Evolución de red en sucursales a SD-WAN

José Luis Vargas Bravo
Administración de redes y sistemas operativos
Grado de Ingeniería Informática

José Manuel Castillo Pedrosa

Fecha Entrega (Junio 2020)

Dedicatoria y Agradecimientos

A mis padres, Luis y Eulogia, por la educación y valores que me dieron, y aunque ya no están entre nosotros, siempre he sentido su apoyo con cada uno de mis pasos en la vida. Ahora con este logro, siento una alegría especial, porque sé que estarán muy orgullos de aquel niño travieso, su pequeño.

A mi hijo Alejandro, lo más grande que he hecho, haré y tendré siempre en mi vida y en mi corazón. Gracias, por todas esas tardes y fines de semana de estudio juntos, por tus visitas constantes a mi lugar de estudio, por tu besos, por tu abrazos, porque sin todo eso, este camino hubiera sido mucho más duro. Gracias "Yalex".

Y sobre todo, a Mayte, mi esposa. El amor de mi vida. La persona que siempre está a mi lado, me apoya, me completa, me entiende y me hace feliz. Gracias, por tu fuerza, aliento y optimismo en todo lo que hago y especialmente en este gran proyecto universitario en el que me embarqué hace ya cuatro años. Gracias de corazón.

Y a mi amigo, compañero y mejor persona, Carlos de Manuel, por su total disponibilidad a ayudarme, aconsejarme y a enseñarme todo sobre el mundo de las redes y como no, de la SD-WAN. He aprendido mucho de ti, muchas gracias, querido amigo. Siempre te estaré agradecido.

Gracias a Carlos Coque y Javier Pérez de Aruba, por su disposición y contribución para realizar este proyecto.

Finalmente, a José Manuel Castillo, mi director del TFG, porque a pesar de las grandes dificultades que se han presentado de manera imprevista durante la realización de este trabajo, siempre ha confiado en mí y ha estado dispuesto a dedicarme su tiempo y apoyo. Gracias de verdad.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Evolución de Red en sucursales a SD-WAN
Nombre del autor:	José Luis Vargas Bravo
Nombre del consultor:	José Manuel Castillo Pedrosa
Fecha de entrega (mm/aaaa):	06/2020
Área del Trabajo Final:	Administración de Redes y Sistemas Operativos
Titulación:	*Grado de Ingeniería Informática*

Resumen del Trabajo (máximo 250 palabras):

Hoy día, la forma de trabajar de las organizaciones conectadas en red ha cambiado notablemente en estos últimos años, y mucho más, cuando su trabajo lo desarrollan desde más lugares y de forma geográficamente distribuida. Todo ello, junto con Internet como foco de negocio empresarial, hace necesario que las instituciones adapten y evolucionen sus sistemas de comunicaciones tradicionales a los cambios que los actuales servicios y aplicaciones demandan para una alta disponibilidad, un óptimo rendimiento y una buena gestión de sus infraestructuras.

Este TFG tiene como finalidad ofrecer un análisis de la posible evolución de conexión de red tradicional en sucursales remotas hacia una solución de red SD-WA y para ello, el estudio del trabajo se realiza sobre tres ejes:

En primer lugar, el estudio de la red actual de una institución universitaria distribuida geográficamente y la descripción de su infraestructura en producción. Un análisis, respecto a costes recurrentes, necesidades de ancho de banda y problemas de administración y gestión de incidencias en aquellas sucursales remotas conectadas mediante enlaces alquilados, tipo MPLS o punto a punto.

En segundo lugar, el estudio de la tecnología SD-WAN, con una amplia exposición de lo que es, lo que aporta, sus ventajas y los distintos costes a los que una organización tendría que hacer frente al implantar esta infraestructura.

Finalmente, el análisis de un piloto de red SD-WAN, entre el nodo principal y una sucursal remota, desde el que se extraerán las conclusiones respecto a la evolución de la conexión red tradicional a SD-WAN.

Abstract (in English, 250 words or less):

Today, the way in which networked organizations work has changed significantly in recent years, and much more, when their work is carried out from more places and geographically distributed. All this, together with the Internet as a focus for business, makes it necessary for institutions to adapt and evolve their traditional communication systems to the changes that current services and applications demand for high availability, optimal performance and good management of their infrastructures.

The purpose of this dissertation is to offer an analysis of the possible evolution of the traditional network connection in remote branches towards an SD-WA network solution and for this, the study of the work is carried out on three axes:

First, the study of the current network of a geographically distributed university institution and the description of its production infrastructure. An analysis regarding recurring costs, bandwidth needs and problems of administration and incident management in those remote branches connected on rented links, such as MPLS or point-to-point.

Secondly, the study of SD-WAN technology, with an exposition of what it is, what it contributes, its advantages and the different costs to implement this infrastructure in an organization.

Finally, the analysis of an SD-WAN network pilot, between the main node and a remote branch, with the conclusions extracted regarding the evolution of the traditional network connection to SD-WAN.

Palabras clave (entre 4 y 8):

Red, redundancia, escalabilidad, flexibilidad, despliegue, monitorización, sucursal y servicios

Índice

Lista de figuras

1. Introducción

1.1. Contexto y justificación del trabajo

En la actualidad, la forma de trabajar de organizaciones e instituciones conectadas en red ha cambiado notablemente en los últimos años, pero es ahora cuando este cambio se hace más latente fruto de que el trabajo se realiza en más lugares distribuidos de manera global. Además, Internet es un foco de atención para ellas, donde por un lado, de manera significativa su negocio se desarrolla y logran una ventaja competitiva respecto a sus competidores y por otro lado, existe un aumento significativo de usuarios heterogéneos.

Este nuevo escenario obliga a que el medio sea necesariamente adaptativo para dar cabida a los distintos actores que entran en escena: nuevas sucursales, distintos usuarios estáticos y móviles, así como los servicios y aplicaciones en la nube.

Fruto de la reflexión anteriormente expuesta, este proyecto tiene como finalidad ofrecer una solución de conexión, de forma genérica, que sea aplicable a cualquier organización que tenga sucursales con la necesidad de estar conectados, pero con un plus de ventajas sobre los sistemas de interconexión más tradicionales.

Así, los sistemas tradicionales de conexión, como MPLS, son una primera opción para muchas organizaciones debido a su madurez, ya que es altamente confiable y proporciona alta disponibilidad. Sin embargo, también es cierto que tiene unos elevados costes recurrentes y no proporciona redundancia por si sola, ya que necesita de la contratación de accesos redundantes, lo que aumenta los costes recurrentes muy por encima del ratio coste/beneficio que la organización puede soportar.

La WAN definida por software (SD-WAN) da respuesta a las desventajas que ofrece MPLS, proporcionando una mayor escalabilidad, un menor coste recurrente y una óptima calidad de servicio, es decir, un conjunto de beneficios como se puede ver a continuación:

- Costes reducidos, al permitir implementarse con soluciones de conexión de bajo coste.
- Mejora del rendimiento, pues enruta el tráfico eficazmente a través de la red en función las necesidades de la aplicación subyacente.
- Proporciona una mayor agilidad, debido a que la capa de red se abstrae al permitir usar distintos mecanismos de transporte diferentes (fibra, cable, xDSL, 4G ...).
- Proporciona redundancia y más capacidad de ancho de banda, debido al uso de múltiples conexiones en cada ubicación.

- Mide en tiempo real: la latencia y perdida de paquetes de cada una de las conexiones. Además, aplica enrutamiento basado en políticas, para así enviar el tráfico específico a través del transporte más apropiado.

Por todo lo anteriormente expuesto, esta tecnología da respuesta al cambio tecnológico que el mundo empresarial necesita, pues por un lado, se encuentra en presupuesto y por otro lado, resuelve los inconvenientes de las conexiones tradicionales.

1.2. Objetivos del Trabajo

Los objetivos que se persiguen en la realización de este proyecto son:

- Conocer y detallar la infraestructura de red actual de una organización para conectarse con sus sucursales mediante enlaces tradicionales de operador de telecomunicaciones
- Explicar los problemas y desventajas, en base a los enlaces tradicionales, que sufren las comunicaciones de las sucursales remotas de una organización
- Explicar las ventajas y desventajas de la tecnología SD-WAN frente a la infraestructura actual de conexión con sucursales
- Conocer y detallar los requerimientos específicos de las sucursales candidatas a evolucionar hacia la tecnología SD-WAN
- Conocer el equipamiento e infraestructuras necesarios para la implementación de SD-WAN en la organización
- Conocer detalladamente los distintos costes de la tecnología SD-WAN:
    - Costes de inversión
    - Costes de puesta en producción
    - Costes recurrentes
- Implementar una red SD-WAN entre sucursal y sede central
- Conocer el resultado de distintas pruebas de monitorización y rendimiento de la red
- Estar en disposición de evaluar la nueva infraestructura respecto a la anterior, en base a: costes, gestión, administración, calidad de servicio, redundancia, escalabilidad...

1.3. Enfoque y método seguido

En primer lugar, se estudiará la infraestructura actual de red en producción de la organización, donde se analizará ampliamente el entorno actual de la red de la empresa y de manera más específica, las conexiones con sus sucursales mediante enlaces tradicionales alquilados a operadores. A partir de ese análisis

se explicarán los inconvenientes y problemas derivados de estos tipos de conexiones tanto a nivel técnico como económico.

Para ello, se mantendrán distintas reuniones con el personal de la Unidad de Redes y Sistemas de la organización, así como el acceso a la documentación necesaria para la elaboración del estudio y análisis de su situación de red actual.

En segundo lugar, se hará un estudio detallado de la tecnología SD-WAN, para exponer de manera detallada los requerimientos específicos respecto a instalaciones e infraestructuras necesarias para evolucionar una conexión de red de las sucursales de una organización. Además, por un lado, se estudiarán los beneficios que SD-WAN puede ofrecer respecto a los sistemas tradicionales analizando las ventajas e inconvenientes que SD-WAN ofrece a las organizaciones y por otro lado, se analizarán detalladamente los distintos costes que la implantación de una red SD-WAN supondría para una organización.

Finalmente, se implementará un piloto de red SD-WAN en la organización, donde evaluaremos objetivamente la nueva infraestructura de conexión de sucursales respecto a la inicial, en base al estudio de diferentes parámetros: costes, administración, calidad de servicio, escalabilidad, redundancia... Analizando su comportamiento mediante pruebas de rendimiento y monitorización de la red.

Para ello, se contará por un lado, con el equipamiento de red necesario que un proveedor proporcionará para tal fin y por otro lado, con la colaboración de la institución, en particular con su Área TIC, lo que permitirá llevar a cabo tanto la instalación, como el estudio de la nueva infraestructura.

1.4. Planificación del Trabajo

Para la realización de la entrega final de este proyecto (TFG) es necesaria la entrega de varios trabajos parciales dentro de la fecha límite establecida.

En este apartado se incluye una tabla donde se puede observar las entregas parciales de forma genérica y sus fechas de entrega, un cronograma detallado generado a partir de un diagrama de Gantt, así como el diagrama de Gantt donde se está detallada la planificación completa del proyecto a realizar.

Descripción de la entrega	Fecha
Tema del proyecto	24-02-2020
PEC1- Propuesta del plan de trabajo	06-03-2020
PEC2- Primera entrega del TFG	10-04-2020
PEC3- Segunda entrega del TFG	15-05-2020
Entrega final del TFG	08-06-2020
Inicio del tribunal	09-06-2020
Fin del tribunal	19-06-2020

Ilustración 1: Tabla de fechas claves

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Evolución de red en sucursales a SD-WAN**	**122 días**	**mié 19/02/20**	**vie 19/06/20**	
2	Consensuar tema del proyecto con el consultor	6 días	mié 19/02/20	lun 24/02/20	
3	**PEC1 - Propuesta del Plan de Trabajo**	**11 días**	**lun 24/02/20**	**vie 06/03/20**	**2**
4	Recopilar información	2 días	mar 25/02/20	mié 26/02/20	
5	Desarrollo de los puntos del plan de trabajo	4 días	jue 27/02/20	dom 01/03/20	4
6	Entrega de primera versíon al consultor	1 día	lun 02/03/20	lun 02/03/20	5
7	Realización de correcciones	3 días	mar 03/03/20	jue 05/03/20	6
8	Entrega en el REC de la PEC1	1 día	vie 06/03/20	vie 06/03/20	7
9	**PEC2 - Primera entrega del TFG**	**35 días**	**sáb 07/03/20**	**vie 10/04/20**	
10	**Desarrollo del apartado de infraestructura actual**	**20 días**	**sáb 07/03/20**	**jue 26/03/20**	
11	Recopilación de información de la infraestructura en producción	13 días	sáb 07/03/20	jue 19/03/20	
12	Incorporación de la información a la memoria	7 días	vie 20/03/20	jue 26/03/20	11
13	**Inicio del desarrollo del apartado de infraestructura SD-WAN**	**15 días**	**vie 27/03/20**	**vie 10/04/20**	
14	Recopilación de información de la tecnología SD-WAN	10 días	vie 27/03/20	dom 05/04/20	
15	Incorporación de la información a la memoria	4 días	lun 06/04/20	jue 09/04/20	14
16	Entrega en el REC de la PEC2	1 día	vie 10/04/20	vie 10/04/20	15
17	**PEC3 - Segunda entrega del TFG**	**35 días**	**sáb 11/04/20**	**vie 15/05/20**	
18	**Finalización del apartado de infraestructura SD-WAN**	**7 días**	**sáb 11/04/20**	**vie 17/04/20**	
19	Estudio de costes	4 días	sáb 11/04/20	mar 14/04/20	
20	Incorporación de la información a la memoria	3 días	mié 15/04/20	vie 17/04/20	19
21	**Creación de piloto SD-WAN**	**28 días**	**sáb 18/04/20**	**vie 15/05/20**	
22	Definición	5 días	sáb 18/04/20	mié 22/04/20	
23	Especificación	5 días	jue 23/04/20	lun 27/04/20	22
24	Diseño	5 días	mar 28/04/20	sáb 02/05/20	23
25	Construcción	7 días	dom 03/05/20	sáb 09/05/20	24
26	Pruebas	5 días	dom 10/05/20	jue 14/05/20	25
27	Incorporación de la información a la memoria	27 días	sáb 18/04/20	jue 14/05/20	
28	Entrega en el REC de la PEC3	1 día	vie 15/05/20	vie 15/05/20	27
29	**Entrega final del TFG**	**24 días**	**sáb 16/05/20**	**lun 08/06/20**	
30	Incorporar a la memoria las conclusiones del trabajo	4 días	sáb 16/05/20	mar 19/05/20	
31	Revisar y realizar posibles correcciones a la memoria	5 días	mié 20/05/20	dom 24/05/20	30
32	Relizar la presentación	14 días	lun 25/05/20	dom 07/06/20	31
33	Entrega final del TFG	1 día	lun 08/06/20	lun 08/06/20	32
34	**Tribunal**	**11 días**	**mar 09/06/20**	**vie 19/06/20**	
35	Contestar a las cuestiones planteadas por el tribunal	11 días	mar 09/06/20	vie 19/06/20	

Ilustración 2: Cronograma de tareas

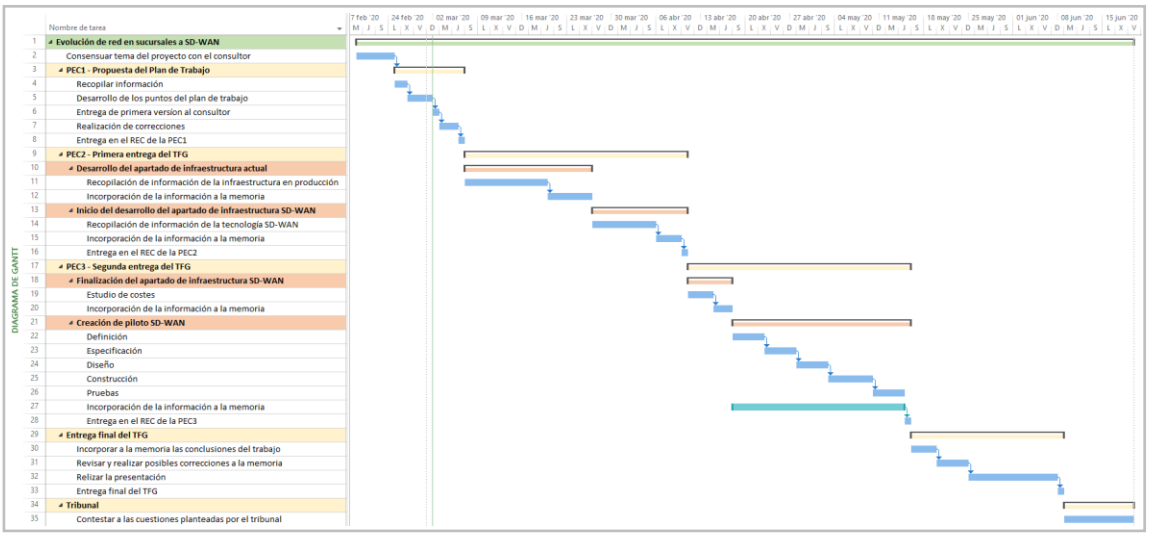


Ilustración 3: Diagrama de Gantt

1.5. Breve sumario de productos obtenidos

Este trabajo analizará la posible evolución de los sistemas de conexión tradicionales, como MPLS, que actualmente son usados para conectar las sucursales de una institución hacia una solución con tecnología SD-WAN, y para ello los productos obtenidos son los siguientes:

En primer lugar, un estudio de la situación de red actual de una organización, donde se describirá su infraestructura en producción. Además, se profundizará en aquellas sedes que utilizan servicios alquilados de operador basados en tecnología MPLS y circuitos alquilados punto a punto. También, se analizarán los costes y los problemas actuales de configuración, administración y la gestión de incidencias.

En segundo lugar, un estudio referido a la evolución hacia el nuevo modelo SD-WAN, donde se analizarán las nuevas infraestructuras y los distintos costes asociados: inversión, puesta en producción, recurrentes. Así como, la exposición de sus ventajas e inconvenientes.

Finalmente, se creará un piloto SD-WAN para demostrar la viabilidad funcional del nuevo diseño, así como sus ventajas frente al modelo anterior.

1.6. Breve descripción de los otros capítulos de la memoria

Este proyecto estará constituido por tres apartados principales: La infraestructura inicial, la infraestructura SD-WAN y la Creación de un piloto de red SD-WAN sobre una sucursal. A continuación, se realiza una descripción breve sobre cada uno de los apartados:

La infraestructura inicial

En este apartado se analizará la situación actual de una organización sobre la que se estudiará la evolución de red de una de sus sucursales al modelo SD-WAN. Se detallará la infraestructura en producción y sus costes actuales recurrentes y se analizarán los problemas actuales de cortes, gestión y administración, que las sucursales tienen en su conexión de red mediante enlaces tradicionales alquilados a operador de comunicaciones.

La infraestructura SD-WAN

En este apartado se introducirán los conceptos básicos de esta tecnología de conexión de red, exponiendo objetivamente sus ventajas e inconvenientes frente a las conexiones tradicionales de red, como MPLS. Además, se analizarán las necesidades de infraestructura y equipamiento necesarios para llevar a cabo una evolución de la conexión de red tradicional a SD-WAN, estudiando los distintos costes asociados.

La creación de un pilo SD-WAN sobre una sucursal

Finalmente, en este apartado se llevará a cabo la creación de un piloto SD-WAN que conectará una sucursal con la organización. Se realizarán diferentes

pruebas para demostrar la viabilidad de la evolución de conexión tradicional de sucursales a SD-WAN

1.7. Análisis y gestión de riesgos

Ningún proyecto está exento de diversos riesgos, en el caso que nos ocupa el mayor riesgo al que está expuesto este trabajo está centrado sin lugar a duda en el capítulo: "*Creación de piloto SD-WAN*" que es el eje fundamental del proyecto que aporta un mayor valor a este trabajo.

A continuación se exponen los riesgos y la forma de mitigarlos:

- **Riesgo**

  La institución no permite crear el piloto SD-WAN sobre su infraestructura, a pesar de su gran interés en el estudio de una posible evolución de red en sus sucursales durante los contactos establecidos con su dirección.

  Mitigación

  Se implementará la solución SD-WAN sobre otras dos sucursales que nos permitan llevar a cabo el estudio sobre el piloto.

- **Riesgo**

  El proveedor de la solución SD-WAN finalmente no nos entrega el equipamiento en el tiempo establecido a pesar de su compromiso antes de la propuesta de este tema para el TFG.

  Mitigación 1

  Se dispone de cierto margen de tiempo para buscar otro proveedor con disposición a prestarnos el equipamiento en tiempo y forma.

  Mitigación 2

  En caso de no encontrar un segundo proveedor que facilite el equipamiento necesario y debido al tiempo tan ajustado que existe para realizar este proyecto, se llevará a cabo una implementación de una solución SD-WAN sobre un simulador. De esta manera, se podrá llevar a cabo un análisis de la nueva implementación mediante los datos obtenidos en las distintas pruebas realizadas.

Los riesgos anteriormente descritos son los considerados más importantes, pues afectan de forma importante a la realización de este trabajo y además, son los más difíciles de controlar debido a la existente dependencia de terceros para un caso de éxito.

2. Infraestructura inicial

Esta primera parte del trabajo consiste en el estudio de la infraestructura de red que una institución universitaria tiene actualmente en producción. Así, este capítulo se centrará en conocer, con el detalle necesario, como es la comunicación de red entre sus distintas sedes y sucursales para poder llevar a cabo la finalidad que este trabajo tiene: analizar la viabilidad de evolución de red en las sucursales, que actualmente se comunican mediante enlaces alquilados de operador, a SD-WAN.

Se quiere advertir, que la exposición de la infraestructura de red en producción de esta institución tiene como único objetivo el que se persigue en el ámbito de este trabajo.

2.1. Exposición de infraestructura en producción

La exposición de la infraestructura de red en producción de la institución universitaria, objeto de estudio, se introducirá mediante distintos apartados a lo largo de este capítulo para una mejor comprensión. Esta institución tiene una particular distribución geográfica al disponer de cuatro campus. Cada uno de estos campus está ubicado en una capital de provincia de una misma comunidad autónoma, situada en el estado español.

Además, la mayoría de estos campus, como se verá más adelante, están conectados a distintas sucursales mediante enlaces alquilados a un operador de telecomunicaciones.

2.1.1. Red IP

El direccionamiento de red IP de esta institución universitaria está divida en zonas y estas a su vez en los diferentes campus. Sin embargo, en la actualidad esta subdivisión está sufriendo modificaciones para poder albergar las nuevas necesidades de red, como por ejemplo: las redes necesarias para incorporar CPDs remotos en la nube que la organización necesita para implementar nuevos servicios.

Algunas de las zonas en las que está dividido el direccionamiento público son: PDI (Personal docente e investigador), PAS (Personal de administración y servicios), Investigación, DMZ, entre otras.

Esta universidad tiene asignada la subred IP pública: 161.67.0.0/16, que ha estado hasta ahora distribuyendo mediante un direccionamiento específico para todos sus clientes: cable e inalámbricos.

Subnet ID	Subnet Address	Host Address Ragnd	Broadcast Address
1	161.67.0.0	161.67.0.1 – 161.67.255.254	161.67.255.255

Ilustración 4: Subred IP pública

Actualmente, la unidad de redes y sistemas del área TIC de esta universidad está realizando un proceso de cambio para adaptar las redes de los clientes con IP pública a direccionamiento privado. A fecha de redacción de este trabajo todos los clientes de red inalámbrica ya utilizan direccionamiento privado.

Subnet ID	Subnet Address	Host Address Range	Broadcast Address
1	172.16.0.0	172.16.0.1 – 172.31.255.254	172.31.255.255

Ilustración 5: Subred IP privada

Algunas de las zonas en las que se divide el direccionamiento privado son: telefonía IP, televisión universitaria, puntos de información universitarios, los clientes WLAN, servidores comunes, servidores de datos corporativos, la gestión de la red como nodos, transporte troncal, transporte provincial/local, direccionamiento para clientes, CPD externo (actualmente solo con Azure)...

2.1.2. Red troncal

La red troncal de esta institución universitaria comunica sus cuatro campus y sus distintas sucursales mediante distintas tecnologías de conexión y transporte. A cada uno de los distintos campus se les denominarán con las siglas: AB, CR, CU y TO. El nodo principal está ubicado en el campus CR, donde además de estar la ubicación del CPD y de prestarse los servicios de seguridad perimetral, también se realiza la interconexión principal con Internet.

Una primera aproximación de la distribución geográfica de los distintos Campus se puede ver en la siguiente imagen, en ella se observan los cuatro campus sobre un mapa real de la comunidad autónoma y su interconexión mediante RedIRIS Nova(*).

(*) En el Anexo I se puede encontrar información adicional respecto a RedIRIS Nova.

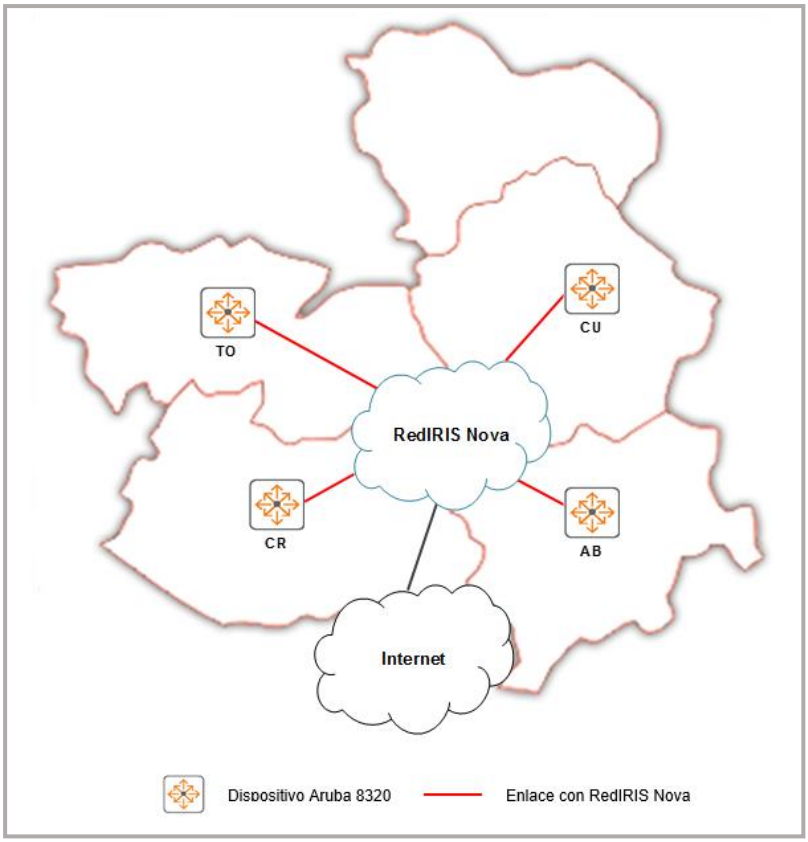


Ilustración 6: Red troncal de los nodos principales

La comunicación entre las sedes de AB, CR, CU y TO la proporciona RedIRIS Nova mediante interfaces ópticos de nivel 2. Así, los campus de CR y AB disponen de tres interfaces ópticos cada uno y dos interfaces ópticos en cada uno de los campus de CU y TO. Cada uno de los interfaces ópticos tienen implementado un servicio asociado para la comunicación con otro de los campus.

A esta universidad se le ha asignado un identificador de VLAN para realizar una red IP de transporte entre todos sus campus. La unidad de redes y sistemas de la propia institución es la responsable de la gestión y configuración de la electrónica de la red troncal, así como de la interlocución con RedIRIS.

La siguiente tabla muestra la asignación de identificador de vlan y red IP:

VLAN	Sede	Sede	Red IP
395	CR	TO	172.16.4.16/29
394	CR	CU	172.16.4.0/29
392	CR	AB	172.16.4.32/29
295	AB	TO	172.16.4.24/29
294	AB	CU	172.16.4.9/29

Ilustración 7: Tabla de identificadores de vlan y red IP

Los identificadores de la columna VLAN de la tabla anterior siguen un criterio de asignación realizado por la unidad de redes y sistemas. De esta manera, el criterio es el siguiente: el primer dígito, el de mayor peso, es la sede de mayor relevancia, el segundo dígito el operador y el tercer dígito es la sede remota. La asignación numérica para las distintas sedes es 2 para AB, 3 para CR, 4 para Cu y 5 para TO, y la asignación numérica para el operador RedIRIS Nova es el 9.

Los nodos principales de la red troncal se encuentran en los siguientes edificios de cada una de las sedes principales o campus de la organización:

Sede	Edificio
CR	CTIC
AB	Vicerrectorado
TO	F. de Armas
CU	Servicios Generales

Ilustración 8: Tabla de ubicación de nodos principales

Cada uno de los nodos principales dispone de dos dispositivos Aruba 8320[(1)] para dar redundancia a sus interconexiones con otros campus y a la distribución de sus distintos centros. Además, también disponen de un conmutador Aruba 2930F[(1)] conectado de forma redundante para dar cabida, tanto a los servicios de distribución 1000BatseT, como a servicios del propio nodo, por ejemplo: los servidores locales.

La unidad de redes y sistemas de esta institución universitaria basa la redundancia en la implementación de las siguientes características:

- La utilización de las diferentes capacidades VSX[(2)] de los equipos Aruba 8320. Cabe incluir que el nivel 2 y 3 de estos equipos usan VSX o VRRP cuando el SVI[(3)] tiene mapeadas diferentes redes IP
- El uso de dos o más interconexiones con otros campus y protocolo de enrutamiento dinámico OSPF
- El uso de dos interfaces de nivel 2 tanto al propio nodo como a otros centros interconectados al nodo
- La instalación de dos fuentes de alimentación por dispositivo Aruba 8320

Las interconexiones de los nodos principales con RedIRIS Nova están implementadas mediante interfaces ópticos de nivel 2. A cada enlace de comunicación le corresponde una VLAN, que es etiquetada en la configuración de cada conmutador.

[(1)] En el Anexo II se puede encontrar información adicional respecto al equipamiento Aruba de la red troncal.
[(2)] En los aparatados: Anexo II y Glosario se puede encontrar información adicional respecto a VSX.
[(3)] En el Anexo III se encuentra una configuración tipo de un interfaz físico, así como del SVI.

Tal como se ha comentado anteriormente, todos los nodos principales están dotados de una pareja de Aruba 8320 y al menos un conmutador Aruba 2930F conectado y redundado. Sin embargo, actualmente la institución solo dispone de un interfaz óptico de 10 G para configurar un enlace de comunicación entre campus(*).

En un futuro inmediato, se prevé una renovación de los servicios de RedIRIS Nova que permitirá el uso de interfaces de 100 Gbps y 10x10 Gbps para cada nodo, lo que permitirá la duplicación de interfaces para cada enlace entre campus y por lo tanto, una redundancia completa a nivel troncal.

En la siguiente imagen se muestra la visión real y más completa de la red troncal actual de la institución universitaria.

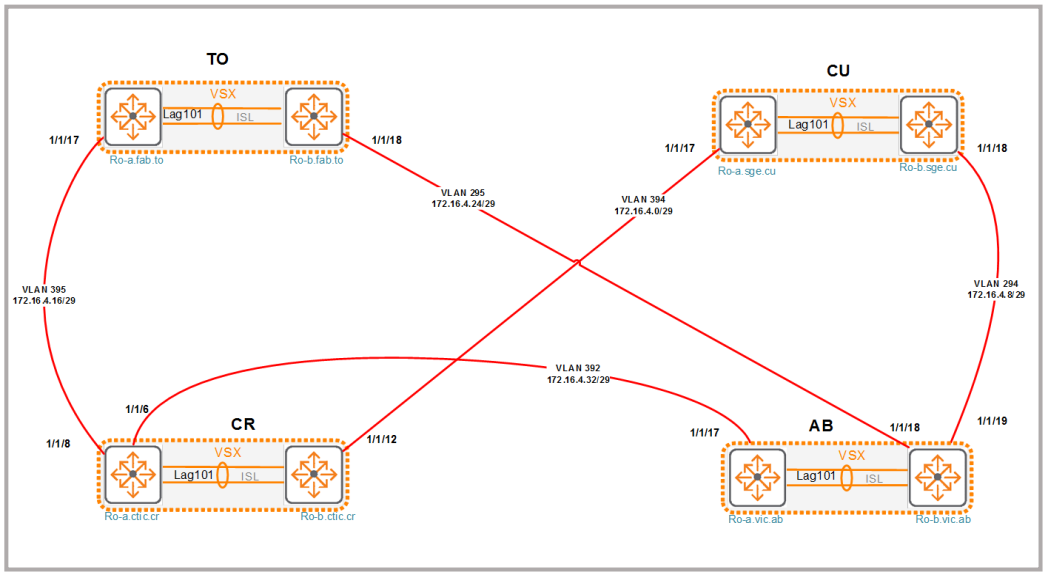


Ilustración 9: Diagrama de red troncal con RedIRIS NOVA(**)

2.1.3. Red de distribución y acceso por campus

En este apartado, se explicará como el nodo principal de cada campus se conecta con el resto de los edificios o sucursales bien mediante enlaces propios o alquilados a un operador de comunicaciones, estos últimos son los que serán tratados con más profundidad en el apartado: "2.2 Principales sucursales objeto de estudio", motivo principal de este trabajo.

2.1.3.1. Campus CR

En el edificio CTIC de este campus se encuentran tanto el nodo principal del campus, así como el de la institución universitaria. Esto es así, debido a que por un lado, se encuentran los enlaces troncales contra los campus CU, AB y TO mediante RedIRIS Nova y por otro lado, se encuentra el acceso a Internet, el CPD físico y toda la infraestructura hacia el CPD virtual de Azure.

(*) En el Anexo IV se explica la conexión de los enlaces de RedIRIS Nova y la electrónica de la organización.

(**) **Fuente de la imagen:** *Arquitectura General Servicio de Comunicaciones*.(2019). De Manuel, Carlos.

Así pues, desde este edificio se distribuye la red a más de 20 edificios, entre centros universitarios y otros nodos de distribución. Esta distribución se realiza mediante fibras propias redundadas a excepción de la realizada a dos centros, denominados mediante el nombre de AL y AGR, que lo hace mediante enlaces alquilados a un operador de comunicaciones.

Estos dos centros AL y AGR se analizan en el apartado: "2.2 Principales sucursales objeto de estudio" de este documento, pues ambas por su características son candidatas a una posible evolución de red a SD-WAN.

En la siguiente ilustración podemos ver una aproximación en forma gráfica:

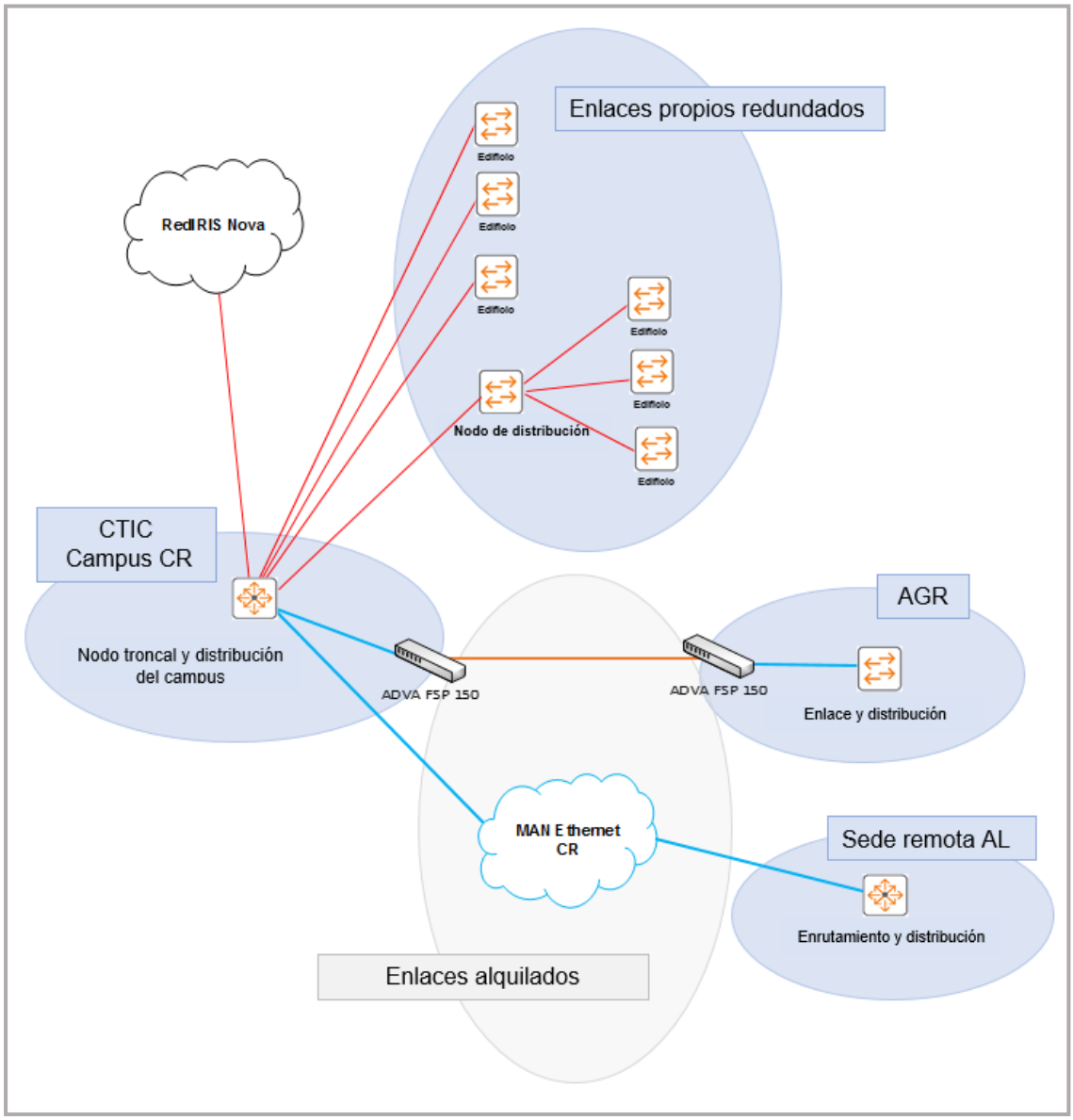


Ilustración 10: Distribución de Red Campus CR

Nota: Los enlaces propios redundados se han dibujado simples para una mayor claridad en la ilustración

2.1.3.2. Campus AB

En este campus, el edificio del Vicerrectorado alberga el nodo principal que está interconectado con el resto de los campus (CR, CU y TO) mediante enlaces proporcionados por RedIRIS Nova.

Al igual que pasaba en el campus CR, desde este nodo se distribuye la red mediante fibras propias redundadas tanto al propio edificio como a más de 14 edificios (centros universitarios). Sin embargo, tiene la necesidad de conectar al edificio FMyF mediante un enlace alquilado.

Así, este edificio FMyF del campus AB será objeto de este estudio con más detalle en el apartado: "2.2 Principales sucursales objeto de estudio", de este documento.

En la siguiente ilustración podemos ver una aproximación en forma gráfica:

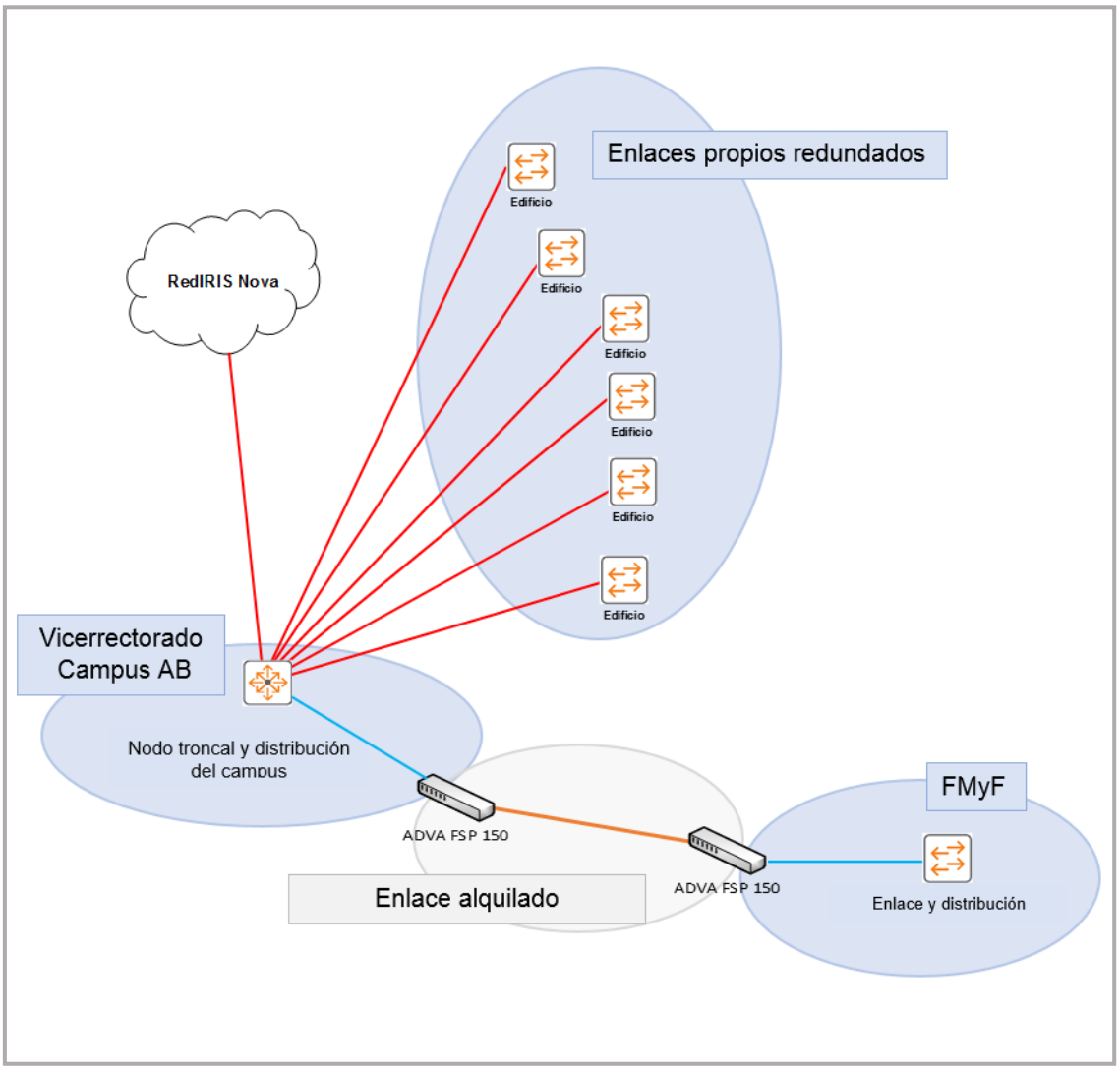


Ilustración 11: Distribución de Red campus AB

Nota: Los enlaces propios redundados se han dibujado simples para una mayor claridad en la ilustración

2.1.3.3. Campus CU

En el edificio de Servicios Generales de este campus se encuentra su nodo principal, que está conectado con los campus de CR y AB mediante enlaces proporcionados por RedIRIS Nova.

Desde este nodo se distribuye la red a un total 7 edificios (entre centros universitarios y otro nodo de distribución, que distribuye a otros centros) mediante fibras propias redundadas. El campus CU es el más pequeño de los cuatro que componen esta institución universitaria y no dispone de centros que puedan ser motivo de estudio para una posible evolución a SD-WAN.

En la siguiente ilustración podemos ver una aproximación en forma gráfica:

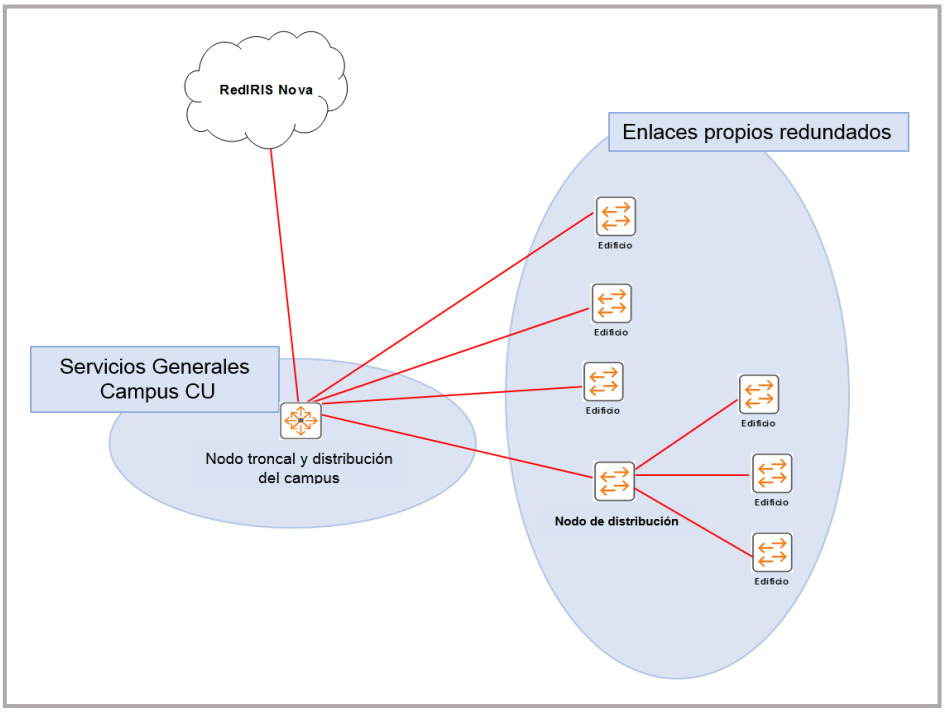


Ilustración 12: Distribución de Red campus CU

2.1.3.4. Campus TO

Este campus dispone de una complejidad añadida, pues aunque el nodo principal del campus está en la Fábrica de Armas, también este campus dispone de instalaciones en el casco histórico de la ciudad. Esta característica aumenta la complejidad de la distribución de la red, debido a la falta de infraestructuras de comunicaciones propias, así como la dificultad de encontrar servicios de operador.

Esta dificultad radica en la protección del patrimonio de carácter histórico que tiene esta parte del campus, en relación con la consecución de obras civiles necesarias para dotarla de infraestructuras.

Así pues, desde el nodo principal se distribuye la red mediante fibras propias redundadas a más de 14 edificios (centros universitarios), pero también hace uso

Nota: Los enlaces propios redundados se han dibujado simples para una mayor claridad en la ilustración

de enlaces alquilados para por un lado, conectar tanto a una sucursal que dista a más de 100 km del nodo principal (que denominamos TA), como a otro edificio del campus denominado TR y por otro lado, un nodo de distribución, ubicado en el casco histórico denominado SPM, tal como hemos comentado anteriormente.

Por lo tanto, y por la comentada complejidad que este campus tiene, el nodo ubicado en SPM distribuye la red a otros dos edificios LO y PA mediante enlaces alquilados también. En este campus existen varias sucursales (TA, TR, SPM, LO y PA) que se estudiará con más detalle en el apartado: "2.2 Principales sucursales objeto de estudio", de este documento.

La siguiente ilustración ayuda a entender la complejidad de interconexión del campus TO:

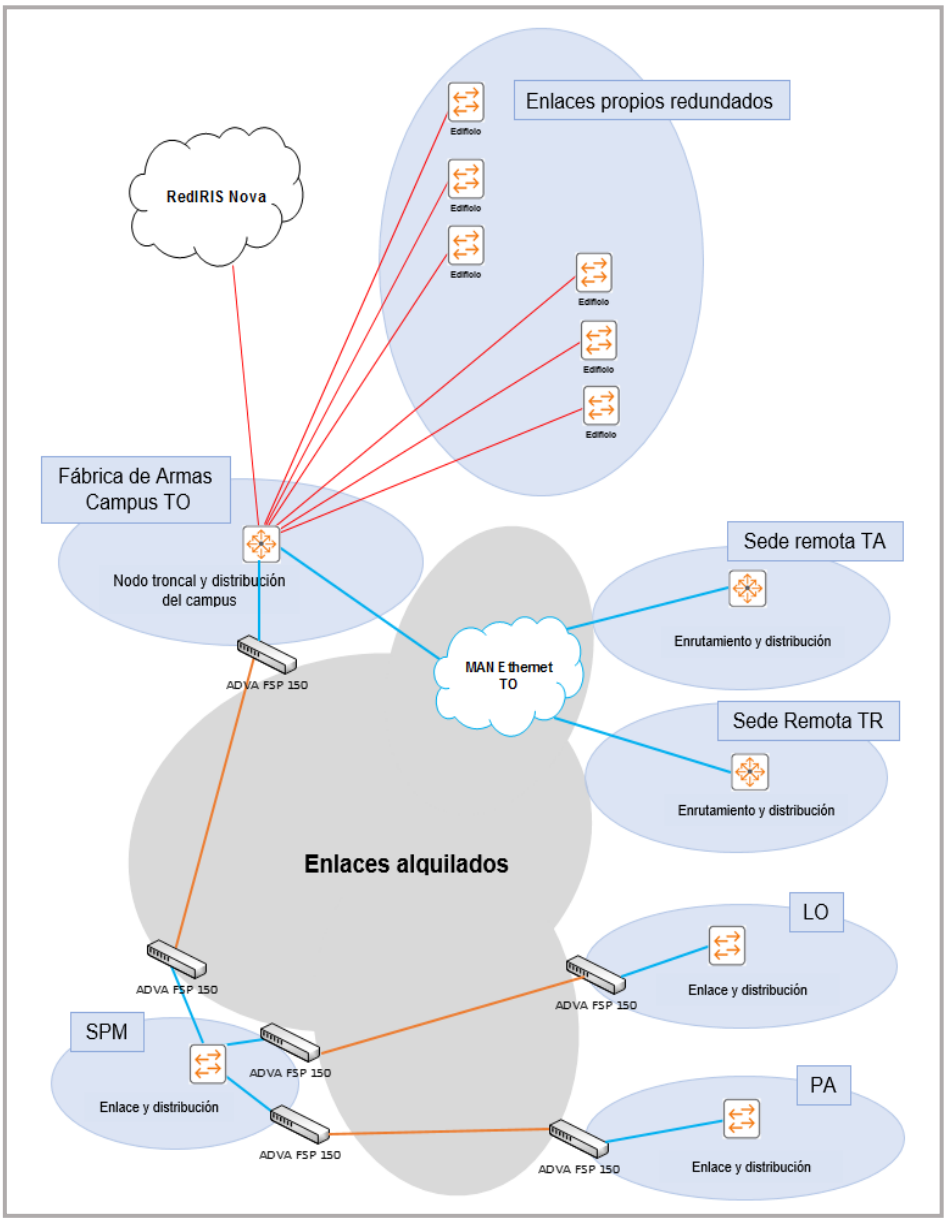


Ilustración 13: Distribución de RED campus TO

Nota: Los enlaces propios redundados se han dibujado simples para una mayor claridad en la ilustración

2.1.4. Sedes remotas de baja capacidad

La institución dispone de algunas sedes remotas, en algunos de sus campus con poco tráfico de red: como gimnasios, aulas abierta a exposiciones..., estas sedes están conectadas mediante servicios FTTH o ADSL, que usan servicios tunelizados hacia la red universitaria. El uso, en base a servicios tunelizados, se realiza en las controladoras Aruba del campus CR, como se verá en el apartado: "2.1.5 Red inalámbrica" de este documento.

En estas sedes, el servicio se presta configurando los APs en modo RAP, de esta manera permiten que cada AP se conecte a su controladora desde redes externas, tunelizando todo el tráfico de servicio hacía la controladora de red inalámbrica. El fabricante de la solución Aruba de red inalámbrica también dispone de dispositivos capaces de distribuir redes cableadas, mediante tunelización de su tráfico hacia las controladoras.

Estas sedes no se contemplan en el apartado: "2.2 Principales sucursales objeto de estudio" de este trabajo, que hace referencia a las sucursales que son susceptibles de evolución a SD-WAN. Sin embargo, una vez implantado un proyecto de este tipo en explotación, serían fácilmente incorporarlas al mismo, adquiriendo todas las posibles ventajas de la solución final.

2.1.5. Red inalámbrica

Esta institución universitaria presta el servicio de red inalámbrica en base a una infraestructura de controladoras centralizadas y situadas en el nodo CR. La infraestructura consta de dos controladoras Aruba 7220(*) y aproximadamente 1091 puntos de acceso, estos últimos con diversidad de modelos.

En un pasado reciente ambas controladoras estaban configuradas para soportar redundancia, pero la gran demanda del servicio obligo a tomar la decisión de renunciar a la redundancia debido al crecimiento en la instalación de puntos de acceso y por lo tanto, a la superación de 1024 APs de la controladora Aruba 7220.

Debido a lo anteriormente expuesto, la controladora CR2 tiene asignados todos los APs del campus CU y la controladora CR1 los APs del resto de campus (CR, AB y TO) además de los servicios de AP remotos externos.

Para la gestionar y monitorizar el servicio de red inalámbrica la institución dispone de la plataforma AirWave 8.2.7 virtualizada(*).

Existe una previsión futura de implantación de un servicio redundante, que consistirá en una tercera controladora Aruba 7220 con la versión 8.3 y una *Mobility Master* virtual(*) con el objetivo de montar la configuración, validar y proceder a la migración de puntos y sus controladoras a la nueva versión de la infraestructura de controladoras de redundancia 3 a 1.

(*) En el apartado: Anexo V se puede consultar el equipamiento Aruba de red inalámbrica con más detalle.

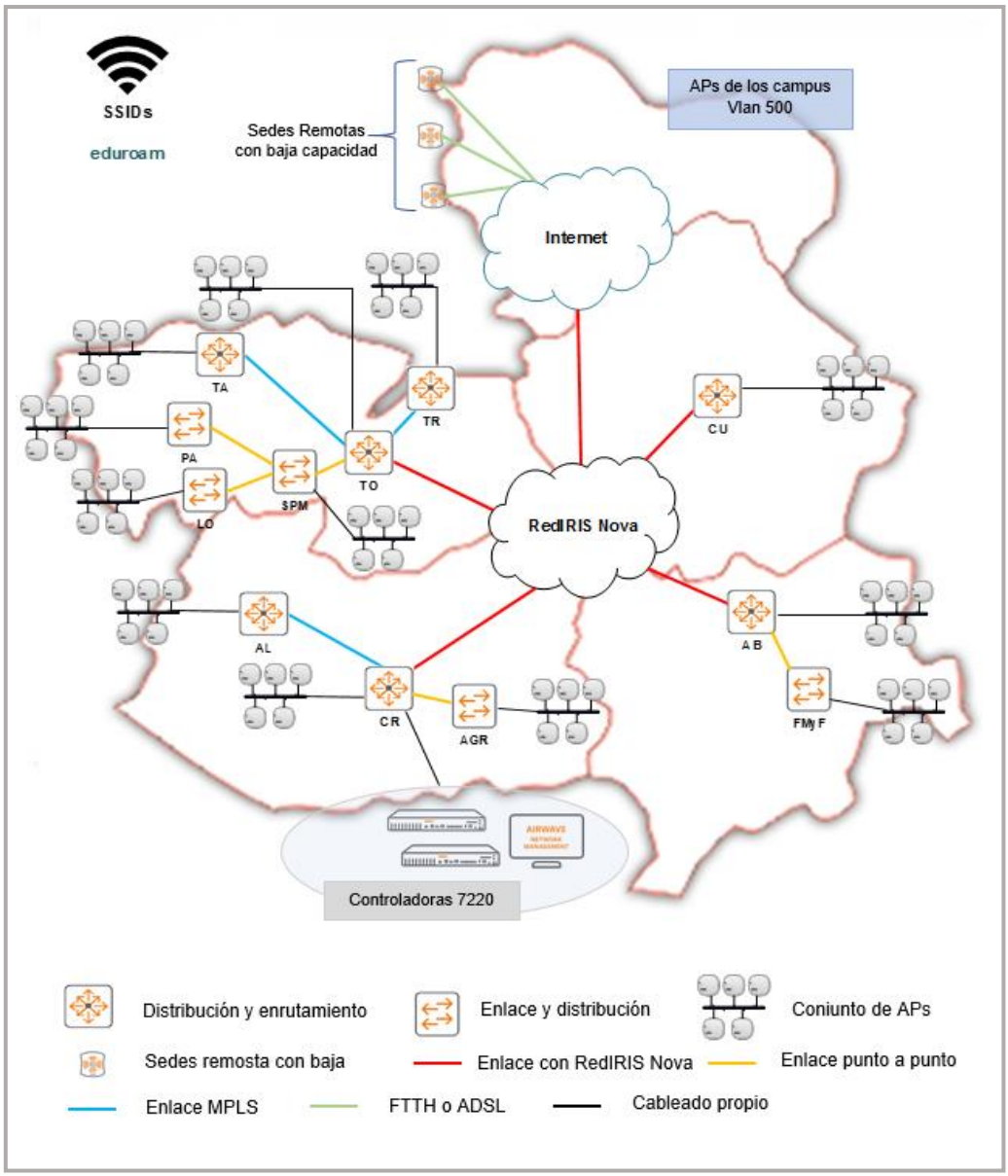


Ilustración 14: Red Inalámbrica(*)

2.1.6. Red del CPD, conexión con Internet y Azure

El CPD de esta universidad se encuentra ubicado junto al nodo principal de la institución, es decir, en el campus CR y más específicamente en el edificio CTIC. La interconexión en la sala de comunicaciones del CPD se realiza mediante fibras propias donde se encuentran tanto la electrónica principal de red, así como el nodo de RedIRIS Nova.

La red del CPD se basa en dos equipos Arista(**) DCS-7050SX2-72Q-R interconectados entre sí con dobles enlaces de 40 Gbps y conectados a fuentes de alimentación redundadas. En estos equipos se realiza las funciones de nivel 3 del CPD basada en enrutamiento estático. Además, ambos equipos Arista

(*) Imagen basada en el documento: *Arquitectura General Servicio de Comunicaciones*. (2019). De Manuel, Carlos.
(**) En el apartado: Anexo VI se puede consultar el equipamiento Arista del CPD con más detalle.

7050 se encuentran conectados mediante fibras redundadas de 40 Gbps a cuatro equipos Arista DCS-7020TR-48-R[(*)] encargados de prestar el acceso de nivel 2 en 1000BaseT.

