



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Profesional de Ingeniería de Telecomunicaciones

**Diseño de una red de campus corporativa para brindar
servicios de calidad global en la sede principal de una
entidad financiera**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de
Telecomunicaciones

AUTOR

Brandon Wilder FLORES HUAMANI

ASESOR

Mg. Jesús Otto VILLANUEVA NAPURÍ

Lima, Perú

2024



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Flores, B. (2024). *Diseño de una red de campus corporativa para brindar servicios de calidad global en la sede principal de una entidad financiera*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Telecomunicaciones]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Brandon Wilder Flores Huamani
Tipo de documento de identidad	DNI
Número de documento de identidad	74171271
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Jesús Otto Villanueva Napurí
Tipo de documento de identidad	DNI
Número de documento de identidad	25726864
URL de ORCID	https://orcid.org/0000-0002-3380-4991
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Celso Ysidro Geronimo Huaman
Tipo de documento	DNI
Número de documento de identidad	09191500
Miembro del jurado 1	
Nombres y apellidos	Manuel Francisco Bermeo Noriega
Tipo de documento	DNI
Número de documento de identidad	08437735
Miembro del jurado 2	
Nombres y apellidos	Arlich Joel Portillo Allende
Tipo de documento	DNI
Número de documento de identidad	10125495
Datos de investigación	

Línea de investigación	C.0.3.28. Comunicación/redes y sistemas distribuidos
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica
Ubicación geográfica de la investigación	Edificio: Niubiz País: Perú Departamento: Lima Provincia: Lima Distrito: Miraflores Latitud -12.119236 Longitud -77.037461
Año o rango de años en que se realizó la investigación	Julio 2020 – Octubre 2020
URL de disciplinas OCDE	Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05 Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Ingeniería eléctrica, Ingeniería electrónica https://purl.org/pe-repo/ocde/ford#2.02.01



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



ACTA DE SUSTENTACIÓN TRABAJO DE SUFICIENCIA PROFESIONAL

ACTA N°072/FIEE-CTGT/2024

Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 09 de septiembre del 2024, como presidente de Jurado el **DR. CELSO YSIDRO GERONIMO HUAMAN**, integrado por el Miembro de Jurado el **MG. ARLICH JOEL PORTILLO ALLENDE**, el Miembro de Jurado **MG. MANUEL FRANCISCO BERMEO NORIEGA** y Miembro Asesor el **MG. JESÚS OTTO VILLANUEVA NAPURÍ**.

Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional del Bachiller **BRANDON WILDER FLORES HUAMANI** código N° 11190064 que para optar el Título Profesional de Ingeniero de Telecomunicaciones sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO DE UNA RED DE CAMPUS CORPORATIVA PARA BRINDAR SERVICIOS DE CALIDAD GLOBAL EN LA SEDE PRINCIPAL DE UNA ENTIDAD FINANCIERA**.

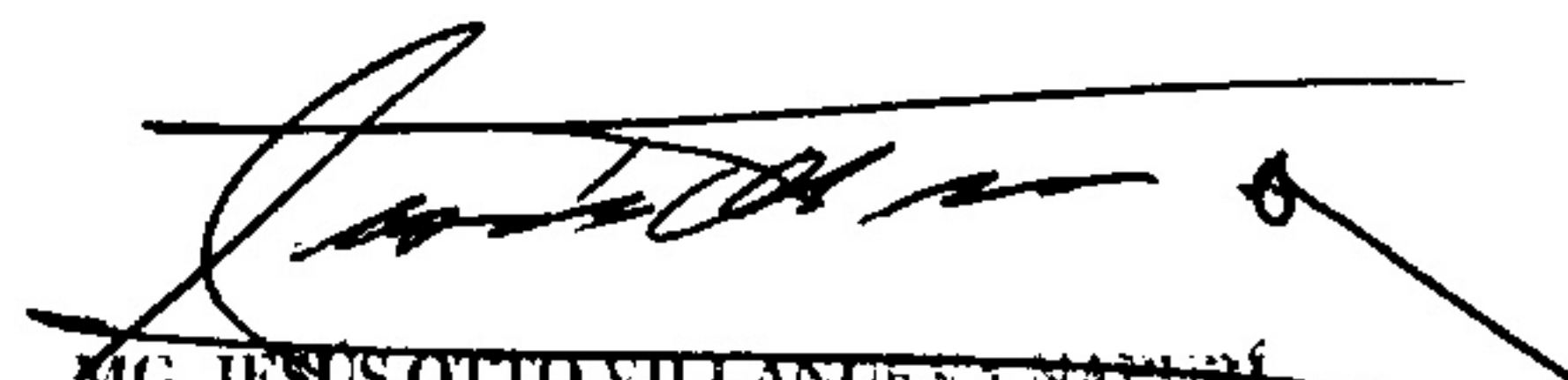
El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de ...1.6... (*Pienso*)

Ciudad Universitaria, 09 de septiembre del 2024


DR. CELSO YSIDRO GERONIMO HUAMAN
Presidente Jurado


MG. ARLICH JOEL PORTILLO ALLENDE
Miembro Jurado


MG. MANUEL FRANCISCO BERMEO NORIEGA
Miembro Jurado


MG. JESÚS OTTO VILLANUEVA NAPURÍ
Miembro Asesor



Universidad Nacional Mayor de San Marcos

Universidad del Perú, Decana de América

Vicerrectorado de Investigación y Posgrado



CERTIFICADO DE SIMILITUD

Yo Jesús Otto Villanueva Napurí mi condición de asesor acreditado con el Acta de Sustentación de Trabajo de Suficiencia Profesional: **DISEÑO DE UNA RED DE CAMPUS CORPORATIVA PARA BRINDAR SERVICIOS DE CALIDAD GLOBAL EN LA SEDE PRINCIPAL DE UNA ENTIDAD FINANCIERA** presentado por el bachiller **BRANDON WILDER FLORES HUAMANI**, para optar al título profesional de Ingeniero de Telecomunicaciones. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 12% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**. Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado correspondiente.

Firma del Asesor

DNI: 25726864

Nombres y apellidos del asesor:

Mg. Jesús Otto Villanueva Napurí

DEDICATORIA

Este trabajo está dedicado a mis padres, hermanos y a toda mi familia en general por lo que ellos representan mucho en mi vida personal y profesional.

AGRADECIMIENTOS

Agradecer a todos mis amigos y compañeros de profesión que me ayudaron y me dieron la oportunidad para seguir creciendo como profesional.

RESUMEN

El presente documento tiene como objetivo diseñar una nueva solución de arquitectura de Red de Campus, donde se contemple el despliegue de los equipos de networking en las distintas capas de Acceso, Distribución y Core; y con esto realizar una nueva y ordenada distribución de los equipos que pertenecen a la actual red de la sede principal de la entidad bancaria Niubiz, así como una gestión y acceso centralizado tanto para los dispositivos como los usuarios finales.

El diseño cumple con los requerimientos para una óptima instalación y configuración tanto física como lógica de los equipos involucrados. Dentro de las consideraciones de diseño se tienen en cuenta las mejores prácticas para la instalación y configuración de los diferentes elementos y las funcionalidades a aplicar como método base para el despliegue.

Se proporcionará modos de red de campus típicos, lo que permitirá encontrar rápidamente ejemplos de implementación de características específicas facilitando el despliegue y configuración de los equipos involucrados en esta nueva red de campus.

Finalmente, se mostrarán resultados en cuanto a cobertura inalámbrica para los usuarios, a través de los dispositivos Wireless Local Area Network (WLAN), así como también de las funciones de gestión centralizada de la solución y acceso controlado.

Palabras clave: red de campus, wlan, mejores prácticas, controlador de acceso, gestión centralizada.

ABSTRACT

The objective of this document is to design a new Campus Network architecture solution, which contemplates the deployment of networking equipment in the different layers of Access, Distribution and Core; and with this, carry out a new and orderly distribution of the equipment that belongs to the current network of the main headquarters of the Niubiz banking entity, as well as centralized management and access for both the devices and the end users.

The design meets the requirements for optimal installation and configuration, both physically and logically, of the equipment involved. Within the design considerations, the best practices for the installation and configuration of the different elements and the functionalities to be applied as a base method for deployment are taken into account.

Typical campus network modes will be provided, allowing you to quickly find implementation examples of specific features, facilitating the deployment and configuration of the equipment involved in this new campus network.

Finally, results will be shown regarding wireless coverage for users, through the Wireless Local Area Network (WLAN) devices, as well as the centralized management functions of the solution and controlled access.

Keywords: campus network, wlan, best practices, access controller, centralized management.

TABLA DE CONTENIDO

RESUMEN.....	iv
ABSTRACT	v
TABLA DE CONTENIDO	vi
LISTA DE FIGURAS.....	viii
LISTA DE TABLAS	ix
CAPITULO I: INTRODUCCIÓN	1
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	3
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD	5
3.1 Organización de la actividad	5
3.2 Problemática	5
3.2.1 Problema General	6
3.2.2 Problemas Específicos	6
3.3 Objetivos	6
3.3.1 Objetivo General	6
3.3.2 Objetivos Específicos.	7
3.4 Justificación e importancia de la investigación	7
3.4.1 Justificación técnica	7
3.4.2 Justificación operativa	8
3.5 Metodología.....	9
3.5.1 Antecedentes	9
3.5.2 Bases teóricas.....	11
3.5.3 Mejores prácticas de diseño de red.....	13
3.5.4 Marco conceptual	13
3.6 Procedimiento	22
3.6.1 Introducción de la Red.....	22
3.6.2 Topología General de la Red Campus Miraflores.....	22
3.6.3 Descripción de la nueva red de Campus	23
3.6.4 Estandarización	24
3.6.5 Versiones de Software de los equipos	26
3.6.6 Servicios Campus Miraflores.....	28
3.6.7 Conexiones en la Red Campus Miraflores	28
3.6.8 NAC Server – Agile Controller Campus.....	35
3.6.9 Plataforma de Gestión – eSight.....	39

3.6.10	Mapeo de Puertos de la red de Campus Miraflores	42
3.6.11	Mapeo de puertos Red Campus.....	42
3.6.12	Mapeo de puertos Red Paralela	43
3.6.13	Distribución de equipos en el rack Campus Miraflores	43
3.7	Resumen de la actividad	45
CAPITULO IV: RESULTADOS		48
4.1	Justificación.....	48
4.2	Evaluaciones	48
4.2.1	Evaluación presupuestal	48
4.2.2	Evaluación técnica	49
4.2.3	Configuraciones de dispositivos de red	49
4.3	Descripción de la implementación	50
4.3.1	Cobertura Wifi Access Points	50
CAPITULO V CONCLUSIONES		52
CAPITULO VI: RECOMENDACIONES.....		53
CAPITULO VII: REFERENCIAS		54
ANEXOS		57
Anexo A: Topología General a detalle de la red Campus Miraflores.....		58
Anexo B: Componentes de networking del nuevo diseño de la red.....		59
Anexo C: Mapeo de puertos de la Red Campus.....		61
Anexo D: Mapeo de puertos de la Red Paralela.....		63
Anexo E: Documento LLD (Lower Level Design) entregable diseño.....		64
Anexo F: Configuración de los dispositivos de la red.....		66
Anexo G: Implementación del Agile Controller Campus e Implementación del eSight Campus.....		75
Anexo H: Cobertura inalámbrica.....		98

LISTA DE FIGURAS

<i>Figura 1 Agregación de enlaces</i>	14
<i>Figura 2 Alta Disponibilidad conexión</i>	15
<i>Figura 3 Factores que contribuyen a la calidad de servicio global</i>	17
<i>Figura 4 Diseño clásico jerárquico de red</i>	19
<i>Figura 5 Clásica solución de gestión centralizada</i>	20
<i>Figura 6 Stacking Switches.....</i>	22
<i>Figura 7 Topología General detalle Campus Miraflores.....</i>	24
<i>Figura 8 Topología de alto nivel Nueva Red de Campus.....</i>	25
<i>Figura 9 Conexiones Switches Core a Switches Acceso.....</i>	30
<i>Figura 10 Conexiones Switches Core a Controladores AC6508.....</i>	31
<i>Figura 11 Conexiones Switches Core a Switches Servidores</i>	32
<i>Figura 12 Conexiones Switches Servidores a las plataformas</i>	33
<i>Figura 13 Conexiones Switches Multigigabit a AP y usuarios.....</i>	34
<i>Figura 14 Conexiones Switches Acceso PoE – Red Paralela</i>	35
<i>Figura 15 Control de Acceso a la Red - NAC</i>	36
<i>Figura 16 Conexión Switches Servidores - Agile Controller Campus</i>	38
<i>Figura 17 Conexiones entre el Switch Servidor y el equipo eSight.....</i>	42
<i>Figura 18 Rack Layout ubicación de equipos</i>	44

LISTA DE TABLAS

Tabla 1 Nombre Equipos de Red Campus	27
Tabla 2 Versiones de software de los equipos	28
Tabla 3 Asignación de redes para Campus Miraflores	29
Tabla 4 Datos servidor Taishan 200 - Agile.....	37
Tabla 5 Parámetros físicos del servidor TaiShan 200 - Agile	37
Tabla 6 Sistema operativo servidor Agile	37
Tabla 7 Mapeo de puertos servidores Agile	39
Tabla 8 Conexiones Servidores Agile.....	39
Tabla 9 Usuarios y contraseñas por default Agile	40
Tabla 10 Datos servidor Taishan 200 - eSight	41
Tabla 11 Parámetros físicos del servidor TaiShan 200 - eSight.....	41
Tabla 12 Sistema operativo servidor eSight	41
Tabla 13 Mapeo de puertos servidor eSight.....	42
Tabla 14 Usuarios y contraseñas por default eSight	43
Tabla 15 Costo dispositivos Red de Campus	48

CAPITULO I: INTRODUCCIÓN

Las mejoras en la implementación de conectividad en una red empresarial, de Campus, se manifiestan en la mejora de las comunicaciones, así como el orden y distribución de los dispositivos de las diferentes capas en lo que se conoce como un diseño jerárquico de red.

En la tecnología de redes, un diseño jerárquico implica dividir la red en capas, donde los dispositivos están ubicados en niveles según la función que desempeñan. Cada nivel proporciona funciones específicas para los dispositivos correspondientes.

Un diseño jerárquico de red de campus, ayuda a definir las características de hardware y software adecuados para así definir la cantidad de equipos de networking que serán necesarios para llevar a cabo las funciones específicas de cada capa de red.

Un diseño típico de red jerárquica de campus empresarial incluye tres principales capas, las cuales son la Capa de Acceso, Capa de Distribución y finalmente la Capa de Core.

El proyecto de diseño de la nueva red de campus de la empresa Niubiz de su red empresarial en Lima, Perú, transportará los servicios de usuarios finales a través de los dispositivos, en sus redes LAN y WLAN, e incluye la gestión centralizada de los equipos y el acceso centralizado y seguro a la red vía un servidor de Network Access Control (NAC).

Este informe cuenta con la siguiente Organización:

- El Capítulo I desarrolla la introducción del trabajo de suficiencia profesional para el diseño de una red de campus en un entorno corporativo.
- El Capítulo II brinda información sobre el lugar donde se desarrolló la actividad que sustenta el presente trabajo de suficiencia profesional.

- El Capítulo III trata sobre toda la actividad desarrollada en el proyecto de diseño que fui parte, todo esto planteado en un esquema según las pautas del trabajo de suficiencia profesional, donde en el capítulo se trabajan los puntos como los objetivos, la problemática, la metodología empleada, la teoría y todo el diseño de red que se planteó en el proyecto.
- El Capítulo IV desarrolla las conclusiones del trabajo, así como la justificación, una evaluación final con respecto al presupuesto, evaluación técnica, descripción para una futura implementación del Servidor de Control de Acceso (NAC) y del servidor de Gestión Centralizada (eSight).
- El capítulo V del presente trabajo brinda unas recomendaciones de buenas prácticas para la institución financiera.
- El capítulo VI desarrolla la bibliografía de la cual se basó el presente trabajo de suficiencia profesional.
- El capítulo VII se muestran los anexos que se hacen referencia en el presente documento.

CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución – Actividad que desarrolla

La actividad se desarrolló para la empresa Niubiz.

2.2 Periodo de duración de la actividad.

Las actividades se realizaron desde el 01 de julio del 2020 al 05 octubre del 2020

2.3 Finalidad y objetivos de la entidad

La empresa Niubiz brinda servicios relacionados con pagos digitales, contribuyendo con la digitalización de la economía, mediante diferentes opciones de pagos.

2.4 Razón social

La razón social de la empresa es COMPAÑIA PERUANA DE MEDIOS DE PAGO S.A.C

2.5 Dirección postal

Dirección: Av. Jose Pardo Nro. 831. Miraflores, Lima - Perú

2.6 Correo electrónico del profesional a cargo.

El profesional que supervisó el desarrollo del proyecto fue el Ingeniero James Cusco de Huawei. Correo: james.cusco@huawei.com

CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

Las actividades del proyecto, informe de Trabajo de Suficiencia profesional fueron:

- Revisión del Background Técnico de la organización, donde se definen los conceptos básicos de conectividad de red, topologías, protocolos y acceso inalámbrico en una red de Campus.
- Descripción de la nueva Red Campus.
- Licenciamiento Software equipos.
- Servicios en la Red de Campus (Vlans y redes definidas para los servicios).
- Diseño de la red y conexiones (Port mapping de los dispositivos y la distribución de los equipos en los racks).
- Tecnología de Control de acceso a la red (NAC).
- Plataforma de Gestión eSight Huawei.
- Plantillas de configuración de los protocolos a usarse en los dispositivos de la red de campus.

3.2 Problemática

Las instituciones que implementaron sus redes de entornos empresariales existentes tienen nuevas amenazas técnicas debido a las nuevas aplicaciones y dificultan la gestión de los recursos de la red en, haciéndolas menos eficientes. Las redes previas se diseñaron sin tomar en cuenta criterios de diseño importantes como la escalabilidad, la alta disponibilidad, la velocidad de conexión, la seguridad de los equipos de la red y de los usuarios.

3.2.1 Problema General

¿Cómo actualizar el diseño de una red de campus corporativa de la empresa Niubiz para que brinde servicios de comunicaciones de calidad global?

3.2.2 Problemas Específicos

- ¿Cómo garantizar la seguridad para los recursos de la red cuando necesiten ser accedidos?
- ¿Cómo se puede obtener una gestión centralizada de los equipos de red?
- ¿Cómo se puede lograr un control de acceso a la red para los usuarios finales?
- ¿Cómo atender la creciente demanda de cobertura para la comunicación en la red de campus de la sede central?
- ¿Cómo lograr un diseño de red de campus escalable?

3.3 Objetivos

En síntesis, la red a implementar debe garantizar que las comunicaciones sean calidad global, es decir técnicamente, sin interrupciones y de manera segura, soportada por una gestión centralizada de los equipos de red (networking) y el control seguro para el acceso a la red.

3.3.1 Objetivo General

Diseñar una red de campus corporativa para la empresa Niubiz que brinde servicios de calidad global considerando criterios de escalabilidad, disponibilidad y velocidad de conexión de los equipos.

3.3.2 Objetivos Específicos

- Proporcionar una mayor seguridad para los recursos de la red cuando necesiten ser accedidos a partir de la administración de políticas de seguridad en los dispositivos de la red.
- Garantizar la gestión de los equipos de red implementando una solución centralizada que gestione los dispositivos de networking.
- Implementar el control de acceso a la red para los usuarios configurando políticas de autorización y autenticación.
- Garantizar la mejora de la cobertura mediante el despliegue de conexiones alámbricas e inalámbricas para los equipos que se conectan a los diferentes puntos de acceso inalámbrico.
- Diseñar una red que sea escalable considerando dispositivos de networking para futuras expansiones de la red.

3.4 Justificación e importancia de la investigación

3.4.1 Justificación técnica:

Este trabajo tiene como justificación técnica el de renovar la red actual de la entidad financiera Niubiz a una nueva red de campus que brinde servicios de calidad global.

- Como justificación operativa es necesario este trabajo debido a que en este nuevo diseño de red se va a brindar una solución para el control de acceso a los usuarios, ya sean usuario corporativos o invitados y así poder realizar un monitoreo y definir límites en el acceso de los usuarios. Se afirma en documento (Soporte Huawei - 2022. Agile Controller Documentation)

- Como justificación económica, es necesario este nuevo diseño de campus debido a que en la red actual la empresa está expuesta a amenazas externas ya que no se cuenta con políticas de seguridad ni un diseño seguro, lo que conllevaría a pérdidas económicas para la empresa. (García, 2007)

La renovación y rediseño de las redes de entornos corporativos es una política técnico-operativa de todas las empresas migrando a redes basadas en una nueva arquitectura de red para entornos corporativos, que considera alta disponibilidad, capacidad de ancho de banda, calidad de servicio, cobertura, acceso a la red y seguridad., que permitirán la implementación de nuevas soluciones, generando una mejor experiencia de usuario. Se afirma en documentos (Cabral, 2020. Obis, 2014)

3.4.2 Justificación operativa:

Como justificación operativa, es necesario el nuevo de diseño de red de campus debido a que en este nuevo diseño se obtendrá mejoras en los siguientes aspectos técnicos:

- Se configura protocolos seguros, como los protocolos HTTPS y SSH, para la gestión de los dispositivos de la nueva red corporativa. (Configuración de los protocolos se muestra en Anexo F. (Documentación proveedor Huawei)
- Se implementa la solución de gestión centralizada para los dispositivos de networking de la red. (Se afirma en documento de proveedor. Huawei – 2022. Esight Documentation).
- Se implementa la solución de control de acceso a la red con políticas de seguridad para los usuarios finales que necesiten acceder. (Se afirma en documento de proveedor. Huawei – 2022. Agile Controller Documentation).
- Se logra una red escalable considerando los equipos switches y Access Points con amplia capacidad de puertos y conexiones. (Se afirma en documento de proveedor. Huawei – 2022. Switches Documentation)

3.5 Metodología

3.5.1 Antecedentes

García (2007) enfatiza la importancia de aplicar conceptos de seguridad en las redes o sistemas informáticos, que se alcanza considerando cuatro pilares como la respuesta a incidentes, prevención y monitoreo, sistemas de gestión y nuevas redes/servicios, y concluye que:

- La gestión de la seguridad en las redes corporativas aún es limitada en muchas empresas, debido a la falta de conciencia de la importancia, de los directivos, para implementar estos sistemas.
- En toda organización es importante reconocer que los incidentes de seguridad, que se perpetran a través de los ataques, solo pueden ser mitigados, y cuanto más prontamente se enfrenten disminuirán los riesgos de ataques.
- Si no existe un sistema de gestión de seguridad de los activos, así como el control respectivo, la empresa será vulnerable a estos ataques que ocasionarán interrupción del servicio, lo que genera pérdidas económicas en el sector de banca y finanzas.

Cabral (2020) presenta una solución para el despliegue y mantenimiento de la infraestructura completa de una sede corporativa, en la que se desea potenciar los servicios de la red corporativa, además de establecer una mejor integración con el resto de la Intranet de dicha entidad. El estudio concluye que:

- La metodología de ITIL brinda un orden de cada tarea, la cual se estudia y valida previamente, de tal manera que los trabajos no afectan a los usuarios finales.
- La estructura diseñada es fácilmente escalable, estando preparada para poder atender a un mayor número de usuarios.

Obis (2014) trata sobre la implementación de una red IP de datos y voz, basándose en diferentes niveles de infraestructura de comunicaciones de Red y equipamientos de voz y datos, para 4 sedes corporativas de una entidad, concluye que:

- La solución unifica 3 servicios (WAN, LAN y VOZ IP), logrando una convergencia entre estos tres servicios.
- A nivel LAN se ha mejorado la administración de la red, ya que ahora se cuenta con una gestión centralizada y es más fácil gestionar los recursos de la red.
- Se logró obtener un sistema de voz con capacidad de realizar llamadas de videoconferencia.

Ávila, Allauca. (2022) proponen y describen los principales problemas de ciberseguridad a nivel de infraestructura de red con los que actualmente los clientes corporativos se ven amenazados, para finalmente definir un conjunto de recomendaciones para mitigar las distintas amenazas en las redes corporativas. El estudio concluyó en los siguientes puntos:

- A partir de los problemas ciberseguridad que presentan los clientes corporativos, se concluye que con ayuda de la norma ISO 27032, se obtienen mayor seguridad en las comunicaciones de redes en entornos corporativos.
- Los estudios comparativos de diferentes ataques de ciberseguridad a clientes corporativos permitieron conocer que el mayor ataque al que se ven afectado dichos clientes son Ataque de denegación de servicio (DoS).
- La definición de recomendaciones en redes LAN de clientes corporativos, así como el análisis de normas y estándares internacionales, son la base para las mejores prácticas de seguridad a aplicar en entornos corporativos y disminuir la afectación de un ataque de red.

