Network Gateway* (BNG) ofrecidas por los siguientes:

Nokia. BNG es una función de red clave que se sitúa entre la red de acceso de banda ancha y la columna vertebral IP, y se conecta a servicios como Internet y redes de distribución de contenido. Autentica y autoriza el acceso de los suscriptores a los servicios de red y contenido, aplica políticas de gestión de ancho de banda y registra datos de uso para fines de contabilidad (Nokia, 2023, p.3).

Cisco. BNG actúa como el punto de acceso para los suscriptores. Cuando la conexión entre el CPE y el enrutador BNG está establecida (por ejemplo, mediante una sesión IPoE) el suscriptor puede acceder a los servicios ofrecidos por el proveedor de servicios de Internet (ISP) (Cisco, 2021, p.20).

Juniper. El BNG realizan la gestión de los suscriptores, que incluye la administración de las sesiones, autenticación, autorización y contabilidad (AAA), QoS, entre otras. Además, se encarga de la asignación de las IP, servicios, monitoreo, control de tráfico de y hacia los suscriptores (Juniper, 2023, p.10).

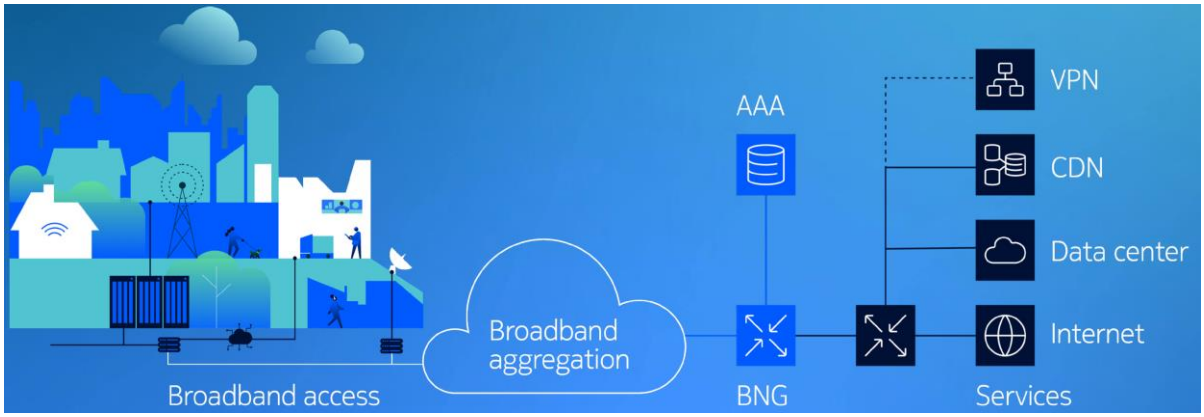
Huawei. BNG es crucial para la operación eficiente de los proveedores de redes de banda ancha. Sus características incluyen la autenticación, autorización de los CPE, así como de la asignación de direcciones IP a los CPE, el control del ancho de banda, y la gestión del tráfico y seguridad mediante el uso de firewall y filtros de acceso que protegen la red de ciberataques y garantizando la privacidad de los usuarios finales (Huawei, 2023).

En la figura 8, se muestra una red con BNG a alto nivel. A la izquierda de la imagen, se ubica el *Broadband Access,* que es parte de la red de acceso de última milla, en medio la nube *Broadband* Aggregation, la cual está compuesta por equipos de agregación de tráfico. A la derecha el BNG, que es el *Gateway* de los abonados. Este se puede comunicar

con un servidor AAA para autenticación de los suscriptores y, finalmente, se encuentran los servicios que el proveedor puede brindar, estos pueden ser VPN (*Virtual Private Network*), internet, entre otros.

Figura 8

Diagrama de red de banda ancha con Broadband Network Gateway (BNG)



Nota: en este esquema a alto nivel, el lado derecho de la imagen es el cercano a los usuarios finales, y en el lado izquierdo están los servicios que puede proporcionar el BNG, como VPN (*Virtual Private Network*), CDN (*Content Delivery Network*), recursos del Data center e internet. Nokia (2023).

Capítulo II. Marco teórico y conceptual

2.1 Marco teórico

2.1.1 Sistemas autónomos

Como parte de las definiciones iniciales de Internet, se pensó en el crecimiento de la cantidad de dispositivos (*gateways*) conectados y se planteó este crecimiento en conjuntos separados de sistemas autónomos que usarían protocolos y algoritmos relativamente homogéneos que sean de manera privada sin necesidad de ser usados fuera de ese dominio (IETF – RFC 827, 1982, p.1).

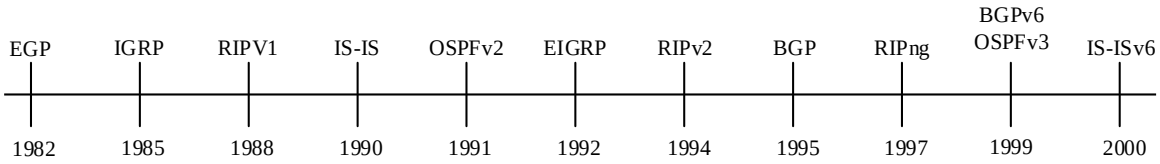
Un sistema autónomo (AS) es un segmento conectado de una topología de red que consiste en una colección de subredes (con *host* conectados) interconectadas por un conjunto de rutas. Se espera que las subredes y los enrutadores estén bajo el control de una única organización de operaciones y mantenimiento (O&M). Dentro de un AS, los enrutadores pueden utilizar uno o más protocolos de ruteo interior y, a veces, varios conjuntos de métricas. Se espera que un AS presente, a otros AS, la apariencia de un plan de enrutamiento interior coherente y una imagen coherente de los destinos a los que se puede llegar a través del AS. Un AS se identifica con un número de sistema autónomo (IETF, 1995, p.21). Como se menciona, a un sistema autónomo se le asigna un número de identificación. Este es administrado por la IANA y puede ser privado (IETF – RFC 6996, 2013, p.1) o público, de 16 bits (IETF – RFC 5398, 2008, p.2). o 32 bits (IETF – RFC 6793, 2012, p.1).

2.1.2 Protocolos de enrutamiento

El protocolo de enrutamiento se encarga de la selección del camino para esta transmisión de los datagramas. A continuación, se muestra la figura 9 donde aparecen, en orden cronológico, los protocolos de enrutamiento dinámicos, los cuales se pueden clasificar según el tipo de enrutamiento interno y externo de vector distancia, estado de enlace y vector de ruta, con clase y sin clase. Esto se muestra en la tabla 2.

Figura 9

Protocolos de enrutamiento



Nota: los protocolos no propietarios más usados en la actualidad son BGP, IS-IS y OSPF, cada uno en la versión de IPv4, IPv6 u otra extensión necesaria según la red. Cisco (2010, p. 5)

Tabla 2

Clasificación de los protocolos de enrutamiento

	Internal Routing Protocol				*External Routing Protocol*
	Por Vector Distancia		Por Estado de Enlace		Por Vector de Ruta
Con Clase	RIP	IGRP			EGP
Sin Clase	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGP-4 para IPv6

Nota: la clasificación de los protocolos de enrutamiento puede ser por su uso (interno o externo), por vector distancia o estado de enlace y para el caso de IPv4 si usa o no clase. Adaptado de Cisco (2010, p.5)

En el presente informe se revisarán los protocolos IS-IS y BGP.

2.1.2.1 Sistema intermedio a sistema intermedio (IS-IS)

Inicialmente implementado por *Digital Equipment Corporation,* a fines de 1970. Se adaptó posteriormente para ambientes OSI y TCP/IP (IETF – RFC 1195, 1990, p.1). Actualmente, definido en el ISO/IEC 10589:2002, es un protocolo basado en el estado del enlace y, como tal, es responsable de describir sus enlaces vecinos como el tipo de enlace (*point-to-point* o *broadcast*), la métrica, subredes directamente conectadas y externas al dominio de enrutamiento y su respectiva métrica. IS-IS usa encapsulación de capa 2 para sus mensajes con direcciones *Ethernet multicast* para comunicarse con otros equipos que tengan habilitado el protocolo.

2.1.2.2 Protocolo de puerta de enlace de frontera (BGP)

BGP es un protocolo de enrutamiento. La función principal de un sistema que habla BGP es intercambiar NLRI (*Network Layer Reachability Information*) con otros sistemas BGP. Los NLRI incluyen información sobre la lista de sistemas autónomos (AS) atravesados. Esta información es suficiente para construir una tabla de conectividad de AS, a partir de la cual se pueden eliminar bucles de enrutamiento y aplicar algunas políticas de decisiones (IETF – RFC 4271, 2006, p.7).

2.1.3 Conmutación de etiquetas multiprotocolo (MPLS)

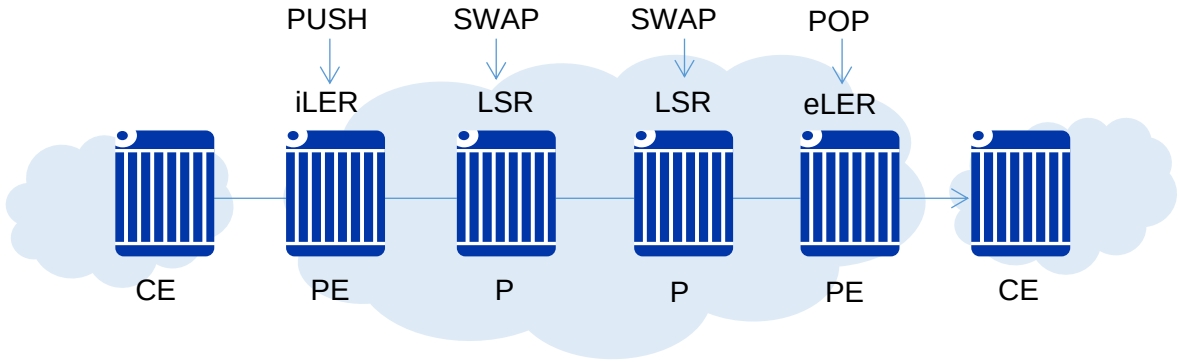
El término multiprotocolo hace referencia a que es una técnica aplicable a cualquier protocolo de la capa de red. Aquí se enfoca al protocolo IP. A diferencia del reenvío convencional de paquetes IP, donde se considera las IP de destino para atravesar la red, en MPLS cada paquete se encapsula con una 'etiqueta' antes de ser reenviado. En los saltos siguientes no se realiza un análisis de la cabecera IP sino de la etiqueta. Al entrar a la red MPLS, los paquetes son clasificados. Los paquetes que pertenecen a una misma clase se les llama FEC (*Forwarding Equivalence Class*). Los paquetes que pertenezcan a un mismo FEC y partan de un mismo nodo seguirán el mismo camino (IETF – RFC 3031, 2001a, p.4). A continuación, se muestra la terminología utilizada en MPLS.

Terminología para MPLS

- iLER (*Ingress Label Edge Router*): añade una etiqueta MPLS (*push*) al tráfico entrante enviado por el CE y lo envía a su siguiente salto.
- LSR (*Label Switch Router*): reemplaza la etiqueta (*swap*) del paquete entrante con la etiqueta correspondiente antes de enviarlo al siguiente salto.
- eLER (*Egress Label Edge Router*): remueve la etiqueta (*pop*) del paquete MPLS y la envía al CE.

Figura 10

Diagrama de la arquitectura MPLS



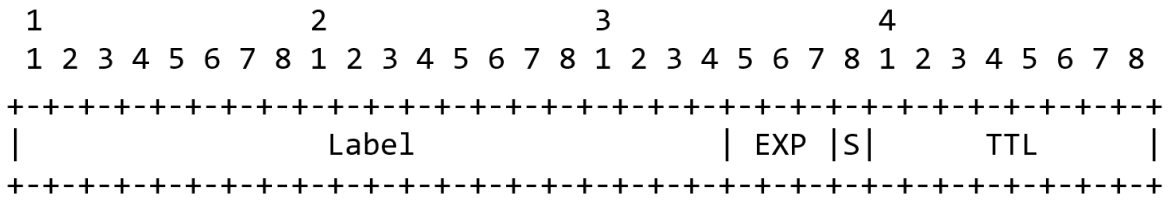
Nota: dentro de la red del proveedor de servicios los enrutadores se clasifican en PE (*Provider Edge Router*), P (*Provider Router*) y CE (*Customer Edge Router*). Nokia (2021b, p.26)

Los paquetes IP son encapsulados con la cabecera MPLS, la cual tiene un tamaño de 32bits como se muestra en la figura 11 y contiene los siguientes campos:

- Label (MPLS *Label*): el valor de la etiqueta MPLS.
- EXP (*Experimental*): mapeo de QoS de los bits ToS/CoS
- S (*Bottom of Stack*): un indicador para identificar la última cabecera MPLS
- TTL (*Time To Live*): tiempo de vida del paquete en saltos.

Figura 11

Diagrama de la cabecera MPLS



Nota: las etiquetas pueden asignarse para la creación de túneles de transporte y también para túneles de servicio VPN. Thomas (2023)

Por otro lado, para el funcionamiento de MPLS se requiere de un protocolo de distribución de dichas etiquetas entre los nodos. Estos pueden ser LDP, RSVP-TE y BGP-LU.

2.1.3.1 Protocolo de distribución de etiquetas (LDP)

Es un protocolo para la distribución de etiquetas. Los enrutadores que corren el protocolo LDP establecen sesiones con otros enrutadores para intercambiar información a

través de un grupo de mensajes y procedimientos. LDP mapea a cada FEC con una etiqueta (*label*), e informa a otros enrutadores del mapeo *Label*/FEC para el establecimiento de los LSP (*Label Switched Path*) a través de la red (IETF – RFC 5036, 2007, p.5). Se basa en IGP para la construcción de los LSP, por lo que su tiempo de convergencia depende de la convergencia del IGP. Es de fácil configuración y anuncia la información de label/FEC de manera automática manteniendo todos los FEC recibidos, aunque no estén siendo utilizados.

2.1.3.2 BGP - Unidifusión etiquetada (BGP - LU)

Cuando BGP se usa para distribuir una ruta, puede distribuir una etiqueta MPLS que esté mapeada a esa ruta; es decir, esta etiqueta es enviada dentro del mismo mensaje NLRI usando un atributo adicional definido en el RFC 2283 (MP_UNREACH_NLRI) (IETF – RFC 3107, 2001b, p.2).

En la figura 12, se muestra un registro de cómo se recibe una ruta IPv4 con una etiqueta MPLS dentro de un mensaje *UPDATE* de BGP. Esta extensión dentro de BGP también permite extender dominios MPLS más allá del sistema autónomo.

Figura 12

Mensaje UPDATE de BGP Labeled-IPv4

```
2 2013/05/16 10:03:57.33 UTC MINOR: DEBUG #2001 vprn100 Peer 2: 192.168.0.2
"Peer 2: 192.168.0.2: UPDATE
Peer 2: 192.168.0.2 - Received BGP UPDATE:
    Withdrawn Length = 0
    Total Path Attr Length = 41
    Flag: 0x90 Type: 14 Len: 17 Multiprotocol Reachable NLRI:
        Address Family IPV4-Labeled
        NextHop len 4 NextHop 192.168.0.2
        192.0.2.22/32 Label 262138
    Flag: 0x40 Type: 1 Len: 1 Origin: 0
    Flag: 0x40 Type: 2 Len: 6 AS Path:
        Type: 2 Len: 1 < 64496 >
    Flag: 0x40 Type: 3 Len: 4 Nexthop: 192.168.0.2
"
```

Nota: dentro del mensaje UPDATE se encuentra el Label 262138 asignado al segmento 192.0.2.22/32. Bookham (2014).

2.1.4 Traducción de direcciones de red (NAT)

Es una técnica para compartir una IP entre múltiples hosts. El dispositivo NAT realiza la traslación de dirección de la cabecera IP de los paquetes entre un host y un servidor, cambia algunos (o todos) de los siguientes campos: dirección de origen, dirección de destino, puerto de origen (UDP/TCP), puerto de destino (UDP/TCP), o ID de consulta en ICMP (ping) (Nokia, 2016a). Esta técnica es útil en las redes actuales, mientras se realiza la transición de IPv4 a IPv6.

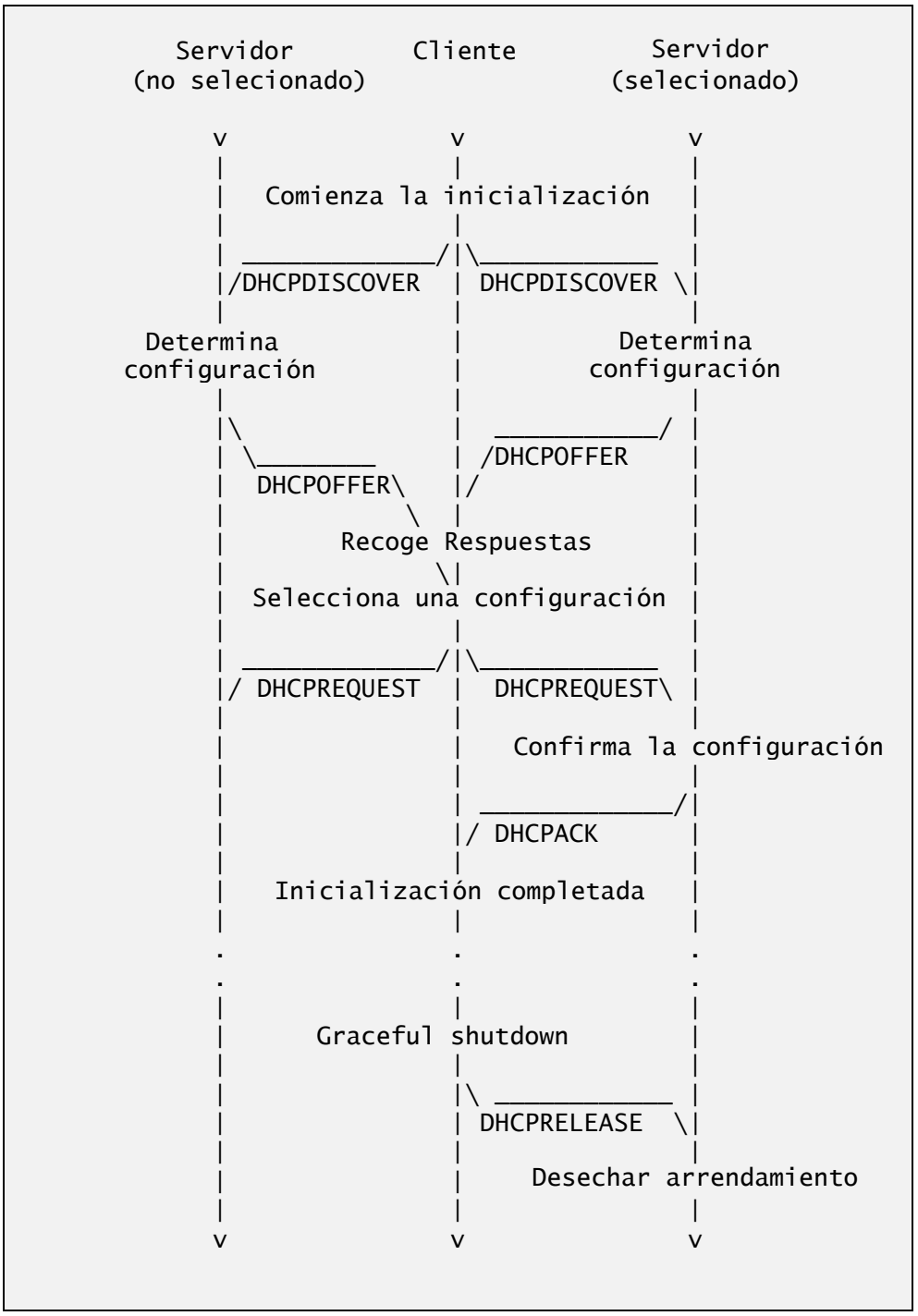
2.1.5 Protocolo de configuración dinámica de huésped (DHCP)

DHCP (*Dynamic Host Configuration Protocol*) proporciona una estructura para la configuración automática de los *hosts* en una red TCP/IP. Consiste en dos componentes: un protocolo para el envío de los parámetros de configuración del *host* y un mecanismo para la asignación de direcciones a los *hosts* (IETF – RFC 2131, 1997, p.2).