En la sala de comunicaciones, también se encuentran dos Firewalls del fabricante PaloAlto y los dispositivos balanceadores de carga A10[(*)] conectados a la electrónica de red Arista. Estos equipos proporcionan la seguridad perimetral y los servicios de balanceo de carga.

En la siguiente ilustración podemos ver una aproximación de la conexión física del equipamiento en el CPD.

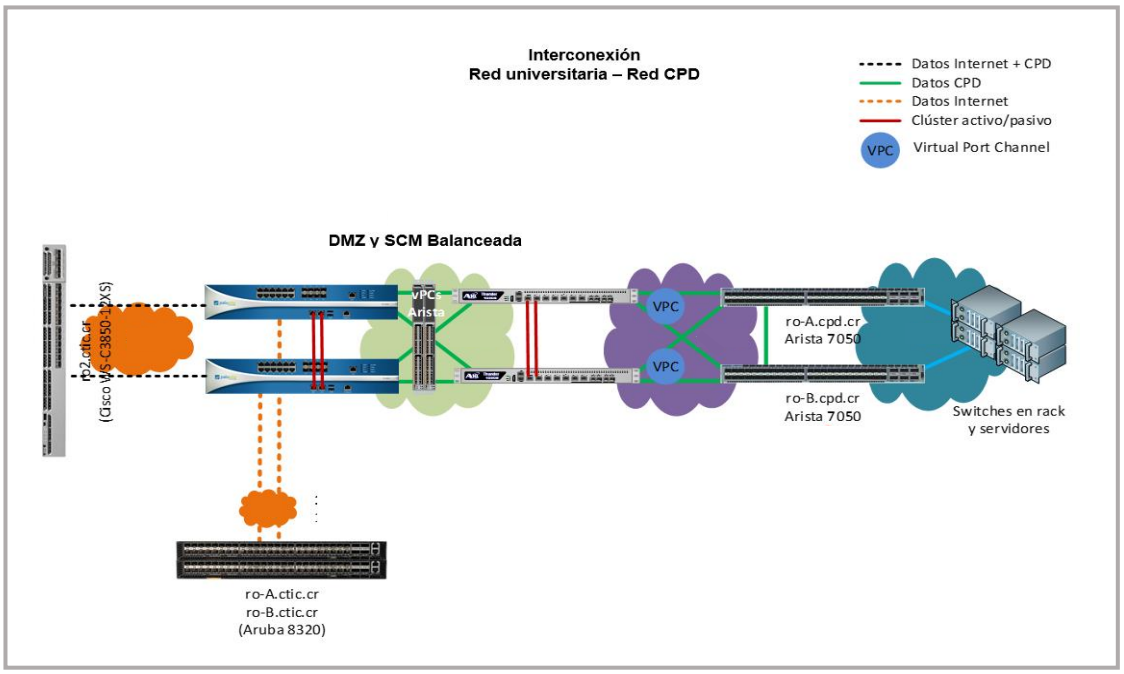


Ilustración 15: Interconexión Red universitaria - Red CPD(**)

La institución universitaria realiza la conexión con Internet mediante RedIRIS Nova mediante un único interfaz óptico de 10 Gbps. RedIRIS Nova proporciona redundancia de nivel 2 y establece el nivel 3 público de esta organización en el nodo del CIEMAT de Madrid. En la actualidad, están en proceso de establecer redundancia de nivel 3 que sería proporcionado por el CICA en Andalucía.

La conexión a Internet de esta universidad se basa en un interfaz de 10 Gbps de fibra óptica con enrutamiento estático y capacidad QinQ, para establecer vlans con el CPD virtual (VCPD) que la institución tiene en la nube de Azure. En dicho interfaz óptico, RedIRIS entrega una vlan con ID 50, donde se realiza la conexión de transporte.

Además, se proporcionan dos vlans redundadas, vlan 403 y vlan 404 con terminación en dos nodos geográficamente distantes del proveedor de servicios de nube privada, que usando QinQ establecen la vlan 1401 de comunicación

---

[(*)] En el apartado: Anexo VI se puede consultar el equipamiento Arista y A10 del CPD con más detalle.

[(**)] **Fuente de la imagen:** *Arquitectura General Servicio de Comunicaciones*.(2019). De Manuel, Carlos.

entre el CPD físico y el CPD virtual de Azure de forma segura, al usar el servicio *ExpressRoute*(*) de Microsoft a través de RedIRIS y GEAN.

Podemos ver en la siguiente imagen tanto la conexión como la dirección del diferente tráfico desde o hacia la institución, así como desde o hacia Internet.

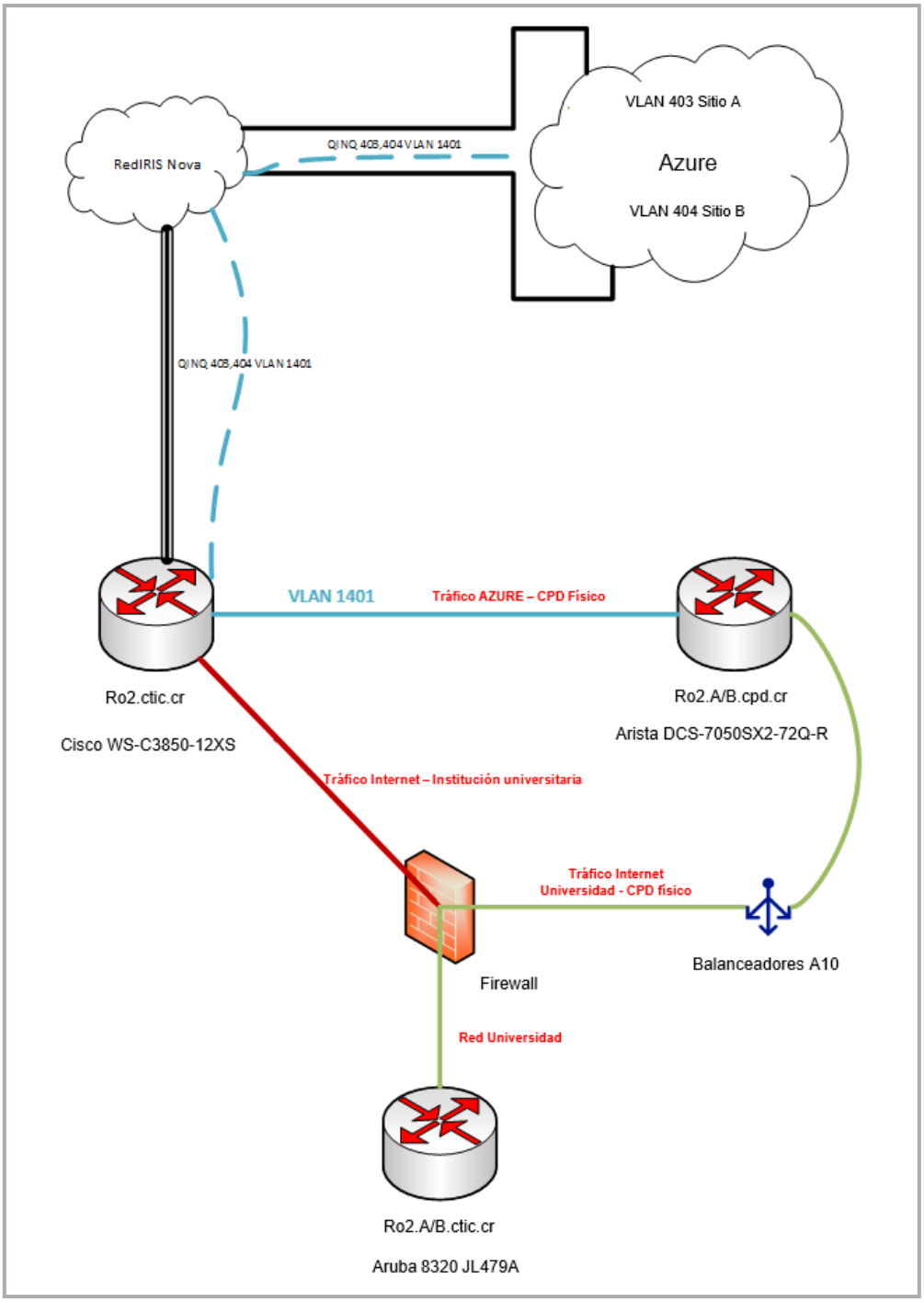


Ilustración 16: Red CPD - VCPD – Internet(**)

(*) En el aparatado: anexo VII se puede encontrar información relativa a *ExpressRoute*

(**) **Fuente de la imagen:** *Arquitectura General Servicio de Comunicaciones*. (2019). De Manuel Carlos.

Finalmente, se incluyen unas gráficas obtenidas con el programa Cacti sobre el router *ro2.ctic.cr*. En estas gráficas se observa el tráfico que la institución universitaria ha tenido tanto con Internet, como con los dos sitios de Azure. Las gráficas comprenden un periodo de tres meses: del 27-12-2019 a 27-03-2020, siendo la última fecha, la de redacción del apartado de este documento.

En estas gráficas se puede ver por un lado, como existe un tráfico balanceado entre la subida y la descarga del tráfico entre la institución y las dos sedes remotas de Azure y por otro lado, se puede ver como debido a la crisis mundial que todos los países, incluido España, están sufriendo por el coronavirus (Covid-19) el tráfico respecto a Internet ha disminuido de forma muy notable en las dos últimas semanas del periodo medido, debido al estado de alerta decretado en el estado español.

En primer lugar, se observa que el tráfico con sitio A de Azure respecto a la descarga y a la subida:

- Un pico máximo entorno a los 200 Mbps tanto de descarga, como de subida
- Una media entorno a los 111 Mbps para la descarga y 106 Mbps para la subida
- La actual (medida el 27 de marzo) fue de alrededor de 170 Mbps para la descarga y de 60 Mbps la de subida

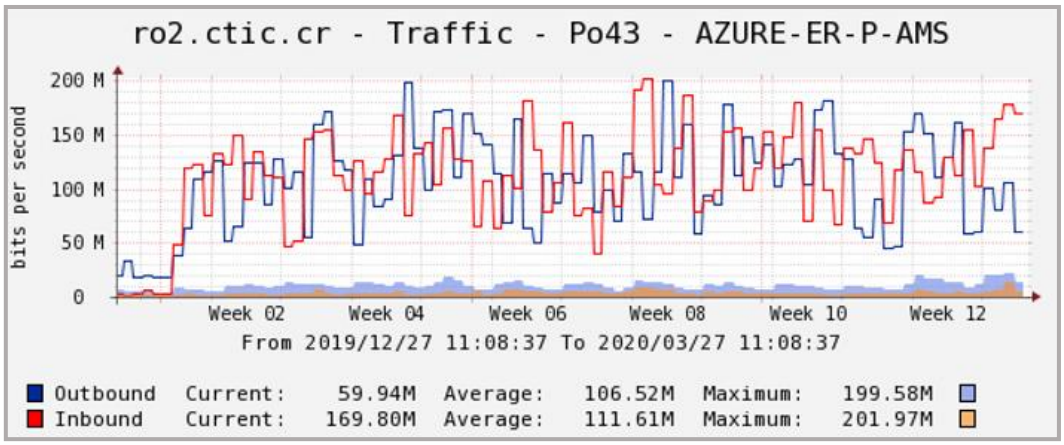


Ilustración 17: Tráfico Institución - Sitio A de Azure

En segundo lugar, se puede ver que el tráfico con sitio B de Azure respecto a la descarga y a la subida:

- Un pico máximo de 217 Mbps en la descarga y de 228 Mbps de subida
- Una media entorno a los 114 Mbps para la descarga y 109 Mbps para la subida.

- La actual (medida el 27 de marzo) fue de alrededor de 84 Mbps para la descarga y de 171 Mbps la de subida.

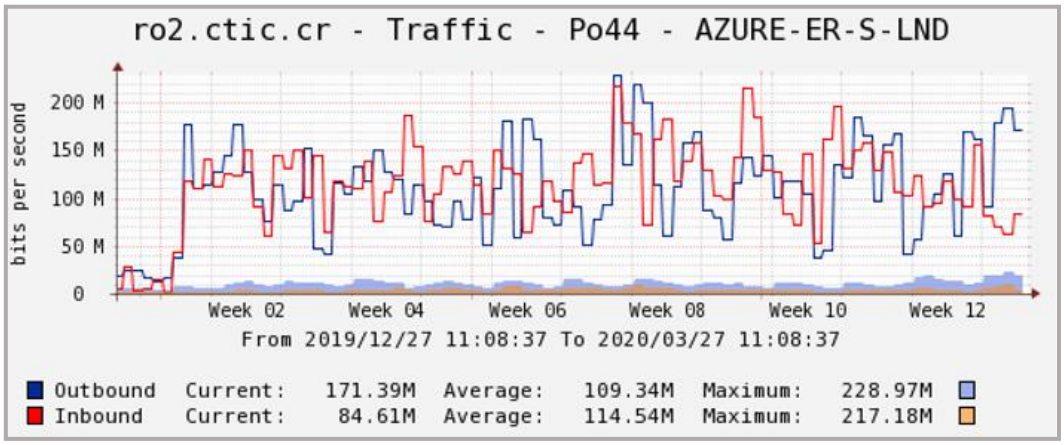


Ilustración 18: Tráfico Institución - Sitio B de Azure

Finalmente, se observa que el tráfico con Internet respecto a la descarga y a la subida:

- El pico máximo está en 3,5 Gbps de descarga y en los 1,5 Gbps de subida
- La media en el periodo ha estado entorno a los 1,45 Gbps para la descarga y 525 Mbps para la subida.
- La actual (medida el 27 de marzo) fue de alrededor de 753 Mbps para la descarga y de 701 Mbps la de subida.

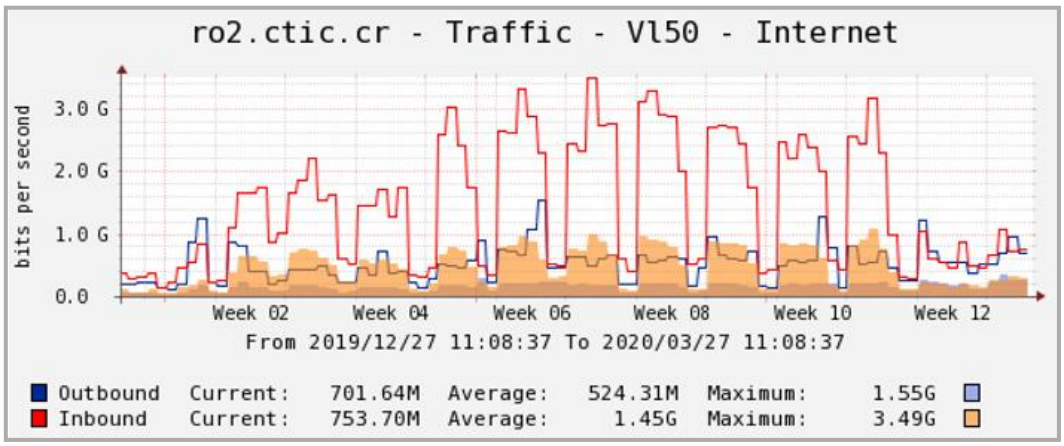


Ilustración 19: Tráfico Institución - Internet

Tal como se ha comentado antes, se puede observar como la actividad de descarga respecto a Internet ha descendido de manera notable, lo que se atribuye a como está afectando la crisis del coronavirus.

2.2. Principales sucursales objeto de estudio

En este apartado se describe, de una manera más detallada, las diferentes sucursales que están conectadas con los nodos principales de cada campus mediante enlaces alquilados a un operador de comunicaciones.

Así pues, como se vio en el apartado: "2.1.3 Red de distribución y acceso por campus" existe un número significativo de sucursales susceptibles de estudio para una posible evolución de red a SD-WAN. En estas sucursales es necesario actualmente hacer uso de enlaces alquilados a un operador de comunicaciones y que son de dos tipos:

- Enlaces punto a punto de 1 Gbps del operador, servicio nivel 2, donde el operador no realiza ninguna gestión sobre el enlace, excepto la de monitorizar que su estado sea operativo.
- Accesos a la red Metrolan de Telefónica, donde el operador asigna un identificador de VLAN en los accesos de las diferentes sedes para comunicarlas a través de su red. El caudal garantizado es el que cliente (institución universitaria) y proveedor (operador de telecomunicaciones) hayan estipulado según contrato.

A continuación, se analizarán las sucursales por campus que cumplen los requisitos para ser evolucionadas a SD-WAN:

2.2.1. Sucursales en el campus CR

En este campus se tienen dos sucursales a estudiar:

2.2.1.1. Sucursal AGR

Es un centro universitario donde se imparten titulaciones universitarias oficiales ubicado a 2 Km aproximadamente del edifico CTIC (nodo principal del campus CR). El tipo de conexión que interconecta el nodo principal y este centro es un enlace punto a punto alquilado de 1 Gbps y servicio de nivel 2.

En este centro se cuenta con un equipo Cisco Catalyst 2960(*), en el que se produce el acceso a la red de nivel 2, así como la distribución a las diferentes verticales del centro mediante enlaces no redundados.

En la siguiente figura podemos ver una representación de la conexión entre el nodo principal y este centro:

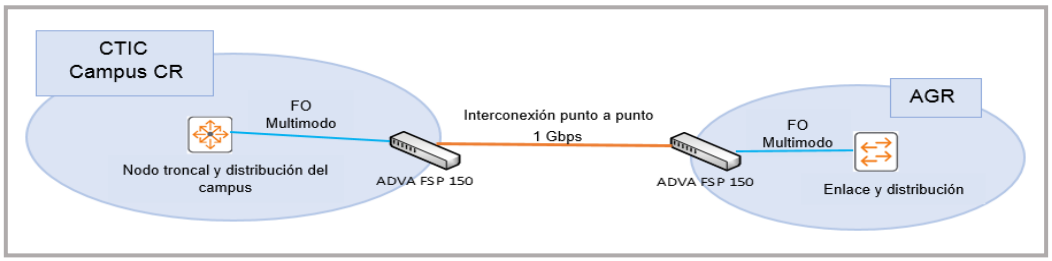


Ilustración 20: Conexión nodo principal campus CR - sucursal AGR

(*) En el apartado: Anexo VIII se puede consultar el equipo Cisco Catalyst 2960 con más detalle.

La siguiente imagen, obtenida con el programa Cacti, refleja el tráfico generado entre el nodo principal y la sede remota en el último mes. Se puede observar como el tráfico máximo de descarga de la sede remota es de aproximadamente 232 Mbps y el de subida de 85 Mbps.

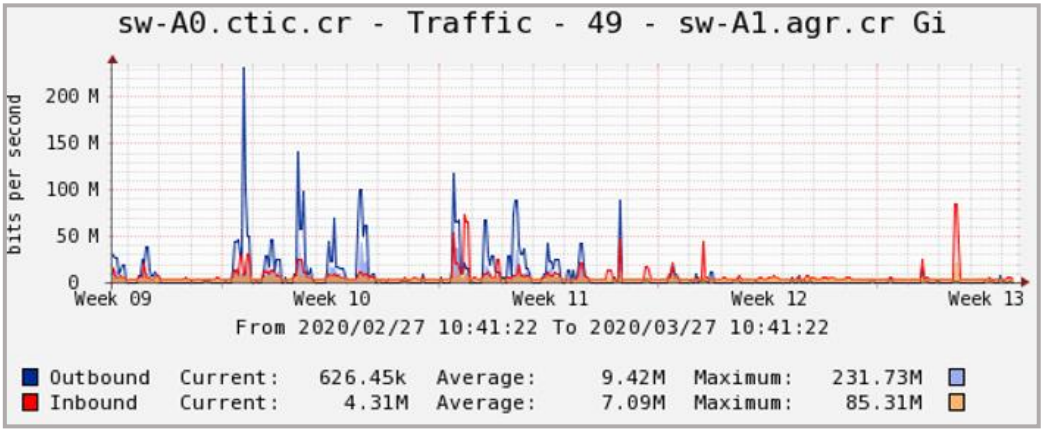


Ilustración 21: Tráfico de red sede principal - AGR

Con este ancho de banda demandado en pico máximo y con una media de 9 y 7 Mbps de descarga y subida respectivamente, es más que viable respecto al tráfico que la sede AGR pueda evolucionar a la SD-WAN.

2.2.1.2. Sucursal AL

Es un centro universitario donde se imparten dos grados universitarios oficiales de ingeniería está ubicado a 102 Km aproximadamente del nodo principal del campus CR (edifico CTIC). El tipo de conexión que interconecta el nodo principal y esta sucursal es un enlace alquilado MPLS no redundado con un acceso de 1 Gbps, un ID vlan 917 proporcionado por el operador y un caudal contratado de 100 Mbps simétricos, excepto para la descarga de la sucursal que es de 200.

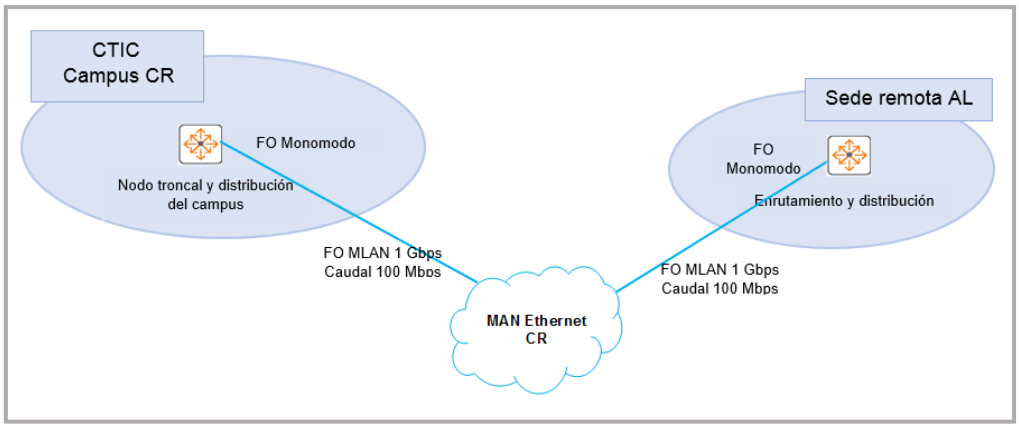


Ilustración 22: Conexión nodo principal campus CR – sede remota AL

En la figura anterior se puede ver una representación de la conexión entre el nodo principal y esta sede remota. Esta sucursal cuenta con un equipo Aruba 3810(*) provisto de fuentes de alimentación redundadas, que provee de nivel 3

(*) En el apartado: Anexo IX se puede consultar más información sobre el equipo Aruba 3810 de esta sucursal.

con protocolo de enrutamiento OSPF integrado en el mismo área de la red troncal. La interconexión entre las dos sedes se produce a través de una red IP de transporte. Además, realiza la distribución de nivel 2 a las diferentes verticales del centro mediante enlaces no redundados.

La siguiente imagen refleja el tráfico generado entre el nodo principal y la sede remota en los últimos seis meses y podemos observar como el tráfico máximo de descarga de la sede remota es de aproximadamente 200 Mbps y el de subida de 98 Mbps y con una media aproximada de 53 y 22 Mbps de descarga y subida respectivamente.

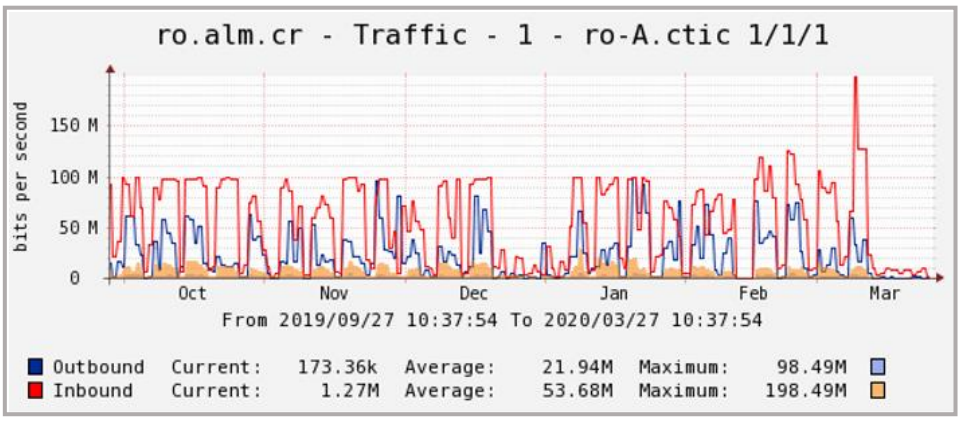


Ilustración 23: Tráfico de red sede principal – sucursal remota AL

2.2.2. Sucursales en el campus AB

En este campus tenemos una sucursal al objeto de estudio:

2.2.2.1. Sucursal FMyF

Es un centro universitario donde se imparten dos titulaciones universitarias de la rama sanitaria. El tipo de conexión que interconecta el nodo principal y este centro es un enlace punto a punto alquilado de 1 Gbps y servicio de nivel 2.

En este centro se cuenta con un equipo HPE 5130, en el que se produce el acceso a la red de nivel 2, así como la distribución a las diferentes verticales del centro mediante enlaces no redundados.

En la siguiente figura se puede ver una representación de la conexión entre el nodo principal y este centro:

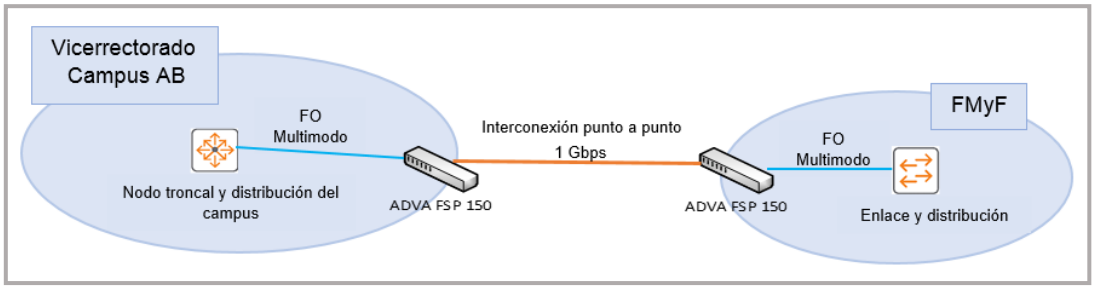


Ilustración 24: Conexión nodo principal campus AB - sucursal FMyF

(*) En el apartado: Anexo X se puede consultar más información sobre el equipo HPE5130 de esta sucursal.

La siguiente imagen, obtenida con el programa Cacti, refleja el tráfico generado entre el nodo principal y la sede remota en el último mes. Se puede observar como el tráfico máximo de descarga de la sede remota es de 255 Mbps y el de subida de 202 Mbps y con una media de media de 27 y 14 Mbps de descarga y subida respectivamente.

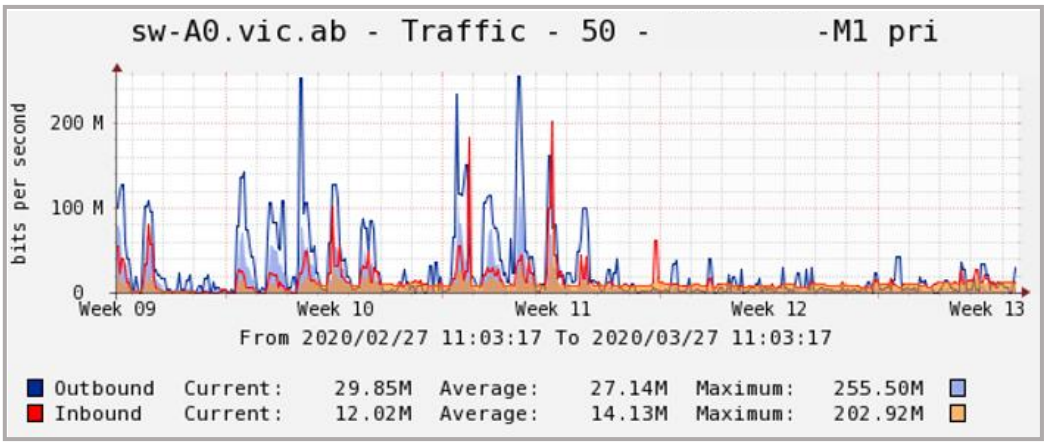


Ilustración 25: Tráfico nodo principal campus AB - FMyF

2.2.3. Sucursales en el campus TO

En este campus se estudiarán hasta cinco sucursales donde es posible una evolución de red basada en enlaces tradicionales a una red gestionada por software.

2.2.3.1. Sucursal TA

Es un centro universitario donde se imparten varios grados universitarios oficiales, está ubicado aproximadamente a 100 Km del nodo principal del campus TO (situado en la Fábrica de Armas). El tipo de conexión que interconecta el nodo principal y esta sucursal es un enlace alquilado MPLS no redundado con un acceso de 1 Gbps, un ID vlan 926 proporcionado por el operador y un caudal contratado actualmente de 1Gbps simétricos (hasta mediados de febrero el caudal contratado era de 100 Mbps) simétricos.

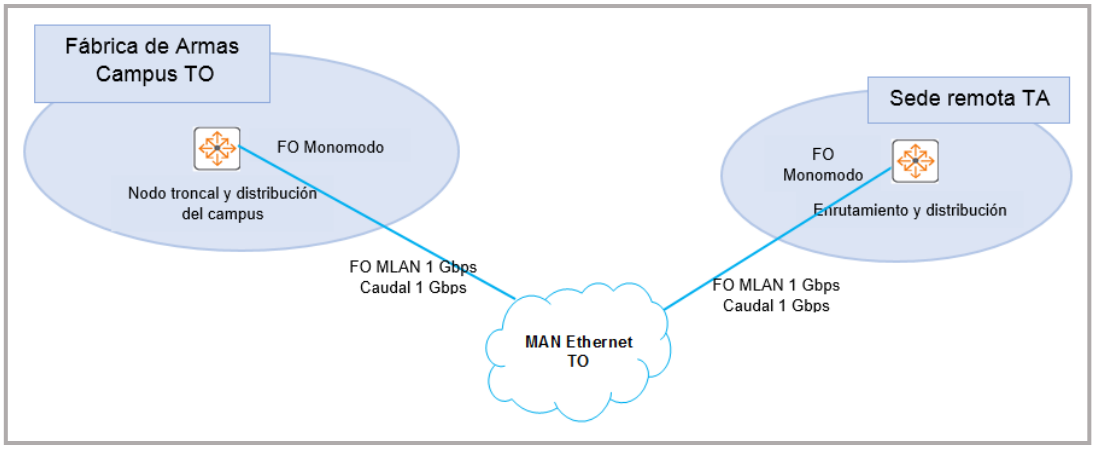


Ilustración 26: Conexión nodo principal campus TO – sede remota TA

En la figura anterior, se puede ver una representación de la conexión entre el nodo principal y esta sede remota. Esta sucursal cuenta con un equipo Aruba 3810(*) provisto de fuentes de alimentación redundadas, que provee de nivel 3 con protocolo de enrutamiento OSPF integrado en el mismo área de la red troncal. La interconexión entre las dos sedes se produce a través de una red IP de transporte. Además, realiza la distribución de nivel 2 a las diferentes verticales del centro mediante enlaces no redundados.

A mediados del mes de febrero se realizó una modificación del caudal contratado pasando de 100 Mbps a 1 Gbps simétricos en ambos casos. Por este motivo, el gráfico respecto al tráfico se divide en dos imágenes.

En la primera imagen, la correspondiente desde finales de diciembre de 2019 a mediados de febrero de 2020, se observa que el tráfico máximo de descarga de la sede remota es de aproximadamente 100 Mbps y el de subida de 53 Mbps.

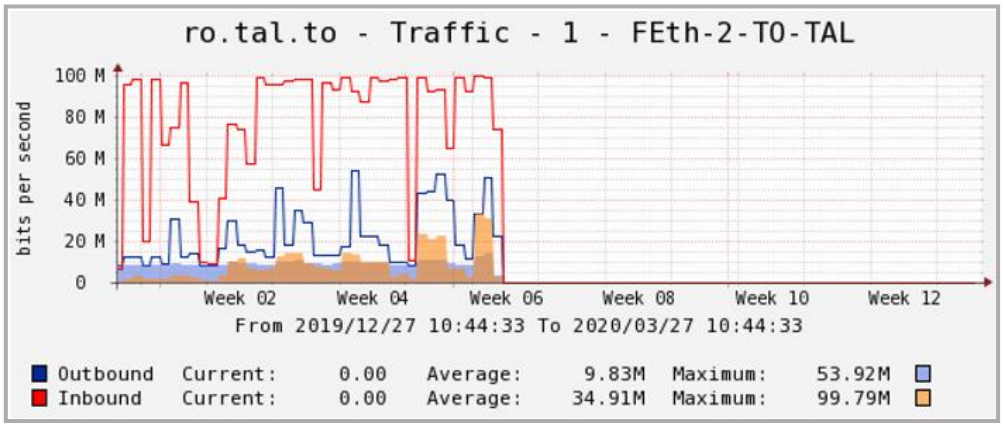


Ilustración 27: Tráfico nodo principal campus TO – sucursal remota TA (I)

En esta segunda imagen, la correspondiente a partir de mediados del mes de febrero hasta la redacción de este documento, se puede observar, ya con la ampliación de caudal a 1Gbps, como el tráfico máximo de descarga de la sede remota es de aproximadamente 201 Mbps y el de subida de 121 Mbps. Apreciándose la necesidad de la ampliación de caudal llevada a cabo por la institución universitaria.

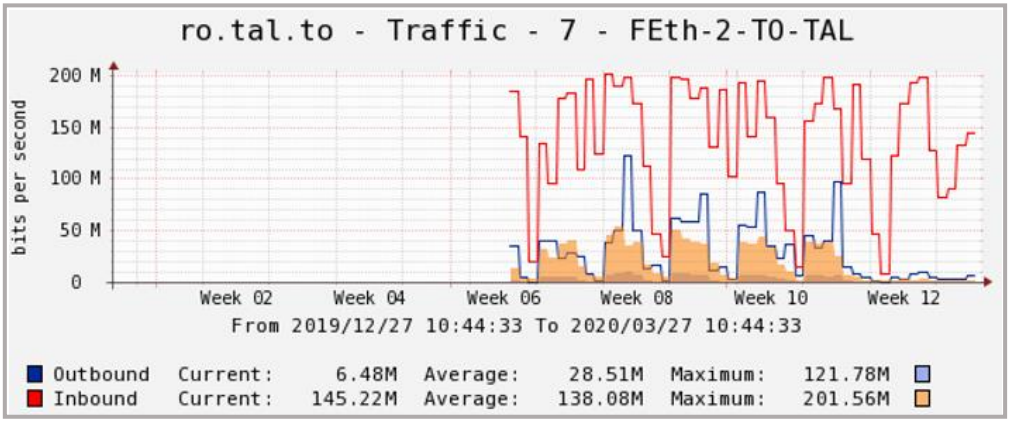


Ilustración 28: Tráfico nodo principal campus TO – sucursal remota TA (II)

(*) En el apartado: Anexo IX se puede consultar más información sobre el equipo Aruba 3810 de esta sucursal.

2.2.3.2. Sucursal TR

Este centro universitario se conecta con el nodo principal del campus TO (situado en la Fábrica de Armas) mediante un enlace alquilado MPLS no redundado con un acceso de 1 Gbps, un ID vlan 928 proporcionado por el operador y un caudal contratado de 100 Mbps simétricos.

Esta sucursal cuenta con un equipo Aruba 2930F(*) con el nivel 3 activado con enrutamiento vía rutas estáticas en ambos extremos (Fábrica de Armas – TR). La interconexión entre las dos sedes se produce a través de una red IP de transporte. Además, realiza la distribución de nivel 2 a las diferentes verticales del centro mediante enlaces no redundados. En la siguiente figura se puede ver una representación de la conexión entre el nodo principal y esta sede remota.

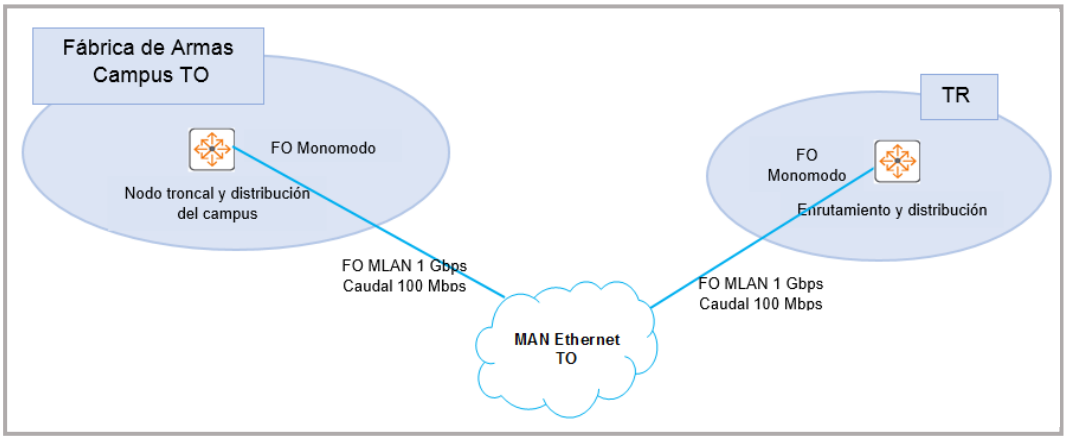


Ilustración 29: Conexión nodo principal campus TO - sucursal TR

La siguiente imagen refleja el tráfico generado entre el nodo principal y la sede remota en el último mes y podemos observar como el tráfico máximo de descarga de la sede remota es de aproximadamente 64 Mbps y el de subida de 16,5 Mbps. En este caso la media no es relevante debido a la crisis del coronavirus (Covid-19), ya que en las dos últimas semanas de la gráfica no existe actividad presencial en el centro al estar prohibida por decreto del gobierno del estado español.

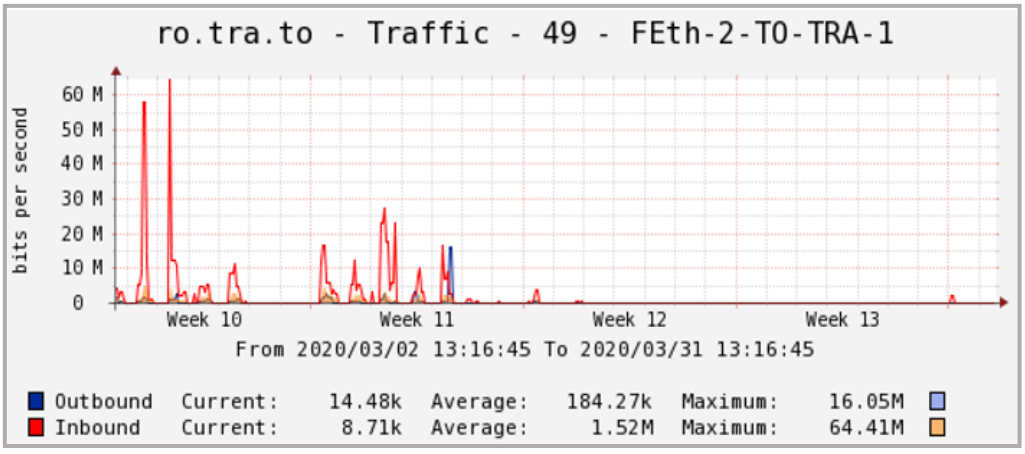


Ilustración 30:Tráfico nodo principal campus TO – sucursal remota TR

(*) En el apartado: Anexo II se puede consultar más información sobre el equipo Aruba 2930F de esta sucursal.

2.2.3.3. Sucursal SPM

Esta sede fue hace unos años el nodo principal del campus TO hasta su traslado a la Fábrica de Armas. Actualmente, SPM es el nodo principal del casco histórico del campus TO. El tipo de conexión que interconecta el nodo principal del campus TO y SPM es un enlace punto a punto alquilado de 1 Gbps y servicio de nivel 2.

En este centro se cuenta con un Aruba 3810(*) con doble fuente de alimentación como electrónica principal. Desde este nodo además de distribuir red de nivel 2 por un gran número de verticales en el propio edificio, también distribuye la red mediante enlaces alquilados a otros dos centros que se estudiarán más adelante: LO y PA.

En la siguiente figura se puede ver una representación de la conexión entre el nodo principal y este centro:

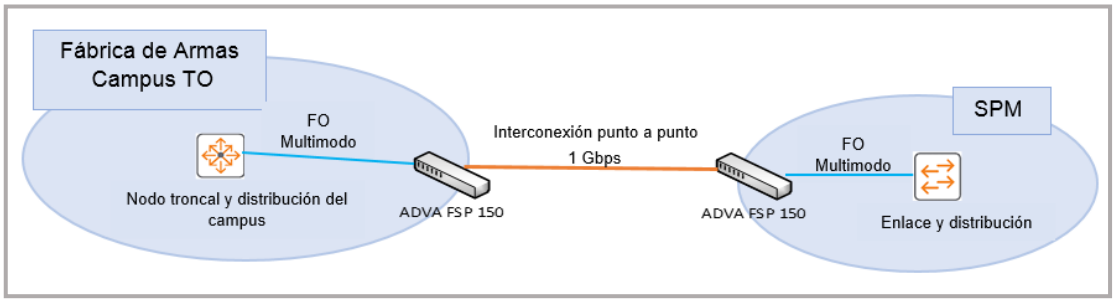


Ilustración 31: Conexión nodo principal campus TO - sucursal SPM

La siguiente imagen, obtenida con el programa Cacti, refleja el tráfico generado entre el nodo principal y la sede remota en los tres últimos meses. Se puede observar, como el tráfico máximo de descarga de la sede remota es alrededor de 579 Mbps y el de subida de 202 Mbps y con una media de media de 219 y 66 Mbps de descarga y subida respectivamente.

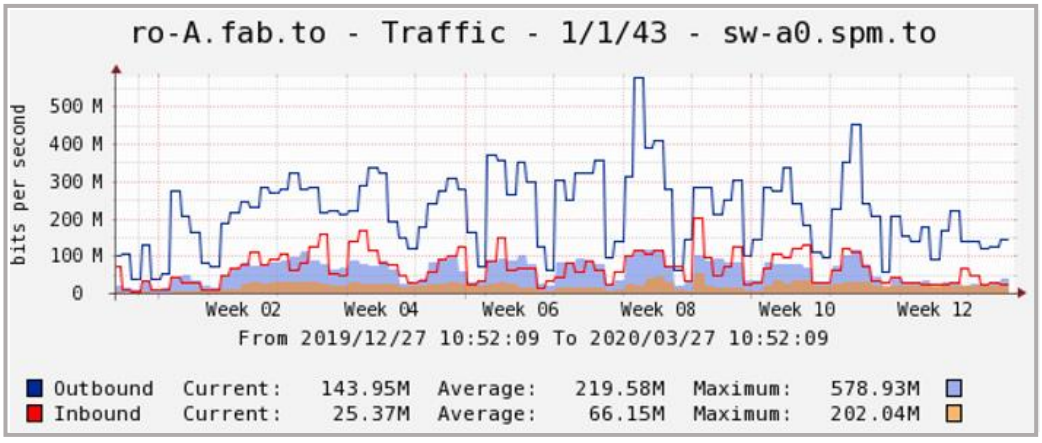


Ilustración 32: Tráfico nodo principal campus TO - SPM

(*) En el apartado: Anexo IX se puede consultar más información sobre el equipo Aruba 3810 de esta sucursal.

2.2.3.4. Sucursal LO

Este centro universitario se conecta con SPM (situado en el casco histórico del campus de TO) mediante un enlace punto a punto alquilado de 1 Gbps y servicio de nivel 2. En este centro se cuenta con un equipo Cisco Catalyst 2960(*), en el que se produce el acceso a la red de nivel 2, así como la distribución a las diferentes verticales del centro mediante enlaces no redundados.

En la siguiente figura se ve una representación de la conexión entre el nodo principal y este centro:

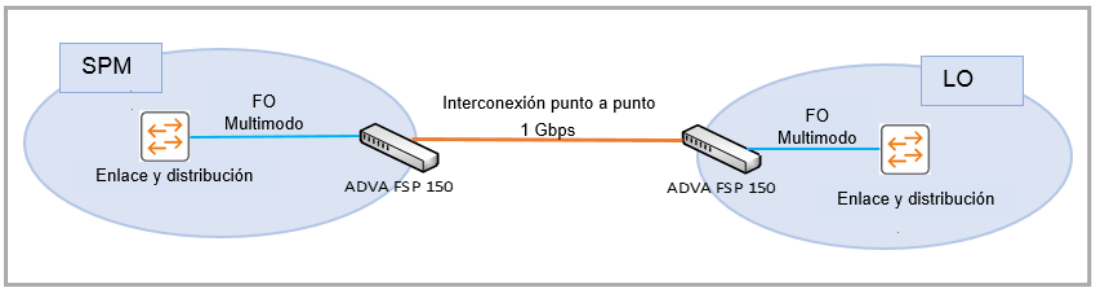


Ilustración 33: Conexión sucursal SPM - sucursal LO

En la siguiente imagen se puede ver reflejado el tráfico generado de los últimos tres meses, a fecha de redacción de este trabajo, entre el nodo del casco histórico SPM y la sede remota, en este caso, LO. Se observa como el tráfico máximo de descarga de la sede remota fue de alrededor de 84 Mbps y el de subida de 77 Mbps y con una media de media de 17 y 6 Mbps de descarga y subida respectivamente.

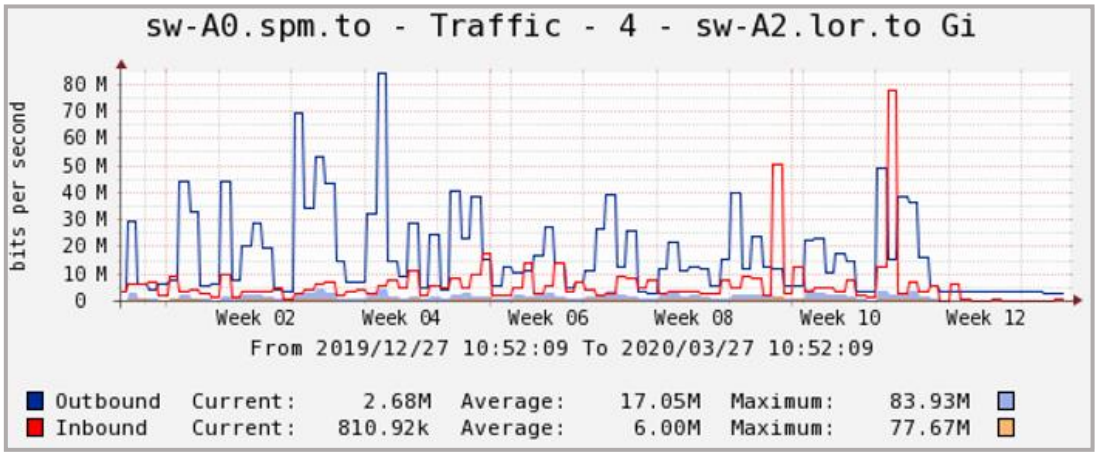


Ilustración 34: Tráfico nodo casco histórico SPM - LO

(*) En el apartado: Anexo VIII se puede consultar más información del equipo Cisco Catalyst 2960 de esta sucursal.

2.2.3.5. Sucursal PA

Este centro universitario se conecta con SPM (situado en el casco histórico del campus de TO) mediante un enlace punto a punto alquilado de 1 Gbps y servicio de nivel 2. Este centro cuenta con un equipo Cisco Catalyst 2960(*), en el que se produce el acceso a la red de nivel 2, así como la distribución a las diferentes verticales del centro mediante enlaces no redundados.

En la siguiente figura se ve una representación de la conexión entre el nodo principal y este centro:

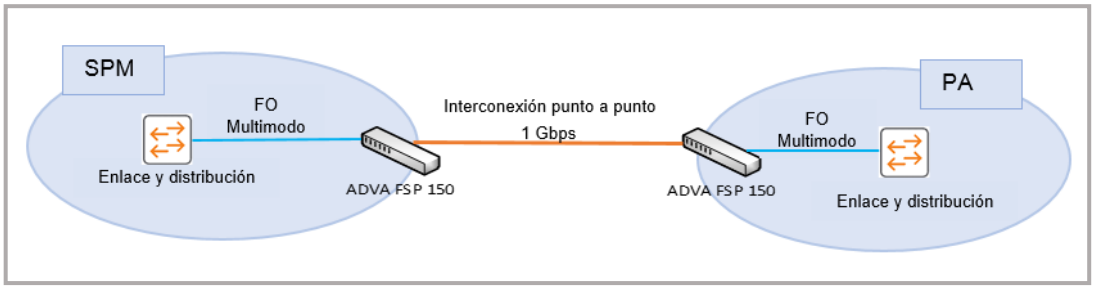


Ilustración 35: Conexión sucursal SPM - sucursal PA

En la siguiente imagen se puede ver reflejado el tráfico generado en los últimos tres meses, a fecha de redacción de este trabajo, entre el nodo del casco histórico SPM y la sede remota, en este caso, PA. Se observa como el tráfico máximo de descarga de la sede remota fue de 283 Mbps y el de subida de 96 Mbps y con una media de media de 133 y alrededor de 27 Mbps de descarga y subida respectivamente.

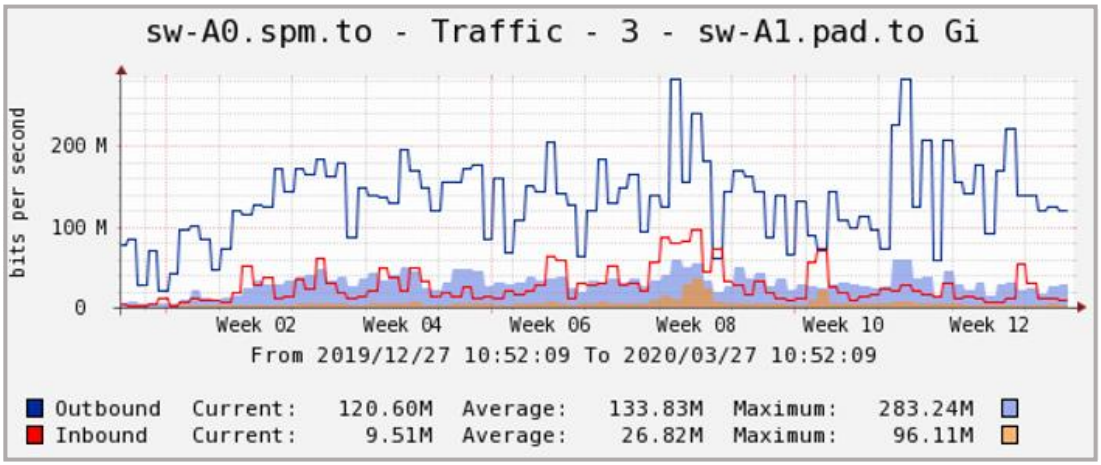


Ilustración 36: Tráfico nodo casco histórico SPM - PA

(*) En el apartado: Anexo VIII se puede consultar más información del equipo Cisco Catalyst 2960 de esta sucursal.

2.2.4. Costes de los enlaces alquilados

Esta institución universitaria contrata los diferentes servicios de interconexión de red mediante un concurso público, donde los diferentes operadores de comunicaciones presentan sus ofertas en base a un pliego prescripciones técnicas.

El detalle de la documentación de adjudicación respecto a los costes no puede ser anexado a este trabajo, debido a que está limitado por un acuerdo de confidencialidad entre cliente y proveedores.

No obstante, la institución durante la elaboración de este trabajo ha facilitado los costes medios de las ofertas presentadas por los diferentes proveedores, que reunían los requisitos de prestación del servicio licitado por la institución universitaria.

La siguiente tabla muestra los datos más relevantes de los enlaces alquilados, respecto al tipo de conexión, precio y sucursales implicadas.

Campus	Sedes implicadas	Conexión	Caudal contratado	Coste anual(*)
CR	Nodo principal CTIC – Sucursal AGR	Punto a punto	1 Gbps	3.200 €
	Nodo principal CTIC – Sucursal AL	MPLS	100Mbps	8.800 €
AB	Nodo Vicerrectorado - Sucursal FMyF	Punto a punto	1 Gbps	3.200 €
TO	Nodo Fábrica de Armas – Sucursal TA	MPLS	1 Gbps	12.200 €
	Nodo Fábrica de Armas – Sucursal TR	Punto a punto	100 Mbps	8.800 €
	N. principal Fábrica A. – Sucursal SPM	Punto a punto	1 Gbps	3.200 €
	Sucursal SPM – Sucursal LO	Punto a punto	1 Gbps	3.200 €
	Sucursal SPM – Sucursal PA	Punto a punto	1 Gbps	3.200 €

Ilustración 37: Costes anuales de los enlaces alquilados(*)

2.2.5. Problemas actuales

Los problemas que la organización tiene en los centros conectados con enlaces alquilados son variados, en función del tipo de enlace (punto a punto o MPLS) y/o la distancia geográfica entre el nodo principal del campus con respecto a ellos. Así, pues se listarán una serie de los problemas más frecuentes que esta institución tiene respecto a estas sucursales en el ámbito que estamos tratando.

- Uno de los principales problemas es la falta de redundancia entre el nodo principal y la sede remota. Pues aunque, sobre el total de caídas de conexión, entre la sucursal y su nodo principal, las imputables directamente al enlace alquilado es inferior al 2%, según dato facilitado por la institución durante la realización de este trabajo, también indican desde la misma, que la importancia de sus servicios IT hace que cada vez sea más imprescindible garantizar la conectividad de la sede remota.

(*) Los costes anuales incluyen tasas, impuestos, licencias y cualquier otro gasto que origine la ejecución del contrato.

Un ejemplo de ello es el abandono hace años, por parte de la organización, de las comunicaciones clásicas basadas en líneas analógicas y digitales como RDSI. Actualmente, dispone de un servicio de comunicaciones unificadas basado en su red IP, que hace imprescindible que su red tenga una completa disponibilidad y seguridad.

- Otro de los problemas es el elevado coste económico anual que suponen los enlaces alquilados, sobre todo los MPLS, que la institución tiene contratados con un ancho de banda de tan solo 100 Mbps. Este problema se intensifica más al llevar a cabo una ampliación de este ancho de banda, tal y como se puede comprobar en el apartado "2.2.4 Costes de los enlaces alquilados" respecto a la sucursal TA.
- La falta de monitorización del tipo de tráfico entre la sucursal y el nodo principal.
- La no existencia de una gestión dinámica del ancho de banda de la sucursal, que permita priorizar un cierto tipo de tráfico sobre otros.
- En determinadas sedes, o bien no hay personal técnico o es insuficiente para abordar los distintos procesos tanto de gestión, actualización o mantenimiento, así como el despliegue de nuevos servicios. Por lo tanto, se hace imprescindible una solución que permita realizar todas estas operaciones de una forma automatizada y en algunos casos sin necesidad de personal cualificado.

2.2.6. Conclusiones

A lo largo del apartado "2.2 Principales sucursales objeto de estudio" han sido analizadas las distintas sucursales de cada uno de los distintos campus que utilizan enlaces alquilados y se ha incorporado información sobre distintos aspectos:

- Tipo de enlace y ancho de banda disponible contratado
- Necesidades reales del ancho de banda requerido, en función del tráfico de subida y de descarga, que las distintas gráficas ofrecen como información
- Los costes anuales recurrentes de los enlaces
- Un conjunto de problemas comunes que se dan en estas sucursales, desde la falta de redundancia y el elevado coste recurrente del alquiler del enlace, hasta la imposibilidad de priorizar cierto tráfico sobre otros, así como la necesidad de personal técnico para el despliegue de un simple punto de acceso

El objetivo de los siguientes capítulos es demostrar en base a la información expuesta a los largo del apartado: "2.2 Principales sucursales objeto de estudio",

que es posible la evolución de esas sucursales a un modelo de red basado en software (SD-WAN) proporcionando:

- Una mayor escalabilidad
- Mayor capacidad de ancho de banda a un menor coste recurrente
- Una óptima calidad de servicio
- Una mayor redundancia
- Una gestión dinámica del tráfico
- Una mejora sustancial para gran parte de los procesos de gestión, mantenimiento, actualización y despliegue de servicios en la sede remota.

3. Infraestructura SD-WAN

3.1. Conceptos básicos

La mejor forma de introducir en este apartado es sin lugar a duda contestar a la pregunta: ¿Qué es SD-WAN?. Cooney, Michael (2019) señala que SD-WAN es la aplicación de la tecnología SDN a través de una WAN. Así pues, antes de contestar a la pregunta, se introducirá en primer lugar el concepto de SDN.

Las redes definidas por software o SDN hacen posible la separación de la administración del tráfico de red de la infraestructura física de transporte subyacente, lo que permite adaptar de forma dinámica, la implementación preprogramada del flujo del tráfico de red hacia unas necesidades reales y todo ello de manera automatizada.

Desde Citrix, en su glosario, señalan que una red definida por software se compone de tres capas: aplicación, control e infraestructura que conectadas por medio de APIs permiten la comunicación de una capa a otra de forma bidireccional.

- La capa de aplicación se compone de las aplicaciones y funciones de red como firewalls o balanceadores de carga
- La capa de control gestiona y administra las políticas de enrutamiento, así como el flujo de tráfico que circula por la red
- La capa de infraestructura contiene la electrónica de red como los conmutadores

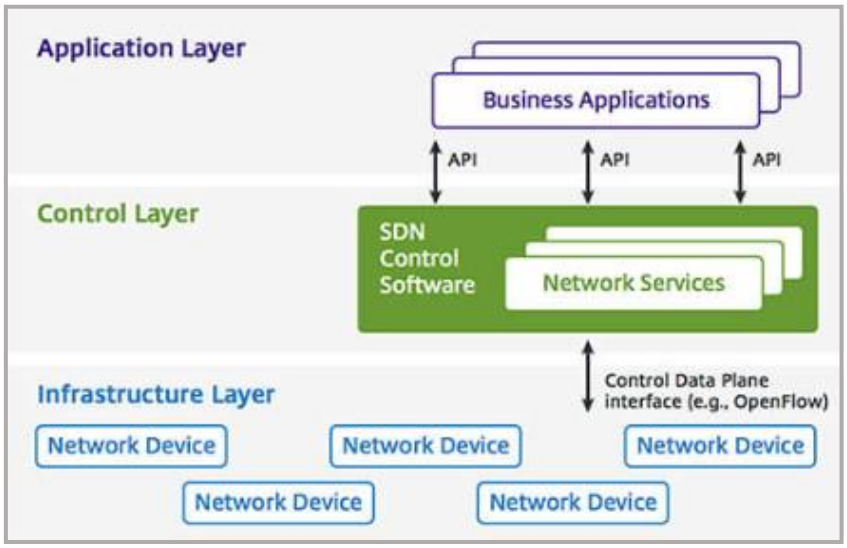


Ilustración 38: Arquitectura SDN(*)

(*) **Fuente de la imagen:** ONF, https://www.opennetworking.org/ (citado en Citrix, https://www.citrix.com/es-mx/glossary/what-is-software-defined-networking.html)

SDN son un tipo de redes que gracias a la capacidad de programación, las hacen flexibles, ágiles y escalables. Flexibles porque utilizan políticas de enrutamiento según las necesidades de redireccionamiento del tráfico, Ágiles porque de forma dinámica y en tiempo real son capaces de aplicar esas políticas en función de las situaciones cambiantes de la red y escalables porque gracias a la virtualización posibilitan el uso mediante la unión de varios recursos como si de uno solo se tratase.