3.5.2 Bases teóricas

Las “redes de campus” se definen como una infraestructura de red que brinda acceso a servicios y recursos de comunicación de red a usuarios finales y dispositivos que se distribuyen en una ubicación geográfica, se diseñan para mejorar la conectividad de una red de datos en universidades, entornos corporativos e industriales. Las redes de área de campus brindan más control sobre los recursos de la red y se basan en una gestión centralizada al que se conectan todos los recursos de la red.

Las redes de área de campus proporcionan una forma sencilla para que las organizaciones controlen sus recursos de red, centralicen sus esfuerzos de seguridad y compartan datos rápidamente.

- El diseño de red de campus, consta de los elementos integrados que comprenden el conjunto de servicios utilizados por un grupo de usuarios y dispositivos de estación final que comparten el mismo medio de comunicación. Estos incluyen los servicios de transporte de paquetes (alámbricos e inalámbricos), la identificación y el control del tráfico (seguridad), la supervisión y gestión del tráfico. Estas funciones básicas se implementan de tal manera que brindan y respaldan directamente los servicios de nivel superior proporcionados por la organización para uso de los usuarios finales.
- La topología de red refiere al diseño general de la red, que suelen ser el inicio del proceso de diseño. Un diagrama de red es una representación espacial de la red e integra información referida a conexiones físicas; cantidad, tipo y ubicación de todos los dispositivos y terminales; direccionamiento IP; y procesos y arquitectura de seguridad. Al construir una red desde cero, el primer paso es armar una lista de todos los activos, puntos finales, usuarios, dispositivos, LAN y otros elementos de la red.
- Para el diseño de la red de campus, se toma en cuenta el modelo jerárquico de tres capas, la cual es un conjunto de recomendaciones que describen cómo se debe diseñar una red de campus. Este modelo

sugiere que, en lugar de diseñar una red de campus plana, se debe diseñar una red jerárquica. El modelo de red jerárquico contiene tres capas las cuales son: Capa de Acceso, Capa Distribución y Capa Core.

- Capa de Acceso: Proporciona acceso a la red para los grupos de trabajo y los usuarios. Los dispositivos en esta capa brindan acceso alámbrico o inalámbrico.
 - Capa de Distribución: Proporciona una conectividad basada en políticas y controla el límite entre las capas de acceso y de Core. Estos dispositivos suelen ser switches capa 3 en los que se configuran políticas de calidad de servicio.
 - Capa de Core: Proporciona un transporte rápido entre los switches de distribución dentro del campus empresarial. Estos dispositivos, en la mayoría de casos en diseño jerárquicos, son routers con mucha capacidad de procesamiento.
- La topología de red designa la disposición de equipos, nodos y enlaces de una red de campus. Los tipos de topologías de red son:
 - Topología de bus. La topología de bus conecta cada dispositivo en la red a un cable principal común, creando una única ruta de comunicación para todos los nodos.
 - Topología de anillo. Los dispositivos en una topología de anillo están interconectados en un patrón circular o similar a un anillo, que forma un circuito cerrado.
 - Topología en estrella. En una red de topología en estrella, todos los dispositivos se vinculan directamente a equipo central, que actúa como punto de conexión central.
 - Topología de malla. En una topología de malla, los canales de red conectan cada nodo con todos los demás nodos que pertenecen a la topología.
 - Topología de árbol. Una topología de árbol consta de una estructura jerárquica que se asemeja a un árbol. En este tipo de topología de red, un nodo central se conecta a uno o más nodos, que a su vez se conectan a nodos adicionales.

3.5.3 Mejores prácticas de diseño de red

- **Diseño para la seguridad**

La seguridad de la red debe incorporarse durante las primeras etapas de diseño, no reforzarse más tarde. Si la seguridad no se tiene en cuenta en el diseño, las herramientas de seguridad incompatibles pueden afectar el rendimiento de la red, la experiencia del usuario y la capacidad de administración.

- **Diseño para la resiliencia**

Este proceso comienza con la creación de una lista de los desafíos de resiliencia que enfrenta una organización, como incidentes de seguridad y problemas de red.

- **Diseño para la escalabilidad**

Se evalúa que tipo de escalamiento es necesario para la organización, como agregar usuarios de manera constante y reducir rápidamente los servicios para adaptarse a flujos de trabajo específicos.

- **Diseño para la visibilidad**

Un sistema de gestión de red centralizada puede ayudar a proporcionar visibilidad en la red, lo que facilita la detección de problemas potenciales.

- **Diseño para la sostenibilidad**

Para diseñar una red sostenible, se puede implementar un sistema de Gestión y sostenibilidad energética global. Las iniciativas incluyen la reducción de las emisiones de gases de efecto invernadero y la implementación de características energéticas para reducir la demanda mundial de energía.

3.5.4 Marco conceptual

La nomenclatura y conceptos utilizados en el diseño y tratamiento de las redes y sus componentes son variados y por ello requieren precisarlos, en el sentido en que se utilizan en este proyecto.

- **Agregación de enlace.**

Se definió la agregación de enlaces (link aggregation) como la combinación de múltiples conexiones físicas de red en paralelo para transformarse en una sola conexión lógica. La agregación de enlaces aumenta el rendimiento total más allá de lo que podría soportar una sola conexión y proporciona redundancia donde todos menos uno de los enlaces físicos puede fallar sin perder la conectividad, esto aumenta el ancho de banda del enlace. Un grupo de agregación de enlaces (LAG) es la combinación de puertos físicos. La agregación de enlaces proporciona mecanismos de respaldo de enlaces, lo que mejora en gran medida la confiabilidad del enlace y también balanceo de carga. Quintero (2018). IEEE (1997).

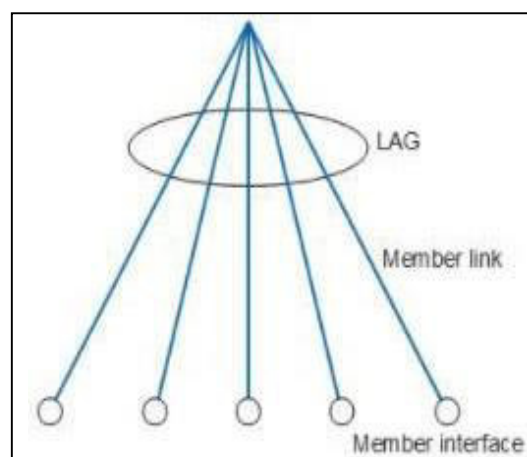


Figura 1: Agregación de enlaces. Fuente: Portal Soporte Huawei

- **Alta Disponibilidad.**

La alta disponibilidad significa que un sistema, componente o aplicación de TI puede funcionar a un alto nivel, de forma continua, sin intervención, durante un período de tiempo determinado. La infraestructura de alta disponibilidad está configurada para brindar un rendimiento de calidad y manejar diferentes cargas y fallas con un tiempo de inactividad mínimo o nulo. La alta disponibilidad (High Availability) es la eliminación de puntos únicos de falla para permitir que las aplicaciones continúen funcionando incluso si falla uno de los

componentes de la red, como un servidor, un switch, un router, etc. Oggerino, Cisco (2001). Hendel (1997).

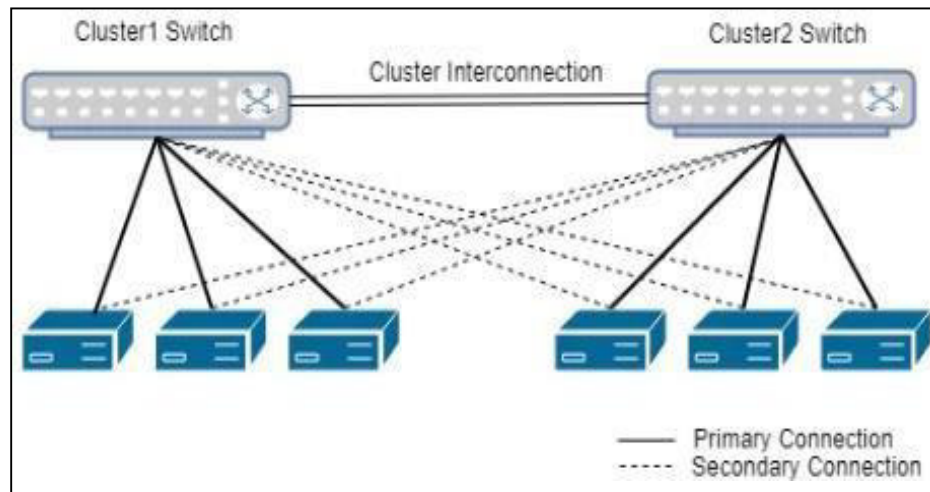


Figura 2: Alta Disponibilidad de conexión. Fuente: Portal Soporte Huawei

• Calidad de Servicio

La “calidad de servicio” es definida por la Unión Internacional de Telecomunicaciones (UIT) como el efecto global de la calidad de funcionamiento de un servicio que determina el grado de satisfacción de un usuario de dicho servicio.

La regulación con respecto a la calidad de servicio en la prestación de los servicios de telecomunicaciones, se establece en la norma IET/1090/2014 (Orden de Calidad) y busca los siguientes objetivos:

- Facilitar la transparencia con herramientas que muestren el estado de los dispositivos de la red.
- Garantizar niveles mínimos de calidad de Servicio determinado por políticas de seguridad.
- Mecanismos de compensación en caso de incumplimiento del Acuerdo de Nivel de Servicio a partir del monitoreo.
- Verificar siempre si haya alguna caída en la red que afecte la calidad del servicio.
- Velocidad de transmisión de datos con dispositivos de gama

alta y políticas de QoS. Ministerio Transformación Digital (2023)

- **Calidad de Servicio global**

La figura N° 3 considera los factores que contribuyen, en conjunto a la calidad de servicio global. La contribución de la red a la calidad de servicio tiene tres conceptos de calidad de funcionamiento:

- Facilidad de utilización (de un servicio), incluidas las características del equipo terminal, la inteligibilidad de tonos y mensajes, etc.
- Tiempo de respuesta (de un servicio), describe la respuesta de la red durante el establecimiento, la retención y la liberación de una conexión de servicio. Conjuga la aptitud de ser obtenido cuando se solicite y continuar siendo prestado con la duración deseada, con las tolerancias y condiciones especificadas.
- La integridad del servicio, que es mantener el grado de servicio sin degradaciones excesivas. Se refiere al nivel de reproducción de la señal transmitida en el receptor.

UIT (2007)

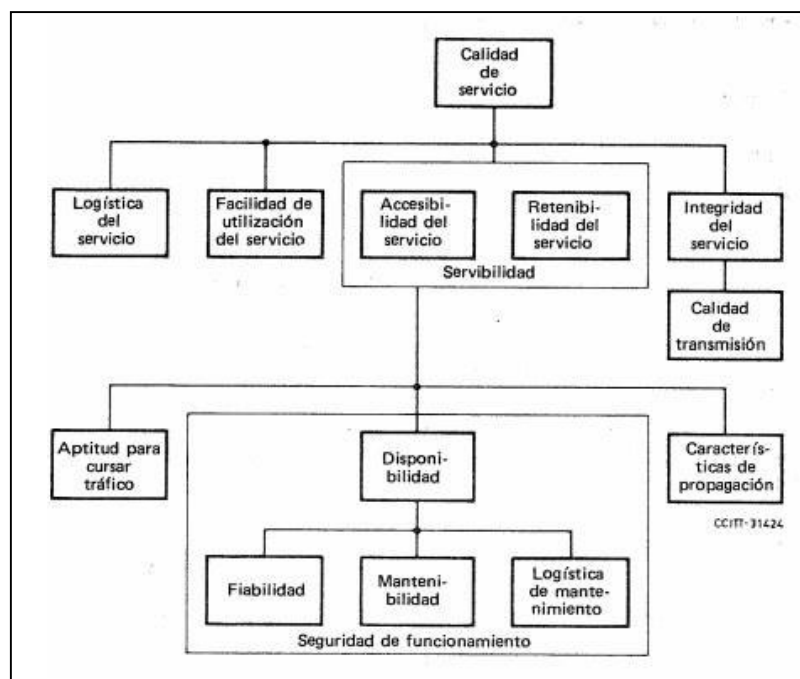


Figura 3: Factores que contribuyen a la calidad de servicio global. Fuente: UIT 2007

- **Capa de Enlace de datos Capa 2 del modelo OSI.**

Capa ubicada entre la capa física (1) y la capa de Red (3) proporciona transferencia de tramas de paquetes entre dos dispositivos conectados físicamente, estableciendo el protocolo para el control de flujo entre ellos, para establecer y terminar una conexión entre dos dispositivos conectados físicamente. ITU-T, OSI (1984).

- **Capa de red, capa 3 del modelo OSI**

Está ubicado entre la capa de Enlace de Datos y la capa de Transporte. Proporciona los medios funcionales y de procedimiento para transferir paquetes de un nodo a otro conectado en "diferentes redes", direccionando los paquetes y encargándose de su entrega. En esta capa se agrega direcciones lógicas a los paquetes entregados por la capa de enlace de datos. ITU-T, OSI (1984)

- **Conectividad.**

Es el extenso proceso de conectar, de manera cableada o inalámbrica, varias partes de una red entre sí y crear un vínculo entre diferentes dispositivos mediante el uso de routers, switches y gateways. Peter Barry, Patrick Crowley (2012)

- **Control de Acceso.**

Las soluciones de control de acceso a la red, o NAC, son soluciones que admiten la visibilidad de la red y la gestión del acceso a través de la aplicación de políticas en dispositivos y usuarios de redes corporativas. Un sistema NAC puede denegar el acceso a la red a los dispositivos que no cumplen con los requisitos, colocarlos en un área en cuarentena o brindarles solo acceso restringido a los recursos informáticos, evitando así que los nodos inseguros infecten la red. Hay muchas herramientas NAC disponibles y las funciones a menudo las realiza un servidor de acceso a la red. Se definen las políticas de seguridad que deciden qué dispositivos o aplicaciones cumplen con los requisitos de seguridad de punto final y se le permitirá el acceso a la red. Las soluciones NAC ayudan a las organizaciones a controlar el

acceso a sus redes a través de capacidades como la creación de perfiles y visibilidad, acceso a la red de invitados, respuesta rápida ante incidentes y la evaluación del cumplimiento de la política de seguridad por tipo de usuario o tipo de dispositivo. Fitzgerald, Foley y Foghlú (2008).

- **Diseño de red Jerárquico.**

Diseño que separa una red en distintas capas, donde cada una tiene funciones que definen su rol en la red. Debido a esto se puede elegir el hardware, el software y las funciones para asumir un rol particular para esa capa de red. La gestión de datos es muy eficiente.

En un diseño jerárquico, el tráfico local permanece local y solo pasa a una capa superior cuando se dirige a otra red. Cisco (2002)

Una red jerárquica de tres capas consta de:

- Capa Core. Esta es la columna vertebral de la red. Ofrece un transporte rápido entre los switches de distribución de la red.
- Capa de Distribución. Esta capa intermedia ofrece conectividad basada en políticas y regula el límite entre las otras dos capas. Es donde se lleva a cabo el enrutamiento y el filtrado de datos.
- Capa de acceso. Donde los dispositivos finales locales acceden a la red vía alámbrica o de manera inalámbrica.

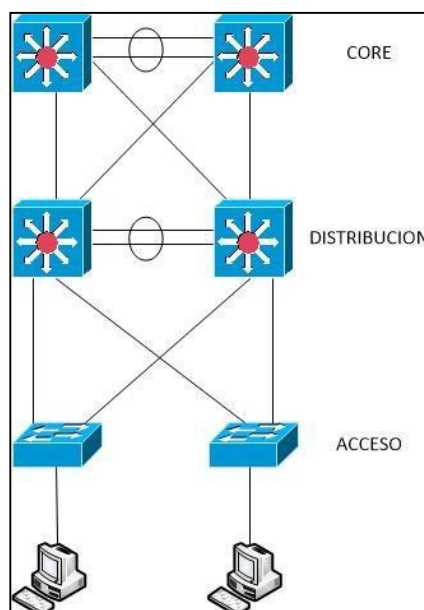


Figura 4: Diseño clásico jerárquico de red. Fuente: Diseño de Red Cisco 2002

- **Gestión Centralizada.**

Hace referencia a la gestión centralizada cuando todos los datos de administración (pings, SNMP, etc.) se envían desde un único sistema/ servidor de administración. Una red corporativa suele estar formada por muchos dispositivos de red y estaciones de trabajo, por lo que, con la gestión de red centralizada, todo esto se puede gestión

ar desde una única estación de control o servidor. Un servidor que realice esta función de administración de dispositivos de red permitiría que los dispositivos (como switches, routers, firewalls y dispositivos WLAN) se conecten a este servidor para la gestión centralizada. Un servidor de gestión de red centralizada debe proporcionar funciones de gestión básicas, como gestión de alarmas y rendimiento para dispositivos conectados; así como la de supervisar los dispositivos de forma visualizada en pantalla. James D. McCabe (2007).

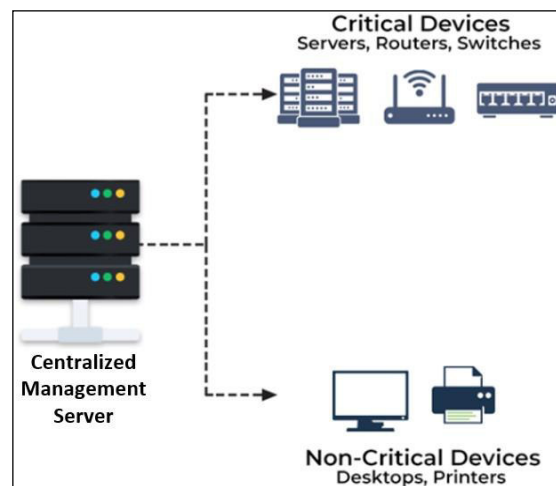


Figura 5: Clásica solución de gestión centralizada. Fuente: Elaboración Propia

- **Redes de área local (LAN).**

Son redes que tienen la capacidad de transmisión de alta velocidad, para una transferencia de datos entre dispositivos finales, como

computadoras ubicadas en un solo edificio o en un solo sitio. Una LAN también puede incluir una conexión (switch) a otra LAN y una conexión (gateway) a redes fuera de la LAN. IEEE (1991)

- **Red Wireless Local Area Network (WLAN)**

Se refiere a las redes de área local inalámbricas compuesta por puntos de acceso inalámbrico e infraestructura asociada, dentro de un límite área geográfica, como un edificio de oficinas o campus, que utilizan enlaces de radio de alta frecuencia. Las WLAN son usualmente implementadas como extensiones de redes LAN cableadas para mejora en la movilidad del usuario conectado. Flickenger (2005)

- **Seguridad de Redes.**

Se definió la seguridad de la red como la protección de la infraestructura de red contra el acceso no autorizado, el uso indebido o el robo. Implica crear una infraestructura segura para que los dispositivos, los usuarios y aplicaciones funcionen de manera segura. La seguridad de la red combina múltiples capas de defensas en el perímetro y en la red. Cada capa de seguridad de la red implementa políticas y controles. Los usuarios autorizados obtienen acceso a los recursos de la red, pero los actores maliciosos no pueden realizar ataques y amenazas. La seguridad de red es un término que describe soluciones de hardware y software, así como procesos o reglas y configuraciones relacionadas con el uso de la red, la accesibilidad y la protección general contra amenazas. IEEE (2005).

- **Stacking Switch.**

El apilamiento de switches (Stacking switch) es una tecnología que conecta varios switches a través de cables de pila para formar un conmutador lógico para el reenvío de datos. Como tecnología de virtualización horizontal ampliamente utilizada, puede mejorar la confiabilidad, aumentar la cantidad de puertos, aumentar el ancho de banda y simplificar las redes. Los switches apilables se pueden agregar o quitar de un stack según sea necesario sin afectar el rendimiento general del stack. Dependiendo de la topología, una pila

(stack) puede continuar transfiriendo datos incluso si falla un enlace o una unidad dentro de la pila. Esto hace que el apilamiento sea una solución efectiva, flexible y escalable para expandir la capacidad de la red. Netgear Inc (2001).

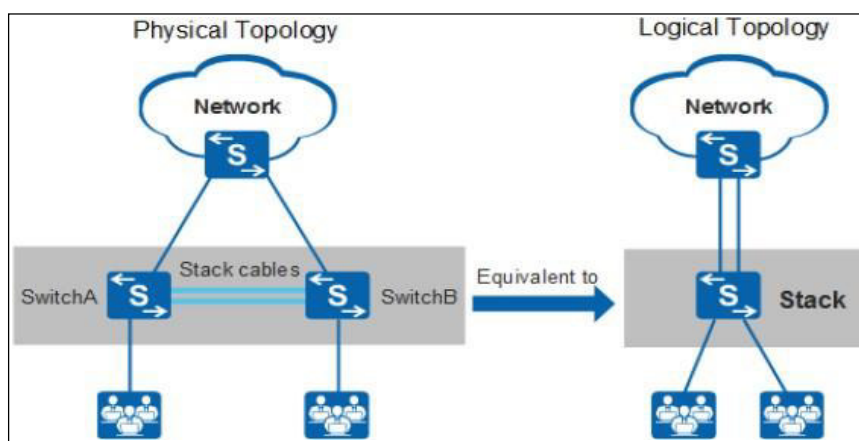


Figura 6: Stacking Switches. Fuente: Portal Soporte Huawei.

- **Subneteo de Redes**

Hace referencia al network subnetting como el proceso de dividir las direcciones IP en subunidades más pequeñas que luego se pueden asignar a varios dispositivos de red en una red, esto se denomina división en subredes. La división en subredes permite que la red evite los frecuentes problemas de tráfico que ocurren en las de datos, lo que da como resultado una transmisión fluida de la información en la red. Las unidades de red más pequeñas, también conocidas como subredes, se pueden configurar individualmente según los requisitos del usuario. Paul Browning (2018)

- **Telefonía IP - Voz sobre IP (VoIP).**

Servicio que permite la transmisión de la voz utilizando una red de datos, en una red LAN o a través de internet; facilita las comunicaciones internas de una empresa y en videoconferencias. Las llamadas VoIP son independientes de las telefónicas convencionales y no están sujetas a una tarifa telefónica. Carballar (2008)

- **VLAN.**

Se define a las redes VLAN, como su mismo nombre lo dice, una LAN virtual (VLAN) que es una red lógica que agrupa un subconjunto de dispositivos que comparten una LAN, aislando el tráfico para cada grupo. Una VLAN, opera en la Capa 2 de la red, el nivel de Ethernet. Las VLAN dividen una sola red conmutada en un conjunto de redes virtuales superpuestas que pueden cumplir diferentes requisitos funcionales y de seguridad. Esta partición evita la necesidad de tener múltiples redes físicas distintas para diferentes casos de uso. Las vlans se pueden implementar atendiendo al criterio de puertos de un switch. Las VLAN cumplen distintos requerimientos como el de mejorar el rendimiento de la red, reforzar la seguridad y facilitar la administración de los dispositivos. Las VLAN dividen los dominios de broadcast. IEEE (2005).

3.6 Procedimiento

El proyecto para la empresa financiera Niubiz consiste en construir una red de campus para la oficina principal en Miraflores e implementar varios servicios, como la comunicación de usuarios internos con los distintos servicios existentes y proporcionar las mejores prácticas para su futura implementación.

3.6.1 Introducción de la Red

La oficina Miraflores de la empresa Niubiz tiene usuarios corporativos de las diversas áreas operativas y administrativas; cuenta con una salida a internet para los usuarios corporativos e invitados en Miraflores.

3.6.2 Topología General de la Red Campus Miraflores

A partir del diseño planteado para la nueva red de campus de la entidad

financiera, desarrollado en los capítulos previos donde se mostraron las conexiones entre los equipos de networking a ser implementados en la nueva red de campus. A continuación, se muestra el diseño a detalle de la topología general de la nueva red de campus Miraflores.

La topología General a detalle del Campus Miraflores se observa en el **Anexo A** del presente documento.

3.6.3 Descripción de la nueva red de Campus

El proyecto de diseño de nueva red de campus Miraflores se desarrolló a partir de un requerimiento de una red de Campus, consistente en: Una capa de dos Switches Core, una capa de Switches Acceso Multigigabit, dos Switches Servidores Multigigabit, dos Controladores de Acceso, un Servidor NMS (eSight), dos servidores NAC (Agile-Controller Campus y equipos de acceso AP wifi para los usuarios corporativos.

En una red paralela existente se diseñó un despliegue de dos switches Distribuidores conectados a Switches Acceso PoE que brindan conexión a internet para las cámaras IP, televisores y usuarios invitados. Los dispositivos para esta nueva red de Campus son fabricados por marca Huawei.