Se construye bajo un modelo cliente-servidor. El servidor es el que provee de los parámetros de configuración y el cliente quien los solicita. DHCP soporta tres mecanismos para la asignación de IP: asignación automática, asignación dinámica y asignación manual. La asignación dinámica es la única que permite el reúso de direcciones IP que los clientes dejan de utilizar. Es muy útil cuando los clientes se conectan a una red temporalmente o cuando las direcciones IP son pocas y se requieren recuperar las IP cuando se retiren (IETF – RFC 2131, 1997, p.3).

Figura 13

Mensajes enviados entre el cliente y servidor DHCP



Nota: tomado de IETF – RFC 2131 (1997).

El proceso que sigue un cliente-servidor para la asignación de una IP de la red es el mostrado en la figura 13 y se puede describir como sigue (IETF - RFC 2131, 1997, p.13 – p17).

1. El cliente transmite un mensaje broadcast *DHCPDISCOVER*, que puede incluir algunas opciones que sugieran la asignación del servidor.
2. Cada servidor puede responder con un mensaje *DHCPOFFER*, incluyendo la IP y otros parámetros de configuración sin reservar aún la IP ofrecida.
3. El cliente recibe uno o más mensajes *DHCPOFFER*. El cliente elige un servidor basándose en los parámetros ofrecidos, luego transmite un mensaje *DHCPREQUEST,* que incluye la IP del servidor escogido y las opciones donde se especifican los valores de configuración deseados.
4. Los servidores reciben el mensaje *broadcast DHCPREQUEST* del cliente, el servidor seleccionado se compromete con el cliente y responde con un mensaje *DHCPACK*.
5. El cliente recibe el mensaje *DHCPACK* con los parámetros de configuración. En este punto el cliente está configurado.
6. El cliente puede elegir renunciar a la IP enviando un mensaje *DHCPRELEASE* hacia el servidor.

2.1.6 Servicio de usuario de marcación remota (RADIUS)

Las principales características del protocolo *RADIUS* (*Remote Authentication Dial In User Service*) relacionadas a la autenticación de usuarios residenciales son: modelo Cliente/Servidor y protocolo ampliable (IETF – RFC 2865, 2000, p.4).

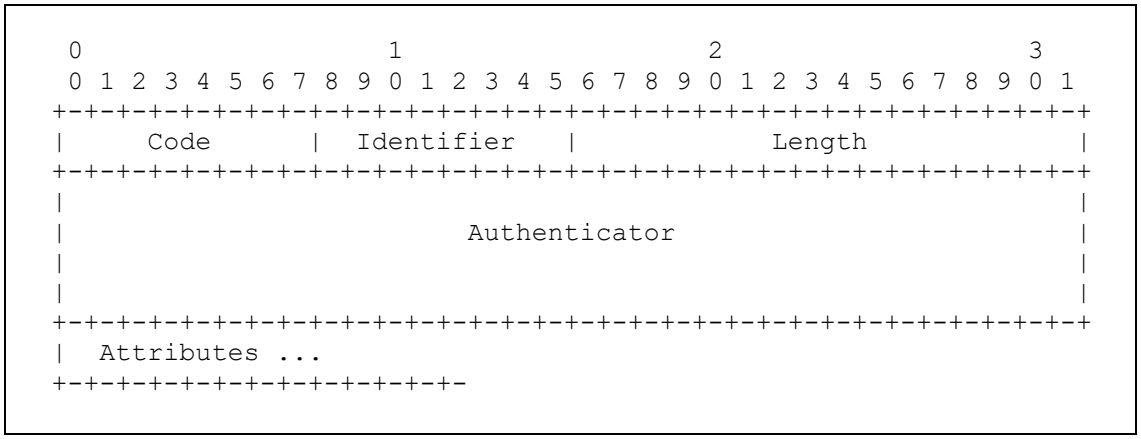
Modelo cliente/servidor. Un NAS (*Network Access Server*) opera como un cliente de *RADIUS.* Es responsable de pasar la información de los usuarios a servidores *RADIUS* designados. Los servidores son responsables de recibir las solicitudes de conexión de los usuarios, autenticarlos y regresar toda la información de configuración necesaria para que el cliente brinde el servicio al usuario. Además, un servidor *RADIUS* puede actuar como un cliente proxy para otros servidores *RADIUS* u otros tipos de servidores de autenticación (IETF – RFC 2865, 2000, p.4).

Protocolo ampliable. Todas las transacciones se componen de tuplas de tres datos: atributo, longitud y valor. Nuevos atributos pueden añadirse sin perturbar las implementaciones existentes del protocolo.

Los paquetes *RADIUS* son encapsulados en UDP con puerto destino 1812. Cuando se genera una respuesta, los puertos origen y destino son invertidos. El formato de los paquetes se muestra a continuación (IETF – RFC 2865, 2000, p.13).

Figura 14

Formato de Trama RADIUS



Nota: tomado de IETF – RFC 2865 (2000).

El campo ‘Code’ identifica el tipo de paquete *RADIUS* (*Access-Request, Access-Accept, Access-Reject,* etc.). El campo ‘Identifier’ ayuda a hacer coincidir las solicitudes y respuestas (el servidor *RADIUS* puede detectar una solicitud duplicada si el paquete tiene la misma IP origen, Puerto UDP e ‘Identifier’). El campo ‘Length’ indica la longitud total del paquete (considera los campos ‘Code’, ‘Identifier’, ‘Length’, ‘Authenticator’ y ‘Attributes’). El campo ‘Authenticator’ se usa para autenticar la respuesta del servidor *RADIUS.* Por último, el campo ‘Attributes’ es un campo variable y contiene la lista de atributos que son requeridos para cada tipo de servicio, así como los atributos opcionales (IETF – RFC 2865, 2000, p.15).

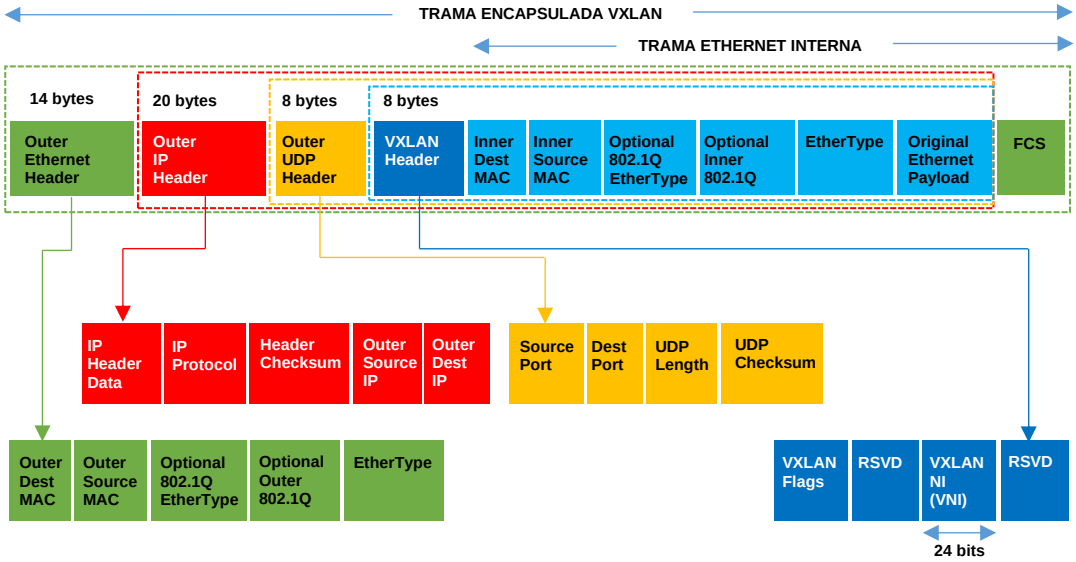
2.1.7 Red de área local virtualmente extensible (VXLAN)

VXLAN (*Virtual eXtensible Local Area Network*) es una estructura para manejar redes virtualizadas de capa 2 y 3. La virtualización de servidores ha impuesto mayores exigencias a la infraestructura física de redes. Un servidor físico ahora tiene múltiples máquinas virtuales (VM) cada una con su propia dirección MAC (*Media Access Control*). Esto requiere de largas tablas de direcciones MAC en la red *Ethernet* debido a la posible conexión y comunicación entre cientos de miles de máquinas virtuales. En el caso de VM, en un Data Center son agrupados en VLAN. Una puede necesitar de miles de VLAN para particionar el tráfico de acuerdo con el grupo específico al que la VM pertenece. El actual límite de VLAN es 4094, es inadecuado para estas situaciones. Junto a otros escenarios, son los requerimientos de la construcción de una red '*overlay',* la cual se construye sobre una capa de red (IP/MPLS). Esta red se usa para enviar tráfico MAC de las VM individuales en un formato encapsulado sobre un túnel lógico (IETF – RFC 7348, 2014, p.3).

En resumen, VXLAN es un esquema de capa 2 '*overlay'* en una red de capa 3. Cada *overlay* se denomina Segmento VXLAN. Solo las VM dentro del mismo segmento VXLAN se pueden comunicar entre sí. Cada segmento se identifica con un ID de 24 bits denominado VNI (*VXLAN Network Identificator*). Esto permite que coexistan hasta 16M de segmentos VXLAN dentro del mismo dominio administrativo. El VNI identifica el alcance de la trama MAC; por lo tanto, se podría tener direcciones MAC superpuestas en todos los segmentos, pero nunca tener un tráfico 'cruzado'; ya que se aíslan por el VNI. El VNI está en un encabezado externo que encapsula la trama MAC originada por la VM. Debido a la encapsulación, VXLAN podría denominarse un esquema de tunelización para superponer redes de Capa 2 sobre redes de Capa 3 (IETF – RFC 7348, 2014, p.7).

Figura 15

Formato de trama VXLAN con cabecera IPv4



Nota: tomado de Chang E. (2015).

2.2 Marco conceptual

2.2.1 Redes privadas virtuales (VPN)

A lo largo de los años, se han desarrollado diferentes tecnologías como TDM (*Time-Division Multiplexing*) para voz en tiempo real, *Frame Relay* y ATM para servicios privados, IP para servicios de datos de mejor esfuerzo (*best-effort*). Los cuales eran desplegados en redes separadas para proveer estos distintos servicios. Un enfoque, para el desarrollo de servicios bajo una infraestructura común, usa una red IP/MPLS que soporta un grupo de servicios VPN (*Virtual Private Network*) (Nokia, 2022a, p.11)

Para el cliente, una VPN es una red privada; para el proveedor de servicios, una red virtual, que puede ser desplegada en múltiples instancias para diferentes clientes en una sola infraestructura física. Entre los posibles tipos de servicios VPN se tienen los siguientes:

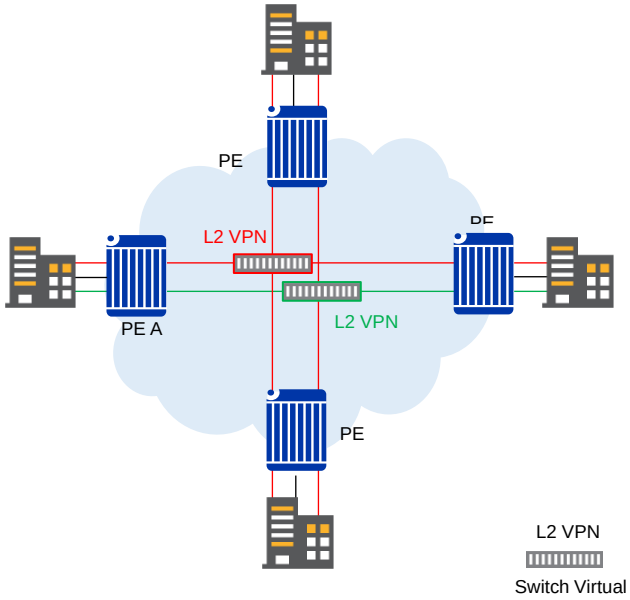
- L2 VPN (*Layer 2 Virtual Private Network*) provee un servicio *Ethernet* Multipunto
- L3 VPN (*Layer 3 Virtual Private Network*) provee un servicio IP Multipunto

2.2.1.1 Servicios L2 VPN

L2 VPN es un servicio que conecta múltiples sitios en un solo dominio conmutado sobre la red IP/MPLS del proveedor. Como se muestra en la figura 16, una L2 VPN es adecuada para un cliente que requiere un simple servicio Ethernet para conectar más de dos sitios (Glenn, 2011a, p.2).

Figura 16

Servicios L2 VPN usando el mismo core IP/MPLS



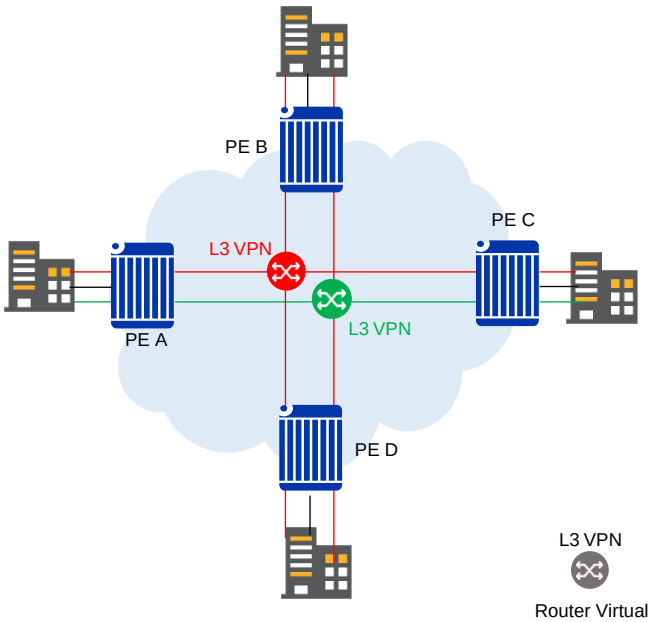
Nota: múltiples servicios pueden ser desplegados, en la figura se muestra dos servicios L2 VPN independientes que unen cuatro sedes. Adaptado de Glenn (2011a).

2.2.1.2 Servicios L3 VPN

L3 VPN es un servicio IP de capa 3 que conecta múltiples sitios en un solo dominio enrutado sobre la red IP/MPLS del proveedor. Como se muestra en la figura 17, una L3 VPN es adecuada para un cliente que requiere un servicio enrutado IP para conectar múltiples sitios (Glenn, 2011b, p.8).

Figura 17

Servicios L3 VPN usando el mismo core IP/MPLS



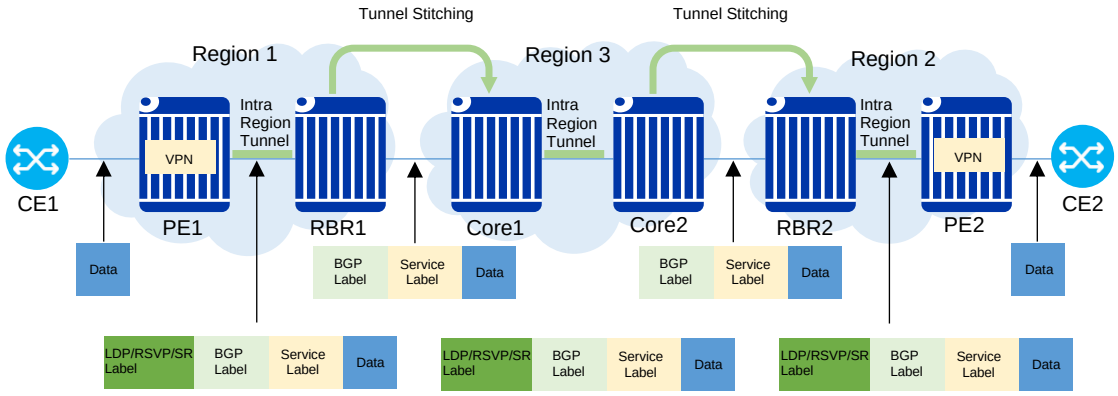
Nota: múltiples servicios pueden ser desplegados, en la figura se muestra dos servicios L3 VPN independientes que unen cuatro sedes. Adaptado de Glenn (2011b).

2.2.2 MPLS sin interrupciones (*Seamless* MPLS)

Seamless MPLS es una estructura que puede usarse para extender las redes MPLS a través de los dominios de acceso y agregación con lo que la red completa puede considerarse un solo dominio MPLS. La arquitectura usa el enfoque ‘divide y vencerás’. Construye sobre una topología típica de proveedor de servicios, donde la jerarquización es un elemento clave. El dominio de enrutamiento interno se implementa usando OSPF o IS-IS, y el dominio de enrutamiento externo se implementa usando BGP LU para distribuir la dirección IP *loopback* de servicio entre dominios (Bookham, 2014, p.107).

Figura 18

Encapsulación en el plano de datos con Seamless MPLS



Nota: tomado de Nokia (2021a, p.123).

2.2.3 Proveedor de servicios de internet (ISP)

Internet es un grupo de redes interconectadas que son operadas por proveedores de servicios de internet (ISP) y operadores de telecomunicaciones. El direccionamiento IP usado en Internet es administrado por la IANA (*Internet Assigned Numbers Authority*), operada por la ICANN (*Internet Corporation for Assigned Names and Numbers*). La ICANN/IANA administra la asignación en cinco RIR (*Regional Internet Registries*) (Warnock, Ghafary & Shaheen, 2006, p.21).