Además, distintos autores (Uppal, Sanjay et al.(2018); Cooney, Michael (2019); Networking (2018)) señalan que SDN generalmente han sido utilizadas para los centros de datos, añadiendo como reflexión que SD-WAN es la aplicación en la WAN lo que SDN es para los centro de datos.

Finalmente, ahora se está en condiciones de contestar a la pregunta que en inicio de este apartado se formulaba: ¿Qué es SD-WAN? Y para ello, se comenzará con la transcripción de algunas definiciones encontradas en distintos recursos:

Cisco en https://www.cisco.com/*ini*, indica:

> *"SD-WAN es un enfoque definido por software de la gestión de la red de área amplia o WAN"*

Wikipedia en https://www.wikipedia.org/, indica:

> *"SD-WAN es un acrónimo para redes definidas por software en una red de área amplia (WAN) que simplifica la gestión y el funcionamiento de una WAN al desacoplar el hardware de red de su mecanismo de control"*

Aruba en https://www.arubanetworks.com/, indica:

> *"La WAN definida por software es una nueva forma de dirigir el enrutamiento sobre cualquier combinación de conexiones WAN, que hace que la WAN sea más fácil de implementar y administrar mejorando los costes soportados por la organización"*

Catonetworks en *https://www.catonetworks.com/*, indica:

> *"La WAN definida por software (SD-WAN), es una nueva forma de administrar y optimizar una red de área amplia que está diseñada para abordar el uso cambiante de las redes empresariales debido al crecimiento de la computación en la nube y los dispositivos móviles. Es una solución más flexible que MPLS pues admite mejor el trabajo de forma distribuida y móvil al ser más confiable y escalable que la WAN basada en VPN"*

Uppal, Sanjay Uppal; Woo, Steve y Pitt, Dan (2018), señalan que:

> *"La WAN definida por software proporciona la ventajas típicamente asociadas con redes definidas por software (SDN) en centro de datos, pero para soluciones de red de área amplia para sucursales empresariales. Tanto SDN como SD-WAN virtualizan recursos para proporcionar una aceleración en la prestación de servicios, mejor rendimiento y disponibilidad mejorada por la automatización de la implementación y administración de la red mientras se mejora el retorno de la inversión y la reducción de costes en la organización"*. (p.5)

Sin embargo, al leer las definiciones anteriores se echa en falta el paradigma de su abstracción, es decir, el concepto diferencial que hace de SD-WAN una nueva tecnología. Ese concepto radica en posibilitar la transformación de las WAN tradicionales, fundamentadas en redes estáticas centradas en hardware, en

WAN flexibles y ágiles basadas en software, al separar eficazmente la gestión del tráfico de red de la infraestructura física de transporte subyacente.

Así, las SD-WAN pueden incorporar varias conexiones de Internet (cable, xDSL, FTTH, 4G / LTE) y opcionalmente enlaces MPLS, que bien utilizando políticas de enrutamiento y/o evaluación dinámica del tráfico selecciona la conexión óptima para cada aplicación. Esta característica hace que las redes definidas por software tengan una ventaja adicional, además de flexibilidad y agilidad, que no es otra que la rentabilidad al hacer uso de enlaces de bajo coste de Internet público.

En la siguiente imagen se puede ver la conexión de sucursales con un centro de datos de una organización. Por una lado, la sucursal 1 se conecta mediante un enlace MPLS al centro de datos de la organización, de esta manera todo el tráfico, de subida y descarga, hacia o desde Internet e incluso a la nube tiene que pasar por el centro de datos. Este hecho puede incrementar la latencia y originar cuellos de botella.

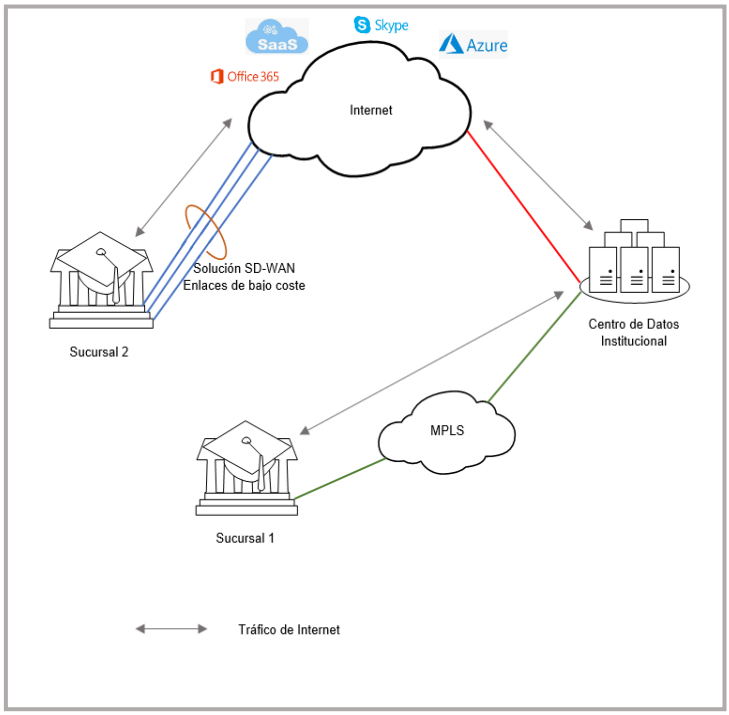


Ilustración 39: Conexión de sucursales

Por otro lado, la sucursal 2 se ha implementado con una solución SD-WAN que conecta a Internet mediante enlaces de bajo coste de proveedores de comunicaciones, en este caso el tráfico solicitado de Internet irá directamente de la sucursal 2 hacia Internet y viceversa. Además, en caso de servicios solicitados a la nube, dependiendo de las políticas de enrutamiento, también podrán ir a la sucursal 2 directamente, por ejemplo: la interacción de los alumnos de un centro docente con el campus virtual.

Además, las redes definidas por software al poder utilizar varios enlaces en una sucursal aportan un valor añadido frente a las conexiones tradicionales:

- Aumento del ancho de banda, al hacer funcionar varios enlaces como uno solo
- Dirigir mediante políticas de enrutamiento el tráfico de una aplicación específica por un enlace concreto
- Selección dinámica del enlace más idóneo, en función del tráfico o aplicación seleccionada
- Enviar el tráfico por otro enlace ante la caía del enlace predeterminado

3.2. ¿Por qué SD-WAN?

La forma de trabajar en las organizaciones ha ido sufriendo cambios notables en estos últimos años. Así, hasta hace poco resultaba factible para una institución trabajar mediante conexiones de red estáticas con sus sucursales, sin embargo, hoy en día con la llegada de los distintos servicios y aplicaciones en la nube, les surge la necesidad de expandirse geográficamente para mantenerse competitivas en un mercado cada vez más global.

Esta mayor distribución geográfica de las instituciones les obliga a disponer de una infraestructura de red dinámica, flexible y contenida en costes. Así pues, las organizaciones necesitan resolver algunos problemas que las conexiones de red tradicionales, como MPLS, tienen:

- Un incremento del coste ante la necesidad de un mayor ancho de banda, para soportar el rendimiento de ciertos servicios o aplicaciones
- Una gran complejidad y un mayor tiempo en el despliegue e implementación de nuevas sucursales
- La rigidez de la arquitectura WAN tradicional no permite de forma dinámica la migración de servicios a entornos públicos.

SD-WAN resuelve eficazmente los problemas anteriores debido a que es una WAN escalable, pues permite:

- Ampliar el ancho de banda con servicios de proveedores de Internet de bajo coste
- Desplegar e implementar nuevas sucursales, evitando la demora de tiempo que supone la adquisición e instalación de un enlace privado, así como la configuración de distintos equipos de red, que en la mayoría de las ocasiones tienen que ser instalados y configurados presencialmente en la sucursal.

Con SD-WAN el despliegue, gestión y configuración se realiza en un tiempo mínimo con escasa intervención técnica presencial.

Finalmente, en la actualidad muchas aplicaciones empresariales se trasladan a centro de datos virtuales (en la nube) e incluyen nuevos servicios (SaaS, FaaS...), donde la comunicación mediante MPLS no es las más apropiada debido a su rigidez. Por lo tanto, las instituciones deben adaptarse y evolucionar para el nuevo entorno computacional que necesitan sus servicios.

3.3. ¿Qué aporta SD-WAN?

Uppal, Sanjay et al. (2018) señalan que SD-WAN no es solo una WAN con múltiples enlaces con políticas de enrutamiento**,** es mucho más, es una tecnología que:

- Virtualiza la red al permitir que enlaces de distintos proveedores constituyan un grupo unificado de recursos
- Tiene la facultad de admitir nuevos recursos a su infraestructura al tiempo que interactúa con el equipamiento ya existente
- Rentabiliza el hardware existente (dispositivos de red, servidores...), gracias a su conceptualización respecto de la red, al separar eficazmente la gestión del tráfico de red de la infraestructura física de transporte subyacente
- Ofrece una precisa monitorización de uso y rendimiento, que permiten manejar el tráfico generado por las aplicaciones de manera eficiente empleando los enlaces más apropiados, que hace posible la virtualización de la WAN
- Posibilita una mayor automatización en el despliegue de equipos y servicios, debido a que los nuevos dispositivos no requieren de una configuración previa, al heredar la configuración y políticas según un rol preestablecido
- Permite una simplificación en la entrega de servicios, al estar definidas unas políticas de enrutamiento para los distintos actores: cliente local o externo, nube, Internet, centro de datos...

3.4. Ventajas y desventajas de SD-WAN

La red definida por software para sucursales (SD-WAN) ofrece distintas ventajas sobre la WAN tradicional construida por enlaces alquilados, tipo MPLS:

WAN de costes reducidos

En el apartado: “2.2.4 Costes de los enlaces alquilados” de este documento se refleja el alto coste que una conexión MPLS supone y se puede comprobar cómo tan solo 100 Mbps de ancho de banda supone un coste aproximado de 9.000 euros anuales.

Además, en el apartado: "3.6.2 Costes recurrentes" de este documento, se puede comprobar como una red definida por software con mayor ancho de banda supone un ahorro del orden del 50% en los costes recurrentes de los enlaces.

WAN con gestión simplificada

A medida que una organización crece más compleja es la gestión de la administración de su red, debido a los múltiples dispositivos que son usados para optimizar la red. SD-WAN permite, como se vio anteriormente, un despliegue con una implementación automatizada, unas comunicaciones seguras y escalables sobre cualquier transporte, y todo ello con una gestión centralizada.

WAN más eficiente y altamente disponible

SD-WAN permite convertir todos sus enlaces de forma virtual en uno solo, este hecho hace posible contar con un ancho de banda superior en caso de necesidad. Además, la disponibilidad de diferentes enlaces activo-activo dota a las sucursales de una redundancia sin coste adicional ante la caída de forma imprevista de un enlace. Sin embargo, MPLS se basa en la confiabilidad del servicio ya que contar una redundancia activo-activo o activo-pasivo supondría un sobrecoste que pocas organizaciones, en realidad, pueden o están dispuestas a asumir.

WAN más ágil, flexible y con rendimiento asegurado

SD-WAN se abstrae de la parte física de la red y permite satisfacer la demanda variable de tráfico de las aplicaciones eligiendo dinámicamente el enlace óptimo, así como, el envío del tráfico mediante políticas definidas de enrutamiento, lo que permite utilizar entre los enlaces de transporte disponibles el más adecuado: FTTH, xDSL, cable, 5G...

Además, asegura una descongestión de la red de la organización al evitar que el tráfico no necesario pase por su centro de datos. Por ejemplo, el tráfico enviado o descargado hacia o desde Internet por una sucursal. Con SD-WAN este tráfico va directamente desde Internet a la sucursal o viceversa.

WAN segura y más controlada

Los dispositivos SD-WAN actuales disponen de firewall incorporado, que ofrecen una óptima seguridad perimetral. Además, se autentican debido a un intercambio de claves de manera escalable e implementan con una seguridad definida por software el cifrado de extremo a extremo, proporcionando una conectividad segura.

SD-WAN permite una monitorización en tiempo real y permite, tanto una medición verídica de la latencia, así como una posible pérdida de paquetes en cada una de las conexiones. Por lo tanto, tal como hemos mencionado anteriormente, SD-WAN es capaz de adaptarse dinámicamente ante estas situaciones, al elegir el transporte más adecuado aplicando las políticas de enrutamiento implementadas.

Las desventajas más notables encontradas y además de forma recurrente, durante la realización de este trabajo, entre variada literatura consultada (ver apartado bibliográfico) son:

1. La implementación de SD-WAN necesita de la incorporación de equipamiento de seguridad adicional en las sucursales. Esto es debido a que el tráfico ya no es filtrado necesariamente por el centro de datos o nodo principal.
2. El ancho de banda de las conexiones a Internet público no está garantizado.

Actualmente, respecto a esas dos desventajas cabe puntualizar:

1. El equipamiento SD-WAN para sucursales que actualmente proveedores como Aruba y Cisco, entre otros, tienen en catálogo dispone de firewall incorporado: (puerta de enlace para sucursal descrito en la parte de equipamiento dentro del apartado: "3.5.1 Equipamiento necesario" de este documento)
2. Si bien es cierto, que las conexiones a Internet público no garantizan el ancho de banda contratado, sí lo es el hecho, que las soluciones a empresas de este tipo de conexiones de ciertos proveedores, como Movistar, Vodafone, entre otros, ofrecen un porcentaje de ancho de banda garantizado sobre el contratado, eso sí con un coste adicional.

3.5. Exposición de infraestructura y equipamiento necesario

En este apartado se expondrá la infraestructura y el equipamiento necesario para evolucionar la red de las diferentes sucursales conectadas mediante enlaces tradicionales alquilados, como MPLS, a SD-WAN en una organización que, tal como se ha venido exponiendo a lo largo de este trabajo, cuenta con distintas sucursales distribuidas geográficamente.

La exposición del contenido de este apartado no será específica respecto a fabricantes y proveedores, pues eso se abordará en el capítulo "4. Creación de un Piloto SD-WAN" . En este sentido el desarrollo de este apartado seguirá las siguientes directrices:

- La exposición, aquí realizada, será genérica, es decir, válida para cualquier organización que tenga:
    - Sucursales distribuidas geográficamente
    - Servicios en la nube (opcionalmente)
    - Y que esté en disposición de obtener distintos beneficios como los expuestos en los apartados: "3.3 ¿Qué aporta SD-WAN?" y "3.4 Ventajas y desventajas de SD-WAN"
- Ante la existencia de distintos fabricantes de equipamiento de red para la implementación de una SD-WAN como: Cisco, Aruba, Citrix... entre otros,

la descripción de los equipos se realizará de forma genérica. De la misma manera se procederá con los distintos proveedores de conexiones de comunicaciones. Sin embargo, se incluye algunas fotografías que hacen referencia a proveedores concretos.

3.5.1. Equipamiento necesario

Puertas de enlace SD-WAN para sucursal. Este dispositivo es necesario en todas aquellas sucursales en las que se pretenda implementar una red definida por software.

El diseño de estos dispositivos soporta múltiples enlaces heterogéneos como: enlaces de banda ancha, MPLS, 4G / LTE... Además entre sus características tienen la capacidad de enrutar y priorizar el tráfico (mediante políticas, de forma dinámica...) que se envía al centro de datos, nube o Internet.

Ilustración 40: Serie 7000 de Aruba SD-WAN para sucursales(*)

Estos equipos permiten dotar al sitio de una alta disponibilidad al dotarlo de una completa redundancia, al admitir configuraciones diferentes: activo / activo / activo, activo / activo / pasivo...
En el mercado, existen diferentes modelos según las necesidades o el tamaño de la organización, que aportan características respecto a sus especificaciones de fabricación, entre las más importantes destacar:

- Número máximo de clientes del sitio
- Rendimiento del firewall (Gbps)
- Rendimiento de encriptación AES-CBC (Gbps)
- Sesiones activas del firewall
- Número de interfaces WAN / LAN

Puertas de enlace SD-WAN para el centro de datos o nodos principales. La instalación de este dispositivo es necesario en el centro de datos o en el entorno de cabecera. Actúan como VPNC (concentradores de VPN) para realizar la finalización del tráfico que viene desde las puertas de enlace de las sucursales.

(*) Fuente de la Imagen: https://www.arubanetworks.com/

Estos dispositivos pueden llegar a soportar miles de puertas de enlace de sucursales (dependiendo de sus especificaciones). Además, permiten que en un modelo *dual hub-and-spoke*, se usen más de una puerta de enlace cabecera para terminar los túneles IPSec establecidos a partir de las puertas de enlaces cabeceras derivadas.

En el mercado se pueden encontrar distintos modelos para cubrir las necesidades específicas de las organizaciones. Las especificaciones de fabricación más destacadas que se pueden encontrar son:

- Rendimiento de encriptación 3DES (Gbps)
- Rendimiento de encriptación AES-CBC (Gbps)
- Rendimiento de la compresión WAN (Gbps)
- Número máximo de túneles

Ilustración 41: Serie 7200 de Aruba, SD-WAN para cabeceras(*)

Puertas de enlace SD-WAN para nube pública. En este caso son dispositivos virtuales que suelen implementarse en arquitecturas de nube pública, como una red virtual de *Microsoft Azure* (VNET) o en una nube privada virtual como *Amazon Web Services* (AWS VPC).

Estas puertas de enlace virtuales funcionan de forma similar a las puertas de enlace virtuales tipo cabecera, permitiendo la conectividad de todas las sucursales y centro de datos a las nubes públicas. Este tipo de puertas de enlace se gestionan de manera centralizada, permitiendo: monitorizar, administrar y completamente el estado de la red definida por software. Además, estos dispositivos pueden llegar a ofrecer actualmente un rendimiento por encima de los 4 Gbps.

Software orquestador. Es el software centralizado, generalmente en una plataforma unificada para todas las operaciones, encargado de la administración, gestión, monitorización y despliegue de la red SD-WAN.

(*) Fuente de la imagen: https://www.arubanetworks.com/

3.5.2. Infraestructura necesaria

Como infraestructura la organización necesita contar con diferentes enlaces de conexión tanto para el centro de datos, como para las distintas sucursales. Como se ha expuesto anteriormente, una de las características que singularizan a las redes definidas por software SD-WAN, es la admisión de múltiples enlaces de conexión. De esta manera, se podrán instalar tantas conexiones en las puertas de enlace como se necesiten con las dos únicas restricciones siguientes: el coste que la organización esté dispuesta a asumir y la capacidad de puertos del propio dispositivo. Por lo tanto, se podrán incorporar(*):

- Enlaces de banda ancha
- Enlaces alquilados(**) tipo MPLS y punto a punto
- Enlaces propios
- Enlaces tipo 4G / LTE

En la ilustración siguiente se puede ver el diagrama de la implementación de una solución SD-WAN:

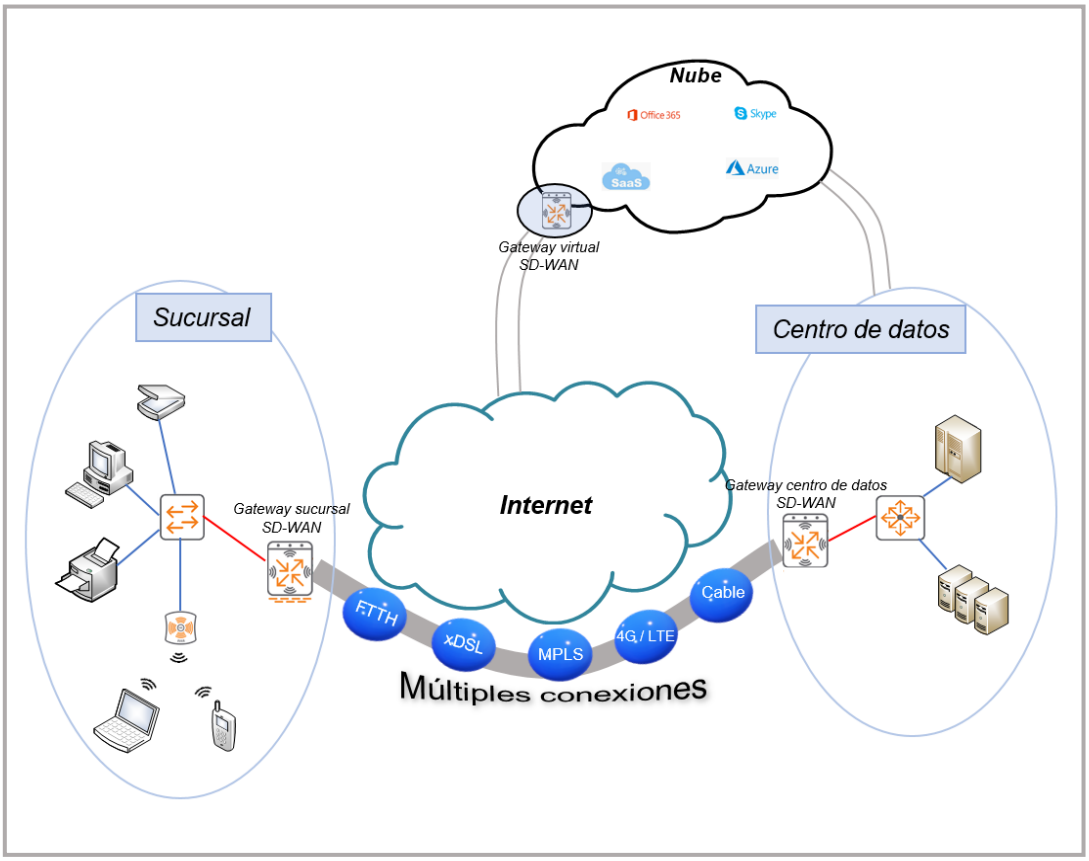


Ilustración 42: Solución SD-WAN empresarial

(*) Según disponibilidad geográfica y de proveedores

(**) Aunque, el objetivo principal de este trabajo es analizar la posibilidad de evolución las sucursales conectadas actualmente mediante enlaces alquilados a SD-WAN, eliminando este tipo de conexiones, debe quedar claro que SD-WAN admite este tipo de enlaces a su infraestructura, gestionándolo como uno más.

3.6. Costes

Antes de comenzar con lo que este apartado incluirá respecto a la infraestructura SD-WAN, se indica lo que no incluye: En este apartado no se tratarán los costes de contratar una SD-WAN como un servicio o producto que actualmente ofrecen distintos proveedores de comunicaciones como: Vodafone[(1)], Catonetworks[(2)], entre otros.

Este apartado incluye la exposición de los diferentes costes económicos a los que una organización tendrá que hacer frente, para implantar una red definida por software SD-WAN con equipos en propiedad y cuya gestión, administración y despliegue puede recaer en ella o en terceros, pero siempre por decisión de la propia institución. Los costes económicos que se incluirán serán los de inversión, los recurrentes y los de puesta en producción.

Además, en los costes se contemplan distintos escenarios tanto para la sede principal como para las sucursales remotas e incluso para los servicios virtuales en la nube. Esta diferenciación de escenarios se justifica, por un lado, para optimizar los recursos económicos de la empresa, es decir, comprar lo que realmente se necesita y por otro lado, para ajustar las especificaciones que ofrece un modelo de equipo determinado a las necesidades reales (actuales o futuras) que una organización tiene en cada una de sus sedes: número de usuarios simultáneos, sesiones de aplicaciones, servicios en la nube, ancho de banda requerido...

En el mercado existen diferentes fabricantes de equipamiento SD-WAN, entre ellos por nombrar algunos están: Cisco, Citrix, Juniper, Aruba..., cada uno de estos fabricantes dispone de su propio catálogo de equipamiento que incluye diferentes modelos con características específicas.

Con el fin de enriquecer el trabajo y poder comparar, se incluirán los precios de dos fabricantes: Citrix y Aruba. Ambos fabricantes han tenido a bien proporcionar los precios de sus equipos, licencias y soporte, lo que contribuye a la elaboración de un trabajo más objetivo.

Finalmente, hay que indicar que implementar y poner en marcha una infraestructura SD-WAN conlleva:

- Los costes de: equipamiento, puesta en marcha, licenciamiento, mantenimiento y enlaces durante el primer año.
- Los coste llamados recurrentes: licenciamiento, mantenimiento y enlaces durante los años sucesivos, siempre que los dos primeros se opten por pagarlos de forma anual y no por periodos mayores.

[(1)] Vodafone: https://www.vodafone.es/c/empresas/pymes/es/conectividad/vodafone-conectividad-aumentada/
[(2)] CatoNetworks: https://www.catonetworks.com/cato-cloud#edge-sd-wan

3.6.1. Costes de inversión

Tal como vimos en el apartado: "3.5.1 Equipamiento necesario", el equipamiento necesario para implantar una red SD-WAN se compone de una gateway para cada una de las sucursales remotas en las que se quiera instalar o evolucionar hacia este modelo de red, una gateway para la sede principal, una gateway virtual para los servicios en la nube y el software orquestador.

El gateway virtual para servicios en la nube, es opcional y dependerá de distintos factores, como por ejemplo: que la organización disponga de servicios virtualizados, lo contemple en su diseño y/o en sus políticas de red para ofrecerlos por la Internet pública sin pasar por su centro de datos...

A continuación, se exponen los costes del distinto equipamiento para los dos fabricantes de tecnología SD-WAN, que incluye el equipo para las distintas sedes (principal, remota y virtual) en función de su tamaño y/o necesidades:

3.6.1.1. Equipamiento SD-WAN Citrix

En el anexo XI de este trabajo se puede encontrar el presupuesto remitido por el proveedor de Citrix fruto de distintos encuentros mantenidos con su unidad técnica y comercial para la obtención del coste económico ante los distintos escenarios propuestos.

En la siguiente tabla se muestra el detalle del equipamiento:

Coste de equipamiento Citrix					
Gateways	Sede	Tamaño	Modelo	Tráfico encriptado(1)	Precio(2)
	Cabecera		4100 SE	Hasta 6 Gbps	7.685 €
	Remotas	pequeña	210 SE	Hasta 600 Mbps	389 €
		mediana	2100 SE	Hasta 4 Gbps	3.380 €
		grande	2100 SE	Hasta 4 Gbps	3.380 €
	Nube		VPX SE	Hasta 2 Gbps	14.629 €
Software	Orquestador(3)				-

Ilustración 43: Costes Gateways SD-WAN Citrix

(1) Tráfico encriptado se refiere a la cantidad máxima total con el licenciamiento contratado.
(2) El precio de los equipos es de lista, no lleva aplicado ni impuestos ni descuentos.
(3) El software orquestador va incluido con la adquisición de los gateways

Como se observa en la tabla anterior, el gateway 2100 SE tiene el mismo precio para una sucursal mediana y grande. Esto se debe a que el equipo es válido para ambos escenarios y la diferencia está en su licencia. El licenciamiento de los gateways Citrix se realiza por el máximo de tráfico encriptado que se contrate y no por el máximo de sus capacidades.

Así pues, el coste del equipo físico se paga una sola vez, pero su licencia tendrá un gasto anual recurrente, que como se verá en el apartado: "3.6.2 Costes recurrentes" un mismo gateway se puede licenciar para distintos anchos de

banda de encriptación y por lo tanto, el coste de licencia anual será diferente para cada caso. En el anexo XII de este documento se encuentran las especificaciones del equipamiento Citrix para SD-WAN.

3.6.1.2. Equipamiento SD-WAN Aruba

El fabricante Aruba, ha proporcionado una dirección web desde la que se pueden obtener los costes económicos de sus productos SD-WAN. En el Anexo XIII de este trabajo se encuentra toda la información relativa a precios oficiales de lista de este fabricante.

En la siguiente tabla se muestra el detalle del equipamiento:

Coste de equipamiento Aruba					
Gateways	Sede	Tamaño	Modelo[1]	Tráfico encriptado[2]	Precio[3]
	Cabecera	pequeña	7010	2,6 Gbps/ 512 túneles	3.748 €
		mediana	7210	7 Gbps/ 512 túneles	16.397 €
		grande	7220	22Gbps/ 4096 túneles	24.361 €
	Remotas	pequeña	7005[4]	1,2 Gbps/ 1024 usuarios	1.588 €
		mediana	7010	2,6 Gbps/ 2048 usuarios	3.748 €
		grande	7210	6 Gbps/ 16 K usuarios	16.397 €
	Nube[5]		VNET	500 Mbps	-
			VNET	2 Gbps	-
			VNET	4 Gbps	-
Software	Orquestador[6]				-

Ilustración 44: Costes Gateways SD-WAN ARUBA

(1) Todos los modelos de gateways de Aruba pueden ser instaladas en sitios remotos o cabeceras indistintamente, excepto los modelos 9004 y 7005. Los equipos serie 72xx llevan fuentes redundadas.
(2) Tráfico máximo encriptado para cada modelo como AES-CBC-256 sin limitación por licencia. Máximo de túneles y máximo de usuarios concurrentes.
(3) El precio de los equipos es de lista, no lleva aplicado ni impuestos ni descuentos.
(4) Los equipos más pequeños como 7005 y 7008 la licencia base está limitada a 75 usuarios concurrentes,. Sin embargo, en los diferentes encuentros que se han mantenido con el proveedor, nos han indicado que esa limitación, en la licencia base de esos equipos, se va a suprimir en los próximos meses dejando los equipos en su licencia base con el máximo de usuarios que admiten en sus especificaciones. En el coste va incluido el kit opcional para rack de 19 pulgadas por un precio de 187 euros.
(5) El gateway virtual para la nube no tiene coste de compra, solo tiene el coste de licencia que será visto en el apartado: "3.6.2 Costes recurrentes"
(6) El software orquestador de gestión en este caso va incluido con la adquisición de un gateway cabecera y con tantas licencias como número de gateways adquiridos. (Anexo XVI)

El coste de los equipos físicos se paga una sola vez, pero su licencia tendrá un gasto anual recurrente, que como se explica en el apartado: "3.6.2 Costes recurrentes".

En el Anexo XIV de este documento se encuentran las especificaciones del equipamiento Aruba para SD-WAN.

3.6.2. Costes recurrentes

Este tipo de gastos son los realizados de forma reiterada por las organizaciones por periodos de tiempo iguales. De esta manera, una organización que cuente o quiera contar con una infraestructura de red SD-WAN tendrá que frente principalmente a los siguientes costes: licencias y mantenimientos de los gateways SD-WAN, así como los enlaces contratados a operadores de comunicaciones.

En general, este tipo de proyectos son a largo plazo y por lo tanto, la contratación de licencias y servicios de mantenimiento se realiza por periodos mayores a un año, normalmente entre 3 y 5 años, fundamentalmente a dos razones:

- Los proveedores permiten fraccionar el pago en anualidades sin sobrecoste, tal como nos indicaron desde la comercial de Citrix y Aruba.
- El coste anual es entorno a un 30% menor, respecto al coste de contratación anual de los servicios, lo que supone un ahorro considerable.

En primer lugar, se detallará el coste económico de las licencias y mantenimiento de los equipos incluidos en el apartado: "3.6.1 Costes de inversión" para cada uno de los dos fabricantes Citrix y Aruba, tal como se hizo con el precio de los equipos dicho apartado. En segundo lugar, se detallará el coste de distintas conexiones de proveedores de comunicaciones para completar los costes de la infraestructura SD-WAN.

3.6.2.1. Mantenimiento y licenciamiento SD-WAN Citrix

En el Anexo XI de este trabajo se puede encontrar el presupuesto remitido por el proveedor de Citrix, que contiene el coste de mantenimiento y de licencia para cada uno de los equipos presupuestados. Las características de los equipos se pueden encontrar en el Anexo XII. En la siguiente tabla se muestra el detalle de costes:

Costes de mantenimiento y licenciamiento de Citrix							
	Sede	Tamaño	Modelo	Licenciamiento		Mantenimiento	
				Ancho de banda(1)	Precio(2)	Tipo(3)	Precio(4)
Gateways	Cabecera		4100 SE	2 Gbps	9.234 €	Gold	1.217 €
	Remotas	pequeña	210 SE	200 Mbps	1.107 €	Silver	48 €
		mediana	2100 SE	500 Mbps	1.254 €	Silver	365 €
		grande	2100 SE	1 Gbps	6.721 €	Silver	365 €
	Nube		VPX SE	500 Mbps	2.192 €(5)	-	-
Software	Orquestador(6)			-	-	-	-

Ilustración 45: Costes de mantenimiento y licenciamiento Citrix

(1) Ancho de banda máximo contratado por licencia (tráfico encriptado).
(2) El precio del licenciamiento está anualizado y lleva un 40 % de descuento aplicado sobre el precio de lista. No lleva incluido impuesto.
(3) El mantenimiento Gold lleva incluido atención 24x7 hardware y software, envío de hardware en 24 horas. El mantenimiento Silver lleva incluido reposición hardware en 24 horas y atención software, en ambos casos en horario comercial.
(4) El precio de mantenimiento es anualizado y no lleva aplicado ni descuentos y tampoco impuestos.
(5) El precio de licenciamiento del gateway virtual para la nube es de 1.931 euros a los que hay que sumarle 261 euros del coste anual del orquestador.
(6) El precio del licenciamiento del orquestador va incluido en el precio de licenciamiento de los Gateways, excepto en el gateway virtual para la nube que se ha sumado de forma independiente.

3.6.2.2. Mantenimiento y licenciamiento SD-WAN Aruba

En el Anexo XIII de este trabajo se encuentra el coste de licenciamiento y mantenimiento para cada uno de los equipos presupuestados. Las características de los equipos se encuentran en el Anexo XIV, así como la guía sobre licenciamiento en el Anexo XV.

En la siguiente tabla se muestra el detalle de costes:

Costes de mantenimiento y licenciamiento de Aruba							
	Sede	Tamaño	Modelo	Licenciamiento		Mantenimiento	
				Tipo/Ancho de banda(1)	Precio(2)	Tipo(3)	Precio(4)
Gateways	Cabecera	pequeña	7010	*Foundation*	721 €	NBD E/R	280 €
		mediana	7210	*Foundation*	7.207 €	NBD E/R	1.189 €
		grande	7220	*Foundation*	7.207 €	NBD E/R	1.783 €
	Remotas	pequeña	7005	*Foundation*	721 €	NBD E/R	105 €
		mediana	7010	*Foundation*	721 €	NBD E/R	280 €
		grande	7210	*Foundation*	7.207 €	NBD E/R	1.189 €
	Nube(5)		VNET	500 Mbps	2.273 €	-	-
			VNET	2 Gbps	4.766 €	-	-
			VNET	4 Gbps	5.958 €	-	-
Software	Orquestador(6)			-	-	-	-

Ilustración 46: Costes de mantenimiento y licenciamiento de Aruba

(1) El licenciamiento *Foundation* permite el uso del equipo por el máximo de sus capacidades. Las características de la gateways de Aruba se encuentran en el Anexo XIV . El gateway virtual para la nube se licencia en función del ancho de banda.
(2) El precio del licenciamiento es de lista y está anualizado. No incluye descuentos y tampoco impuestos.
(3) El mantenimiento NBD E/R lleva incluido el envío de hardware intercambiable en 24 horas y mantenimiento software en horario comercial. Puede encontrarse el detalle completo en: https://techlibrary.hpe.com/us/en/networking/products/configurator/index.aspx#.XrBSRY0Unuj
(4) El precio de mantenimiento es anualizado y lleva aplicado un descuento y no incluye impuestos.
(5) El precio de licenciamiento del gateway virtual para la nube es según el ancho de banda contratado y es el único coste que tiene este dispositivo.
(6) El precio del licenciamiento del orquestador va incluido al adquirir un gateway cabecera (Anexo XVI).

3.6.2.3. Conexiones de proveedores de comunicaciones

En este apartado se incluyen los costes anualizados para diferentes anchos de banda y tipos de enlace. En el mercado existen muchos proveedores como puede ser: Vodafone, Movistar, Orange, Yoigo, Ono, Viasat, SkyDSL, entre otros. Estos operadores ofrecen diferentes anchos de banda y precios en sus productos para empresas.

En la siguiente tabla se incluyen diferentes tipos de enlaces con distintos anchos de banda y con un precio promediado de entre varios proveedores. Estos se han extraído de la sección para empresas de su páginas web a fecha de redacción de este trabajo y que están disponibles en apartado: "7. Bibliografía" de este documento.

Tipo	Ancho de banda[1]	Limitación datos[2]	Coste[3]
FTTH	100 Mbps	-	420 €
	200 Mbps	-	440 €
	300 Mbps	-	480 €
	600 Mbps	-	540 €
	1 Gbps	-	660 €
xDSL	20 Mbps	-	240 €
4G	Hasta máxima de 4G[4]	110GB	492 €
		-	780 €
5G	Hasta máxima de 5G[4]	60 GB	600 €
		-	840 €
B. ancha móvil	2 Mbps	-	420 €
	10 Mbps	-	480 €
HFC	50 Mbps	-	420 €
	120 Mbps	-	480 €
	300 Mbps	-	540 €
Satelite[5]	30 Mbps	-	600 €
	50 Mbps	-	720 €
FTTH + 5G	1 Gbps	-	1.068 €
	600 Mbps	-	960 €
MPLS[6]	100 Mbps	-	8.800 €
	1 Gbps	-	12.200 €
Punto a Punto[7]	1 Gbps	-	3.200 €

Ilustración 47: Costes enlaces

(1) El ancho de banda es el máximo pero no está garantizado excepto en la línea MPLS y punto a punto. Respecto al 4G y 5G, además de no estar garantizado, será el máximo que haya disponible en la zona.

(2) En el caso donde está limitado el uso de datos a una cantidad, por un lado, es por mes a máxima velocidad y por otro lado, una vez agotada la cantidad contratada se sigue haciendo uso de la red a menor velocidad entre 64 y 128 Kbps.

(3) Los costes están anualizados y no incluyen impuestos, además están promediados de entre distintos proveedores del estado español y son solo una referencia en una mercado cambiante diariamente. Los costes de las líneas MPLS y punto a punto son los incluidos en el apartado: "2.2.4 Costes de los enlaces alquilados", fruto del promedio de una licitación pública.

(4) La contratación de 4G y 5G, no implica el acceso a la red a su máxima velocidad.

(5) La velocidad de acceso a la red incluida en la tabla mediante satélite no es simétrica para esto anchos de banda.

(6) El coste del enlace MPLS fue licitado entre poblaciones de una misma provincia.

(7) El coste del enlace punto a punto fue licitado para sitios dentro de la misma población.

La lista de productos, que las distintas empresas de servicios de comunicaciones ofertan, puede ser interminable a la vez que cambiante con aumentos de anchos de banda y rebaja de precios. Además, para grandes empresas estos proveedores disponen un espacio web propio, donde solicitar una reserva para la obtención de servicios y precios personalizados a las necesidades concretas de cada organización.

Por otro lado, no todos los operadores disponen de todos los servicios y tampoco todos los servicios están disponibles en todos los territorios, ya sean nacionales o internacionales. Además, un punto muy importante cuando se implanta una infraestructura SD-WAN, es que en las sucursales los diferentes enlaces de comunicaciones que se contraten sean a diferente proveedor y con diferente zanja.

3.6.3. Costes de puesta en producción

Estos costes son los que incluyen la instalación y configuración de los distintos elementos SD-WAN, como gateways y el software orquestador, así como la integración con el resto de infraestructura de la organización.

Estos procesos pueden ser realizados bien por integradores y *partners* o bien por el propio personal TIC de la organización. En los distintos encuentros que se han mantenido con Citrix y Aruba, estos proveedores insisten que el equipamiento es de instalación toque cero, es decir, que al conectarlos a la red su disponibilidad es inmediata y señalan que una vez conectados, desde el software orquestador, se realiza fácilmente y de forma intuitiva el despliegue, administración y gestión de los equipos.

Por un lado, Aruba ante la petición de un precio de instalación, indican que en su configurador de costes web[(1)] existe una opción de instalación y puesta en marcha de sus equipos (*Install & Start up*)[(2)]. Así, en los presupuestos de los distintos gateways de Aruba, incluidos en el Anexo XIII, se encuentra este servicio con código H1RS8E por un coste de 2.838 euros, impuestos no incluidos y para todos los gateways SD-WAN de Aruba expuestos en este trabajo.

Por otro lado, desde Citrix no pueden ofrecernos un precio sobre la instalación y puesta en marcha, ya que ese servicio es ofrecido por personal externo. Sin embargo, ofrecen gratuitamente al igual que Aruba, varias sesiones de formación para el personal de la organización al adquirir el equipamiento.

Así pues, en el caso de ser realizado por personal externo (integradores o *partners*), el precio variará en función de las características de nuestra organización respecto a los servicios locales y *cloud*, aplicaciones y tipo de tráfico, infraestructura actual... y por supuesto, a las de las propias sucursales: tipos de enlaces contratados, servicios como los de voz, videoconferencias, clases on-line..., configuración del firewall...

---

(1) Costes Aruba: https://techlibrary.hpe.com/us/en/networking/products/configurator/index.aspx#.XrBSRY0Unuj

(2) *Install & Start up*: Se encuentra como opción en el mantenimiento del producto de la web anterior

Además, de las distintas configuraciones a realizar sobre el equipamiento SD-WAN, por ejemplo: definición de caminos del tráfico predeterminados en función de la aplicación o servicio utilizado en cada sede, reserva de ancho de banda para determinadas aplicaciones o servicios, establecimiento de los umbrales mínimos aceptables por servicio o aplicación, la configuración de caminos alternativos para el tráfico bien por caída del enlace predeterminado o deterioro de la calidad de servicio...

Por todo lo anteriormente expuesto, es difícil ofrecer en este trabajo un precio objetivo sobre este tipo de costes cuando una empresa externa lleva a cabo este tipo de proyecto. Sin embargo, consultado el Colegio Oficial de Ingenieros Técnicos en Informática de Castilla-La Mancha (COITICLM) indican que la hora de ingeniería para este tipo de proyectos está entre la horquilla de 70 y 100 euros/hora para un ingeniero sénior y entre 35 y 45 euros/hora para un ingeniero júnior, costes que trasladan para la elaboración de este apartado, según los datos obtenidos de distintos colegiados consultados.

Por lo tanto, el coste sería la suma del número de horas dedicadas por cada tipo de ingeniero multiplicadas por su coste hora correspondiente.

Por otro lado, si la organización dispone del personal propio cualificado, este será el encargado de todo el proceso (instalación y configuración). De esta manera, el coste es mínimo. Por un lado, porque no existen costes de contratación de personal externo y por otro lado, debido a que los fabricantes ofrecen gratuitamente varias sesiones formativas de configuración del equipamiento SD-WAN, así lo transmitieron los proveedores Aruba y Citrix en las distintas reuniones que se mantuvieron con ellos.

Además, la organización también cuenta con el soporte hardware y software incluido en el contrato de mantenimiento suscrito con el fabricante.

Así pues, la forma de cuantificar el coste de puesta en producción cuando recae en el personal de la propia organización sería: cuantificar el número total de horas de formación recibidas, de dedicación a la instalación y configuración de la infraestructura SD-WAN, y multiplicarlas por el coste hora/salario de cada empleado implicado en este proyecto.

4. Creación de piloto SD-WAN

Este apartado tiene por objetivo, diseñar una infraestructura SD-WAN entre una sucursal remota y una sede principal de la institución universitaria, que ha sido objeto de estudio en este trabajo. Además, se implementará una red SD-WAN en pruebas, es decir, un piloto entre la sede principal de uno de los campus de la institución universitaria estudiada a lo largo del capítulo 2 de este documento "1. Infraestructura inicial", y una de sus sucursales que utiliza como medio de acceso a la red un enlace alquilado. Para ello:

En primer lugar, se definirá entre que nodo principal y sucursal se va a llevar a cabo la realización del piloto de red SD-WAN.

En segundo lugar, partiendo del tipo de tráfico y aplicaciones que actualmente utiliza la sucursal remota, se especificarán las decisiones de gestión y administración de la red y de sus servicios.

En tercer lugar, se diseñará la infraestructura de red para este piloto en base a: equipamiento específico para su construcción: equipamiento, enlaces... (descripción y costes).

En cuarto lugar, se llevará a cabo la construcción de la red SD-WAN, es decir, la puesta en marcha de los tres pasos anteriores: definición, especificación y diseño.

En quinto lugar, se realizarán algunas pruebas sobre esta red: redundancia, monitorizaciones, calidad de servicio...

Finalmente, se incluirán unas conclusiones sobre el piloto SD-WAN implementado en base a los cinco pasos anteriormente expuestos.

4.1.1. Definición

A lo largo del capítulo 2 se introdujo la infraestructura de red que una institución universitaria tiene actualmente en producción, y como esta organización está distribuida geográficamente en distintos campus universitarios situados en varias provincias de una comunidad autónoma del estado español. Además, varias de sus sucursales no están conectadas a la red por medio de enlaces propios, sino alquilados a un proveedor de comunicaciones.

Así, en el apartado: "2.2 Principales sucursales objeto de estudio" de este documento, se describieron todas aquellas sucursales que tienen acceso a la red con enlaces alquilados tipo MPLS o punto a punto y cuyo coste, falta de redundancia, entre otras características, las hace especialmente idóneas para llevar a cabo la evolución hacia una red SD-WAN.

En el apartado referenciado, se incluye distinta información para cada una de las sucursales, como: la descripción del equipamiento y medio con el que accede a la red, así como algunas gráficas respecto al ancho de banda demandado.

En la siguiente tabla, se encuentran de forma resumida algunos de los datos más representativos de red en esas sucursales:

Campus	Sucursal	Tráfico Descarga		Tráfico Subida		Tipo enlace	Ancho de banda[1] subida / descarga	Coste
		Máximo	Medio[2]	Máximo	Medio[2]			
CR	AGR	232 Mbps	9 Mbps	85 Mbps	7 Mbps	Punto a punto	1 Gbps / 1 Gbps	3.200 €
	AL[3]	200 Mbps	53 Mbps	98 Mbps	22 Mbps	MPLS	100 Mbps / 200 Mbps	8.800 €
AB	FMyF	255 Mbps	27 Mbps	202 Mbps	14 Mbps	Punto a punto	1 Gbps / 1 Gbps	3.200 €
TO	TA	201 Mbps	138 Mbps	28,5 Mbps	121 Mbps	MPLS	1 Gbps / 1 Gbps	12.200 €
	TR	64 Mbps	-	16,5 Mbps	-	MPLS	100 Mbps / 100 Mbps	8.800 €
	SPM	579 Mbps	219 Mbps	202 Mbps	66 Mbps	Punto a punto	1 Gbps / 1 Gbps	3.200 €
	LO	84 Mbps	17 Mbps	77 Mbps	6 Mbps	Punto a punto	1 Gbps / 1 Gbps	3.200 €
	PA	283 Mbps	133 Mbps	96 Mbps	27 Mbps	Punto a punto	1 Gbps / 1 Gbps	3.200 €
CU	-	-	-	-	-	-	-	-

Ilustración 48: Tabla resumen sucursales remotas

(1) El ancho de banda se realiza sobre enlaces de 1 Gbps, aunque el caudal contratado es el que refleja la tabla. El tráfico de descarga se refiere al que hace la sucursal de la sede principal de su campus y el de subida el que sube la sucursal a la sede principal de su campus.

(2) Los datos del tráfico de subida y descarga en sus valores medios no son objetivos debido al estado de alarma que desde el 13 de marzo y actualmente a fecha de redacción de este documento, tiene el estado español en todo su territorio. Durante el estado de alarma los edificios universitarios permanecen cerrado y sin clases presenciales, lo que hace que el tráfico medio no sea relevante.

(3) El enlace de la sucursal AL hasta el operador tiene contratado 200 Mbps.

Para establecer las ubicaciones (cabecera y sucursal) sobre la que implementar el piloto SD-WAN se han mantenido distintas reuniones con responsables de los servicios de red de la institución.

Por un lado, indican que la sucursal TA, aunque tiene el coste más elevado del enlace podría considerarse una de las principales candidatas. Sin embargo, hay que descartarla debido a que RedIRIS ha comunicado a la organización que en breve dispondrán del servicio de RedIRIS-Nova(*) en esa sucursal.

Por otro lado, desde el Área TIC de esta universidad indican que la mejor ubicación para instalar la cabecera es en el nodo principal del campus CR, debido a que por un lado, están ubicados el CPD físico y la salida a Internet de la organización y por otro lado, ese campus dispone de dos sucursales con enlaces alquilados AGR y AL.

Finalmente, la organización selecciona la sucursal remota AL para llevar a cabo el piloto SD-WAN, argumentando que, sobre la sucursal AGR, hay prevista una obra civil para instalar fibra propia entre ella y el nodo principal, con lo que el coste recurrente del enlace desaparecería y la redundancia quedaría asegurada.

(*) En el Anexo I se puede encontrar información adicional respecto a RedIRIS Nova.

Así pues, el piloto SD-WAN se llevará a cabo sobre el nodo principal del campus CR y la sucursal AL. Los detalles de esta sucursal se describieron en el apartado: "2.2.1.2 Sucursal AL" .

La siguiente ilustración muestra la situación actual de red entre la sucursal AL y su nodo principal, así como algunos datos relativos al tráfico entre ambas.

Campus	Sucursal	Tráfico Descarga		Tráfico Subida		Tipo enlace	Ancho de banda subida / descarga	Coste
		Máximo	Medio	Máximo	Medio			
CR	AL	200 Mbps	53 Mbps	98 Mbps	22 Mbps	MPLS	100 Mbps / 200 Mbps	8.800 €

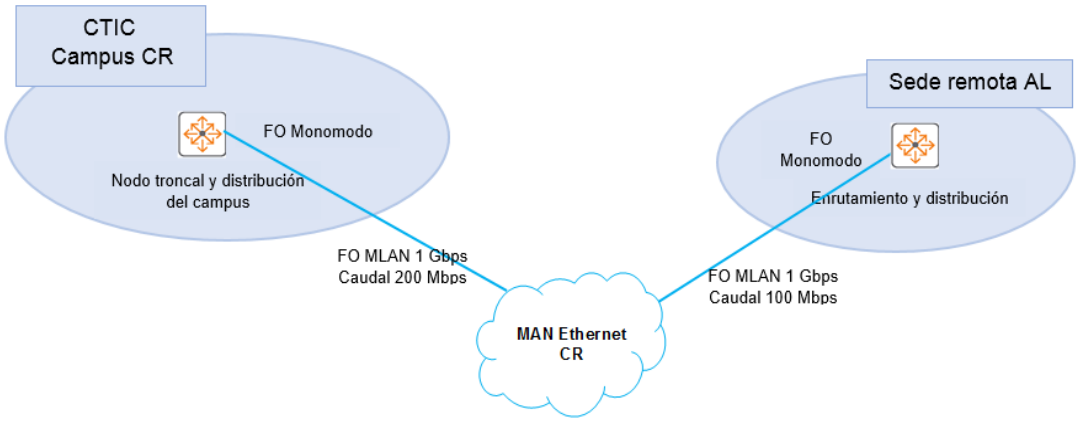


Ilustración 49: Situación actual sucursal AL

4.1.2. Especificación

Actualmente, con la infraestructura en producción existente entre la sucursal remota y la sede principal, (una conexión MPLS sobre la que se tuneliza todo el tráfico), la organización no dispone de los datos necesarios para poder realizar un análisis y segmentación por cantidad y tipo de tráfico.

Sin embargo, de entre el distinto de tráfico que existe entre ambos sitios: comunicaciones unificadas, redes sociales, servicios office 365..., la institución es consciente de cuál es el nivel de priorización sobre el tráfico generado entre los distintos servicios y aplicaciones.

Una aproximación respecto a la prioridad del tráfico, que el responsable de red de la organización tiene, la divide en: oro, plata y bronce, es decir, oro es la prioridad más alta, plata aun siendo importante iría por debajo de oro y por último, más baja la denomina bronce.

En la siguiente tabla se muestran distintas aplicaciones y servicios que generan tráfico entre sucursal y nodo principal, así como la prioridad otorgada a cada una de ellas.

Tráfico		
Prioridad		**Servicios y aplicaciones**
Oro	Comunicaciones corporativas unificadas	• Voz • Videoconferencia — por Skype empresarial
Plata	Office 365	• Correo corporativo • Servicios de corporativos de almacenamiento y compartición corporativos en la nube: ▪ SharePoint ▪ OneDrive • Teams
	Campus virtual	• Tráfico de ida y vuelta
	Gestión institucional	• RRHH • Académico • Investigación • Contabilidad • ...
Bronce	Redes sociales	• Twitter • Facebook • Telegram • ...
	YouTube	
	Google drive	• Almacenamiento y compartición de servicios no corporativos
	Web	• Navegación • Aplicaciones — no corporativa
	... ...	

Ilustración 50: Prioridades de servicio y aplicaciones

La forma de implementar este tipo de prioridades es mediante políticas de selección dinámica de la ruta (DPS)[(1)].

4.1.3. Diseño

En este apartado se describirá, de forma específica, los componentes necesarios para evolucionar, entre la sucursal remota AL y el nodo principal del campus CR, la infraestructura de red actual hacia una red SD-WAN y para ello se especificará:

- El hardware que se usará y sus características principales
- El software de gestión y administración necesario tanto para el despliegue como la monitorización de la red SD-WAN
- El conjunto de enlaces que formarán parte de la infraestructura
- El coste de la solución

Finalmente, se incluirá de manera gráfica el resultado teórico final de la infraestructura SD-WAN entre la sucursal y el nodo principal del campus CR.

---

(1) En el "Anexo XIX" se puede encontrar información detallada sobre las políticas de selección de la ruta DPS.

4.1.3.1. Equipos hardware (Gateways) del piloto SD-WAN

La elección del fabricante del equipamiento hardware para el diseño del piloto entre la sucursal remota y el nodo principal de la institución universitaria que se ha estudiado a lo largo de este trabajo es Aruba.

Esta decisión ha sido tomada en base a dos razones principales:

En primer lugar, es un fabricante de primer nivel. Además, la segmentación de modelos es amplia y por lo tanto, se puede elegir el equipo óptimo entre el abanico amplio que su catálogo ofrece. Así, por un lado cumple con las necesidades demandadas por la institución y por otro lado, incluye las posibilidades de un crecimiento futuro.

En segundo lugar, la electrónica que la institución tiene en su red troncal en los cuatro campus, las controladoras de red WIFI y una amplia cantidad de los conmutadores de distribución y acceso, en los diferentes edificios, son del mismo fabricante.

Finalmente, una integración de equipamiento uniforme en cuanto a fabricante y software de gestión hace que el conjunto tenga una funcionalidad óptima. Sin embargo, no quiere decir que ir hacia un solo fabricante no conlleve sus riesgos.

El equipamiento gateway para la cabecera seleccionado es un Aruba 7210(1), es un equipo apto para cabecera de tamaño medio / grande según la hoja de datos del fabricante. Además, dispone de unas características como: 7Gbps de cantidad de encriptación de tráfico, un óptimo rendimiento, un gran número de túneles posibles y de sesiones concurrentes, además de doble fuente extraíble redundada... que lo hacen idóneo para la ubicación seleccionada. En la ilustración 52 de la página siguiente, se puede ver un resumen de sus características principales.

A continuación, se pueden ver algunas vistas reales del equipo:

Ilustración 51: Vistas del gateway Aruba 7210(*)

El equipo gateway para la sucursal elegido es un Aruba 7008(2), es un equipo diseñado para un sitio de tamaño pequeño según la hoja de datos del fabricante. Las características del equipo, que se pueden ver, de manera resumida, en la tabla de la ilustración 52 de la página siguiente.

(*) La imagen del equipo Aruba 7210, 7210 y 7240 son iguales exteriormente

(1)(2) En el Anexo XIV se puede encontrar las especificaciones de los distintos gateways SD-WAN de Aruba.

(1)(2) Los equipos 7210 y 7008 de Aruba puede funcionar como controladora WIFI, en el Anexo XVII se encuentra información complementaria

Este equipo, por sus características, encaja sobradamente con las necesidades de sitio remoto, al ser capaz de manejar hasta 1.024 clientes simultáneos con una capacidad de encriptación de tráfico de hasta 1,2 Gbps y una filtración de su firewall de 2 Gbps, datos muy por encima del ancho de banda contratado en la conexión MPLS que tiene actualmente 200 Mbps de descarga y 100 Mbps de subida. A continuación, se pueden ver algunas imágenes reales del equipo:

Ilustración 52: Vistas del gateway Aruba 7008

Las principales características técnicas del modelo 7210[(1)] y 7008[(2)] de Aruba, se exponen en la siguiente tabla:

Características técnicas de los gateway del piloto		
Especificaciones	**7210**	**7008**
Clientes máximos	16 K	1.024
Rendimiento del firewall	20 Gbps	2 Gbps
Rendimiento de encriptación (AES-CBC)	7 Gbps	1,2 Gbps
Sesiones activas de firewall	2 M	64 K
Túneles GRE concurrentes	1.024	256
Sesiones IPsec concurrentes	16.384	1.024
Sesiones SSL concurrentes	8.192	1.024
Rendimiento por cable puenteado	20 Gbps	4 Gbps
Interfaces WAN/LAN (10/100/1000BASE-T)	2 combo	8
Interface 1000BASE-X	2 combo	-
Puertos 10 G (Suporta 10 G o 1 G)	4xSFP+	-
PoE in/out	-	Out
Potencia máxima total PoE	-	100 W
Máximo de puertos con PoE concurrentes	-	8
USB (WAN)	Sí 1; USB 2.0	Sí 2; USB 2.0
Leds de gestión / estado	Sí	Sí
Leds LINK/ACT y estado	Sí	Sí
Puerto de consola	Mini USB / RJ45	RJ45
Panel LCD de navegación	Sí	No
Forma equipo / rack	Sobremesa / 1 RU	1 RU
Dimensiones (alto x ancho x profundo) (cm)	4,4 x 44,5 x 44,5	4,1 x 20 x 20
Peso	7,45 kg	1 kg

Ilustración 53: Características técnicas gateways piloto

[(1)(2)] En el Anexo XIV se puede encontrar las especificaciones completas de los gateways SD-WAN de Aruba

[(1)(2)] Los equipos 7210 y 7008 de Aruba puede funcionar como controladora WIFI, en el Anexo XVII se encuentra información complementaria

4.1.3.2. Software de gestión y administración del piloto SD-WAN

Desde Aruba, indican que *Aruba Central* es el software adecuado para realizar de forma simplificada el despliegue, gestión y optimización tanto de SD-WAN como de WLAN, LAN y VPN.