Sede Miraflores – Nueva Red de Campus

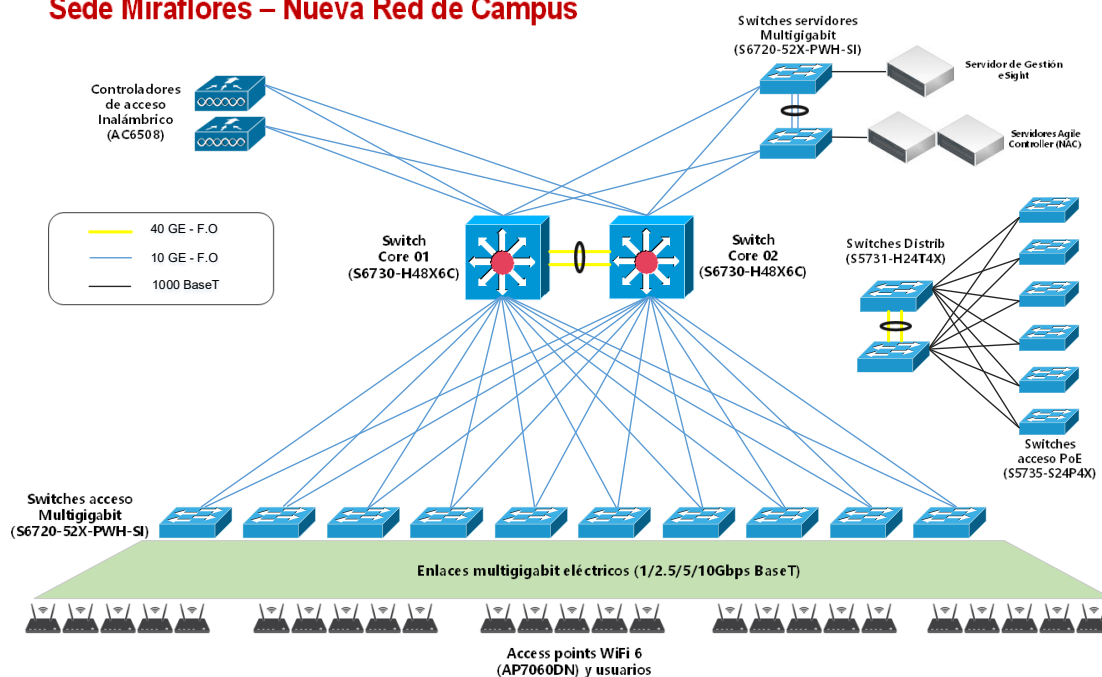


Figura 8: Topología de alto nivel Nueva Red de Campus. Fuente: Elaboración propia

3.6.4 Estandarización

La estandarización es la definición (dispositivo, descripción, rol en la red y hostname) de los equipos que forman parte de la nueva red de Campus Miraflores.

Los componentes, partes de la red, que se listan en el **Anexo B** son:

- Switch Core.
- Switch Acceso/Servidor
- Controlador
- Servidores
- Switch Distribuidor/Acceso
- Punto de acceso (Access Points)

La **Tabla 1** muestra los equipos a ser usados en la Red de Campus

Tabla 1: Nombre Equipos de Red Campus

Dispositivo	Descripción	Rol	Hostname
S6730	Cloud Engine Switch DC	Core	SW-CORE-DC-01
S6730	Cloud Engine Switch DC	Core	SW-CORE-DC-02
S6720	Switch Multigigabit	Acceso	SW-ACC-P07-1
S6720	Switch Multigigabit	Acceso	SW-ACC-P07-2
S6720	Switch Multigigabit	Acceso	SW-ACC-P08-1
S6720	Switch Multigigabit	Acceso	SW-ACC-P08-2
S6720	Switch Multigigabit	Acceso	SW-ACC-P09-1
S6720	Switch Multigigabit	Acceso	SW-ACC-P09-2
S6720	Switch Multigigabit	Acceso	SW-ACC-P10-1
S6720	Switch Multigigabit	Acceso	SW-ACC-P10-2
S6720	Switch Multigigabit	Acceso	SW-ACC-P11-1
S6720	Switch Multigigabit	Acceso	SW-ACC-P11-2
S6720	Switch Multigigabit	Acceso	SW-ACC-P12-1
S6720	Switch Multigigabit	Acceso	SW-ACC-P12-2
AC6508	Access Controller DC	Controlador	AC-CTRL-DC-01
AC6508	Access Controller DC	Controlador	AC-CTRL-DC-02
S6720	Switch Servidor DC	Sw Servidor	SW-SERV-DC-01
S6720	Switch Servidor DC	Sw Servidor	SW-SERV-DC-02
Taishan 2280	Agile Controller Campus	Server NAC	ACS-DC-01
Taishan 2280	Agile Controller Campus	Server NAC	ACS-DC-02
Taishan 2280	eSight Network	Server MGMT	ES-DC-01
S5731	Switch Distribuidor DC	Distribuidor	SW-DIST-DC-01
S5731	Switch Distribuidor DC	Distribuidor	SW-DIST-DC-02
S5735	Switch Acceso PoE	Acceso	SW-PAR-P07-1
S5735	Switch Acceso PoE	Acceso	SW-PAR-P08-1
S5735	Switch Acceso PoE	Acceso	SW-PAR-P09-1
S5735	Switch Acceso PoE	Acceso	SW-PAR-P10-1
S5735	Switch Acceso PoE	Acceso	SW-PAR-P11-1
S5735	Switch Acceso PoE	Acceso	SW-PAR-P12-1
AP7060DN	Access Point	Access Point	AP-P12-1
AP7060DN	Access Point	Access Point	AP-P12-2
AP7060DN	Access Point	Access Point	AP-P12-3
AP7060DN	Access Point	Access Point	AP-P12-4
AP7060DN	Access Point	Access Point	AP-P11-1
AP7060DN	Access Point	Access Point	AP-P11-2
AP7060DN	Access Point	Access Point	AP-P11-3
AP7060DN	Access Point	Access Point	AP-P11-4
AP7060DN	Access Point	Access Point	AP-P10-1

AP7060DN	Access Point	Access Point	AP-P10-2
AP7060DN	Access Point	Access Point	AP-P10-1
AP7060DN	Access Point	Access Point	AP-P10-2
AP7060DN	Access Point	Access Point	AP-P10-3
AP7060DN	Access Point	Access Point	AP-P09-1
AP7060DN	Access Point	Access Point	AP-P09-2
AP7060DN	Access Point	Access Point	AP-P09-3
AP7060DN	Access Point	Access Point	AP-P08-1
AP7060DN	Access Point	Access Point	AP-P08-2
AP7060DN	Access Point	Access Point	AP-P08-3
AP7060DN	Access Point	Access Point	AP-P07-1
AP7060DN	Access Point	Access Point	AP-P07-2
AP7060DN	Access Point	Access Point	AP-P07-3

3.6.5 Versiones de Software de los equipos

Para el diseño de la red de Campus Miraflores se necesitará reemplazar los equipos antiguos con los que cuenta la entidad financiera en su red, estos serán reemplazados por equipos marca Huawei en las diferentes capas de la red de Campus. En la Tabla N° 2 se describen los dispositivos que corresponden, la cantidad, su versión de software recomendada y su función.

Tabla 2: Versiones de software de los equipos

Modelo de Equipo	Cantidad	Versión	Función
AC6508	2	V200R019 C00SP C500	Tiene las funciones de control de acceso wireless. Recibe las solicitudes de conexión de los usuarios conectados a los AP y redirigirá al Agile Controller Campus las solicitudes. Se conecta a los switches Core.
AP7060DN	20	V200R019 C00SP C803	Proporciona acceso vía wireless a los usuarios corporativos
S6730-H48X6C	2	V200R019 C10SP C500	Los dos Switches Core de la red Campus se conectan a los Controladores de Acceso, a los switches distribuidores y a los Switches Acceso Multigigabit
S6720-52X-PWH-SI	14	V200R019 C10SP C500	12 de estos equipos Switches Multigigabit se conectarán a los equipos AP para brindar acceso a la red interna e internet para los usuarios de la red corporativa. 2 de estos switches multigigabit serán switches servidores que se conectarán al eSight, a los Agile Controller y a los Switches Core.
S5731-H24T4XC	2	V200R019 C10SP C500	Son los dos equipos Switches Distribuidores para la red aislada de los usuarios Guest. Estos se conectarán a los Switches Core para pasar una VLAN de Gestión de los equipos.
S5735-S24P4X	6	V200R019 C10SP C500	proporcionan un acceso PoE para los usuarios Guest y conexión a los equipos que pertenecen a esta red en paralelo que es dedicada para televisores y cámaras IP
Agile Controller Campus	2	V100R003 C60SP C208	Equipo Controlador de Acceso a la Red (NAC), que cumple las funciones de controlador de acceso de usuarios de la Red de Campus.
eSight	1	V300R010 C00SP C600	Plataforma de Gestión básica, monitoreo y diagnóstico de la red de Campus.

3.6.6 Servicios Campus Miraflores

En la Tabla N° 3 se describen las vlans y subredes IP correspondientes a la nueva distribución de los servicios que se encuentran en la red de Campus. Se consideraron dos observaciones importantes a desarrollarse en la etapa de migración de los antiguos equipos switches a los nuevos:

- Para el usuario final, el VLAN ID o el segmento IP son indistintos, su relevancia es esencialmente para el control, operación y mantenimiento. Es finalmente el administrador de la red quien define que VLAN ID y segmentos IP usar para su propia LAN.
- Durante escenarios de migración, es opcional para el administrador utilizar esta coyuntura en pro de unificar y ordenar los VLAN ID y segmentos IP a utilizar en su red por un tema de control y facilidad para la resolución de problemas en su red.

Tabla 3: Asignación de redes para Campus Miraflores

Asignación de redes para Campus Miraflores		
Vlan ID	Nombre	Subnet
305	Vlan_Corporativa	10.185.14.0/23
306	Vlan_Corporativa_Wifi	10.185.16.0/23
307	Vlan_IT	10.185.18.0/23
308	Vlan_IT_Wifi	10.185.20.0/23
343	Vlan_Camaras	10.185.34.0/24
344	Vlan_VoIP	10.185.35.0/24
345	Vlan_Mgmt_SW	10.185.36.0/24
346	Vlan_Visitas	10.185.37.0/24
347	Vlan_Visitas_Wifi	10.185.38.0/24
355	Vlan_Solucion_Bank	10.185.39.0/24
505	Vlan_Servicio_Agile	10.185.50.0/28
506	Vlan_Servicio_eSight	10.185.50.16/28
507	Gestion_iBMC_Servers	10.185.50.32/28

3.6.7 Conexiones en la Red Campus Miraflores

En los siguientes subcapítulos, se muestra el diseño de las conexiones de los equipos que pertenecen a la red de Campus, tanto de los equipos que forman parte de las conexiones corporativa, como de la red paralela.

Conexiones Switches Core a Switches Multigigabit Acceso

En la Figura N° 7 se muestra un ejemplo de las conexiones entre los Switches Core y los switches acceso Multigigabit para las conexiones corporativas.

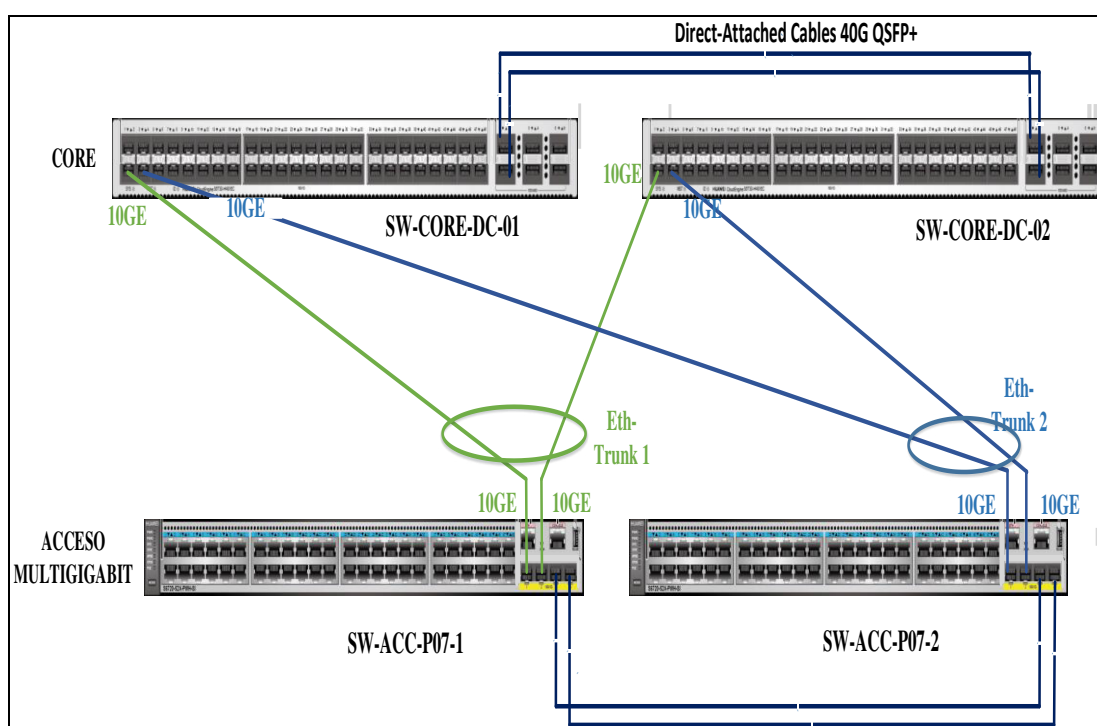


Figura 9: Conexiones Switches Core a Switches Acceso. Fuente: Elaboración propia.

Las conexiones entre los Switches Core DC-01 y DC-02 y los switches Acceso de la Red Corporativa SW-ACC-P07-1 y 2 se harán a través de las interfaces de 10GE ópticas de los equipos S6720. Estas dos interfaces se van a configurar en modo agregación de enlace desde los dos Switches Core para contar con el enlace activo alternativo en caso haya falla en una de las interfaces. Sobre estos enlaces troncales pasan las vlans que correspondan a varios servicios, como Vlan de voz, vlan de datos, vlan de gestión, etc.

El cableado de la conexión entre los equipos Switches Core S6730-H48X6C forman un solo switch lógico a través de una conexión de fibra entre ellos, el tipo de cable de fibra que se utiliza para formar esta conexión entre los dos Switches Core es un Cable de fibra de 40G.

El cableado de la conexión entre los equipos Switches Acceso S6720 para formar un solo switch lógico entre ellos, es un cable de fibra de 10G.

Conexiones Switches Core a Controladores de Acceso

En la figura N° 8 se muestra un ejemplo de las conexiones entre los SwitchesCore y los controladores de acceso AC6508:

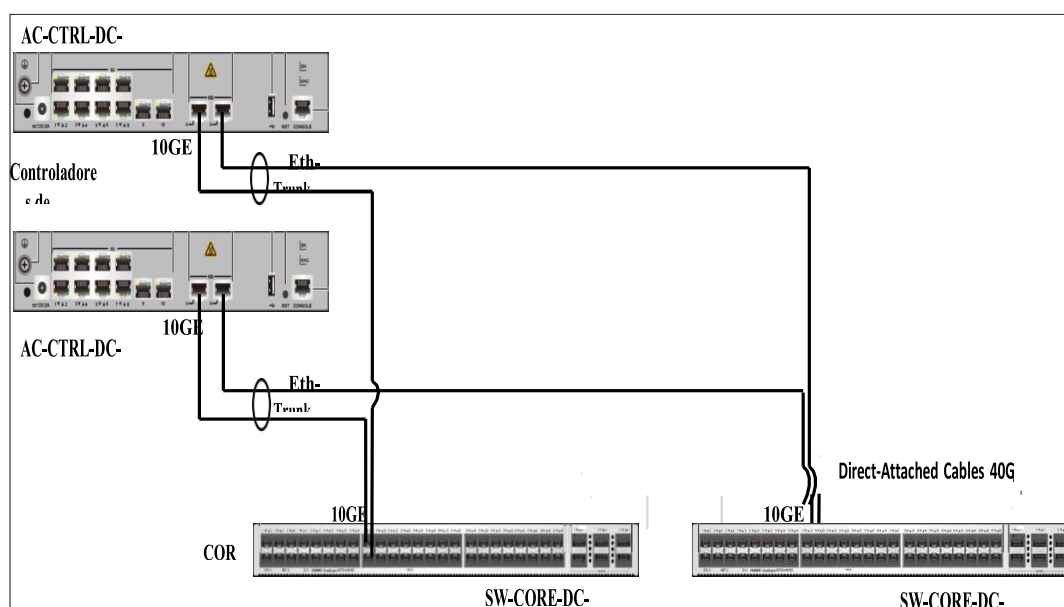


Figura 10: Conexiones Switches Core a Controladores AC6508. Fuente: Elaboración propia

Se observa que las conexiones entre los Switches Core S6730-H48X6C y los Controladores de Acceso serán a través de las interfaces de 10GE ópticas de los equipos AC6508. Estas dos interfaces se van a configurar como un link Aggregation desde los dos switches Core para contar con el enlace activo en caso haya una falla en alguna de las interfaces en estas conexiones.

Sobre estos enlaces troncales se van a dejar pasar las vlans que correspondan a servicios y gestión del equipo AC6508.

Conexiones Switches Core a Switches Servidores

En la figura N° 9 se muestra un ejemplo de las conexiones entre los SwitchesCore y los Switches Acceso a los Servidores:

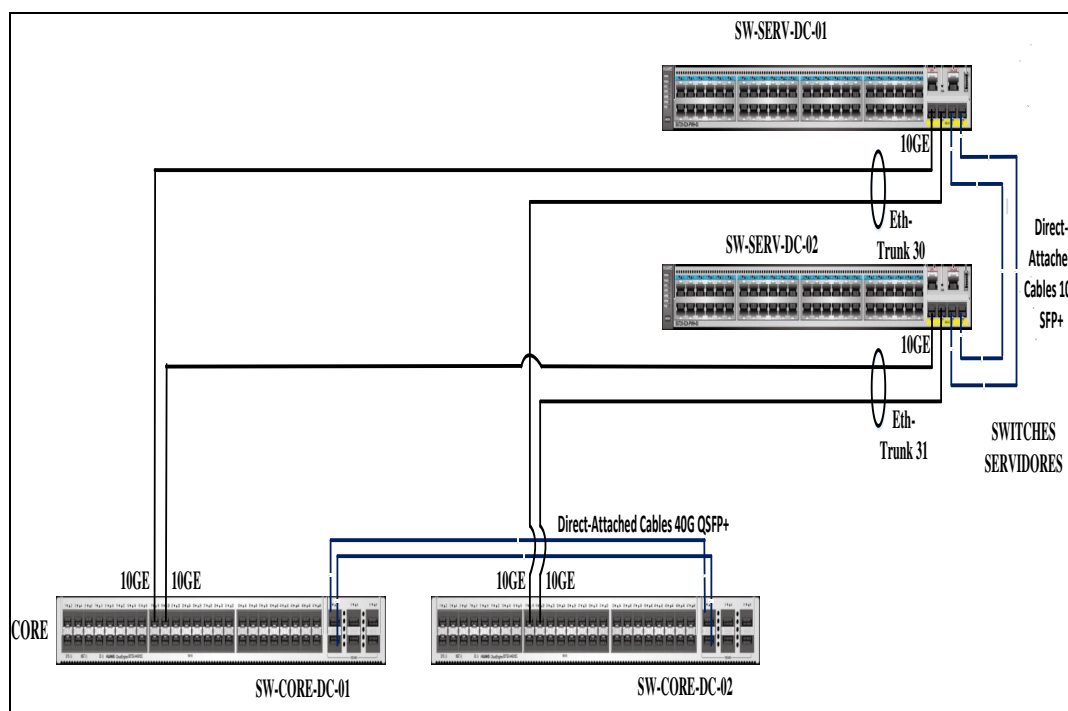


Figura 11: Conexiones Switches Core a Switches Servidores. Fuente: Elaboración propia

Se observa que las conexiones entre los Switches Core S6730-H48X6C y los switches Servidores S6720-52X-PWH-SI serán a través de las interfaces de 10GE ópticas de los equipos S6720. Estas dos interfaces se van a configurar como un link Aggregation desde los dos Switches Core para contar con el enlace activo en caso haya una falla en alguna de las interfaces en estas conexiones.

Sobre estos enlaces troncales se van a dejar pasar las vlans que correspondan a servicios y gestión de los servidores Agile Controller Campus y el eSight Network.

El cableado de la conexión entre los equipos Switches Acceso S6720 para formar un solo switch lógico entre ellos, es un cable de fibra de 10G.

Conexiones Switches Servidores a las plataformas

En la figura N° 10 se muestran las conexiones entre los Switches Servidores y los correspondientes servidores para cada una de las plataformas de Agile Controller Campus y del eSight Network.

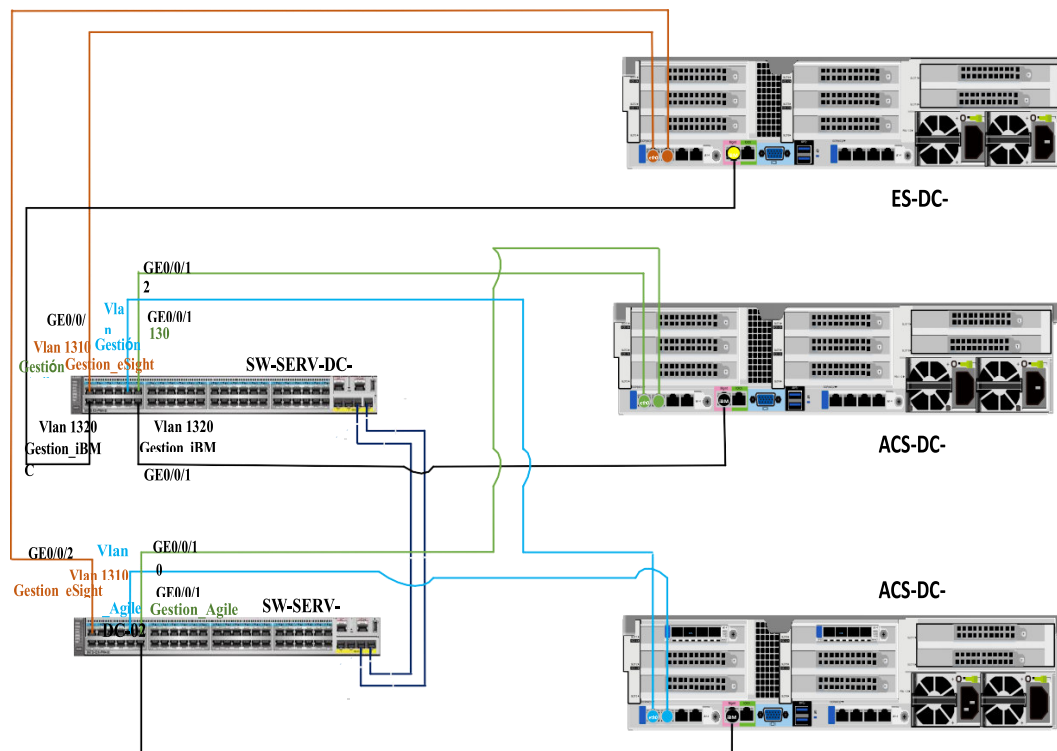


Figura 12: Conexiones Switches Servidores a las plataformas. Fuente: Elaboración propia

Se observa que las conexiones entre los Switches Servidores y los Servidores de los Agile Controller Campus y del eSight serán a través de interfaces Ethernet de 1GE de capacidad. Esas interfaces que muestra la topología hacia los servidores son las conexiones de servicio y de gestión de los servidores.

Conexiones Switches Acceso a Terminales y APs

En la figura N° 11 se muestra un ejemplo de las conexiones entre los Switches Acceso Multigigabit y los AP7060DN, así como a los usuarios finales de la red Corporativa.