- AfriNIC – *African Network Information Centre*
- APNIC – *Asia Pacific Network Information Centre*
- ARIN – *American Registry for Internet Numbers*
- LACNIC – *Latin America and Caribbean Network Information Centre*
- RIPE NCC – *Réseaux IP Européens Network Coordination Centre*

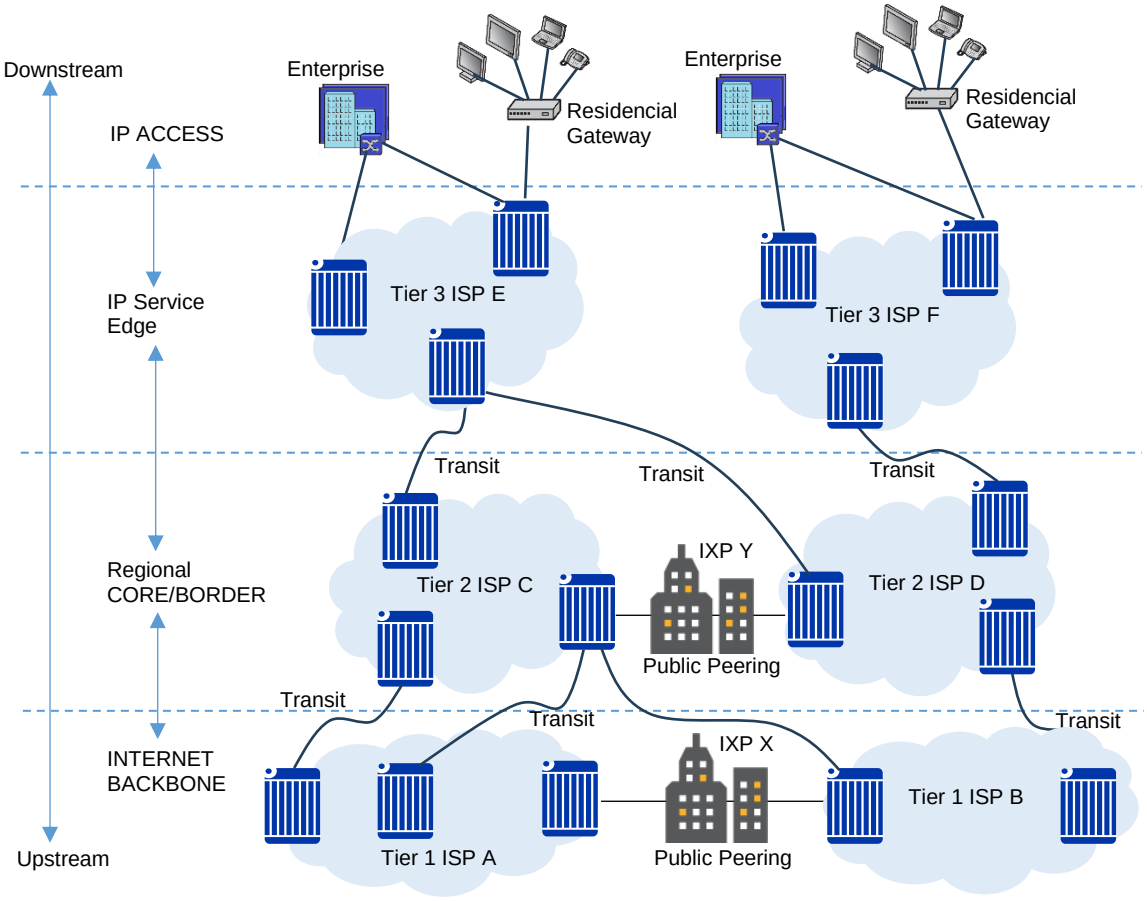
Los ISP se clasifican en uno de los tres diferentes niveles.

- Nivel 1 (Tier 1). Es un ISP que puede alcanzar cualquier red en Internet sin pagar tarifas de tránsito. Los ISP tier 1 deben ser peer de todos los otros ISP tier 1.

- Nivel 2 (Tier 2). Son ISP que abarcan grandes áreas regionales de un país o un continente, pero no tiene el mismo alcance global que un ISP tier 1. Se basa en relaciones con otros ISP tier 2 y compra servicios de tránsito de ISP tier 1.
- Nivel 3 (Tier 3). Es un ISP que sirve a pequeñas áreas regionales y depende solo de comprar servicios de tránsito de ISP más grandes, usualmente de ISP tier 2.

Figura 19

Representación de los niveles de proveedores de internet



Nota: tomado de Warnock, Ghafary y Shaheen (2006).

2.2.4 Red de acceso de banda ancha

Según el artículo 4 de la Ley N° 29904, “Ley de promoción de Banda Ancha”, la cual impulsó este proyecto, se puede dar una definición de Banda Ancha:

> […] entiéndase por Banda Ancha a la conectividad de transmisión de datos principalmente a internet, en forma permanente y de alta velocidad, que permite al

> usuario estar siempre en línea, a velocidades apropiadas para la obtención y emisión interactiva de información multimedia, y para el acceso y utilización adecuada de diversos servicios y aplicaciones de voz, datos y contenidos audiovisuales. (Congreso de la República, 2012, p.1)

En línea con esto, en el artículo 6 de la Ley 31207, se le da al MTC el rol de fijar la velocidad mínima para considerar una conexión de banda ancha, mientras que al Osiptel se le otorga el rol vigila y actualiza los parámetros regulatorios para su cumplimiento:

> El Ministerio de Transportes y Comunicaciones determina y actualiza anualmente la velocidad mínima para que una conexión sea considerada como acceso a internet de banda ancha, que será aplicable con independencia de la ubicación geográfica de los usuarios. Los prestadores de servicios de internet deberán garantizar el 70% de la velocidad mínima ofrecida en los contratos con los consumidores o usuarios (…). El Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), a través del Registro Nacional de Monitoreo y Vigilancia del Servicio de Internet (RENAMV), vigila y actualiza periódicamente la velocidad de internet y otras características técnicas de las conexiones a internet de banda ancha. (Congreso de la República, 2021, p.2)

Con esto en consideración, en el año 2022, se emite la Resolución Ministerial N° 1197-2022-MTC/01.03, donde se realizó la aprobación de la velocidad mínima para el acceso a internet de banda ancha para red fija con los parámetros de 20 Mbps (descarga efectiva) y 7 Mbps (carga efectiva) con un porcentaje mínimo entre la velocidad mínima y la velocidad contratada de 70%.

Por otro lado, el actual Reglamento General de Calidad de los Servicios Públicos de Telecomunicaciones, para la supervisión de los parámetros mencionados, fue aprobado en la Resolución N° 00214-2024-CD/OSIPTEL emitido por el Consejo Directivo del Osiptel.

El Reglamento General de Calidad de los Servicios Públicos de Telecomunicaciones define, entre otros parámetros, el Indicador de Cumplimiento de Velocidad Mínima (CVM) y el Indicador de Asimetría. Establece que el Indicador de Cumplimiento de Velocidad Mínima (CVM) se refiere al porcentaje de mediciones de las velocidades de bajada y subida que cumplen con la velocidad mínima establecida y el Indicador de Asimetría corresponde a la relación de las velocidades de subida y bajada que son ofrecidas por las empresas operadoras en sus planes comerciales (Osiptel, 2024, p.5-6).

Asimismo, en el reglamento se define la manera de medición de dichos parámetros y los valores que deben cumplir (Osiptel, 2024, p.26-27). Para el indicador CVM de los servicios de acceso a Internet fijo y de acceso a Internet móvil que califican como banda ancha (CVM_{BA}), conforme a la definición del MTC, se considera que las empresas operadoras garanticen al menos el 70 % de la velocidad contratada; el operador cumple con este indicador (CVM_{BA}) si el resultado de la ecuación (1), es igual o superior al 70 %.

$$\mathrm{CVM_{BA}} = \frac{\sum \left[\frac{\text{Valor resultante de medicion TTD expresado en Mbps}}{\text{Velocidad nominal contratada expresada en Mbps}}\right] \times 100\%}{\text{Total de mediciones TTD}} \qquad (1)$$

Donde TTD es la tasa de transferencia de datos:

$$\mathrm{TTD} = \frac{\text{Volumen de datos (bits)}}{\text{Duración de la prueba (segundos)}} \qquad (2)$$

En el caso de los servicios que no califican como banda ancha**,** el reglamento establece un estándar diferente: las empresas deben garantizar un mínimo del 40 % de la velocidad contratada. Sin embargo, para que el indicador (CVM_{NBA}) se considere cumplido el resultado de la ecuación (3) debe ser igual o superior al 95 %.

$$\mathrm{CVM_{NBA}} = \frac{\text{Número de mediciones TTD} \geq 40\% \text{ de la velocidad contratada}}{\text{Total de mediciones TTD}} \times 100\% \qquad (3)$$

Por otro lado, el reglamento introduce el Indicador de Asimetría, el cual evalúa la relación entre las velocidades de subida y bajada ofrecidas comercialmente por las empresas. Esta relación resultante de la ecuación (4) no debe ser menor a 1:3, lo que significa que la velocidad de subida debe representar al menos el 33,33 % de la velocidad de bajada:

$$\text{Asimetría} = \frac{\sum\left(\frac{\min[V_{sm}, V_{sm}]}{\min[V_{bm}, V_{bc}]}\right) \times 100\%}{\text{Total de mediciones TTD}} \quad (4)$$

Donde:

V_{sm}: Velocidad de subida resultante de la medición TTD expresada en Mbps

V_{sc}: Velocidad de subida contratada expresada en Mbps

V_{bm}: Velocidad de bajada resultante de la medición TTD expresada en Mbps.

V_{bc}: Velocidad de bajada contratada expresada en Mbps.

Arquitectura de una red de Acceso de Banda Ancha

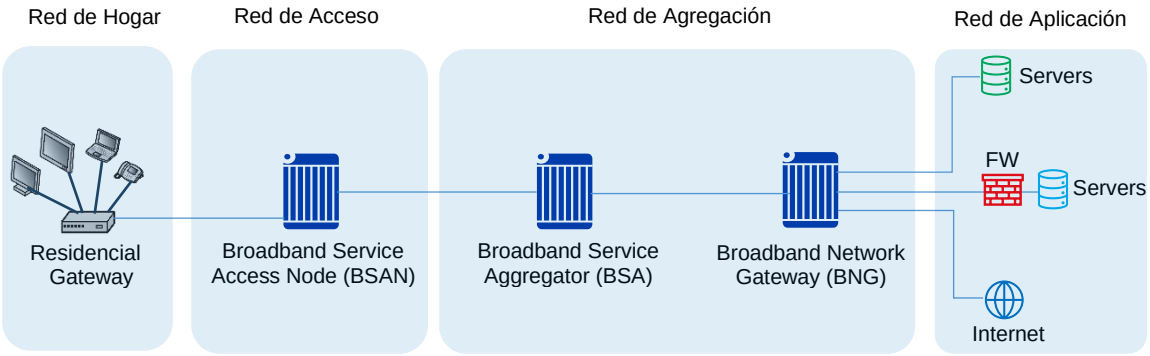
En relación a la infraestructura, las redes de acceso de banda ancha (Broadband Access Network) pueden dividirse en segmentos de red de la siguiente manera (Nokia, 2016b, p.15):

- Red de hogar. Su principal función es de interconectar los dispositivos de usuarios residenciales a la red del proveedor de servicios a través del *Residential Gateway* (RG), el RG provee un *Gateway* local e información de direccionamiento a los dispositivos de los usuarios finales.
- Red de acceso. Su principal función es de soportar diferentes tecnologías físicas de acceso hacia la Red de hogar, el *Broadband Service Access Network (*BSAN*)* se conecta al RG.
- Red de agregación *Network*. Su principal función es agregar los dispositivos de la *Access Network* hacia la red de aplicación. Contiene dos tipos de dispositivos: *Broadband Service Aggregator* (BSA), que opera en modo conmutador, y el *Broadband Network Gateway* (BNG), que opera en modo enrutador.

- Red de aplicación. Consiste en servidores DHCP, AAA, Internet y otros servidores usados para proveer el servicio a los usuarios.

Figura 20

Diagrama de una Red de Banda Ancha con Broadband Network Gateway



Nota: tomado de NOKIA (2016b)

Esta arquitectura se usa para brindar acceso a internet y otros recursos en la red.

2.2.5 Redes definidas por *software* (SDN)

SDN ha emergido como una arquitectura de redes y es una nueva manera de usar software para manejar y operar redes. Sus principales principios son los siguientes (Nuage Networks, 2020a, p.16).

- Separación del plano de control y de datos, la ONF (*Open Networking Foundation*) ha estandarizado un protocolo de control del plano de datos: *OpenFlow*.
- Interfaz programable. A través de API (*Application Programming Interface*) es posible tener una vista abstracta de la red física, correr aplicaciones que usen las API para controlar o manipular la red.
- Típicas aplicaciones usando API pueden realizar ingeniería de tráfico, flujo de tráfico basado en políticas, monitoreo central de la red.

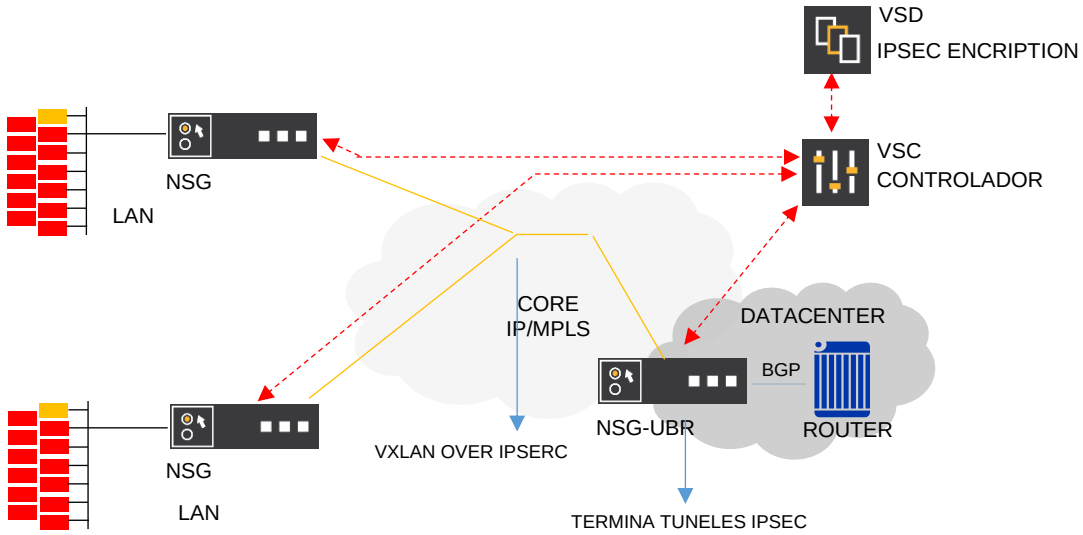
También, ya que el plano de control y la programabilidad están centralizadas, se puede usar modelos basados en políticas para automatizar varias tareas en la red.

Entre las soluciones de SDN está la ofrecida al acceso, esta se denomina *overlay;* ya trabaja sobre una arquitectura de red y crea servicios usando túneles VXLAN, similares a las VPN basadas en MPLS (Nuage Networks, 2020a, p.17).

A continuación, se muestra una representación de la arquitectura de red SDN de *Nuage Networks*.

Figura 21

Arquitectura de red Software Defined Network (SDN)



Nota: tomado de Nuage Networks (2020a).

Capítulo III. Desarrollo del trabajo de investigación

3.1 Requerimientos para la implementación

Como se describió en la sección 1.2.2, se parte del hecho de que ya se dispone de una infraestructura establecida para red de acceso a la cual le hace falta incluir la funcionalidad de red de banda ancha con *Broadband Network Gateway* (BNG). Para lo cual se requiere lo siguiente:

- Definir la función de los enrutadores de la red y la ingeniería de servicios L2 VPN y L3 VPN necesarios para brindar la conectividad de los CPE con el enrutador BNG, y el servicio para los usuarios de la red.

Además, para la implementación de los enrutadores BNG, se extraen los requerimientos relacionados como se describe en el Anexo 8-B de las Bases – Especificaciones Técnicas numeral 3.7 Acceso a Internet, del contrato del financiamiento (PROINVERSIÓN, 2017, pp.3) para la red de acceso de la región Puno:

> *"El CONTRATADO brindará a las INSTITUCIONES ABONADAS OBLIGATORIAS acceso a Internet con las siguientes características técnicas mínimas:*
>
> *a. Cuarenta por ciento (40%) de velocidad garantizada de bajada y de subida, respecto de la velocidad nominal.*
>
> *b. Relación entre la velocidad de transmisión de bajada (velocidad de descarga) y la velocidad de transmisión de subida de 4 a 1.*
>
> *c. Acceso Full Dúplex."*

Adicionalmente, se debe atender la demanda de acceso a intranet como se describe en las mismas bases, numeral 3.8 Acceso a Intranet inciso "b" (PROINVERSIÓN, 2017, pp.4):

> […] Para el acceso a Intranet a través de computadoras (PC, laptops, tabletas y equipos móviles con acceso a redes wifi), el CONTRATADO deberá asegurar prestar el servicio con las siguientes características:
>
> a. Cuarenta por ciento (40%) como mínimo de la velocidad de transmisión...

b. Relación entre la velocidad de transmisión de subida respecto de la velocidad de transmisión de bajada es de 1:1.
c. Acceso Full Dúplex.

[…]

Para cumplir lo señalado se deberá realizar la configuración de PIR/CIR por suscriptor para asegurar las velocidades garantizadas. Finalmente, se debe atender quinientos ochenta y un (581) locales escolares, según se señala en las bases, sección 2.2 (PROINVERSIÓN, 2017, pp.1).

Cabe resaltar que los requerimientos técnicos establecidos en el contrato firmado en 2017, como la garantía del 40 % de la velocidad nominal en ambos sentidos y una relación de asimetría de hasta 4:1, se encuentran alineados con el marco normativo vigente en ese momento. Sin embargo, según lo descrito en la sección 2.2.4, estos parámetros resultan menos exigentes frente a los criterios actuales para considerar un servicio como banda ancha en el Perú. Conforme a lo establecido por el MTC mediante la Resolución Ministerial N.º 1197-2022-MTC/01.03, una conexión de banda ancha (en el caso de Internet fijo), debe alcanzar una velocidad mínima efectiva de 20 Mbps en descarga, 7 Mbps en carga y garantizar como mínimo el 70 % de la velocidad contratada. Asimismo, el Reglamento General de Calidad aprobado en la Resolución N° 00214-2024-CD/OSIPTEL exige que la relación de asimetría no sea inferior a 1:3. Esta diferencia normativa evidencia la evolución del estándar de calidad para el servicio de acceso a Internet y refuerza la necesidad de considerar adecuaciones futuras para mantener la compatibilidad con los marcos regulatorios vigentes.