Para la realización de este piloto, Aruba además de contribuir con el préstamo del equipamiento de gateways, como veremos más adelante, también aportan una licencia en prueba de 90 días para poder llevar a cabo el despliegue, la gestión, administración y monitorización del piloto de red SD-WAN que se va a llevar a cabo.

Respecto a SD-WAN, *Aruba Central* ofrece la orquestación, gestión, monitorización y control sobre todos los gateways, ya sean virtuales, cabecera o de sucursal. Además, permite la administración centralizada de infraestructuras y enrutamiento del tráfico a través de MPLS, banda ancha y enlaces como LTE / 4G...

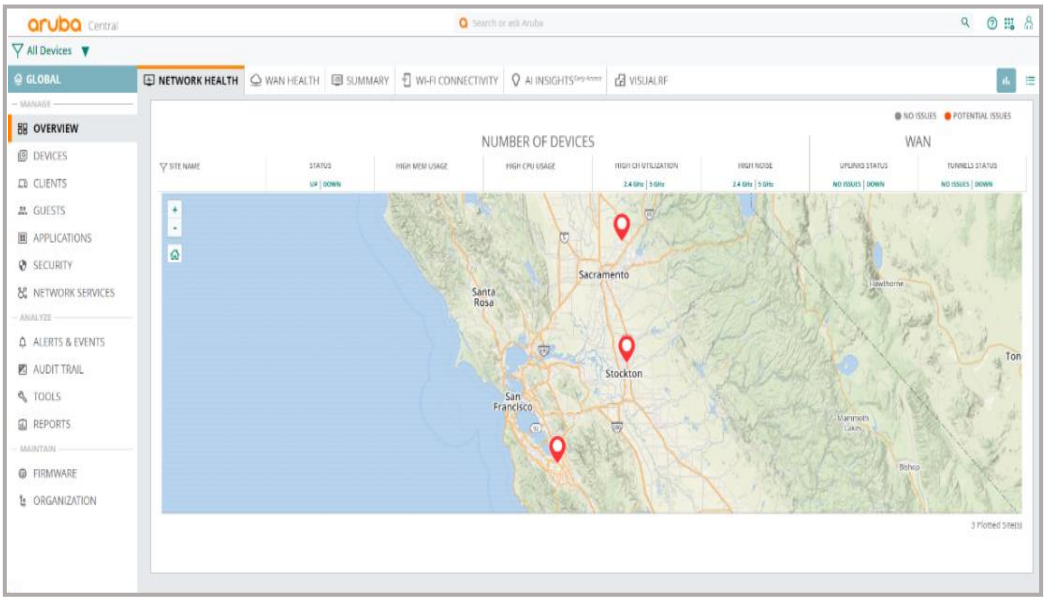


Ilustración 54: Panel inicial Aruba Central

Aruba Central también proporciona a SD-WAN:

- Vistas de topología integrada para la representación gráfica de las gateways y detalle por sitio
- Vistas de rendimiento de las aplicaciones para el estado del circuito WAN, disponibilidad del ancho de banda y estado del túnel para cada sitio
- Orquestación WAN para las preferencias de gestión del enrutamiento en sucursales y centro de datos
- Gestión del gateway virtual, que permiten extender directamente las políticas a las puertas de enlace alojadas en la nube pública
- Servicios VPN para AP remotos (IAP-VPN) y cliente VIA

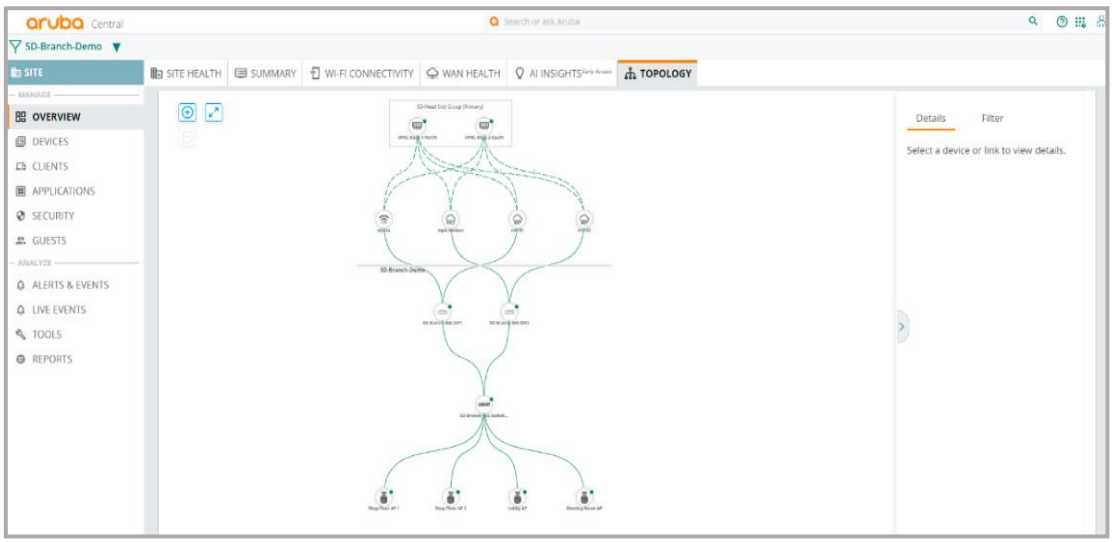


Ilustración 55: Topología de una SD-Branch en Aruba Central

Además, *Aruba Central* permite la existencia de flujos de trabajo para que los equipos TI accedan a la información de un equipo específico de configuración de políticas o circuitos, para mejorar la experiencia de usuario.

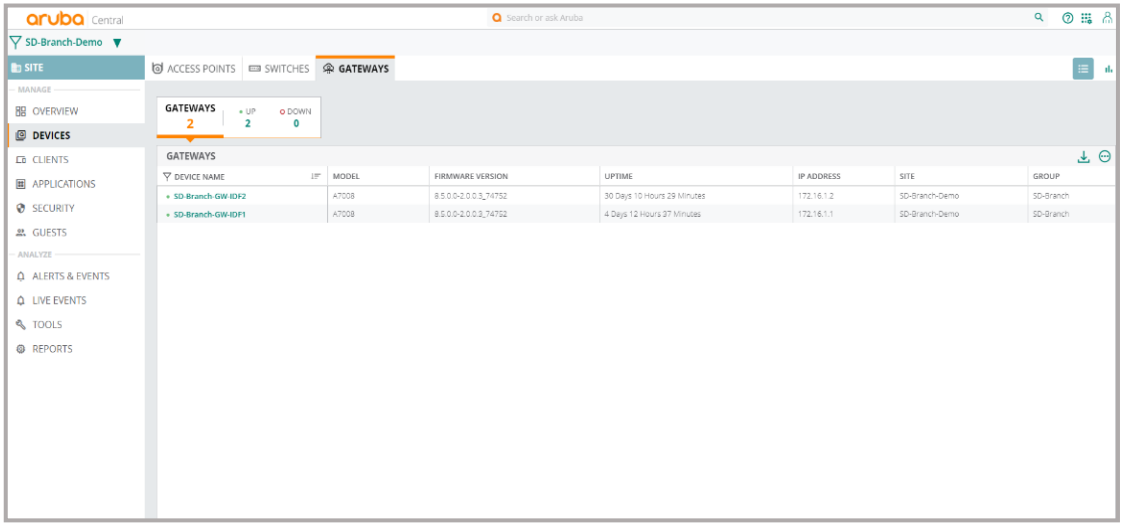


Ilustración 56: Información general de gateways SD-WAN en Aruba Central

Finalmente, para mejorar la seguridad contra un ataque, las gateways implementadas en modo SD-WAN agregan funciones de detección y prevención de intrusiones basada en identidad (IDS / IPS). Además, el panel de seguridad de *Aruba Central* proporciona a los equipos TI:

- Visibilidad de toda la red
- Métricas de amenazas multidimensionales
- Datos precisos de las amenazas
- Gestión del incidentes

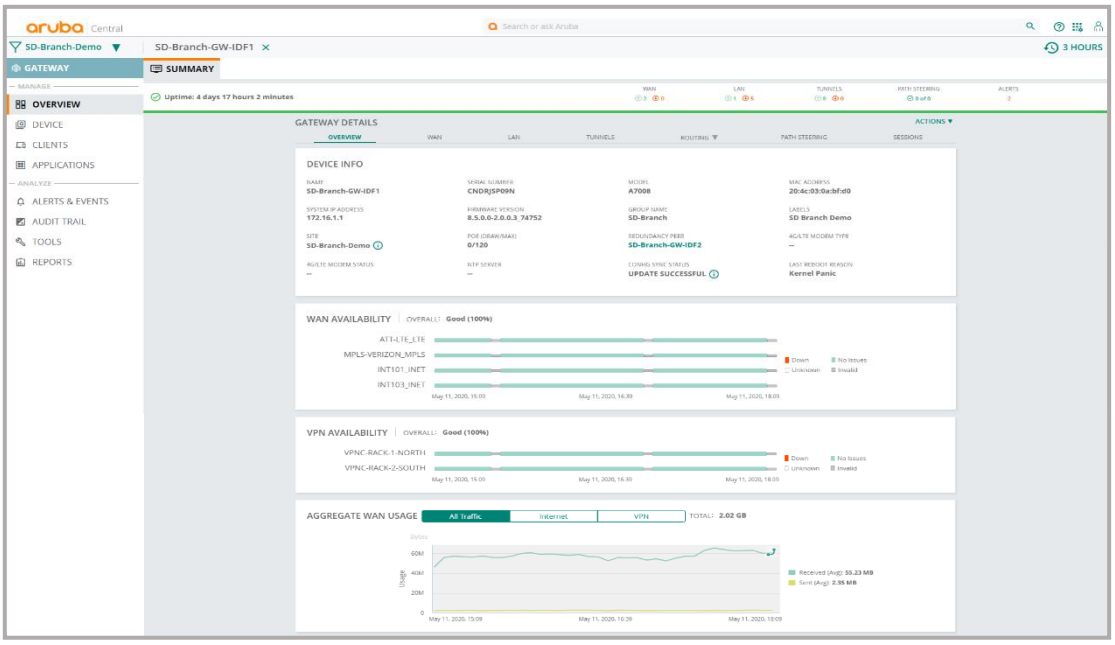


Ilustración 57: Detalles generales de un gateway SD-WAN en Aruba

En el Anexo XVI se puede encontrar las características completas del software Aruba Central.

4.1.3.3. Enlaces de conexión

El piloto de red SD-WAN se implementará con los siguientes enlaces:

Sucursal remota AL

- Enlace FTTH a Internet con un ancho de banda de 600 Mbps, contratado a proveedor de comunicaciones 1
- Enlace MPLS con el nodo principal CR con una ancho de banda de 200 Mbps para descarga de la sucursal y 100 Mbps de subida de la sucursal
- Enlace FTTH a Internet con una ancho de banda de 600 Mbps a proveedor de comunicaciones 2

Nodo principal CR

- Enlace FTTH a Internet con un ancho de banda de 600 Mbps, contratado a proveedor de comunicaciones
- Enlace MPLS con la sucursal remota AL con un ancho de banda de 100 Mbps desde la sucursal al nodo principal y 200 Mbps hacia la sucursal desde el nodo principal
- Conexión a Internet a través de RedIRIS a través de un interfaz de 1 Gbps

4.1.3.4. Diseño gráfico del piloto SD-WAN

En la siguiente imagen, se puede ver una aproximación real al piloto de red SD-WAN entre la sucursal remota AL y el nodo principal del campus CR.

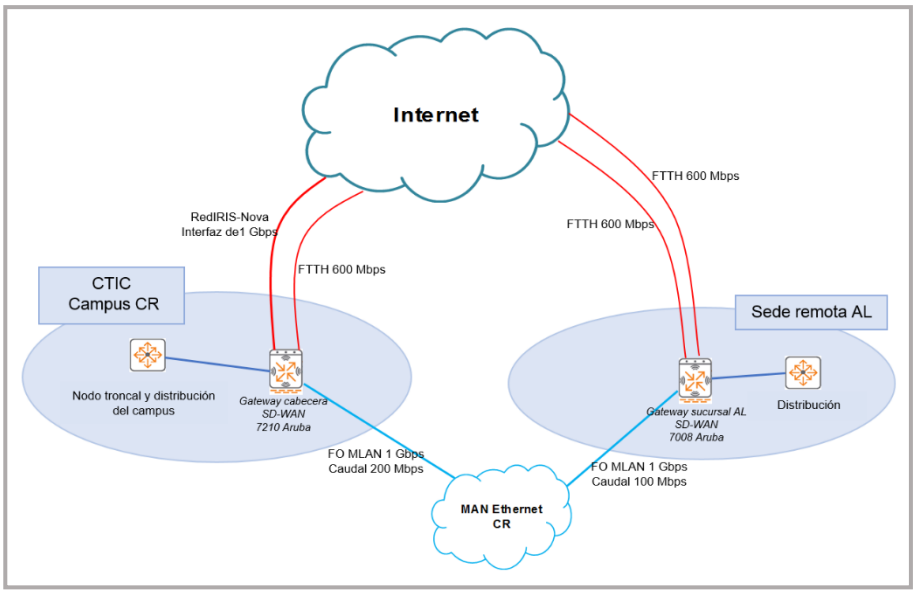


Ilustración 58: Diseño del piloto SD-WAN entre AL y CR

4.1.3.5. Costes del piloto SD-WAN

En este apartado, se exponen los costes que supondría la implantación del piloto de red SD-WAN, con las características descritas a lo largo del capítulo "4. Creación de piloto SD-WAN"

Coste del piloto SD-WAN entre la sucursal AL y el nodo principal CR			
Costes inversión	**Equipamiento**	**Descripción**	**Precio**
	Gateway cabecera	Aruba 7210	16.397 €
	Gateway sucursal	Aruba 7008	2.764 €
	Software gestión	Aruba Central	-
Costes recurrentes[1]	**Tipo**	**Descripción**	**Precio**
	Licenciamiento	Gateway Cabecera máx. capacidades	7.207 €
		Gateway Sucursal máx. capacidades	721 €
		Software de gestión: Aruba Central	-
	Mantenimiento	*Foundation* gateway cabecera	1.189 €
		Foundation gateway sucursal	183 €
	Enlaces	3 enlaces FTTH 600 Mbps	1.620 €
		Interfaz 1 Gbps RedIRIS nodo principal	-
		Enlace MPLS 200Mbps / 100Mbps	8.800 €
Costes puesta en producción[2]	**Tipo**	**Descripción**	**Precio**
	Formativas	20 horas dedicadas a la formación	300 €
	Técnicas	40 horas dedicadas a la construcción	800 €

Ilustración 59: Coste del piloto SD-WAN

[1] Los costes recurrentes están anualizados (el mantenimiento y licenciamiento está calculado para un contrato de 3 años. El software de gestión Aruba Central va incluido con el licenciamiento de los gateways. El presupuesto del equipo Aruba se encuentra en el Anexo XIII.

[2] El coste de puesta en producción ha sido calculado bajo una estimación de 15 horas en formación y 40 horas en la definición, especificación, diseño y construcción de un piloto tal y como se ha implementado en el apartado "4.1.4.3 Construcción del piloto SD-WAN". El coste de la hora de una persona de la institución, nivel A2 (al menos ingeniero técnico) es de 15 euros/hora brutos, calculados a partir del importe bruto de la nómina mensual de 30 días.

4.1.4. Construcción

4.1.4.1. Introducción

Durante la maduración de la idea para la realización de este trabajo, se mantuvieron distintos contactos con proveedores de equipos SD-WAN. Estos contactos encaminados a contar la idea de realizar un TFG, sobre la evolución de red en sucursales conectadas por enlaces tradicionales (tipo MPLS), hacia el modelo SD-WAN, tal como se ha desarrollado a lo largo de este trabajo.

Evidentemente, la adquisición del equipamiento necesario tiene unos costes importantes, tal como se ha expuesto a lo largo del apartados: "3.6. Costes" y "4.1.3.5 Costes del piloto SD-WAN" de este trabajo. Costes difícilmente de asumir, por un lado, por el autor de este trabajo y por otro lado, por la institución académica donde se instalaría el piloto, debido a que la adquisición de equipamiento de estas características se debe hacer por licitación pública.

Además, el equipamiento es necesario para implementar un piloto y no una infraestructura definitiva, al menos de momento. Por lo tanto, en uno de los contactos mantenidos con Aruba se les hizo la petición de dos equipos SD-WAN en préstamo para montar esta red SD-WAN, la petición realizada fue de un gateway 7008(*) para la sucursal y de un gateway 7210 para la cabecera.

Desde, Aruba accedieron al préstamo de dos gateways SD-WAN modelo 7008(*), debido a que de este modelo contaban con existencias para el préstamo y además admite la instalación como sucursal y cabecera.

A continuación, se pueden ver algunas imágenes reales del equipo:

Ilustración 60: Vistas del gateway Aruba 7008

(*) En el Anexo XIV se puede encontrar las especificaciones completas del equipo SD-WAN modelo 7008 de Aruba
(*) El equipo 7008 de Aruba puede funcionar como controladora WIFI, en el Anexo XVII se encuentra toda la información

Finalmente, se muestra en la parte superior de la siguiente ilustración la parte frontal donde se observan los leds de alimentación y de estado, así como un micro pulsador para resetear la configuración. En la parte inferior, se observa el conjunto de interfaces WAN/LAN, los dos puertos USB, el puerto de consola, la conexión para el alimentador externo y un punto de toma tierra.

Ilustración 61: Frontal y trasera Aruba 7008

4.1.4.2. Consideraciones actuales

Desgraciadamente, desde el 13 marzo de 2020 y debido al pandemia originada por el Covid-19, el estado español se encuentra en estado de alarma. Esta situación ha tenido las siguientes consecuencias, con respecto a este trabajo:

- La suspensión de la docencia en la institución universitaria objeto de estudio de este trabajo.
- El cierre de todas las dependencias de la institución.
- La suspensión del trabajo presencial de todos los trabajadores.

Desde el pasado 18 de mayo de 2020, las provincias restantes que quedaban en fase 0 de Castilla-La Mancha pasan a fase 1, entre ellas Ciudad Real que es la provincia donde está ubicada la sede central y la sucursal objeto de la implantación de este piloto de red SD-WAN.

Que actualmente en esta fase, la institución:

- Solo mantiene abiertas las bibliotecas con el personal mínimo suficiente, en horario reducido de 9:00 a 14:00, con cita previa y solo para préstamo de libros.
- Centros de investigación, solo para aquellas tareas de investigación solicitadas al vicerrectorado de investigación y por el tiempo necesario, para el personal investigador, técnicos de laboratorio y el ordenanza necesario.
- El registro, con solo una persona por registro.

Por todo lo anteriormente expuesto, es imposible acceder a las instalaciones de ambas ubicaciones para proceder al montaje e instalación del equipamiento.

Ante esta situación y dada la fecha actual de redacción de este apartado (27 de mayo de 2020) a falta de 11 días para entrega de esta memoria al tribunal. Se toma la decisión de seguir adelante con la construcción del piloto tal como se explica a continuación:

- Se expondrá como se va a implementar
- Se identificará cada uno de los parámetros necesarios para su configuración
- Se indicará paso a paso como se ha de hacer la configuración en cada uno de los equipos que intervienen en la infraestructura propia de SD-WAN, es decir, gateway cabecera y gateway sucursal.
- Se incluirán los comentarios necesarios de las decisiones tomadas en cada uno de los pasos
- Se acompañarán las imágenes de cada uno de los pasos necesarios sobre *Aruba Central* (software de gestión y orquestador), para llevar a cabo toda la configuración.

A partir, de aquí comienza el desarrollo de implementación del piloto SD-WAN entre el nodo principal del campus CR y la sucursal AL, actualmente conectada mediante un enlace MPLS, tal como se ha expuesto a lo largo de este trabajo y de forma específica como se explicado en el párrafo anterior .

4.1.4.3. Implementación del piloto SD-WAN

La implementación de este piloto se realizará en base a la ilustración 62 que podemos ver en la página siguiente, esta ilustración guiará todo el proceso durante toda la configuración que se va a realizar para llevar a cabo la implementación.

La institución universitaria y más concretamente su responsable de seguridad del área TIC indica el siguiente requisito para la implementación de esta infraestructura:

- Todo el tráfico se ha de reenviar a través de túneles VPN al nodo central, ya sea tráfico destinado a la red corporativa, otras sucursales o Internet, debido a las políticas actuales de la organización, entre ellas, es que todo el tráfico (incluido el de Internet) sea inspeccionado por los firewalls perimetrales de la organización.

Así pues, para cumplir este requisito, la implementación se realizará entre cabecera (VPNC) y sucursal (BGW, Branch gateway) mediante túneles completos.

En la página siguiente podemos ver de manera completa, las características necesarias para llevar a cabo la configuración del piloto SD-WAN.

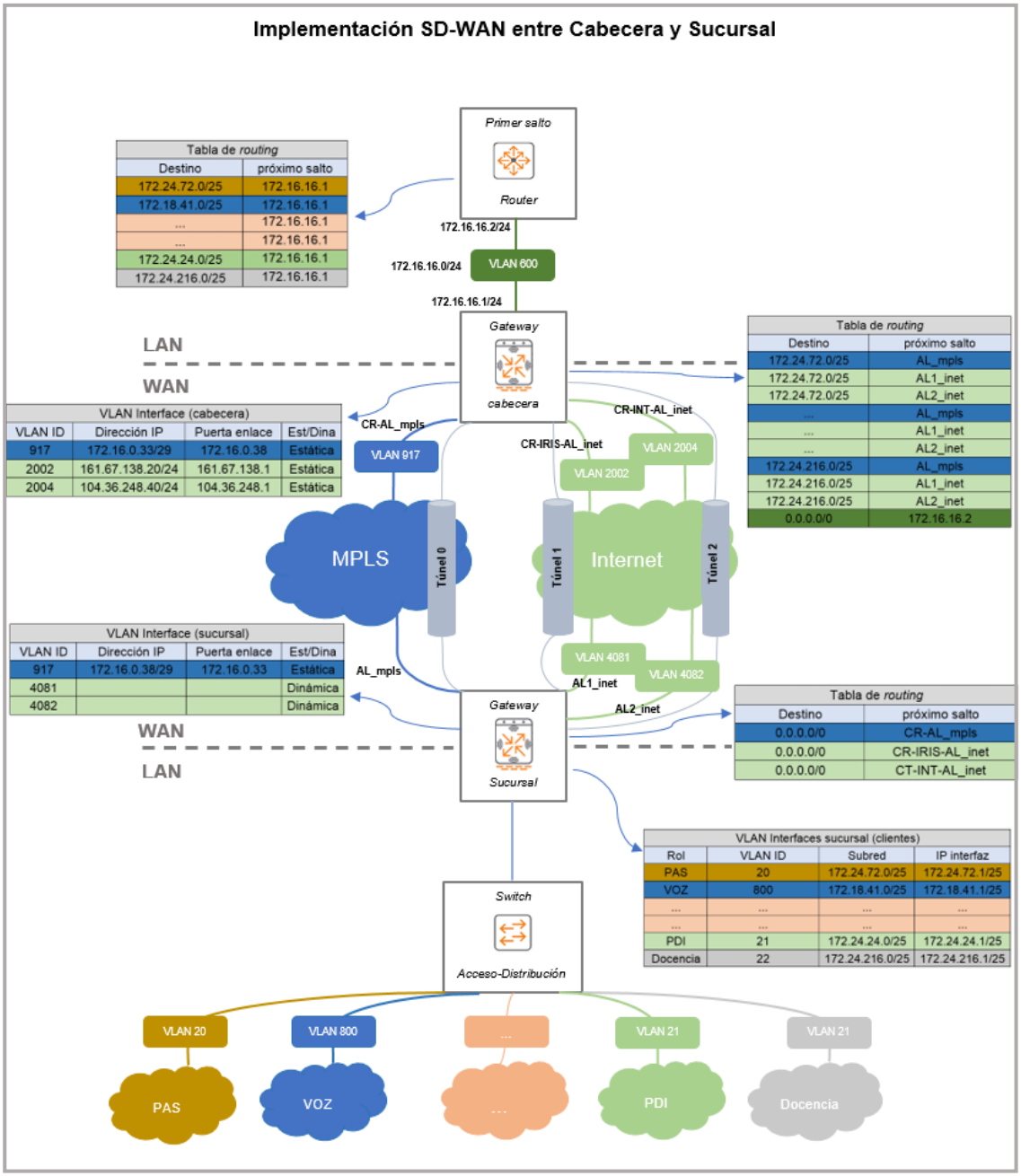


Ilustración 62: Implementación real piloto SD-WAN

En primer lugar, los gateways SD-WAN: cabecera (VPNC) y sucursal (BGW) deben tener una IP del sistema. De esta manera, cada equipo SD-WAN utiliza una interfaz VLAN como IP del sistema. Así, cada gateway Aruba usa esta interfaz para comunicarse con servicios de red, como: RADIUS, syslog, TACACS+ y SNMP. Por lo tanto, hasta que la interfaz VLAN asignada no esté activa y operativa el gateway SD-WAN no se inicializará completamente.

VLAN Interface (IP del sistema)			
Equipo	Denominación	VLAN ID	IP
Cabecera	VPNC-Control	3701	172.17.175.2/24
Sucursal	BGW-Control	3702	172.17.175.3/24

Ilustración 63: Tabla interfaces VLAN de IP del sistema

El procedimiento de creación de la IP del sistema es el siguiente:

- Se selecciona el equipo sobre el que se va a realizar la configuración
- Se crea la interfaz VLAN con los datos de la tabla anterior
- Se selecciona esa interfaz VLAN como IP del sistema.

A continuación se puede ver el proceso en *Aruba Central* de cada uno de los pasos anteriores para el equipo cabecera. **El proceso para el otro equipo es repetir los mismos pasos.**

Seleccionar el equipo

Conectado el equipo a la corriente eléctrica y conectándolo a la red con salida a Internet, el equipo se registrará de manera automática en Aruba Central y preguntará por un nombre de equipo y la zona de ubicación. Después, seleccionaremos tal como se puede ver en la siguiente imagen.

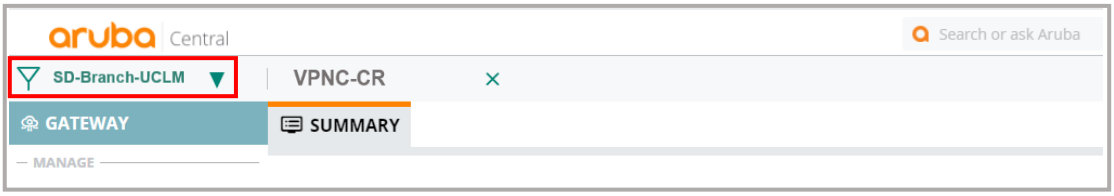


Ilustración 64: Seleccionar equipo SD-WAN

Crear la interfaz VLAN

Para crear la interfaz de VLAN, seleccionamos **DEVICE-LAN-VLANs** y presionamos sobre el icono + para crearla.

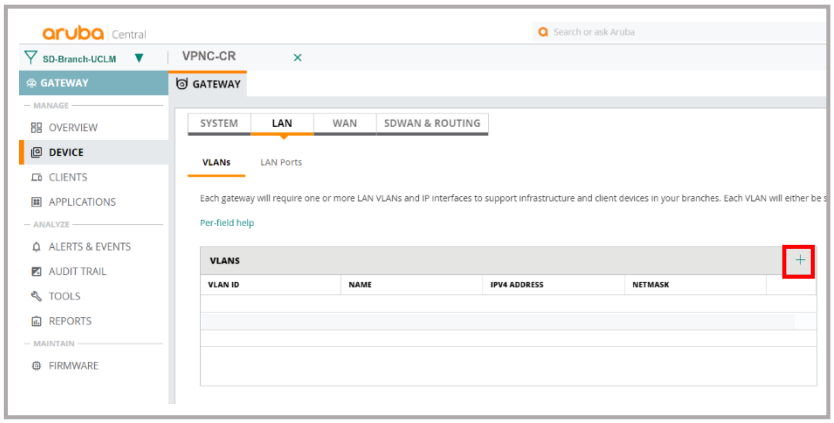


Ilustración 65: Crear Interfaz VLAN - IP sistema

Posteriormente, rellenamos los datos y procedemos a guardar la configuración.

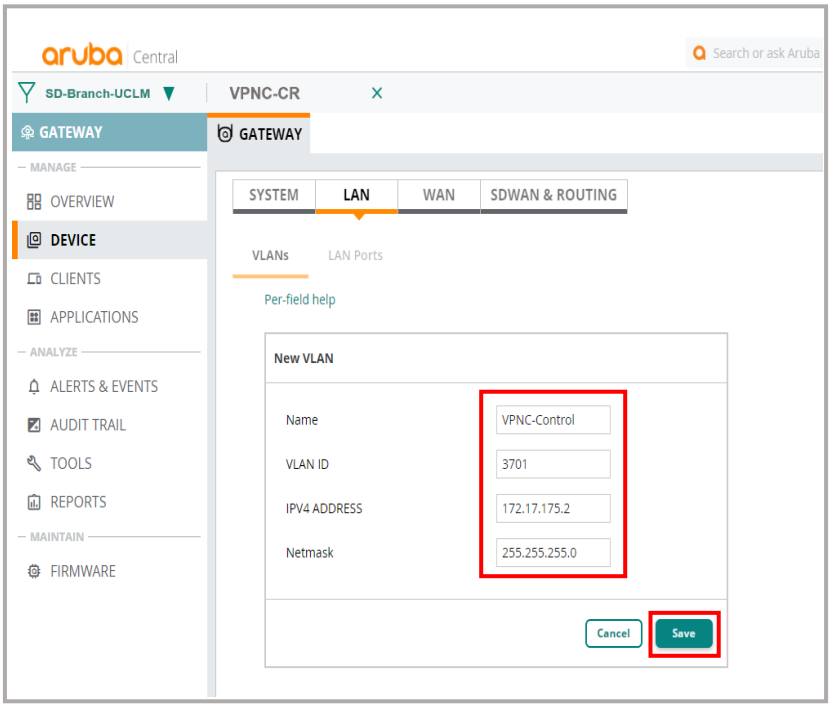


Ilustración 66:Introducir datos interfaz VLAN - IP sistema

Seleccionar la interfaz VLAN como IP del sistema

Para realizar este paso es necesario ir a **DEVICE-SYSTEM-System IP** y desplegar, para hacer la selección de la interfaz VLAN correcta.

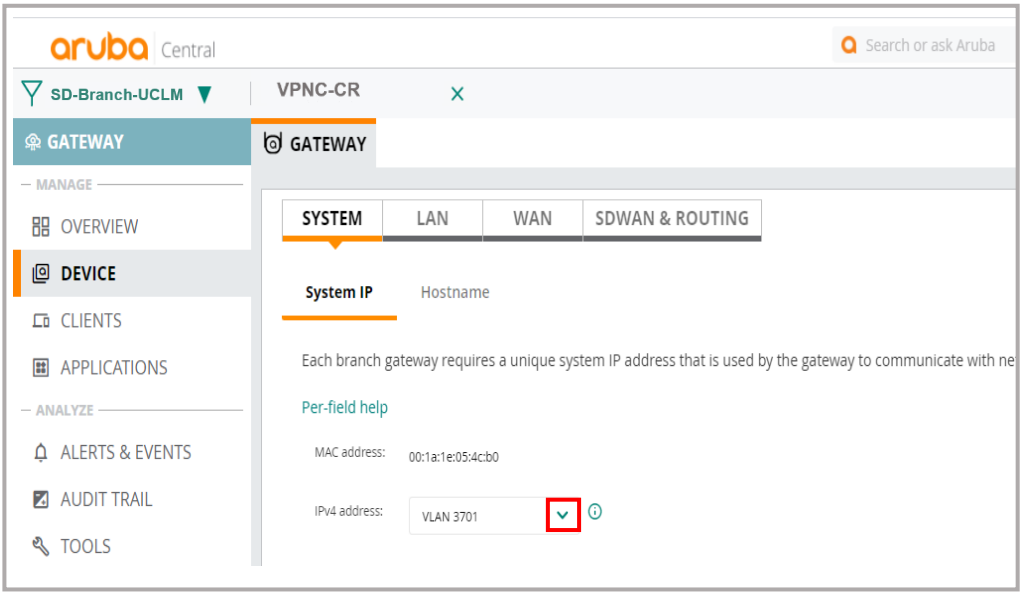


Ilustración 67: Seleccionar interfaz VLAN como IP del sistema

La configuración de IP del sistema quedaría así completada en el equipo.

Configuración de la parte WAN del piloto

El siguiente paso es crear las interfaces VLAN tanto para la sucursal como para la cabecera.

- En la cabecera se crearán las interfaces VLAN para terminar los túneles VPN, que en este caso serán las pertenecientes a las VLAN 917, 2002 y 2003. También se creará la interfaz VLAN para reenviar el tráfico de superposición en este caso VLAN 600, esta última se realizará en la parte LAN.

- En el caso de la sucursal se crearán las interfaces VLAN para iniciar los túneles VPN (WAN), que en este caso son VLAN 917, 4081 y 4082. También se crearán las interfaces VLAN para admitir los clientes que en este caso serán las VLAN 1, 5, 9, 10,15, 20, 21, 22, 23, 26, 27, 68, 69, 450, 500 y 800. Las VLAN para admitir clientes se realizarán en la parte LAN.

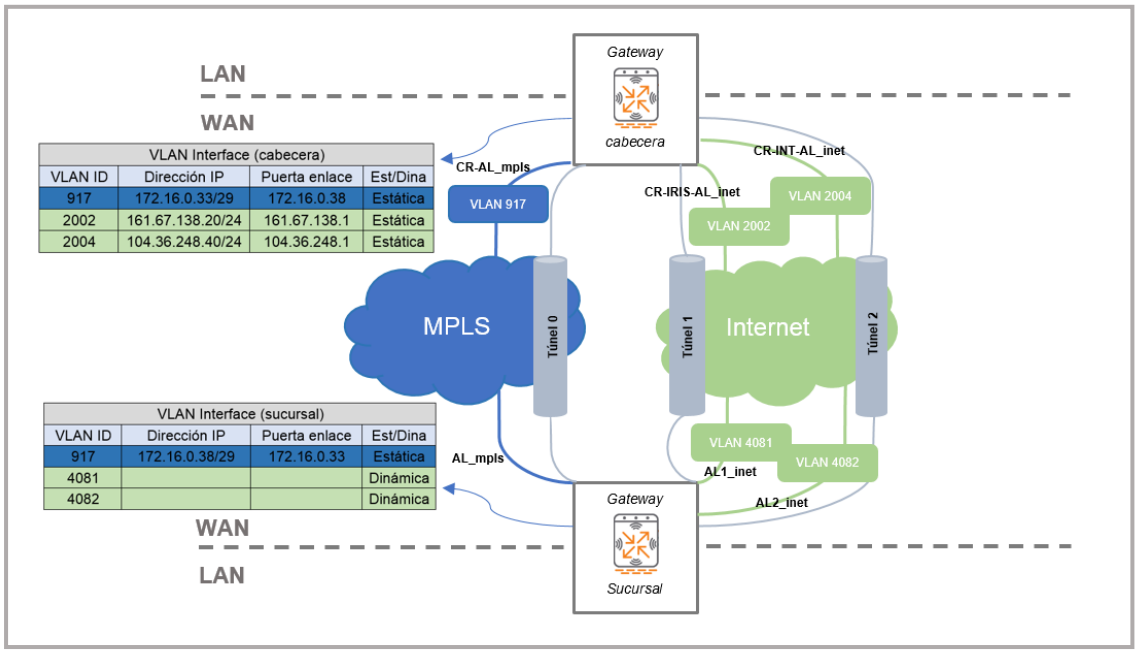


Ilustración 68: Sección WAN piloto SD-WAN

Se comenzará creando las interfaces VLAN para iniciar los túneles VPN en la sucursal, los datos son los siguientes:

VLAN Interface (sucursal)						
VLAN ID	Dirección IP	Puerta enlace	Puerto	Est/Dina	Tipo	Nombre
917	172.16.0.38/29	172.16.0.33	GE-0/0/2	Estática	MPLS	AL
4081			GE-0/0/3	Dinámica	Internet	AL1
4082			GE-0/0/4	Dinámica	Internet	AL2

Ilustración 69: Tabla de las interfaces VLAN (WAN) de sucursal

Cabe indicar, que en el caso de la sucursal las direcciones IP de las líneas internet se las dará el router del proveedor de forma dinámica, de ahí que carezca la tabla de dicha información, al no ser necesaria su configuración manual.

Los pasos para crear las interfaces VLAN de inicio de los túneles son los siguientes:

- Seleccionar el equipo sobre el que se va a realizar la configuración
- Crear cada una de las interfaces VLAN, con los datos de la tabla anterior, teniendo en cuenta que el sistema añadirá al nombre el siguiente sufijo "_mpls" o "_inet" en función si el enlace es MPLS o fibra Internet respectivamente
- Configurar el próximo salto para aquellos enlaces WAN cuyo direccionamiento es estático

En este caso se obvia como se selecciona el equipo, debido a que ya se explicó anteriormente durante la creación de la IP del sistema.

Crear la interfaz VLAN para iniciar los túneles

Para crear la interfaz de VLAN, seleccionamos **DEVICE-WAN-WAN Details** y presionamos sobre el icono + para crearla.

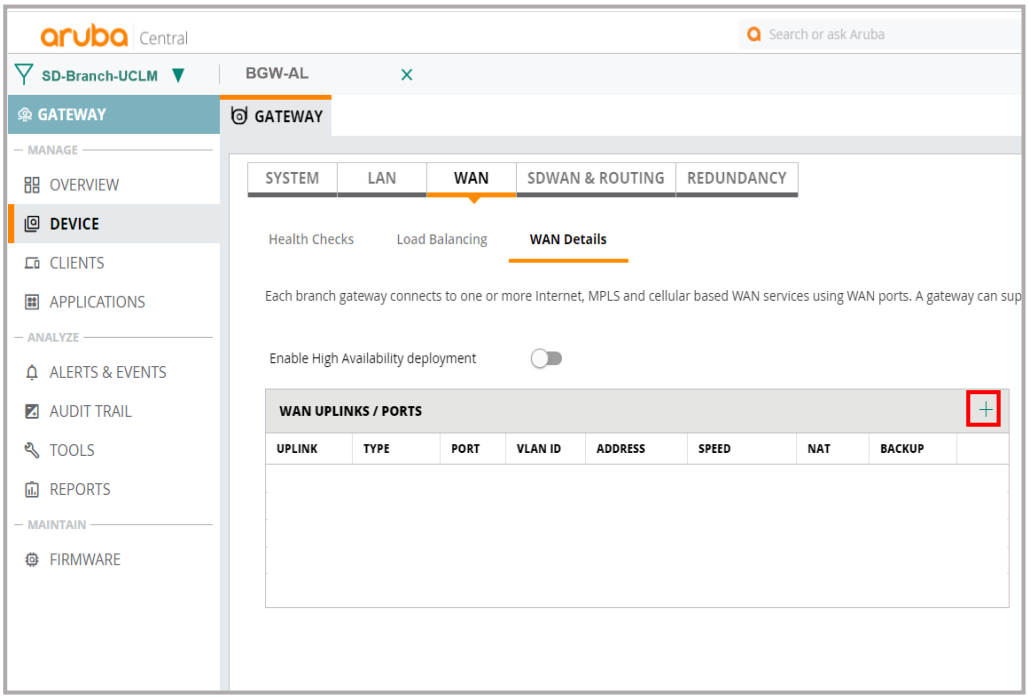


Ilustración 70: Crear interfaces VLAN (WAN) de sucursal

Se completa la información para cada una de las VLAN interfaces de WAN, teniendo en cuenta que la velocidad de los enlaces de Internet debe ser la aproximada a una garantía real.

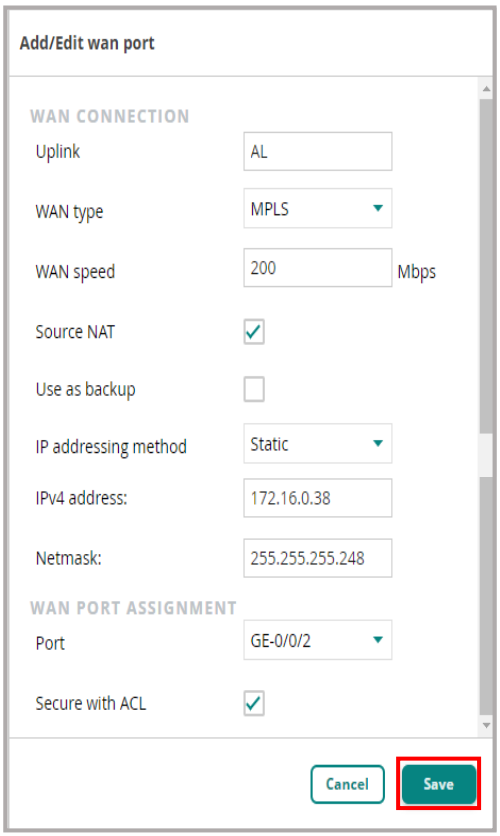


Ilustración 71: Introducir datos interfaz VLAN - MPLS

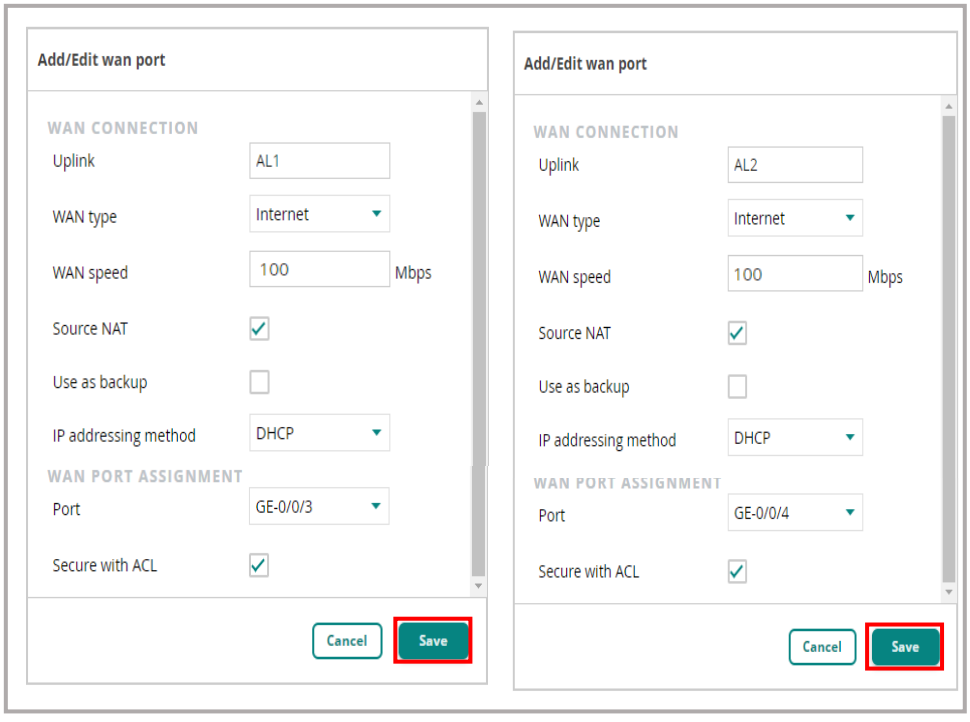


Ilustración 72: Introducir datos interfaz VLAN de enlaces de Internet

Configurar el próximo salto para MPLS

Seleccionamos **DEVICE-SDWAN & ROUTING-Static Routing** y presionamos sobre el icono + para configurarlo.

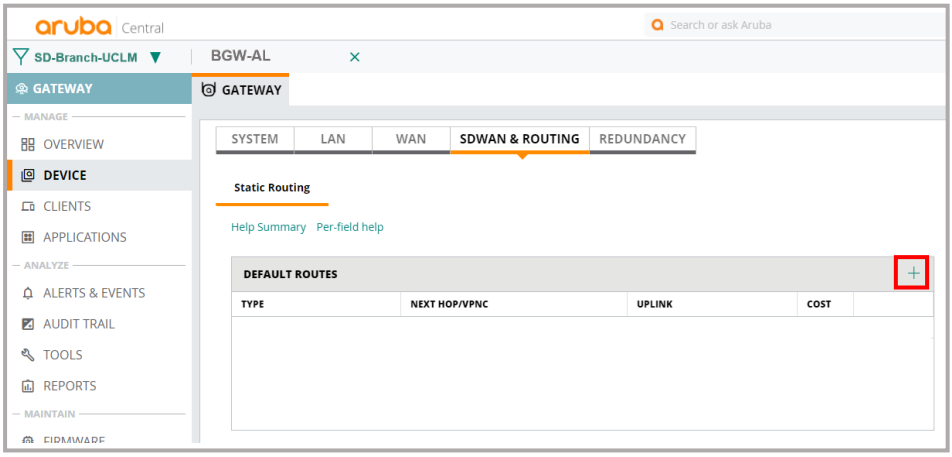


Ilustración 73: Configurar próximo salto MPLS sucursal

Se introduce la puerta de enlace para MPLS

Ilustración 74: Introducción datos próximo salto MPLS sucursal

Ahora se crearán las interfaces VLAN (WAN) para finalizar los túneles VPN en la cabecera, los datos son los siguientes:

VLAN Interface (cabecera)						
VLAN ID	Dirección IP	Puerta enlace	Puerto	Est/Dina	Tipo	Nombre
917	172.16.0.33/29	172.16.0.38	GE-0/0/2	Estática	MPLS	CR-AL
2002	161.67.138.20/24	161.67.138.1	GE-0/0/3	Estática	Internet	CR-IRIS-AL
2004	104.36.248.40/24	104.36.248.1	GE-0/0/4	Estática	Internet	CR-INT-AL

Ilustración 75: Tabla de las interfaces VLAN (WAN) de cabecera

En primer lugar, hay que seleccionar el equipo cabecera y después:

Crear la interfaz VLAN para iniciar los túneles

Para crear la interfaz de VLAN, seleccionamos **DEVICE-WAN-VLANs** de la misma manera que se hizo con la sucursal anteriormente y completamos como sigue, teniendo en cuenta que en este caso las tres conexiones obtienen direccionamiento de manera estática:

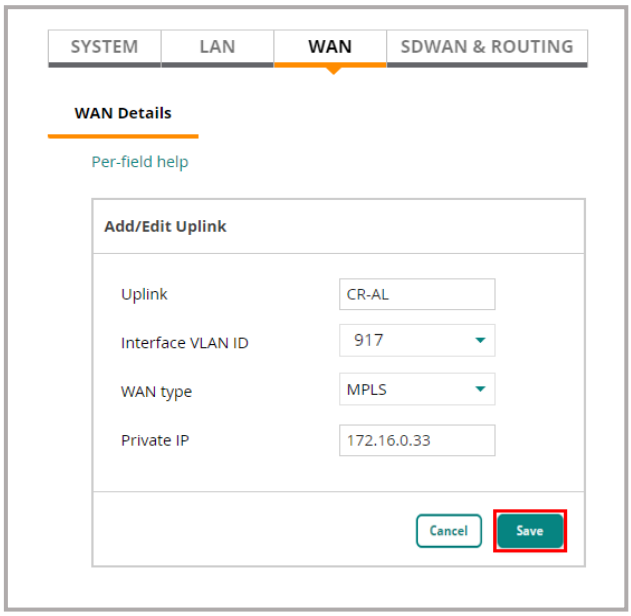


Ilustración 76: Introducción datos interface VLAN MPLS cabecera

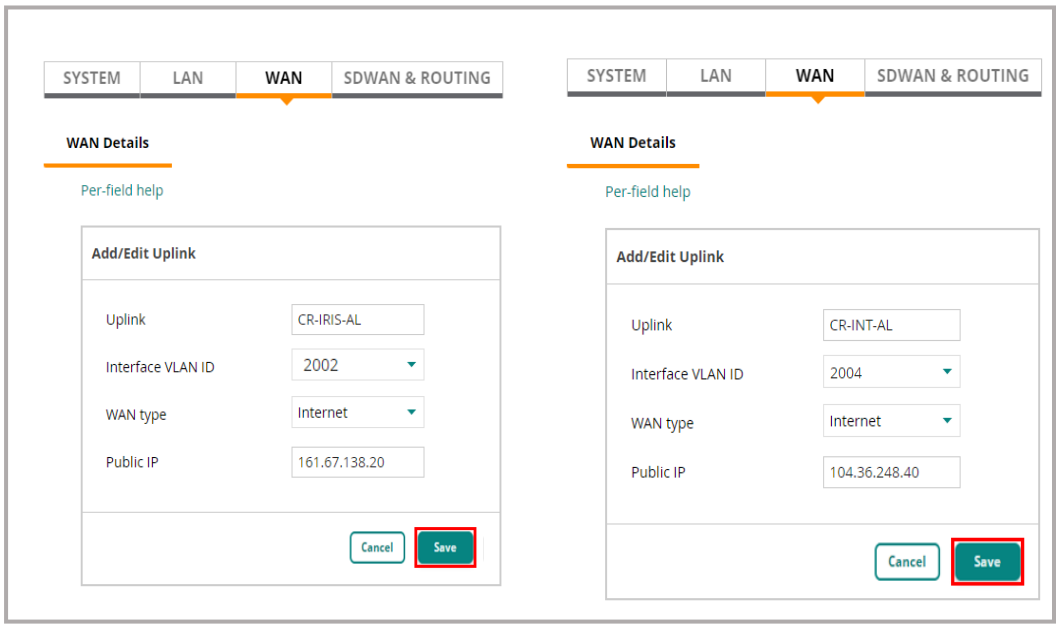


Ilustración 77: Introducción datos interfaces VLAN Internet cabecera

Configurar el próximo salto para todas las conexiones WAN de cabecera

Seleccionamos **DEVICE-SDWAN & ROUTING-Static Routing** y presionamos sobre el icono + para configurarlo.

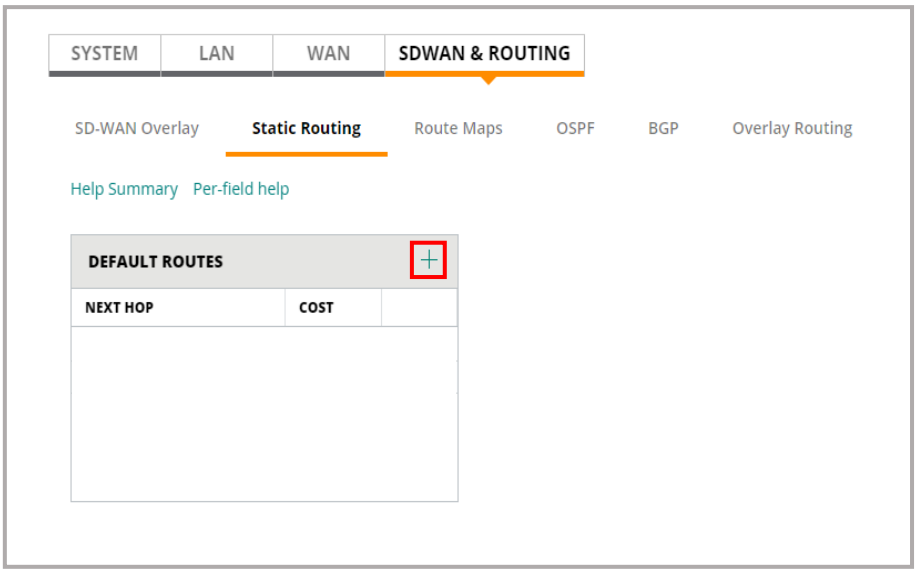


Ilustración 78: Selección próximo salto en cabecera para WAN estáticas

Una vez completado el campo, se repetirá hasta completar todos los próximos saltos.

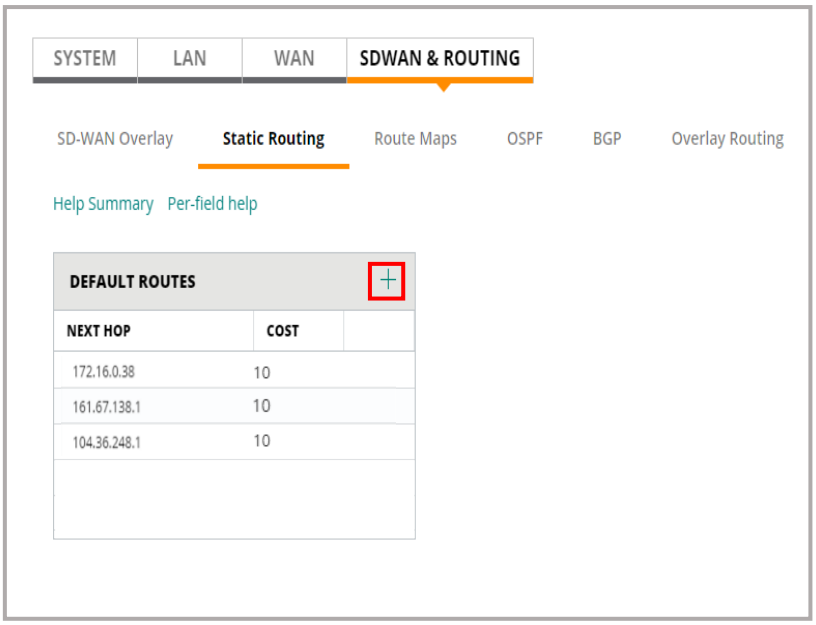


Ilustración 79: Introducir datos de próximo salto Interfaces VLAN cabecera

Hasta aquí, la configuración de la parte WAN de la implementación del piloto de la ilustración 62 de este trabajo. Más adelante, se explicará la configuración necesaria para el intercambio de rutas entre cabecera y sucursal, respecto a los túneles de superposición SD-WAN que se han de crear sobre los enlaces WAN que los interconecta.

A continuación, se configurará la parte LAN de la sucursal.

Configuración de la parte LAN en la sucursal

Para configurar la parte LAN de la sucursal, se tienen que configurar tantas interfaces VLAN como roles de clientes haya.

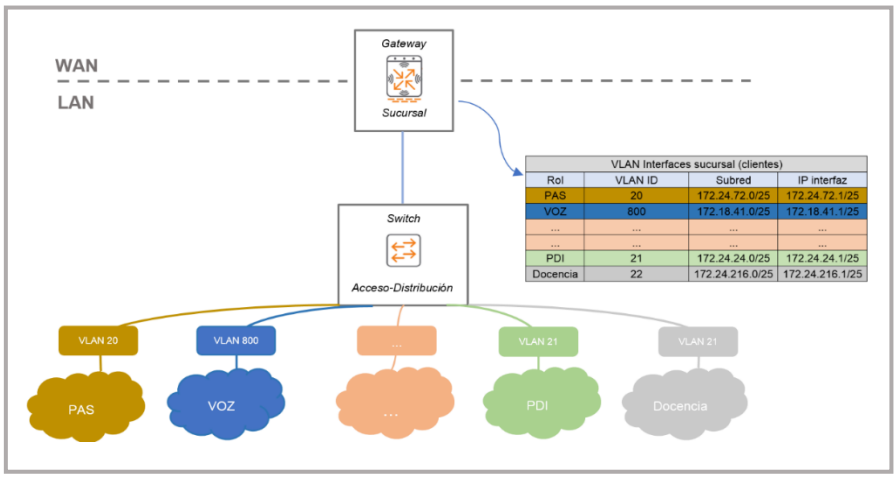


Ilustración 80: Sección LAN de la sucursal SD-WAN

Los pasos que hay que llevar a cabo son los siguientes:

- Disponer de un listado completo de las interfaces VLAN que hay que configurar en la parte LAN de la sucursal
- Seleccionar el equipo sucursal en *Aruba Central*
- Crear cada una de las interfaces VLAN

Disponer del listado completo de las interfaces VLAN

La institución dispone de alrededor de 20 VLANs diferentes en la sucursal, aunque actualmente son 16 las que están operativas. A continuación, se pueden ver cada una de las VLANs con sus datos más relevantes.