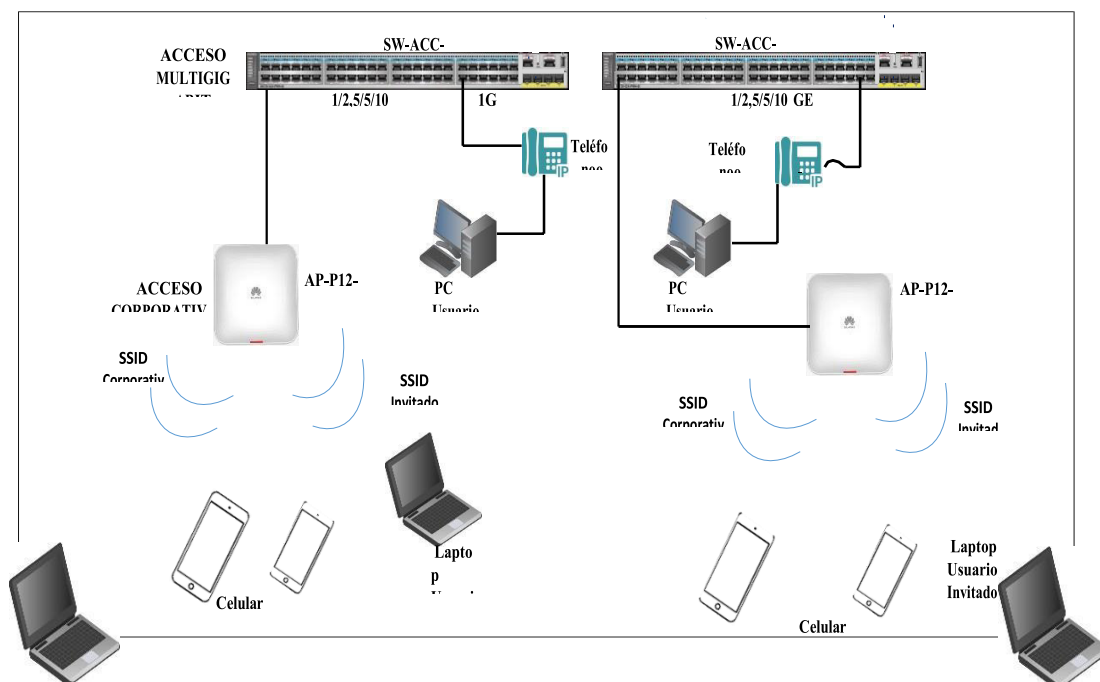


Figura 13: Conexiones Switches Multigigabit a AP y usuarios. Fuente: Elaboración propia

Se observa que las conexiones entre los Switches Acceso Multigigabit S6720-52X-PWH-SI y los equipos AP7060DN serán a través de conexiones 1/2.5/5/10 GE, esto debido a que los puertos de los Switches acceso cuenta con esas capacidades y el equipo AP7060DN cuenta con dos interfaces de 10GE y 1 GE.

Como se observa también desde los Switch de Acceso se conectarán a los usuarios finales de la red Corporativa y visitas a través de interfaces 1GE hacia los teléfonos IP y a las PC de los usuarios. En las interfaces de los Switch multigigabit se configurarán dos vlan sobre el puerto, la vlan de voz y vlan de datos correspondientes.

Se muestra también un ejemplo de las conexiones entre los equipos AP7060DN y los equipos wireless como son Laptops, tablets y teléfonos móviles que pertenecen a la red Corporativa. Las conexiones entre los equipos AP7060DN y los usuarios finales inalámbricos serán a través de conexiones Wifi, dependiendo del Wifi al cual se conecten.

Conexiones Red Paralela

En la Figura N° 12 se muestra las conexiones entre los equipos Switches Distribuidores S5731-H24T4X y los equipos Switches PoE S5735-S24P4X estos pertenecientes a la red Paralela de Niubiz que conectan usuarios invitados, así como también a las cámaras IP y televisores informativos.

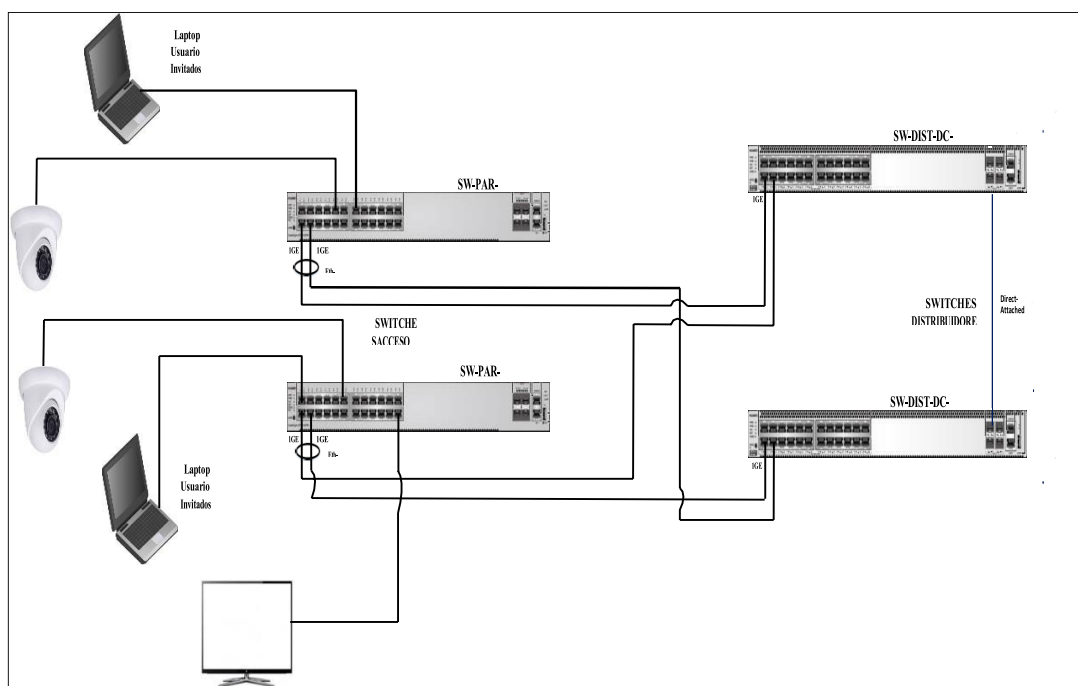


Figura 14: Conexiones Switches Acceso PoE – Red Paralela. Fuente: Elaboración propia

En la figura se observa que las conexiones entre los Switches Distribuidores S5731-H24T4X y los switches Acceso PoE S5735-S24P4X serán a través de interfaces de 1GE Ethernet. Estas dos interfaces se van a configurar como un link Aggregation desde los dos Switches Distribuidores para contar con el enlace activo en caso una falla en una de las interfaces en estas conexiones. Sobre estos enlaces troncales se van a dejar pasar las vlans que correspondan a servicios y gestión de los switches Acceso PoE, así como también las vlan para los usuarios invitados y para las cámaras IP y los televisores informativos.

El cableado de la conexión entre los equipos Switches Distribuidores S5731

para formar un solo switch lógico entre ellos, es un cable de fibra de 10G. Hay un cableado de conexión entre el Switch Distribuidor y el Switch Core, esto para pasar una vlan de gestión de los equipos que pertenecen a esta red Paralela. Sin embargo, el servicio de esta red pasa por el router dedicado para estas Cámaras IP, Televisores y usuarios Guest.

3.6.8 NAC Server – Agile Controller Campus

El Agile Controller-Campus proporciona acceso diversificado para usuarios corporativos e invitados, así como confiabilidad. Controla de manera uniforme los permisos de servicio en toda la red y programa los recursos de seguridad para garantizar el acceso flexible de los usuarios y el uso compartido de los recursos de seguridad.

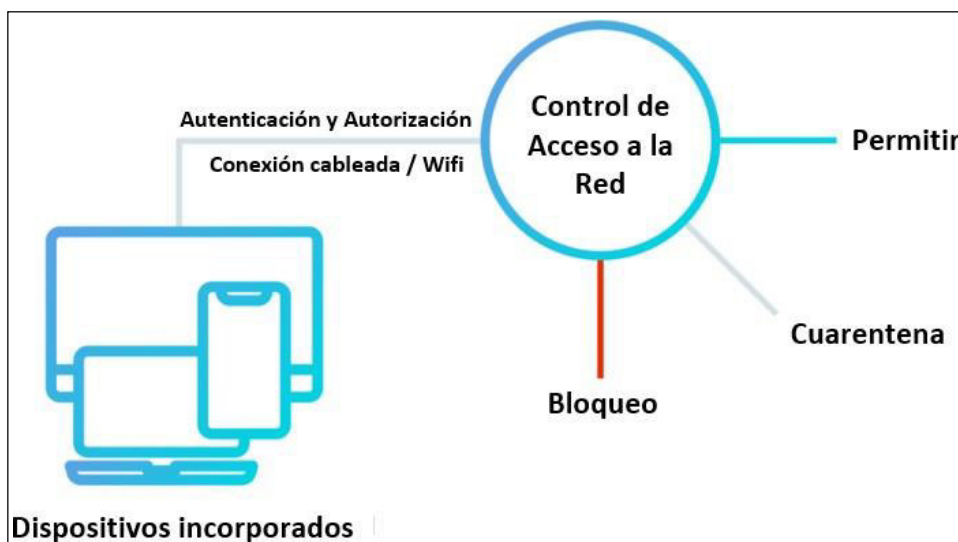


Figura 15: Control de Acceso a la Red – NAC. Fuente: Portal Soporte Huawei

Hardware y Software OS

A continuación, se detalla la configuración del servidor Hardware TaiShan 200 donde se instalará la plataforma de Agile Controller-Campus:

En la tabla N° 4 se hace referencia a los Datos del servidor Taishan 200.

Tabla 4 Datos servidor TaiShan 200 - Agile

Cantidad	2 servidores TaiShan 200 (Model 2280)
CPU	2*Kunpeng 920-32Core
Memoria	128 GB
Disco Duro	4*1200 GB SAS HDD
Tarjeta RAID	Avgo3508 (2 GB Cache) Raid Card + SuperCap
Interfaces de red	2*4 GE electrical port, 2*4 10GE/25GE SFP+ optical port

En la tabla N°5 se muestra los parámetros físicos del servidor TaiShan 200 (Model 2280) son:

Tabla 5 Parámetros físicos del servidor TaiShan 200 - Agile

Equipo Hardware	Ancho (mm)	Fondo (mm)	Alto (mm)	Peso (kg)	Consumo máximo energía (W)	Voltaje entrada (V) /Corriente (A)	Fuentes Energía
TaiShan 200 (Model 2280)	447	790	86.1	32	500	AC: 200 V to 240 V, 10 ADC: -48V to -60V, 32A	2

En la tabla N°6 se muestra el sistema operativo del Agile Controller-Campus tendrá como base el siguiente:

Tabla 6 Sistema operativo servidor Agile

CPU del Servidor	Configuración Software	Software Versión	Comentarios
ARM	Sistema Operativo	Euler V2.8	EulerOS es un sistema operativo propio de Huawei. El Agile Controller-Campus genera solo imágenes para el sistema operativo Euler, que se usa junto con los servidores de Huawei.

Planificación IP Agile Controller Campus

En esta sección se va a detallar la planificación de las conexiones y direcciones IP de los puertos de los servidores Agile Controller-Campus. Las conexiones físicas tanto para los Agile Controller Campus y los switches servidores.

En la Figura N° 14 se muestra la conexión desde los dos Switches Servidores a los puertos servicio e iBMC de los Agile Controller Campus. La siguiente figura muestra las conexiones físicas del mismo:

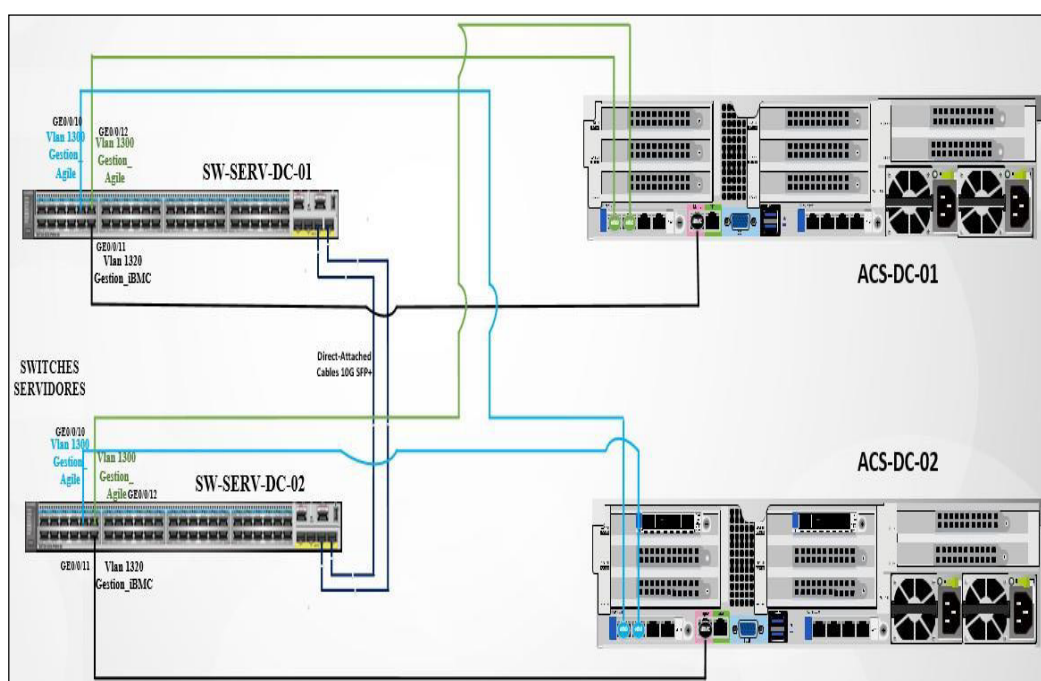


Figura 16: Conexión Switches Servidores - Agile Controller Campus. Fuente: Elaboración propia

La Tabla N° 7 contiene el mapeo de puertos para las conexiones planteadas para los Agile es la siguiente

La Tabla N° 8 corresponde a las conexiones del servidor Agile

Tabla 7 Mapeo de puertos servidores Agile

Servidor Agile Controller 01					
Nodo	Dirección IP	Bond	VLAN ID	Puerto Red	Dirección IP/Máscara de subred/Puerta de enlace
ACS-DC-01	Gestión Agile (SM/SC)	bond1	505	eth0	10.185.50.4/255.255.255.240/10.185.50.1
	Gestión Agile (SM/SC)	bond1	505	eth1	
	IP iBMC management		507	Management port	10.185.50.37/255.255.255.255.240/ 10.185.50.33
Servidor Agile Controller 02					
Nodo	Dirección IP	Bond	VLAN ID	Puerto Red	Dirección IP/Máscara de subred/Puerta de enlace
ACS-DC-02	Gestión Agile (SM/SC)	bond2	505	eth0	10.185.50.5/255.255.255.240/10.185.50.1
	Gestión Agile (SM/SC)	bond2	505	eth1	
	IP iBMC management		507	Management port	10.185.50.38/255.255.255.240/ 10.185.50.33

Tabla 8 Conexiones Servidores Agile

Equipo Origen			Equipo Destino		
Servidor	Plano de Red	NIC	Switch	Puerto	Tipo
ACS-DC-01	Gestión Agile (SM/SC)	Eth0	SW-SERV-DC-01	GE0/0/12	1G
	Gestión Agile (SM/SC)	Eth1	SW-SERV-DC-02	GE0/0/12	1G
	iBMC Management	iBMC	SW-SERV-DC-01	GE0/0/11	1G
Equipo Origen			Equipo Destino		
Servidor	Plano de Red	NIC	Switch	Puerto	Tipo
ACS-DC-02	Gestión Agile (SM/SC)	Eth0	SW-SERV-DC-01	GE0/0/10	1G
	Gestión Agile (SM/SC)	Eth1	SW-SERV-DC-02	GE0/0/10	1G
	iBMC Management	iBMC	SW-SERV-DC-02	GE0/0/11	1G

Contraseñas Agile Controller Campus

El Servidor Agile Controller-Campus en un servidor TaiShan tiene las siguientes contraseñas de usuario por defecto, estas deben ser reemplazadas por contraseñas predeterminadas después de la instalación para garantizar la seguridad del sistema.

La tabla N° 9 enumera los nombres de usuario y contraseñas involucrados en la instalación.

Tabla 9 Usuarios y contraseñas por default Agile

Objeto	Nombre de Usuario	Default Password	Requerimientos complejidad de Password
iBMC Gestión	Administrator	Admin@9000	• Contiene de 8 a 20 caracteres. • Contiene un carácter de espacio al menos uno de los siguientes caracteres especiales: !"\$%&'()*+,-./:;<=>?@[\\]^_`{ }~ • Contiene al menos dos de los siguientes: dígitos, letras mayúsculas y letras minúsculas.
Sistema Operativo del Agile Controller Campus	root	Changeme_123	• Contiene al menos 8 caracteres. • Debe ser una combinación de letras mayúsculas, minúsculas, dígitos y cualquiera de los siguientes caracteres especiales: ~@#^*-_+[]{}:./? • No puede contener el nombre de usuario. • No puede contener comillas (").

3.6.9 Plataforma de Gestión – eSight

eSight es un sistema de gestión de red de última generación para redes de campus empresariales que ofrece visualización y O&M de múltiples dimensiones como gestionar el dispositivo, el volumen de tráfico de red y alarmas. Asimismo, gestiona de manera uniforme los recursos, asocia diversas funciones que facilitan la gestión de la red y los dispositivos de terceros.

Hardware y Software OS

La configuración del servidor Hardware TaiShan 200 donde se instalará la plataforma de eSight:

En la tabla N° 10 se hace referencia a los Datos del servidor Taishan 200.

Tabla 10 Datos servidor Taishan 200 - eSight

Cantidad	1 servidor TaiShan 200 (Model 2280)
CPU	2*Kunpeng 920 4826
Memoria	4*32G DIMM
Disco Duro	2*1200GB SAS
Network Interface	8*GE

La Tabla N° 11 resume los parámetros físicos del servidor.

Tabla 11 Parámetros físicos del servidor TaiShan 200 - eSight

Equipo Hardware	Ancho (mm)	Fondo (mm)	Alto (mm)	Peso (kg)	Consumo máximo energía (W)	Voltaje entrada (V) /Corriente (A)	Fuentes Energía
TaiShan 200 (Model 2280)	447	790	86.1	32	500	AC: 200 V to 240 V, 10 ADC: -48V to -60V, 32A	2

La Tabla N° 12 corresponde al sistema operativo base del eSight Network:

Tabla 12 Sistema operativo servidor eSight

CPU del Servidor	Configuración Software	Software Versión	Comentarios
ARM	Sistema Operativo	Euler V2.8	EulerOS es un sistema operativo propiodesarrollado por Huawei.

Planificación IP Servidor eSight

En esta sección se detalla la planificación de las conexiones y direcciones IP

de los puertos del servidor eSight. Las conexiones físicas del eSight Server son hacia los dos switches servidores para una redundancia del servicio.

Como se muestra en la figura N° 15, se tiene la conexión desde los dos Switches Servidores a los puertos servicios eth0, eth1 e iBMC del eSight. La siguiente figura muestra las conexiones físicas del mismo:

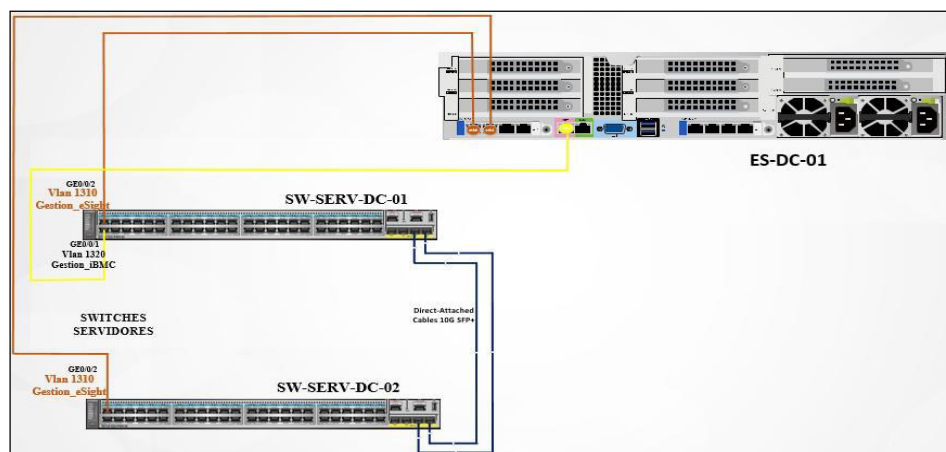


Figura 17: Conexiones entre el Switch Servidor y el equipo eSight. Fuente: Elaboración propia

El mapeo de puertos es planteado en la Tabla N° 13:

Tabla 13 Mapeo de puertos servidor eSight

Servidor eSight					
Nodo	Dirección IP	Bond	VLAN ID	Puerto de Red	Dirección IP/Máscara de subred/Puerta de enlace
ES-DC-01	Gestión eSight	bond0	506	eth0	10.185.50.20/ 255.255.255.240/ 10.185.50.17
	Gestión eSight	bond0	506	eth1	
	IP management iBMC		507	Management port	10.185.50.36/ 255.255.255.240/ 10.185.50.33
Equipo Origen			Equipo Destino		
Servidor	Plano de Red	NIC	Switch	Puerto	Tipo
ES-DC-01	Gestión eSight	Eth0	SW-SERV-DC-01	GE0/0/2	1G
	Gestión eSight	Eth1	SW-SERV-DC-02	GE0/0/2	1G
	iBMC Management	iBMC	SW-SERV-DC-01	GE0/0/1	1G

Contraseñas eSight

El Servidor eSight Network en un servidor TaiShan tiene las siguientes contraseñas de usuario por defecto, estas deben ser reemplazar por contraseñas predeterminadas después de la instalación para garantizar la seguridad del sistema. En la Tabla N° 14 se enumeran los nombres de usuario y contraseñas involucrados en la instalación.

Tabla 14 Usuarios y contraseñas por default eSight

Objeto	Nombre de Usuario	Default Password	Requerimientos de Complejidad de Password
iBMC Gestión	Administrator	Admin@9000	• Contiene de 8 a 20 caracteres. • Contiene un carácter de espacio o al menos uno de los siguientes caracteres especiales: !"\$%&'()*+,-./:;<=>?@[^`{ }~ • Contiene al menos dos de los siguientes: dígitos, letras mayúsculas y letras minúsculas.
Sistema Operativo del eSight Network	root	Changeme_123	• Contiene al menos 8 caracteres. • Debe ser una combinación de letras mayúsculas, minúsculas, dígitos y cualquiera de los caracteres especiales: ~@#^*-_+[]{}:./? • No puede contener el nombre de usuario. • No puede contener comillas (").

3.6.10 Mapeo de Puertos de la red de Campus Miraflores

Los mapeos de puertos de las conexiones entre los distintos equipos que conforman la red Campus Miraflores son descritos en esta parte.

3.6.11 Mapeo de puertos Red Campus

El mapeo de puertos es la conexión entre los equipos de networking a ser desplegados en la red de campus se realiza como parte del diseño de una red de campus para tener una visión de clara de cómo se va a realizar las conexiones en la etapa de implementación.

La tabla de las conexiones de la Red Campus se observa en el **Anexo C** del presente documento.

3.6.12 Mapeo de puertos Red Paralela

El mapeo de puertos es la conexión a realizarse en la etapa de implementación. Se compone de las conexiones entre los equipos de networking a ser desplegados en la red, este caso la red Paralela, como parte del diseño de una red.

La tabla de las conexiones de la Red Paralela se observa en el **Anexo D** del presente documento.

3.6.13 Distribución de equipos en el rack Campus Miraflores

Como parte del diseño de la red, en la Figura N° 16 se muestra la distribución de los equipos de networking que serán ubicados en los gabinetes del DataCenter de la empresa. Estos equipos son: 3 servidores, 2 switches core, 2 Controladores de acceso, 2 switches servidores y 2 switches distribuidores.