3.2 Implementación de una red con *Broadband Network Gateway* (BNG)

3.2.1 Definición de las funciones de los enrutadores y de los servicios VPN

Como se explicó en la sección 2.2.4, con base en la arquitectura *Broadband Access Network* para brindar el servicio de internet. A continuación, se detalla la función asignada a cada tipo enrutador para esta arquitectura.

- **RG (*Residencial Gateway*).** El equipo CPE cumplirá la función del RG. Además, por pertenecer a una solución de SND, recibirá una configuración específica desde su controlador y realizará el reenvío de tráfico de usuarios encapsulándolo en un túnel VXLAN. La descripción de las características del equipo escogido se muestra en el anexo 2.
- **BSAN (*Broadband Service Access Node*).** El enrutador terminal e intermedio cumplirán con la función del BSAN. Este equipo recibe los paquetes enviados por los CPE (de datos y control) y son encapsulados dentro en un servicio L2 VPN, que tiene como destino al enrutador distrital. La descripción de las características del equipo escogido se muestra en el anexo 3.
- **BSA (*Broadband Service Aggregator*).** El enrutador distrital cumplirá con la función de BSA. Se encargará de agregar todo el tráfico enviado desde los equipos terminales e intermedios Los paquetes son recibidos en un servicio L2 VPN y luego es reenviado, en un nuevo túnel MPLS señalizado por BGP (BGP LU), hacia los dos enrutadores del *core* de acceso. La descripción de las características del equipo escogido se muestra en el anexo 3.
- **BNG (*Broadband Network Gateway*).** Los enrutadores de *core* de acceso cumplirán el rol principal de BNG y recibirán el tráfico procedente de todos los CPE conectados a la red de acceso. La descripción de las características del equipo escogido se muestra en el anexo 4.

Luego, se procede a crear, en todos clústeres, los servicios L2 VPN necesarios que conecten a los CPE con los *core* de la red de acceso (CR1 y CR2). Para esto se debe considerar lo siguiente:

- Creación de túneles MPLS bidireccionales señalizados por LDP entre el enrutador terminal (e intermedio) y el enrutador distrital
- Creación de túneles MPLS bidireccional señalizado por BGP LU entre el enrutador distrital y los enrutadores de *core* de acceso.
- Creación de un servicio L2 VPN entre los enrutadores terminal (e intermedio) y el enrutador distrital.
- Creación de un servicio L2 VPN entre el enrutador distrital y los enrutadores de *core* de acceso (CR1 y CR2) usando redundancia de *Pseudo Wire* (PW *Redundancy*). El CR1 es el nodo principal o activo y el CR2 el secundario o en espera.

Además, es necesaria la creación de servicios L3 VPN para el enrutamiento final de los usuarios hacia internet o intranet. Para esto se debe considerar lo siguiente:

- Creación de un servicio L3 VPN para conectar a todos los usuarios de las instituciones educativas. Desde la cual podrán ser enrutados a una L3 VPN donde reside el servidor de Intranet o hacia una L3 VPN donde pasan a un proceso de NAT para su salida a Internet.

El siguiente paso implica el cálculo de los parámetros necesarios para cumplir con los requerimientos. Para ello, se toma en cuenta la cantidad total de 581 instituciones educativas y la definición de tres (03) planes de navegación para internet e intranet.

3.2.2 Cálculo de la máscara de red para los CPE de las instituciones educativas

Una vez que el servidor AAA ha autenticado y autorizado al CPE, los enrutadores de *core* de acceso se comunicarán con el servidor DHCP para la asignación de una dirección IP al dispositivo. Para este propósito, es crucial considerar un segmento de red

lo suficientemente amplio para alojar a los 581 CPE del total de instituciones educativas. Para determinar el tamaño adecuado de este segmento, emplearemos la siguiente fórmula (Wendell, 2020):

$$\#\text{Dispositivos} \leq 2^{n} - 2 \quad (5)$$

Donde n es un número entero que representa el número de bits en la parte de host de la dirección IP. Resolviendo está inecuación para n encontramos que

$$581 \leq 2^{n} - 2$$

$$n \geq \log_2 583$$

$$n \geq 9.187$$

$$n = 10$$

Es decir, con el valor de n=10 se garantizará un segmento lo suficientemente grande para acomodar los 581 CPE. Para poder apreciar mejor esta relación a continuación se muestra una tabla con la cantidad de host por mascara de red.

Tabla 3

Cantidad de host por segmento de red

N.º hosts	n	CIDR	Mascara de Red en Binario	Mascara de Red en Decimal
…		…	…	…
126	7	/25	11111111.11111111.11111111.10000000	255.255.255.128
254	8	/24	11111111.11111111.11111111.00000000	255.255.255.0
510	9	/23	11111111.11111111.11111110.00000000	255.255.254.0
1022	**10**	**/22**	**11111111.11111111.11111100.00000000**	**255.255.252.0**
2046	11	/21	11111111.11111111.11111000.00000000	255.255.248.0
4094	12	/20	11111111.11111111.11110000.00000000	255.255.240.0
…		…	**…**	…

Nota: CIDR (*Classless Inter-Domain Routing*), RFC 4632. Con esta interpretación el uso de las direcciones IPv4 se volvió más eficiente.

En consecuencia, se decide asignar el segmento privado 10.0.32.0/22 para todos los CPE.

3.2.3 Cálculo del ancho de banda de internet e intranet para los CPE

En esta sección, se detallan los cálculos realizados con la ecuación (6) para establecer los valores de CIR (Tasa de información comprometida) y PIR (Tasa de información pico). Los cuales distribuyen eficientemente los recursos de la red tanto en las

conexiones a internet como en intranet para los tres (03) planes de navegación establecidos por el proveedor.

$$\text{Tasa de Información (CIR o PIR)} = \text{Porcentaje Garantizado\%} \times \text{BW(Mbps)} \quad (6)$$

- **Cálculo de anchos de banda para un plan de 2 Mbps**

  Intranet (Simetría 1:1)

  Velocidad de bajada = 2 Mbps, con PIR 100% y CIR 40%:

$$\text{CIR} = 40\% \times 2\ \text{Mbps} = 0.8\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 2\ \text{Mbps} = 2\ \text{Mbps}$$

  Velocidad de subida = 2 Mbps, con PIR 100% y CIR 40%:

$$\text{CIR} = 40\% \times 2\ \text{Mbps} = 0.8\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 2\ \text{Mbps} = 2\ \text{Mbps}$$

  Internet (Simetría 4:1)

  Velocidad de bajada = 2 Mbps, con PIR 100% y CIR 40%:

$$\text{CIR} = 40\% \times 2\ \text{Mbps} = 0.8\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 2\ \text{Mbps} = 2\ \text{Mbps}$$

  Velocidad de subida = 1/4 de 2 Mbps, con PIR 100% y CIR 40%:

$$\text{BW} = \frac{2\ \text{Mbps}}{4} = 0.5\ \text{Mbps}$$

$$\text{CIR} = 40\% \times 0.5\ \text{Mbps} = 0.2\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 0.5\ \text{Mbps} = 0.5\ \text{Mbps}$$

- **Cálculo de anchos de banda para el plan de 4 Mbps**

Intranet (Simetría 1:1)

Velocidad de bajada = 4 Mbps, con PIR 100% y CIR 40%:

$$\text{CIR} = 40\% \times 4\ \text{Mbps} = 1.6\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 4\ \text{Mbps} = 4\ \text{Mbps}$$

Velocidad de subida = 4 Mbps, con PIR 100% y CIR 40%:

$$\text{CIR} = 40\% \times 4\ \text{Mbps} = 1.6\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 4\ \text{Mbps} = 4\ \text{Mbps}$$

Internet (Simetría 4:1)

Velocidad de bajada = 4 Mbps, con PIR 100% y CIR 40%:

$$\text{CIR} = 40\% \times 4\ \text{Mbps} = 1.6\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 4\ \text{Mbps} = 4\ \text{Mbps}$$

Velocidad de subida = 1/4 de 4 Mbps, con PIR 100% y CIR 40%:

$$\text{BW} = \frac{4\ \text{Mbps}}{4} = 1\ \text{Mbps}$$

$$\text{CIR} = 40\% \times 1\ \text{Mbps} = 0.4\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 1\ \text{Mbps} = 1\ \text{Mbps}$$

- **Cálculo de anchos de banda para el plan de 8 Mbps**

Intranet (Simetría 1:1)

Velocidad de bajada = 8 Mbps, con PIR 100% y CIR 40%:

$$\text{CIR} = 40\% \times 8\ \text{Mbps} = 3.2\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 8\ \text{Mbps} = 8\ \text{Mbps}$$

Velocidad de subida = 8 Mbps, con PIR 100% y CIR 40%:

$$\text{CIR} = 40\% \times 8\ \text{Mbps} = 3.2\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 8\ \text{Mbps} = 8\ \text{Mbps}$$

Internet (Simetría 4:1)

Velocidad de bajada = 8 Mbps, con PIR 100% y CIR 40%:

$$\text{CIR} = 40\% \times 8\ \text{Mbps} = 3.2\ \text{Mbps}$$

$$\text{PIR} = 100\% \times 8\ \text{Mbps} = 8\ \text{Mbps}$$

Velocidad de subida = 1/4 de 8 Mbps, con PIR 100% y CIR 40%:

$$\mathrm{BW} = \frac{8\ \mathrm{Mbps}}{4} = 2\ \mathrm{Mbps}$$

$$\mathrm{CIR} = 40\% \times 2\ \mathrm{Mbps} = 0.8\ \mathrm{Mbps}$$

$$\mathrm{PIR} = 100\% \times 2\ \mathrm{Mbps} = 2\ \mathrm{Mbps}$$

La siguiente tabla resume los valores calculados para los planes de internet e intranet considerados.

Tabla 4

Planes de navegación de internet e intranet

	Internet				**Intranet**			
	Bajada		**Subida**		**Bajada**		**Subida**	
	PIR	**CIR**	**PIR**	**PIR**	**CIR**	**CIR**	**PIR**	**CIR**
Plan 2 Mbps	2 Mbps	0.8 Mbps	0.5 Mbps	0.2 Mbps	2 Mbps	0.8 Mbps	2 Mbps	0.8 Mbps
Plan 4 Mbps	4 Mbps	1.6 Mbps	1 Mbps	0.4 Mbps	4 Mbps	1.6 Mbps	4 Mbps	1.6 Mbps
Plan 8 Mbps	8 Mbps	3.2 Mbps	2 Mbps	0.8 Mbps	8 Mbps	3.2 Mbps	8 Mbps	3.2 Mbps

3.3 Pruebas de funcionamiento del BNG en la red regional de acceso

A continuación, se muestran los resultados obtenidos luego de la configuración de los túneles, servicios VPN y el *Subscriber Management* en el enrutador BNG.

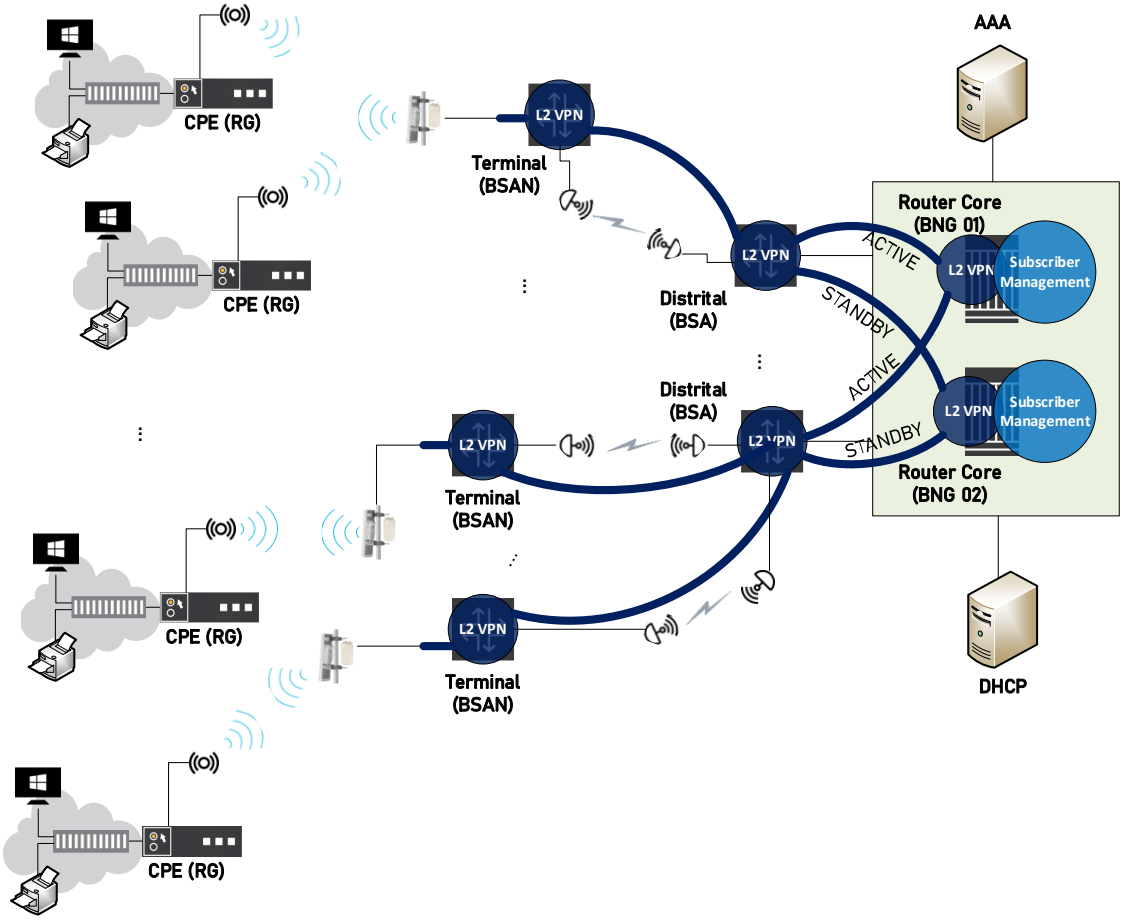
3.3.1 Pruebas de funcionamiento de BNG

Se crearon los servicios de L2 VPN en los clústeres desde los enrutadores terminales e intermedios hasta el enrutador distrital en una topología *Hub and Spoke*. Desde el distrital, se continúa el servicio L2 VPN añadiendo PW *Redundancy* hasta los enrutadores de *core* de la red de acceso (CR1 y CR2), siendo el túnel al enrutador de *core* de acceso 1 (CR1) el activo y el túnel al enrutador de *core* de acceso 2 (CR2) en espera (pasando al estado activo cuando el enrutador de *core* acceso 1 presente una falla).

En la siguiente figura se resume la topología lógica de la red de acceso con la estructura de servicios L2 VPN implementada.

Figura 22

BNG en la red de acceso región Puno



Nota: en el diagrama se ha omitido los equipos intermedios. Los CPE están situados en las IIEE de cada localidad, los círculos azules representan el servicio L2 VPN, las líneas azules los túneles MPLS y el circulo celeste la funcionalidad de 'Gestor de Suscriptores' (*Subscriber Management*) que realiza el BNG.

Como resultado, cuando un CPE inicia su proceso de encendido y origina paquetes DHCP, estos paquetes son recibidos en el CR1 a través del servicio L2 VPN, donde se ha establecido una asociación con el *Subscriber Management*, como se muestra en la figura 22. El mensaje DHCP enviado por el CPE es recibido en el CR1 y dispara un mensaje *RADIUS* al Servidor AAA para llevar a cabo su autenticación. Si el equipo se encuentra autorizado el CR1, permite al CPE el uso de los recursos de ancho de banda para Internet e Intranet y se comunica con la funcionalidad de Servidor DHCP para la asignación de una IP del pool asignado (10.0.32.0/22). A continuación, se muestra un registro de los mensajes intercambiados entre el enrutador BNG, el servidor AAA y la funcionalidad de servidor DHCP.

Figura 23

Registro de mensajes intercambiados desde el BNG

```
1 EL ENRUTADOR DE CORE SE COMUNICA CON EL SERVIDOR AAA PARA AUTENTICAR AL CPE

"RADIUS: Transmit
  Access-Request(1) 10.254.151.2:1812 id 1 len 165 vrid 2 pol AAA-OROCOM
    USER NAME [1] 17 e8:93:63:06:68:f8
    PASSWORD [2] 16 wlzPjV/1IJrZq6u5Pud6Gk
    NAS IP ADDRESS [4] 4 10.254.134.66
    NAS PORT ID [87] 11 pw-1101:200
    NAS IDENTIFIER [32] 11 PA-A-0001-NC-N-N05-01
    VSA [26] 105 Nokia(6527)
      CHADDR [27] 17 e8:93:63:06:68:f8
      DHCP VENDOR CLASS ID [36] 28 Nuage Networks|7850 NSG-C601
      TO-SERVER DHCP OPTIONS [102] 54
        Message type [53] 1 discover
        End [255]
"

2 EL SERVER AAA RESPONDE LA VERIFICACIÓN, Y COMPARTE LA AUTORIZACIÓN QUE TIENE PERMITIDO

"RADIUS: Receive
  Access-Accept(2) id 213 len 107 from 10.254.134.75:1812 vrid 3 pol AAA-OROCOM
    NAS IDENTIFIER [32] 13 10.254.134.65
    VSA [26] 19 Nokia(6527)
      CHADDR [27] 17 e8:93:63:06:05:f8
    VSA [26] 11 Nokia(6527)
      SUBSC ID STR [11] 9 Educacion_ESM
    VSA [26] 9 Nokia(6527)
      SUBSC PROF STR [12] 7 IIBB_8Mbps
    VSA [26] 9 Nokia(6527)
      SLA PROF STR [13] 7 IIBB_8Mbps
"

3 SE DISPARA LA ASIGNACIÓN DE IP AL SERVIDOR DHCP

"DHCP server:  DHCP-SERVER
Rx DHCP Discover

   ciaddr: 0.0.0.0           yiaddr: 0.0.0.0
   siaddr: 0.0.0.0           giaddr: 10.0.32.1
   chaddr: 00:50:79:66:68:09    xid: 0xa441741c

   DHCP options:
   [53] Message type: Discover
   [61] Client id: (hex) 01 00 50 79 66 68 09
   [255] End
"

4 EL SERVIDOR DHCP RESPONDE LA SOLICITUD Y OFRECE UNA IP

"DHCP server:  DHCP-SERVER
lease added for 10.0.32.5 state=offer
"

5 SE TRANSMITE LA OFERTA DE IP AL CPE

"DHCP server:  DHCP-SERVER
Tx DHCP Offer to relay agent at 10.0.32.1 vrId=3

   ciaddr: 0.0.0.0           yiaddr: 10.0.32.5
   siaddr: 10.0.100.1        giaddr: 10.0.32.1
   chaddr: 00:50:79:66:68:09    xid: 0xa441741c

   DHCP options:
   [53] Message type: Offer
   [54] DHCP server addr: 10.0.100.1
   [51] Lease time: 3600
   [1] Subnet mask: 255.255.252.0
   [3] Router: 10.0.32.1
   [6] Domain name server: 8.8.8.8
   [255] End
"

6 EL CPE RESPONDE LA OFERTA Y SOLICITA USAR LA IP OFRECIDA

"DHCP server:  DHCP-SERVER
Rx DHCP Request
```

```
   ciaddr: 10.0.32.5    yiaddr: 0.0.0.0
   siaddr: 0.0.0.0          giaddr: 10.0.32.1
   chaddr: 00:50:79:66:68:09    xid: 0xa441741c

   DHCP options:
   [53] Message type: Request
   [54] DHCP server addr: 10.0.100.1
   [50] Requested IP addr: 10.0.32.5
   [61] Client id: (hex) 01 00 50 79 66 68 09
   [55] Param request list: len = 4
             1  Subnet mask
             3  Router
             6  Domain name server
            15  Domain name
   [255] End
"
```