VLAN sucursal				
ID	**Nombre**	**Subred**	**IP interfaz**	**Descripción**
1	DEFAULT_VLAN	172.17.164.0/24	172.17.164.1/24	Gestión
5	Domo-cam-al	172.20.163.0/26	172.20.163.1/26	Domótica (cámaras...)
9	EDI-cam-alm	172.20.164.0/24	172.20.164.1/24	Edificios (control temperatura...)
10	PIU-alm-cr	172.19.32.128/26	172.19.32.129/26	Punto de información universitaria
15	PTR-alm-cr	172.20.167.0/27	172.20.167.1/27	Equipos de impresión
20	PAS-alm-cr	172.24.72.0/25	172.24.72.1/25	Personal de administración y servicios
21	PDI-alm-cr	172.24.24.0/25	172.24.24.1/25	Personal docente e investigador
22	DOC-alm-cr	172.24.108.0/25	172.24.108.1/25	Aulas de docencia
23	INV-alm-cr	172.24.216.128/25	172.24.216.129/25	Investigación
26	SCM-alm-cr	172.20.36.0/24	172.20.36.1/24	Servidores
27	CUA-alm-cr	172.19.38.0/24	172.19.38.1/24	Equipos en cuarentena
68	VCpri-alm-cr	172.18.59.192/26	172.18.59.193/26	Videoconferencia principal
69	VCinv-alm-cr	172.19.32.192/26	172.19.32.193/26	Videoconferencia invitados
450	DOC-lib-alm-cr	172.24.216.128/26	172.24.216.129/26	Aulas de libre uso
500	WIFI-gesycontrol-alm	172.17.174.32/27	172.17.174.33/27	Gestión y control WIFI
800	VOZ-alm-cr	172.18.41.0/25	172.18.41.1/25	Voz

Ilustración 81: Listado VLAN sucursal en LAN

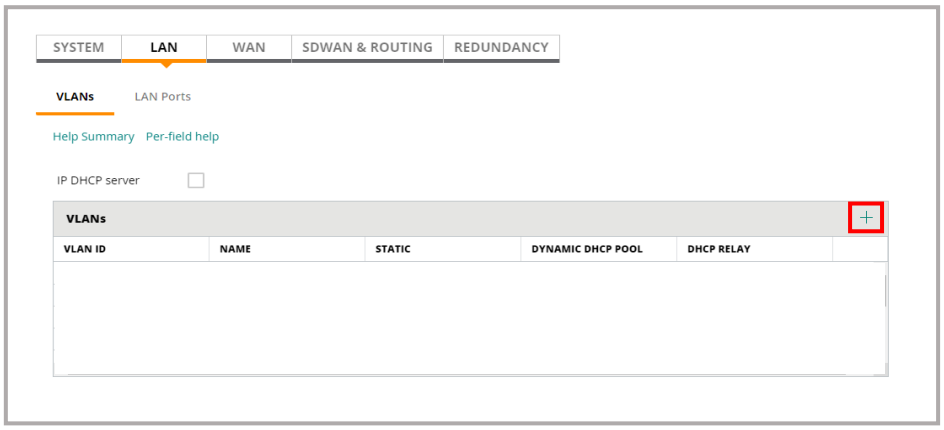
Seleccionar el equipo de la sucursal

Desde el nombre de nuestro piloto SD-WAN se selecciona el equipo de la sucursal.

Ilustración 82: Selección equipo sucursal en Aruba Central

Crear las interfaces VLAN de la LAN en equipo de la sucursal

Para crear una interfaz de VLAN, seleccionamos **DEVICE-LAN-VLANs** y presionamos sobre el icono + para crearla.



Se introducen los datos para cada VLAN de la tabla de la ilustración 81 de la página anterior. Como ejemplo guía, se hará con la VLAN 20 perteneciente al colectivo PAS. Hay que en este piloto, el equipo SD-WAN de la sucursal no actuará como DHCP, debido a que será el servidor de la institución quien lo haga, para ello se habilitará la opción "*Enable DHCP relay*".

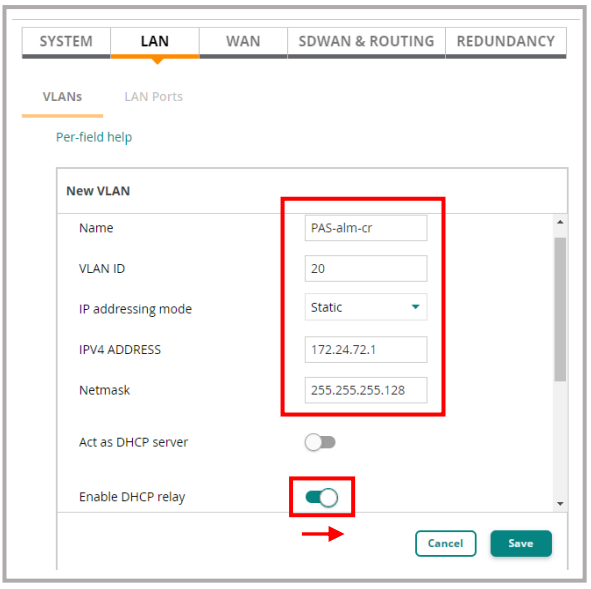


Ilustración 84: Introducir datos interfaz VLAN sucursal

Posteriormente, se presiona el signo +, para añadir los servidores DHCP de la organización, en este caso serán dos. Por último, hay que salvar la configuración introducida.

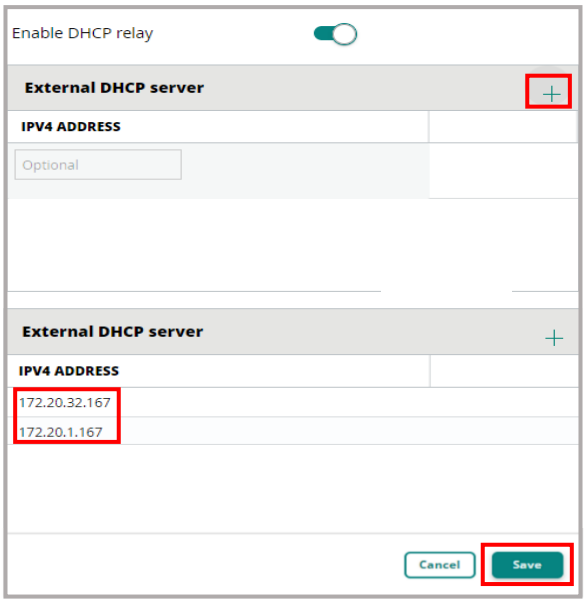


Ilustración 85: Configurar DHCP para subredes de VLAN sucursal

Este proceso realizado para la VLAN 20 de PAS hay que realizarla de forma individual para cada una de las 15 VLANs restantes, incluidas en la tabla de la ilustración 81.

Para terminar, se configurará el puerto GE0/0/0 del equipo SD-WAN para que deje pasar todas las VLAN configuradas, en este caso lo configuraremos en modo *trunk*, aunque esta no es la única configuración válida admitida en esta parte. Además, este puerto será conectado al switch que realiza la distribución a otros conmutadores instalados en el edificio para dar red a los distintos equipos clientes de la sucursal.

Para configurar el puerto GE0/0/0, seleccionamos **DEVICE-LAN-LAN Port** y presionamos sobre el icono +.

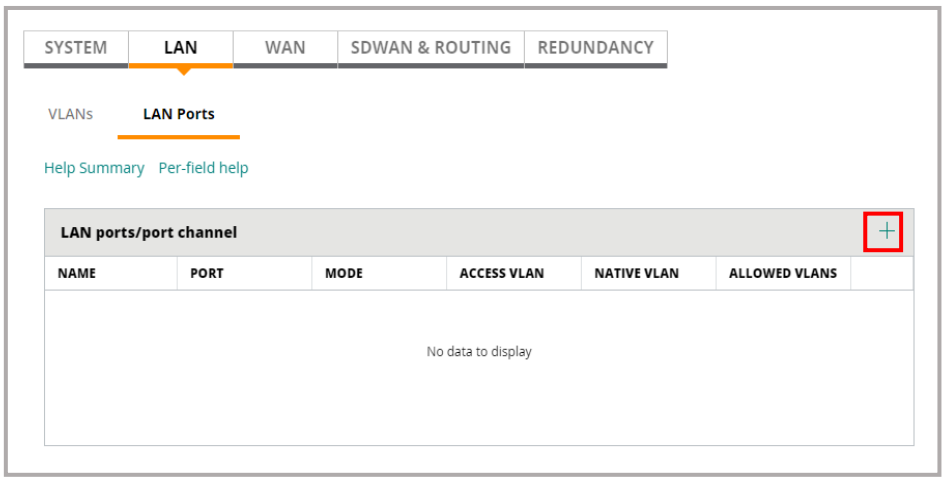


Ilustración 86: Configuración puerto para acceso LAN (I)

Se le dará un nombre, se escogerá el puerto, el modo si es acceso o *trunk* y los campos adicionales si fueran necesarios.

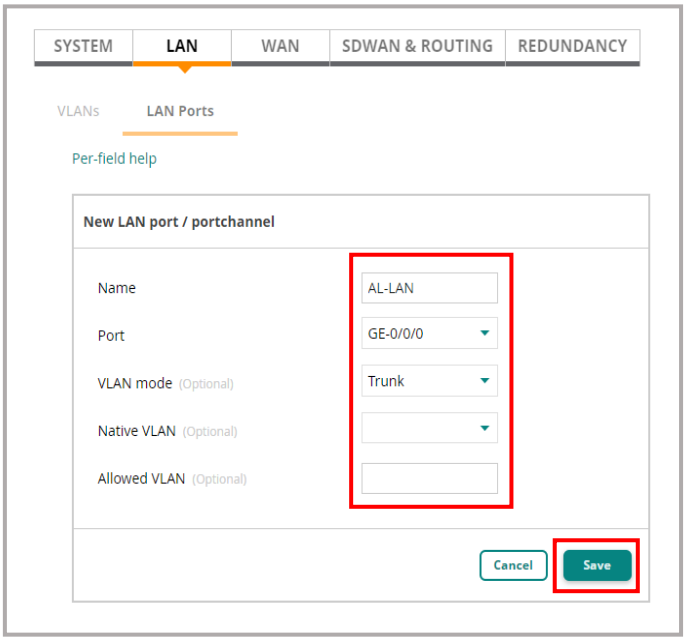


Ilustración 87:Configuración puerto para acceso LAN (II)

Configuración de la parte LAN en la cabecera

Para configurar la parte LAN de la sucursal, en este caso se configurará la interfaz VLAN 600, tal como se puede ver en la siguiente imagen.

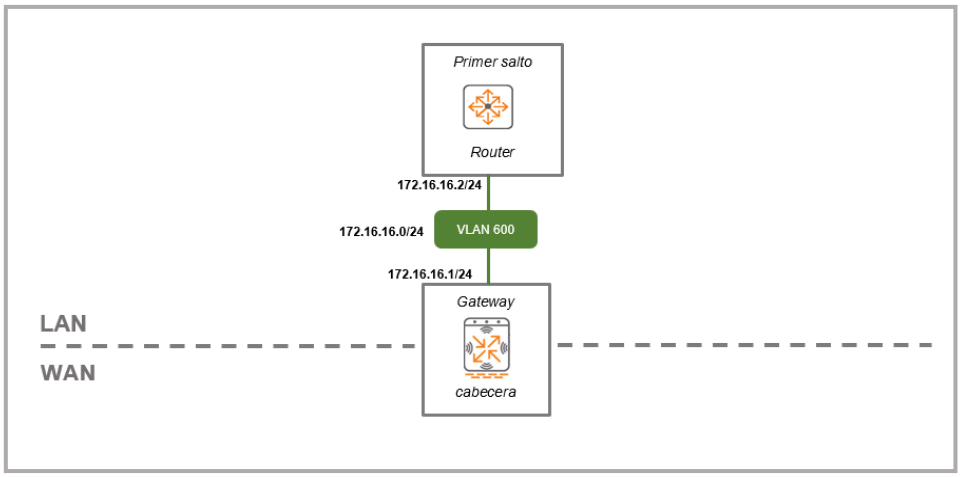


Ilustración 88: Sección LAN de la cabecera SD-WAN

Los pasos que hay que llevar a cabo son los mismos que los realizados para la parte LAN de la sucursal. Así pues, una vez seleccionado el equipo cabecera y desde **DEVICE-LAN-VLANs**

A continuación se puede ver el proceso de configuración de forma simplificada:

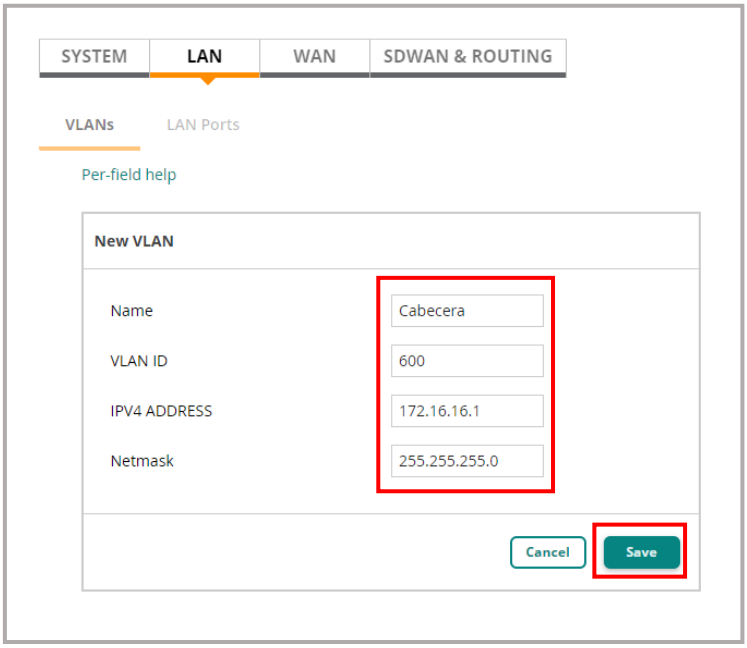


Ilustración 89: Introducir datos interfaz VLAN cabecera LAN

Para terminar, se configurará el puerto GE0/0/0 del equipo SD-WAN cabecera en modo *trunk*, sin más, no siendo la única opción válida . Además, este puerto será conectado al router del nodo principal. Para configurar el puerto GE0/0/0 se selecciona **DEVICE-LAN-LAN Port** y se presiona sobre el icono +. Posteriormente, se le dará un nombre, se escogerá el puerto y si es acceso o *trunk*, junto con los campos adicionales si fueran necesarios.

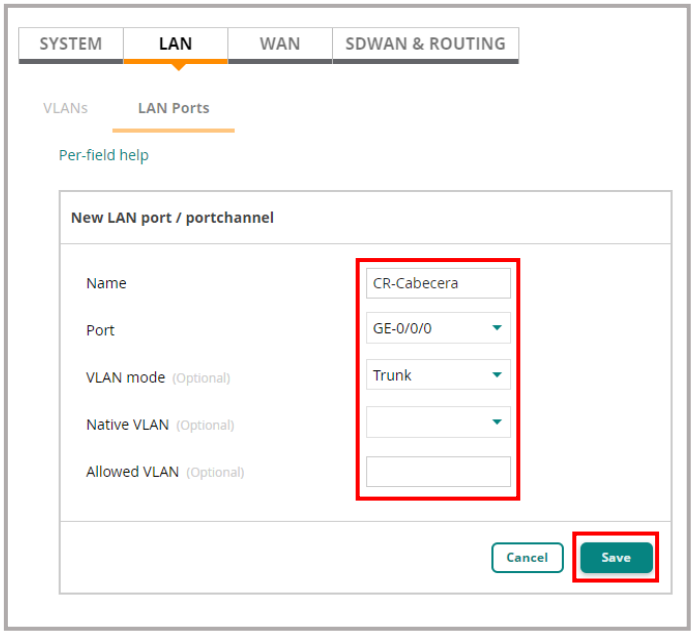


Ilustración 90: Configuración puerto LAN cabecera

***Routing* del piloto SD-WAN**

Para terminar de configurar y esté operativa la red SDWAN implementada faltan los siguientes pasos:

- Realizar, respecto a la parte WAN, la configuración para la creación de los túneles entre sucursal y cabecera. De esta manera, la solución SD-Branch de Aruba aprovechará los servicios WAN que interconectan cabecera y sucursal para establecer los túneles VPN que encapsulan y reenvían el tráfico corporativo. Así, cada servicio WAN se conoce como red subyacente y los túneles VPN forman la red superpuesta. La accesibilidad y el reenvío a través de las redes se logra utilizando el enrutamiento en las puertas de enlace.
- Realizado el paso anterior, ya se tendrá la red superpuesta y será necesario realizar el enrutamiento para proporcionar la accesibilidad. Por un lado, la cabecera requiere rutas para saber que redes son accesibles a través de la sucursal y por otro lado, la sucursal requiere rutas para saber qué redes corporativas son accesibles a través de la cabecera.

Tal como vimos en la configuración WAN, tanto de la sucursal y cabecera, se realizó la configuración del próximo salto en la red subyacente. Para realizar el enrutamiento de superposición entre los equipos SD-WAN de sucursal y cabecera, se puede optar por hacerlo de dos formas: manual y automática

De forma manual, donde se configurará en la sucursal las subredes que anunciará, que serán aquellas VLANs que queramos conectar automáticamente con el equipo cabecera (imagen de la izquierda) y en la cabecera la conexión con la lista de sucursales (imagen de la derecha).

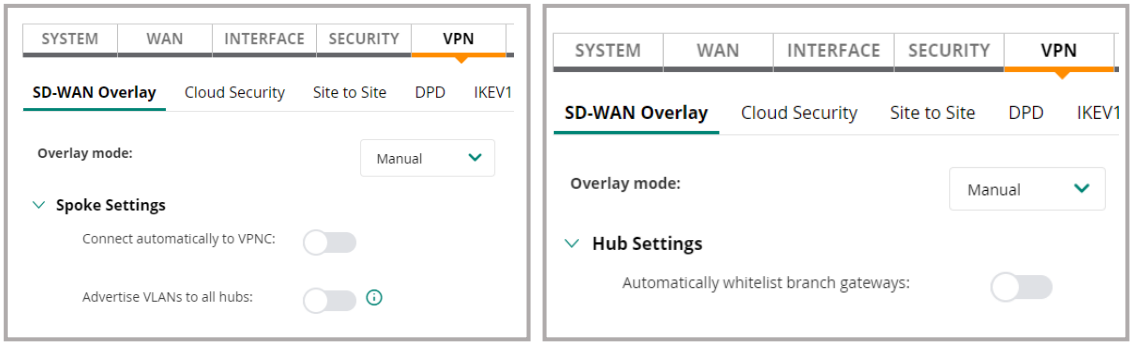


Ilustración 91: Configuración manual de anuncio de redes

De forma automática, opción elegida para realizar este piloto, ya que se realizará mediante un conexión de servicio centralizado del orquestador de rutas que incorpora *Aruba Central*. De esta manera, se hace posible el intercambio de rutas entre sitios sobre los túneles de superposición SD-WAN de forma automática, los túneles que se crearán son:

- Un túnel sobre la MPLS entre cabecera y sucursal

- Dos túneles sobre los enlaces de Internet, dos a dos, entre cabecera y sucursal. En este caso al haber más de una posibilidad lo realizará según disponibilidad o por orden de configuración

Así pues, activaremos tanto en el equipo cabecera como en la sucursal "*Overlay Orchestrator Peering*" y para ello, una vez seleccionado el equipo se irá a: **DEVICE-SDWAN & ROUTING- SD-WAN Overlay** y se deslizará hacia la derecha la selección, tal como podemos ver en la siguiente imagen.

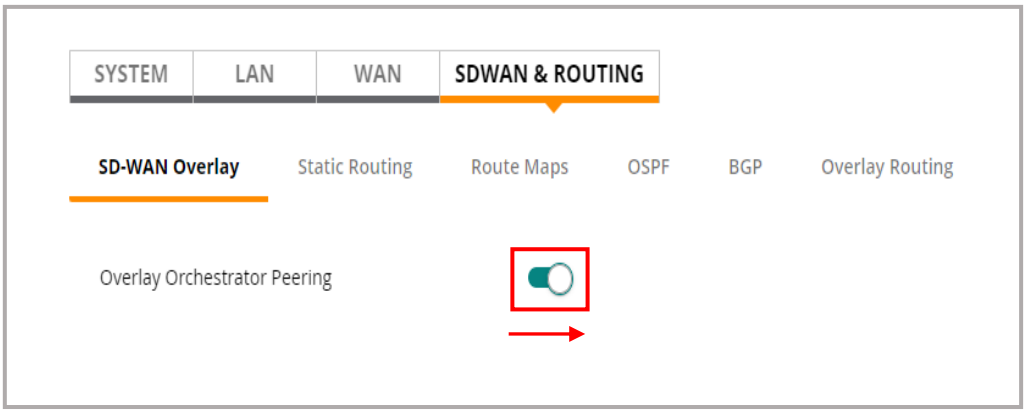


Ilustración 92: Establecimiento de túneles WAN

Para finalizar, hay que realizar sobre el equipo de la sucursal dos últimos pasos. En primer lugar, desde **DEVICE – WAN- Load Balancing**, se escogerá el algoritmo de equilibrio de carga. Este algoritmo hará que el tráfico coincidente, bien mediante políticas DPS que se hayan implementado en la sucursal o bien, cuando haya más de una ruta al destino, se distribuya entre los enlaces ascendentes WAN activos, en nuestro caso: MPLS, AL1 y AL2.

El algoritmo de equilibrio de carga determina cómo se distribuirán las sesiones entre los enlaces ascendentes WAN activos. Las opción que Aruba Central ofrece respecto a este tipo de algoritmos son tres[(1)]: *Round Robin*, recuento de sesiones y el de uso de enlace ascendente.

Por otro lado, el este software de gestión ofrece la posibilidad de configurar políticas DPS[(2)] (selección dinámica de ruta), que son las encargadas de determinar los enlaces ascendentes WAN que se seleccionarán para determinados usuarios, aplicaciones y destinos específicos.

Este tipo de políticas son las que se deben establecer para cumplir con las prioridades para los servicios y aplicaciones que generaban tráfico entre la sucursal y el nodo principal. Las aplicaciones y servicios, así como las prioridades se expusieron en el apartado: "4.1.2 Especificación" de este documento.

---

(1) Se puede encontrar información adicional los algoritmos que ofrece *Aruba Central* en el "Anexo XVIII"
(2) En el "Anexo XIX" se puede encontrar información adicional sobre políticas DPS

Sin embargo, en una primera configuración se seleccionará el algoritmo *Round Robin* para poner en funcionamiento, de manera sencilla, este piloto. Posteriormente, mediante distintas pruebas, se puede seleccionar cualquiera de los otros dos algoritmos, así como establecer diferentes políticas DPS.

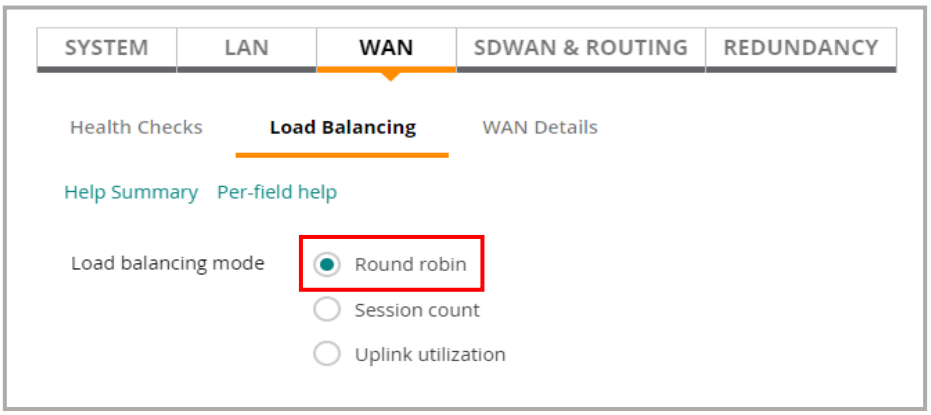


Ilustración 93: Selección algoritmo equilibrio de carga

En segundo lugar, se configura el chequeo de los enlaces WAN para determinar que existe conexión, así desde **DEVICE – WAN- Health Checks**, activamos el chequeo, elegimos la opción sobre dónde y con qué modo de prueba.

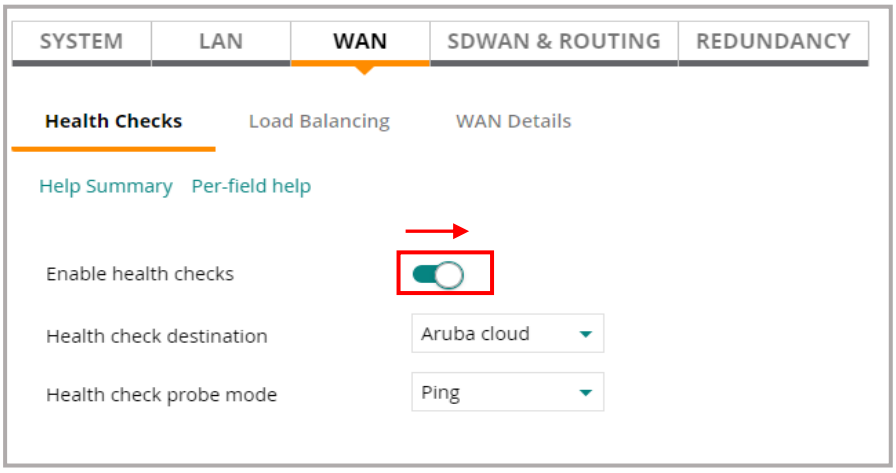


Ilustración 94: Chequeo enlaces WAN

Una vez establecidos los túneles y tener el conocimiento de las redes, al realizarlo de forma automática mediante el orquestador, será necesario realizar el enrutamiento con el centro de datos. Es decir, los enrutadores y firewall del centro de datos y la red corporativa necesitarán saber cómo llegar a las redes de la sucursal, que hay detrás del equipo cabecera. Hay dos opciones, bien mediante rutas estáticas o aprovechar el enrutamiento dinámico a través de OSPF.

En el caso que nos ocupa, al haber solo un equipo cabecera la opción de rutas estáticas hubiera sido una buena opción si las subredes de la sucursal hubieran sido contiguas, pero en este caso no lo son, lo que haría que tener que introducir hasta 16 de forma manual. Por lo tanto, se opta por la configuración OSPF en la

cabecera y el router de primer salto para intercambiar dinámicamente las rutas de la sucursal y las corporativas.

De esta manera, OSPF no solo se usará para anunciar las redes de sucursales en un área OSPF, sino que también se usará por la cabecera para aprender rutas corporativas. Los pasos para configurar OSPF en el equipo cabecera (VPNC) serán al menos los siguientes pasos:

- Habilitar OSPF
- Configurar un ID de enrutador, está dirección puede ser la dirección asignada a la interfaz de bucle invertido de VPNC.
- Definir un área o áreas OSPF y establecer el tipo

En primer lugar, se configura la interfaz *loopback*, una dirección IP válida puede ser la IP del sistema que ya está configurada (172.17.175/24) y además tiene la interfaz VLAN asociada 3701. Así, desde el equipo cabecera desde **DEVICE – SYSTEM – Loopback Interface**, se completará:

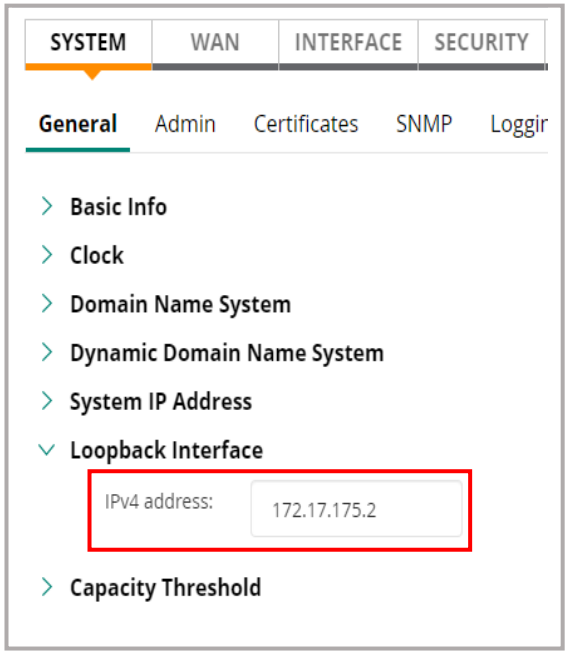


Ilustración 95: Configurar interface loopback equipo cabecera

Ahora, desde **DEVICE – ROUTING – OSPF – General**, se habilita globalmente OSPF en el equipo cabecera, se introduce el ID del router que en este caso es la interfaz loopback y el área. El área consultada en el router de primer salto de la institución es la 0.0.0.100, aunque tienen previsión de cambiarla a 0.0.0.0.

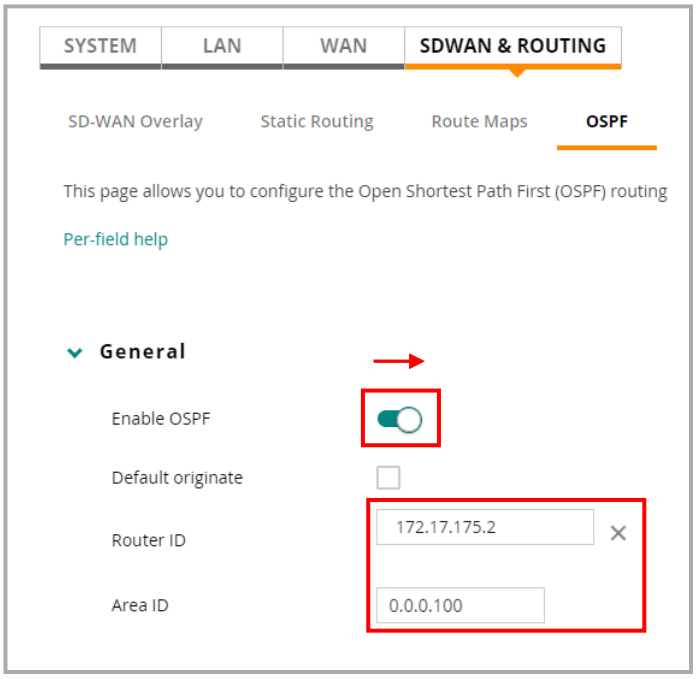


Ilustración 96: Configurar OSPF cabecera (I)

Ahora desde el mismo sitio, pero en la parte **Interface** se selecciona la interfaz VLAN 600 que se configuró en la parte LAN de la cabecera y le asocia un área.

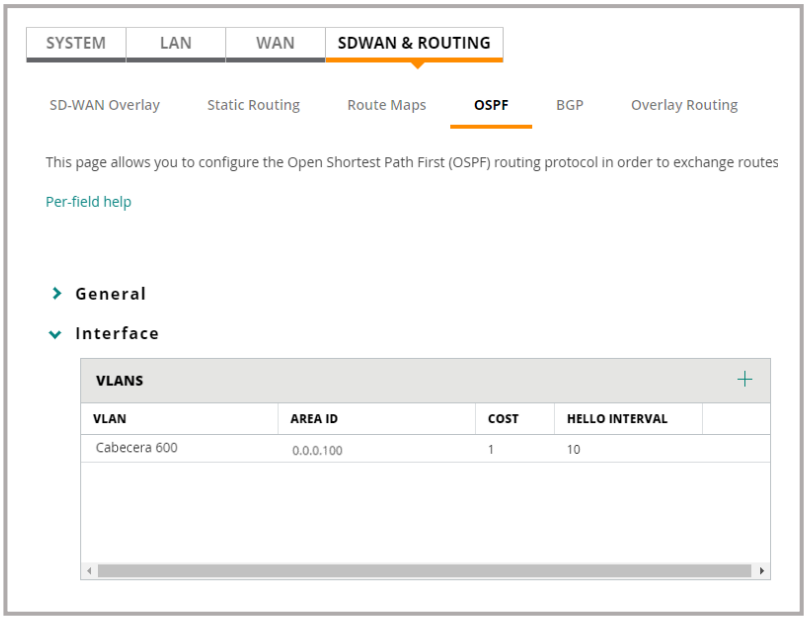


Ilustración 97: Configurar OSPF cabecera (II)

Finalmente, en la parte de ***Redistribution*** se selecciona como protocolo fuente ***SD-WAN Overlay***. Esta configuración permite al equipo cabecera SD-WAN distribuir las rutas superpuestas. Cabe precisar, que el protocolo fuente

seleccionado es porque la configuración que se estableció anteriormente fue de forma orquestada.

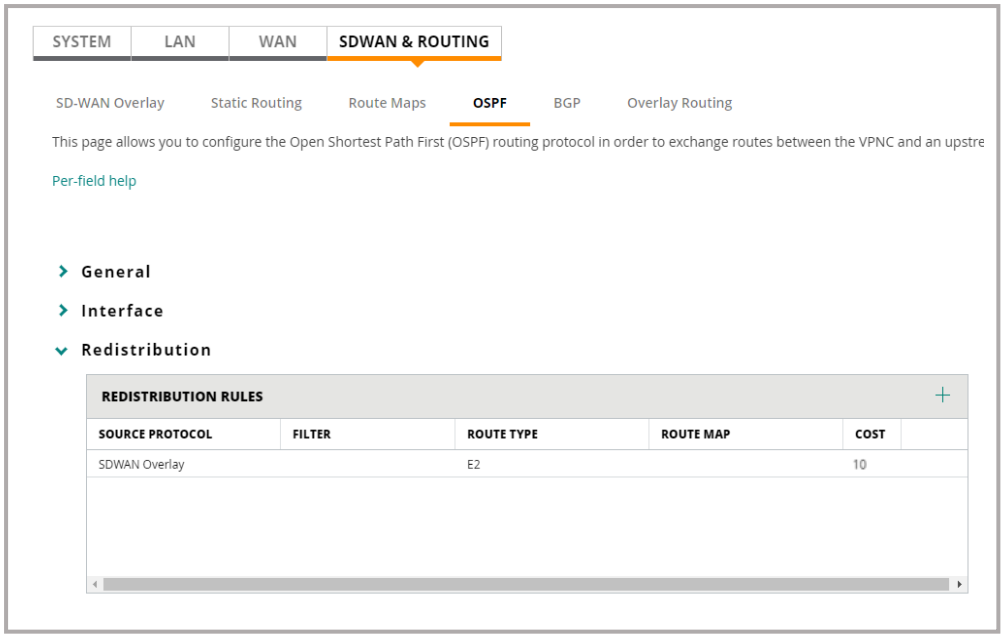


Ilustración 98: Configurar OSPF cabecera (III)

Finalmente, se configura en la cabecera el chequeo de la LAN, el activar esta característica es por si hay perdida de rutas corporativas OSPF.

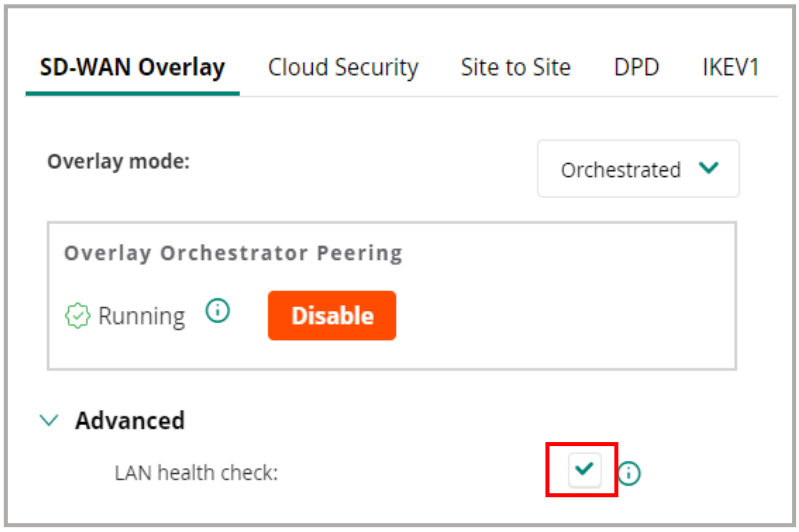


Ilustración 99: Chequeo LAN cabecera

Finalmente, con el puerto GE0/0/0 del equipo cabecera conectado al puerto 1/1/11 del router de la red troncal de la institución (ro-A-ctic.cr-ges.uclm.es)[*], se está en disposición de realizar la configuración en dicho router para establecer el acceso a red, los trabajos realizados son los siguientes:

[*] Se puede consultar información adicional sobre la red troncal en los apartados: "2.1.2 Red troncal" – "Anexo IV

- Observar en el archivo de su última copia de seguridad de configuración en ejecución a fecha de redacción de este trabajo (*172.17.161_running_20200530060034.cfg*) la siguiente información relativa a OSPF:

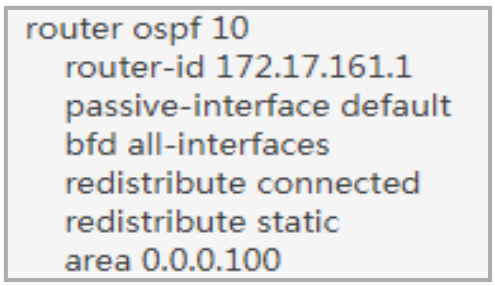


Ilustración 100: OSPF router red troncal

- Crear VLAN 600:

```
vlan 600
    name cabecera-SDWAN-cr
    vsx-sync
```

- Configurar interface 1/1/11

```
interface 1/1/11
    vsx-sync vlans
    no shutdown
    description vpnc-cr Ge0/0/0
    no routing
    vlan trunk native 1
    vlan trunk allowed 600
    spanning-tree bpdu-filter
```

- Configurar interface vlan600

```
interface vlan600
    description VPNC-cabecera-cr
    vsx-sync active-gateways
    ip address 172.16.16.2/24
    active-gateway ip mac 00:00:5E:00:03:00
    active-gateway ip 172.16.16.1
    ip helper-address 172.20.1.67
    ip heper-address 172.20.32.167
```

Llegado este punto, la construcción del piloto SD-WAN entre la sucursal AL y el nodo principal CR, estaría terminada como punto de partida y a la espera de las diferentes pruebas a realizar sobre ella, tal como podemos ver en el siguiente apartado.

(*) Se puede consultar información adicional sobre la red troncal en los apartados: "2.1.2 Red troncal" – "Anexo IV

4.1.5. Pruebas

En este punto y construido el piloto SD-WAN, se realizarían diferentes pruebas para evaluarlo. Sin embargo, tal como expuso en el subapartado "4.1.4.2 Consideraciones actuales" del apartado "4.1.4 Construcción" del pilo SD-WAN, la pandemia originada por el Covid-19, no ha permitido poder realizar una construcción del piloto física, tal y como estaba proyectado en este trabajo, al estar cerrados los edificios implicados en este proyecto. Aunque, de manera exhaustiva y con explicaciones paso a paso se ha realizado todo el proceso de implementación y configuración sobre el software de gestión *Aruba Central*, como si de una implementación física se tratase.

En este apartado de pruebas, se tiene el mismo problema, porque aunque el piloto se hubiera podido construir en las ubicaciones, las pruebas a realizar sobre la red hubieran sido mínimas y con poca validez, debido a la escasez de tráfico que habría en la red superpuesta del piloto SD-WAN, al no contar con usuarios.

Los usuarios de la sucursal, respecto al rol de PDI no están, al estar la docencia presencial suspendida, respecto al PAS el formato de tareas es teletrabajo no existiendo la actividad presencial. Además, no hay alumnos en los edificios...

Por lo todos los motivos anteriormente expuestos, se realizará una enumeración de algunas de las pruebas que se podrían llevar a cabo. Estas pruebas aportarían información suficiente para realizar modificaciones en el algoritmo de equilibrio de carga e implementar políticas de selección de rutas dinámicas DPS, en función de las aplicaciones, servicios y usuarios, según las prioridades establecidas por la organización.

Con todas estas pruebas, que podrían incluso incluir la simulación de cortes de red, por ejemplo del enlace MPLS, aportarían información suficiente para saber si en un horizonte de tiempo razonablemente corto, la institución podría prescindir de dicho enlace y por lo tanto, del gran coste recurrente que tiene.

A continuación, se detalla un listado de pruebas. Estas pruebas que se referencian al Anexo XX de este trabajo y donde se puede ver de manera gráfica y real el resultado de cada una de las pruebas. Esto lo ha hecho posible la autorización de Aruba al autor de este trabajo, para poder acceder en modo usuario (sin privilegios) a una red SD-WAN que tienen desplegada en pruebas.

Esta red, aunque es más compleja en cuanto a diseño y construcción que la del piloto de este trabajo, aportará el valor necesario para este apartado, debido a las circunstancias tan especiales que se está viviendo a nivel mundial.

Algunas de la pruebas que se pueden llevar a cabo tanto a nivel de sucursal, de equipo de cabecera, de red, aplicaciones, clientes,... son las siguientes:

- Detalle general del equipo sucursal o cabecera con las características más importantes, como el estado de enlaces WAN, túneles VPN...

- Detalle de la parte WAN a nivel de equipo, donde se pueden ver el estado de puertos, interfaces WAN, tráfico, comprensión, latencia y perdida de paquetes.
- Detalle de la parte LAN a nivel de equipo, donde se pueden ver el estado de puertos, interfaces LAN e interfaces VLAN, entre otras informaciones.
- Detalle de los túneles VPN y routing, ya sea, estático, OSPF, BGP u orquestado.
- Detalle de las políticas DPS, que se están aplicando
- El número de sesiones, activas o no, así como el detalle de cada una de ellas al seleccionarla.
- La cantidad y lista de clientes conectados, sesiones activas a nivel de equipo, red o usuario. Permitiendo ver el detalle al seleccionar cualquiera de ellas.
- Lista de las aplicaciones por sucursal, red o usuario, además de una categorización de sitios web visitados.
- Detalle de cualquier aplicación seleccionada
- Listado de alertas y eventos sobre la red
- Disponibilidad de herramientas de chequeo y comandos
- La creación de informes por secciones, permitiendo el envío de cualquiera de ellos por email o exportación a ficheros PDF.
- La simulación de corte en cualquiera de los enlaces de la sucursal

4.1.6. Conclusiones sobre el piloto SD-WAN

A lo largo del capítulo 4, de este trabajo, se han desarrollado todas las fases para la creación de un piloto SD-WAN: definición, diseño, especificación, construcción y pruebas.

Se puede constatar, que la red se puede desplegar con escasa intervención de personal en el lugar remoto, solo siendo necesario en el equipo SD-WAN, la conexión a la red eléctrica y las cuatro conexiones de red (los 3 enlaces WAN y una conexión al conmutador de distribución), esta característica hace posible la configuración y despliegue con escasa presencia, por no decir ninguna, de personal técnico en la sucursal.

Además, un punto ventajoso es la gran redundancia con la que la sucursal cuenta, debido a los múltiples enlaces en la infraestructura WAN de la sucursal, en este caso: dos enlaces FTTH de Internet de bajo coste y un enlace MPLS. También, se ha podido ver como gracias a la orquestación, que el software *Aruba Central* ofrece, se han realizado de forma automatizada, tanto la implementación de túneles VPN sobre la red subyacente, como el aprendizaje de las rutas hacia

las diferentes redes de la sucursal en el VPNC (cabecera). Todo ello, posibilita despliegues de sucursal en tiempo récord.

Así, por un lado, la seguridad es completa al estar todo el tráfico cifrado y posteriormente filtrado por los firewalls perimetrales de la organización. Aunque, esta última característica, merma la flexibilidad y ventajas respecto a las posibilidades que una red SD-WAN puede ofrecer. Sin embargo, era un requisito impuesto por la organización para poder llevar a cabo la implantación inicial del piloto en su infraestructura.

Además, la integración con la red del centro de datos es perfecta al disponer de distintas posibilidades de enrutamiento: estático y dinámico. En el caso que nos ocupa, se ha implementado mediante el protocolo de enrutamiento OSPF, entre el equipo cabecera SD-WAN (VPNC) y el router de primer salto de la institución.

Por un lado, se ha realizado un resumen respecto la una gran cantidad de pruebas. Estas pruebas de monitorización se pueden realizar con un alto grado de granularidad, lo que permite realizarlas de manera tan específica e individualizada como se quiera: red SD-WAN, sucursal, cabecera, cliente/s, aplicación/s, sesión/es... y además, permite la elaboración automática de informes personalizados.

Por otro lado, con las distintas pruebas e informes se estará en disposición de tomar las decisiones y/o realizar aquellos ajustes de configuración y gestión que fueran necesarios, para optimizar más aún la red, como:

- La selección del algoritmo de equilibrio de carga óptimo al tráfico generado
- La definición, en caso necesario, de políticas de selección de rutas dinámicas (DPS), en función de las prioridades definidas respecto a servicios, aplicaciones y roles de usuario que la sucursal tiene y demanda.
- La posibilidad de supresión del enlace MPLS o la sustitución de este por otro de bajo coste de Internet, tipo FTTH, LTE..., lo que conlleva un ahorro económico sin la merma en la calidad y cantidad de servicios.

Finalmente, la comercial de Aruba en uno de los últimos contactos, informan que los costes de equipamiento y licenciamiento pueden llegar a tener entre un 40% y un 50% sobre el precio de lista, al tratarse de un cliente potencial como es el caso de la institución universitaria objeto de este estudio.

Esta información hace que el coste, el primer año para la sucursal y cabecera, (equipo, licencia, mantenimiento, enlaces a excepción del MPLS, instalación y configuración) este en torno a 3.600 euros y 14.100 euros respectivamente, bajando el segundo y tercer año a 1.650 euros anuales para la sucursal y 5.300 euros anuales para la cabecera, frente a los 8.800 euros anuales solo del enlace MPLS. Estos datos hacen que la inversión de la cabecera se diluya si finalmente más sucursales forman parte de este tipo de tecnología. Además, la inversión es fácilmente amortizable en un horizonte no muy lejano, si definitivamente se puede prescindir de los enlaces alquilados (MPLS).

5. Conclusiones

A lo largo del desarrollo de este proyecto se ha seguido la planificación inicial tal como estaba programada, aunque con algunos matices. Por un lado, se han mantenido distintas reuniones con el personal del área TIC de la institución, para conocer con el detalle necesario la red de comunicaciones de la organización. Por otro lado, un trabajo personal e individualizado de investigación, para conocer en profundidad la tecnología de las redes definidas por software en sucursales y como incorporarla en la organización. Finalmente, un trabajo colaborativo con la unidad responsable de la red universitaria para llevar a cabo la integración de la parte final de este proyecto, un piloto SD-WAN, en su infraestructura de red.

Toda la planificación ha sido correcta a lo largo del desarrollo del trabajo, excepto por la irrupción de la pandemia originada por el COVID-19 (Coronavirus) que ha provocado el estado de alarma en todo el territorio del estado español, desde el 13 de marzo y actualmente, prorrogado al menos hasta el 21 de junio.

Este imprevisto ha incidido directamente en el desarrollo del proyecto, fundamentalmente en la construcción del pilo SD-WAN. Esto es debido a que los edificios de la institución universitaria han permanecido y permanecen cerrados actualmente, en las distintas fases de desescalada 0 y 1, siendo esta última en la que actualmente a 31 de mayo se encuentra la provincia implicadas en este proyecto.

La única excepción al cierre, en esta fase 1 e incluso en la posible fase 2, se encuentra en bibliotecas solo para préstamo y con cita previa, investigación para el personal investigador, con permiso autorizado por el Vicerrectorado de Investigación y solo por el tiempo necesario, por último el servicio de registro, con cita previa. Todos esos servicios en horario reducido de mañanas.

Sin embargo y dejando a un lado, la parte negativa que esta situación ha provocado en el desarrollo de este trabajo, he de decir, que de alguna manera ha influido positivamente en mi persona debido a que de una parte, he tenido que adaptar la forma de trabajar a un nivel colaborativo mayor (videoconferencias, desarrollo de documentos compartidos...) y de otra parte, he tenido que reconducir el proyecto, sobre todo en la construcción del piloto SD-WAN, para poder cumplir los objetivos marcados inicialmente y que no mermara el valor que esta parte del trabajo aporta al proyecto en su conjunto y en las líneas de trabajo posteriores.

Las lecciones en la vida se aprenden viviendo, decía mi abuelo y ese consejo me ha aportado una lección importantísima respecto a la dirección y ejecución del proyecto: por muchos riesgos que se hayan previsto, por mucho confianza que se tenga en tenerlo todo bajo control, las distintas situaciones que se pueden presentar pueden hacerlo tambalear e incluso fracasar.

Sin embargo, lo importante es no decaer y seguir adelante para conseguir dirigirlo y conseguir una línea de trabajo abierta, aprovechable y con continuidad futura una vez la situación vuelva a la normalidad. Este aspecto, verdaderamente, se ha conseguido en este trabajo.

Finalmente, las líneas de trabajo futuro se pueden dirigir sobre dos ejes estructurales: las condiciones respecto al Coronavirus y la gran amplitud de este proyecto.

Respecto a las líneas de trabajo futuro debido a la incisión del Coronavirus en el proyecto, quedaría seguir la guía elaborada sobre la construcción del piloto paso a paso, una vez abierta la sucursal y la sede central. Además, es necesaria la incorporación de usuarios (alumnos, personal de administración y servicios, personal docente investigador,...) para tener dentro de la infraestructura el tráfico real y así, una vez con el funcionamiento normalizado, extraer mediante distintas pruebas datos objetivos para realizar algunas de las líneas de trabajo respecto a la dimensión del proyecto.

Respecto a las líneas de trabajo futuro debido a la profundidad del proyecto se tendrían:

- Por un lado, con los datos obtenidos de unas primeras pruebas los reajustes necesarios para hacer una red óptima (elección del algoritmo de equilibrio de carga adecuado, implementar políticas DPS...) e incluso la toma de decisiones sobre la supresión de parte de la infraestructura con altos costes recurrentes (conexión MPLS)
- Por otro lado, una vez optimizada la red, en un primer nivel, otras líneas de trabajo serían:
    - En primer lugar, modificar los túneles completos VPN hacia un modelo de túneles híbridos en la parte WAN, integrando las medidas de seguridad necesarias. Así, de esta manera el tráfico de Internet de los clientes de la sucursal no tendrá que llegar hasta el centro de datos y retornar de nuevo
    - En segundo lugar, incorporar un gateway virtual SD-WAN en la nube de Azure e integrarlo con el piloto SD-WAN. De esta manera, los servicios y aplicaciones, que la institución tiene desplegados en esa nube, se ofrecerían directamente a los clientes de la sucursal que los demanden por enlaces WAN de la Internet pública
    - Finalmente, desplegar este tipo de red en todas aquellas sucursales de los distintos campus con enlaces alquilados

6. Glosario

- **1000Base-T**. “Es un estándar recogido en IEEE802.3ab para redes de área local tipo Gigabit Ethernet sobre cable de par trenzado sin apantallamiento”
- **1000Base-X**. Ampliación del estándar Ethernet con una capacidad de 1 gigabit por segundo sobre medio de fibra
- **3DES**. En criptografía se llama al algoritmo que hace triple cifrado del DES
- **4G**. En telecomunicaciones se refiere a la cuarta generación de tecnologías de telefonía móvil
- **5G**. En telecomunicaciones se refiere a la quinta generación de tecnologías de telefonía móvil
- **802**.1X. Es una norma IEEE para el control de acceso a red basada en puertos
- **Acceso**. (*Access*) referido al modo acceso de un puerto de un conmutador es la configuración de este en el que se permite pasar solo una VLAN
- **ACL**. (*Access Control List*) traducido como lista de control de acceso. Es usado en seguridad informática para determinar permisos de acceso sobre un determinado objeto
- **ADSL**. (*Asymmetric Digital Subscriber Line*) Utilizada para la transmisión de dato digitales sobre cable de pares simétricos de cobre que lleva la línea telefónica convencional
- **AP**. También conocido como WAP (Wireless Access Point), para referirse a un punto de acceso inalámbrico como dispositivo que permite conectarse distintos equipos de forma inalámbrica para formar una red inalámbrica
- **API**. (*Application Programming Interface*) traducido como interfaz de programación de aplicaciones es un conjunto de funciones y procedimientos utilizados para la comunicación entre distintos componentes de software
- **AES**. (*Advanced Encryption Standar)* es uno de los algoritmos más populares utilizados en criptografía simétrica
- **Azure (Microsoft)**. Conjunto de servicios en la nube para entre otros: construir, probar, desplegar y administrar aplicaciones y servicios mediante el uso de sus centro de datos

---

El recurso consultado y/o cita textual respecto a la definición del glosario ha sido https://www.wikipedia.org/ excepto aquellos términos con posibilidad de realizar búsqueda en su propia web

- **BGW**. (*Branch Gateway) es el equipo SD-WAN de la sucursal.*
- **CACTI**. Aplicación que aporta una solución completa de red para crear gráficos en función de la fuente de datos
- **CBC**. Utilizado en criptografía mediante un algoritmo que utiliza cifrado de bloques
- **CICA**. Centro informático científico de Andalucía concebido para prestar servicios a la comunidad científica andaluza
- **CIEMAT**. Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas adscrito como un organismo de público de investigación adscrito al Ministerio de Ciencia e Innovación
- **Conmutador (*switch*)**. Dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI
- **Coronavirus**. Véase la entrada Covid-19 de este glosario.
- **Covid-19**. Conocida como enfermedad por coronavirus es una enfermedad infecciosa causada por el virus SARS-CoV.2 que se detectó por primera vez en la ciudad china de Wuhan en diciembre de 2019 y que actualmente en marzo de 2020 se ha convertido en una pandemia global a nivel mundial. El estado español está declarado desde el pasado 13 de marzo de 2020 en estado de alerta
- **CPD**. Denomina al centro de procesamiento de datos como el espacio donde están los recursos para ese procesamiento
- **CRM**. (*Customer relationship management*) es un software para la administración de la relación con los clientes de una organización
- **DoS**. (*Denial of Service*) es un ataque para la denegación de servicios en un sistema de computadoras en red para provocar que un recurso o servicio sea inaccesible a los usuarios legítimos del sistema
- **DDoS**. (*Distributed Denial of Service*) es un ataque de denegación de servicios distribuido (ver DoS), es decir, generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto destino, para provocar la inaccesibilidad de la información o servicio a los usuarios legítimos del sistema
- **DHCP**. (*Dynamic Host Configuration Protocol*) es el protocolo de configuración dinámica de host donde el servidor asigna dinámicamente una dirección IP junto con otros parámetros de configuración de red
- **DPS**. (*Dynamic Path Selection*) es selección dinámica de la ruta, referido a las políticas que se pueden implementar en una red de comunicaciones

- **DMZ**. En seguridad informática es conocida como zona desmilitarizada y es la red que está entre la red interna de una organización y una red externa, normalmente en Internet
- **FaaS**. (*Function as a Service*) es una categoría de servicios de computación en la nube que permite a los clientes desarrollar y ejecutar aplicaciones sin la necesidad de construir y mantener la infraestructura asociada al desarrollo y ejecución de la aplicación
- **Firewall**. Conocido en castellano como cortafuegos, es la parte de un sistema informático o de una red informática que permite bloquear el acceso no autorizado permitiendo al mismo tiempo comunicaciones que sí lo están.
- **FTTH**. (*Fiber To The Home*) Tecnología basada en cable de fibra óptica y sus sistemas de distribución para el suministro de servicios avanzados de telecomunicaciones en hogares y negocios
- **GÉANT.** Red paneuropea de investigación y educación que interconecta las Redes nacionales de Investigación y Educación (NREN) de Europa
- **GRE**. (*Generic Routing Encapsulation*) es un protocolo de tunelización desarrollado por Cisco System que encapsula una gran variedad de protocolos de capa de red sobre enlaces
- **HFC.** (*Hybrid Fiber-Coaxial*) traducido como hibrido de fibra coaxial que en red de comunicaciones define una red de banda ancha donde la red de fibra óptica incorpora también cable coaxial
- **Hub-and-spoke**. Es una forma de optimización en la topología de redes organizando la ruta en forma de estrella
- **IDS**. (*Instrusion Detection System*) Un sistema de detección de intrusos es un programa de detección de accesos no autorizados a una computadora o red
- **IEEEN**. Instituto de Ingeniería Eléctrica y Electrónica dedicado a la normalización y desarrollo en áreas técnicas
- **IPS**. Un sistema de prevención de intrusos es un software que ejerce el control de acceso en una red informática
- **IPSec**. (*Internet Protocol security*) Es un conjunto de protocolos para asegura las comunicaciones sobre el protocolo de internet (IP) autenticando y/o cifrando cada paquete en un flujo de datos
- **IPv6**. (*Internet Protocol version 6*) es la versión del protocolo de Internet (IP) en su versión 6 y sucesor de IPv4.
- **IT**. Tecnología informática

El recurso consultado y/o cita textual respecto a la definición del glosario ha sido https://www.wikipedia.org/ excepto aquellos términos con posibilidad de realizar búsqueda en su propia web.

- **LCD**. Pantalla de cristal líquido, generalmente usado en dispositivos electrónicos para mostrar información
- **Loopback**. Es la dirección que se suele utilizar cuando en una transmisión de datos tiene como destino el propio host
- **LTE**. (*Long Term Evolution*) es un estándar para comunicaciones inalámbricas de transmisión de datos de alta velocidad para teléfonos móviles y terminales de datos
- **MAC**. Identificador único de los interfaces de red
- **MPLS**. (*Multiprotocol Label Switching*) Es un estándar para el transporte de datos creado por *Internet Engineering Task Force* (IETF)(*)
- **Multicast**. Envía desde un emisor a ciertos destinatarios específicos
- **OSPF**. (*Open Shortest Path First*) Es un protocolo definido en RFC 2328 y es utilizado para el encaminamiento jerárquico de pasarela interior que utiliza el algoritmo Dijkstra para calcular la ruta más corta entre dos nodos
- **PAS**. Personal de administración y servicios
- **PDF**. (*Portable Document Format*) Formato portable de documento
- **PDI**. Personal docente e investigador
- **PoE**. (*Power over Ethernet*) es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN para alimentar, entre otros: conmutadores, puntos de acceso, router, teléfono, cámara IP...
- **QinQ**. Ethernet referida al estándar IEEE802.1ad que permite insertar múltiples etiquetas VLAN en una sola trama
- **QoS**. (*Quality of Service*) traducido como calidad de servicio, es amenudo el rendimiento promedio de una red de computadores
- **Radius**. (*Remote Authentication Dial-In User Service*) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP
- **RedIRIS**. Red española para interconectar los recursos informáticos de las universidades y centro de investigación
- **RedIRIS Nova**. Red óptica de alta capacidad de RedIRIS
- **RIP**. (*Routing Information Protocol*) es un protocolo de enrutamiento con algoritmo basado en vector distancia.
- **Round-robin**. Es un protocolo de planificación de procesos sencillo de implementar

---

El recurso consultado y/o cita textual respecto a la definición del glosario ha sido https://www.wikipedia.org/ excepto aquellos términos con posibilidad de realizar búsqueda en su propia web.