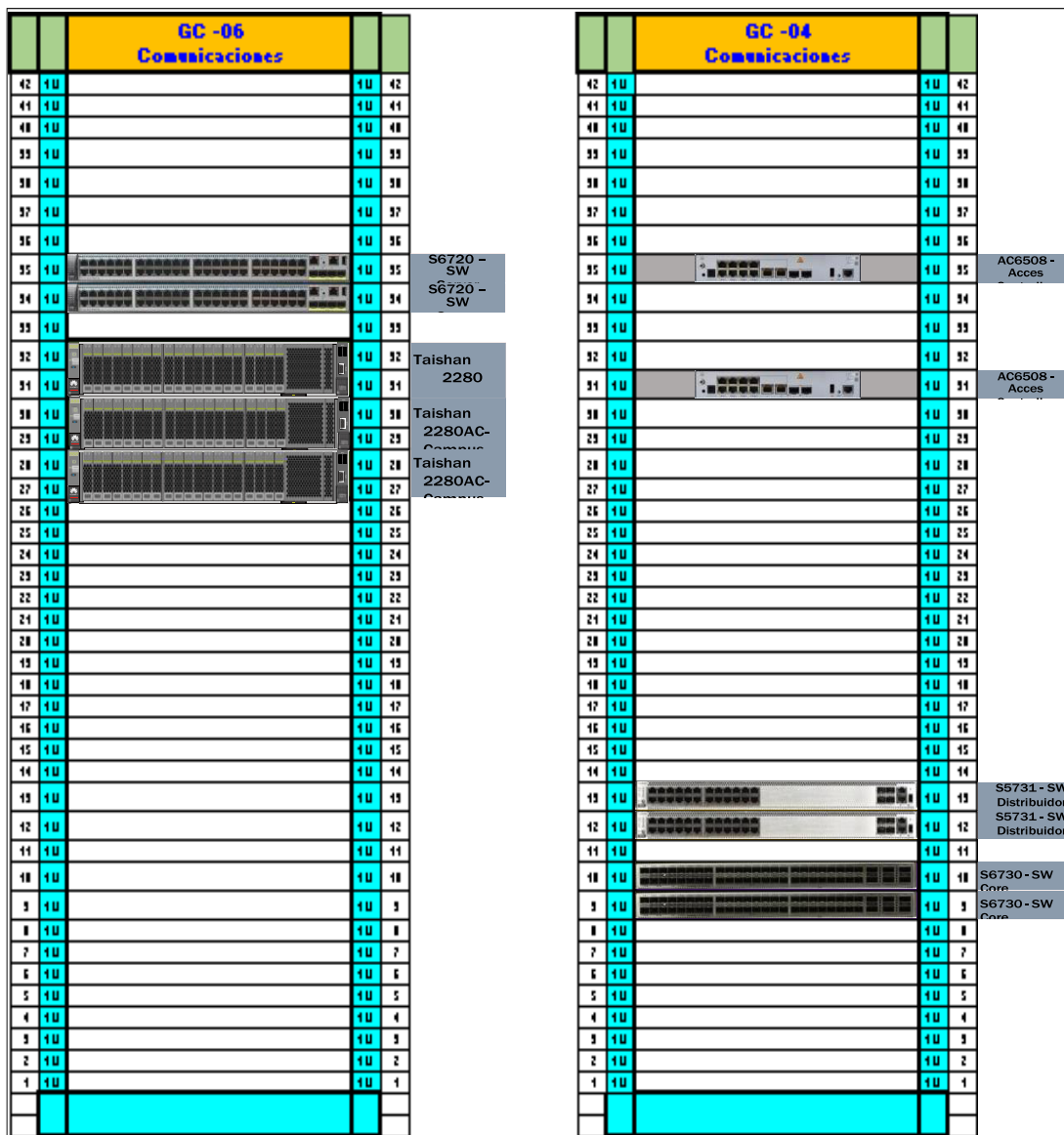


Figura 18: Rack Layout ubicación de equipos. Fuente: Elaboración propia

3.7 Resumen de la actividad

A partir del proyecto realizado el 01 de julio de 2020 para la empresa Niubiz, en donde se planificó un nuevo diseño de red de Campus para la entidad financiera. Como resultado de la planificación y diseño de la nueva red corporativa, se elaboró un documento de entrega al cliente llamado Diseño de Bajo Nivel (LLD - Lower Lever Design) en donde a través del documento se especificó a detalle el diseño de topologías, parámetros y configuraciones para la nueva solución de campus del cliente.

A continuación, se detalla lo realizado en el documento de entrega hacia el cliente - LLD (diseño de bajo nivel). En el **anexo E** se muestra las dos primeras páginas del documento LLD elaborado como entregable del proyecto realizado el cual la entidad lo tomó como un acta de conformidad.

- En el primer capítulo del documento se desarrolló el Background técnico (Conceptos técnicos), en donde se desarrollaron conceptos como arquitecturas de red capa 2, conexiones en apilamiento (stack), cobertura inalámbrica, alta disponibilidad.
- Posteriormente en el segundo capítulo, se describieron las asunciones y supuestos del diseño de campus propuestos, basándose en los lineamientos requeridos por el cliente Niubiz.
- Como tercer capítulo se especificó el nombre a configurarse en los equipos de networking de la red.
- En el cuarto capítulo se definió las versiones de software en los dispositivos adquiridos para la futura implementación, así como las subredes que se encuentran en la sede principal del cliente.
- A continuación, en el capítulo quinto, se desarrolló el diseño general de la red, donde se detallaron las conexiones entre los equipos de networking a ser desplegados en la red, así como el mapeo de los puertos entre los equipos, ubicación de los equipos del DataCenter en los gabinetes de DataCenter del cliente y una visión de la topología general de la red de campus Miraflores.

- Para el capítulo sexto se desarrolló todo lo concerniente al diseño como el mapeo de puertos y planeamiento de IPs de los servidores de Agile Controller Campus (Servidor de control de acceso a la red para los usuarios).
- En el sexto capítulo se describió todo lo concerniente al diseño para el servidor eSight como el mapeo de puertos y planeamiento de IPs, así como algunas de sus funciones.
- En el capítulo final, se proporcionaron plantillas de configuración y una breve descripción de los protocolos a ser configurados en los equipos de red de Campus en la futura implementación a partir del diseño realizado.

Con respecto al presente trabajo, se menciona que la disposición física de los dispositivos, equipos y otros componentes de la red, es producto del diseño y para la futura implementación de la red de Campus, la cual cumple con los lineamientos y requerimientos de la entidad financiera, como se detallan:

- Los equipos de la red estarán distribuidos en los pisos de la oficina de la entidad financiera como única sede del cliente.
- Los doce equipos Switches Acceso Multigigabit estarán distribuidos en parejas de dos en cada piso y los dos switches para conexión a los servidores eSight y Agile Controller Campus estarán ubicados en el DataCenter, ubicado en las oficinas del cliente.
- Los doce equipos Switches Acceso Multigigabit son distribuidos en parejas de dos en cada piso, y a una distancia menor a 3 metros entre sí para la conexión vía fibra óptica para formar el stack.
- Los equipos AP7060DN se distribuyan entre cuatro y tres equipos por piso dependiendo de la disposición de la entidad financiera y así completar los 20 equipos AP7060DN.
- Los puertos en los switches Acceso Multigigabit S6720 destinados a conexiones de usuarios finales Corporativos, estén en el rango desde el puerto GE0/0/13 al GE0/0/48 de cada Switch.

- Los dos Controladores AC6508, los dos Switches Core S6730, los dos Switches Servidores S6720, los dos Servidores Agile Controller y el Servidor eSight, estarán en la sala de Servidores (Data Center).
- La Red Paralela incluirá a los seis equipos Switches de Acceso PoE S5735 uno en cada piso de las oficinas de Niubiz, y los dos equipos Distribuidores en la Sala de Servidores del Piso 12.
- Para las conexiones de los Switches S5735 en la Red Paralela, a las cámaras IP, Televisores y a los usuarios finales invitados, se propone usar los puertos del rango GE0/0/7 al GE0/0/24
- Para la gestión de los equipos de la Red Paralela, se deberá tener una conexión entre los Switches Core a los equipos Distribuidores por medio de la vlan de gestión.

CAPITULO IV: RESULTADOS

4.1 Justificación

La red de campus tradicional con la que contaba la entidad financiera ya no podía cumplir con las expectativas empresariales, ya que fue diseñada considerando requisitos industriales no relevantes en la actualidad. La red actual no puede aprovechar las ventajas de las tecnologías emergentes y los modelos operativos de red, tampoco pueden escalar al ritmo de los requerimientos crecientes del usuario en tráfico de datos y comunicaciones. La nueva red de área de campus proporcionará una forma de control de recursos de red bastante sencilla, haciendo posible que la organización, centralice sus esfuerzos de seguridad y compartan datos rápidamente.

4.2 Evaluaciones

4.2.1 Evaluación presupuestal

A partir del diseño realizado y validado por la entidad financiera, se presentó la propuesta, conteniendo los dispositivos y las licencias de los servidores Agile-Controller Campus (NAC) y Esight para la gestión.

En la tabla N° 15 se muestran los productos que se utilizaran para el despliegue de la nueva red de Campus en la sede de Miraflores, así como la cantidad y el coste de los equipos.

Tabla 15 Costo dispositivos Red de Campus

Nombre dispositivo	Cantidad	Precio en USD	Precio total en USD
Controlador de Acceso	2	1,756.28	3,512.56
Access Points Wifi6	20	857.80	17,156.00
Switch Core	2	9,124.34	18,248.68
Switches de Acceso Multigigabit	14	5,136.31	71,908.34
Switches de Distribución	2	2,784.55	5,569.10
Switches de Acceso	6	1,575.87	9,455.22
Agile Controller-Campus	1	29,557.34	29,557.34
eSight	1	14,578.15	14,578.15
Precio Total			169,985.39

4.2.2 Evaluación técnica

A partir de todo el diseño previo, planteado a detalle para la sede principal de la corporación financiera, se elaboró:

- La topología General final de la Red Campus Miraflores propuesta,
- Los lineamientos/configuraciones a aplicarse en los dispositivos de red en la etapa de implementación del trabajo.

4.2.3 Configuraciones de dispositivos de red

El diseño plantea el uso de equipos de networking y versiones de software, así como una breve descripción de los protocolos a ser configurados en los equipos de la red de Campus:

- VLAN
- Alta Disponibilidad
- Agregación de enlace
- AAA (Autenticación, Autorización, contabilidad)
- ACL (Lista de Control de Acceso)
- SNMP
- NTP, MSTP
- Port Security (Seguridad de Puerto)

En el **Anexo F** se observa la configuración de los dispositivos de red.

4.3 Descripción de la implementación

El nuevo diseño de red de campus corporativo incluye las pautas para una futura implementación.

En el Anexo G se muestran los procesos para la implementación de los servidores Agile Controller Campus (Servidor de Control de Acceso) y del servidor eSight (Servidor de Gestión Centralizada) que se basan en la documentación oficial para la implementación de estas soluciones del vendor Huawei, que comprende:

- Implementación de Agile Controller-Campus
 - * Instalación del Agile Controller Campus
 - * Configuración de autorización por VLAN
 - * Configuración de autorización por ACL dinámica
 - * Configuración de la autenticación inalámbrica 802.1X
- Implementación del eSight Campus
 - * Instalación del eSight Campus
 - * Administrar y mantener dispositivos de Red
 - * Gestión de los equipos de red en la vista de topológica
 - * Agregar un servidor
 - * Visualización de datos de rendimiento

4.3.1 Cobertura Wifi Access Points

A partir del dispositivo Access Point AP7060DN planteado en el presente trabajo de diseño de la red de campus para la cobertura inalámbrica Wifi, se realizó una simulación de cobertura en las frecuencias de 2.4G y 5G, así como de la simulación del SINR (relación de señal a ruido) en las oficinas de la entidad financiera donde se muestra la cobertura alcanzada por estos dispositivos Access Point Wifi.

A partir de la simulación de cobertura 2.4G y 5G, así como de la simulación del SNR (relación del nivel de señal al nivel de ruido) se determinó que con solo 3 Access Points por piso se puede dar cobertura a todas las zonas dentro de las oficinas ya sea para usuarios corporativos o visitas

La cobertura de los Access Points se muestra en el **anexo H** del documento.

.

-

CAPITULO V CONCLUSIONES

- El diseño de la red corporativa para la empresa Niubiz, considera criterios de escalabilidad, disponibilidad y velocidad de conexión, características que contribuyen a la calidad de servicio global. Este diseño se planteó como ingeniería base para la futura implementación.
- La implementación de la solución de eSight de Huawei permite la gestión centralizada de los dispositivos de networking de la red de campus.
- La solución de control de acceso a la red (NAC) del Agile Controller-Campus, garantiza la aplicación de políticas de seguridad para el control de acceso de los usuarios a los servicios de la red.
- Se mejora la cobertura para las comunicaciones mediante el despliegue de equipos Switches para conexiones alámbricas y de dispositivos Access Point para la cobertura inalámbrica. Asimismo, estos equipos proporcionan la escalabilidad necesaria, con amplia capacidad de puertos y conexiones
- Se garantiza la seguridad para los recursos de la red mediante la aplicación políticas de seguridad que se implementan en todos los equipos de networking que forman parte de la red.

CAPITULO VI: RECOMENDACIONES

- Las expansiones requeridas se realizarán luego de una evaluación financiera en la que intervenga el personal técnico encargado del diseño e implementación de nuevos productos.
- Los firmwares y parches del software de los equipos de networking deben mantenerse siempre actualizados, así como de la solución de eSight y Agile-Controller campus, para estar en línea con los cambios de mejora en los dispositivos.
- Se recomienda instalar los equipos de networking en ambientes adecuados que permitan el correcto funcionamiento y alcanzar la vida útil de los dispositivos.
- Es necesario la continua capacitación y estudio en las soluciones de Huawei eSight y Agile-Controller campus para que puedan realizar una correcta lectura y análisis de las funciones de ambos sistemas.

CAPITULO VII: REFERENCIAS

Ávila Pesantez Diego Fernando y Allauca Carrillo Elías Fernando (2022). Propuesta de mejores prácticas de ciberseguridad para la comunicación en redes de clientes corporativos. Obtenido de: <https://repositorio.pucesa.edu.ec/handle/123456789/3779>

Barry Peter, Crowley Patrick (2012). Modern Embedded Computing. Hawthorne, USA. Obtenido de: <https://www.sciencedirect.com/topics/computer-science/network-connectivity>

Browning Paul (2017). IP Subnetting, from zero to guru. California, USA. Obtenido de: <https://bookauthority.org/books/best-subnet-books>

Cabral Otero Assumpta María (2020). Integración de sedes en una red corporativa utilizando ITIL. Sevilla, España. Obtenido de: <https://idus.us.es/handle/11441/104144>

Carballar Jose Antonio (2008). VoIP La telefónica de Internet. Madrid, España. Obtenido de: <https://www.paraninfo.es/catalogo/9788428329521/voip--la-telefonía-de-internet>

Cisco Network Academy (2014). Hierarchical Network Design. California, USA. Obtenido de: <https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>

Fitzgerald, Foley, Foghlú. (2008). Network Access Control Interoperation using Semantic Web Techniques. Cork, Irlanda. Obtenido de: <https://www.scitepress.org/PublishedPapers/2008/17433/17433.pdf>

Ministerio Transformación Digital, Avance Digital (2023), España. Obtenido de: <https://advancedigital.mineco.gob.es/es-es/Servicios/CalidadServicio/Paginas/Calidad.aspx>

García Pagan Juan José (2007). Gestión de seguridad en redes corporativas. Lima, Perú. Obtenido de: <https://revistas.ulima.edu.pe/index.php/Interfases/article/view/162/110>

Hendel Ariel (1997). Link Aggregation Trunking. California, USA. Obtenido de: <http://www.cs.uccs.edu/~scold/doc/linkage%20aggregation%202.pdf>

Obis Joan Anna (2014). Diseño de una red corporativa. Catalunya, España. Obtenido de: <http://hdl.handle.net/10609/28625>

Oggerino Chris, Cisco (2001). High availability network fundamentals. San Jose, USA. Obtenido de: <https://www.ciscopress.com/store/high-availability-network-fundamentals-9781587130175>

Quintero Sanabria Flor Maria (2018). Solución de cuellos de botella a través de agregación de enlaces en entornos LAN. Norte de Santander, Colombia. Obtenido de: <http://repositorio.ufpso.edu.co/handle/123456789/2328>

Soporte Huawei A (2022). S300, S500, S2700, S5700, and S6700 Series Ethernet Switches Product Documentation. Shanghai, China. Obtenido de: <https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210952&id=index>

Soporte Huawei B (2022). eSight Product Documentation. Shanghai, China. Obtenido de: <https://support.huawei.com/hedex/hdx.do?docid=EDOC1100207403>

Soporte Huawei C (2022). Agile Controller-Campus Product Documentation. Shanghai, China. Obtenido de:

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100181203&id=index>

UIT Unión Internacional de Telecomunicaciones, Vocabulario de Calidad de servicio y Seguridad de funcionamiento, Reedición de la Recomendación E.800 del CCITT publicada en el Libro Azul, Fascículo II.3 (1988), 2007.

ANEXOS

Anexo A: Topología General a detalle de la red Campus Miraflores

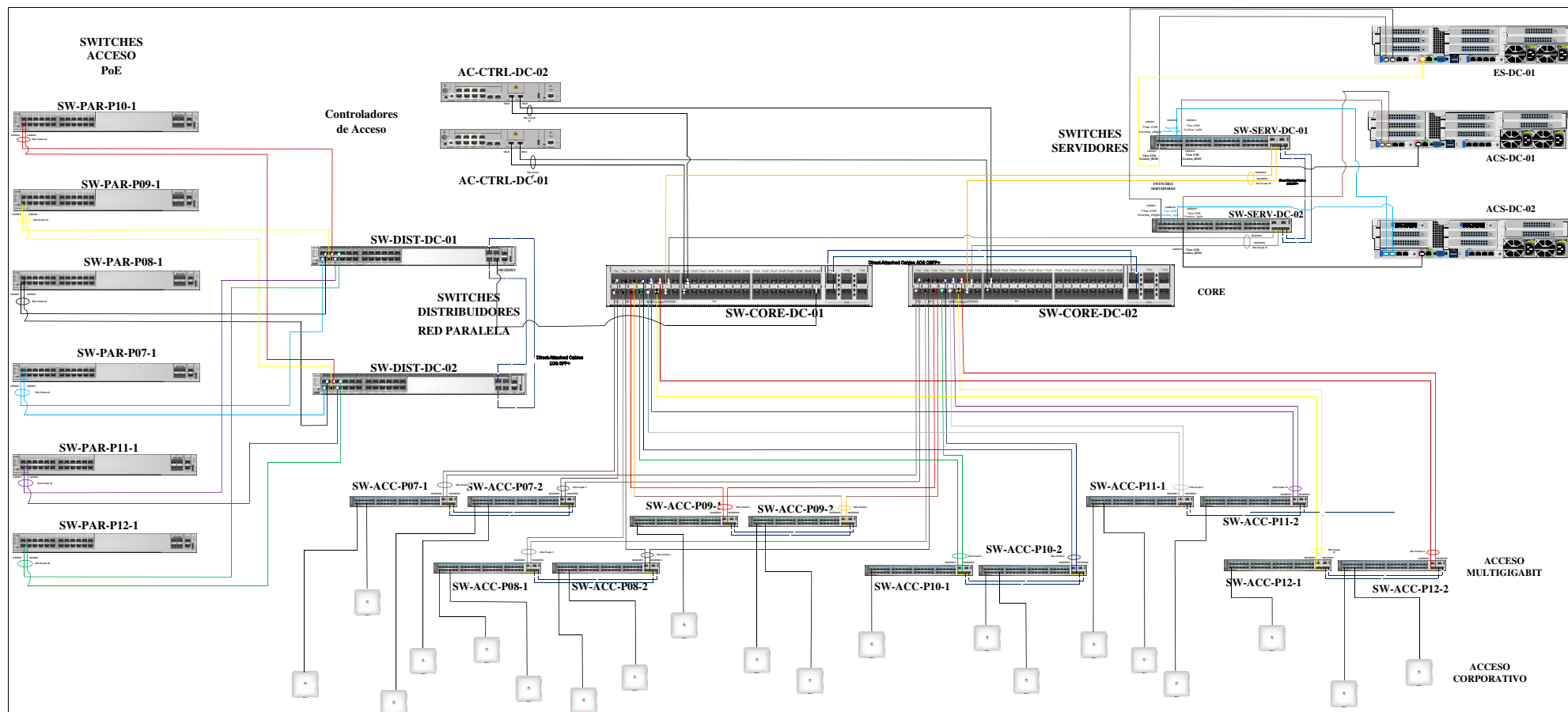


Figura: Topología General a detalle de Red Campus Miraflores. Fuente: Elaboración Propia

Anexo B: Componentes de networking del nuevo diseño de la red

Switch Core



Figura: Switch S6730-H48X6C. Fuente: Portal Soporte Huawei

Switch Acceso/Servidor

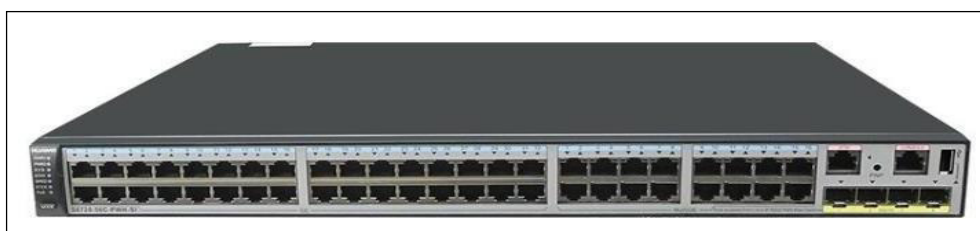


Figura: Switch S6720-52X-PWH-SI. Fuente: Portal Soporte Huawei

Controlador



Figura: Controlador de Acceso AC6508. Fuente: Portal Soporte Huawei

Servidores



Figura: Servidor TaiShan 200 (Modelo 2280). Fuente: Portal Soporte Huawei

Switch Distribuidor/Acceso

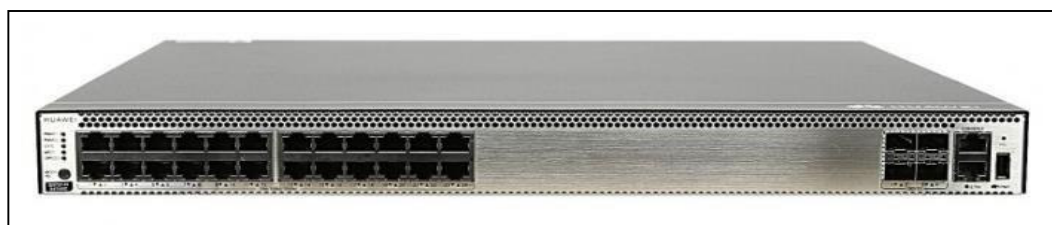


Figura: Switch S5731-H24T4XC. Fuente: Portal Soporte Huawei

Punto de acceso (Access Points)



Figura: Punto de Acceso AP7060DN. Fuente: Portal Soporte Huawei

ANEXO C: Mapeo de puertos de la Red Campus

Tabla: Mapeo conexiones de la Red Campus.

ORIGEN			DESTINO			
Hostname	Interface	Interface Type	Hostname	Interface	Interface Type	Interfaz Troncal
SW-CORE-DC-01	10GE0/0/1	Optical Port	SW-ACC-P07-1	10GE0/0/1	Optical Port	Eth-Trunk 1
	10GE0/0/2	Optical Port	SW-ACC-P07-2	10GE0/0/1	Optical Port	Eth-Trunk 2
	10GE0/0/3	Optical Port	SW-ACC-P08-1	10GE0/0/1	Optical Port	Eth-Trunk 3
	10GE0/0/4	Optical Port	SW-ACC-P08-2	10GE0/0/1	Optical Port	Eth-Trunk 4
	10GE0/0/5	Optical Port	SW-ACC-P09-1	10GE0/0/1	Optical Port	Eth-Trunk 5
	10GE0/0/6	Optical Port	SW-ACC-P09-2	10GE0/0/1	Optical Port	Eth-Trunk 6
	10GE0/0/7	Optical Port	SW-ACC-P10-1	10GE0/0/1	Optical Port	Eth-Trunk 7
	10GE0/0/8	Optical Port	SW-ACC-P10-2	10GE0/0/1	Optical Port	Eth-Trunk 8
	10GE0/0/9	Optical Port	SW-ACC-P11-1	10GE0/0/1	Optical Port	Eth-Trunk 9
	10GE0/0/10	Optical Port	SW-ACC-P11-2	10GE0/0/1	Optical Port	Eth-Trunk 10
	10GE0/0/11	Optical Port	SW-ACC-P12-1	10GE0/0/1	Optical Port	Eth-Trunk 11
	10GE0/0/12	Optical Port	SW-ACC-P12-2	10GE0/0/1	Optical Port	Eth-Trunk 12
SW-CORE-DC-02	10GE0/0/1	Optical Port	SW-ACC-P07-1	10GE0/0/2	Optical Port	Eth-Trunk 1
	10GE0/0/2	Optical Port	SW-ACC-P07-2	10GE0/0/2	Optical Port	Eth-Trunk 2
	10GE0/0/3	Optical Port	SW-ACC-P08-1	10GE0/0/2	Optical Port	Eth-Trunk 3
	10GE0/0/4	Optical Port	SW-ACC-P08-2	10GE0/0/2	Optical Port	Eth-Trunk 4
	10GE0/0/5	Optical Port	SW-ACC-P09-1	10GE0/0/2	Optical Port	Eth-Trunk 5
	10GE0/0/6	Optical Port	SW-ACC-P09-2	10GE0/0/2	Optical Port	Eth-Trunk 6
	10GE0/0/7	Optical Port	SW-ACC-P10-1	10GE0/0/2	Optical Port	Eth-Trunk 7
	10GE0/0/8	Optical Port	SW-ACC-P10-2	10GE0/0/2	Optical Port	Eth-Trunk 8
	10GE0/0/9	Optical Port	SW-ACC-P11-1	10GE0/0/2	Optical Port	Eth-Trunk 9
	10GE0/0/10	Optical Port	SW-ACC-P11-2	10GE0/0/2	Optical Port	Eth-Trunk 10
	10GE0/0/11	Optical Port	SW-ACC-P12-1	10GE0/0/2	Optical Port	Eth-Trunk 11

	10GE0/0/1 2	Optical Port	SW-ACC-P12-2	10GE0/0/2	Optical Port	Eth-Trunk 12
SW-CORE- DC-01	40GE0/0/1	Optical Port	SW-CORE- DC-02	40GE0/0/1	Optical Port	NA
	40GE0/0/2	Optical Port		40GE0/0/2	Optical Port	NA
SW-CORE- DC-01	10GE0/0/1 5	Optical Port	AC-CTRL-DC- 01	10GE0/0/1	Optical Port	Eth-Trunk 20
	10GE0/0/1 6	Optical Port		10GE0/0/1	Optical Port	Eth-Trunk 21
SW-CORE- DC-02	10GE0/0/1 5	Optical Port	AC-CTRL-DC- 01	10GE0/0/2	Optical Port	Eth-Trunk 20
	10GE0/0/1 6	Optical Port		10GE0/0/2	Optical Port	Eth-Trunk 21
SW-CORE- DC-01	10GE0/0/2 1	Optical Port	SW-SERV- DC-01	10GE0/0/1	Optical Port	Eth-Trunk 30
	10GE0/0/2 2	Optical Port	SW-SERV- DC-02	10GE0/0/1	Optical Port	Eth-Trunk 31
SW-CORE- DC-02	10GE0/0/2 1	Optical Port	SW-SERV- DC-01	10GE0/0/2	Optical Port	Eth-Trunk 30
	10GE0/0/2 2	Optical Port	SW-SERV- DC-02	10GE0/0/2	Optical Port	Eth-Trunk 31
SW-SERV- DC-01	10GE0/0/3	Optical Port	SW-SERV- DC-02	10GE0/0/3	Optical Port	NA
	10GE0/0/4	Optical Port	SW-SERV- DC-02	10GE0/0/4	Optical Port	NA
SW-SERV- DC-01	GE0/0/1	Ethernet Port	ES-DC-01	iBMC	Ethernet Port	NA
	GE0/0/2	Ethernet Port	ES-DC-01	Eht0	Ethernet Port	NA
	GE0/0/10	Ethernet Port	ACS-DC-02	Eht0	Ethernet Port	NA
	GE0/0/11	Ethernet Port	ACS-DC-01	iBMC	Ethernet Port	NA
	GE0/0/12	Ethernet Port	ACS-DC-01	Eht0	Ethernet Port	NA
SW-SERV- DC-02	GE0/0/2	Ethernet Port	ES-DC-01	Eht1	Ethernet Port	NA
	GE0/0/10	Ethernet Port	ACS-DC-02	Eht1	Ethernet Port	NA
	GE0/0/11	Ethernet Port	ACS-DC-02	iBMC	Ethernet Port	NA
	GE0/0/12	Ethernet Port	ACS-DC-01	Eht1	Ethernet Port	NA

ANEXO D: Mapeo de puertos de la Red Paralela

Tabla: Mapeo conexiones de la Red Paralela.