7 EL SERVIDOR DHCP ASIGNA LA IP SOLICITADA

```
"DHCP server:  DHCP-SERVER
lease update for 10.0.32.5 state=stable
"
```

8 EL SERVIDOR DHCP ENVÍA UN MENSAJE ACK CONFIRMANDO LA ASIGNACIÓN

```
"DHCP server:  DHCP-SERVER
Tx DHCP Ack to relay agent at 10.0.32.1 vrId=3

   ciaddr: 10.0.32.5    yiaddr: 10.0.32.5
   siaddr: 10.0.100.1        giaddr: 10.0.32.1
   chaddr: 00:50:79:66:68:09    xid: 0xa441741c

   DHCP options:
   [53] Message type: Ack
   [54] DHCP server addr: 10.0.100.1
   [51] Lease time: 3600
   [1] Subnet mask: 255.255.255.240
   [3] Router: 10.0.32.1
   [6] Domain name server: 8.8.8.8
   [255] End

"
```

9 EN EL CORE DE ACCESO SE ESTABLECE LA ASOCIACIÓN DEL SUSCRIPTOR

```
A:PU-A-0001-NC-N-N05-01# show service id 80 subscriber-hosts mac e8:93:63:06:68:f8 detail

===============================================================================
Subscriber Host table
===============================================================================
Sap
  IP Address
    MAC Address                PPPoE-SID       Origin          Fwding State
      Subscriber
-------------------------------------------------------------------------------
[pw-1091:200]
  10.0.32.5 ------------------------------------------------------------------> IP Asignada
    e8:93:63:06:68:f8          N/A             DHCP            Fwding
      Educacion_E8:93:63:06:68:F8 ----------------------------------------> Nombre del CPE
-------------------------------------------------------------------------------
Subscriber-interface  : NUAGE-IIBB
Group-interface       : pw-1091-acora ---------------------------------------> Localidad
Sub Profile           : IIBB_8Mbps
SLA Profile           : IIBB_8Mbps ------------------------------------------> Plan Asignado
App Profile           : N/A
Egress Q-Group        : N/A
Egress Vport          : N/A
Acct-Session-Id       : A10F1B001E71E765F09C6C
Acct-Q-Inst-Session-Id: A10F1B001E71E865F09C6C
Address Origin        : Dynamic
OT HTTP Rdr IP-FltrId : N/A
OT HTTP Rdr Status    : N/A
OT HTTP Rdr Fltr Src  : N/A
HTTP Rdr URL Override : N/A
GTP local break-out   : No
DIAMETER session ID Gx: N/A
-------------------------------------------------------------------------------
Number of subscriber hosts : 1
===============================================================================
```

10 VALIDACIÓN DE LA CONECTIVIDAD DESDE EL CORE DE ACCESO CON LA IP ASIGNADA AL CPE

```
A:PU-A-0001-NC-N-N05-01# ping router 80 10.0.32.5
PING 10.0.32.5 56 data bytes
```

```
64 bytes from 10.0.32.5: icmp_seq=1 ttl=64 time=12.3ms.
64 bytes from 10.0.32.5: icmp_seq=2 ttl=64 time=12.4ms.
64 bytes from 10.0.32.5: icmp_seq=3 ttl=64 time=9.86ms.
64 bytes from 10.0.32.5: icmp_seq=4 ttl=64 time=12.4ms.
64 bytes from 10.0.32.5: icmp_seq=5 ttl=64 time=9.88ms.

---- 10.0.32.5 PING Statistics ----
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min = 9.86ms, avg = 11.4ms, max = 12.4ms, stddev = 1.21ms
A:PU-A-0001-NC-N-N05-01#
```

Nota: en el registro se ha omitido información irrelevante para un mejor entendimiento.

El resultado se puede resumir en la siguiente tabla:

Tabla 5

Pasos para la asignación de una IP a un CPE

N° Paso	Suceso	Mensaje resumido
1	El enrutador de *core* se comunica con el servidor AAA para autenticar al CPE	USER NAME [1] 17 e8:93:63:06:68:f8 PASSWORD [2] 16 wlzPjV/1IJrZq6u5Pud6Gk
2	El Server AAA responde la verificación, y comparte la autorización que tiene permitido	SUBSC ID STR [11] 9 Educacion_ESM SUBSC PROF STR [12] 7 IIBB_8Mbps SLA PROF STR [13] 7 IIBB_8Mbps
3	Se dispara la asignación de IP al servidor DHCP	Message type: Discover
4	El servidor DHCP responde la solicitud y ofrece una IP	Lease added for 10.0.32.5 state=offer
5	Se transmite la oferta de IP al CPE	Message type: Offer
6	El CPE responde la oferta y solicita usar la IP ofrecida	Message type: Request Requested IP addr: 10.0.32.5
7	El servidor DHCP asigna la IP solicitada	Lease update for 10.0.32.5 state=stable
8	El servidor DHCP envía un mensaje ACK confirmando la asignación	Message type: Ack
9	En el core de acceso se establece la asociación del suscriptor	10.0.32.5, Educacion_E8:93:63:06:68:F8 Group-interface : pw-1091-acora Sub Profile : IIBB_8Mbps SLA Profile : IIBB_8Mbps
10	Validación de la conectividad desde el Core de Acceso con la IP asignada al CPE	5 packets transmitted, 5 packets received, 0.00% packet loss

Una vez el CPE obtiene la IP de WAN puede establecer comunicación con su plataforma SDN para recibir la configuración automática del sitio, la cual incluye el direccionamiento LAN asignado para los usuarios y el establecimiento de un túnel VXLAN

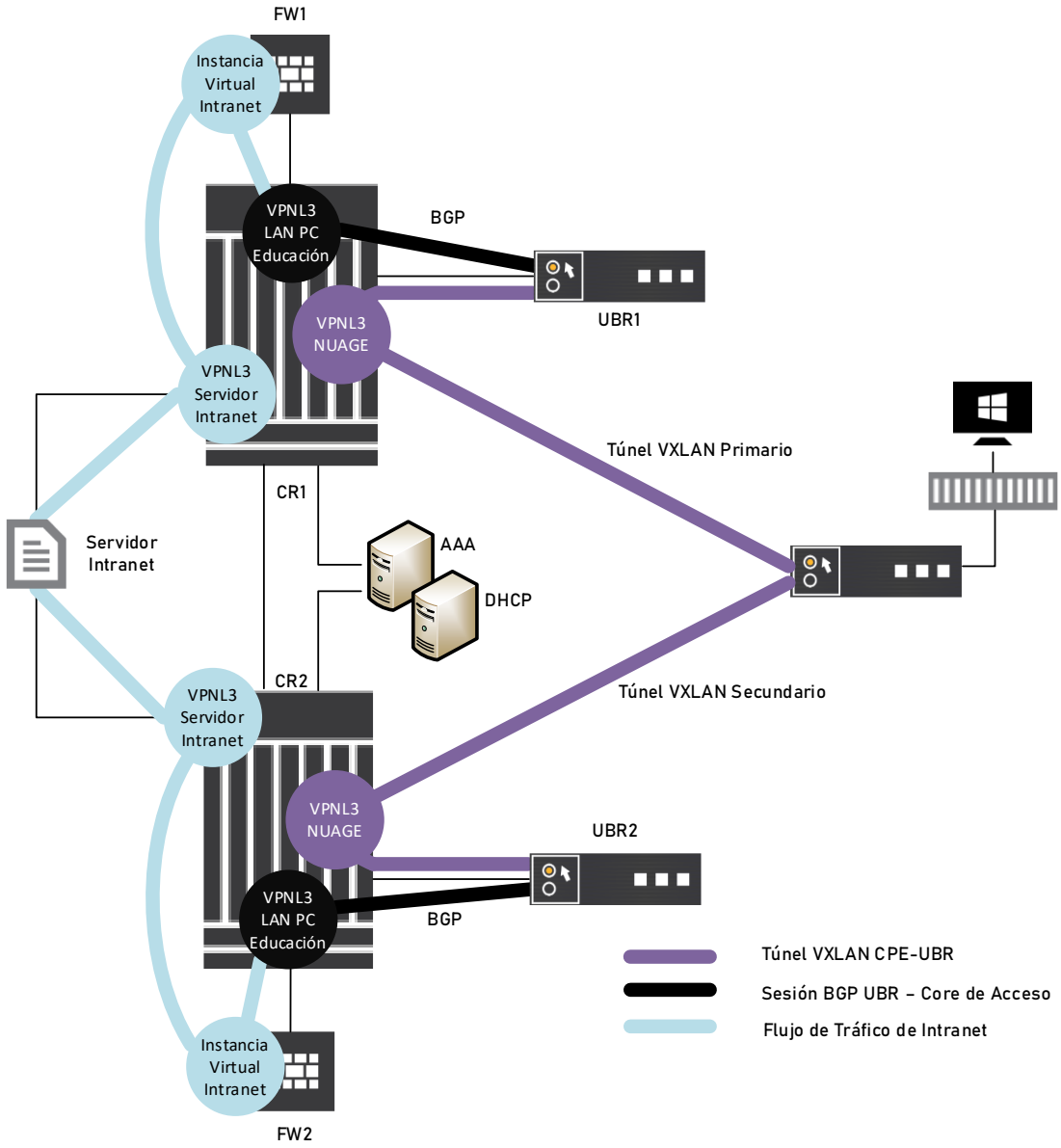
con el *Underlay Border Router* (UBR). La asignación de IP para los dispositivos de los usuarios finales dentro de la institución educativa se realiza de forma dinámica siendo el CPE como servidor DHCP y puerta de enlace.

Posteriormente, los paquetes del tráfico de usuario son encapsulados por el CPE en un túnel VXLAN y enviados hacia el UBR. Los datos nuevamente son encapsulados en el enrutador terminal con destino el enrutador distrital. Este los reenvía hacia el enrutador de *core* de acceso 1 (CR1), donde son desencapsulados de MPLS y reenviados al UBR, que lo desencapsulará de VXLAN, se los reenviará al CR1 mediante una sesión BGP IPv4 y serán recibidos en un servicio L3 VPN con nombre 'LAN PC Educación' como se muestra en la figura 24. Sobre esta sesión BGP, el UBR envía las subredes privadas de los usuarios de los todos los CPE y a su vez el CR1 envía una ruta *default* (0.0.0.0/0), que luego será distribuida a los CPE.

En caso los usuarios requieran alcanzar al servidor de Intranet, el servicio L3 VPN 'LAN PC Educación' enrutará los datos hacia una interfaz de una *Virtual Domain* (VDOM) llamada "Intranet" en el *Firewall*, la cual luego de aplicar los filtros necesarios enruta los datos a un servicio L3 VPN aislada llamada 'Servidores de Intranet' dando así seguridad al servidor.

Figura 24

Diagrama de flujos de datos a intranet

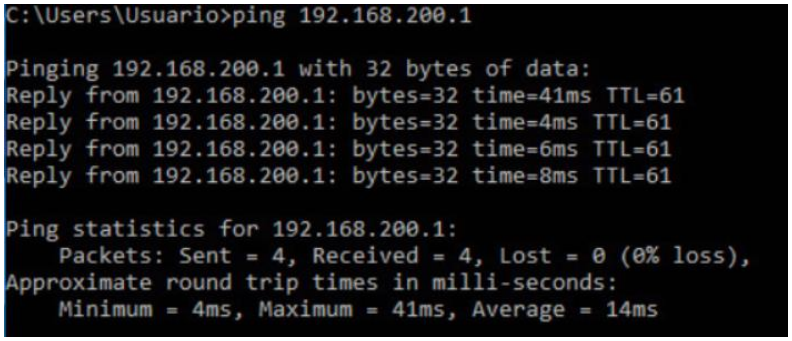


Nota: el túnel VXLAN entre el CPE y el UBR es enrutado a través del enrutador de Core de la Red de Acceso. La L3 VPN "LAN PC Educación" está representada con el círculo negro y la L3 VPN "Servidor Intranet" es representada como el círculo celeste, al igual que la VDOM Intranet en el FW.

En resumen, los datos del usuario pasarán a través de dos túneles, terminan, finalmente, sin encapsular en un servicio L3 VPN. Luego serán filtrados por el *Firewall* para llegar al Servidor Intranet (192.168.200.1), que se encuentra en otro servicio L3 VPN. A continuación, se muestra la conectividad final al servidor desde un dispositivo conectado en una institución educativa.

Figura 25

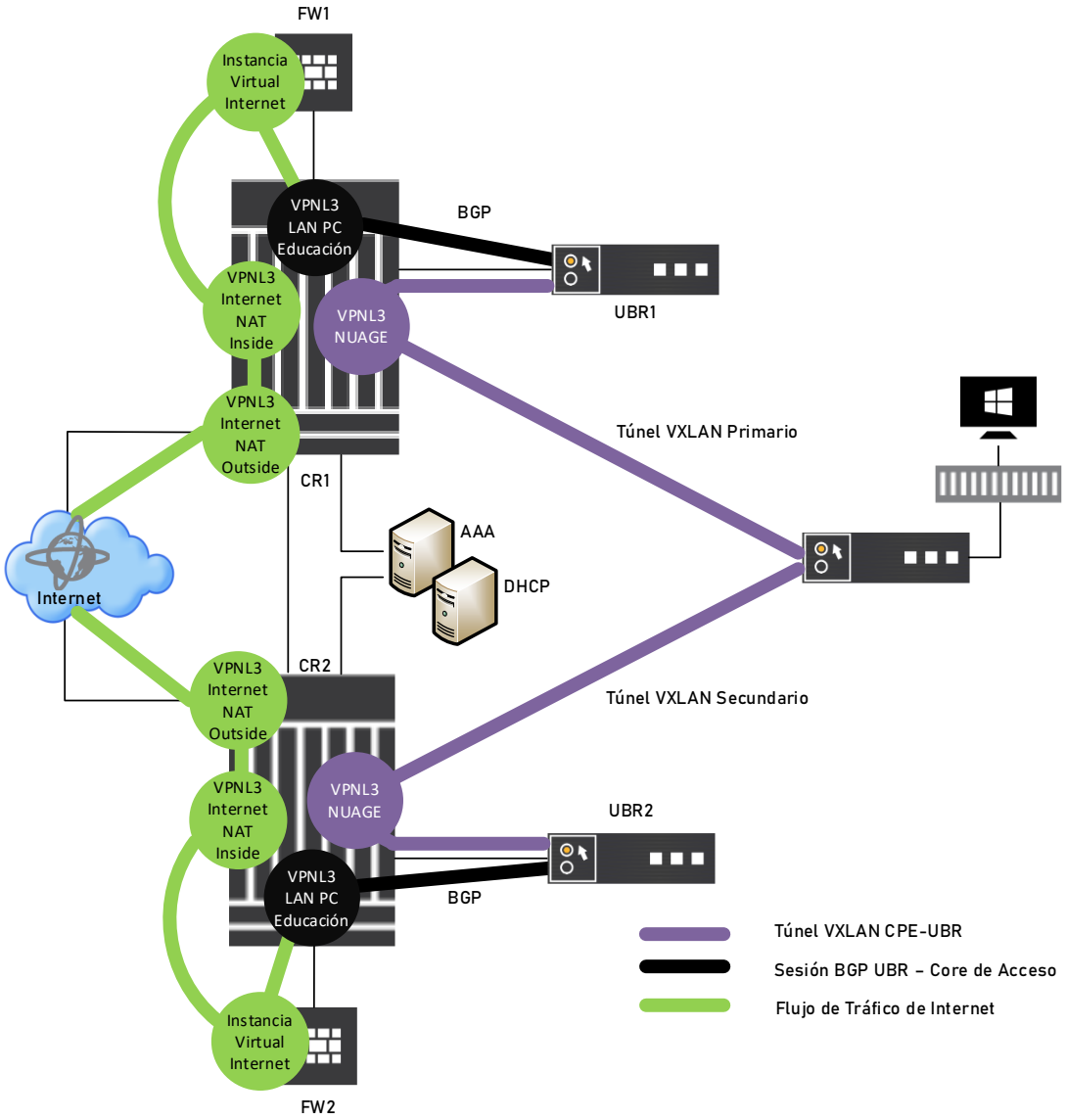
Conectividad a intranet



Por otro lado, en caso el tráfico de datos sea hacia Internet, el camino desde el CPE hasta el servicio L3 VPN ‘LAN PC Educación’ será el mismo. La diferencia es que luego se enrutará los datos hacia una interfaz de otra *Virtual Domain* (VDOM) llamada "Internet" en el *Firewall.* La cual, luego de aplicar los filtros necesarios, enruta los datos a un servicio L3 VPN denominado "NAT Inside" como se observa en la figura 26, que mediante un proceso interno se encarga de la traducción de IP privadas a públicas y de pasar el tráfico traducido a un nuevo servicio L3 VPN llamada *NAT Outside*. Este servicio L3 VPN "NAT Outside" se conecta con el ISP mediante BGP para la salida a internet.

Figura 26

Diagrama de flujo de datos a internet

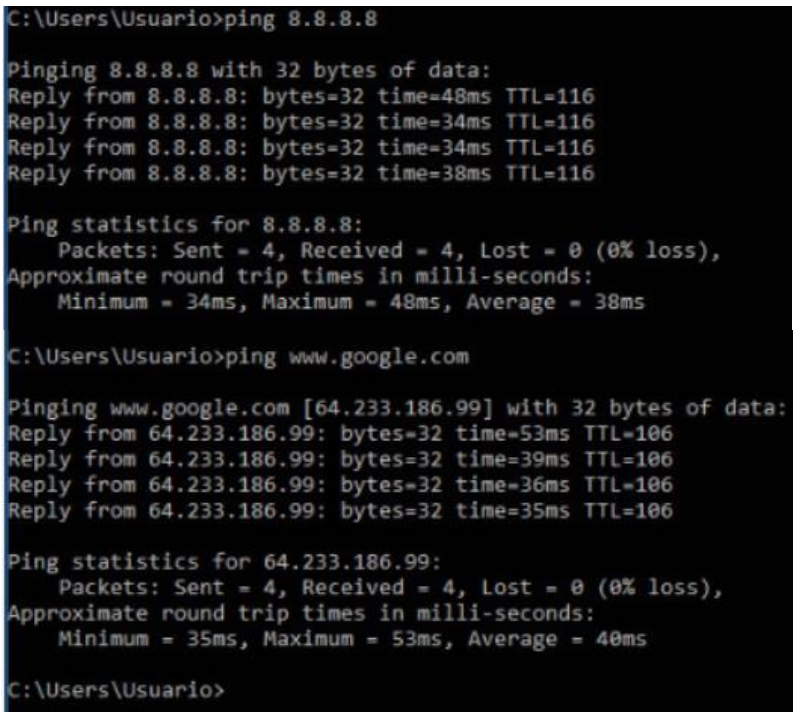


Nota: en la figura muestra los flujos seguidos dependiendo el tipo de tráfico (internet o intranet) a su vez la conexión con el ISP de la región y cómo ingresa el flujo de los usuarios en la L3 VPN por la sesión BGP.