- **Router**. Dispositivo que permite establecer la ruta destino a cada paquete de datos dentro de una red informática
- **SaaS**. (*Software as a Service*) es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía a la que se accede desde Internet
- **SDN**. Red definida por software generalmente para centro de datos
- **SNMP**. (*Simple Network Management Protocol*) traducido como protocolo simple de administración de red. Este protocolo de la capa de aplicación facilita el intercambio de información de administración entre dispositivos en red
- **SPF**. (*Small form-Factor Pluggable transceptor*) es un transceptor compacto y conectable en caliente usado para las aplicaciones de datos y telecomunicaciones. Están diseñados para usar: fibra, Gigabit Ethernet, entre otros
- **SSH**. (*Secure SHell*) es el nombre de un protocolo y del programa que lo implementa. Su función es el acceso de forma remota a un servidor mediante un canal seguro por donde la información va cifrada
- **SSL**. (*Secure Sockets Layer*), es un protocolo criptográfico para comunicaciones seguras por red
- **SVI**. (*Switch Virtual Interfaces*) Representa una interfaz lógica en un conmutador y asociada a una VLAN concreta
- **Syslog**. Es un estándar de hecho para el envío de mensajes de registro en una red IP
- **TACAS+**. (*Terminal Access Controller Access Control System*) es sistema decontrol de acceso del controlador de acceso a terminales. Es un protocolo de autenticación remota usado para la gestión de acceso a dispositivos de comunicaciones incluidos servidores
- **TI**. Tecnologías de la información
- **TIC**. Tecnología de información y comunicación
- **Trunk**. Es el modo de un puerto que por defecto es miembro de todas las VLANs, aunque la lista puede ser configurable
- **Unicast**. Es el envío de información desde un único emisor a un único receptor.
- **USB**. (*Universal Serial Bus*) Es un estándar que establece especificaciones para cableado y conectores para la comunicación y conexión entre dispositivos electrónicos

---

El recurso consultado y/o cita textual respecto a la definición del glosario ha sido https://www.wikipedia.org/ excepto aquellos términos con posibilidad de realizar búsqueda en su propia web.

- **VCPD**. Es un CPD virtual, es decir, es un centro de proceso de datos en la nube
- **VLAN**. (*Virtual LAN*) Denominada como red de área local virtual, utilizada para crear redes lógicas independientes dentro de una misma red física
- **VPC**. Red privada virtual en la nube
- **VPN**. (*Virtual Private Network*) se traduce como red privada virtual y es una tecnología para realizar una extensión segura de la red de área local (LAN) sobre una red pública como Internet
- **VRRP**. (*Virtual Router Redundancy*) es un protocolo de comunicaciones no propietario definido en el RFC 3768**VSX**. (*Virtual Switching Extension*) Es utilizado para evitar tiempos de inactividad de red durante caídas o ciclo de mantenimiento
- **WAN**. (*Local Area network*) Puede traducirse como Red de área Local
- **WLAN**. (*Wireless Local Area network*) Puede traducirse como Red de área Local Inalámbrica
- **xDSL**. Línea de abonado digital que consiste en la transmisión de datos digitales sobre un par de cables de cobre

El recurso consultado y/o cita textual respecto a la definición del glosario ha sido https://www.wikipedia.org/ excepto aquellos términos con posibilidad de realizar búsqueda en su propia web.

7. Bibliografía

- A10 networks, disponible en Internet, https://www.a10networks.com/, consultado en abril 2020.
- Arista, disponible en Internet, https://www.arista.com/en/, consultado en abril de 2020.
- Aruba, disponible en Internet, https://www.arubanetworks.com/, consultado en marzo y abril 2020.
- Aruba, disponible en Internet, https://www.arubanetworks.com/products/networking/management/central/, consultado en mayo de 2020.
- Aruba, disponible en Internet, https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf, consultado en abril y mayo 2020.
- Aruba, disponible en Internet, https://www.arubanetworks.com/assets/og/OG_SD-WAN.pdf, consultado en abril y mayo 2020.
- Aruba, disponible en Internet, https://www.arubanetworks.com/assets/ds/DS_9000Series.pdf, consultado en abril y mayo 2020.
- Aruba, disponible en Internet, https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf, consultado en abril y mayo 2020.
- Aruba, disponible en Internet, https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf, consultado en abril y mayo 2020.
- Aruba, disponible en Internet, https://help.central.arubanetworks.com/2.4.9/documentation/online_help/content/gateways/vgw/vgw.htm, consultado en abril y mayo 2020.
- Aruba, 2019, “User Roles and User-Based Tunneling”, disponible en Internet, https://community.arubanetworks.com/t5/Wired-Intelligent-Edge-Campus/Aruba-Wired-Intelligent-Edge-Dynamic-Segmentation/m-p/464717, consultado en abril y mayo de 2020.
- Azure, disponible en Internet, https://azure.microsoft.com/es-es/services/expressroute/#security, consultado en abril 2020.
- Cato networks, disponible en Internet, https://www.catonetworks.com/sd-wan/, consultado en marzo y abril 2020.

- Cisco, disponible en Internet, https://www.cisco.com/, consultado en marzo 2020.
- Citrix, disponible en Internet, https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf, consultado en mayor 2020.
- Citrix, disponible en Internet, https://www.citrix.com/es-mx/glossary/what-is-software-defined-networking.html, consultado en marzo y abril.
- Citrix, disponible en Internet, https://www.citrix.com/es-es/products/citrix-sd-wan/, consultado en marzo y abril.
- Community arubanetworks, disponible en Internet, https://community.arubanetworks.com/t5/Validated-Reference-Design/SD-Branch-Fundamentals-Guide/ta-p/482038, consultado en abril y mayo.
- Cooney, Michael, 16-4-2019, disponible en Internet, https://www.networkworld.com/article/3209131/what-sdn-is-and-where-its-going.html, consultado en abril 2020.
- de Manuel Clemente, Carlos, sin terminar – fecha de inicio: marzo de 2019, "Arquitectura General Servicios Comunicaciones", consultado marzo y abril de 2020.
- Hewlett Packard Enterprise, disponible en internet, https://buy.hpe.com/mx/es/networking/networking-switches/hpe-flexnetwork-5130-ei-switch-series/p/7399420, consultado en abril 2020.
- Hewlett Packard Enterprise, disponible en Internet, https://techlibrary.hpe.com/us/en/networking/products/configurator/index.aspx#.XrBSRY0Unuj, consultado en mayo de 2020.
- Insoltec, disponible en Internet, https://www.insoltec.cl/, consultado en abril 2020.
- Jazztel, disponible en Internet, https://www.jazztel.com/, consultado en abril y mayo 2020.
- Marshall K. y Tanguay A., 2018, "SD-Branch Fundamentals Guide – Versión 1.1.1", disponible en Internet, https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/128/14/SD-Branch%20Fundamentals%20Guide%20-%20Final%20-%20Fulldocv2.pdf, consultado entre enero y mayo de 2020.
- Marshall K. y Tanguay A., 2018, "SD-Branch Fundamentals Guide – Chapter 2 – Central – Version 1.1.0", disponible en Internet, https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/128/10/SD-Branch%20Fundamentals%20Guide%20-%20Final%20-%20Central%20Only.pdf, consultado entre enero y mayo de 2020.

- Marshall K. y Tanguay A., 2018, “SD-Branch Fundamentals Guide – Chapter 3 – Provisioning – Version 1.1.0”, disponible en Internet, https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/128/11/SD-Branch%20Fundamentals%20Guide%20-%20Final%20-%20Provisioning%20Only.pdf, consultado entre enero y mayo 2020.
- Marshall K. y Tanguay A., 2018, “SD-Branch Fundamentals Guide – Chapter 4- Aruba Gateways - Versión 1.1.1”, disponible en Internet, https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/128/15/SD-Branch%20Fundamentals%20Guide%20-%20Final%20-%20Gateways%20Only.pdf, consultado entre enero y mayo de 2020
- Marshall K. y Tanguay A., 2018, “SD-Branch Fundamentals Guide – Chapter 5- Topologies – Version 1.1.0”, disponible en Internet, https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/128/13/SD-Branch%20Fundamentals%20Guide%20-%20Final%20-%20Topologies%20Only.pdf, consultado entre enero y mayo de 2020.
- Microsoft, disponible en Internet, https://docs.microsoft.com/es-es/azure/security/fundamentals/overview, consultado en abril 2020.
- Ministerio de ciencia e innovación , disponible en Internet, https://www.rediris.es/, consultado en marzo 2020.
- Movistar, disponible en Internet, https://www.movistar.es/empresas/, consultado en abril y mayo 2020.
- Networking, disponible en Internet, (21-05-2018), https://www.networkworld.es/networking/llega-la-adopcion-de-sdn-y-sdwan, consultado en abril 2020.
- Orange, disponible en Internet, https://www.orange.es/, consultado en abril y mayo 2020.
- Sanjay Uppal; Steve Woo; Dan Pitt (2018). Software-Defined WAN for dummies, 2ª edición, New Jersey, fecha de consulta: marzo y abril 2020.
- Skydsl, disponible en Internet, http://www.skydsl.eu/es-ES/Aut%C3%B3nomos-y-empresas/Internet-por-satelite, consultado en abril y mayo 2020.
- Turner, Jay. 19-01-2017, disponible en Internet, https://www.networkworld.com/article/3159067/the-future-of-sdn.html, consultado en marzo de 2020.
- Velocloud, disponible en Internet, https://www.velocloud.com/sd-wan, consultado en marzo 2020.
- Viasat, disponible en Internet, https://www.viasat-internetsatelite.es/, consultado en abril y mayo 2020.

- Vodafone, disponible en Internet, https://www.vodafone.es/c/empresas/pymes/es/, consultado en abril y mayo 2020.
- Weingberg, Neal y Til, Johna, 16 – 03- 2018, "*What is MPLS: What you need to know about multi-protocol label switching*", disponible en internet, https://www.networkworld.com, consultado en febrero de 2020.
- Wikipedia, disponible en Internet, https://www.wikipedia.org/, consultado en marzo y abril 2020.
- Yoigo, disponible en Internet, https://empresas.yoigo.com/, consultado en abril y mayo 2020.

8. Anexos

En este apartado se compone de 20 anexos que son referenciados mediante enlaces desde distintas partes del documento. Cada uno de los anexos se compone de una o más páginas y dan comienzo, cada uno de ellos, en una nueva página. Los anexos incluidos en este trabajo no son necesarios para la comprensión del trabajo aquí expuesto, pero sin embargo, sí aportan diversa información complementaria que lo enriquece.

En ellos se puede encontrar información adicional sobre instituciones, configuraciones y equipamiento (software y hardware) que se ha referenciado en la elaboración de este trabajo.

Anexo I

Según el contenido de https://www.rediris.es/ : RedIRIS es la red académica y de investigación española que proporciona servicios avanzados de comunicación a la comunidad científica y universitaria nacional y que se encarga de la gestión de Red.es del Ministerio de Economía y Empresa. Además, cuenta con más de 500 instituciones adheridas entre universidades y centros públicos de investigación.

La red de RedIRIS cuenta con RedIRIS-Nova que es la red troncal óptica avanzada basada en fibra oscura que ofrece a la comunidad universitaria e investigadora hasta 100 Gbps desde los principales centros investigadores. Además, RedIRiS-Nova proporciona acceso a la red de investigación mundial a través de la red paneuropea GÈANT, una infraestructura de red con fibra oscura híbrida que soporta tanto los servicios de conmutación de circuitos como de conmutación de paquetes que interconecta a 33 redes nacionales y da acceso a otras redes de investigación a nivel mundial como: Internet2 (USA), RedCLARA (América Latina), EUMEDCONNET3 (Norte de África) entre otras muchas.

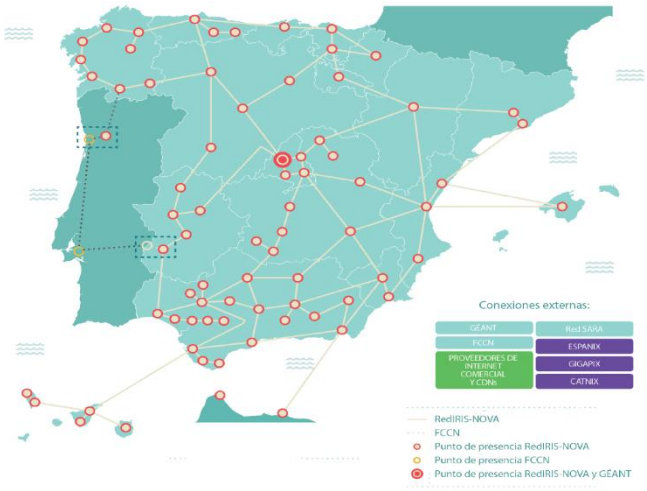


Ilustración 101: Mapa de interconexión de RedIRIS(*)

El catálogo de servicios de RedIRIS son:

- Comunicación y dinamización
- Soporte técnico a instituciones
  - Transferencia de datos
  - Movilidad
  - Calidad del correo electrónico
  - Cloud
  - Identidad digital
  - Colaboración
- Seguridad
- Conectividad
- Redes privadas

Finalmente, cabe destacar que RedIRIS participa en distintos proyectos de I+D e I+D+i que permiten validad nuevas tecnologías acumulando conocimiento para mejorar la red académica española.

Fuente del texto e imagen(*): https://www.rediris.es/
Apartado desde el que se referencia este anexo: "2.1.2 Red troncal"

Anexo II

Aruba serie 8320

Según *ArubaNetworks*, la serie de conmutadores Aruba 8320 son el equipamiento idóneo para implementar centros de datos, núcleo y agregación de sedes empresariales debido a su alta disponibilidad.

Estos conmutadores de 1U proporcionan 32 puertos de 40GbE o 48 puertos de 10 GbE (SFP /SFP+ y 10GBASE-T) con 6 puertos de 40 GbE y alguno de sus modelos con doble fuente de alimentación. Dispone de un sistema operativo de red totalmente programable y un diseñó centrado en la nube que ofrece herramientas de configuración. Además la monitorización y el análisis incorporados mejoran la experiencia de usuario en relación con la resolución de incidencias.

El documento completo de especificaciones se puede descargar a fecha de redacción de este documento en:

https://www.arubanetworks.com/assets/ds/DS_8320Series.pdf

Ilustración 102: Aruba 8320(*)

La extensión de conmutación virtual (VSX) de Aruba proporciona una arquitectura redundante tanto en hardware como en software para garantizar que no haya tiempo de inactividad, incluso durante las actualizaciones que se llevan a cabo en las sucursales como en el centro de datos.

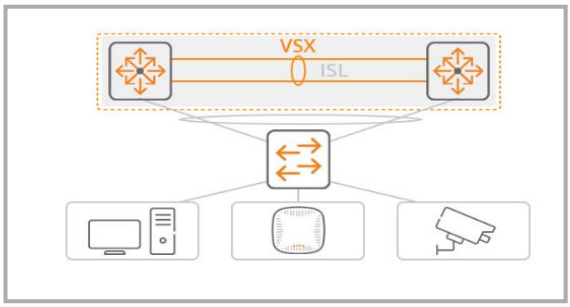


Ilustración 103: Diagrama VSX de Aruba(*)

El resumen técnico sobre la extensión virtual (VXS) de Aruba se puede descargar a fecha de redacción de este documento en:

https://www.arubanetworks.com/assets/tg/TB_VSX.pdf

Fuente del texto e imágenes(*): https://www.arubanetworks.com/
Apartados desde los que se referencia este anexo: "2.1.2 Red troncal" – "2.2.3.2 Sucursal TR"

Aruba serie 2930F

Según *ArubaNetworks*, la serie de conmutadores Aruba 2930F son equipos de acceso básico de capa 3 sencillos de implementar, administrar, con seguridad avanzada y con una variedad de herramientas disponibles para su administración:

- Aruba *ClearPass* para un control seguro de acceso a la red[(1)]
- Aruba *AirWave* para una gestión óptima de la red[(2)]

Los conmutadores 2930F soportan enrutamiento de acceso OSPF, enrutamiento RIP e IPV6 con una calidad de servicio robusta. Estos conmutadores de 1U proporcionan 24 o 48 puertos, 4 SPF+ y con la opción de PoE de hasta 370 W.

Ilustración 104: Aruba serie 2930F(*)

El documento completo de especificaciones se puede descargar a fecha de redacción de este documento en:

https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf

---

[(1)] Información adicional de *ClearPass*: https://www.arubanetworks.com/es/productos/seguridad/gestion-de-politicas/

[(2)] En el anexo V se puede encontrar más información sobre Aruba *AirWave*

Fuente del texto e imagen[(*)]: https://www.arubanetworks.com/

Apartado desde el que se referencia este anexo: "2.1.2 Red troncal" – "2.2.3.2 Sucursal TR"

Anexo III

A continuación se expone la configuración tanto de un interfaz físico como del SVI de los enlaces con RedIRIS Nova.

- Configuración tipo de uno de los interfaces físicos con sus comandos y comentarios[(*)]:

interface 1/1/6
vsx-sync vlans →(se sincronizan vlan vía vsx de los Aruba 8320)
no shutdown
description IrisNova-4-CR-AB → (a fecha de redacción se observa que el 4 debe ser un 9)
no routing
vlan trunk native 392 → (se etiqueta la ID de la vlan que presta el servicio en el interfaz, se pueden establecer otras vlanes o permitir el paso etiquetado de paquetes)
vlan trunk allowed 392 → solo se permite el tráfico de las vlanes que interesan
spanning-tree bpdu-filter → si filtran paquetes BPDU para evitar problemas de Spaning-Tree
exit

- La configuración del SVI con sus comandos y comentarios[(*)]:

interface vlan392
description IrisNova-4-CR-AB
ip address 172.16.4.33/29 → La IP dirección menor corresponde a la sede mayor relevancia
ip ospf 10 area 0.0.0.100 → Área 100. Pendiente de reconfiguración como área 0.
no ip ospf passive → declaración explicita como interface no pasivo para OSPF
ip pim-sparse enable → habilitación PIM en uso para servicios multicast de videovigilancia
ip pim-sparse dr-priority 10
exit

Fuente del contenido de este anexo: "*Arquitectura General Servicios Comunicaciones*". (2019). De Manuel, Clemente.
Apartado desde el que se referencia este anexo: "2.1.2 Red troncal"

Anexo IV

En el apartado "2.1.1.2 Red troncal" de la infraestructura actual de la organización, donde se realiza la exposición de la infraestructura actual, se documenta que actualmente la red troncal de la organización solo dispone de un interfaz óptico de 10 G para configurar el enlace de comunicación existente entre dos campus.

Actualmente, la electrónica que la institución tiene en explotación por cada uno de sus nodos principales son parejas de equipos Aruba 8320 con posibilidad de trabajar con enlaces redundados. Sin embargo, la organización no dispone de más interfaces para cada enlace, por lo que han optado por el uso de interfaces en cada nodo de la pareja de Aruba. De esta manera, garantizan las comunicaciones entre de los distintos campus al máximo pues las interconexiones a los distintos centros de cada campus si se encuentran, en su mayoría, redundados contra ambos Aruba 8320 de su nodo.

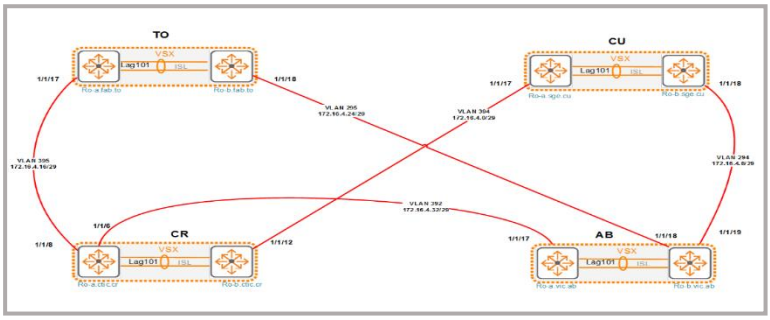


Ilustración 105: Diagrama de red troncal con RedIRIS NOVA(*)

Así del diagrama anterior se desprende respecto a la interconexiones:

- La existencia de un único interfaz físico en cada uno de los extremos del enlace que une los campus de CR y CU
- En los campus CU y TO la conexión de cada uno de sus enlaces con otro campus está repartido entre ambos nodos de la pareja de Aruba
- En los campus de CR y AB uno de los miembros de la pareja Aruba tiene conectadas dos interfaces mientras que el otro miembro solo uno

Esta topología de interconexión entre campus, haciendo uso de un solo interfaz por enlace, viene a proporcionar redundancia ante caía de uno de los nodos o ante actuaciones controladas.

Finalmente, en un futuro inmediato se procederá a la renovación de los servicios de RedIRIS Nova lo que permitirá el uso de interfaces 100 G y 10x10G para cada nodo principal, lo que posibilitará, entre otras, la duplicación de interfaces y por lo tanto una redundancia completa a nivel troncal.

Contenido del texto de este anexo basado en: *Arquitectura General Servicios Comunicaciones*. (2019). De Manuel, Clemente.
Fuente de la imagen(*): *Arquitectura General Servicios Comunicaciones*. (2019). De Manuel, Carlos.
Apartado desde el que se referencia este anexo: "2.1.2 Red troncal" – "4.1.4.3 Implementación del piloto SD-WAN"

Anexo V

Controladoras de la seria 7200 de Aruba

Según *ArubaNetworks*, los equipos Aruba de la serie de *Mobility Controller* 7200, son equipos de nueva generación optimizados para la entrega de aplicaciones móviles y garantizar una adecuada experiencia de movilidad a través de Wi-Fi.

Estos equipos son capaces de gestionar la autenticación, el cifrado y las conexiones VPN, así como los servicios IPv4 e IPv6 de capa 3. Además, está preparado para dotar de protección contra intrusos, al aplicar políticas de firewall de hasta 40 Gbps y más de 2 millones de sesiones concurrentes, dependiendo del modelo.

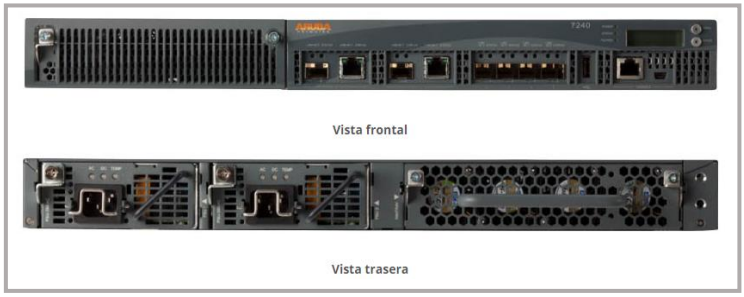


Ilustración 106: Controladora Aruba 7240(*)

La serie 7200 admite fuentes dobles redundantes y reemplazables en caliente para dotar de máxima disponibilidad en las implementaciones cliente. Algunos de sus modelos como 7220 las llevan incorporadas de serie. A partir del modelo 7210 dispone de 4 puertos 10GBASE-X (SPF +).

La siguiente imagen muestra las especificaciones técnicas de la serie 7200 para sus distintos modelos:

Caracteristicas	7205	7210	7220	7240 / 7240XM
Rendimiento y capacidad				
AP máximos (licencias)	256	512	1,024	2,048
RAP máximos	256	512	1,024	2,048
Máximo de dispositivos concurrentes	8,192	16,384	24,576	32,768
VLAN	2,048	4,094	4,094	4,094
Túneles GRE concurrentes (BSSID del sistema)	8,192	8,192	16,384	32,768
Puertos tunelizados concurrentes	4,096	8,192	12,288	16,384
Sesiones concurrentes de IPSec	4,096	16,384	24,576	32,768
Sesiones simultáneas de respaldo SSL	4,096	8,192	8,192	8,192
Sesiones de firewall activo (sesiones concurrentes)	1,000,000	2,015,291	2,015,291	2,015,291
Rendimiento por cable (paquetes grandes)	12 Gbps	20 Gbps	40 Gbps	40 Gbps

Ilustración 107: Especificaciones técnicas de la serie 7200 de Aruba(*)

La documentación técnica completa de la serie 7200 de Aruba se puede descargar, a fecha de redacción de este documento, en:

https://www.securewirelessworks.com/datasheets/Controllers/DS_7200Series.pdf

---

Fuente del texto e imágenes(*): https://www.arubanetworks.com/
Apartado desde el que se referencia este anexo: "2.1.5 Red inalámbrica"

Aruba AirWave

Según *ArubaNetworks*, este es un dispositivo que de manera centralizada es capaz de administrar tanto la infraestructura de cable como la inalámbrica de una organización. Además, es capaz de hacerlo sobre dispositivos Aruba y de otros fabricantes, ofreciendo una gran visibilidad de dispositivos, usuarios y aplicaciones en la red.

La interfaz de usuario centralizada de AirWave proporciona una monitorización en tiempo real de alertas, reportes históricos y localización de fallos de manera rápida y eficiente.

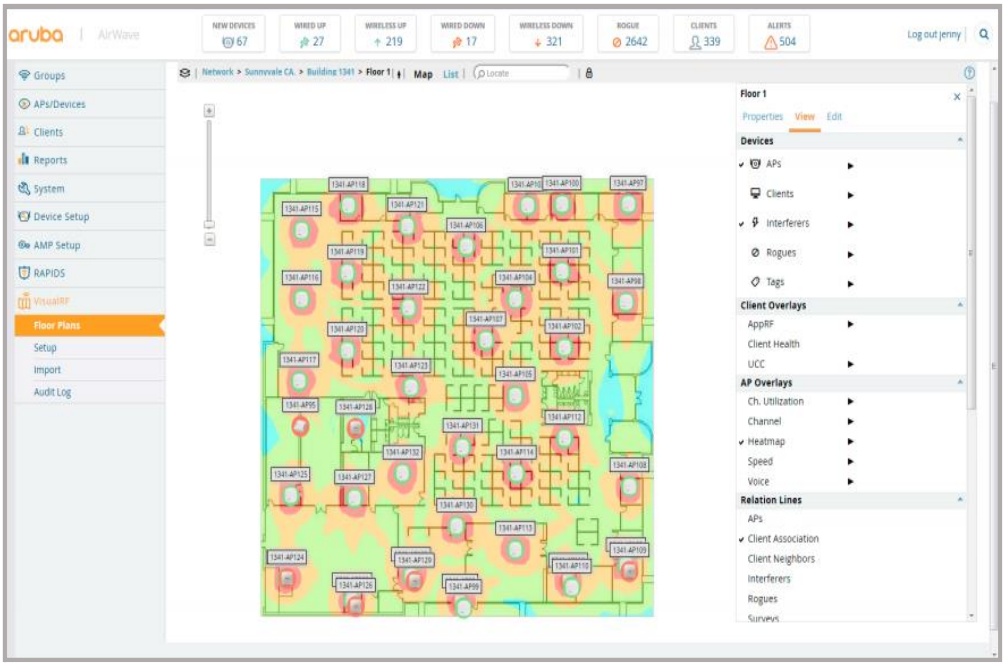


Ilustración 108: Interfaz de usuario de Aruba AirWave(*)

En la Web de Aruba está disponible la documentación referente a AirWave, entre ellas:

- La ficha de datos completa de AirWave de Aruba puede descargarse, a fecha de redacción de este documento, en:

  https://www.arubanetworks.com/assets/ds/DS_AW.pdf

- La guía de instalación de AirWave 8.2.10.1 se puede descargar, a fecha de redacción de este documento, en:

  https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/37098/Default.aspx

---

Fuente texto e imágenes(*): https://www.arubanetworks.com/
Apartado desde el que se referencia este anexo: "2.1.5 Red inalámbrica"

Aruba Mobility Master

Según *ArubaNetworks*, este dispositivo es la siguiente generación de un controlador maestro que se puede desplegar como una máquina virtual o instalar en un equipo basado en arquitectura hardware x86. Además, aseguran que proporciona una inmejorable experiencia de usuario, un despliegue flexible y operaciones simplificadas.

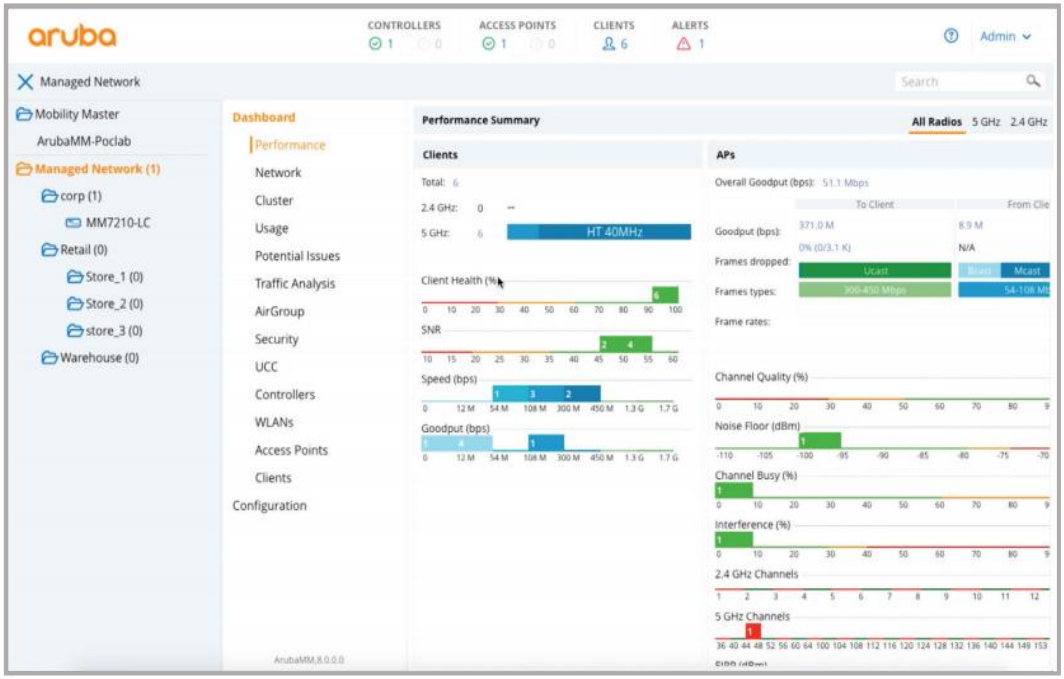


Ilustración 109: Tablero de control de ArubaOS(*)

Así pues, los clientes de Aruba existentes pueden migrar sus configuraciones y licencias de controlador maestro a *Mobility Master* para disfrutar, entre otras, de las siguientes ventajas:

- Una implementación flexible, al poder hacerlo sobre una máquina virtual o un dispositivo hardware (x86)
- Diversas operaciones simplificadas, como:
    - Configuración y visibilidad centralizada
    - Actualizaciones dinámicas
    - Permite múltiples redes seguras utilizando el mismo AP
- Una estabilidad y experiencia de usuario mejorada

La ficha de datos completa de *Aruba Mobility Master* puede descargarse, a fecha de redacción de este documento, en:

https://www.arubanetworks.com/assets/ds/DS_MobilityMaster.pdf

---

Fuente del texto e Imágenes (*): https://www.arubanetworks.com/
Apartado desde el que se referencia este anexo: "2.1.5 Red inalámbrica"

Anexo VI

Arista DCS-7050 series

En la web de arista indican que esta serie consta de conmutadores de 10 G y 40 G con un rendimiento en las capas 2, 3 y 4 que combina una gran velocidad, baja latencia y funciones avanzadas para redes de nube. Desde Arista, añaden que la serie 7050 ofrece una gran versatilidad para diseños de red escalables de dos niveles, incorporando funciones de control del tráfico, monitorización y aprovisionamiento, todo ello con una gran experiencia de usuario. Además, indican que son equipos ideales para:

- Aplicaciones críticas empresariales
- La necesidad de un gran rendimiento de computación
- Infraestructuras con una amplia virtualización en la nube

Ilustración 110: Arista serie 7050SX(*)

En la siguiente tabla se encuentran algunas de las características de los distintos modelos de la serie 7050:

	7050SX-64	7050SX-72Q	7050SX2-72Q	7050SX-128	7050SX2-128
Total de puertos SFP +	48	48	48	96	96
Total de puertos QSFP +	4 4	6 6	6 6	8	8
Max 10G Interfaces	64	72	72	96	96
Max 40G Interfaces	4 4	6 6	6 6	8	8
Latencia	550ns	550ns	550ns	550ns	550ns
Consumo de energía típico	140W	144W	127W	235W	214W

Ilustración 111: Características serie 7050SX Arista(**)

En la Web de Arista está disponible la ficha de datos completa de la serie 7050SX que puede descargarse, a fecha de redacción de este documento, en:

https://www.arista.com/assets/data/pdf/Datasheets/7050SX-128_64_Datasheet_S.pdf

---

Fuente del texto: traducción de la web. https://www.arista.com/en/
Fuente de la Imagen(*) y tabla(**): https://www.arista.com/en/
Apartado desde el que se referencia este anexo: "2.1.6 Red del CPD, conexión con Internet y Azure"

Arista DCS-7020 series

En la web de Arista, indican que la serie 7020R es una solución de alto rendimiento que está diseñada para centros de datos con alto grado de tráfico. Estos conmutadores ofrecen hasta 1.04 Tbps sin bloqueo para funciones de capa 2 y 3. Estos equipos se pueden instalar como servidor de borde o como conmutador de alto rendimiento donde son necesarias características avanzadas para la virtualización de red, monitorización y análisis de red.

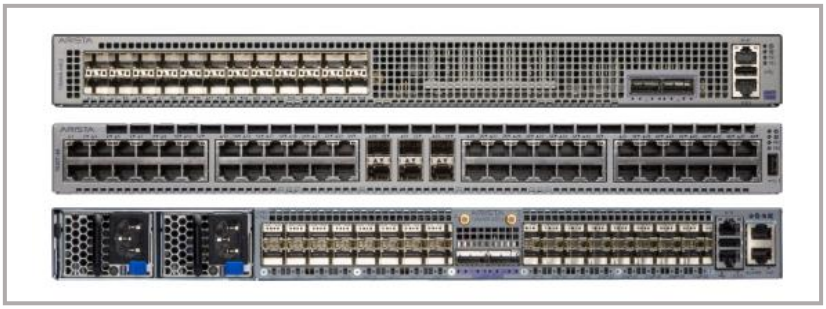


Ilustración 112: Arista serie 7020R(*)

Las características más notables de estos equipos son:

- Alto rendimiento al tener la capacidad de hasta 1,04 Tbps y 300 millones de paquetes por segundo, unicast y multicast, latencia inferior a 3,8us, búfer dinámico de 3Gbytes y un consumo inferior a 2 watios por cada 10 Gbps de rendimiento, que los hace energéticamente muy eficientes.
- Alta escalabilidad y opciones de configuración de puertos: 24, 32 y 48 con velocidades de hasta 100 Gbps. Además, estos equipos admiten la posibilidad de poderlos apilar en columna.

La siguiente tabla muestra las características más destacables:

Característica	Descripción
CloudVision	La automatización del flujo de trabajo en toda la red y la organización de la carga de trabajo como una solución llave en mano para la red en la nube
Amortiguadores profundos dinámicos	3GB de memoria de paquetes por conmutador, eliminando virtualmente las caídas de paquetes en escenarios de congestión
Ruta múltiple de igual costo (ECMP)	Todas las rutas entre el lomo y la hoja se ejecutan activo / activo utilizando protocolos de enrutamiento estándar como BGP y OSPF y ECMP se utiliza para ejecutar todas las rutas en modo activo / activo
Soporte de enrutamiento IPv4 e IPv6	El enrutamiento IPv4 e IPv6 de capa 3 (OSPF, BGP, ISIS y PIM) está disponible en la licencia de enrutamiento mejorado, lo que permite redes de múltiples rutas altamente resistentes
Aprovisionamiento Zero Touch	Con ZTP, un conmutador carga su imagen y configuración desde una ubicación centralizada dentro de la red. Esto simplifica la implementación, permitiendo que los recursos de ingeniería de red se utilicen para tareas más productivas.
Enrutamiento VXLAN de velocidad de cable	Integración perfecta entre entornos VXLAN y L2 / L3, redes físicas y virtualizadas
VPN IPSec	VPN IPSec de sitio a sitio para conexiones seguras entre el centro de datos y los puntos de presencia (solo 7020SR)
Analizador de latencia	Visibilidad en tiempo real de la latencia del puerto y marcas de agua por puerto para proporcionar retroalimentación inmediata y monitoreo de precisión
Virtualización de red amplia	Soporte de API de múltiples proveedores con eAPI, VXLAN y NSX, y otras técnicas de encapsulación
Plano de control de alto rendimiento	CPU de cuatro núcleos y 8 GB de memoria del sistema para admitir tablas de enrutamiento más grandes, vrfs y una convergencia más rápida.

Ilustración 113: Características serie 7020R de Arista(**)

La ficha de datos se encuentra, a fecha de redacción de este documento, en: https://www.arista.com/assets/data/pdf/Datasheets/7020R-48_Datasheet.pdf

---

Fuente del texto: traducción del texto. https://www.arista.com/en/
Fuente de la Imagen(*) y tabla(**): https://www.arista.com/en/
Apartado desde el que se referencia este anexo: "2.1.6 Red del CPD, conexión con Internet y Azure"

A10 Networks

En a10networks.com son conscientes del que el tiempo de inactividad del servicio es costoso. Además, con el incremento de la movilidad y usuarios, las aplicaciones y las infraestructuras asociadas a estas, ya no residen solo en los centros de datos locales de las organizaciones, sino en nubes públicas, privadas e híbridas. Esto obliga a que la gestión del tráfico se tenga que realizar de manera óptima, para ello A10 ofrece una solución de equilibrio de cargas y entrega de aplicaciones.

Ilustración 114: Balanceador de carga de A10(*)

Las soluciones de A10 garantizan que las aplicaciones de una organización sean seguras, consistentes y altamente disponibles en cualquier entorno de múltiples nubes, ofreciendo:

- **Alta disponibilidad y rendimiento**. Mediante un equilibrio de carga avanzado que permite, por un lado, una alta disponibilidad para los servicios de aplicaciones y por otro lado, una gestión dinámica del tráfico para permitir una óptima distribución del servicio demandado o durante los mantenimientos.
- **Seguridad integral de aplicaciones**. Esta característica se realiza de forma centralizada sin tener que realizar cambios en el servidor. Además, cuenta con distintas funciones de seguridad contra malware, ataques DDoS... y firewall de aplicaciones.
- **Despliegue flexible**. Está disponible para nube pública y privada, así como en hardware y software, permitiendo una administración unificada.
- **Análisis**. Ofrece una gran visibilidad en tiempo real por cada aplicación, garantizando a través de instantáneas la resolución eficaz de problemas.

Fuente del texto: traducción del texto. https://www.a10networks.com/
Fuente imagen(*): https://www.insoltec.cl/servicio/balanceadores-de-carga-a10-networks/
Apartado desde el que se referencia este anexo: "2.1.6 Red del CPD, conexión con Internet y Azure"

Anexo VII

Según *Microsoft, ExpressRoute* es un servicio de Azure que permite crear conexiones privadas entre los centros de datos de Microsoft y la infraestructura local de una organización. Una particularidad de *ExpressRoute* es que ofrece una mayor confiabilidad, seguridad y velocidad, con una menor latencia al no realizarse sobre conexiones de Internet público.

Gracias a *ExpressRoute*, una organización puede tener una extensión de su red local hacia la nube de Microsoft mediante una conexión privada y dedicada de un proveedor de comunicaciones.

Microsoft Azure, *Office 365* y *CRM* en línea, son algunos de los servicios de la nube de Microsoft a los que se puede acceder mediante *ExpressRoute*.

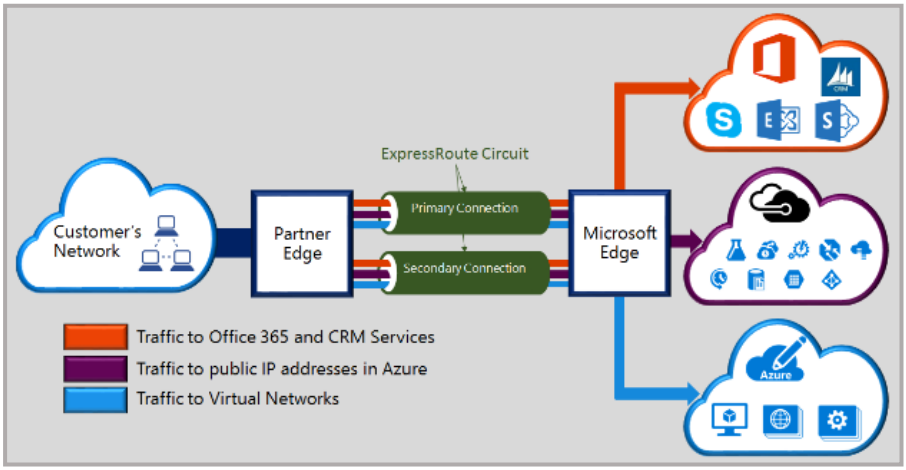


Ilustración 115: Servicios Microsoft Cloud y ExpressRoute(*)

El sitio web de Microsoft ofrece algunas características de *ExpressRoute*:

- **El uso de nube privada virtual para almacenamiento, copia de seguridad y recuperación**. Azure ofrece conexiones confiables con un ancho de banda de hasta 100 Gbps. Este ancho de banda es ideal para: la migración, replicación y recuperación de datos, así como para otras estrategias que requieran de una alta disponibilidad
- **Ampliación y conexión de los centros de datos de una organización**, porque gracias a su alto rendimiento y una mínima latencia hará parecer una extensión del centro de datos local. Esta característica permite un alto escalado a precio de nube pública
- **Creación de aplicaciones híbridas**. Las conexiones de ExpressRoute ofrecen un alto rendimiento tanto para las aplicaciones que se encuentren en local, como en Azure. Además, cuentan con una total privacidad sin que se vea afectado su alto grado de rendimiento

---

Fuente del texto e imagen(*): https://docs.microsoft.com/es-es/
Apartado desde el que se referencia este anexo: "2.1.6 Red del CPD, conexión con Internet y Azure"

Anexo VIII

Cisco Catalyst serie 2960

Según Cisco, la serie 2960 son conmutadores, de coste razonable, para organizaciones empresariales que necesitan escalabilidad, seguridad y unos equipos energéticamente eficientes. Estos equipos disponen de funciones avanzadas de Capa 2 y 3, así como opcionalmente de alimentación a través de Ethernet (PoE+).

Esta serie cuenta con modelos de 24 o 48 puertos Gigabit *Ethernet* y 4 enlaces ascendentes fijos de 1 Gigabit *Ethernet* SPF o 2 enlaces ascendentes fijos de 10 Gigabit Ethernet SFP+. Además, incorporan la tecnología *FlexStack-Plus* que posibilita apilar hasta 8 conmutadores proporcionando mediante una capacidad de hasta 80 Gbps una alta escalabilidad.

Ilustración 116: Cisco Catalyst 2960 series(*)

Las características de capa 3 permiten OSPF, RIP y enrutamiento estático. Algunos modelos disponen de doble fuente redundante u opcionalmente con fuente de alimentación redundante externa reemplazable en caliente.

El documento completo de especificaciones se puede descargar a fecha de redacción de este documento en:

https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/catalyst/pdfs/switches_cisco_catalyst_serie_2960_x.pdf

---

Fuente del texto: https://www.cisco.com/
Fuente imagen(*):https://www.senetic.es/
Apartados desde que se referencia este anexo: "2.2.1.1 Sucursal AGR" - "2.2.3.4 Sucursal LO" - "2.2.3.5 Sucursal PA"

Anexo IX

Aruba serie 3810

Según *ArubaNetworks*, la serie Aruba 3810 son conmutadores avanzados de capa 3 con una baja latencia y con la posibilidad de apilamiento. Además, son aptos para puntos de acceso de alta velocidad con Ethernet multi-gigabit. Estos equipos son una óptima solución, tanto para grandes entornos empresariales, como para sucursales.

Los conmutadores 2930F soportan enrutamiento de acceso OSPF, enrutamiento RIP e IPV6 con una calidad de servicio robusta. Estos conmutadores de 1U proporcionan diferentes configuraciones de puertos RJ45 y SPF+ y con la opción de PoE, así como la posibilidad de incorporar fuentes de alimentación redundadas.

Ilustración 117: Aruba serie 3810(*)

El documento completo de especificaciones se puede descargar, a fecha de redacción de este documento, en:

https://www.arubanetworks.com/es/productos/productos-de-red/switches/serie-3810/

Fuente del texto e imagen(*): https://www.arubanetworks.com/
Apartados desde los que se referencia este anexo: "2.2.1.2 Sucursal AL" – "2.2.3.1 Sucursal TA" - "2.2.3.3 Sucursal SPM"

Anexo X

HPE serie 5130

Según *Hewlett Packard Enterprise***,** esta serie conmutadores dispone de las siguientes características:

Conmutadores de nivel de acceso seguros y escalables al ofrecer flexibilidad y escalabilidad para entornos empresarias medianos y grandes. Este equipo es compatible con puertos de 10GbE fijos, enrutamiento estático de capa 3 y RIP en sus versiones 1 y 2, PoE+, ACL, IPv6 y con una alta eficiencia energética.

Con *Intelligent Resilient Fabric* (IRF) virtualiza hasta nueve conmutadores físicos en un único dispositivo lógico. Además, incluye funciones de red definida por software.

Mejora de la calidad de servicio con la gestión del tráfico pues admite QoS avanzada que clasifica y dirige el tráfico mediante diversos criterios basados en la información de nivel 2 y 3 como: establecimiento de prioridad y limitación de velocidad para determinado tráfico y puerto, VLAN o conmutador completo.

Control de seguridad completa pues es compatible con los métodos de autenticación más habituales como: 802.1X, MAC y ACL. Además, incluye seguridad con cifrado de acceso a través de SSHv2, SSL y SNMPv3.

Vista única de la red al poder gestionar con *Intelligent Management Center* (ICM) la red de extremo a extremo mediante una gestión integral de políticas.

Ilustración 118: HPE serie 5130(*)

En la siguiente dirección web, a fecha de redacción de este trabajo, se puede encontrar información adicional sobre la serie 5130 de HPE:

https://buy.hpe.com/mx/es/networking/networking-switches/hpe-flexnetwork-5130-ei-switch-series/p/7399420

Fuente del texto e imagen(*): https://buy.hpe.com/us/en
Apartado desde el que se referencia este anexo: "2.2.2.1 Sucursal FMyF"

Anexo XI

Se adjunta copia del documento donde figura el presupuesto emitido por la comercial de Citrix y que incluye los distintos costes de los gateways SD-WAN, así como su licenciamiento y mantenimiento.

CITRIX®

Suggested License Program Pricing for Universidad

Date: 4/28/2020
Reference Number: Q-01162775

End User Org ID	**35758500**	**Sales Exception Number**	**-**
End User Name	**Universidad**	**Proposal Expires**	**6/30/2020**
End User Contract Number		**Citrix Sales Person**	
Current Contract Level	**GELA-1**	**Description/Comments**	
Calculated Contract Level	**GELA-1**	**Maintenance Compliance**	
		Maintenance Quantity Failures	

Products:

								Standard Conditions		
SKU	**Product Description**	**Quantity**	**Quote Term**	**Co Term End Date (If Applicable)**	**No of Months (If Applicable)**	**SRP (EUR)**	**Extended SRP (EUR)**	**End User Discount %**	**End User Unit Cost (EUR)**	**End User Total Cost (EUR)**
3017618-G1	*Citrix Zero-Capacity SD-WAN 2100 Z Standard Edition*	*2*			*0*	*3,379.63*	*6,759.26*	*0.00*	*3,379.63*	*6,759.26*
4060209-G1	*3 Year Silver Citrix ZeroCapacity SDWAN 2100 Z Standard Edition*	*1*			*0*	*1,095.11*	*1,095.11*	*0.00*	*1,095.11*	*1,095.11*
3017817-G1	*Citrix SD-WAN 2100 Standard Edition 1 Gbps 3 year Subscription with Orchestrator*	*1*			*0*	*33,604.28*	*33,604.28*	*40.00*	*20,162.57*	*20,162.57*
3017816-G1	*Citrix SD-WAN 2100 Standard Edition 500 Mbps 3 year Subscription with Orchestrator*	*1*			*0*	*25,085.20*	*25,085.20*	*40.00*	*15,051.12*	*15,051.12*
3017616-G1	*Citrix Zero-Capacity SD-WAN 4100 Z Standard Edition*	*2*			*0*	*7,685.19*	*15,370.38*	*0.00*	*7,685.19*	*15,370.38*
4054832-G1	*3 Year Gold Maintenance Citrix Zero-Capacity SD-WAN 4100 Z Standard Edition*	*2*			*0*	*3,652.00*	*7,304.00*	*0.00*	*3,652.00*	*7,304.00*
3017813-G1	*Citrix SD-WAN 4100 Standard Edition 2 Gbps 3 year Subscription with Orchestrator*	*2*			*0*	*46,169.73*	*92,339.46*	*40.00*	*27,701.84*	*55,403.68*
3017321-G1	*Citrix SD-WAN VPX 500-Standard Edition (500Mbps) Virtual Appliance*	*1*			*0*	*14,629.63*	*14,629.63*	*40.00*	*8,777.78*	*8,777.78*
3027764-G1	*Citrix SD-WAN VPX Standard Edition 500 Mbps 3 year Orchestrator Add-On Subscription*	*1*			*0*	*1,302.58*	*1,302.58*	*40.00*	*781.55*	*781.55*
4050617-G1	*CSS Select Citrix SD-WAN VPX 500-Standard Edition (500Mbps) Virtual Appliance 3 Years*	*1*			*0*	*9,655.56*	*9,655.56*	*40.00*	*5,793.34*	*5,793.34*
3022640-G1	*Citrix SD-WAN 210 Zero Capacity Standard/Advanced Appliance*	*1*			*0*	*388.89*	*388.89*	*0.00*	*388.89*	*388.89*
4059931-G1	*3 Years Silver Maintenance Citrix SD-WAN 210-Z-SE Zero Capacity Standard Edition Appliance*	*1*			*0*	*143.73*	*143.73*	*0.00*	*143.73*	*143.73*
3027149-G1	*Citrix SD-WAN 210 Standard Edition 200 Mbps 3 year Subscription with Orchestrator*	*1*			*0*	*5,533.85*	*5,533.85*	*40.00*	*3,320.31*	*3,320.31*
							TOTAL CUSTOMER PRICE:		**140,351.72**	

Disclaimer:

This is not an offer or a price commitment. Citrix does not control reseller prices or discounts. Please contact your authorized Citrix reseller for a binding price quotation. This document may contain errors. These suggested prices exclude any applicable customs, taxes, shipping or other local country fees. Unscheduled changes may take up to 24 hours to be reflected on the price list.

Payments into a bank account of Citrix Systems International GmbH on or after 23 January 2016 will be deemed to be a payment to Citrix Systems UK Limited. Orders placed on Citrix Systems International GmbH on or after 23 January 2016 will be deemed to be an order placed on Citrix Systems UK Limited.

Ilustración 119: Presupuesto Citrix

Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Anexo XII

Se adjunta copia de las páginas del documento "*Citrix SD-WAN Data Sheet*", donde se encuentran las especificaciones técnicas del equipamiento SD-WAN de Citrix y que a fecha de redacción de este documento se puede descargar en la siguiente dirección:

https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf

CITRIX

Data Sheet

Citrix SD-WAN Data Sheet

Citrix SD-WAN (formerly NetScaler SD-WAN) is a next-generation WAN Edge solution that simplifies digital transformation for enterprises. It offers the best application experience for SaaS, cloud, and virtual apps & desktops; comprehensive security; and cloud choice with automation to ensure an always-on workspace.

Why Citrix SD-WAN?

- Ability to detect, classify and accelerate over 4,500 SaaS, cloud, and virtual applications and sub applications
- Integrated branch security with options for next-generation firewall and cloud-based secure web gateway
- Real-time, packet-based traffic handling routes traffic on the most optimal links
- Traffic shaping and bi-directional QoS on diverse, bonded links to optimize performance
- Sub-second failover ensures the highest network resiliency
- Integration with Citrix Virtual Apps and Desktops for automated fine-grained QoS and deep visibility into HDX/ICA traffic

Citrix SD-WAN Features

Application Control

Citrix SD-WAN includes an industry-leading Application Control Engine with deep packet inspection, providing:

- Detection, classification, and acceleration of over 4,500 SaaS, cloud, and virtual applications and sub applications.
- The best application experience through real-time, packet-based path selection and bi-directional QoS.
- The highest network resiliency through sub-second failover.
- Deployment on any public cloud or in conjunction with SaaS applications.

Dynamic Routing

- Inserts services into networks easily through either inline or edge routed modes.
- Provides an alternative to the legacy edge router, enabling a simpler branch network with lower infrastructure and support costs.
- Creates multiple software-defined network overlays and applies separate policies and security rules to each.

Virtualized WAN

- Bonds diverse network links, including MPLS, broadband, and 4G/LTE.
- Monitors latency, jitter, congestion and loss in real time and performs intelligent load balancing to match applications to optimal WAN links.
- Uses selective packet replication for real-time and other latency-sensitive applications to ensure consistent experience.

Integrated, Automated Security

- A built-in, application-aware stateful firewall integrates with application QoS to allow centrally-defined security policies to limit or reject application traffic.
- Zone-based segmentation segregates users and traffic, while maintaining policies specific to each group.

Citrix.com 1

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

- Optionally, next-generation firewall capabilities can be added as a VNF (virtualized network function) on select SD—WAN appliances.
- Strong encryption using HTTPS/TLS and AES 256 provides security across the control and data planes.
- The creation of highly available IPsec tunnels can be automated from the branch to Zscaler Secure Internet Gateway or Palo Alto Networks Prisma Access to simplify operations.

Enterprise-Grade Access On-ramp to Cloud/SaaS

Citrix SD-WAN Cloud Direct service enables resilient, high performance access from SD-WAN sites to thousands of SaaS, UCaaS, and one-hundred fifty cloud exchanges.

- Turnkey service that deploys in minutes, centrally managed with real-time visibility.
- Intelligently load balances and QoS optimizes up to four Internet links into redundant carrier-grade points-of-presence (PoPs), with "hit-less" failover.
- "Hit-less" failover mitigates internet circuit outages and even those difficult-to-detect brown-out conditions without disrupting any applications: CRM, ERP, UCaaS, virtual desktop sessions, and more.
- PoPs are interconnected via a high-speed, fully redundant global IP network, and directly peered to over 1,000 SaaS platforms and 150 major network and cloud exchanges.

WAN Optimization

- TCP optimization, compression, data deduplication, and protocol optimization further help improve application experience while reducing bandwidth expenses.

Management and Visibility

Citrix SD-WAN Orchestrator, a SaaS-based provisioning and management solution enables customers and partners to:

- Centrally manage and monitor users, permissions, applications, and WAN links for control and visibility across the entire network.
- Quickly and easily deploy new sites on the network with zero touch deployment.
- Automate the setup of cloud services, security, and applications.
- Monitor and optimize the quality of experience for applications.

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Standard Edition Appliances

Appliance	6100 SE††			5100 SE		
Model	6100-4000-SE	6100-5000-SE	6100-6000-SE	5100-4000-SE	5100-5000-SE	5100-6000-SE
Total Encrypted Throughput[1]	8 Gbps	10 Gbps	12 Gbps	8 Gbps	10 Gbps	12 Gbps
Max Virtual Paths (Static/Dynamic)	1000	1000	1000	550/32	550/32	550/32

Appliance	4100 SE		2100 SE			
Model	4100-2000-SE	4100-3000-SE	2100-0300-SE	2100-0500-SE	2100-1000-SE	2100-2000-SE
Total Encrypted Throughput[1]	4 Gbps	6 Gbps	600 Mbps	1 Gbps	2 Gbps	4 Gbps
Max Virtual Paths (Static/Dynamic)	550/32	550/32	256/32	256/32	256/32	256/32

Appliance	1100 SE		
Model	1100-200-SE	1100-300-SE	1100-500-SE
Total Encrypted Throughput[1]	400 Mbps	600 Mbps	1 Gbps
Max Virtual Paths (Static/Dynamic)	64/32	64/32	64/32
Third-party Firewall as VNF*	Yes	Yes	Yes
Supports Citrix SD-WAN Cloud Direct	Yes	Yes	Yes

Appliance	210 SE/210 LTE (R1/R2/RC)				
Model	210-020-SE	210-050-SE	210-100-SE	210-200-SE	210-300-SE
Total Encrypted Throughput[1]	40 Mbps	100 Mbps	200 Mbps	400 Mbps	600 Mbps
Max Virtual Paths (Static/Dynamic)	16/4	16/4	16/4	16/4	16/4
Supports Citrix SD-WAN Cloud Direct	Yes	Yes	Yes	Yes	No

Appliance	110 SE/110 LTE WiFi† SE		
Model	110-20-SE	110-50-SE	110-100-SE
Total Encrypted Throughput[1]	40 Mbps	100 Mbps	200 Mbps
Max Virtual Paths (Static/Dynamic)	8/4	8/4	8/4

[1] Total encrypted throughput refers to total amount of bandwidth that the appliance model is licensed for, both upstream and downstream, and is based on AES-128 encryption.
* Palo Alto Networks Next Generation Firewall (NGFW) can be hosed as VNF on Citrix SD-WAN 1100 SE.
† Starting 1Q 2020, 110-LTE-Wifi will be shipped as "Wi-Fi Ready." The Wi-Fi feature will ready to use in 2Q and will require a software upgrade.
†† 6100 SE can support 1000 nodes per RCN starting 11.1.0 release and only for deployments with Orchestrator. Deployments with SD-WAN Center will only be able to support 550 nodes per RCN.