ORIGEN			DESTINO			
Hostname	Interface	Interface Type	Hostname	Interface	Interface Type	Interfaz Troncal
SW-DIST-DC-01	GE0/0/1	Ethernet Port	SW-PAR-P07-1	GE0/0/1	Ethernet Port	Eth-Trunk 41
	GE0/0/2	Ethernet Port	SW-PAR-P08-1	GE0/0/1	Ethernet Port	Eth-Trunk 42
	GE0/0/3	Ethernet Port	SW-PAR-P09-1	GE0/0/1	Ethernet Port	Eth-Trunk 43
	GE0/0/4	Ethernet Port	SW-PAR-P10-1	GE0/0/1	Ethernet Port	Eth-Trunk 44
	GE0/0/5	Ethernet Port	SW-PAR-P11-1	GE0/0/1	Ethernet Port	Eth-Trunk 45
	GE0/0/6	Ethernet Port	SW-PAR-P12-1	GE0/0/1	Ethernet Port	Eth-Trunk 46
SW-DIST-DC-02	GE0/0/1	Ethernet Port	SW-PAR-P07-1	GE0/0/2	Ethernet Port	Eth-Trunk 41
	GE0/0/2	Ethernet Port	SW-PAR-P08-1	GE0/0/2	Ethernet Port	Eth-Trunk 42
	GE0/0/3	Ethernet Port	SW-PAR-P09-1	GE0/0/2	Ethernet Port	Eth-Trunk 43
	GE0/0/4	Ethernet Port	SW-PAR-P10-1	GE0/0/2	Ethernet Port	Eth-Trunk 44
	GE0/0/5	Ethernet Port	SW-PAR-P11-1	GE0/0/2	Ethernet Port	Eth-Trunk 45
	GE0/0/6	Ethernet Port	SW-PAR-P12-1	GE0/0/2	Ethernet Port	Eth-Trunk 46
SW-DIST-DC-01	10GE0/0/1	Optical Port	SW-DIST-DC-02	10GE0/0/1	Optical Port	NA
	10GE0/0/2	Optical Port		10GE0/0/2	Optical Port	NA
SW-CORE-DC-01	10GE0/0/47	Optical Port	SW-DIST-DC-01	10GE0/0/3	Optical Port	NA

ANEXO E: Documento LLD (Lower Level Design) entregable diseño

A continuación, se muestran las dos primeras páginas del documento LLD (diseño de bajo nivel) elaborado como entregable de diseño del proyecto el cuales la base para la elaboración del presente trabajo de suficiencia profesional.

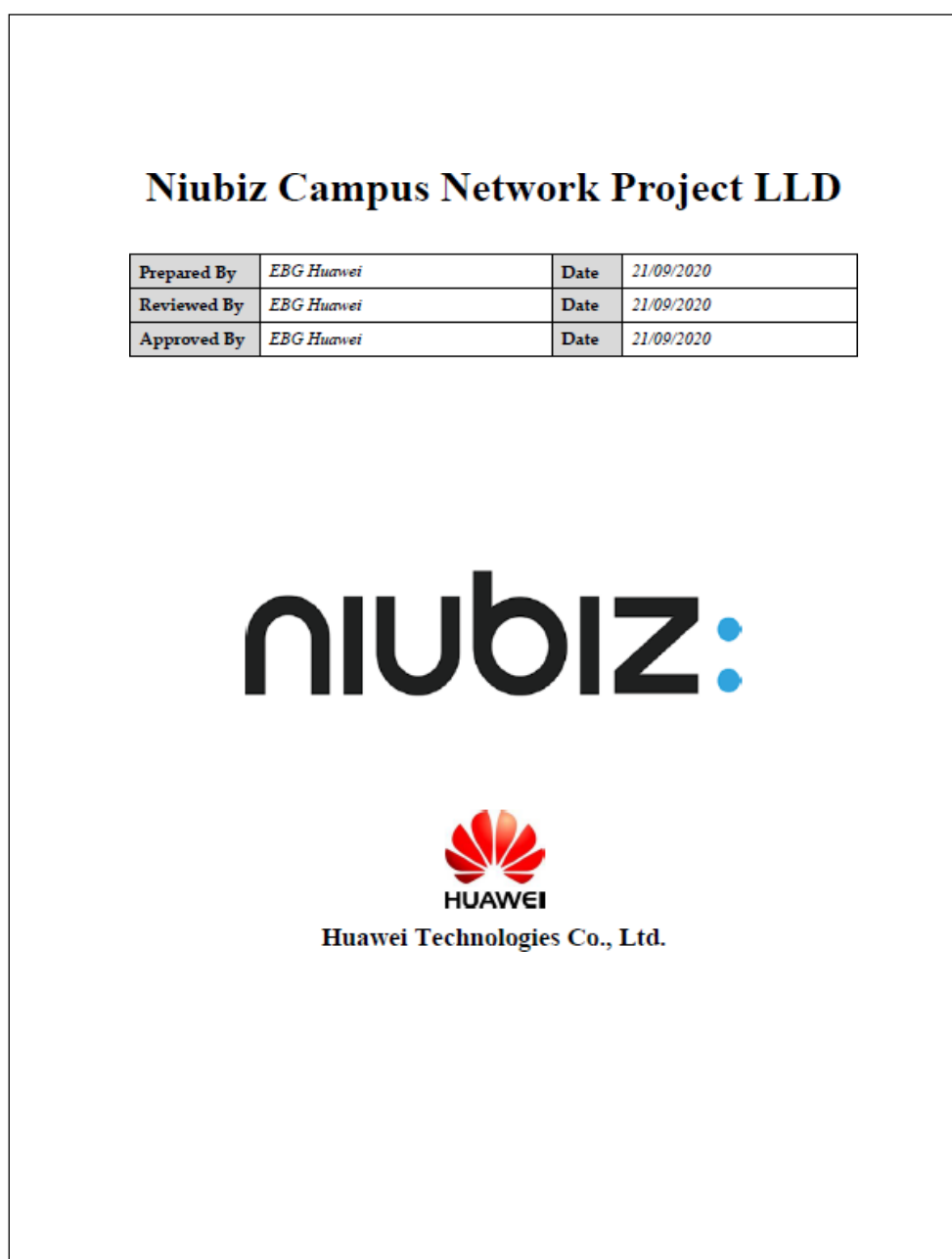


Figura: LLD Niubiz Campus Network Pag 1. Fuente: Elaboración propia

Sobre este documento

Introducción

El presente documento es la LLD de la solución Campus para el proyecto Niubiz. El diseño de topologías, parámetros y configuración de funciones, incluye la implementación de topologías y ofrece orientación para la configuración y el despliegue del proyecto.

Es posible que algunas configuraciones de este documento deban determinarse en la fase de despliegue de la red.

Audiencia

Este documento está destinado a diseñadores de redes, arquitectos de redes, administradores de redes e ingenieros de mantenimiento responsables de la red empresarial de NIUBIZ, y lectores que desean comprender los principios básicos del diseño de redes de Campus.

Pautas de Uso

Este documento proporciona una guía para el despliegue de la red. Los ingenieros de implementación deben comprender y utilizar los planes y las tecnologías que se proporcionan en este documento en combinación con las condiciones prácticas del proyecto, facilitando el despliegue y la configuración de la red.

El LLD puede ser modificado durante el despliegue y la prueba de la red.

Historial de Cambio

Los cambios entre las emisiones de documentos son acumulativos. La última edición del documento contiene todos los cambios realizados en ediciones anteriores.

Version	Date	Description
01	21-09-2020	This is the first release.

Figura: LLD Niubiz Campus Network Pag 2. Fuente: Elaboración propia

Anexo F - Configuración de los dispositivos de la red

Se proporciona las líneas de comando y una breve descripción de los protocolos a ser configurados en los equipos de la red de Campus

VLAN

Una LAN física se puede segmentar lógicamente en varias VLAN para aislar los dominios de transmisión. Los hosts dentro de una VLAN pueden comunicarse directamente solo con otros hosts en la misma VLAN y deben usar un enrutador para comunicarse con hosts en otras VLAN.

Configuración puerto de Acceso

```
<NBZ-SW> system-view
[NBZ-SW] vlan [vlan-id]
[NBZ-SW-vlan-id] description [description]
[NBZ-SW-vlan-id] quit
[NBZ-SW] interface GigabitEthernet [port]
[NBZ-SW-Ethernet0/0/1] port link-type access
[NBZ-SW-Ethernet0/0/1] port default vlan [vlan-id]
```

Configuración puerto Hybrid

```
<NBZ-SW> system-view
[NBZ-SW] vlan [VOICE-vlan-id]
[NBZ-SW-vlan-id] description [description]
[NBZ-SW] vlan [DATA-vlan-id]
[NBZ-SW-vlan-id] description [description]
[NBZ-SW-vlan-id] quit
[NBZ-SW] interface GigabitEthernet [port]
[NBZ-SW-Ethernet-port] port link-type hybrid
[NBZ-SW-Ethernet-port] port hybrid pvid vlan [vlan-id]
[NBZ-SW-Ethernet-port] voice-vlan [vlan-id] enable
[NBZ-SW-Ethernet-port] voice-vlan remark-mode vlan
```

Configuración puerto Troncal

```
<NBZ-SW> system-view
[NBZ-SW] interface GigabitEthernet [port]
[NBZ-SW-Ethernet-port] port link-type trunk
[NBZ-SW-Ethernet0/0/1] port trunk allow-pass vlan all
[NBZ-SW-Ethernet0/0/1] port trunk pvid vlan [vlan-id]
```

Configuración IP en interfaz Vlan

```
<NBZ-SW> system-view
[NBZ-SW] vlan batch [vlans-id]
[NBZ-SW] interface vlanif [vlan-id]
[NBZ-SW-Vlanif-id] ip address [ip-address] [mask]
```

Configuración DHCP Relay Agent

```
[NBZ-SW] dhcp enable
[NBZ-SW] interface vlanif [vlan-id]
[NBZ-SW-Vlanif-id] ip address [ip-address] [mask]
[NBZ-SW-Vlanif-id] dhcp select relay
[NBZ-SW-Vlanif-id] dhcp relay server-ip [ip-address server]
[NBZ-SW-Vlanif-id] quit
```

Disponibilidad

La confiabilidad de los dispositivos incluye intercambio en caliente y redundancia de dispositivos clave y módulos de servicio importantes. Esta solución implementa la confiabilidad del dispositivo mediante Stack y la redundancia de dispositivos clave y fuentes de alimentación, así como enlaces troncales. Se muestran configuraciones para la disponibilidad de los equipos de la redde Campus Miraflores, a través de las configuraciones Stack.

Configuración de Stack

```
<NBZ-SW> system-view
[NBZ-SW] interface stack-port 0/1
[NBZ-SW-stack-port0/1] port interface gigabitethernet [port-X] enable
[NBZ-SW-stack-port0/1] quit
[NBZ-SW] interface stack-port 0/2
[NBZ-SW-stack-port0/2] port interface gigabitethernet [port-Y] enable
[NBZ-SW-stack-port0/2] quit
```

Configuración de la prioridad

```
[NBZ-SW] stack slot [slot-id] priority [priority]
```

Configuración del StackID

```
[NBZ-SW] stack slot [slot-id] renumber [stack-id]
```

Link Aggregation

La agregación de enlaces Ethernet, también llamada Eth-Trunk, agrupa varios enlaces físicos en un enlace lógico para aumentar el ancho de banda del enlace, sin tener que actualizar el hardware.

Configuración de Puerto Eth-Trunk

```
<HUAWEI> system-view
[HUAWEI] sysname NBZ-SW
[NBZ-SW] interface eth-trunk [id]
[NBZ-SW-Eth-Trunkid] mode lacp
[NBZ-SW-Eth-Trunkid] quit
```

Agregar las interfaces miembros al Eth-Trunk en el Switch

```
[NBZ-SW] interface gigabitethernet [port-1]
[NBZ-SW-GigabitEthernetport-1] eth-trunk [id]
[NBZ-SW-GigabitEthernetport-1] quit
[NBZ-SW] interface gigabitethernet [port-2]
[NBZ-SW-GigabitEthernetport-2] eth-trunk [id]
[NBZ-SW-GigabitEthernetport-2] quit
```

Configuración para Establecer la prioridad del Switch para ser el actor.

```
[Switch] lacp priority [priority-id]
```

Establezca LACP priority de la interfaz y determine enlaces activos en el Switch.

```
[NBZ-SW] interface gigabitethernet [port-1]
[NBZ-SW-GigabitEthernetport-1] lacp priority [id]
[NBZ-SW-GigabitEthernetport-1] quit
[NBZ-SW] interface gigabitethernet [port-2]
[NBZ-SW-GigabitEthernetport-2] lacp priority [id]
[NBZ-SW-GigabitEthernetport-2] quit
```

Crear las vlans y configure Eth-Trunk para permitir los paquetes las Vlans pasen

```
[NBZ-SW] vlan batch [vlans-id]
[NBZ-SW] interface eth-trunk [id]
[NBZ-SW-Eth-Trunkid] port link-type trunk
[NBZ-SW-Eth-Trunkid] port trunk allow-pass vlan [vlans-id]
[NBZ-SW-Eth-Trunkid] quit
```

AAA Radius y SSH

AAA es un marco arquitectónico para configurar un conjunto de tres funciones de seguridad independientes de manera coherente. AAA proporciona una forma modular de realizar los siguientes servicios: Autenticación, Autorización y Contabilidad.

Configuración de SSH

Genere una llave local en el Switch

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] dsa local-key-pair create
Info: The key name will be: Switch_Host_DSA.
Info: The key modulus can be any one of the following: 1024, 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
```

Configure el modo de autenticación y el protocolo para acceder a las interfaces de usuario VTY 0 a 14 en AAA y SSH, respectivamente.

```
[Switch] user-interface vty 0 14
[Switch-ui-vty0-14] authentication-mode aaa
[Switch-ui-vty0-14] protocol inbound ssh
[Switch-ui-vty0-14] quit
```

Habilitar el SSH

```
[NBZ] stelnet server enable
```

Configuración de Autenticación Radius

Configure una plantilla de servidor RADIUS en el dispositivo para permitir que el dispositivo se comuniquen con el servidor RADIUS.

```
[Switch] radius-server template 1
[Switch-radius-1] radius-server authentication 10.1.6.6 1812
[Switch-radius-1] radius-server accounting 10.1.6.6 1813
[Switch-radius-1] radius-server shared-key cipher YsHsjx_202206
[Switch-radius-1] quit
```

Configure un esquema de autenticación AAA llamado sch1 y establezca el modo de autenticación en RADIUS+local.

```
[Switch] aaa
[Switch-aaa] authentication-scheme sch1
[Switch-aaa-authen-sch1] authentication-mode radius local
[Switch-aaa-authen-sch1] quit
```

Configure un esquema de contabilidad llamado acc1 y establezca el modo de contabilidad en contabilidad RADIUS.

```
[Switch-aaa] accounting-scheme acc1
[Switch-aaa-accounting-acc1] accounting-mode radius
[Switch-aaa-accounting-acc1] accounting start-fail online
[Switch-aaa-accounting-acc1] quit
```

Aplicar el esquema de autenticación AAA y la plantilla del servidor RADIUS al dominio ejemplo.com.

```
[Switch-aaa] domain example.com
[Switch-aaa-domain-example.com] authentication-scheme sch1
[Switch-aaa-domain-example.com] accounting-scheme acc1
[Switch-aaa-domain-example.com] radius-server 1
[Switch-aaa-domain-example.com] quit
[Switch-aaa] quit
```

Especifique el dominio ejemplo.com como dominio administrativo predeterminado global.

```
[Switch] domain example.com admin
```

Configuración de AAA

Configure la cuenta local en usuario1, la contraseña en YsHsjx_202206 y el nivel de privilegio en 15.

```
[Switch] aaa
[Switch-aaa] local-user user1 password irreversible-cipher YsHsjx_202206
[Switch-aaa] local-user user1 service-type ssh
[Switch-aaa] local-user user1 privilege level 15
[Switch-aaa] return
```

ACL

Las listas de control de acceso (ACL) filtran los paquetes en función de un conjunto ordenado de reglas que definen las condiciones de filtrado de paquetes, como la dirección de origen, la dirección de destino y el número de puerto de los paquetes.

Configuración de ACL

Configuración de reglas para una ACL básica

```
< NBZ-SW > system-view
[NBZ-SW] acl [acl-id]
[NBZ-SW-acl-basic-2001] rule permit source [source] [wildcard]
[NBZ-SW-acl-basic-2001] rule deny source [source] [wildcard]
```

Configuración de ACL avanzada por número

```
< NBZ-SW > system-view
[NBZ-SW] acl [acl-number]
[NBZ-SW-acl-adv-number] rule permit [protocol] source [source] [wildcard]
destination [destination] [wildcard]
```

Configuración de ACL avanzada por nombre

```
< NBZ-SW > system-view
[NBZ-SW] acl name [acl-name]
[NBZ-SW-acl-adv-deny-telnet] rule deny [protocol] destination-port eq
[protocol-port] source [source] [wildcard] destination [destination]
[wildcard]
```

SNMP

SNMP administra los elementos de la red mediante una computadora central, conocida como estación de administración de red (NMS), en la que se instala el software de administración de la red. SNMPv3 es lanzado como un protocolo recomendado sobre su antecesor SNMPv2.

Configuración de SNMP

```
snmp-agent
snmp-agent sys-info version v3
snmp-agent group v3 [group-name] authentication read-view rd write-view wt
notify-view nt
snmp-agent group v3 [group-name] privacy read-view iso-view write-view iso-
view notify-view iso-view
snmp-agent mib-view included nt iso
snmp-agent mib-view included rd iso
snmp-agent mib-view included wt iso
snmp-agent mib-view included iso-view iso
snmp-agent usm-user v3 Snmpv3mgr
snmp-agent usm-user v3 Snmpv3mgr group [group-name]
snmp-agent usm-user v3 Snmpv3mgr authentication-mode md5 //Press Enter.
huawei@123

snmp-agent trap source [interface] //Determine si utilizar la interfaz de gestión en
banda o fuera de banda en función de la situación real.
snmp-agent trap enable
```

NTP

Network Time Protocol (NTP) sincroniza la hora entre los servidores horarios y los clientes. La transmisión NTP se produce a través del puerto UDP 123.

Configuración de NTP

```
[NBZ-SW] ntp-service server disable
[NBZ-SW] ntp-service ipv6 server disable
[NBZ-SW] ntp-service authentication enable
[NBZ-SW] ntp-service authentication-keyid [key] authentication-mode hmac-sha256 cipher [password]
[NBZ-SW] ntp-service reliable authentication-keyid [key]
[NBZ-SW] ntp-service unicast-server [server-ip] authentication-keyid [key]
```

HTTPS

Hypertext Transfer Protocol Secure o HTTPS) es un protocolo de aplicación basado en el protocolo http, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP. La transmisión HTTPS se produce a través del puerto TCP 443.

Configurar HTTPS

```
<HUAWEI> system-view
[HUAWEI] http secure-server enable
```

MSTP

El Protocolo de árbol de expansión múltiple (MSTP) permite asignar varias instancias de VLAN al mismo árbol de expansión sin crear bucles. MSTP genera múltiples árboles de expansión que se utilizan de forma independiente entre sí para reenviar el tráfico en diferentes VLAN, lo que permite implementar el equilibrio de carga sin el riesgo de tormentas de transmisión.

Configuración de MSTP

```
<HUAWEI> system-view
[HUAWEI] sysname NBZ-SW
[NBZ-SW] stp region-configuration
[NBZ-SW-mst-region] region-name [region-name]
[NBZ-SW-mst-region] instance [instance-id-X] vlan [vlan-id] to [vlan-id]
[NBZ-SW-mst-region] instance [instance-id-Y] vlan [vlan-id] to [vlan-id]
[NBZ-SW-mst-region] active region-configuration
```

```
[NBZ-SW-mst-region] quit
```

En la region MST, configure el root bridge y el secondary root bridge

```
[NBZ-SW] stp instance [instance-id] root [primary/secondary]
```

Habilitar MSTP en el Switch

```
[NBZ-SW] stp enable
```

Configure Switch para calcular el costo de la ruta.

```
[NBZ-SW] stp pathcost-standard legacy
```

Configure Switch para establecer el costo de la ruta de un puerto de una región

```
[NBZ-SW] interface gigabitethernet [port]
[NBZ-SW-GigabitEthernet-port] stp instance [instance-id-X/Y] cost [cost-value]
[NBZ-SW-GigabitEthernet-port] quit
```

Configurar un puerto como un edge port

```
[NBZ-SW] interface gigabitethernet [port]
[NBZ-SW-GigabitEthernet-port] stp edged-port enable
[NBZ-SW-GigabitEthernet-port] quit
```

Configure BPDU protection en el Switch.

```
[NBZ-SW] stp bpdu-protection
```

Port Security

El conmutador realiza acciones predeterminadas después de que el número de direcciones MAC seguras alcanza el límite, esta función evita que usuarios no autorizados se comuniquen con el conmutador mediante esta interfaz y, por lo tanto, mejora la seguridad del dispositivo.

Configuración de Port Security

```
[NBZ-SW] interface gigabitethernet [port]
[NBZ-SW-GigabitEthernet-port] port-security enable
[NBZ-SW-GigabitEthernet-port] port-security mac-address sticky
[NBZ-SW-GigabitEthernet-port] port-security max-mac-num [max-value]
[NBZ-SW-GigabitEthernet-port] port-security protect-action [ protect | restrict | shutdown]
```

Calidad de Servicio (QoS)

Configurar clasificadores de tráfico (Traffic Classifiers). Crear y configurar los clasificadores de tráfico c1, c2 y c3 para clasificar paquetes según las prioridades 802.1p.