En resumen, los datos del usuario pasarán a través de dos túneles, terminan, finalmente, sin encapsular en un servicio L3 VPN: Luego serán filtrados por el *Firewall* para llegar al servicio de NAT, que se encuentra en otro servicio L3 VPN. A continuación, se muestra la conectividad final a Internet.

Figura 27

Conectividad a internet

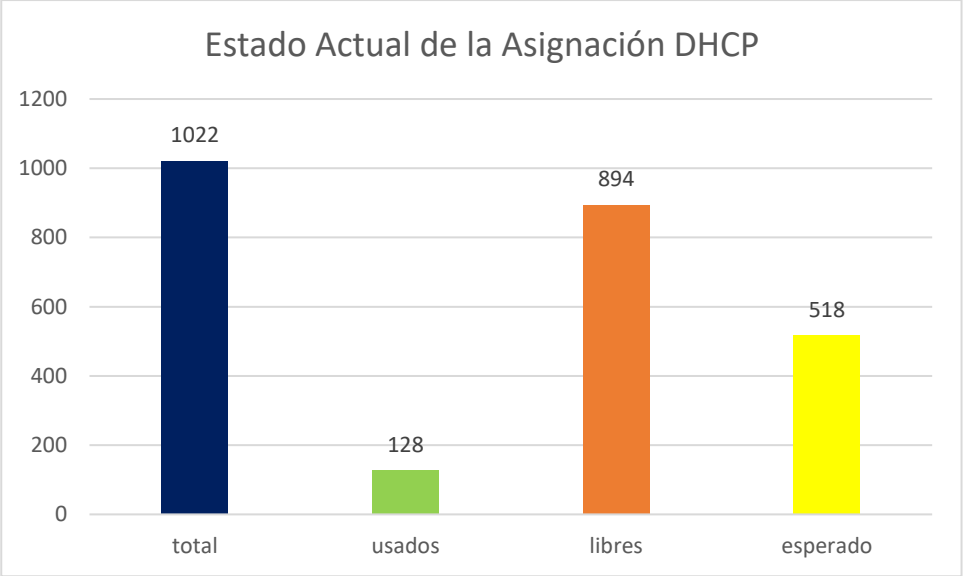


3.3.2 Asignación de la dirección IP a los CPE

El segmento 10.0.32.0/22 asignado para los CPE es usado en ambos CR como un pool de direcciones para DHCP, prefiriendo al CR1; es decir, ambos pueden soportar la totalidad de los suscriptores en caso de una caída de uno de los enrutadores del *core* de acceso. Como se observa en la figura 28, se tienen 128 CPE activos (barra verde) lo cual representa un 24.71% de los 518 (barra amarilla) por ser desplegados. También se puede apreciar que la cantidad de IP disponibles es 894 (barra naranja) siendo un 87.47% del total (barra azul) de IP del pool.

Figura 28

Asignación de IP por DHCP para CPE

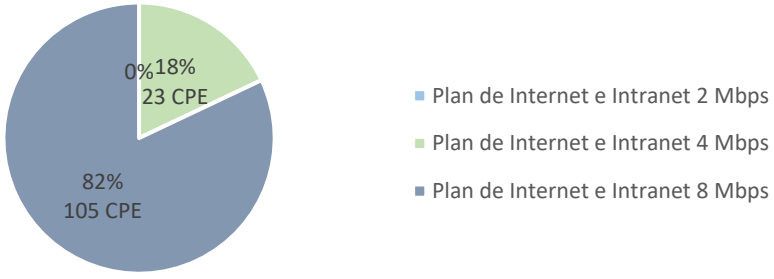


Nota: actualmente se continúa desplegando los CPE en las Instituciones Educativas, al momento de la elaboración se encuentran 128 CPE autenticados en la red.

Considerando esta cantidad de CPE, en la figura 29 se muestra la distribución de planes asignados (2 Mbps, 4 Mbps y 8 Mbps). Se observa que 105 correspondiente al 82% del total de CPE activos tiene un plan de 8 Mbps, mientras que el 18% restante tiene un plan de 4 Mbps. Por tanto, cada uno de los CPE ha recibido uno de los planes establecidos:

Figura 29

Asignación de planes de internet e intranet



En resumen, los dispositivos CPE se vienen autenticando y obteniendo el plan de navegación y una IP por DHCP que utilizarán para la creación de túneles VXLAN y transportar así los datos encapsulados de la institución educativa.

Tabla 6

Asignación y ocupación de planes

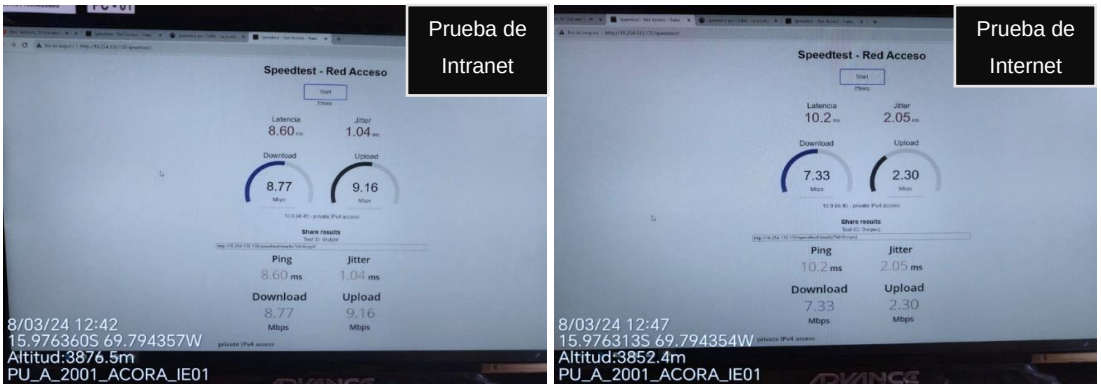
Cantidad asignada	Plan de 8 Mbps	Plan de 4 Mbps
128	105	23

3.3.3 Prueba de ancho de banda de internet e intranet

Luego de la asignación del plan de navegación y de la asignación de IP a los dispositivos de los usuarios finales, estos pueden acceder a la L3 VPN 'Servidores Intranet'. Y también salir a Internet, luego de pasar por el proceso de NAT en el enrutador de *core* de acceso. Se realizó la prueba de velocidad de navegación para verificar el ancho de banda del plan de 8 Mbps. En la figura 30, se muestra el resultado, la primera imagen es el resultado de la prueba de velocidad de intranet de una institución educativa en la localidad de Acora. La segunda imagen es el resultado de la prueba de velocidad de internet en la misma institución.

Figura 30

Prueba de velocidad del plan de 8 Mbps en la localidad de Acora



Nota: en la imagen de la arriba se aprecia la prueba de velocidad de internet y en la de abajo la prueba de velocidad para intranet.

El resumen de los resultados obtenidos para la prueba de internet e intranet para el plan de navegación de 8 Mbps en la institución educativa de Acora se muestra en la siguiente tabla:

Tabla 7

Resultados de las pruebas de velocidad a 8 Mbps

Prueba	Velocidad teórica	Velocidad obtenida
Internet Bajada	8 Mbps	7.33 Mbps
Internet Subida	2 Mbps	2.3 Mbps
Intranet Bajada	8 Mbps	8.77 Mbps
Intranet Subida	8 Mbps	9.16 Mbps

Capítulo IV. Análisis y discusión de resultados

4.1 Análisis y discusión de funcionamiento del BNG en la red regional de acceso

Según lo descrito en la sección 3.3.1, el proceso para la asignación de IP y de plan de navegación se inicia desde que el CPE envía un mensaje DHCP para solicitar una IP. Este proceso se realiza según la tabla 5. El siguiente paso es que el enrutador de *core* de la red de acceso se comunique con el servidor AAA para verificar los permisos que tiene el CPE. Si el CPE tiene permitido usar los recursos de la red el enrutador de *core* de la red de acceso, disparará la asignación de IP mediante un DHCP *Relay*. El servidor DHCP comenzará el proceso completo para la asignación de IP. Cuando el CPE tiene la IP asignada, el enrutador del *core* de la red de acceso guarda esta asociación en su base de datos de suscriptores, al igual que la asignación de la IP al CPE.

De esta forma se logra y valida el funcionamiento del BNG. Los demás dispositivos CPE seguirán el mismo proceso para obtener una IP y los permisos de utilización de ancho de banda (plan de navegación).

Por otro, lado ambos enrutadores del *core* de la red de acceso funcionan en forma redundante. La base de datos de suscriptores y asignación de IP por DHCP son guardadas en ambos enrutadores. Además, los túneles al proceso de BNG son redundantes como se muestra en la figura 24. De esta manera, ante una pérdida de conectividad con uno de los enrutadores, el otro tomará su lugar.

4.2 Análisis y discusión de la asignación de las direcciones IP a los CPE

Según lo descrito en la sección 3.3.2, en el momento de la redacción del presente documento, se encontraban 128 CPE conectados. De estos, todos fueron asignados por el DHCP ubicado dentro del enrutador del *core* de acceso 1 (CR1). Esto se debe a que actualmente el proceso de DHCP *server* está ubicado directamente en el enrutador activo (CR1) y está siendo escogido como el preferido por el CPE.

Según la tabla 6, 105 de la cantidad actual de CPE conectados está siendo autenticada y autorizada para navegar con el plan de internet e intranet de 8 Mbps. Los otros 23 están utilizando un plan de 4 Mbps. La asignación del plan depende de la configuración realizada en el AAA y esto depende de la configuración del proveedor de servicios, en este caso la empresa adjudicada.

Además, se puede observar que la cantidad de IP total del pool es de 1022. Esto sobrepasa la cantidad total de direcciones que serán asignadas (518), lo cual permite un futuro crecimiento de la cantidad de CPE (504).

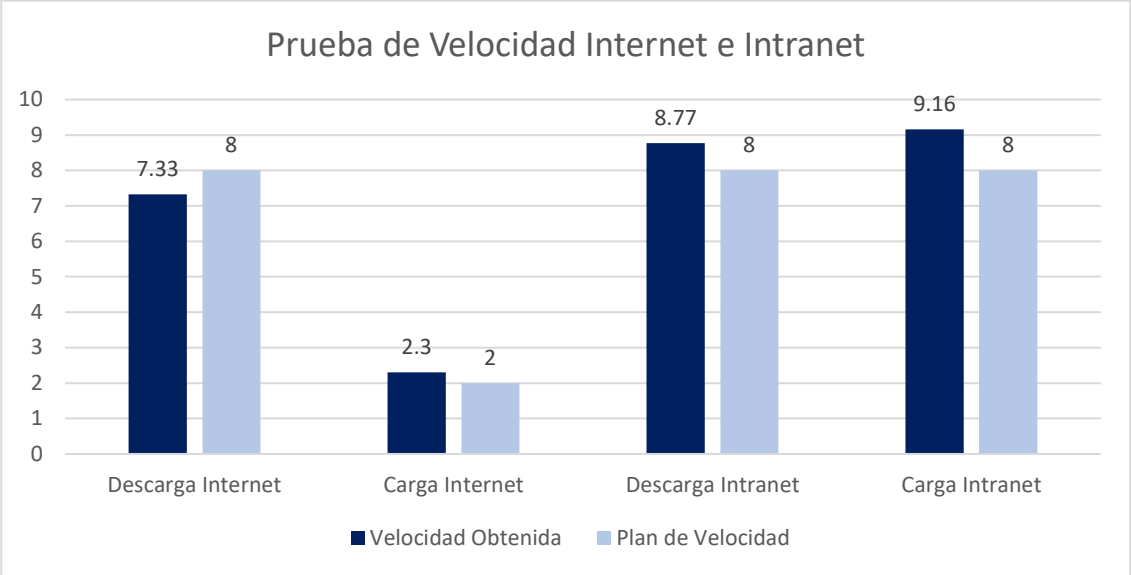
4.3 Análisis y discusión de la prueba de ancho de banda de internet e intranet

Como muestra la tabla 7, los valores de velocidad obtenidos para internet e intranet están dentro de los valores esperados. Comienza con la velocidad de bajada de internet. La velocidad de 7.33 Mbps supera el CIR de 3.2 Mbps mostrado en la tabla 4 y representa el 91.6% del PIR (8 Mbps). Esto puede suceder en ocasiones cuando el medio está saturado al tener tráficos simultáneos de otros CPE, lo que hace que no todos los suscriptores lleguen a la tasa pico (PIR). Por eso, el valor de CIR, que representa la tasa comprometida al suscriptor, suele ser el indicador en caso de alguna saturación, mostrando en este caso un resultado favorable.

En el caso de la velocidad para la carga en internet, se obtuvo 2.3 Mbps de los 2 Mbps esperado; pues, en la configuración de los valores en las políticas de calidad de servicio, el proveedor se suele colocar un pequeño margen de guarda para que el cliente obtenga una mejor experiencia y, siempre y cuando la red tenga los recursos disponibles, el suscriptor pueda usarlo.

Figura 31

Resumen de las pruebas de velocidad del plan de 8 Mbps



Como se muestra en la figura 31, en las pruebas de velocidad de subida y bajada de intranet se observa lo descrito anteriormente, donde las velocidades fueron configuradas con un pequeño margen (1.5Mbps) para obtener una mejor experiencia en el uso del plan. En este caso es más notorio; ya que ambos llegan al PIR esperado y un poco más. Esto también puede deberse a que, a diferencia de internet, para intranet los recursos están dentro de la propia red de acceso y no requieren un arrendamiento al ISP.

Estos resultados reflejan que, las mediciones obtenidas cumplen satisfactoriamente con los valores contratados bajo el marco normativo vigente en 2017. Sin embargo, los parámetros alcanzados quedarían por debajo de los umbrales exigidos actualmente para calificar un servicio como banda ancha, según la normativa del MTC y Osiptel. De acuerdo con los estándares actuales, se requeriría garantizar una mayor velocidad efectiva y una mejor simetría en las velocidades de transmisión. Por tanto, los resultados permiten validar el cumplimiento técnico dentro del marco contractual, pero también ponen de manifiesto la brecha existente con respecto a los estándares modernos de calidad y la necesidad de considerar futuros procesos de adecuación del servicio.

Conclusiones

1. Se logró implementar una red para proveer del servicio de internet e intranet para 581 instituciones educativas de la región Puno.
2. Se consiguió la asignación de 128 IP para los CPE de las instituciones educativas y se tiene el suficiente direccionamiento para poder abastecer a los 581 CPE con un margen de crecimiento para 504 CPE adicionales.
3. La asignación del plan de navegación y de la IP de servicio para el CPE depende de la configuración del servidor AAA y del servidor DHCP, administrados por el proveedor de servicios y resulta en una forma escalable para poder atender más suscriptores.
4. Se obtuvo los valores esperados para el plan de navegación de internet e intranet, llegó, en todos los casos, a valores por encima de la tasa comprometida (CIR).
5. El proveedor de servicio suele aumentar en una pequeña cantidad el PIR para que el cliente experimente dentro de lo posible la tasa máxima (PIR) y en todos los casos llegar a la comprometida (CIR)
6. El análisis realizado ha permitido confirmar que el sistema propuesto cumple con los requerimientos técnicos establecidos. Sin bien los estándares actuales son más exigentes, es posible alinearlos manteniendo la solución técnica brindada.

Recomendaciones

1. Dentro de los clústeres en la red de acceso, se recomienda la conexión física con otro enrutador de la red de transporte; pues, como se muestra en la figura 5, ante una caída del enlace distrital-distribuidor ocasionaría un aislamiento del clúster que afectará a todas las instituciones educativas que pasen por dicho tramo.
2. Dentro del *core* de la red de acceso, se recomienda contar con un respaldo del proveedor de internet (ISP) de la región, pues, como se observa en la figura 22, en la actualidad en caso de falla la red de acceso se podría quedar sin acceso a internet.
3. Se recomienda actualizar y aumentar la capacidad de los planes de navegación de los servicios de internet e intranet. Esto porque la demanda de datos, en la actualidad, está en crecimiento y el proveedor requerirá suplir dichas necesidades. Esto se puede notar ya que, como se muestra en la figura 29, el plan de 2 Mbps actualmente no está siendo utilizado.
4. Se recomienda añadir servidores DHCP exclusivos para la asignación de direcciones dinámicas a los CPE. Esto permitirá una mayor escalabilidad; además de aislar las funcionalidades de la red de acceso permite una mejor administración.
5. En la actualidad, por las pocas conexiones dentro de los clústeres de la red de acceso, el uso de LDP es suficiente; sin embargo, se recomienda que, en un futuro, con el aumento de interconexiones dentro del clúster, se implemente RSVP-TE para añadir mecanismos de mejora para recuperación de caminos como *Fast Reroute*, o implementar *Segment Routing* con *Loop Free Alternate*.
6. Se recomienda realizar un análisis técnico y económico que permita evaluar la actualización gradual del servicio de internet hacia los estándares actuales de banda ancha definidos por el MTC y Osiptel. Esta adecuación permitiría al sistema cumplir con la normativa vigente y mejorar la calidad del servicio brindado a las instituciones educativas.

Referencias bibliográficas

Auris Huamán, A. M. (2020). *Instalación de internet de banda ancha para la conectividad integral y desarrollo social de la región Cajamarca.* Repositorio Institucional de la Universidad Nacional de Ingeniería. http://hdl.handle.net/20.500.14076/21125

Bookham, C. (2014). *Versatile Routing and Services with BGP.* Wiley Publisher.