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Standard Edition Virtual & Cloud Appliances						
Appliance	**VPX SE**					
Model	VPX-020-SE	VPX-050-SE	VPX-100-SE	VPX-200-SE	VPX-500-SE	VPX-1000-SE
Total Encrypted Throughput[1]	40 Mbps	100 Mbps	200 Mbps	400 Mbps	1 Gbps	2 Gbps
Max Virtual Paths (Static/Dynamic)	8	16	16	16	16	16
Hypervisor Support[2]						
Citrix Hypervisor	Citrix Hypervisor 6.5 SP1					
VMware	ESX/ESXi 5.5, 6.0 & 6.5	ESX/ESXi 5.5, 6.0 & 6.5	ESX/ESXi 5.5, 6.0 & 6.5	ESX/ESXi 6.0 & 6.5	ESX/ESXi 6.0 & 6.5	ESX/ESXi 6.0 & 6.5
HyperV	2012 R2					
KVM	Ubuntu 16.04					
Processor	Dual core Intel VTx2	Dual core Intel VTx2	Dual core Intel VTx2	Quad core Intel VTx2	Quad core Intel VTx2	Quad core Intel VTx2
Memory	4 GB	4 GB	4 GB	4 GB	8 GB	8 GB
Virtual CPU	2vCPU @ 2.7 GHz	2vCPU @ 2.7 GHz	2vCPU @ 2.7 GHz	4vCPU @ 2.7 GHz	8vCPU @ 2.7 GHz	8vCPU @ 3.0 GHz
Cloud Support[3]						
AWS	m4.2xlarge	m4.2xlarge	m4.2xlarge	m4.2xlarge	c4.2xlarge	c4.2xlarge
Azure	D3_v2	D3_v2	D3_v2	D3_v2	D3_v2	D4_v2
GCP	N1-standard-4	N1-standard-4	N1-standard-4	N1-standard-4	-	-
Appliance	**VPX-L SE**					
Model	VPX-L 020-SE	VPX-L 050-SE	VPX-L 100-SE	VPX-L 200-SE	VPX-L 500-SE	VPX-L 1000-SE
Total Encrypted Throughput[1]	40 Mbps	100 Mbps	200 Mbps	400 Mbps	1 Gbps	2 Gbps
Max Virtual Paths (Static/Dynamic)	128	128	128	128	128	128
Hypervisor Support[2]						
Citrix Hypervisor	Citrix Hypervisor 6.5 SP1					
VMware	ESX/ESXi 5.5, 6.0 & 6.5	ESX/ESXi 5.5, 6.0 & 6.5	ESX/ESXi 5.5, 6.0 & 6.5	ESX/ESXi 6.0 & 6.5	ESX/ESXi 6.0 & 6.5	ESX/ESXi 6.0 & 6.5
HyperV	2012 R2					
KVM	Ubuntu 16.04					
Memory	16 GB	16 GB	16 GB	16 GB	16 GB	16 GB
Virtual CPU	16vCPU @ 2.7 GHz	16vCPU @ 2.7 GHz	16vCPU @ 2.7 GHz	16vCPU @ 2.7 GHz	16vCPU @ 2.7 GHz	16vCPU @ 2.7 GHz
Cloud Support[3]						
AWS	m4.4xlarge	m4.4xlarge	m4.4xlarge	m4.4xlarge	m4.4xlarge	m4.4xlarge
Azure	F8	F8	F8	F8	F8	F16
GCP	N1-standard-4	N1-standard-4	N1-standard-4	N1-standard-4	-	-

[1] Total encrypted throughput refers to total amount of bandwidth that the appliance model is licensed for, both upstream and downstream, and is based on AES-128 encryption.
[2] The VPX images are qualified to run on Intel processors only.
[3] Cloud server types are the minimum recommended server size to support the listed performance numbers for each model.

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Software Features	
Application Performance	Per packet/app steering, Packet duplication, Packet retransmissions, Dual-ended QoS, Application QoE, Per-app business policies for over 4000 apps, Citrix HDX/ICA integration
Authentication	Local database, RADIUS, TACACS+
Virtual Instance on Public Cloud (IaaS)	Azure, Amazon Web Services, Google Cloud Platform, Oracle Cloud Infrastructure
Configuration	Zero touch deployment service, GUI, Customizable dashboards & templates, REST API
Deployment	In-line overlay, One-armed overlay, Edge gateway, Cloud
High Availability	Parallel Inline HA, Fail-to-Wire HA, One-arm HA, VRRP, Geo-redundant HA (with the MCN)
Layer 2	VLAN (802.1Q), Bridging, SVI, PPPoE
Link Management	Transport Agnostic, Bi-directional link monitoring, Link bonding, Metered links, Standby links, Link of Last Resort
Manageability	SD-WAN Cloud Orchestrator, On-premise SD-WAN Center, SD-WAN Center in AWS and Azure, CLI, SNMP V3, DHCP Server/Relay/ Client, DNS Forwarder, Syslog, NetFlow, IPFIX, REST API
Mobile Broadband	3G/4G/LTE, Zero touch deployment over LTE, Authentication types: PAP/CHAP/PAPCHAP, SIM lock/unlock, Support for antenna extenders
Network Encryption	128 bit AES, 256 bit AES, IPSec
QoS	Scheduling, Shaping, Classification, Remarking, HDX AutoQoS
Routing	eBGP, iBGP, OSPF, Static, Multicast
SaaS	Optimized Office 365 Breakout, Optional Citrix SD-WAN Cloud Direct Service
Security (Cloud)	Zscaler, Palo Alto Prisma Access (Formerly Palo Alto GPCS)
Security (On-Prem)	L4-7 Application Firewall, NAT, Secure Web Gateway connectivity, ICSA Labs certified, FIPS compliant, Palo Alto Networks Next-Gen Firewall as VNF (1100-SE only)
Tunnel Interfaces	GRE, IPSec, Citrix Virtual Path

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Premium Edition Appliances

Appliance	5100 PE		2100 PE		
Model	5100-3000-PE	5100-4000-PE	2100-300-PE	2100-500-PE	2100-1000-PE
Total Encrypted Throughput[4]	6 Gbps	8 Gbps	600 Mbps	1 Gbps	2 Gbps
Max Virtual Paths (Static/Dynamic)	550/32	550/32	256/32	256/32	256/32
Optimized Application Capacity[5,6]	500 Mbps	500 Mbps	50 Mbps	100 Mbps	100 Mbps
Maximum HDX CCUs[7]	750	750	300	300	300
Maximum Accelerated TCP Sessions[8]	60,000	60,000	20,000	20,000	20,000

Appliance	1100 PE		
Model	1100-200-PE	1100-300-PE	1100-500-PE
Total Encrypted Throughput[4]	400 Mbps	600 Mbps	1 Gbps
Max Virtual Paths (Static/Dynamic)	64/32	64/32	64/32
Optimized Application Capacity[5,6]	10 Mbps	20 Mbps	50 Mbps
Maximum HDX CCUs[7]	100	300	300
Maximum Accelerated TCP Sessions[8]	10,000	10,000	10,000

[4] Total encrypted throughput refers to total amount of bandwidth that the appliance model is licensed for, both upstream and downstream, and is based on AES-128 encryption.
[5] Only outbound WAN traffic is counted against the licensed bandwidth. Inbound QoS and/or unaccelerated traffic does not count against the licensed bandwidth. Total inbound optimizable traffic should not exceed this threshold.
[6] Some protocols (ICA, for example) can limit the processing capacity of the appliance before the licensed bandwidth is reached.
[7] User count is based upon a medium-level workload as defined by Login VSI and Virtual Desktops/Apps advanced encryption security. User count is limited by link bandwidth and TCP session counts. No user count is enforced. Published numbers are for guidance purposes only.
[8] TCP session count will be reduced by active HDX sessions. No session count is enforced. Published numbers are for guidance purposes.

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

WANOP Edition Appliances

Appliance	5100 WANOP		4100 WANOP		
Model	5100-1500-WO	5100-2000-WO	4100-310-WO	4100-500-WO	4100-1000-WO
Optimized WAN Capacity[9,10]	1.5 Gbps	2 Gbps	310 Mbps	500 Mbps	1 Gbps
QoS/Unaccelerated Throughput Limit[9]	2 Gbps	4 Gbps	500 Mbps	1 Gbps	2 Gbps
Maximum HDX CCUs[11]	3,500	5,000	750	1,200	2,500
Maximum Accelerated TCP Sessions[12]	120,000	160,000	40,000	60,000	120,000
Concurrent Citrix SD-WAN Client Plug-ins	3,600	4,800	1,100	1,800	3,600
Video Caching					
WCCP Clustering	•	•	•	•	•
Networking Cloud Connector	•	•	•	•	•
Group Mode					

Appliance	3000 WANOP			2000 WANOP		
Model	3000-050-WO	3000-100-WO	3000-155-WO	2000-010-WO	2000-020-WO	2000-050-WO
Optimized WAN Capacity[9,10]	50 Mbps	100 Mbps	155 Mbps	10 Mbps	20 Mbps	50 Mbps
QoS/Unaccelerated Throughput Limit[9]	500 Mbps	500 Mbps	500 Mbps	200 Mbps	200 Mbps	200 Mbps
Maximum HDX CCUs[11]	300	400	500	100	200	300
Maximum Accelerated TCP Sessions[12]	50,000	50,000	50,000	20,000	20,000	20,000
Concurrent Citrix SD-WAN Client Plug-ins	750	1,000	1,200	100	200	750
Video Caching	•	•	•	•	•	•
WCCP Clustering	•	•	•	•	•	•
Networking Cloud Connector						
Group Mode	•	•	•	•	•	•

Appliance	1000 WANOP			800 WANOP		
Model	1000-006-WO	1000-010-WO	1000-020-WO	800-002-WO	800-006-WO	800-010-WO
Optimized WAN Capacity[9,10]	6 Mbps	10 Mbps	20 Mbps	2 Mbps	6 Mbps	10 Mbps
QoS/Unaccelerated Throughput Limit[9]	50 Mbps	50 Mbps	50 Mbps	50 Mbps	50 Mbps	50 Mbps
Maximum HDX CCUs[11]	60	100	200	20	60	100
Maximum Accelerated TCP Sessions[12]	10,000	10,000	10,000	10,000	10,000	10,000
Concurrent Citrix SD-WAN Client Plug-ins	-	-	-	-	-	-
Video Caching	•	•	•	•	•	•
WCCP Clustering	•	•	•	•	•	•
Networking Cloud Connector						
Group Mode	•	•	•	•	•	•

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

WANOP Edition Virtual Appliances

Appliance	VPX						
Model	VPX 2-WO	VPX 6-WO	VPX 10-WO	VPX 20-WO	VPX 50-WO	VPX 100-WO	VPX 200-WO
Optimized WAN Capacity[9,10]	2 Mbps	6 Mbps	10 Mbps	20 Mbps	50 Mbps	100 Mbps	200 Mbps
QoS/Unaccelerated Throughput Limit	15 Mbps	50 Mbps	75 Mbps	150 Mbps	250 Mbps	250 Mbps	300 Mbps
Maximum HDX CCUs[11]	20	60	100	200	300	400	500
Maximum Accelerated TCP Sessions[12]	5,000	5,000	5,000	10,000	10,000	20,000	30,000
Concurrent Citrix SD-WAN Client Plug-ins	20	60	100	200	300	400	500
Video Caching	•	•	•	•	•		
WCCP Clustering					•	•	•
Networking Cloud Connector[13]	•	•	•	•	•	•	•
Group Mode							
Hypervisor	Citrix Hypervisor 5.5-6.2, Hyper-V 2008 R2SP1 - 2012, ESX/ESXi 4.1-6.0						
Processor	Dual core (Quad core recommended) Intel VTx or AMD-V 64-bit x86[14]						
Memory	6 GB					8 GB	16 GB
Virtual CPU	1x Citrix Hypervisor & 2x VMware vSphere (>2.33 GHz)	2-4x Citrix Hypervisor, Hyper-V & VMware vSphere (>2.33 GHz)					2-4x Citrix Hypervisor, Hyper-V & VMware vSphere (~3.0 GHz)
Hard Drive[15]	100 GB	100 GB	250 GB	250 GB	250 GB	500 GB	500 GB
Network Interface	2 Virtual NICs						

[9] Total encrypted throughput refers to total amount of bandwidth that the appliance model is licensed for, both upstream and downstream, and is based on AES-128 encryption.
[10] Some protocols (ICA, for example) can limit the processing capacity of the appliance before the licensed bandwidth is reached.
[11] User count is based upon a medium-level workload as defined by Login VSI and Virtual Desktops/Apps advanced encryption security. User count is limited by link bandwidth and TCP session counts. No user count is enforced. Published numbers are for guidance purposes only.
[12] TCP session count will be reduced by active HDX sessions. No session count is enforced. Published numbers are for guidance purposes.
[13] For Citrix SD-WAN appliances, the Citrix Networking Cloud Connector is delivered as a separate software appliance.
[14] The VPX images are qualified to run on Intel processors only.
[15] For best performance, use solid state drives or high IOPs storage devices.

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Hardware Specifications

Appliance	6100 SE	5100 SE/PE	5100 WO	4100 SE	4100 WO	3000 WO
Model						
Total Disk Space[16]	480 GB (SSD)	2 TB (SSD)	6.8 TB (HDD)	2 TB (SSD)	5.2 TB (HDD)	2.4 TB (SSD)
Compression History (SSD)	SE: N/A	SE: N/A PE: 2.8 TB	4.3 TB	N/A	2.8 TB	1.5 TB
RAM	256 GB	128 GB	128 GB	96 GB	96 GB	32 GB
Network Interfaces[17]						
Fail-to-wire	4x 10GBase-SR 4x 1000Base-TX	4x 10GBase-SR	4x 10GBase-SR	2x 10GBase-SR 4x 1000Base-TX	2x 10GBase-SR 4x 1000Base-TX	6x 1000Base-TX
Non Fail-to-wire	4x 10G SFP+	4x 10G SFP+	4x 10G/1G SFP+	4x 10G SFP+	4x 10G/1G SFP+	-
Management	2x 1000Base-TX	2x 1000Base-TX	2x 1000Base-TX	2x 1000Base-TX	2x 1000Base-TX	2x 1000Base-TX
Mechanical						
Rack Units	2U (3.5 inches/8.90 cm)					1U (1.75 in/4.45 cm)
Rack Options	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets					
System Depth	28 inches (72 cm)					24 in (63.5 cm)
System Weight	60 lbs (27.2 kg)					33 lbs (15 kg)
Shipping Dimensions	36.5" x 24.5" x 11"					32" x 23.5" x 7.5" (81.5 x 59.7 x 19.1 cm)
Shipping Weight	69 lbs (31.3 kg)					40 lbs (18.1 kg)
Power, Environmental, and Regulatory						
Power Supplies	Dual Redundant, Hot Swappable					Single (Optional Dual Redundant)
Wattage (Max)	1000W					450W (900W with redundant PSU)
Input Voltage/Frequency Ranges	100-240 VAC, 47-63 Hz					100-240 VAC, 50-60 Hz
Input Current	5.5-2.8 A	9.0-4.5 A	9.0-4.5 A	7.0-3.5 A	7.0-3.5 A	2.5-1.0 A
Operating Temperature	32-114°F (0-45°C)	32-104°F (0-40°C)				
Operating Altitude	0-16,000 ft (0-5,000 M)					
Storage Temperature	14°F-140°F (-10°C-60°C)					
Allowed Relative Humidity	5%-95%, Non-condensing	20%-80%, Non-condensing				5%-95%, Non-condensing
Safety Certifications	CSA					UL, TUV-C
Electromagnetic Emissions, Safety, & Environmental	FCC (Part 15 Class A), CCC, KCC, NOM, CITC, EAC, MoC, CE, VCCI, RCM, Anatel, BSMI, NTRA					
Environmental Compliance	ROHS, WEEE					
Citrix Compliance Regulatory Model	2U1P1A	2U1P1D	2U1P1D	2U1P1B	2U1P1B	NS 6xSFP 6xCU

[16] Models using HDD (Hard Disk Drive) and SSD (Solid State Drive) are indicated accordingly.
[17] Published Ethernet interfaces compliant per IEEE802.3-2002/2005/2008/2012.

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Hardware Specifications

Appliance	2100 SE/PE	2000 WO	1100 SE/PE	1000 WO	800 WO
Model					
Total Disk Space[16]	720 GB (SSD)	600 GB (SSD)	480 GB (SSD)	300 GB (SSD)	240 GB (SSD)
Compression History (SSD)	SE: N/A PE: 480 GB	275 GB	SE: N/A PE: 148 GB	148 GB	80 GB
RAM	32 GB	32 GB	24 GB	24 GB	8 GB
Network Interfaces[17]					
Fail-to-wire	4x 1000Base-TX	4x 1000Base-TX	4x 10/100/1000 Base-TX	4x 1000Base-TX	4x 1000Base-TX
Non Fail-to-wire	4x 1GE SFP	4x 1GE SFP	2x 10/100/1000 Base-TX, 2x Flexible Ports (SFP or 10/100/1000 Base-TX), 2x POE	-	-
Management	1x 1000Base-TX	1x 1000Base-TX	1x 1000Base-TX	2x 1000Base-TX	2x 1000Base-TX
Mechanical					
Rack Units	1RU (1.75 inches/4.45 cm)				
Rack Options	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets				
System Depth	24 in (63.5 cm)	24 in (63.5 cm)	9.9 in (25 cm)	10.5 in (26.7 cm)	10.5 in (26.7 cm)
System Weight	26 lbs (11.8 kg)	32 lbs (14.6 kg)	4.5 lbs (2.04 kg)	8 lbs (3.63 kg)	8 lbs (3.63 kg)
Shipping Dimensions	32" x 23.5" x 7.5" (81.5 x 59.7 x 19.1 cm)	32" x 23.5" x 7.5" (81.5 x 59.7 x 19.1 cm)	13.66" x 12.75" x 7.48" (34.69 x 32.38 x 18.99 cm)	26" x 18.5" x 6.5" (66.04 x 47 x 16.51 cm)	26" x 18.5" x 6.5" (66.04 x 47 x 16.51 cm)
Shipping Weight	40 lbs (18.1 kg)	39 lbs (17.8 kg)	7.5 lbs (3.4 kg)	14.0 lbs (6.35 kg)	14.0 lbs (6.35 kg)
Power, Environmental, and Regulatory					
Power Supplies	Single (Optional Dual Redundant)	Single	Single (Optional Dual Redundant)	Single	Single
Wattage (Max)	450W	300W	96.8W	200W	200W
Input Voltage/Frequency Ranges	3.4-1.7A	1.5-0.6A	2A	2.6A Max	2.6A Max
Input Current	5.5-2.8 A	9.0-4.5 A	9.0-4.5 A	7.0-3.5 A	7.0-3.5 A
Operating Temperature	32-104°F (0-40°C)				
Operating Altitude	0-16,000 ft (0-5,000 M)	0-6,500 ft (0-2,000 M)	0-16,000 ft (0-5,000 M)	0-6,500 ft (0-2,000 M)	0-6,500 ft (0-2,000 M)
Storage Temperature	14°F-140°F (-10°C-60°C)		-4°F-140°F (-20°C-60°C)		
Allowed Relative Humidity	20%-80%, Non-condensing	5%-95%, Non-condensing			
Safety Certifications	CSA	UL, TUV-C	UL	UL, TUV-C	UL, TUV-C
Electromagnetic Emissions, Safety, & Environmental	FCC (Part 15 Class A), CCC, KCC, FCC (Part 15, Class B) for 1100 SE/PE only, NOM, CITC, EAC, MoC, CE, VCCI, RCM				
Environmental Compliance	ROHS, WEEE				
Citrix Compliance Regulatory Model	1U1P1A	NS 6xCu	SDW-1100	CB504-2	CB504-2

[16] Models using HDD (Hard Disk Drive) and SSD (Solid State Drive) are indicated accordingly.
[17] Published Ethernet interfaces compliant per IEEE802.3-2002/2005/2008/2012.

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Hardware Specifications		
Appliance	**210 SE**	**210 LTE SE (R1/R2/RC)**
Model		
Total Disk Space[16]	64 GB (mSATA)	64 GB (mSATA)
Compression History (SSD)	N/A	N/A
RAM	4 GB	4 GB
Network Interfaces[17]		
Fail-to-wire	1x 10/100/1000 Ethernet with Bypass RJ45	1x 10/100/1000 Ethernet with Bypass RJ45
Non Fail-to-wire	1x 10/100/1000 Ethernet RJ45, 2x Flexible ports (10/100/1000 Ethernet RJ45 or 1GE SFP)	1x 10/100/1000 Ethernet RJ45, 2x Flexible ports (10/100/1000 Ethernet RJ45 or 1GE SFP)
Management	1x 10/100/1000 RJ45	1x 10/100/1000 RJ45
Integrated LTE	-	1x LTE Modem[18]
Mechanical		
Rack Units	1RU (1.75 inches/4.45 cm)	
Rack Options	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets	
System Depth	6.9 in (17.53 cm)	6.9 in (17.53 cm)
System Weight	2.75 lbs (1.25 kg)	3.15 lbs (1.42 kg)
Shipping Dimensions	17.5" X 12" X 2.75" (44.5 x 30.5 x 7.0 cm)	17.5" X 12" X 2.75" (44.5 x 30.5 x 7.0 cm)
Shipping Weight	4.6 lbs (2.09 kg)	5.0 lbs (2.27 kg)
Power, Environmental, and Regulatory		
Power Supplies	Single	Single
Wattage (Max)	45W External	45W External
Input Voltage/Frequency Ranges	100-240 VAC, 47-63 Hz	100-240 VAC, 47-63 Hz
Input Current	4.0-2.1A	4.0-2.1A
Operating Temperature	32-104°F (0-40°C)	
Operating Altitude	0-16,000 ft (0-5,000 M)	0-16,000 ft (0-5,000 M)
Storage Temperature	14°F-140°F (-10°C-60°C)	
Allowed Relative Humidity	5%-90%, Non-condensing	5%-90%, Non-condensing
Safety Certifications	UL	UL
Electromagnetic Emissions, Safety, & Environmental	FCC (Part 15 Class B), CE, Anatel, BIS, BSMI, CCC, CITC, EAC, ICASA, KCC, RCM, VCCI	FCC (Part 15 Class A), CE, Anatel, BIS, BSMI, CCC, CITC, EAC, ICASA, KCC, RCM, VCCI, NAL,SSRC[19]
Environmental Compliance	ROHS, WEEE, Reach	
Citrix Compliance Regulatory Model	SDW-210	NS-SDW-210-LTE-R1, NS-SDW-210- LTE-R2 and NS-SDW-210-LTE-RC

[16] Models using HDD (Hard Disk Drive) and SSD (Solid State Drive) are indicated accordingly.
[17] Published Ethernet interfaces compliant per IEEE802.3-2002/2005/2008/2012.
[18] 210-LTE-R1: Primarily for Americas and EMEA regions. Exceptions apply for some countries. Bands Supported: B1-B5, B7, B12, B13, B20, B25, B26, B29, B30, B41 | 210-LTE-R2: Primarily for APAC Region. Exceptions apply for some countries. Bands Supported: B1, B3, B5, B7, B8, B18, B19, B21, B28, B38-B41 | 210-LTE-RC: For China only. Bands Supported: B1, B3, B5, B7, B8, B18, B19, B21, B28, B38, B40, B41 | Please contact your Citrix sales representative for more information.
[19] 210-LTE-RC: EMC Certifications include CCC, NAL, SRRC – FCC (Part 15 Class A), CE, CITC, EAC, ENACOM, IFT 210-LTE-R2: EMC certifications include – FCC (Part 15 Class A), CE,

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Hardware Specifications		
Appliance	**110 SE**	**110 LTE WiFi SE**
Model		
Total Disk Space[16]	32 GB	32 GB
Compression History (SSD)	N/A	N/A
RAM	4 GB	4 GB
Network Interfaces[17]		
Fail-to-wire	-	-
Non Fail-to-wire	3x 10/100/1000 RJ45	3x 10/100/1000 RJ45
Management	1x 10/100/1000 RJ45	1x 10/100/1000 RJ45
Integrated LTE	-	1x LTE Modem
Integrated WiFi	-	Yes
Mechanical		
Rack Units	1RU (1.75 inches/4.45 cm)	
Rack Options	Shelf	Shelf[21,22]
System Dimensions	8.5" L x 6.25" W x 1.5" H (21.6 x 15.88 x 3.81 cm)	
System Weight	1.37 lbs (0.62 kg)	1.37 lbs (0.62 kg)
Shipping Dimensions	15.16" L x 10" W x 3.55" H (38.51 x 25.4 x 9.02 cm)	
Shipping Weight	2 lbs (0.91 kg)	2 lbs (0.91 kg)
Power Supply Ratings		
Power Supplies	Single (External)	Single (External)
Input Voltage/Frequency Ranges	90-264 VAC, 47-63 Hz	90-264 VAC, 47-63 Hz
Input Current	0.6A	0.6A
Wattage (Max)	24W	24W
Appliance Ratings		
Input Voltage	12 VDC	12 VDC
Input Current	2.0 A	2.0 A
Wattage	10W typ. (15.5W Max)	10W typ. (15.5W Max)
Environmental and Regulatory		
Operating Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)
Operating Altitude	0-16,000 ft (0-5,000 M)	0-16,000 ft (0-5,000 M)
Storage Temperature	14°F-140°F (-10°C-60°C)	14°F-140°F (-10°C-60°C)
Allowed Relative Humidity	5%-90%, Non-condensing	5%-90%, Non-condensing
Regulatory Certifications	Anatel, CE, CCC, ENACOM, FCC, ICASA, ISED, RCM, UL	Anatel, BTK, CE RED, CCC, ENACOM, FCC, ICASA, IFT, ISED, RCM, SRRC, UL, WPC
Industry Certifications	-	GCF, PTCRB, Wi-Fi Certified ™[20]
Environmental Compliance	ROHS, WEEE, Reach	ROHS, WEEE, Reach
Citrix Compliance Regulatory Model	SD-WAN 110	SD-WAN 110-LTE-WiFi

[16] Models using HDD (Hard Disk Drive) and SSD (Solid State Drive) are indicated accordingly.
[17] Published Ethernet interfaces compliant per IEEE802.3-2002/2005/2008/2012.
[20] The Wi-Fi CERTIFIED™ Logo is a certification mark of Wi-Fi Alliance®
[21] WiFi Signal strength will be impaired and WiFi connection to the appliance may not even be possible. Installation onto a shelf in a metal rack is not recommended.
[22] Extender cables required to remotely locate the LTE Antennas.

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

CITRIX

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States

Fuente del anexo: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-sd-wan-data-sheet.pdf
Apartado desde el que se referencia este anexo: "3.6.1.1 Equipamiento SD-WAN Citrix" - "3.6.2.1 Mantenimiento y licenciamiento SD-WAN Citrix"

Anexo XIII

A continuación, se muestra la configuración de los distintos costes de los gateways SD-WAN, así como su licenciamiento (guía de licencias en: Anexo XV) y mantenimiento del proveedor Aruba que se han incluido en el apartado: "3.6.1.2 Equipamiento SD-WAN Aruba". Esta información ha sido obtenida de la siguiente dirección web proporcionada por el departamento comercial de Aruba:

https://techlibrary.hpe.com/us/en/networking/products/configurator/index.aspx#.XrBSRY0Unuj

Equipo gateway 7005

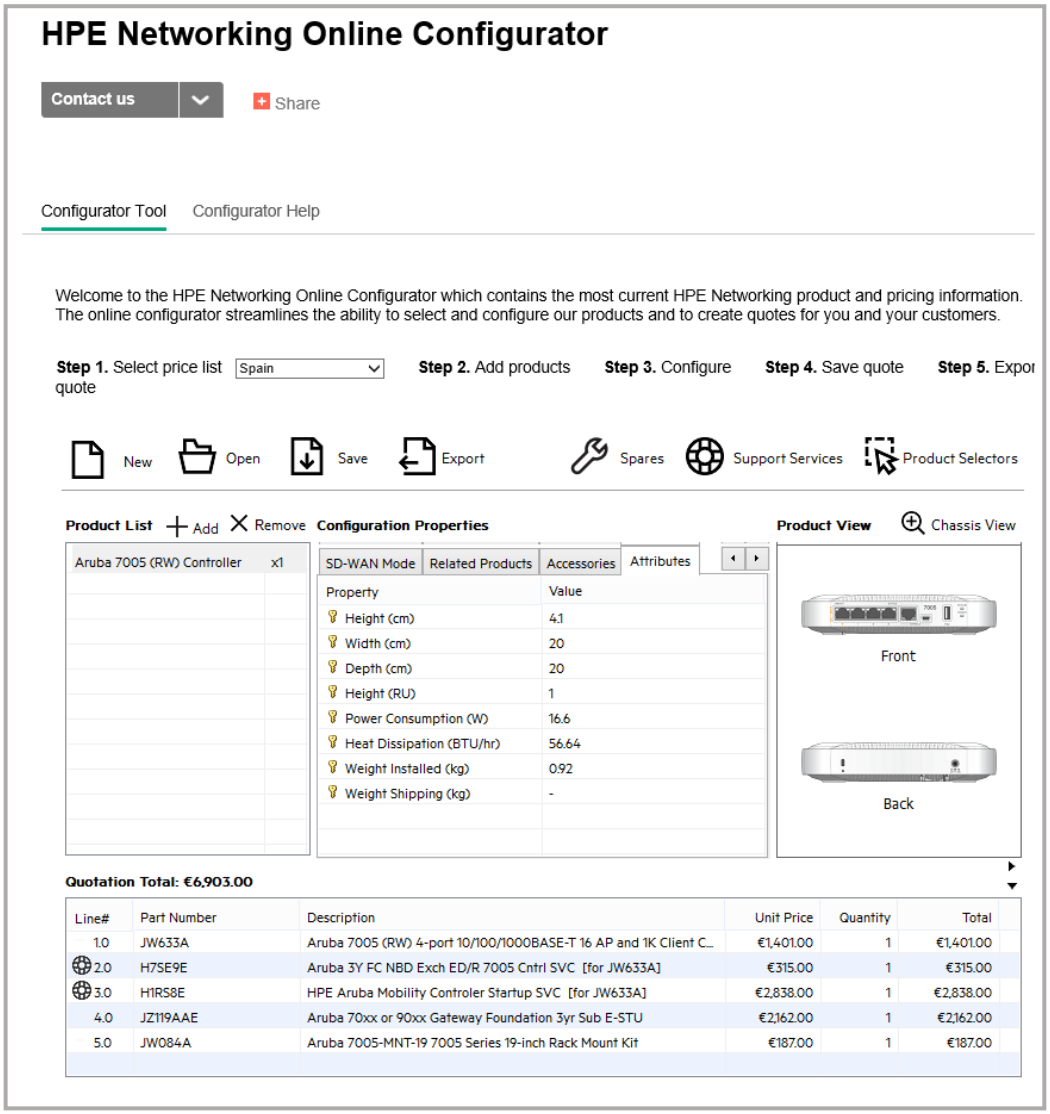


Ilustración 120: Costes gateway 7005 de Aruba

El mantenimiento y licenciamiento código H7SE9E y JW084A respectivamente van presupuestados por un periodo de 3 años al ser más rentable, aunque su pago se realiza anualmente si sobrecoste.

Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" – "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.5 Costes del piloto SD-WAN"

Equipo gateway 7008

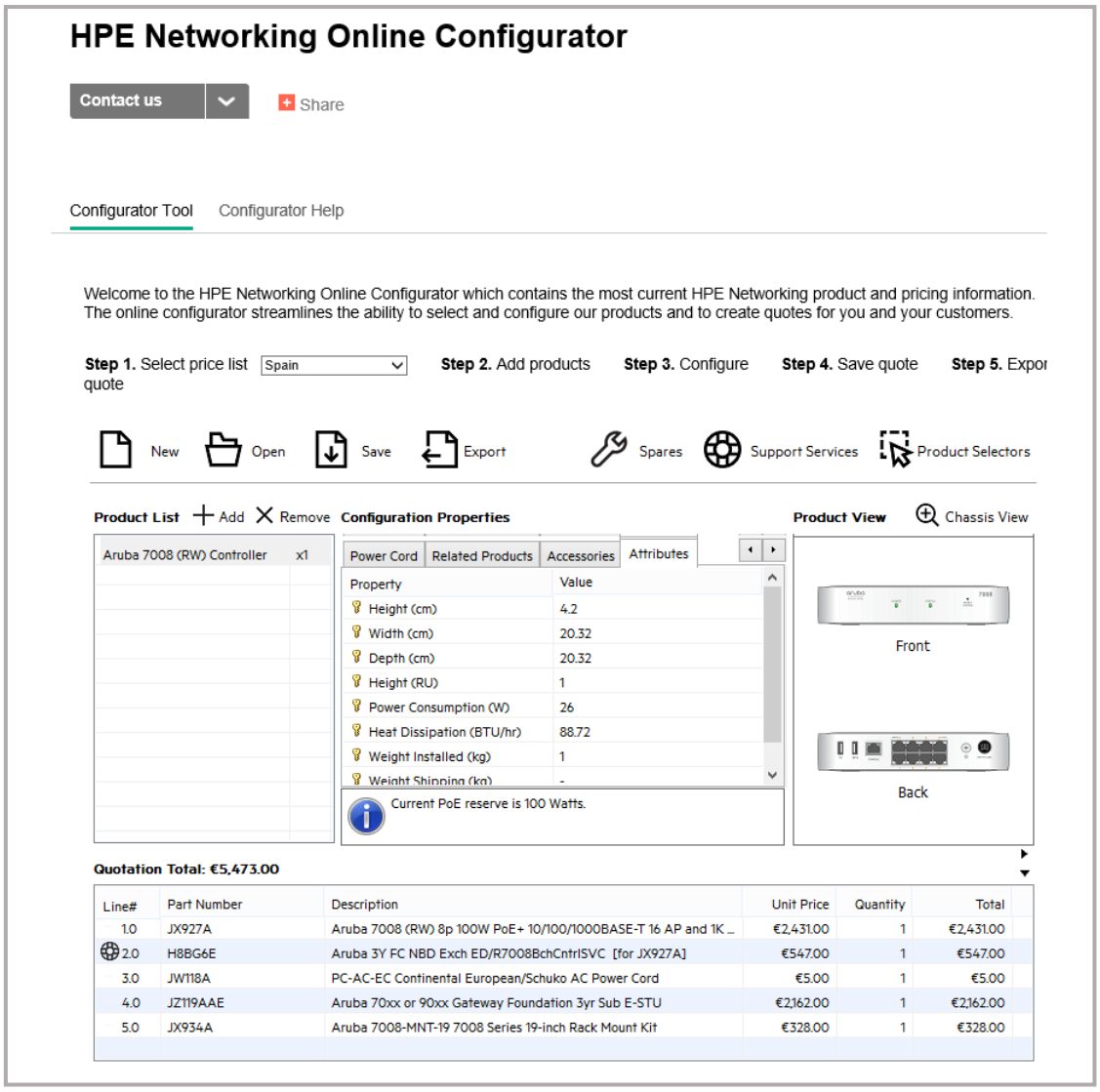


Ilustración 121: Costes gateway 7008 de Aruba

El mantenimiento y licenciamiento código H8BG6E y JZ119AAE respectivamente van presupuestados por un periodo de 3 años al ser más rentable, aunque su pago se realiza anualmente si sobrecoste, debido a que económicamente es mucho más rentable y que generalmente una organización no realiza un proyecto de este tipo solo para un año.

Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" – "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.5 Costes del piloto SD-WAN"

Equipo gateway 7010

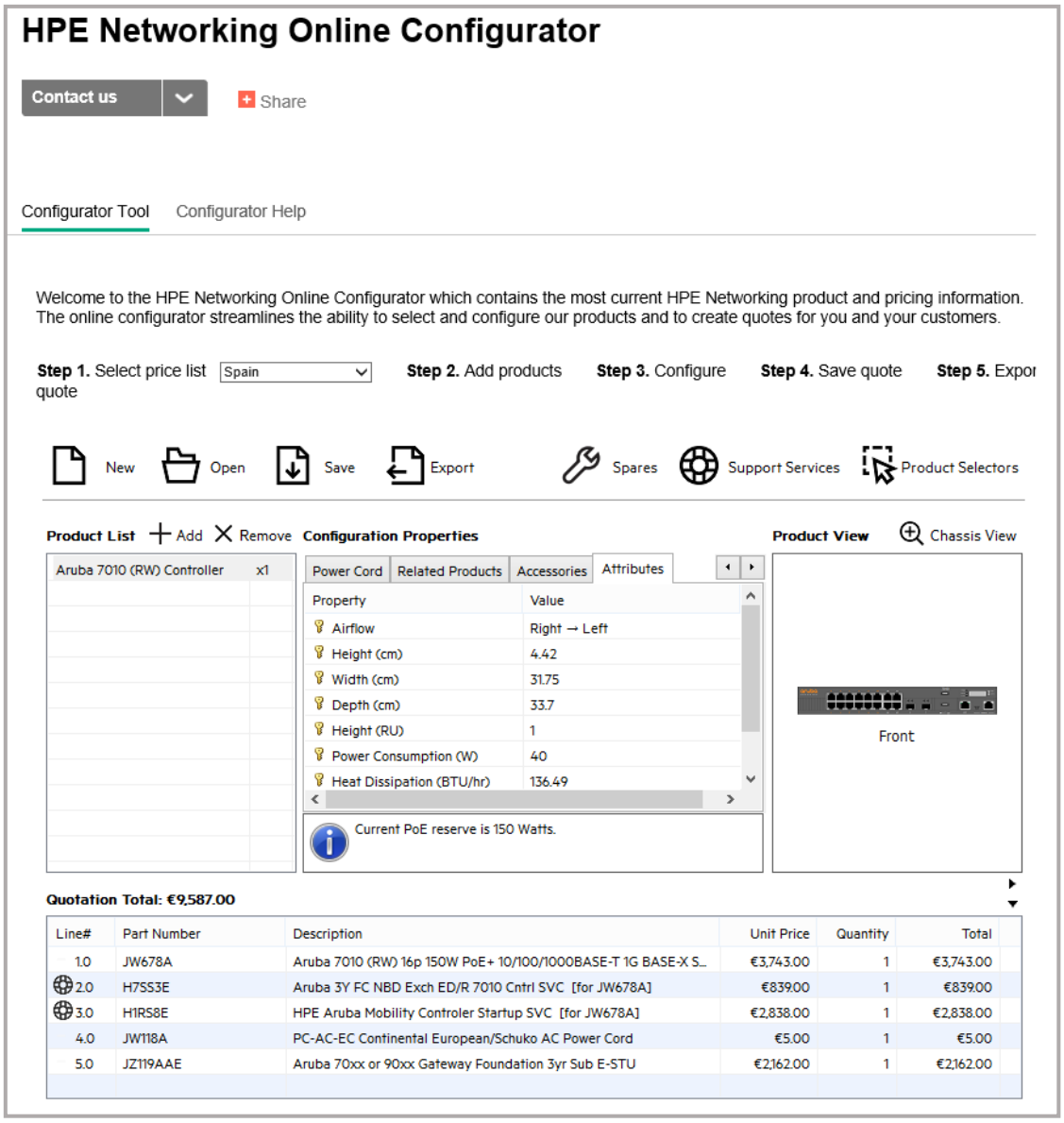


Ilustración 122: Costes gateway 7010 de Aruba

El mantenimiento y licenciamiento código H7SS3E y JZ119AAE respectivamente van presupuestados por un periodo de 3 años, aunque su pago se realiza anualmente sin sobrecoste, debido a que económicamente es mucho más rentable y que generalmente una organización no realiza un proyecto de este tipo solo para un año.

Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" – "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.5 Costes del piloto SD-WAN"

Equipo gateway 7210

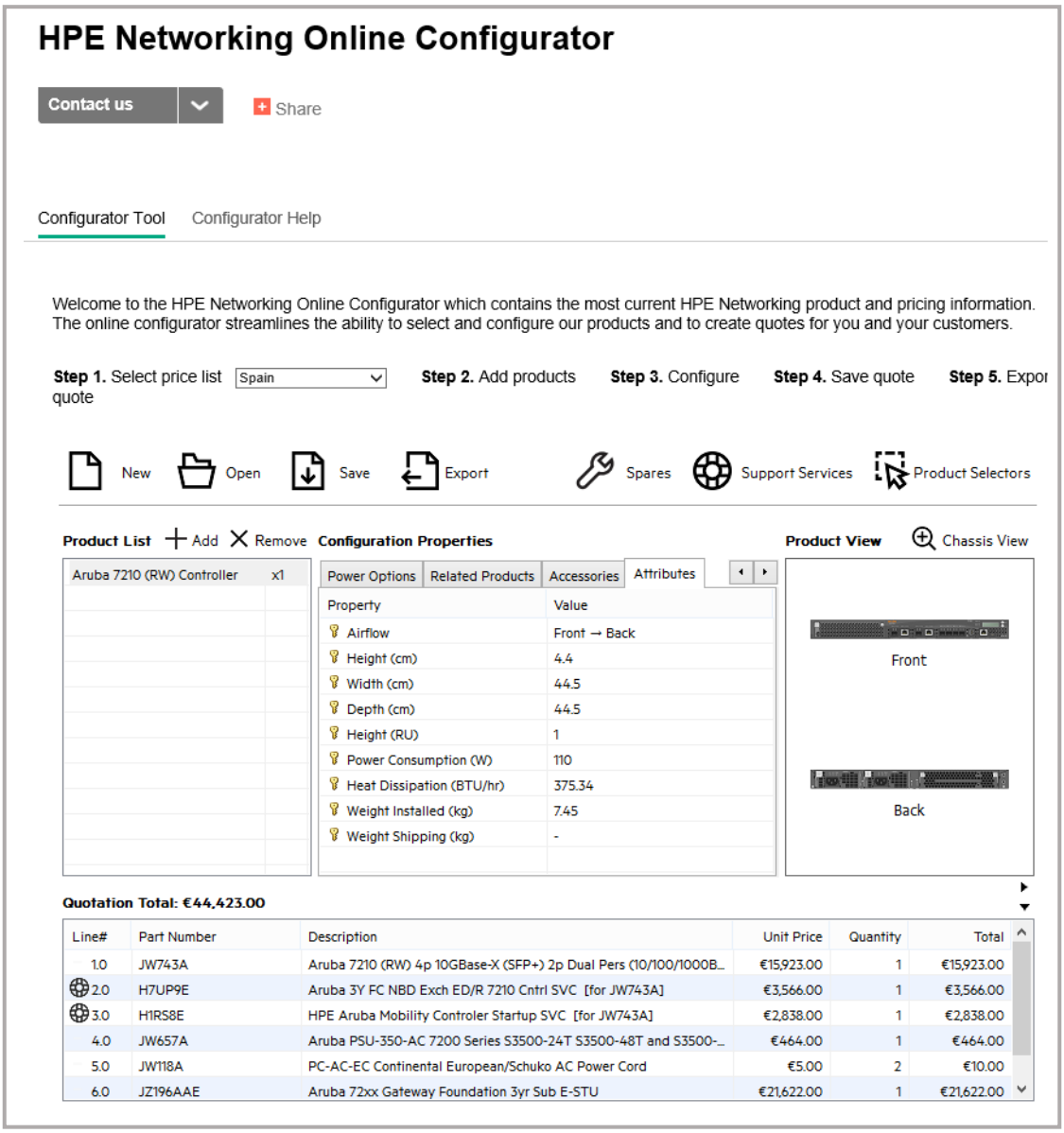


Ilustración 123: Costes gateway 7210 de Aruba

- El mantenimiento y licenciamiento código H7UP9E y JZ196AAE respectivamente van presupuestados por un periodo de 3 años, aunque su pago se realiza anualmente sin sobrecoste debido a que económicamente es mucho más rentable y que generalmente una organización no realiza un proyecto de este tipo solo para un año.
- Este equipo incluye fuentes redundadas con el código JW657A

Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" – "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.5 Costes del piloto SD-WAN"

Equipo gateway 7220

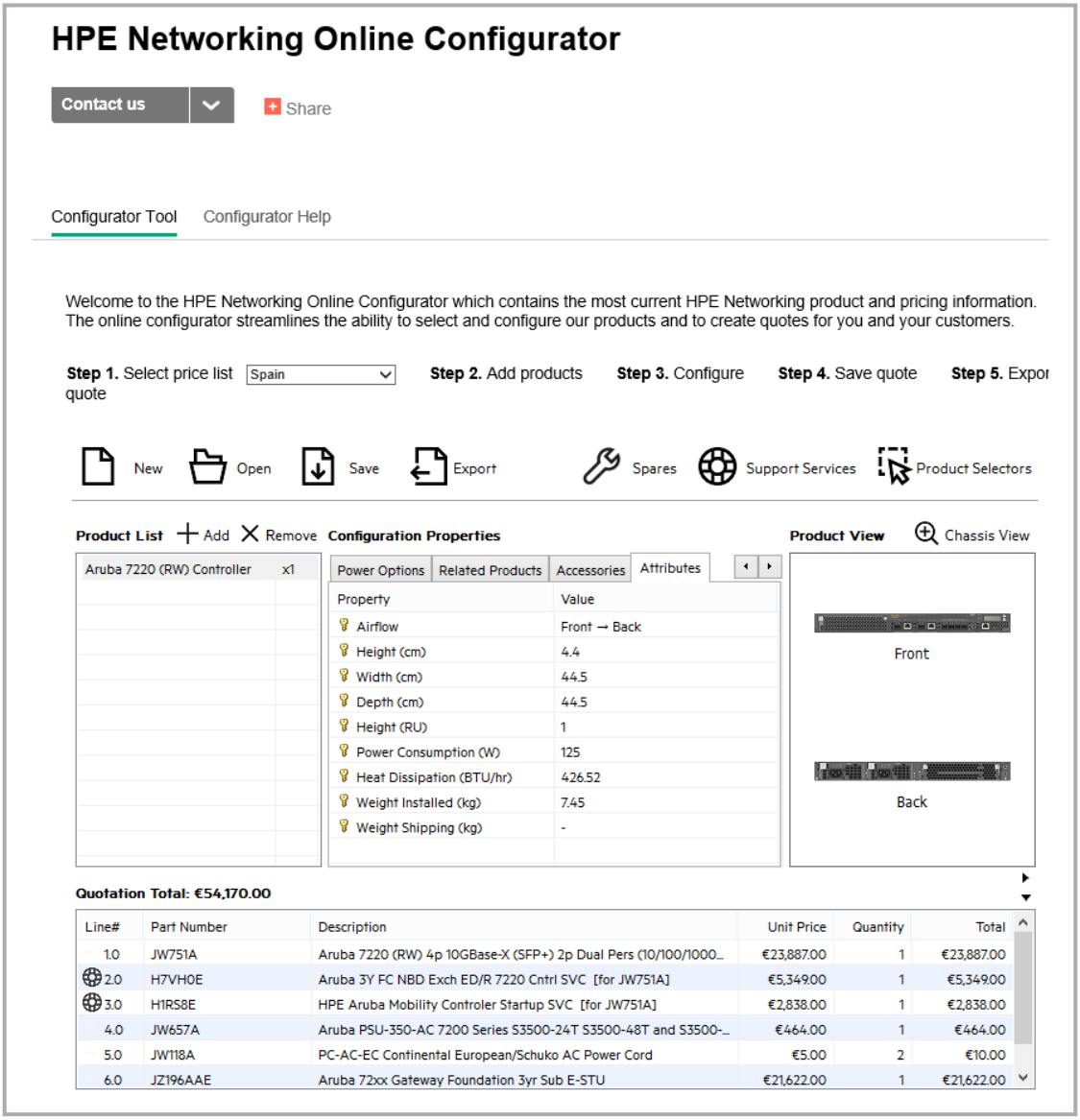


Ilustración 124: Costes gateway 7220 de Aruba

- El mantenimiento y licenciamiento código H7VH0E y JZ196AAE respectivamente van presupuestados por un periodo de 3 años, aunque su pago se realiza anualmente sin sobrecoste debido a que económicamente es mucho más rentable y que generalmente una organización no realiza un proyecto de este tipo solo para un año.
- Este equipo incluye fuentes redundadas con el código JW657A

Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" – "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.5 Costes del piloto SD-WAN"

Equipos gateways virtuales para la nube

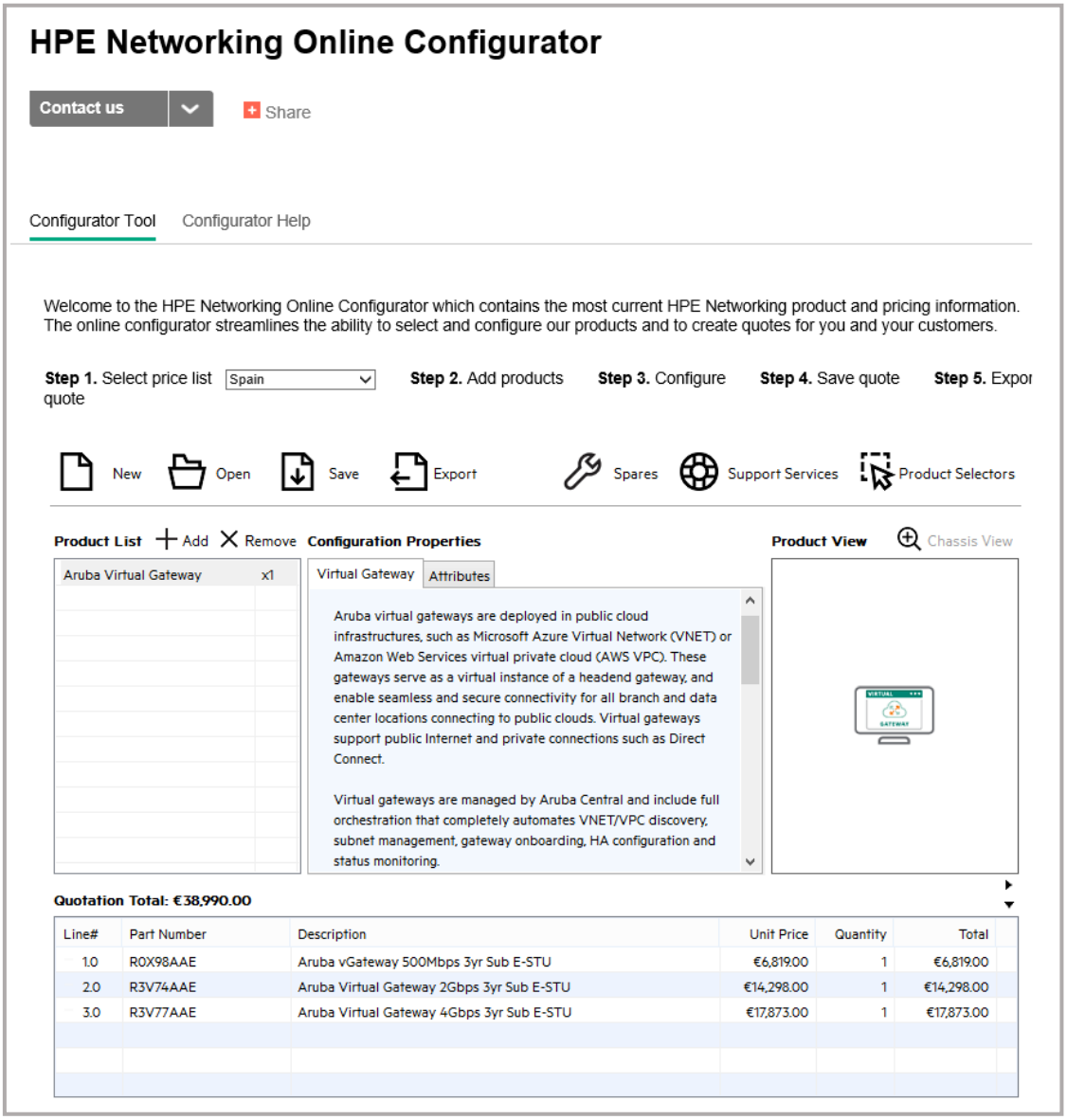


Ilustración 125: Costes gateway virtuales para nube de Aruba

Los licenciamiento códigos R0X98AAE, R3V74AAE y R3V77AAE son para gateways virtuales de 500 Mbps, 2 Gbps y 4 Gbps respectivamente. Además, la licencia va presupuestada por 3 años, aunque su pago se realiza anualmente sin sobrecoste debido a que económicamente es mucho más rentable y que generalmente una organización no realiza un proyecto de este tipo solo para un año.

Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" – "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.5 Costes del piloto SD-WAN"

Anexo XIV

Se adjunta copia de las páginas del documento "*Aruba SD-WAN Data Sheet*", donde se encuentran las especificaciones técnicas del equipamiento SD-WAN de Aruba y que a fecha de redacción de este documento se puede descargar en la siguiente dirección: https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf

aruba
a Hewlett Packard Enterprise company

DATA SHEET

ARUBA SD-WAN

Improved visibility and control at the WAN edge

Software-defined WAN (SD-WAN) technology is the answer to growing bandwidth demands and tightening budget considerations. New solutions offer simplified WAN operations and reduced operational costs for those managing public and private WAN connections, and those shifting toward cloud-based services altogether.

Aruba SD-WAN is designed for all of this and more – optimizing routing decisions and improving visibility across the WAN edge. Full Layer 7 application awareness combines with unique in-branch visibility based on end-user roles, device type, and location context to make Aruba SD-WAN ideal for distributed enterprises.

In fact, organizations in the retail, hospitality and healthcare space – which typically have lean and centralized network teams – can improve the time to deploy, manage and maintain WAN connections, while enhancing the user experience and business operations. Aruba SD-WAN serves a key role in Aruba's overall SD-Branch solution.

INTELLIGENT WAN MANAGEMENT

Through simplified workflows, managing a WAN can be completely orchestrated to improve the speed of deployment, network performance, and ongoing configuration changes. Aruba Central, an AI-powered network operations, assurance, and security platform, provides SD-WAN, as well as WLAN and LAN visibility and controls. Cloud advantages make it easy to to configure and deploy and see data from Aruba branch gateways, headend gateways, and virtual gateways from anywhere. There is no on-premises management equipment to update or maintain.

CLOUD-BASED SD-WAN ORCHESTRATION

Using cloud-scale best practices, Aruba SD-WAN provides end-to-end orchestration to easily distribute routes and build scalable and secure VPN tunnels on-demand. This is based on the data center preference configured in Aruba Central. The orchestrator also simplifies the deployment of virtual gateways within Amazon AWS and Microsoft Azure public cloud infrastructure by automating cloud discovery, onboarding, and management.

KEY FEATURES

- Centralized cloud management
- High performance gateways with ZTP
- Licenses with unrestricted bandwidth for every SD-WAN gateway
- Policy-based routing for 3200+ applications
- Virtual gateways and hub routing available for AWS and Azure
- Policy enforcement firewall, DPI, Web Filtering, and IDS/IPS

UNRESTRICTED BANDWIDTH

Unlike other SD-WAN vendors, Aruba's SD-WAN solution offers unrestricted bandwidth per every gateway license. This means you have access to full hardware performance capabilities right out of the box – no upgrade purchases required.

SD-WAN GATEWAYS

SD-WAN Gateways for Branch

Aruba's SD-WAN gateways are designed to support multiple WAN connections that can be either broadband, MPLS or cellular links. Software features include the ability to route and prioritize traffic being sent to the data center, public cloud infrastructure or the Internet. Each gateway also supports High Availability (HA) requirements (e.g. active/active and active/standby), making it ideal for sites that need full redundancy.

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN" – "Anexo XVII"

SD-WAN Gateways for Headend

Aruba SD-WAN gateways deployed in headend/data center environments act as VPN concentrators (VPNCs) to terminate traffic from branch gateways. These gateways offer support for up to thousands of branch sites. In a typical dual hub-and-spoke model, one or more headend gateways can be used to terminate IPSec tunnels established from branch gateways.

SD-WAN Gateways for Public Cloud

Aruba virtual gateways are deployed in public cloud infrastructures, such as a Microsoft Azure Virtual Network (VNET) or Amazon Web Services virtual private cloud (AWS VPC). These gateways serve as a virtual instance of a headend gateway, and enable seamless and secure connectivity for all branch and data center locations connecting to public clouds. Virtual gateways support public Internet and private connections such as Direct Connect.

Figure 1: Aruba's virtual gateway can be deployed in Azure or AWS.

Virtual gateways are managed by Aruba Central and include full orchestration that completely automates VNET/VPC discovery, subnet management, gateway onboarding, HA configuration and status monitoring.

Virtual gateways support up to 4 Gbps of throughput, with 1, 3, and 5 year subscription options.

MICROSOFT FEATURES

Office 365, Teams and Skype for Business

Aruba's integration with Microsoft enables unique application insight that detects Office 365, Teams and Skype for Business traffic and then prioritizes them over less critical applications. Aruba Central also includes specific call quality heuristics for additional visibility.

Microsoft preferred solution

Aruba Virtual Gateways are a Microsoft preferred solution on the Azure Marketplace. This means the gateway application has been validated by Microsoft experts as having proven competencies and capabilities that meet customer needs.

POLICY-BASED ROUTING AND SUPPORTED PROTOCOLS

With Policy-based Routing (PBR), traffic can be routed across multiple private or public WAN uplinks based on application type and link health, device profile, user role, and destination. Supported protocols include BGP, OSPF and static routes.

SAAS OPTIMIZATION

Aruba Central enables the discovery of SaaS application servers based on geography, monitoring of application performance, and dynamic steering of WAN traffic from one server to another. This capability ensures that users who access SaaS applications such as Microsoft 365 (Office 365), Box, Slack, and Zendesk are matched to the best available points of presence. This feature requires the SD-WAN Advanced License. For more information, please refer to the latest Aruba Central documentation.

KEY WAN FEATURES

Overlay and Hybrid WAN Management

Aruba SD-WAN introduces a new architecture that provides a network overlay for WAN connections to improve visibility and control across private and public connections (hybrid WAN).

Hub-and-Spoke Topology

Secure connections can be established from a branch site to a headend site using public or private connections. This allows users to efficiently access corporate resources hosted in data centers.

Site-to-Site VPNs

Secure connections can also be established from one branch site to another over a public Internet connection. This allows users from different locations to access network resources hosted within the corporate network without going through the data center.

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN" – "Anexo XVII"

Dynamic Path Steering (DPS)

WAN traffic can be automatically routed over the best available uplink based on characteristics, such as WAN throughput, latency, jitter and packet loss.

WAN Visibility

With deep packet inspection technology, Aruba Central provides monitoring for application traffic that enters and exits a branch network – regardless of the uplink type. This makes it easy for IT to manage WAN environments that increasingly utilize public WAN connections.

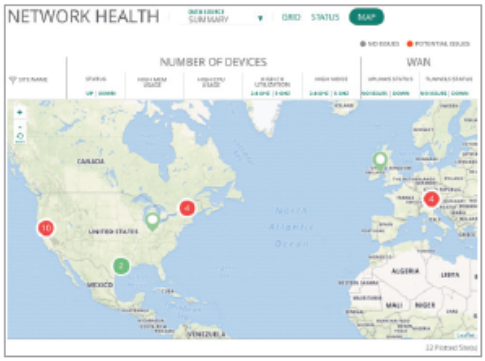


Figure 2: Aruba Central WAN Health Dashboard

WAN Compression

Ideal for use during periods of network congestion, this WAN compression feature allows IT to send more traffic through the same WAN circuit at any given moment or timeframe.

Unrestricted Bandwidth

Aruba SD-WAN licenses provide access to the full bandwidth specification for each gateway. No additional license upgrades required.

KEY CONFIGURATION FEATURES

Simplified Installation Wizard

For easy configuration of SD-WAN gateways, Aruba Central provides users with a step-by-step navigation that simplifies provisioning of the network.