```
[NBZ-SW] traffic classifier c1
[NBZ-SW-classifier-c1] if-match 8021p 2
[NBZ-SW-classifier-c1] quit
[NBZ-SW] traffic classifier c2
[NBZ-SW-classifier-c2] if-match 8021p 5
[NBZ-SW-classifier-c2] quit
[NBZ-SW] traffic classifier c3
[NBZ-SW-classifier-c3] if-match 8021p 6
[NBZ-SW-classifier-c3] quit
```

Configurar comportamientos de tráfico (Traffic Behaviors). Configurar un comportamiento de tráfico denominado b1 y definir la acción de denegación.

```
[NBZ-SW] traffic behavior b1
[NBZ-SW-behavior-b1] deny
[NBZ-SW-behavior-b1] quit
```

Configurar los comportamientos de tráfico b2 y b3 y definir la acción del permiso.

```
[NBZ-SW] traffic behavior b2
[NBZ-SW-behavior-b2] permit
[NBZ-SW-behavior-b2] quit
[NBZ-SW] traffic behavior b3
[NBZ-SW-behavior-b3] permit
[NBZ-SW-behavior-b3] quit
```

Configurar una política de tráfico y aplicarla a una interfaz.

Crear una política de tráfico denominada p1, vincular los comportamientos de tráfico y los clasificadores de tráfico a la política de tráfico y aplicar la política de tráfico a las interfaces en la dirección entrante para filtrar paquetes.

```
[NBZ-SW] traffic policy p1
[NBZ-SW-trafficpolicy-p1] classifier c1 behavior b1
[NBZ-SW-trafficpolicy-p1] classifier c2 behavior b2
[NBZ-SW-trafficpolicy-p1] classifier c3 behavior b3
[NBZ-SW-trafficpolicy-p1] quit
[NBZ-SW] interface gigabitethernet 0/0/1
[NBZ-SW-GigabitEthernet0/0/1] traffic-policy p1 inbound
[NBZ-SW-GigabitEthernet0/0/1] quit
```

ANEXO G

Implementación del Agile Controller Campus e Implementación del eSight Campus

1. Instalación el Agile Controller Campus – NAC

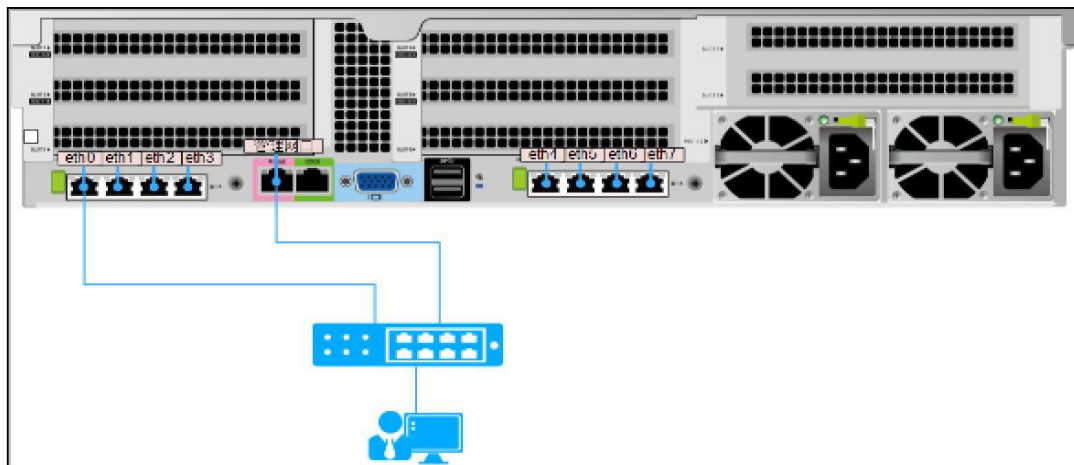


Figura: Instalación Inicial Agile Controller Campus. Fuente: Portal Soporte Huawei

Procedimiento

1. Iniciación de la sesión en el sistema operativo Euler como usuario root (la contraseña predeterminada es Changeme_123).
2. Cargado del paquete de instalación en el servidor Euler.
3. Descomprimir el paquete de instalación en el directorio actual, como/opt.

```
# cd /opt
```

- Euler-Taishan.

```
# unzip Agile_Controller-Campus_version_SM_SC_Install_Euler_TaiShan.zip
```

- Euler-X86.

```
# unzip Agile_Controller-Campus_version_SM_SC_Install_Euler.zip
```

4. Ejecutar el comando setup.sh para iniciar la instalación.

```
# cd /opt/Agile_Controller_Campus_SM_SC
```

```
# sh setup.sh
```

5. Seleccionar el inglés como idioma de instalación.
6. Leer detenidamente el acuerdo de licencia y seleccione Aceptar.

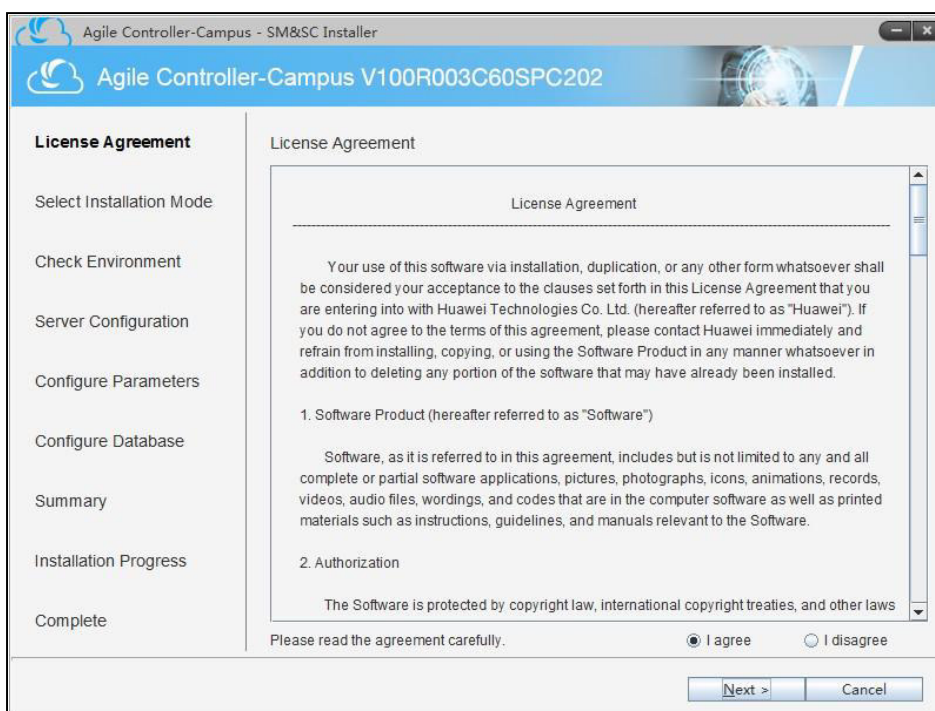


Figura: Acuerdo de Licencia – Agile. Fuente: Portal Soporte Huawei

7. Seleccionar la casilla de I agree, luego clic en Next y luego seleccionar Service Manager y Service Controller.

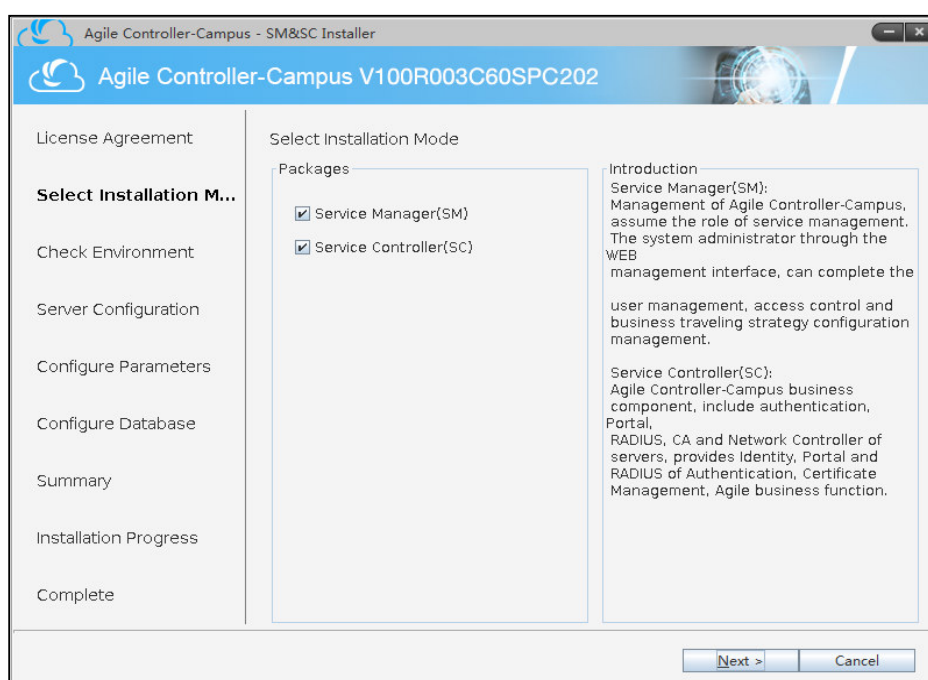


Figura: Seleccionar modo de instalación – Agile. Fuente: Portal Soporte Huawei

8. Verificar el entorno.

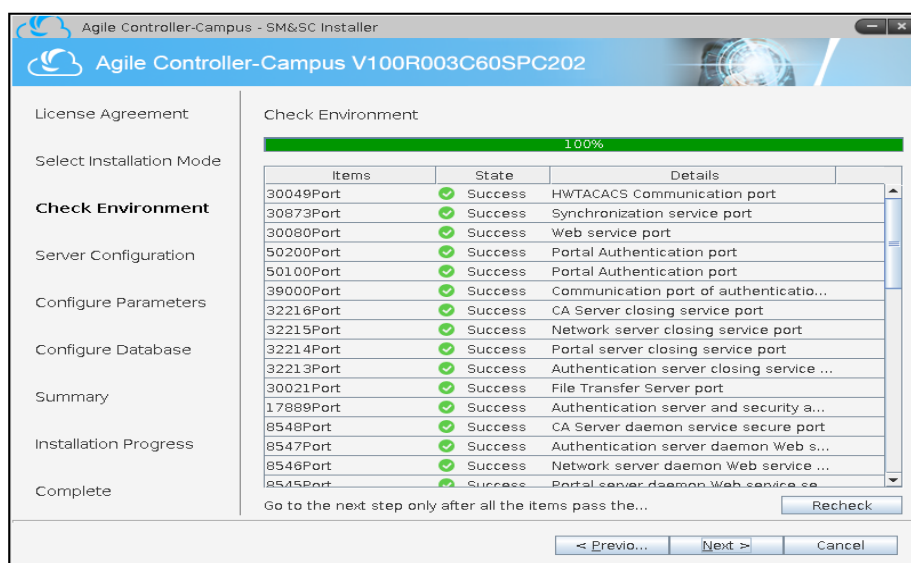


Figura: Entorno de verificación – Agile. Fuente: Portal Soporte Huawei

9. Configurar una dirección IP de gestión, una dirección IP de servicio, la memoria de pila de portales, la memoria de pila de mensajes de texto, la memoria de pila de Radius y el número de puerto FTP del servidor.

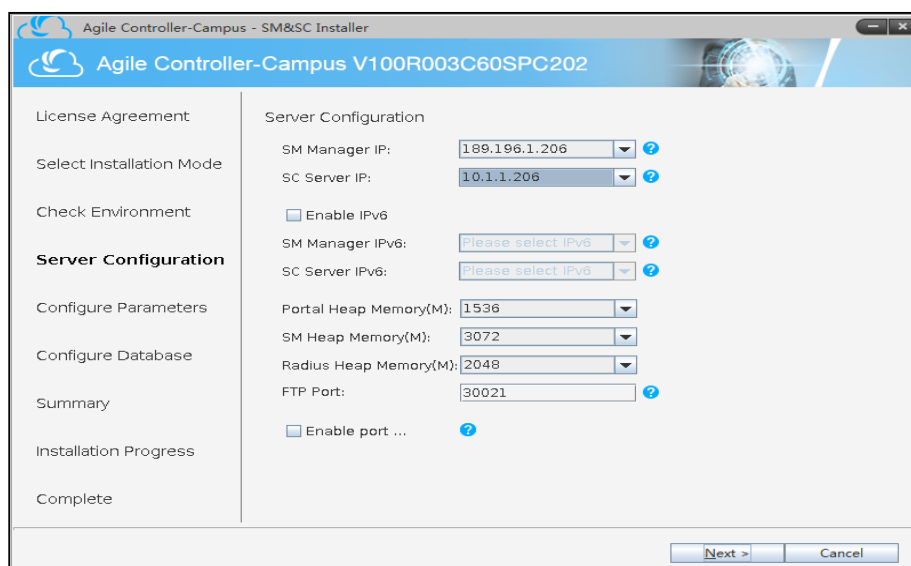


Figura: Configuración del servidor – Agile. Fuente: Portal Soporte Huawei

10. Configurar los parámetros de servidor de hora, hora estándar y especificar el directorio de instalación.

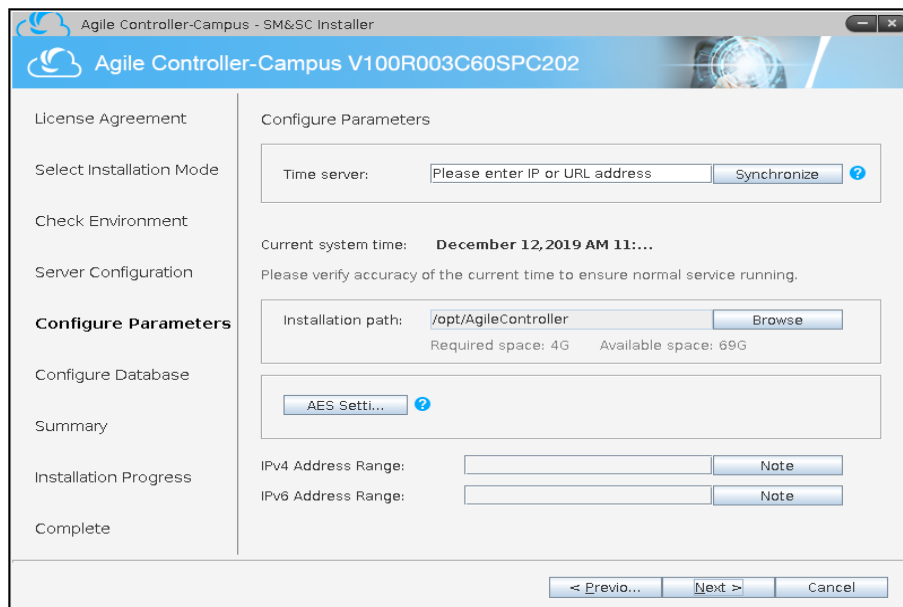


Figura: Configuración de los parámetros de instalación – Agile. Fuente: Portal Soporte Huawei

11. Configurar los parámetros de conexión de la base de datos de GaussDB.

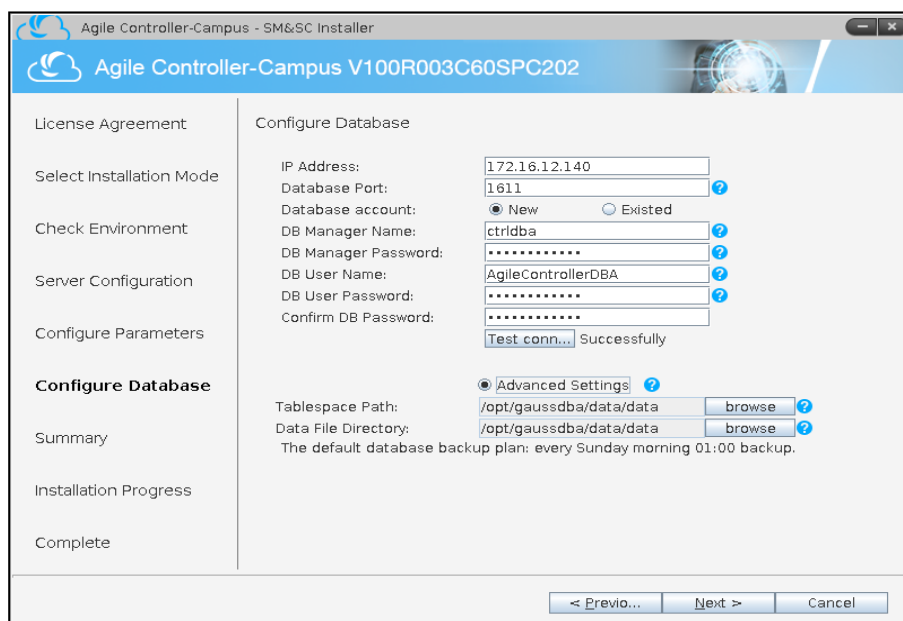


Figura: Configurar base de datos – Agile. Fuente: Portal Soporte Huawei

12. Si el sistema muestra un mensaje que indica que la base de datos ya existe, eliminarla e instalar una nueva versión o seleccionar una cuenta existente.
13. Verificar que el programa de instalación esté configurado correctamente.
14. Si el programa de instalación está configurado correctamente, instalar.
15. Finalizar la instalación.

1.1 Configuración de autorización por VLAN

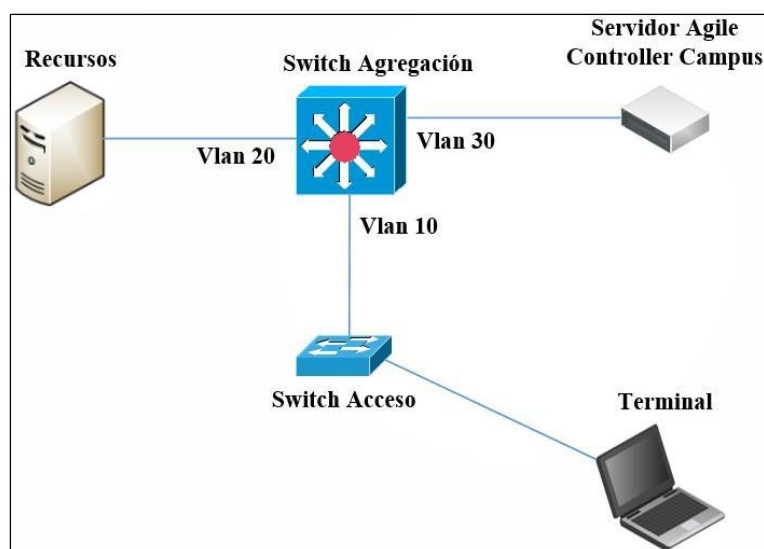


Figura Escenario para configuración de Agile Controller. Fuente: Portal Soporte Huawei

[Agile Controller-Campus] Habilite la autorización por VLAN en un resultado de autorización.

- a) Elija Policy > Permission Control > Authentication and Authorization > Authorization Result para agregar un resultado de autorización para acceder a los recursos de laboratorio.

Add Authorization Result

▼ **Basic Information**

* Name: VLAN20

Service type: ☒ Access ?
☐ Device management ?
☐ MAC bypass authentication ?

Description:

▼ **Authorization Parameter**

Before delivering attributes to a device, verify that the device supports this function.

☐ Select VLAN

VLAN: 20 ?

Dynamic ACL: ... ?

ACL number/AAA user group: ?

Security group: ... ?

Uplink bandwidth(Kbps): ?

Downlink bandwidth(Kbps): ?

Uplink DSCP: ?

Downlink DSCP: ?

OK Cancel

Figura: Agregar resultado de autorización (1) – Agile. Fuente: Portal Soporte Huawei

Elija Policy > Permission Control > Authentication and Authorization > Authorization Rule para asociar el resultado de la autorización con una regla de autorización.

Si un usuario coincide con esta regla de autorización, se otorga al usuario el permiso especificado en el resultado de la autorización (para VLAN 20).

Add Authorization Rule

Access Device Group: ...

IP Address Range: ...

SSID: ...

MDM Information

i For detailed rule matching process after MDM check is enabled, see "[How Is Authorization Rule Matched After MDM Check Is Enabled?](#)"

☐ Enable MDM check

Other Information

Terminal Group: ...

Schedule: ...

☐ AnyOffice security check result **?**

Security Check Result: **?**

Customize Condition: ...

☐ Authenticated terminals added to an AD domain **?**

Authorization Result

i Users matching authorization conditions are given the permissions specified in the authorization result field.

*Authorization result: ... **?**

Figura: Agregar resultado de autorización (2) – Agile. Fuente: Portal Soporte Huawei

1.2 Configuración de autorización por ACL dinámica

[Agile Controller-Campus] Configurar reglas dinámicas de ACL.

Elija Policy > Permission Control > Policy Element > Dynamic ACL.

Al configurar reglas de ACL dinámicas, preste atención a lo siguiente:

- La primera regla (con el número de regla más pequeño) debe permitir el acceso al servidor SC para garantizar que los usuarios autenticados puedan acceder al servidor SC.
- La última regla deniega una dirección de solo 0 para permitir el acceso a recursos específicos y deniega el acceso a otros.

Add Dynamic ACL

Basic Information

* Name:

ACL3000

Description:

Rule List

Add

Delete

	☐	Rule No.	Destination IP	Mask Length	Protocol	Port	Action
1	☐	10000	192.168.11.10	32	ALL	0	Permit
2	☐	10001	192.168.11.200	32	ALL	0	Permit
3	☐	10002	0.0.0.0	0	ALL	0	Deny

Figura: Agregar ACL Dinámica – Agile. Fuente: Portal Soporte Huawei

[Agile Controller-Campus] Seleccione una ACL dinámica en un resultado de autorización.

Elija Policy > Permission Control > Authentication and Authorization > Authorization Result.

Add Authorization Result

▼ **Basic Information**

* Name:

Service type: ☒ Access ? ☐ Device management ? ☐ MAC bypass authentication ?

Description:

▼ **Authorization Parameter**

Before delivering attributes to a device, verify that the device supports this function.

☐ Select VLAN

VLAN:

Dynamic ACL: ... ?

ACL number/AAA user group: ?

Security group: ... ?

Uplink bandwidth(Kbps): ?

Downlink bandwidth(Kbps): ?

Uplink DSCP: ?

Downlink DSCP: ?

OK Cancel

Figura: Añadir resultado de autorización (1) – Agile. Fuente: Portal Soporte Huawei

1.3 Configuración de la autenticación inalámbrica 802.1X

1. [Agile Controller-Campus] Agregue un dispositivo de control de acceso y conéctelo al Agile Controller-Campus a través de RADIUS.

Elija Recurso > Dispositivo > Administración de dispositivos y agregue el AC.

Add Device

* Name: AC

* IP address: 10.10.10.254

Description:

Authentication Parameters | XMPP | SNMP | Telnet

How Do I Configure 802.1X or Portal Authentication on the Switch or AC?

☒ Enable RADIUS. (Mandatory for 802.1X, Portal, and MAC address authentication, Free Mobility, and Service Chain.)

RADIUS Authentication Parameters

Standby device IP address:

* Device series: Huawei S Series

* Authentication/Accounting key:

* Authorization key:

Real-time accounting interval (minute): 15

After a device is added to the Agile Controller, run the `test-aaa user-name user-password radius-template template-name [chap | pap]` command on the device to check whether the authentication/accounting key is correctly configured.

OK Cancel

Figura: Agregar dispositivo – Agile. Fuente: Portal Soporte Huawei

Tabla: Parámetros del Agile Controller Campus

Parámetros de Agile Controller-Campus	Dominio
Clave de autenticación /contabilidad	Cifrado de clave compartida del servidor Radius Admin@123
Clave de autorización	autorización del servidor de radio 192.168.11.10 cifrado de clave compartida Admin@123
Intervalo de contabilidad en tiempo real (minuto)	contabilidad en tiempo real 15

2. [Agile Controller-Campus] Configure las reglas de autenticación y autorización. Los usuarios finales coinciden con las reglas según las condiciones especificadas.

- a. Elija Política > Control de permisos > Autenticación y autorización > Regla de autenticación y modifique la regla de autenticación predeterminada o cree una regla de autenticación.

Agregue el servidor AD a la fuente de datos. De forma predeterminada, una regla de autenticación solo surte efecto en la fuente de datos local. Si el servidor de AD se agrega como fuente de datos, las cuentas de AD no podrán autenticarse.

Modify Authentication Rule

Basic Parameters

* Name: Default Authentication Rule

Description: Default Authentication Rule

Authentication Information

RADIUS Proxy: ☐ Enable ?

* Data Source: 192.168.11.100, Local Data Source ...

i Select a data source based on the actual situation. If accounts are created manually or imported in a batch, select **Local Data Source**. If accounts are synchronized from the AD/LDAP server, select the specific server. If guest accounts are the accounts of a third-party application, select **Third-Party Applications Data Source**. Choose **System > External Authentication** to configure third-party application parameters first.

i Determine the supported protocols based on the data source and terminal type. For details, see **Terminals and Their Supported Functions**. If AD authentication is used, the SC server must be added to an AD domain.

☐ Default Authentication Protocol: EAP-MD5

☐ Be Compatible With Earlier Versions

* Please select the allowed authentication protocol.

☒ PAP (Local Accounts, AD, LDAP, RADIUS Token)

☒ CHAP (Local Account)

☒ EAP-MD5 (Local Account) ?

OK Cancel

Figura: Modificar Regla de Autenticación – Agile. Fuente: Portal Soporte Huawei

- b. Elija Política > Control de permisos > Autenticación y autorización > Resultado de la autorización y agregue una ACL de autorización.

El número de ACL debe ser el mismo que el configurado en el dispositivo de control de autenticación.

Add Authorization Result

Basic Information

* Name: ACL3001

Service type: ☒ Access ?
☐ Device management ?
☐ MAC bypass authentication ?

Description:

Authorization Parameter

Before delivering attributes to a device, verify that the device supports this function.

☐ Select VLAN

VLAN: ?

Dynamic ACL: ... ?

ACL number/AAA user group: 3001 ?

Security group: ... ?

Uplink bandwidth(Kbps): ?

Downlink bandwidth(Kbps): ?

Uplink DSCP: ?

Downlink DSCP: ?

OK Cancel

Figura: Añadir resultado de autorización (2) – Agile. Fuente: Portal Soporte Huawei

- c. Elija Política > Control de permisos > Autenticación y autorización > Regla de autorización y vincule el resultado de la autorización para especificar los recursos accesibles para los usuarios después de una autenticación exitosa.

Add Authorization Rule

Rule match type: ☐ Permission inheritance relationship exists between the rules

Account:

Location Information

Access Device Group:

IP Address Range:

SSID:

Other Information

Terminal Group:

Schedule:

☐ AnyOffice security check result ?

Security Check Result: Failed ?

Customize Condition:

☐ Authenticated terminals added to an AD domain ?

Authorization Result

Users matching authorization conditions are given the permissions specified in the authorization result field.

*Authorization result: ACL3001 ?

OK Cancel

Figura: Agregar regla de autorización – Agile. Fuente: Portal Soporte Huawei

Verificación

1. Use un teléfono móvil para asociarlo con el SSID dot1x_access e ingrese un nombre de usuario y una contraseña de dominio de AD.
2. Obtenga una dirección IP en el segmento de red 172.16.21.0/24 después de una autenticación exitosa y acceda a los recursos de Internet usando esta dirección IP.
3. Ejecute los comandos `display access-user` y `display access-user user-id user-id` en el AC para ver información detallada del usuario en línea.
4. Elija Recurso > Usuario > Registro de RADIUS en Agile Controller-Campus para ver los registros de RADIUS.

2. Implementación del eSight Campus

2.1 Instalación del eSight Campus

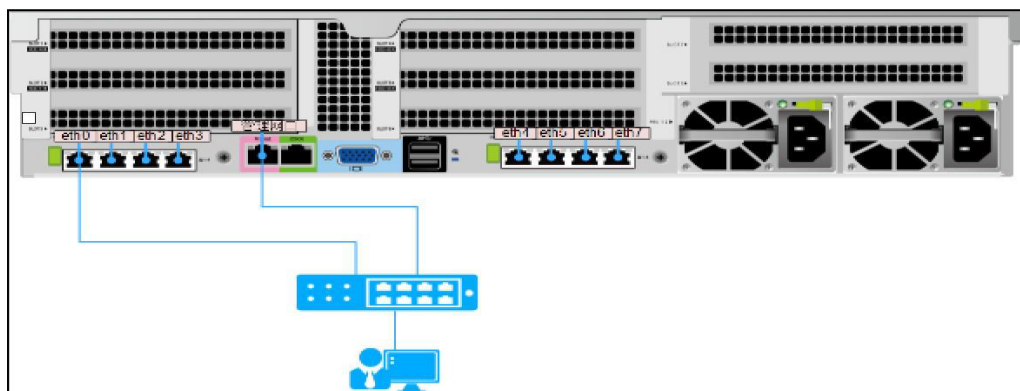


Figura: Instalación Inicial Servidor eSight. Fuente: Portal Soporte Huawei

Procedimiento

1. Inicie sesión en el servidor eSight como usuario root.
2. Ejecute el siguiente comando para cancelar el intervalo de tiempo de espera:

```
# exportar TMOUT=0
```

3. Ejecute el siguiente comando para crear el directorio temporal /opt/install:

```
# mkdir -p /opt/instalar
```

4. Utilice FileZilla para cargar el paquete de software eSight_V300R010C00SPC500_Euler_aarch64.zip en el directorio "/opt/install" como usuario root. Para saber cómo usar FileZilla.
5. Ejecute los siguientes comandos en la CLI para descomprimir el paquete de instalación:

```
# cd /optar/instalar
```

```
#unzip eSight_V300R010C00SPC500_Euler_aarch64.zip -d /opt/install/eSight
```

6. Ejecute el script de instalación silenciosa.

```
# cd /opt/instalar/eSight
```

```
# sh setup_silent.sh
```

```

Seleccione el idioma [1: chino, 2: inglés]:
>2
Seleccione el tipo de dirección IP [1:IPv4,2:IPv6][predeterminado:IPv4]:
>1
Seleccione la dirección IP del servidor [1: 10.10.10.1] [predeterminado:
10.10.10.1]:
>1
Ingrese el puerto del servidor [1024~49151][predeterminado: 8080]:
>8080
Ingrese el directorio de instalación [predeterminado:/opt/eSight]:
>

```

7. Asegúrese de que todos los parámetros estén configurados correctamente y continúe. La instalación tarda unos 10 minutos. Si se muestra la siguiente información, la instalación está completa.

```

8. =====< Instalación exitosa >=====
Finalizar

```

2.2 Adición de dispositivos de red a eSight

Hay tres métodos disponibles para agregar dispositivos a eSight.

Tabla: Adición única de dispositivos en eSight

Adición única	Se agrega un dispositivo a la vez. Este modo se aplica cuando desea agregar uno o varios dispositivos a eSight durante el funcionamiento normal de la red.
---------------	--

- Adición única

1. Elija Recurso > Común > Agregar recurso > Agregar recurso en el menú principal.

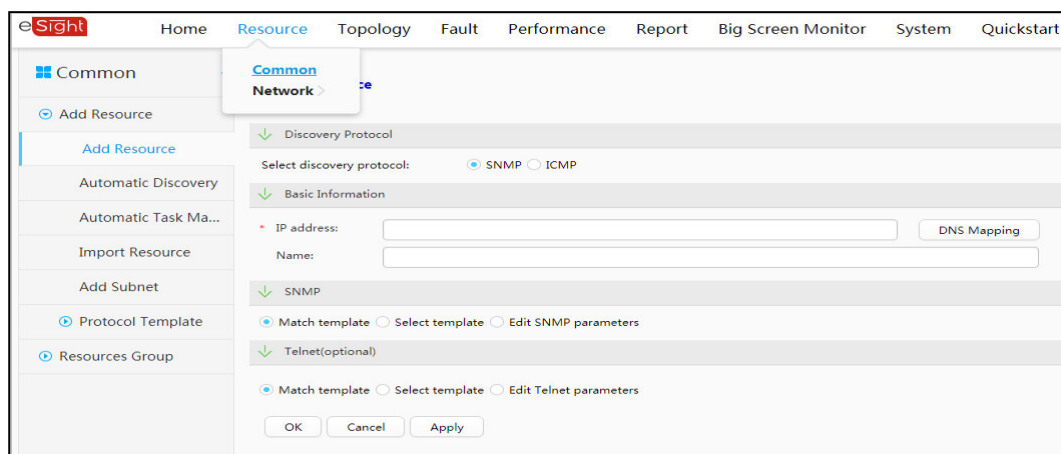


Figura: Agregar recurso – eSight. Fuente: Portal Soporte Huawei

2. Configure los parámetros de SNMP y Telnet.

Discovery Protocol

Select discovery protocol: ☒ SNMP ☐ ICMP

Basic Information

* IP address: DNS Mapping Subnet: ...

Name:

SNMP

☐ Match template ☐ Select template ☒ Edit SNMP parameters

Warning: Set parameters in the template based on the SNMP information on the device. The security level of SNMP V3 is higher than the security levels of SNMP V1 and SNMPv2c. When SNMP V3 is used, the options of Authentication protocol are HMAC_SHA and HMAC_MD5. The security level of HMAC_SHA is higher than the security level of HMAC_MD5 but still cannot meet requirements of NIST specifications. Set Privacy protocol to AES_128 to enhance the security. Authentication password and encryption password are suggested not to be consistent.

Version:

* Security name:

Authentication protocol:

Privacy protocol:

Timeout interval (s):

* Port:

Authentication password:

Encryption password:

Figura: Configurar SNMP – eSight. Fuente: Portal Soporte Huawei

Figura: Configurar Telnet – eSight. Fuente: Portal Soporte Huawei

2.3 Administrar y mantener dispositivos de Red

1. Elija Recurso > Red > Equipo > Dispositivo de red en el menú principal.

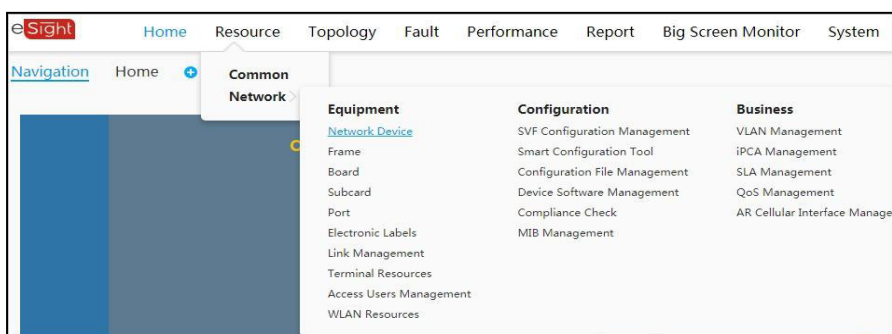


Figura: Dispositivo de red en menú principal eSight. Fuente: Portal Soporte Huawei

2. Haga clic en el nombre del dispositivo que se administrará y mantendrá, vea la información del dispositivo y realice operaciones según los requisitos del sitio.

Tabla: Operaciones en dispositivos de red eSight

Operación relacionada	Entrada de operación
Ver información de alarma.	Lista de alarmas en el árbol de navegación de la izquierda.
Modificar los parámetros de Telnet.	Parámetros de Telnet en el árbol de navegación.

Modificar parámetros SNMP.	Operación: Parámetros de protocolo > Parámetros de SNMP en el árbol de navegación de la izquierda.
Sincronizar datos del dispositivo.	Ver > Información básica en el árbol de navegación de la izquierda y haga clic en Sincronización a la derecha.

2.4 Gestión de los equipos de red en la vista de topológica

Procedimiento

1. Elija Topología > Gestión de topología en el menú principal.



Figura: Gestión de topología en el menú principal – eSight. Fuente: Portal Soporte Huawei

2. Ver alarmas en el panel de alarmas. Si existen alarmas, se recomienda borrarlas primero.
 - a. Haga clic en el icono de alarma para mostrar la página de alarmas actuales.
 - b. Busque la alarma en la página Alarmas actuales. Hacer clic  junto a la alarma para cambiar rápidamente a la topología física.

☐	Severity ▾	Name ▾	Alarm Source ▾	First Occurrence Time ▾	Location Info	Operation
→	☐ Critical	Link Down	headquarters	2014-12-17 19:53:23	If Name=10GE0/0/1, If Index=5	

Figura: Búsqueda de la alarma – eSight. Fuente: Portal Soporte Huawei

- c. En la página Topología física, verifique el estado del dispositivo y la posición del dispositivo en la red. Si el color del dispositivo es rojo en la vista de topología, la alarma existe. Jack necesita enviar una advertencia a otro personal de administración del dispositivo para informar que el dispositivo está defectuoso y que la falla se está rectificando.
- d. Rectificar la falla. Si es una alarma simple y común, rectifique la falla basándose en la experiencia del mantenimiento. Si se trata de una alarma compleja, rectifique la falla consultando Experiencia en manejo en la página Alarmas actuales.

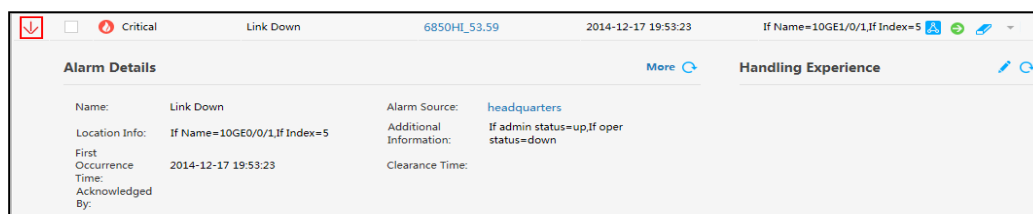


Figura: Verificación de la alarma – eSight. Fuente: Portal Soporte Huawei

3. Ver la topología de la red del campus.
4. Vea los indicadores de rendimiento de los dispositivos principales.
 - a. Mueva el puntero sobre el icono de un dispositivo para ver el uso promedio de la CPU y la memoria del dispositivo.

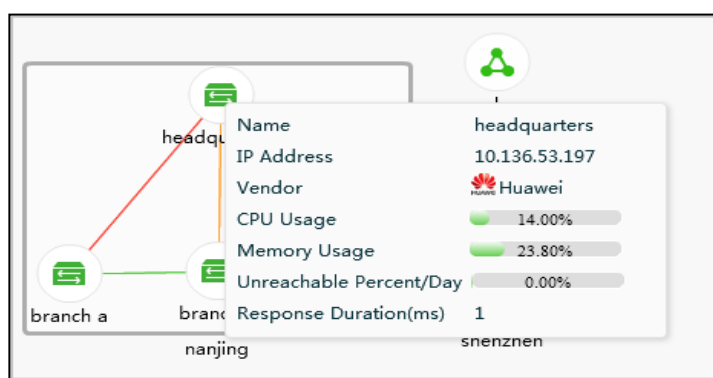


Figura: Indicadores de rendimiento de los dispositivos – eSight. Fuente: Portal

Sugerencias

- Durante el mantenimiento de la red, la topología física se usa comúnmente para el monitoreo de la red.
- eSight proporciona varios menús después de hacer clic con el botón derecho en la topología física. Puede completar las operaciones de mantenimiento de rutina en la vista de topología física.

2.5 Visualización de datos de rendimiento

Se muestra el procedimiento, a partir de la futura implementación del servidor eSight, para visualizar el rendimiento de los dispositivos de la red (status de los equipos, uso de CPU, uso de memoria) desde el panel de visualización del servidor eSight.

Procedimiento

1. Vea los KPI (Key performance Indicators – Indicadores de desempeño) del grupo de dispositivos que se recopilan automáticamente en la página para consultar la información del indicador de rendimiento. Después de instalar eSight, se crea automáticamente una tarea de grupo de dispositivos preconfigurada.
 - a. Elija Rendimiento > Datos de rendimiento en el menú principal.

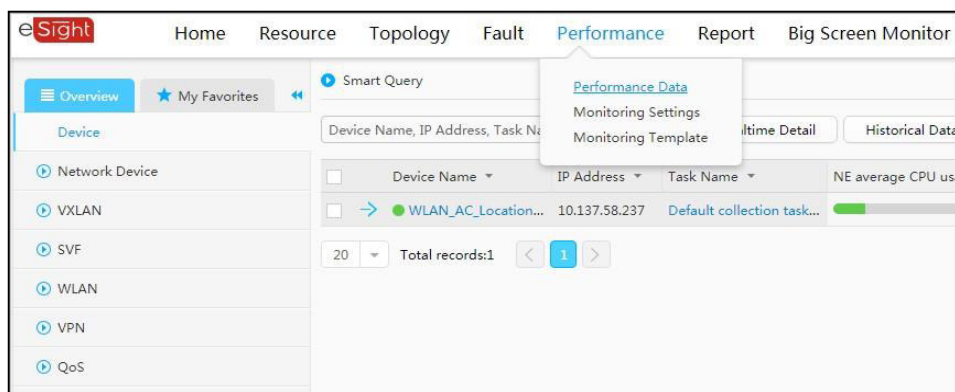
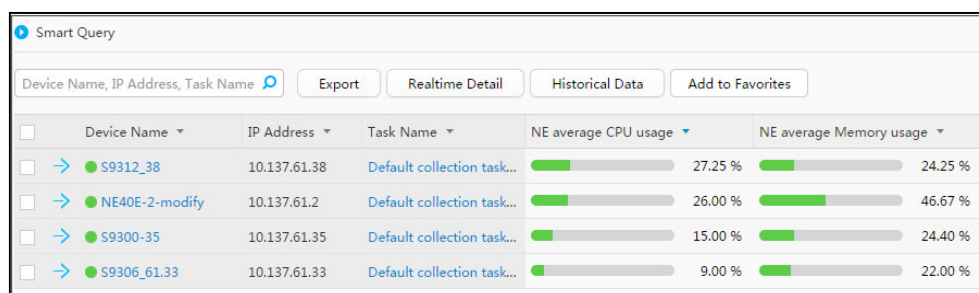


Figura: Datos de rendimiento – eSight. Fuente: Portal Soporte Huawei

- b. Introduzca el AP o cualquier otro dispositivo de red en el cuadro de búsqueda. Se muestra la información de seguimiento de todos los puntos de acceso que cumplen los criterios de búsqueda.



Smart Query					
Device Name, IP Address, Task Name 🔍					
Export Realtime Detail Historical Data Add to Favorites					
	Device Name ▾	IP Address ▾	Task Name ▾	NE average CPU usage ▾	NE average Memory usage ▾
☐	→ ● S9312_38	10.137.61.38	Default collection task...	27.25 %	24.25 %
☐	→ ● NE40E-2-modify	10.137.61.2	Default collection task...	26.00 %	46.67 %
☐	→ ● S9300-35	10.137.61.35	Default collection task...	15.00 %	24.40 %
☐	→ ● S9306_61.33	10.137.61.33	Default collection task...	9.00 %	22.00 %

Figura: Información de KPIs – eSight. Fuente: Portal Soporte Huawei

2.6 Agregar un servidor

Procedimiento

1. Elija Recurso > Común en el menú principal.

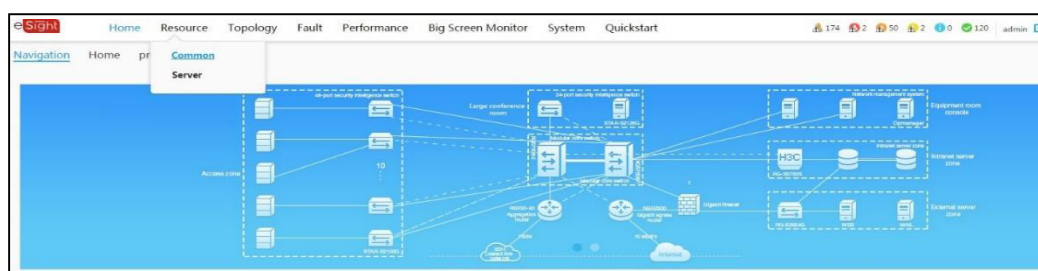


Figura: Recurso común en menú principal – eSight. Fuente: Portal Soporte Huawei

2. En el árbol de navegación de la izquierda, elija Agregar recurso > Agregar recurso.

3. En la lista Servidor, seleccione el tipo de servidor que desea agregar.

Los tipos de servidores disponibles son rack, blade, de alta densidad, KunLun, de terceros y heterogéneos.

4. Configurar la información básica del servidor y el protocolo de acceso.

Server -> Rack Server

Basic Information

Type: Rack server

* IP address:

Application Identification:

Asset State:

Device Location:

* Subnet:

Name:

Storage Time:

Asset Source:

Resource Pool:

Discovery Protocol

Set the parameters in the template based on the SNMP protocol information on the device. You are advised to use SNMPv3, which is more secure. When SNMPv3 is used, you are advised to set Authentication protocol to HMAC_SHA256 or HMAC_SHA and Proprietary protocol to AES_128 or AES_256 to improve security.

When a server is discovered, the eSightMgmt account is automatically created on the device. The account is used for logging in to eSight and invoking the interface on the device.

Protocol: ☒ SNMP ☐ IPMI ☐ Redfish+SNMP ☐ Redfish(Mobile Enterprise Logo)

SNMP Protocol

* Type:

* Retry times(1-20):

* Port(1-65535):

Authentication protocol:

Data encryption protocol:

SNMP template:

* Timeout period(1-60 seconds):

* Username:

* Authentication password:

* Data encryption password:

OK Cancel Apply

Figura: Configuración servidor y protocolo de acceso – eSight. Fuente: Portal Soporte Huawei

Anexo H – Cobertura inalámbrica

Cobertura Access Points



Figura: Cobertura AP - Piso de prueba. Fuente: Test Simulador Huawei



SINR Diagrama Simulación (Signal-to-interference-plus-noise ratio)

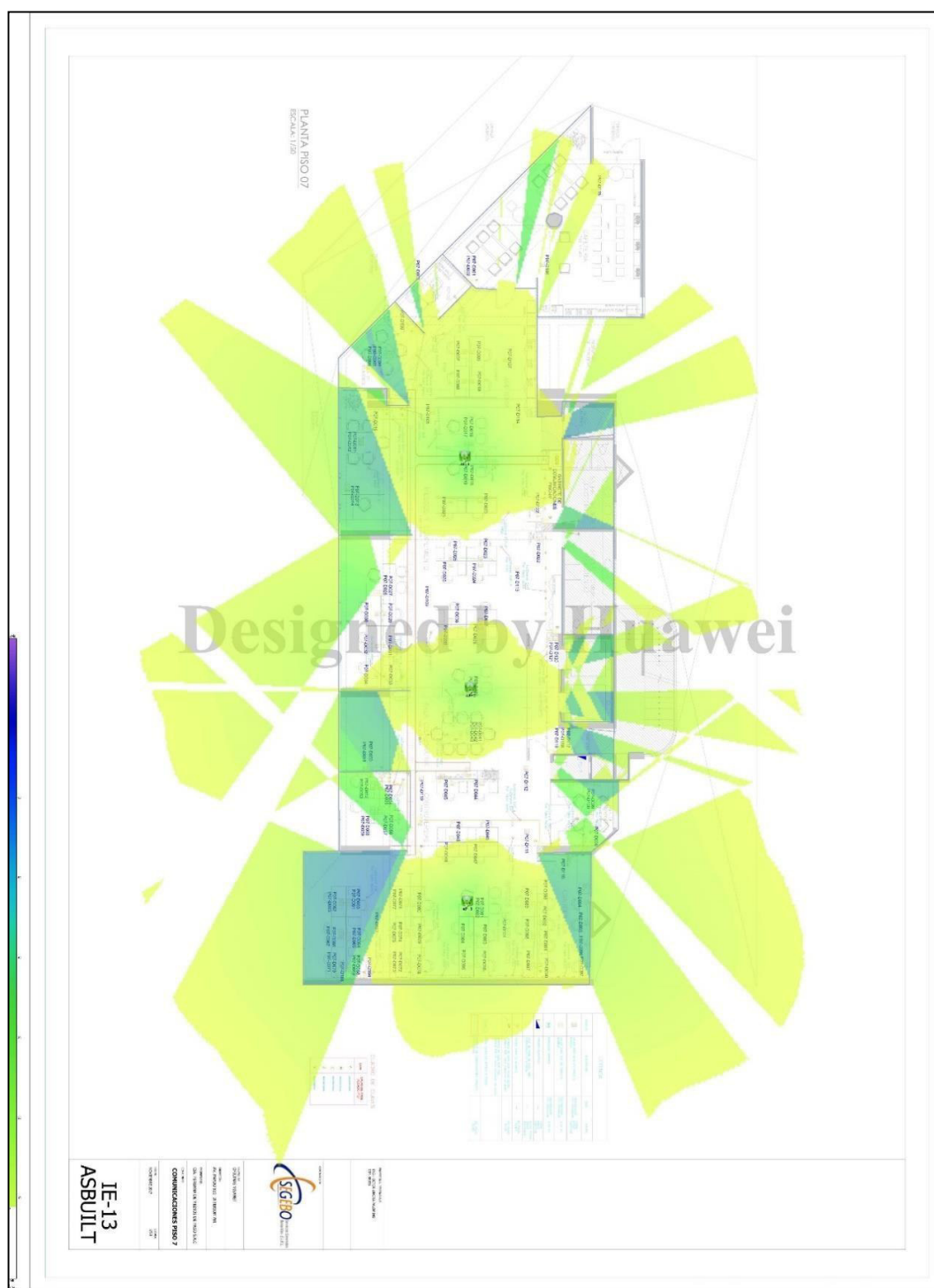


Figura: Relación del nivel de señal a ruido. Fuente: Test Simulador Huawei