Campos Barrientos, M. A. (2020). *Diseño de una red de telecomunicaciones para brindar el servicio de acceso a internet como factor de desarrollo social y económica de la región Pasco.* Repositorio Institucional de la Universidad Nacional de Ingeniería http://hdl.handle.net/20.500.14076/22357

Chan E. (3 de Marzo de 2024). *Chan's Blog* VXLAN & Logical Switch Deployment. https://chansblog.com/tag/vxlan/

Cisco. (2020). *Broadband Network Gateway Configuration Guide for Cisco ASR 9000 Series Routers.* https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-3/bng/configuration/guide/b-bng-cg-asr9000-73x.pdf

Cisco. (2010). I*ntroduction to Dynamic Routing Protocol: Routing Protocols and Concepts*. https://slideplayer.com/slide/12873432/

Cisco. (2021). *Broadband Network Gateway Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.3.x.* https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-3/bng/configuration/guide/b-bng-cg-asr9000-73x.pdf

Congreso de la República. (2012). *Ley Nº 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica*. https://www.leyes.congreso.gob.pe/Documentos/Leyes/29904.pdf

Congreso de la República. (2021). *Ley Nº 31207, Ley que garantiza la velocidad mínima de conexión a internet y monitoreo de la prestación del servicio de internet a favor de los usuarios. https://leyes.congreso.gob.pe/Documentos/2016_2021/ADLP/Normas_Legales/31207-LEY.pdf*

Glenn Warnock, A. N. (2011a). Capítulo 19 VPLS. *Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide. (p.2)*. Wiley Publishing.

Glenn Warnock, A. N. (2011b). Capítulo 20 VPRN. *Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide. (p.8)*. Wiley Publishing.

Huawei. (2023). *What is Broadband Network Gateway?* https://forum.huawei.com/enterprise/en/What-is-Broadband-Network-Gateway/thread/700171314049990656-667213852955258880

INEI. (2017). *Censos 2017: departamento de Puno tiene 1 172 697 habitantes*. https://m.inei.gob.pe/prensa/noticias/censos-2017-departamento-de-puno-tiene-1-172-697-habitantes-11059/

Internet Engineering Task Force. (1982). *RFC 827: Exterior Gateway Protocol (EGP).* IETF. https://datatracker.ietf.org/doc/html/rfc827

Internet Engineering Task Force. (1990). *RFC 1195: Use of OSI IS-IS for Routing in TCP/IP and Dual Environments.* IETF: https://www.rfc-editor.org/rfc/rfc1195

Internet Engineering Task Force. (1995). *RFC 1812: Requirements for IP Version 4 Routers*. IETF. https://datatracker.ietf.org/doc/html/rfc1812

Internet Engineering Task Force. (1997). *RFC 2131:* Dynamic Host Configuration Protocol. IETF. https://datatracker.ietf.org/doc/html/rfc2131

Internet Engineering Task Force. (2000). *RFC 2865: Remote Authentication Dial In User Service (RADIUS)*. IETF: https://www.rfc-editor.org/rfc/rfc2865

Internet Engineering Task Force. (2001a). *RFC 3031: Multiprotocol Label Switching Architecture.* IETF: https://www.rfc-editor.org/rfc/rfc3031

Internet Engineering Task Force. (2001b). *RFC 3107: Carrying Label Information in BGP-4*. IETF: https://www.rfc-editor.org/rfc/rfc3107.html

Internet Engineering Task Force. (2006). *RFC 4271: A Border Gateway Protocol 4 (BGP-4).* IETF: https://www.rfc-editor.org/rfc/rfc4271

Internet Engineering Task Force. (2007). *RFC 5036: LDP Specification*. IETF: https://www.rfc-editor.org/rfc/rfc5036

Internet Engineering Task Force. (2008). *RFC 5398: Autonomous System (AS) Number Reservation for Documentation Use*. IETF. https://datatracker.ietf.org/doc/html/rfc5398

Internet Engineering Task Force. (2012). *RFC 6793: BGP Support for Four-Octet Autonomous System (AS) Number Space*. IETF. https://datatracker.ietf.org/doc/html/rfc6793

Internet Engineering Task Force. (2013). *RFC 6996: Autonomous System (AS) Reservation for Private Use*. IETF. https://datatracker.ietf.org/doc/html/rfc6996

Internet Engineering Task Force. (2014). *RFC 7348: Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*. IETF: https://www.rfc-editor.org/rfc/rfc7348

Juniper. (2023). *Reference Architecture: Broadband Edge Network Design.* https://www.juniper.net/documentation/us/en/software/nce/broadband-edge-ref-arch/broadband-edge-ref-arch.pdf

Midis. (2023). *Reporte Regional de Indicadores Sociales del Departamento de Puno.* https://sdv.midis.gob.pe/redinforma/Upload/regional/Puno.pdf

Minedu. (2107). *Estadistica de la calidad educativa: Presentación del Proceso Censal 2017 - Puno.* https://escale.minedu.gob.pe/c/document_library/get_file?uuid=0fb29dac-09a9-4861-b226-94e0aab41eed&groupId=10156

Minedu. (2022). *Estadistica de la calidad educativa: EduDatos y Perfiles Educativos, Perfil Regional Puno 2022*. https://escale.minedu.gob.pe/perfil-regional

Monteros Montenegro, N. G. (2009). *Diseño de un sistema para la prestación de triple play basado en protocolo IP para el concesionario de audio y video por suscripción.* Repositorio Digital Institucional de la Escuela Politécnica Nacional. https://bibdigital.epn.edu.ec/handle/15000/1586

MTC. (2013). *Exposición de Motivos del Decreto Supremo N°014-2013-MTC.* https://www.gob.pe/institucion/mtc/normas-legales/9994-014-2013-mtc

MTC. (2022). *Resolución Ministerial N° 1197-2022-MTC/01.03*. https://cdn.www.gob.pe/uploads/document/file/3914959/RM%20N%C2%B0%201197-2022-MTC/01.03.pdf?v=1670380825

Nokia. (2016a). *Multiservice Integrated Service Adapter Guide, 7.3.1 Principles of NAT:* https://infocenter.nokia.com/public/7750SR140R4/topic/com.sr.msisa/html/nat.html?cp=10_6

Nokia. (2016b). Service Routing Certification: *"Triple Play Services"* Vol. 3.2.1

Nokia. (2021a). Service Routing Certification: *"Nokia Border Gateway Protocol Fundamentals for Services".* Vol. 1.0.

Nokia. (2021b). Service Routing Certification: *"Nokia Multiprotocol Label Switching"* Vol. 3.0.1.

Nokia. (2022a). Service Routing Certification: "*Nokia Services Arquitecture"*. Vol. 4.0

Nokia. (2022b). *Multiservice ISA and ESA Guide release 22.2.R1.* https://infocenter.nokia.com/public/7750SR222R1A/index.jsp?topic=%2Fcom.sr.msisa%2Fhtml%2Fnat.html&cp=17_6_2&anchor=i1084248

Nokia. (2023). *Nokia Broadband Network Gateway solution brochure.* https://onestore.nokia.com/asset/i/210284

Nokia. (2024a). *Nokia 7210 SAS*. https://onestore.nokia.com/asset/f/184551

Nokia. (2024b). *Nokia 7750 Service Router*. https://www.nokia.com/asset/164728/

Nuage Networks. (2020a). *Nuage Networks Virtuoso Training and Certification: "Virtualized Network Services (VNS) Fundamentals"*. Vol. 2.2.

Nuage Networks. (2020b). *7850 NSG-C600 Series*. https://www.nuagenetworks.net/wp-content/uploads/2020/06/Nuage_Networks_7850_NSG-C601_Data_Sheet_EN.pdf

Osiptel. (2024). *Resolución de Consejo directivo de Osiptel N° 00214-2024-CD/OSIPTEL*. https://www.osiptel.gob.pe/media/mbsnzoiu/resol214-2024-cd.pdf

Proinversión. (2017). *Anexo n° 8-b de las bases, especificaciones técnicas de la Red de Acceso.* https://www.investinperu.pe/RepositorioAPS0/0/2/JER/SC_BANDA_JUNIN_PUNO/Anexo_8_B_LPE_Junin_Puno_Moquegua_Tacna_16Set17.pdf

Sánchez, A. C. (2020). *Propuesta de implementación de Carrier-Grade NAT para Guifi.Net. Repositorio Institucional de la Univesidad Abierta de Cataluña.* https://openaccess.uoc.edu/bitstream/10609/118086/7/aaroncastroTFM0620memoria.pdf

Thomas, T. M.. *Juniper Networks Reference Guide: JUNOS Routing, Configuration, and Architecture.* Boston Pearson Education, 2023

Warnock, G., Ghafary, M., & Shaheen, G. *Alcatel-Lucent Service Routing Architect (SRA) Self-Study Guide: Preparing for the BGP, VPRN and Multicast Exams.* Wiley Publisher, 2006

Wendel Odom. (2020) Capítulo 12 Analyzing Classful IPv4 Networks. *CCNA 200-301 Official Cert Guide. (p.293).* Cisco Press

Anexos

Anexo 1

Glosario de términos

NAT	**:**	Network Address Translation.
CGNAT	**:**	Carrier Grade NAT.
BNG	**:**	Broadband Network Gateway.
MTC	**:**	Ministerio de Transporte y Comunicaciones.
FITEL	**:**	Fondo de Inversión en Telecomunicaciones.
PRONATEL	**:**	Programa Nacional de Telecomunicaciones.
ISP	**:**	Internet Service Provider.
IDB	**:**	Inter-American Development Bank
CEPAL	**:**	Comisión Económica para América Latina
RFC	**:**	Request For Comments
TR	**:**	Technical Report
IETF	**:**	Internet Engineering Task Force
BBF	**:**	Broadband Forum
MINEDU	**:**	Ministerio de Educación
CPE	**:**	Customer Premise Equipment
PBI	**:**	Producto Bruto Interno
CEPAL	**:**	Comisión Económica para América Latina
INEI	**:**	Instituto Nacional de Estadística e Informática
MIDIS	**:**	Ministerio de Desarrollo e Inclusión Social
AS	**:**	Autonomous System
MPLS	**:**	Multiprotocol Label Switching
BGP	**:**	Border Gateway Protocol
BGP LU	**:**	BGP Labeled Unicast

IP	**:**	Internet Protocol
PoP	**:**	Point of Presence
PTP	**:**	Point to Point
IS-IS	**:**	Intermediate System to Intermediate System
LDP	**:**	Label Distribution Protocol
DHCP	**:**	Dynamic Host Configuration Protocol
AAA	**:**	Authentication, Authorization and Accounting
SDN	**:**	Software Defined Network
UBR	**:**	Underlay Border Router
HA	**:**	High Availability
QoS	**:**	Quality of Service
VPN	**:**	Virtual Private Network
L2 VPN	**:**	Layer 2 VPN
L3 VPN	**:**	Layer 3 VPN
CDN	**:**	Content Delivery Network
O&M	**:**	Operations and Maintenance
RIP	**:**	Routing Information Protocol
IGRP	**:**	Interior Gateway Routing Protocol
EIGRP	**:**	Enhanced Interior Gateway Routing Protocol
OSPF	**:**	Open Shortest Path First
OSI	**:**	Open Systems Interconnection
TPC	**:**	Transmission Control Protocol
UDP	**:**	Transmission Control Protocol
NLRI	**:**	Network Layer Reachability Information
FEC	**:**	Forwarding Equivalence Class
LER	**:**	Label Edge Router

LSR	**:**	Label Switch Router
CE	**:**	Customer Edge
PE	**:**	Provider Edge
P	**:**	Provider
ToS/CoS	**:**	Type of Service/Class of Service
RSVP-TE	**:**	Resource Reservation Protocol - Traffic Engineering
RADIUS	**:**	Remote Authentication Dial-In User Service
VXLAN	**:**	Virtual Extensible LAN
ISP	**:**	Internet Service Provider
RG	**:**	Residential Gateway
BSAN	**:**	Broadband Service Access Network
BSA	**:**	Broadband Service Aggregator
API	**:**	Application Programmable Interface
CIR	**:**	Committed Information Rate
PIR	**:**	Peak Information Rate

Anexo 2

Puerta de enlace residencial (*Residential Gateway*)

1. Serie 7850 NSG-C601

Puerta de Enlace Residencial NSG-C601

Nota: tomado de Nuage Networks (2020b).

El Nuage Networks 7850 Network Services Gateway LTE/Wi-Fi 7850 NSG-C601 (7850 NSG-C601) está optimizado para redes de sucursales para impulsar la conectividad requerida por los entornos de TI en la nube actuales. Basada en la solución de redes definidas por software (SDN) más completa de la industria, se integra perfectamente en la solución de servicios de red virtualizados (VNS) de Nuage Networks. Se utiliza para conectar sucursales pequeñas a la SD-WAN empresarial con una eficiencia de red óptima y una gestión de configuración centralizada desde la plataforma de servicios virtualizados (VSP) de Nuage Networks. La solución ofrece múltiples escenarios de servicio, estos son VPN de capa 2, VPN de capa 3 y conexión a Internet (Nuage Networks, 2020b).

La serie 7850 NSG-C601 es un pequeño dispositivo de escritorio y puede enviarse e instalarse en una ubicación empresarial sin necesidad de experiencia en ingeniería de redes. Debido a que se administra de forma centralizada, mejora la eficiencia y la

productividad de las operaciones de las sucursales y, al mismo tiempo, elimina la necesidad de soporte de TI in situ. Se incorpora mediante un proceso de arranque seguro que utiliza autenticación de cero, uno o dos factores según el modelo de confianza y la postura de seguridad de la sucursal y del instalador. Una vez iniciado, habilita las capacidades de red instantáneas en la sucursal (Nuage Networks, 2020b).

Además, se conecta fácilmente a la red IP subyacente de cualquier proveedor (privada, pública o híbrida) a través de cualquier acceso utilizando sus puertos Ethernet Gigabit (RJ-45) orientados a WAN o enlace ascendente LTE. Las capacidades de automatización de red basadas en políticas se extienden sin problemas a la sucursal, lo que permite a los usuarios conectarse automáticamente a cualquier aplicación en cualquier nube (pública o privada). Como resultado, la entrega y el consumo de servicios de red se simplifica enormemente (Nuage Networks, 2020b).

2. Características de *software*

Características de software del equipo NSG-C601

Automatización	Activación y autenticación segura de la serie 7850 NSG-C601 (X.509). Gestión del ciclo de vida del software serie 7850 NSG-C601. API RESTful en dirección norte del servidor de políticas y bus de eventos basado en notificaciones push.
Gestión	La plataforma de servicios virtualizados permite un plano de gestión unificado para servicios de centro de datos en la nube (VCS) y WAN definidas por software (VNS). Gestión de políticas centralizada y basada en plantillas para todos los objetos gestionados (incluidos servicios, seguridad y QoS). Multi-inquilino con administración basada en roles, integración LDAP opcional.
Servicios de Red	Topologías de malla completa y de centro y radio. Servicios de red privada virtual (VPN) de capa 2 y capa 3. Servicio de conexión a Internet local. VLAN 802.1Q de importancia local. Servicios de superposición que admiten la encapsulación VXLAN y VXLANoIPsec con integración en otros entornos IPsec (IKEv1/v2). Servidor DHCPv4, PAT, NAT 1:1, underlay offload NAT trasversal dinámico Equilibrio de carga de enlace ascendente WAN basado en flujo, dirección avanzada del tráfico. Hardware preparado para IPv6 con soporte de software en versiones futuras. Integración con las funciones Border Router y Underlay Border Router implementadas dentro del entorno VNS para proporcionar conectividad SD-WAN sin límites.
Dirección de Trafico	Enrutamiento consciente de aplicaciones (AAR) con detección de aplicaciones (AD) para redirigir el tráfico para que se ajuste mejor al enlace ascendente según la política. La Medición del rendimiento de la red (NPM) monitorea el rendimiento de superposición (retraso de ida y vuelta, pérdida de paquetes, fluctuación) y toma una decisión de reenvío inteligente basada en los requisitos de SLA basados en la aplicación.

Calidad de Servicio	Clasificación basada en DSCP con opciones de reescritura de DSCP. Clasificación de QoS de ingreso y limitación de velocidad. Configuración de salida jerárquica QoS con reconocimiento de color basada en 4 colas WRR. Cola de control de red para el tráfico del plano de control.
Servicios de Seguridad	Clasificación de tráfico direccional de Capa 2 a Capa 4 con acciones de aceptar/denegar/redireccionar. ACL reflexiva y con estado de entrada y salida de todo el dominio basada en plantillas. Creación avanzada de políticas de seguridad dinámicas. Auditoría de políticas mediante herencia de plantillas. Integración con los servicios de seguridad virtualizados (VSS) de Nuage Networks para detectar, prevenir y responder a eventos de seguridad en SD-WAN.
Encriptación	Generación y distribución segura de claves Autenticación IPsec: SHA1, SHA2 Cifrado IPsec: 3DES, AES-128, AES-192 y AES-256 Conexiones del plano de control autenticadas y cifradas
Análisis y Visibilidad	Motor de análisis en tiempo real integrado en el Directorio de servicios virtualizados (VSD) de Nuage Networks. Recopilación centralizada de estadísticas de uso para puertos, flujos y colas de QoS Registro basado en eventos. Integración segura de syslog. Duplicación remota de puertos. Acceso CLI centralizado para diagnósticos centralizados con la capacidad de habilitar/deshabilitar el acceso CLI remoto.
Alta disponibilidad	Infraestructura de recopilación de estadísticas y políticas basada en clústeres. Federación de políticas que respalda la redundancia geográfica y el equilibrio de carga. Arquitectura de plano de control escalable que aprovecha la federación basada en MP-BGP. Configuración de alta disponibilidad para 7850 NSG-C601 con resiliencia por subred. Opciones de redundancia de enlace ascendente WAN con reenvío selectivo de enlace ascendente. Conexiones del plano de control y gestión activa/activa según 7850 NSG-C601.

Nota: tomado de Nuage Networks (2020b)

3. Características de hardware

Características de hardware del equipo NSG-C601

CPU	Intel C3000 series
Interfaces	4 x 10/100/1000BASE-T Gigabit Ethernet (RJ45) 2 x USB 2.0 Standard-A female 1 x RS-232 RJ-45 console
Punto de Acceso Wi-Fi	Soporta canales de operación de 2.4 GHz o 5 GHz Antena: Antena Omnidireccional Dual Band Estándares: 802.11a/b/g/n/ac Soporta 2 SSIDs Encriptación: AES, TKIP, CCMP Métodos de Autenticación: PSK (Pre Shared Key) – WPA/WPA2, WEP, Open, Passthrough Captive Portal
LTE Integrado	Bandas LTE: 1, 2, 3, 4, 5, 7, 8, 12, 13, 18, 19, 20, 25, 26, 28, 38, 39, 40, 41 Bandas UMTS: 1, 2, 4, 5, 6, 8, 19 Bandas GSM: 2, 3, 5, 8 Antena: Antena Omnidireccional Estándares: LTE Categoría 4, HSPA+, UMTS Interfaz SIM: 2FF SIM slot con 3FF e incluye adaptadores 4FF
Dimensiones	255mm x 245mm x 40mm (ancho x profundidad x alto) (antena incluida)
Peso	1.5 kg
Temperatura de Operación	0° to 40° C / 32° to 104° F al nivel del mar. Reducción de la temperatura de funcionamiento de 1 °C por cada 305 m (1000 pies) sobre el nivel del mar
Humedad Relativa de Operación	5% to 90% at 40° C
Potencia	Consumo: 36 W (máximo) Alimentación: 100 to 240 V at 50-60 Hz, rango completo Conector: C14
Refrigeración	Refrigeración pasiva
Cripto-Aceleración	CPU integrated Intel® QuickAssist

Security	Módulo de plataforma confiable incorporado para garantizar la integridad del sistema, el sistema operativo y la confidencialidad de la administración y el cifrado del plano de datos.
Instalación	Instalación sobre mesa

Nota: tomado de Nuage Networks (2020b)

Anexo 3

Nodo de acceso y de agregación (BSAN Y BSA)

1. NOKIA 7210 SAS-S

Como miembro de la cartera de productos Service Router (SR), el 7210 SAS S, mostrado en la Figura 33, aprovecha el probado sistema operativo Nokia Service Router (SR OS) y Nokia Network Services Platform (NSP) para brindar servicio y coherencia operativa en toda la red (Nokia, 2024a).

Enrutador de acceso distrital, intermedio y terminal

Nota: tomado de Nokia (2024a)

El 7210 SAS cumple con la especificación Carrier Ethernet (CE) 3.0 de Metro Ethernet Forum (MEF) y con la calidad de servicio jerárquica (H-QoS) y la operación, administración y mantenimiento integrales (OAM). El 7210 SAS S proporciona flexibilidad de implementación, riqueza de servicios y simplicidad operativa para extender los servicios IP/MPLS y Carrier Ethernet en toda la red (Nokia, 2024a).

2. Beneficios

a) Soporte para servicios diferenciados

Los proveedores de servicios quieren desbloquear nuevas fuentes de ingresos. Los operadores de redes empresariales y de misión crítica deben cumplir con los requisitos específicos de cada una de sus diversas aplicaciones. Para satisfacer estas necesidades, el 7210 SAS ofrece servicios diferenciados, que incluyen Carrier Ethernet, IP VPN y servicios de Internet mejorados junto con QoS por servicio y garantías de ancho de banda. Los proveedores de servicios pueden crear modelos de servicios escalables con opciones de facturación flexibles, adaptando paquetes de servicios según los requisitos de rendimiento y disponibilidad de sus clientes.

Los operadores de redes empresariales y de misión crítica pueden proporcionar perfiles de tráfico y QoS personalizados para garantizar la entrega de aplicaciones individuales y negocios de comunicaciones esenciales (Nokia, 2024a).

b) Satisfacción del cliente y garantía de entrega de aplicaciones

Las capacidades plug-and-play del 7210 SAS junto con el NSP ofrecen una rápida activación del servicio sin necesidad de desplazamientos, lo que acelera los plazos de puesta en servicio y el tiempo de obtención de ingresos, minimizando al mismo tiempo la posibilidad de error del operador. La capacidad de monitorear y medir continuamente el tráfico de un extremo a otro y solucionar problemas de forma proactiva permite encontrar y resolver problemas de red antes de que afecten a los usuarios finales (Nokia, 2024a).

El monitoreo, la medición del desempeño de las métricas del servicio, la predicción de violaciones de umbrales, los informes de los resultados de las pruebas y la facturación precisa brindan un nivel superior de servicio a los usuarios finales. Estas características también aumentan la confiabilidad de las aplicaciones de misión crítica. Para los proveedores de servicios, los portales de autoservicio para clientes con capacidades de gestión personalizadas bajo demanda mejoran la calidad general de la experiencia para sus clientes (Nokia, 2024a).

c) Reducción de costos a través de la simplicidad operativa

Se pueden lograr ahorros de costos mediante la transición de redes heredadas separadas a una única plataforma donde convergen múltiples servicios en un enlace ascendente y cada aplicación puede ser respaldada por una gama completa de servicios Carrier Ethernet e IP/MPLS. Con una variedad de características y factores de forma compactos, el 7210 SAS S se escala de manera rentable para soportar los requisitos actuales y futuros de los clientes y las aplicaciones. Proporciona ahorros a través de QoS avanzada, OAM de extremo a extremo, integración óptica, actualizaciones de red

optimizadas, capacitación reducida, ciclos de prueba y costos de integración del sistema de soporte de operaciones (OSS) (Nokia, 2024a).

3. Características de hardware

Características de hardware del equipo 7210 SAS-S

Red de Transporte	IP/MPLS/segment routing/Ethernet
Temporización y Sincronización	ITU-T SyncE with ESMC IEEE 1588v2 Transparent Clock (TC)
Dimensiones	Altura: 4.32 cm (1.7 in) 1RU Ancho: 44 cm (17.3 in) Profundidad: 38.7 cm (15.2 in)
Opciones de fuente de alimentación	Dos alimentaciones. Un suministro interno fijo y un suministro modular opcional Intercambiables en caliente
Requerimientos de energía	AC input: 100 V to 240 V, 50 Hz to 60 Hz DC input: -40 V DC to -72 V DC
Enfriamiento	Enfriado por ventilador con flujo de aire de adelante hacia atrás
Rango de Temperatura de funcionamiento	0°C to 40°C (32°F to 104°F)

Nota: tomado de Nokia (2024)

4. Características de software

a) Servicios

- Servicios de red privada virtual (VPN) de capa 2:
  - línea arrendada virtual (VLL) y servicio de LAN privada virtual (VPLS).
- Servicios IP VPN (IPv4 e IPv6).
- VPN Ethernet (EVPN):
  - VPLS
  - Alojamiento múltiple con opciones únicas activas y totalmente activas.
- Servicio de Internet mejorado (IPv4 e IPv6).

- VPLS enrutado con IES e interfaces IPv4 e IPv6 de red enrutada privada virtual (VPRN).
- Multidifusión IPv4.
- IPv4 VPN multicast (VPN multicast de próxima generación).
- Asignación dinámica de VLAN (SAP) mediante autenticación Dot1x RADIUS con EHS.

b) Protocolos de red

- IEEE 802.1Q (VLAN) y 802.1ad (QinQ).
- Provider Backbone Bridging (PBB), Backbone Edge Bridge (BEB) y Backbone Core Bridge (BCB) según se define en IEEE 802.1ah.
- Enrutamiento de segmentos:
  - Sistema intermedio a sistema intermedio (IS-IS) y Abrir primero la ruta más corta (OSPF)
  - Alternativa sin bucle (LFA) y LFA remota (RLFA)
- Protocolo de elementos de cálculo de ruta (PCEP)
  - Protocolo de reserva de recursos (RSVP)
- Enrutador de borde de etiquetas MPLS (LER) y LSR.
  - LSP MPLS punto a multipunto (P2MP) para multidifusión NG-MVPN.
  - MPLS-TP (basado en estándares IETF)
  - Protocolo de distribución de etiquetas (LDP), LDPv6, LDP sobre RSVP y LDP dirigido (T-LDP)
  - Protocolo de reserva de recursos — Ingeniería de tráfico (RSVP-TE)

c) Calidad de servicio

- Clasificación de paquetes de entrada de servicio basada en
- Criterios MAC e IP (IPv4 e IPv6), MPLS EXP en el ingreso a la red
- Clasificación de paquetes de entrada de servicio basada en IP DSCP y Dot1p con un gran conjunto de medidores para mayor escalamiento de SAP/servicio
- Reclasificación de la salida del servicio basada en IP DSCP, IP presedence, Dot1p
- Entrada y salida jerárquica por servicio
- vigilancia, colas y configuración
- Almacenamiento en búfer profundo
- Señalización de tráfico autogenerada
- Notificación de ancho de banda Ethernet (ETH-BN) para transporte por enlace de microondas.

Anexo 4

Puerta de enlace de la red de acceso (BNG)

1. NOKIA 7750 SR-7

A medida que las redes experimentan un crecimiento de tráfico sin precedentes y demandas impredecibles, los operadores buscan satisfacer requisitos de rendimiento cada vez mayores mientras implementan nuevos servicios rápidamente a través de una red segura y autodefensa. El 7750 SR aborda estos imperativos, permitiendo a los operadores construir una red más grande, segura, automatizada y sostenible con un retorno de la inversión superior (Nokia, 2024b).

El 7750 SR ofrece certeza de rendimiento para roles de red exigentes. Universales QSFP-DD, QSFP28 y los conectores SFP28 permiten entornos de red de alta densidad de 400GE, 100GE, 25GE y 10GE (Nokia, 2024b).

En el corazón del 7750 SR se encuentra el silicio Nokia 3,0 Tb/s FP4. Es un procesador de red totalmente programable, totalmente determinista y energéticamente eficiente, lo que permite diversas necesidades de implementación y es esencial para el enrutamiento de alto rendimiento. Impulsado por las funciones integrales del sistema operativo Nokia Service Router (SR OS), el 7750 SR admite una gama completa de funciones y servicios de red. Estas capacidades líderes en la industria permiten diseños de redes sin compensaciones entre rendimiento, capacidad, escala y consumo de energía (Nokia, 2024b).

Enrutador Broadband Network Gateway (BNG)

Nota: tomado de Nokia (2024b)

Para protegerse contra las crecientes amenazas a la seguridad, el 7750 SR adopta un enfoque integrado en silicio para la seguridad de la red IP. Actuando como un sensor de ataque de alta precisión y un elemento de mitigación, el 7750 SR hace la parte de red de la solución para ayudar a neutralizar los ataques DDoS, todo sin afectar el rendimiento del enrutador (Nokia, 2024b).

2. Características de hardware

Características de Hardware del equipo 7750 SR-7

Capacidad del Sistema Full Dúplex (FD)	• 4 Tb/s (non-redundante) • 2 Tb/s (redundante)
Capacidad de Ranura (FD)	• 800 Gb/s (non-redundante) • 400 Gb/s (redundante)
Agregación inteligente por ranura (FD)	1.2 Tb/s
Número de IOM y ranuras MS-ISM (máx.)	5
Número de MDAs e ISA2s (máx.)	10
Enfriamiento	De lado a atrás
Sistema de Módulos	SFM6-7, SFM5-12, CPM5, IOM, MDA-e-XP, MDA-e, ISA2, MS-ISM, EFT, PEM
Dimensiones	Altura: 35.56 cm (14.0 in), 8RU Ancho: 44.45 cm (17.5 in) Profundidad: 64.77 cm (25.5 in)
Peso	Vacío: 34 kg (75 lb) Con carga: 70 kg (155 lb)
Alimentación	**Fuente de Alimentación DC** DC-40 V a -72 V, 100 A, 4,000 W máx. o DC-46 V a -72 V, 100 A, 4,600 W máx. Redundancia 1+1 **Fuente de Alimentación AC (opcional)** Voltaje Entrada: 200 V AC a 240 V AC Voltaje Salida: 42 V DC a 56 V DC Corriente: 50 A

Nota: tomado de Nokia (2024b)

a) Módulo de entrada/salida (IOM)

El IOM de ranura completa contiene el complejo de reenvío que realiza funciones típicas como enrutamiento IP/MPLS, búsquedas de paquetes, clasificación, procesamiento y reenvío de tráfico, habilitación de servicios y QoS. Disponible en dos variantes, equipa

hasta dos tipos de adaptador-e dependiente de medios conectables (MDA-e) y admite una serie de configuraciones con licencia de pago a medida que crece. El IOM5-e basado en FP4 ofrece hasta 1,5 Tb/s FD (no redundante) y 1,2 Tb/s FD (redundante). Ofrece hasta 800 Gb/s FD (no redundante) y hasta 400 Gb/s FD (redundante) de capacidad. El IOM4-e basado en FP3 ofrece un rendimiento de FD por ranura de hasta 200 Gb/s (Nokia, 2024b).

Adaptador dependiente de medios (MDA) Los MDA proporcionan conectividad de interfaz modular junto con una variedad de tipos de interfaz y configuraciones de densidad. Los tipos de Ethernet admiten ITU-T Sync-E e IEEE 1588v2 para requisitos de sincronización (Nokia, 2024b).

El MDA-e proporciona un rendimiento de FD de hasta 100 Gb/s en un adaptador de media ranura. Admite conectores QSFP28, SFP28, CSFP, SFP+ y CFP2 con opciones de conexión flexibles, que incluyen 10 x 10GE y 4 x 25GE, MACsec junto con compatibilidad con ITU-T G.709 y red de transporte óptico (OTN) FEC (Nokia, 2024b).

b) Adaptador de servicio integrado (ISA)

Disponibles en dos variantes, los ISA brindan procesamiento y almacenamiento en búfer especializados para niveles más profundos de servicios integrados y aplicaciones avanzadas para el 7750 SR-7. El soporte del servicio incluye: garantía de aplicaciones, firewall con estado de capa 7, servidor de red L2TP (LNS), traducción de direcciones de red de nivel de operador (CG-NAT), IPsec, túnel IP, puerta de enlace LAN inalámbrica (WLGW) y Servicios de vídeo avanzados. El ISA2 es un adaptador de media ranura que ofrece hasta 40 Gb/s de velocidad de procesamiento y es compatible con el IOM4-e. El módulo de servicio integrado multiservicio (MS-ISM) es un módulo de altura completa que aprovecha dos ISA2 y admite una velocidad de procesamiento de hasta 80 Gb/s (Nokia, 2024b).

c) Módulo de estructura de conmutación (SFM)

Las tarjetas Fabric intercambiables en caliente, además de albergar el módulo 5 del procesador de control enchufable (CPM5). El SFM6-7 permite conectividad de velocidad de línea de 800 Gb/s FD (no redundante) o 400 Gb/s FD (redundante). entre todas las ranuras del chasis 7750 SR-7 y SR-12. Las tarjetas Fabric intercambiables en caliente tienen un diseño de carga compartida activo-activo 1+1 o 2+0 no redundantes en una configuración consecutiva. Los módulos SFM6-7 de altura completa controlan las funciones de conmutación del sistema y albergan el CPM5 enchufable para proteger la inversión (Nokia, 2024b).

d) Módulo de procesador de control (CPM5)

El CPM5 está alojado en un SFM5 y es compatible con 7750 SR-7, SR-12 y SR-12e. Proporciona el procesamiento del plano de gestión, seguridad y control. El procesamiento central y la memoria están intencionalmente separados de la función de reenvío en los módulos de interfaz para garantizar la resiliencia del sistema. Las variantes de CPM redundantes funcionan en un modo de conmutación por error con estado y sin interrupciones con enrutamiento completo y servicios sin interrupciones (Nokia, 2024).

3. Características de software

El soporte de funciones y protocolos dentro de la serie 7750 SR incluye, entre otros, lo siguiente (Nokia, 2024):

a) Funciones de enrutamiento IP y MPLS

- Enrutamiento de IP Unicast:
  - Sistema Intermedio a Sistema Intermedio (IS-IS)
  - Open Shortest Path First (OSPF)
  - Protocolo de información de enrutamiento (RIP)
  - Protocolo de puerta de enlace fronteriza multiprotocolo (MBGP)

  - Reenvío de ruta inversa de Unicast (uRPF)
  - Funciones integrales de protección del plano de control para mayor seguridad.
  - Paridad de características de IPv4 e IPv6

- Enrutamiento de IP Multicast:
  - Protocolo de gestión de grupos de Internet (IGMP)
  - Descubrimiento de oyentes de multidifusión (MLD)
  - Multidifusión independiente del protocolo (PIM)
  - Protocolo de descubrimiento de fuente de multidifusión (MSDP)
  - Replicación explícita indexada por bits (BIER)
  - Paridad de características de IPv4 e IPv6

- MPLS:
  - Funciones Label Edge Router (LER) y Label Switch Router (LSR) compatibles con diseños MPLS integrados
  - Perfil de transporte MPLS (MPLS-TP)
  - Protocolo de distribución de etiquetas (LDP) y protocolo de reserva de recursos (RSVP) para señalización MPLS e ingeniería de tráfico
  - Incluye rutas conmutadas por etiquetas (LSP) punto a punto (P2P) y punto a multipunto (P2MP) con LDP de multidifusión (MLDP), RSVP P2MP y ruta múltiple ponderada de igual costo (ECMP)

b) Funciones de enrutamiento de segmentos y SDN

- Algoritmos flexibles de enrutamiento de segmentos para el plano de datos SR-MPLS y SRv6 (128 bits y microsegmentos)
- Compatibilidad con IS-IS y OSPF SR de instancias múltiples con túnel de ruta más corta, enrutamiento de segmentos - Ingeniería de tráfico (SR-TE) LSP, algoritmos flexibles y política estática y BGP SR.
  - La implementación proporciona protección Loop Free Alternate (LFA), LFA remota y topología independiente - LFA (TI-LFA) para todo tipo de túneles, así como protección de extremo a extremo con rutas primarias/secundarias para túneles SR-TE y políticas SR.
  - PCEP permite delegar el LSP SR-TE al NSP de Nokia o a una función PCE de terceros
- Tablas de reenvío programables a través de la función API de base de información de enrutamiento (RIB) basada en gRPC y política de reenvío MPLS
- Amplio conjunto de capacidades que utilizan lógica ACL para dirigir rutas/flujos hacia varios tipos de destino, como IP next-hop, SR-TE/RSVP-TE/MPLS-TP LSP y enrutamiento y reenvío virtual (VRF)
  - Aplicable a una amplia gama de contextos de enrutamiento y servicio, como tabla de enrutamiento global, red enrutada privada virtual (VPRN), servicio virtual LAN privado (VPLS) y servicio E-Pipe.
  - Admite interfaces de control como OpenFlow, FlowSpec, CLI y NETCONF.
- Integración de control SDN de múltiples proveedores a través de OpenFlow, PCEP, BGP-Link State (BGP-LS) y compatibilidad con políticas BGP SR
- Recopilación de estadísticas de tráfico sobre un amplio conjunto de constructos:
  - PLD
  - LSP RSVP-TE y SR-TE
  - Políticas de reenvío MPLS
  - Políticas SR-MPLS y SRv6

- Entradas del túnel RIB API
- SID del protocolo de puerta de enlace interior (IGP)

c) Funciones de capa 2

- LAN Ethernet (E-LAN): BGP-VPLS, PBB-VPLS, EVPN y PBB-EVPN
- BGP-VPWS, EVPN-VPWS y PBB-EVPN
- EVPN y PBB-EVPN
- EVPN, Virtual eXtensible LAN (VXLAN)

d) Funciones de capa 3

- IP-VPN, servicios de Internet mejorados
- EVPN para servicios de unidifusión de capa 3 y multidifusión entre subredes optimizada (OISM) con enrutamiento y puente integrados (EVPN-IRB)
- VPN de multidifusión (MVPN), que incluye inter-AS MVPN y MVPN de próxima generación (NG-MVPN)
- Interconexión entre EVPN y gateway IP-VPN, incluido el atributo D-PATH para protección de bucle en gateways redundantes
- Integración perfecta de MPLS/SRv6 con IP-VRF para inter-funcionamiento o migración entre tecnologías de transporte MPLS y SRv6