Configuration Hierarchy

Network settings can be pre-configured and customized in Aruba Central based on branch-specific requirements. Zero Touch Provisioning (ZTP) provides an easy and error-free deployment model.

Zero Touch Provisioning (ZTP)

Using Zero Touch Provisioning, the hardware gateways can be factory-shipped and deployed onsite using Aruba Activate™, a cloud-based activation service that seamlessly works with Aruba Central. Settings can be applied based on configuration and other network-specific requirements.

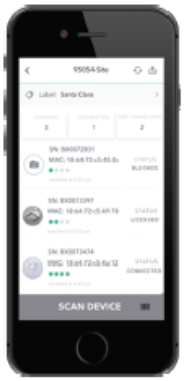


Figure 3: Example of Aruba's mobile installer app for device onboarding.

Simple, mobile provisioning

Aruba's mobile installer app allows on-site personnel to easily onboard gateways. A central IT team can verify device location, licenses, and status with no additional steps required. This is available for iOS and Android.

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN" – "Anexo XVII"

KEY SECURITY AND VISIBILITY FEATURES

Dynamic Segmentation

To simplify and better secure wired and wireless network access, the branch gateway can automatically enforce per user and per-device roles on wired and wireless networks. Integration with ClearPass Policy Manager allows for centralized role and policy management. This ensures consistent policy regardless of user role and device type, and eliminates the need to configure unnecessary SSIDs, ACLs, VLANs and subnets at every node in the network. For more information on Dynamic Segmentation, please refer to the solution overview.

Figure 4: Segment mobile and IoT traffic using Aruba

Policy Enforcement Firewall

Included within the Foundation license, PEF allows for wired and wireless user and application traffic to be sent to a branch gateway through GRE tunnels for inspection. Enforcement of policies based on user role, device type, application and location is accomplished through Aruba Dynamic Segmentation.

Application visibility and control

Also included in the Foundation license is an application visibility feature that uses Deep Packet Inspection (DPI) technology to evaluate and optimize performance and QoS policies for over 3,000 applications, including encrypted and hidden traffic.

Web content filtering

The Web Content Classification (WebCC) bundle is also part of the Foundation license. This classifies websites by content category and rates them by reputation. It can also block, apply QoS, bandwidth-limit, mirror, and log web content.

Threat Defense with IDS/IPS

To improve security against a growing attack surface, gateways deployed in SD-WAN mode add role and identity-based intrusion detection and prevention capabilities (IDS/ IPS) on top of existing security features. An advanced security dashboard provides IT Teams with network-wide visibility, multi-dimensional threat metrics, threat intelligence data, correlation and incident management. This feature requires the appropriate Aruba Central security subscription license.

Third-party security gateway and firewall support

For cloud security threat protection, Aruba gateways can assume the role of an on-premises agent of centrally-hosted firewalls such as those provided by Palo Alto Networks and Check Point Software, or web security gateways such as Zscaler and Symantec.

Unified Communications and Collaboration (UCC)

Measure and troubleshoot networks based on call quality metrics such as Mean Opinion Score, latency, jitter and packet loss. Supported applications include: Teams, Skype for Business®, Wi-Fi Calling, Facetime, SIP, Jabber, Spark and more.

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN" – "Anexo XVII"

TECHNICAL SPECIFICATIONS*

BRANCH GATEWAYS (SMALL AND MEDIUM)

Features	9004	7005	7008	7010	7024
Deployment mode	Small/Medium	Small	Small	Medium	Medium
Maximum clients	Up to 2,048**	Up to 1,024**	Up to 1,024**	2,048	2,048
Firewall throughput	3 Gbps	2 Gbps	2 Gbps	8 Gbps	8 Gbps
Encrypted throughput (AES-CBC)	3 Gbps	1.2 Gbps	1.2 Gbps	2.6 Gbps	2.6 Gbps
Active firewall sessions	64K	64K	64K	32K	32K
WAN/LAN Interfaces	4	4	8	16	24
PoE in/out	–	In; E0	Out; 100W	Out; 150W	Out; 400W
USB (WAN)	Yes (1); USB 3.0	Yes (1); USB 2.0	Yes (2); USB 2.0	Yes (2); USB 2.0	Yes (1); USB 2.0
Form factor/footprint	Desktop/1RU[1]	Desktop/1RU	Desktop/1RU	1RU	1RU

[1] 1RU can support two 9004 gateways side-by-side using an optional mount kit.

BRANCH GATEWAYS (LARGE)

Features	7030	7210	7220	7240XM			
Deployment mode	Large	Large	Large	Large			
Maximum clients	4096	16K	24K	32K			
Firewall throughput	8 Gbps	20 Gbps	40 Gbps	40 Gbps			
Encrypted throughput (AES-CBC)	2.6 Gbps	6 Gbps	20 Gbps	30 Gbps			
Active firewall sessions	64K	2M	2M	2M			
WAN/LAN Interfaces	8 (combo)	2 (combo)	2 (combo)	2 (combo)			
USB (WAN)	Yes (1); USB 2.0	Yes (1); USB 2.0	Yes (1); USB 2.0	Yes (1); USB 2.0			
Form factor/footprint	1 RU	1 RU	1 RU	1 RU			

HEADEND GATEWAYS

Features	7010	7024	7030	7210	7220	7240XM
Deployment mode	VPN Concentrator (VPNC)	VPNC	VPNC	VPNC	VPNC	VPNC
Encrypted throughput (3DES)	2.4 Gbps	2.4 Gbps	2.4 Gbps	7 Gbps	25 Gbps	28 Gbps
Encrypted throughput (AES-CBC)	2.6 Gbps	2.6 Gbps	2.6 Gbps	7 Gbps	22 Gbps	30 Gbps
WAN compression performance	2.5 Gbps	2.5 Gbps	2.5 Gbps	10 Gbps	10 Gbps	10 Gbps
Maximum tunnels	512	512	512	1,024	4,096	6,144
Route scale	3,000	3,000	6,000	6,000	20,000	30,000
Form factor/footprint	1RU	1RU	1RU	1RU	1RU	1RU

*For complete hardware specifications, please see the 9004 Gateway and 7000/7200 Mobility Controller datasheets.

**The 9004 and 7005/7008 offers a base capacity license for up to 75 clients.

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN" – "Anexo XVII"

VIRTUAL GATEWAYS		
Features	**Amazon AWS VPC**	**Microsoft Azure VNET**
Deployment mode	Public Cloud Infrastructure (VPNC)	Public Cloud Infrastructure
Firewall throughput	500 Mbps, 2 Gbps, 4 Gbps	500 Mbps
Number of interfaces	3 (plus 1 for management)	
Virtual CPU	Up to 16	4
Memory	Up to 60GB	14GB
Maximum tunnels	Up to 1600, 4096, 8192	
Infrastructure	Additional VPC infrastructure costs based on a BYOL model	

For additional information on ordering and full gateway hardware specifications, please refer to:

- SD-WAN Ordering Guide
- 7000 Series Mobility Controller Data sheet
- 7200 Series Mobility Controller Data sheet
- 9004 Series Gateways Data sheet

aruba
a Hewlett Packard Enterprise company

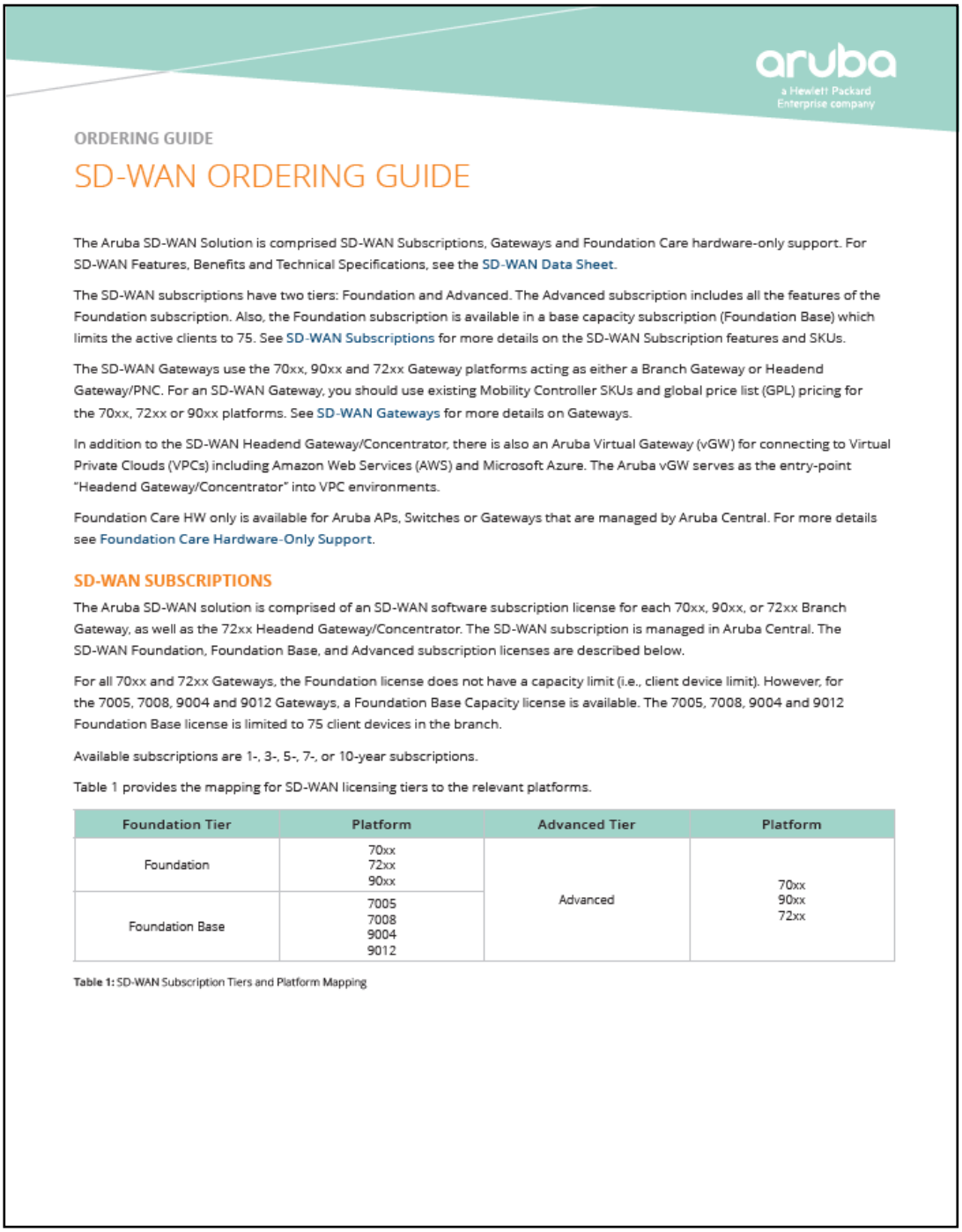
DS_SD-WAN_SK_030320 a00047570enw

Contact Us Share

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba" – "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN" – "Anexo XVII"

Anexo XV

Se adjunta copia de las páginas del documento "*SD-WAN ORDERING GUIDE*", donde se encuentran la guía de pedidos para el licenciamiento del equipamiento SD-WAN de Aruba y que a fecha de redacción de este documento se puede descargar en la siguiente dirección: https://www.arubanetworks.com/assets/og/OG_SD-WAN.pdf.



aruba
a Hewlett Packard Enterprise company

ORDERING GUIDE

SD-WAN ORDERING GUIDE

The Aruba SD-WAN Solution is comprised SD-WAN Subscriptions, Gateways and Foundation Care hardware-only support. For SD-WAN Features, Benefits and Technical Specifications, see the SD-WAN Data Sheet.

The SD-WAN subscriptions have two tiers: Foundation and Advanced. The Advanced subscription includes all the features of the Foundation subscription. Also, the Foundation subscription is available in a base capacity subscription (Foundation Base) which limits the active clients to 75. See SD-WAN Subscriptions for more details on the SD-WAN Subscription features and SKUs.

The SD-WAN Gateways use the 70xx, 90xx and 72xx Gateway platforms acting as either a Branch Gateway or Headend Gateway/PNC. For an SD-WAN Gateway, you should use existing Mobility Controller SKUs and global price list (GPL) pricing for the 70xx, 72xx or 90xx platforms. See SD-WAN Gateways for more details on Gateways.

In addition to the SD-WAN Headend Gateway/Concentrator, there is also an Aruba Virtual Gateway (vGW) for connecting to Virtual Private Clouds (VPCs) including Amazon Web Services (AWS) and Microsoft Azure. The Aruba vGW serves as the entry-point "Headend Gateway/Concentrator" into VPC environments.

Foundation Care HW only is available for Aruba APs, Switches or Gateways that are managed by Aruba Central. For more details see Foundation Care Hardware-Only Support.

SD-WAN SUBSCRIPTIONS

The Aruba SD-WAN solution is comprised of an SD-WAN software subscription license for each 70xx, 90xx, or 72xx Branch Gateway, as well as the 72xx Headend Gateway/Concentrator. The SD-WAN subscription is managed in Aruba Central. The SD-WAN Foundation, Foundation Base, and Advanced subscription licenses are described below.

For all 70xx and 72xx Gateways, the Foundation license does not have a capacity limit (i.e., client device limit). However, for the 7005, 7008, 9004 and 9012 Gateways, a Foundation Base Capacity license is available. The 7005, 7008, 9004 and 9012 Foundation Base license is limited to 75 client devices in the branch.

Available subscriptions are 1-, 3-, 5-, 7-, or 10-year subscriptions.

Table 1 provides the mapping for SD-WAN licensing tiers to the relevant platforms.

Foundation Tier	Platform	Advanced Tier	Platform
Foundation	70xx 72xx 90xx	Advanced	70xx 90xx 72xx
Foundation Base	7005 7008 9004 9012		

Table 1: SD-WAN Subscription Tiers and Platform Mapping

Fuente del anexo: https://www.arubanetworks.com/assets/og/OG_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "Anexo XIII" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba"

Table 2 adds feature details to the subscription tiers outlined in Table 1.

Tier	Features	Gateway Model
Foundation	• Branch Gateway and VPNC Management • Stateful Firewall • IPsec VPN • Client VPN • Routing • Orchestration: Tunnel, Route, Cloud Security • Dynamic Path Steering • Link Redundancy • >> 2 WAN Links • Application-based policies • High Availability (Active-Standby or Active-Active) • Web content filtering • Role Based Access Policy • Full SD-LAN Control	70xx 90xx 7200
Foundation Base	All features in Foundation, limited to 75 concurrent endpoints	7005 7008 9004 9012
Advanced	All features in Foundation plus • SaaS Express	70xx 90xx 72xx

Table 2: SD-WAN Feature Details (per Tier) and Platform Mapping

For each subscription, the stock keeping units (SKUs), along with descriptions and pricing, is listed below. Available subscriptions are 1-, 3-, 5-, 7-, or 10-year subscriptions.

Table 3 provides more details: licensing tiers, SKUs and descriptions. The next tables provide that same information for Foundation, Foundation Base, and Advanced.

FOUNDATION: 70XX, 90XX, 72XX	
SKU	Description
JZ118AAE	Aruba 70xx or 90xx Gateway Foundation 1yr Subscription E-STU
JZ119AAE	Aruba 70xx or 90xx Gateway Foundation 3yr Subscription E-STU
JZ120AAE	Aruba 70xx or 90xx Gateway Foundation 5yr Subscription E-STU
R0G52AAE	Aruba 70xx or 90xx Gateway Foundation 7yr Subscription E-STU
R0G53AAE	Aruba 70xx or 90xx Gateway Foundation 10yr Subscription E-STU
JZ195AAE	Aruba 72xx Gateway Foundation 1yr Subscription E-STU
JZ196AAE	Aruba 72xx Gateway Foundation 3yr Subscription E-STU
JZ197AAE	Aruba 72xx Gateway Foundation 5yr Subscription E-STU
R0G60AAE	Aruba 72xx Gateway Foundation 7yr Subscription E-STU
R0G61AAE	Aruba 72xx Gateway Foundation 10yr Subscription E-STU

Table 3: SD-WAN Foundation Licensing SKUs and Descriptions

Fuente del anexo: https://www.arubanetworks.com/assets/og/OG_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "Anexo XIII" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba"

FOUNDATION BASE: 7005, 7008, 9004, 9012	
SKU	**Description**
JZ124AAE	Aruba 70xx or 90xx Gateway Foundation Base Capacity 1yr Subscription E-STU
JZ125AAE	Aruba 70xx or 90xx Gateway Foundation Base Capacity 3yr Subscription E-STU
JZ126AAE	Aruba 70xx or 90xx Gateway Foundation Base Capacity 5yr Subscription E-STU
R0G56AAE	Aruba 70xx or 90xx Gateway Foundation Base Capacity 7yr Subscription E-STU
JZ126AAE	Aruba 70xx or 90xx Gateway Foundation Base Capacity 10yr Subscription E-STU

Table 4: SD-WAN Foundation Base Licensing SKUs and Descriptions

ADVANCED: 70XX, 90XX, 72XX	
SKU	**Description**
JZ121AAE	Aruba 70xx or 90xx Gateway Advanced 1yr Subscription E-STU
JZ122AAE	Aruba 70xx or 90xx Gateway Advanced 3yr Subscription E-STU
JZ123AAE	Aruba 70xx or 90xx Gateway Advanced 5yr Subscription E-STU
R0G54AAE	Aruba 70xx or 90xx Gateway Advanced 7yr Subscription E-STU
R0G55AAE	Aruba 70xx or 90xx Gateway Advanced 10yr Subscription E-STU
JZ198AAE	Aruba 72xx Gateway Foundation Base Capacity 1yr Subscription E-STU
JZ199AAE	Aruba 72xx Gateway Foundation Base Capacity 3yr Subscription E-STU
JZ200AAE	Aruba 72xx Gateway Foundation Base Capacity 5yr Subscription E-STU
R0G62AAE	Aruba 72xx Gateway Foundation Base Capacity 7yr Subscription E-STU
R0G63AAE	Aruba 72xx Gateway Foundation Base Capacity 10yr Subscription E-STU

Table 5: SD-WAN Advanced Licensing SKUs and Descriptions

ARUBA VIRTUAL GATEWAY	
SKU	**Description**
R0X97AAE	Aruba Virtual Gateway 500Mbps 1yr Sub E-STU
R0X98AAE	Aruba Virtual Gateway 500Mbps 3yr Sub E-STU
R0X99AAE	Aruba Virtual Gateway 500Mbps 5yr Sub E-STU
R3V73AAE	Aruba Virtual Gateway 2Gbps 1yr Sub E-STU
R3V74AAE	Aruba Virtual Gateway 2Gbps 3yr Sub E-STU
R3V75AAE	Aruba Virtual Gateway 2Gbps 5yr Sub E-STU
R3V76AAE	Aruba Virtual Gateway 4Gbps 1yr Sub E-STU
R3V77AAE	Aruba Virtual Gateway 4Gbps 3yr Sub E-STU
R3V78AAE	Aruba Virtual Gateway 4Gbps 5yr Sub E-STU

Table 6: Aruba Virtual Gateway Licensing and Descriptions

Fuente del anexo: https://www.arubanetworks.com/assets/og/OG_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "Anexo XIII" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba"

SD-WAN GATEWAYS

Branch Gateway

For the Branch Gateway, order a region-specific 70xx, 72xx, or 90xx based on scale, performance and port density requirements. Also order the appropriate accessories including region specific power supply and a mounting kit. Select the Ordering Guide links in the **Hardware Ordering Guides** section below for ordering information.

Head End Gateway

For the Head End Gateway, order a region specific 7010, 7024, 7030, 7210, 7220 or 7240XM based on scale, performance and port density requirements. Also order the appropriate accessories including region specific power supply and a mounting kit.

Select the Ordering Guide links in the **Hardware Ordering Guides** section below for ordering information.

Hardware Ordering Guides

7000 Series Ordering Guide

7200 Series Ordering Guide

9000 Series Ordering Guide

Aruba Virtual Gateway

For the Aruba Virtual Gateway, order the capacity (bps) needed for the Virtual Gateway as a "virtual VPNC" in AWS or Azure.

See the Aruba SD-WAN Data Sheet.

FOUNDATION CARE HARDWARE-ONLY SUPPORT

The SD-WAN Subscription licenses include Software support and TAC/Phone Support. For Hardware replacement support, you can order Foundation Care Hardware-only next business day (NBD) or Foundation Care 4 Hour support. For more information on the Hardware-only support SKUs, enter the hardware SKU (refer to: http://ssc.hpe.com/portal/site/ssc/) to look up the Foundation Care Hardware-only Support SKU.

aruba
a Hewlett Packard Enterprise company

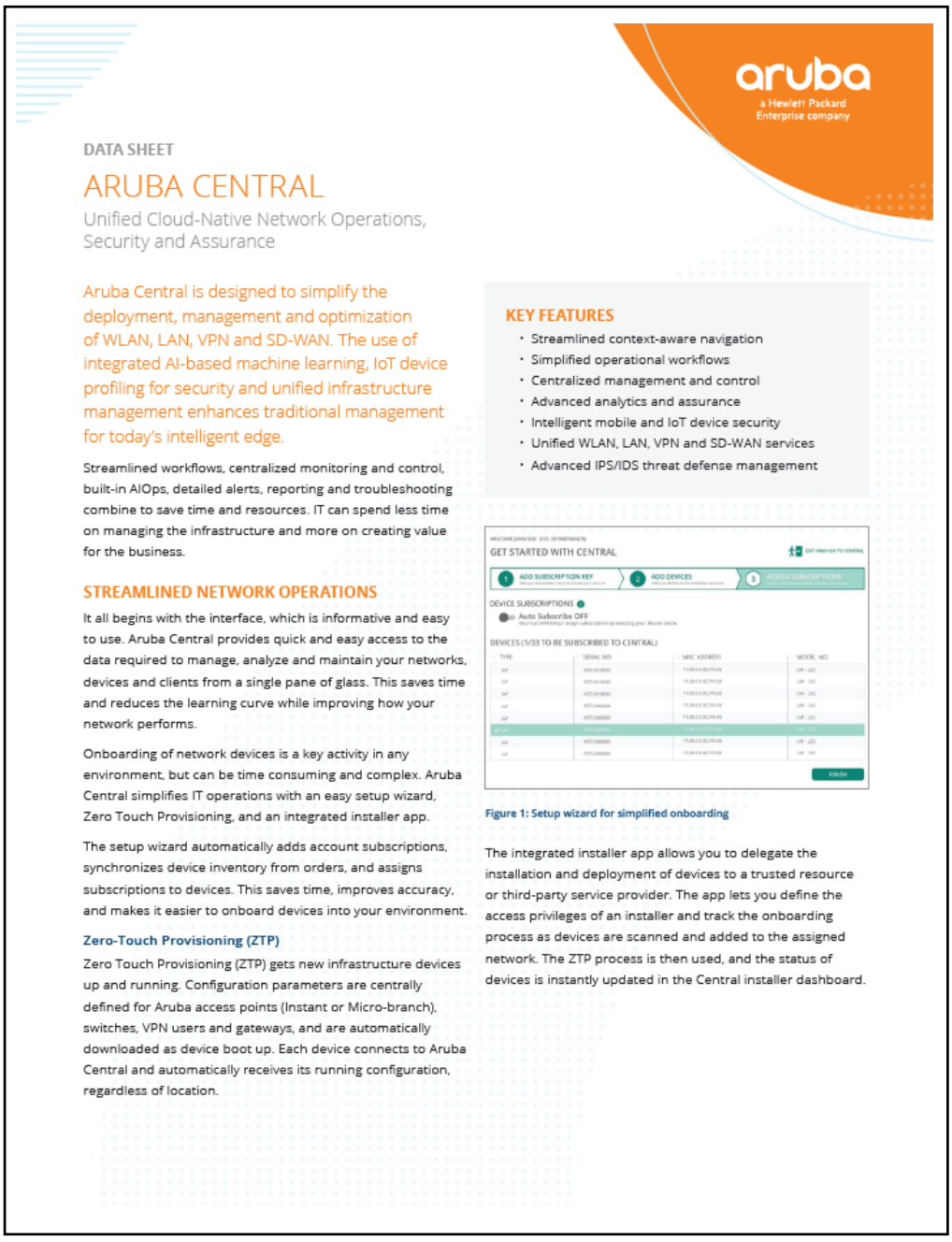
OG_SD-WANorderingguide_SK_040820 a00075200enw

Fuente del anexo: https://www.arubanetworks.com/assets/og/OG_SD-WAN.pdf
Apartado desde el que se referencia este anexo: "Anexo XIII" - "3.6.2.2 Mantenimiento y licenciamiento SD-WAN Aruba"

Anexo XVI

Se adjunta copia de las páginas del documento "*DATA SHEET: ARUBA CENTRAL*", donde se detallan capacidades y característica del software Aruba Central para la gestión, administración, monitorización y despliegue entre otras de equipos e infraestructuras SD-WAN. A fecha de redacción de este trabajo, el documento se puede descargar en la siguiente dirección:

https://www.arubanetworks.com/products/networking/management/central/



aruba
a Hewlett Packard Enterprise company

DATA SHEET

ARUBA CENTRAL

Unified Cloud-Native Network Operations, Security and Assurance

Aruba Central is designed to simplify the deployment, management and optimization of WLAN, LAN, VPN and SD-WAN. The use of integrated AI-based machine learning, IoT device profiling for security and unified infrastructure management enhances traditional management for today's intelligent edge.

Streamlined workflows, centralized monitoring and control, built-in AIOps, detailed alerts, reporting and troubleshooting combine to save time and resources. IT can spend less time on managing the infrastructure and more on creating value for the business.

KEY FEATURES

- Streamlined context-aware navigation
- Simplified operational workflows
- Centralized management and control
- Advanced analytics and assurance
- Intelligent mobile and IoT device security
- Unified WLAN, LAN, VPN and SD-WAN services
- Advanced IPS/IDS threat defense management

STREAMLINED NETWORK OPERATIONS

It all begins with the interface, which is informative and easy to use. Aruba Central provides quick and easy access to the data required to manage, analyze and maintain your networks, devices and clients from a single pane of glass. This saves time and reduces the learning curve while improving how your network performs.

Onboarding of network devices is a key activity in any environment, but can be time consuming and complex. Aruba Central simplifies IT operations with an easy setup wizard, Zero Touch Provisioning, and an integrated installer app.

The setup wizard automatically adds account subscriptions, synchronizes device inventory from orders, and assigns subscriptions to devices. This saves time, improves accuracy, and makes it easier to onboard devices into your environment.

Figure 1: Setup wizard for simplified onboarding

Zero-Touch Provisioning (ZTP)

Zero Touch Provisioning (ZTP) gets new infrastructure devices up and running. Configuration parameters are centrally defined for Aruba access points (Instant or Micro-branch), switches, VPN users and gateways, and are automatically downloaded as device boot up. Each device connects to Aruba Central and automatically receives its running configuration, regardless of location.

The integrated installer app allows you to delegate the installation and deployment of devices to a trusted resource or third-party service provider. The app lets you define the access privileges of an installer and track the onboarding process as devices are scanned and added to the assigned network. The ZTP process is then used, and the status of devices is instantly updated in the Central installer dashboard.

Fuente del anexo: https://www.arubanetworks.com/products/networking/management/central/
Apartado desde el que se referencia este anexo: " 3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y Licenciamiento SD-WAN Aruba" - "4.1.3.2 Software de gestión y administración del piloto SD-WAN"

UNIFIED INFRASTRUCTURE MANAGEMENT

The first thing you'll notice is the network health overview. This primary dashboard provides a global or site view of all managed devices. A detailed list of device usage, utilization and RF noise, along with WAN up link and tunnel status can be easily viewed.

At-a-glance views provide comprehensive visibility and control at the global level. Selecting a site changes the interface to only show those devices relevant for specific sites. The same is true for clients at each site.

Figure 2: Network Summary

ADVANCED AIOps

With continuous monitoring, AI-based insights provide real-time visibility and alerts into what's happening in the wired and wireless LAN. The insights leverage a growing pool of network data, and deep domain experience.

When a problem occurs, quick identification, characterization and resolution are at the core of maintaining a stable environment. Here again, Aruba Central's AI Insights deliver the right context-based information at the right time, thus providing a more efficient alternative to event or command line based troubleshooting. However, detailed events and integrated command line tools are available when needed.

The result is a consistent, reliable and timely flow of information about the RF environment that helps IT work smarter despite increasing demands and the complexity that a growing network often brings.

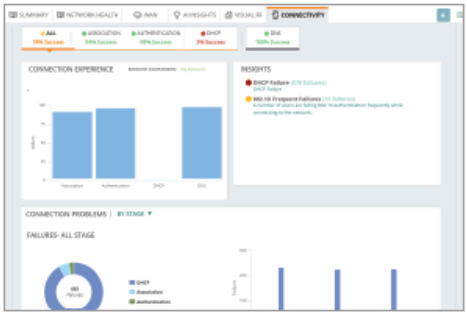


Figure 3: AI-based connectivity insights

REPORTING AND IN-DEPTH TROUBLESHOOTING

Aruba Central includes the ability to create comprehensive reports that cover device connectivity, network health and user account activity. A reporting wizard is also provided to generate scheduled and on-demand reports that highlight network and application health, throughput and usage data, device and client inventory and activity auditing.

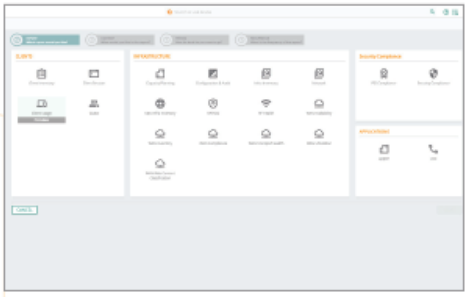


Figure 4: Reporting Wizard

REMOTE TELEWORKER SERVICES

Aruba Central manages secure overlay VPN tunnels from APs and VIA VPN clients to SD-WAN Gateways deployed in data centers or public cloud infrastructure. This enables IT to easily scale network infrastructure to support thousands of remote users who need access to corporate applications and services. For existing customers with APs running Aruba Instant or APs with IAP-VPN connections, it's easy to convert to an Aruba Central-managed VPN platform.

Fuente del anexo: https://www.arubanetworks.com/products/networking/management/central/
Apartado desde el que se referencia este anexo: " 3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y Licenciamiento SD-WAN Aruba" - "4.1.3.2 Software de gestión y administración del piloto SD-WAN"

SD-WAN ORCHESTRATION AND MANAGEMENT

The monitoring and control of SD-WAN virtual, headend and branch gateways allows IT to centrally manage the infrastructure and routing of traffic over MPLS, broadband and cellular links. Aruba Central also provides:

- Integrated topology views for graphical representation of gateways and details per site
- Application performance scores for WAN circuit health, bandwidth availability and tunnel status for each site
- WAN orchestration for the management of routing preferences across branch locations and data centers
- Virtual Gateway management to directly extend policies to the public cloud hosted gateways
- VPN services for remote APs (IAP-VPN) and VIA client users

Workflows also exist that allow IT to look into specific device, policy or circuit configuration information to improve the user experience.

Threat Defense with IPS/IDS

To improve security against a growing attack surface, gateways deployed in SD-WAN mode add role and identity-based intrusion detection and prevention (IDS/IPS) capabilities on top of existing security features. Advanced Aruba Central security dashboard provides IT Teams with network-wide visibility, multi-dimensional threat metrics, threat intelligence data, correlation and incident management. This feature requires an Aruba Central Thread Defense subscription license.

AUTOMATED MOBILE AND IOT DEVICE SECURITY

To facilitate the deployment of mobile and Internet of Things (IoT) devices, Aruba Central can directly display information gathered from Aruba ClearPass Device Insight, which offers AI/ML based profiling. Device Insight automatically categorizes all devices on any wired or wireless network.

The use of packet inspection also allows Aruba Central to create behavioral profiles for the devices connected to the network. IT can use Aruba Central to see specific traffic patterns for any device to ensure that a device is actually what it is displayed as.

Figure 5: Mobile & IoT device visibility for accurate policy use

A MICROSERVICES APPROACH

Agility in the software world is the difference between waiting for months versus days for a new feature or fix. Aruba Central is designed to deliver fault tolerance and flexibility so that new services can easily be added without effecting core functionality.

The flexibility also extends to Aruba's ability to offer a cloud-like experience via an on-premises option if desired.

CLOUD SECURITY AND RELIABILITY

Designed from the ground up, Aruba Central ensures the highest possible availability through:

- A web-scale database design for responsive performance, even when working with large amounts of data
- Service redundancy, hosted from data centers worldwide in multiple locations
- Secure HTTPS connectivity, with certificate-based authentication for the highest level of protection

FLEXIBLE PRICING AND SUPPORT

A predictable, As-A-Service model makes it easy to build the right solution for every business and budgetary need. This includes:

- Device subscriptions for base management, and services subscriptions for value added guest Wi-Fi and user analytics
- Ability to utilize subscriptions across devices and services
- Online and phone support for any technical issue

Fuente del anexo: https://www.arubanetworks.com/products/networking/management/central/
Apartado desde el que se referencia este anexo: " 3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y Licenciamiento SD-WAN Aruba" - "4.1.3.2 Software de gestión y administración del piloto SD-WAN"

ORDERING INFORMATION	
Part Number	**Description**
Device Management Subscription	
JY925AAE	Aruba Central Device Management Subscription for 1 Year
JY926AAE	Aruba Central Device Management Subscription for 3 Years
JY927AAE	Aruba Central Device Management Subscription for 5 Years
Services Subscription	
JY928AAE	Aruba Central Services Management Subscription for 1 Year
JY929AAE	Aruba Central Services Management Subscription for 3 Years
JY930AAE	Aruba Central Services Management Subscription for 5 Years
Refer to the following portfolio pages for additional information on Aruba Access Points, Switches and SD-WAN networking solutions	
Access Points: https://www.arubanetworks.com/products/networking/access-points/	
Switches: https://www.arubanetworks.com/products/networking/switches/	
SD-WAN: https://www.arubanetworks.com/products/networking/gateways-and-controllers/	

Note: Aruba Central Managed (CM) SKUs are available to simplify ordering within the U.S. and Canada. Refer to the Wireless Access Point and Switch Data Sheets for more information.

aruba
a Hewlett Packard Enterprise company

DS_ArubaCentral_SK_032020 a00049630enw

Contact Us Share

Fuente del anexo: https://www.arubanetworks.com/products/networking/management/central/
Apartado desde el que se referencia este anexo: " 3.6.1.2 Equipamiento SD-WAN Aruba" - "3.6.2.2 Mantenimiento y Licenciamiento SD-WAN Aruba" - "4.1.3.2 Software de gestión y administración del piloto SD-WAN"

Anexo XVII

Se adjunta copia del documento "*DATA SHEET: ARUBA 7000 SERIES MOBILITY CONTROLLERS*" y "*DATA SHEET: ARUBA 7200 SERIES MOBILITY CONTROLLERS*", donde se detallan capacidades y características de las controladoras WIFI de la serie 7000 y 7200 respectivamente. Algunas de las características son compatibles y complementarias para las gateways SD-WAN de la mismas series expuestas en el Anexo XIV. A fecha de redacción de este trabajo, el documento se puede descargar en la siguiente dirección:

https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf

https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf

aruba
a Hewlett Packard Enterprise company

DATA SHEET

ARUBA 7000 SERIES MOBILITY CONTROLLERS

Improved network performance, visibility, and control

Aruba 7000 Series Mobility Controllers enhance WLAN performance by centralizing all control functionality for individual Aruba access points (APs) to improve AP utilization, security, and client roaming. Ideally suited for midsize campuses and branches, the 7000 Series can be deployed using Zero Touch Provisioning (ZTP) to simplify deployment.

SIMPLE AND SECURE ACCESS

The 7000 Series serves a key role in Dynamic Segmentation, providing Aruba's Policy Enforcement Firewall (PEF) to enforce policies based on user role, device type, application, and network location - and simplifying and securing wired and wireless network access. Traffic is encapsulated in GRE tunnels for complete encryption all the way from an AP or switch. This feature can be enabled with the ArubaOS PEF license and eliminates the need to manually configure SSIDs, VLANs or ACLs for each new client on the network.

HIGH PERFORMANCE AND RELIABILITY

Each 7000 Series provides connectivity for up to 4,096 concurrent users or client devices, 64 access points and include up to 24 Ethernet ports and multiple WAN uplinks. With 8Gbps of maximum throughput to perform Policy Enforcement Firewall (PEF) features, the 7000 Series delvers plenty of horsepower for the most demanding enterprise environments. These capabilities are over 40 times the client density and 10 times the maximum throughput of typical network appliances.

For enhanced resiliency and availability, the 7000 Series can be clustered together in a network.

24/7 MISSION-CRITICAL NETWORKING

Aruba's unique patented wireless technologies are based on AI-powered machine learning algorithms and integrated directly into ArubaOS. Adaptive Radio Management, AirMatch and ClientMatch (now enhanced with Wi-Fi 6 grouping) provide RF optimization techniques to improve user experience and network health based on changing environmental conditions, correct for noisy or congested RF and resolve sticky client issues during user roaming. RFProtect provides advanced spectrum analysis and wireless intrusion protection (WIPS/WIDS) to help identify and mitigate Wi-Fi and non-Wi-Fi sources of interference, as well as containment of potential security risks. Learn more about Aruba's software features on the ArubaOS datasheet.

When deployed with Aruba Mobility Master, the 7000 Series can be joined to a controller cluster to increase scale, improve reliability using High Availability (HA), adopt configurations seamlessly based on hierarchy, support Live Upgrades to reduce maintenance windows, and share licenses from a global licensing pool. The 7000 Series also serves a key policy enforcement role in Aruba's 360 Secure Fabric. Aruba AirWave provides real-time monitoring, reporting and Wi-Fi planning and visibility services.

Learn more about the 7000 Series Mobility Controller features in the ArubaOS datasheet.

*7005, 7008, 7010 and 7030 Mobility Controllers shown

KEY FEATURES

- Support for new Wi-Fi 6 (802.11ax), WPA3 and Enhanced Open – and existing standards
- Patented ClientMatch technology can now group together Wi-Fi 6 capable devices
- Dynamic Segmentation enforces wired and wireless access policies to simplify and secure the network
- Application awareness for 3,000+ applications without additional hardware
- Built-in AI-powered wireless/RF optimization
- 8 Gbps of maximum firewall throughput

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

SD-WAN DEPLOYMENT

For organizations that are now managing multiple WAN connections, the 7000 Series can be connected to Aruba's SD-WAN fabric right out of the box. SD-WAN is a rich WAN management solutions that is used to simplify management of traffic entering and exiting branch sites. Please refer to the SD-WAN datasheet for more information.

MICROSOFT FEATURES

Aruba's integration with Microsoft enables unique application intelligence that detects Microsoft 365, Teams and Skype for Business traffic and then prioritizes them over less critical applications. Through management interfaces on ArubaOS, Aruba Central, and Aruba AirWave, IT can visualize call quality metrics such as MOS, latency, jitter, and packet loss for additional insights.

ENHANCED CAPABILITIES

Wi-Fi 6 (802.11ax) enhanced with ClientMatch

The latest Wi-Fi standard brings enhanced performance, speed, and efficiency with key features such as OFDMA, 1024-QAM, and bidirectional MU-MIMO. Combined with Aruba's patented ClientMatch technology, 802.11ax clients will now be grouped together to optimize the multi-user experience.

Enhanced wireless security

Support for WPA3 brings stronger encryption and authentication methods, while Enhanced Open brings automatic security to open networks. New WPA2-MPSK feature enables simpler passkey management for WPA2 devices – should the Wi-Fi password on one device need to be changed, no additional key changes are needed for other devices on the network.

Dynamic Segmentation

To simplify and better secure wired and wireless network access, the 7000 Series can enforce per-user and device roles across wired and wireless networks by integrating with ClearPass Policy Manager. This ensures consistent policy regardless of user role and device type, and eliminates the need to configure unnecessary SSIDs, ACLs, VLANs and subnets at every node in the network.

Policy Enforcement Firewall

Enabled by the PEF license, wired and wireless user and application traffic can be tunneled to a stateful firewall on the 7000 Series through GRE tunnels for inspection. Policies are then enforced based on user role, device type, application and location - as described in Dynamic Segmentation.

Application visibility and control

As part of the PEF license, application visibility with Deep Packet Inspection (DPI) technology evaluates and optimizes performance and Quality of Service policies for over 3,000 applications - even for encrypted or hidden traffic.

Web content filtering

WebCC is an add-on subscription-based feature that classifies websites by content category and rates them by reputation. It can also block, apply QoS, bandwidth-limit, mirror, and log web content.

Unified Communications and Collaboration (UCC)

Visualize and troubleshoot networks based on call quality metrics such as MOS, latency, jitter and packet loss. Supported applications include: Teams, Skype for Business®, Wi-Fi Calling, Facetime, SIP, Jabber, Spark and more.

Zero Touch Provisioning

The 7000 Series can be factory-shipped and deployed onsite with cloud-based Aruba Activate. For network-specific requirements, settings can be applied based on hierarchical configuration.

Integrated VPN services

With support for IPSec/SSL VPNs, Aruba remote APs (RAPs) and Aruba VIA VPN users can establish encrypted sessions without any additional hardware required.

Third-party security integration

For advanced malware or antivirus protection, the 7000 Series can assume the role of an on-premises agent of centrally-hosted firewalls such as those provided by Palo Alto Networks and Check Point Software. Dedicated firewall appliances are no longer needed at each branch.

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

PERFORMANCE AND CAPACITY					
Features	**7005**	**7008**	**7010**	**7024**	**7030**
Maximum campus or remote AP licenses	16	16	32	32	64
Maximum concurrent users/devices	1,024	1,024	2,048	2,048	4,096
Maximum VLANs	4,096	4,096	4,096	4,096	4,096
Active firewall sessions	64K	64K	64K	64K	64K
Concurrent GRE tunnels	256	256	512	512	1,024
Concurrent IPsec sessions	1,024	1,024	2,048	2,048	4,096
Concurrent SSL sessions	1,024	1,024	2,048	2,048	4,096
Firewall throughput (Gbps)	4	4	8	8	8
Wired Bridged Throughput (Gbps)	4	4	8	8	8
Encrypted throughput 3DES (Gbps)	1.2	1.2	2.4	2.4	2.4
Encrypted throughput AES-CBC-256 (Gbps)	1.3	1.3	2.6	2.6	2.6
Encrypted throughput AES-CCM (Gbps)	2.0	2.0	3.4	3.4	4.0
Encrypted throughput AES-GCM-256 (Gbps)	1.7	1.7	3.3	3.3	3.4

INTERFACES AND INDICATORS					
Features	**7005**	**7008**	**7010**	**7024**	**7030**
Form factor/footprint	Desktop/fanless	Desktop/fanless	1xRU	1xRU	1xRU
10/100/1000BASE-T	4	8	16	24	8 (combo)
1000BASE-X	–	–	2xSFP	–	
10G Ports (10G or 1G supported)	–	–	–	2xSFP+	–
USB 2.0	1	2	2	1	1
Management/status LEDs	Yes	Yes	Yes	Yes	Yes
LINK/ACT and status LEDs	Yes	Yes	Yes	Yes	Yes
LCD panel and navigation buttons	No	No	Yes	Yes	Yes
Console port	mini USB, RJ-45	RJ-45	mini USB, RJ-45	micro USB, RJ-45	mini USB, RJ-45
Out-of-band management port	No	No	Yes	Yes	No

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

POWER OVER ETHERNET (PoE) SUPPORT

	7005	7008	7010	7024	7030
PoE[1] Role/Mode	Powered Device (PD)	Power Source Equipment (PSE)	PSE	PSE	–
PoE In or Out	In – Port 0	Out	Out	Out	–
Max concurrent of PoE Ports	–	8	12	24	–
Max[2] concurrent PoE+ Ports	–	8	12	24	–
PoE Power Budget	–	100W	150W	400W	–

[1] PoE: 802.3af, up to 15.4W from the PSE and up to 12.95W at the PD, not to exceed the total PoE Power Budget.
[2] PoE+: 802.3at, up to 30W per port from the PSE and up to 25.5W at the PD, not to exceed the total PoE Power Budget.

PHYSICAL

	7005	7008	7010	7024	7030
Dimensions (H x W x D)	4.1 cm x 20 cm x 20 cm (1.6" x 7.9" x 7.9")	4.2 cm x 20.32 cm x 20.32 cm (1.65" x 8.0" x 8.0")	4.42 cm x 31.75 cm x 33.7 cm (1.74" x 12.75" x 13.3")	4.37 cm x 44.2 cm x 31.3 cm (1.72" x 17.4" x 12.32")	4.4 cm x 30.5 cm x 21.1 cm (1.7" x 12" x 8.3")
Weight	0.92 kg (2.03 lbs)	1.0 kg (2.2 lbs)	3.4 kg (7.5 lbs)	5.127 kg (11.3 lbs)	2.06 kg (4.54 lbs)
MTBF (hours, @ 40C)	323,896	300,000	232,843	311,901	390,679

ENVIRONMENTAL RANGE

Specification	7005	7008	7010	7024	7030
Operating temperature	0° C to 40° C				
Storage temperature	-40° C to 70° C				
Humidity/Storage Humidity	5% to 95%, NC	5% to 95%, NC	5% to 95%, NC	10% to 95%, NC	5% to 95%, NC
Operating Altitude	10,000 feet				
Acoustic noise[3]	0 dBA (fanless)	0 dBA (fanless)	39.8 – 58.6 dBA	34.3 – 71.2 dBA	29.1 – 57.4 dBA
Maximum Heat Dissipation (BTU/hour)	51.18	430	300	1842	168
Maximum power consumption	16.6W (with USB)	126W (with PoE)	190W (with PoE)	450W (with PoE)	55W
Power Source	PoE or 12v - 30W	150-watt power supply	internal power supply	internal power supply	internal power supply

[3] Sound power per ETSI 300 753 in accordance with ISO 7779

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

POWER ADAPTER AND SUPPLY SPECIFICATIONS

Features	12v - 30W	150-watt
Input voltage range	90 VAC to 264 VAC	90 VAC to 264 VAC
Output Voltage	+12VDC, 4A	54VDC, 2.78A
Input frequency	47-63 Hz	47-63 Hz
AC line input current (steady state)	1.0A	2.0A
Operating Temperature	-0o to +40o C	-0o to +40o C
Cooling	–	–
Weight	.24 kg (.53 lbs)	.72 kg (1.58 lbs)

REGULATORY AND SAFETY COMPLIANCE

Features	7005	7008	7010	7024	7030
Regulatory SKU information	ARCN01014	ARCN7008	ARCN0103	ARCN7024	ARCN7030
Minimum ArubaOS Release	6.4.1.0	6.5.0.0	6.4.1.0	6.4.3.0	6.4.1.0
	WI-FI CERTIFIED WPA3, AOS 8.4; WI-FI CERTIFIED Enhanced Open, AOS 8.4; Wi-Fi 6 (802.11ax), AOS 8.4; WI-FI CERTIFIED 802.11ad, AOS 8.4				
Safety certifications	UL 60950-1 Second Edition CAN/CSA-C22.2 No. 60950-1 Second Edition EN 60950-1 Second Edition EN 60950:2005 IEC 60950-1 Second Edition NOM (obtained by partners and distributors)				
Electromagnetic emissions certifications	FCC Part 15 Class B CE AS/NZS CISPR22 Class B CISPR22 Class A (7010, 7024, 7030), Class B (7005) EN55022 Class A (7010, 7024, 7030), Class B (7005) ICES-003 Class A (7010, 7024, 7030), Class B (7005) VCCI Class A (7010, 7024, 7030), Class B (7005) EN61000-3-2 EN61000-3-3 EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4- 6, EN 61000-4-8, EN 61000-4-11, AS/NZS 3548 KN22 Class B KCC CNS13438 Class B EN55024/CISPR24 KN24 Industry Canada Class B CE mark, cTUVus, CB, C-tick, Anatel, NOM, MIC				
Telco	Common Language Equipment Identifier (CLEI) Code				

SERVICE AND WARRANTY INFORMATION

- Hardware: 1 year parts/labor, can be extended with support contract
- Software: 90 days, can be extended with support contract

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

ORDERING INFORMATION

Part Number	Description
Aruba 7005 Series Mobility Controllers	
JW633A	Aruba 7005 (RW) 4-port 10/100/1000BASE-T 16 AP and 1K Client Controller
JW634A	Aruba 7005 (US) 4-port 10/100/1000BASE-T 16 AP and 1K Client Controller
JW635A	Aruba 7005 (RW) FIPS/TAA-compliant 4-port 10/100/1000BASE-T 16 AP and 1K Client Controller
JW636A	Aruba 7005 (US) FIPS/TAA-compliant 4-port 10/100/1000BASE-T 16 AP and 1K Client Controller
JW637A	Aruba 7005 (IL) 4-port 10/100/1000BASE-T 16 AP and 1K Client Controller
JW638A	Aruba 7005 (IL) FIPS/TAA-compliant 4-port 10/100/1000BASE-T 16 AP and 1K Client Controller
JW639A	Aruba 7005 (JP) 4-port 10/100/1000BASE-T 16 AP and 1K Client Controller
JW640A	Aruba 7005 (JP) FIPS/TAA-compliant 4-port 10/100/1000BASE-T 16 AP and 1K Client Controller
JY849A	Aruba 7005 (EG) 4x 10/100/1000BASE-T Ports 16 AP Branch Controller
Aruba 7008 Series Mobility Controllers	
JX925A	Aruba 7008 (IL) 8p 100W PoE+ 10/100/1000BASE-T 16 AP and 1K Client Controller
JX926A	Aruba 7008 (JP) 8p 100W PoE+ 10/100/1000BASE-T 16 AP and 1K Client Controller
JX927A	Aruba 7008 (RW) 8p 100W PoE+ 10/100/1000BASE-T 16 AP and 1K Client Controller
JX928A	Aruba 7008 (US) 8p 100W PoE+ 10/100/1000BASE-T 16 AP and 1K Client Controller
JX929A	Aruba 7008 (IL) FIPS/TAA 8p 100W PoE+ 10/100/1000BASE-T 16 AP and 1K Client Controller
JX930A	Aruba 7008 (JP) FIPS/TAA 8p 100W PoE+ 10/100/1000BASE-T 16 AP and 1K Client Controller
JX931A	Aruba 7008 (RW) FIPS/TAA 8p 100W PoE+ 10/100/1000BASE-T 16 AP and 1K Client Controller
JX932A	Aruba 7008 (US) FIPS/TAA 8p 100W PoE+ 10/100/1000BASE-T 16 AP and 1K Client Controller
Aruba 7010 Series Mobility Controllers	
JW678A	Aruba 7010 (RW) 16p 150W PoE+ 10/100/1000BASE-T 1G BASE-X SFP 32 AP and 2K Clients Controller
JW679A	Aruba 7010 (US) 16p 150W PoE+ 10/100/1000BASE-T 1G BASE-X SFP 32 AP and 2K Clients Controller
JW680A	Aruba 7010(IL) 16p 150W PoE+ 10/100/1000BASE-T 1G BASE-X SFP 32 for AP and 2K Clients Controller
JW681A	Aruba 7010 (JP) 16p 150W PoE+ 10/100/1000BASE-T 1G BASE-X SFP for 32 AP and 2K Clients Controller
JW702A	Aruba 7010 (RW) FIPS/TAA 16p 150W PoE+ 10/100/1000BASE-T 1GBASE-X SFP 32 AP and 2K Clients Controller
JW703A	Aruba 7010 (US) FIPS/TAA 16p 150W PoE+ 10/100/1000BASE-T 1GBASE-X SFP 32 AP and 2K Clients Controller
JW704A	Aruba 7010 (IL) FIPS/TAA 16p 150W PoE+ 10/100/1000BASE-T 1G BASE-X SFP 32 AP and 2K Clients Controller
JW705A	Aruba 7010 (JP) FIPS/TAA 16p 150W PoE+ 10/100/1000BASE-T 1GBASE-X SFP 32 AP and 2K Clients Controller
JY850A	Aruba 7010 (EG) 16x 1000BASE-T + 2x SFP Ports 32 AP Branch Controller
Aruba 7024 Series Mobility Controllers	
JW682A	Aruba 7024 (RW) 24-port 400W PoE+ 10G BASE-X SFP+ 32 AP and 2K Clients Controller
JW683A	Aruba 7024 (US) 24-port 400W PoE+ 10G BASE-X SFP+ 32 AP and 2K Clients Controller
JW684A	Aruba 7024 (IL) 24-port 400W PoE+ 10G BASE-X SFP+ 32 AP and 2K Clients Controller
JW685A	Aruba 7024 (JP) 24-port 400W PoE+ 10G BASE-X SFP+ 32 AP and 2K Clients Controller
JW706A	Aruba 7024 (RW) FIPS/TAA-compliant 24p 400W PoE+ 10G BASE-X SFP+ 32 AP and 2K Clients Controller
JW707A	Aruba 7024 (US) FIPS/TAA-compliant 24p 400W PoE+ 10G BASE-X SFP+ 32 AP and 2K Clients Controller
JW708A	Aruba 7024 (IL) FIPS/TAA-compliant 24p 400W PoE+ 10G BASE-X SFP+ 32 AP and 2K Clients Controller
JW709A	Aruba 7024 (JP) FIPS/TAA-compliant 24p 400W PoE+ 10G BASE-X SFP+ 32 AP and 2K Clients Controller

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

ORDERING INFORMATION

Part Number	Description	7010	7024	7030
Aruba 7030 Series Mobility Controllers				
JW686A	Aruba 7030 (RW) 8p Dual Pers 10/100/1000BASE-T/1GBASE-X SFP 64 AP and 4K Clients Controller			
JW687A	Aruba 7030 (US) 8p Dual Pers 10/100/1000BASE-T/1GBASE-X SFP 64 AP and 4K Clients Controller			
JW688A	Aruba 7030 (IL) 8p Dual Pers 10/100/1000BASE-T/1GBASE-X SFP 64 AP and 4K Clients Controller			
JW689A	Aruba 7030 (JP) 8p Dual Pers 10/100/1000BASE-T/1GBASE-X SFP 64 AP and 4K Clients Controller			
JW710A	Aruba 7030 (RW) FIPS/TAA 8p Dual Pers 10/100/1000BASE-T/1GBASE-X SFP 64 AP and 4K Clients Controller			
JW711A	Aruba 7030 (US) FIPS/TAA 8p Dual Pers 10/100/1000BASE-T/1GBASE-X SFP 64 AP and 4K Clients Controller			
JW712A	Aruba 7030 (IL) FIPS/TAA 8p Dual Pers 10/100/1000BASE-T 1GBASE-X SFP 64 AP and 4K Clients Controller			
JW713A	Aruba 7030 (JP) FIPS/TAA 8p Dual Pers 10/100/1000BASE-T/1GBASE-X SFP 64 AP and 4K Clients Controller			
JY851A	Aruba 7030 (EG) 8x 1000BASE-T or 8xSFP64 AP Branch Controller			
Controller Accessories				
JX989A	AP-AC-12V30A 12V 30W Power Adapter			
JX933A	Aruba PSU-150-AC 150W AC Power Supply			
JW083A	Aruba SPR-WL2-MNT S2500/S1500 7024 Wall and Rack Mount Kit			
JW084A	Aruba 7005-MNT-19 7005 Series 19-inch Rack Mount Kit			
JX934A	Aruba 7008-MNT-19 7008 Series 19-inch Rack Mount Kit			
JW085A	Aruba 7010-MNT-19 7010 Series Replacement 19-inch Rack Mounting Kit			
JW082A	Aruba SPR-RK3-MNT 7205/7024/S2500-xx/S1500-24P/48P Spare Front Rack Mount			
JW086A	Aruba 7030-MNT-19 7030 Series Replacement 19-inch Rack Mounting Kit			
Transceivers				
JW087A	Aruba 1000BASE-LX LC Connector SFP XCVR	X	X	X
JW088A	Aruba 1000BASE-SX LC Connector SFP XCVR	X	X	X
JW089A	Aruba 1000BASE-T RJ45 Connector SFP XCVR	X	X	X
JW149A	SFP-EX 1000BASE-EX LC SFP XCVR	X	X	X
JW150A	SFP-ZX 1000BASE-ZX LC SFP XCVR	X	X	X
J4859D	Aruba 1G SFP LC LX 10km SMF Transceiver	X[1]	X[1]	X[1]
J4858D	Aruba 1G SFP LC SX 500m OM2 MMF Transceiver	X[1]	X[1]	X[1]
J4860D	Aruba 1G SFP LC LH 70km SMF Transceiver	X[2]	X[2]	X[2]
J8177D	Aruba 1G SFP RJ45 T 100m Cat5e Transceiver	X[1]	X[1]	X[1]
JW092A	Aruba 10GBASE-LR LC Connector SFP+ XCVR		X	
JW091A	Aruba 10GBASE-SR LC Connector SFP+ XCVR		X	
JW090A	Aruba 10GBASE-LRM LC Connector SFP+ XCVR		X	
JW100A	SFP+ Direct Attach 0.5M Cable		X	
JW101A	SFP+ Direct Attach 1M Cable		X	
JW102A	SFP+ Direct Attach 3M Cable		X	
JW103A	SFP+ Direct Attach 5M Cable		X	
JW104A	SFP+ Direct Attach 7M Cable		X	

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

ORDERING INFORMATION

Part Number	Description	7010	7024	7030
Transceivers (continued)				
JW147A	SFP-10GE-ER 10G LC Cnctr SFP+ XCVR		X	
JW148A	SFP-10GE-ZR 10G LC Cnctr SFP+ XCVR		X	
J9150D	Aruba 10G SFP+ LC SR 300m OM3 MMF Transceiver		X[1]	
J9151E	Aruba 10G SFP+ LC LR 10km SMF Transceiver		X[1]	
J9152D	Aruba 10G SFP+ LC LRM 220m OM2 MMF Transceiver		X[1]	
J9153D	Aruba 10G SFP+ LC ER 40km SMF Transceiver		X[1]	
J9281D	Aruba 10G SFP+ to SFP+ 1m DAC Cable		X[1]	
J9283D	Aruba 10G SFP+ to SFP+ 3m DAC Cable		X[1]	
J9285D	Aruba 10G SFP+ to SFP+ 7m DAC Cable		X[1]	

X: Supported transceiver
[1]Default minimum ArubaOS software version is 6.5.3.0 and 8.1.0.0
[2]Minimum ArubaOS software version is 6.5.4.7 and 8.4.0.0

For additional information on the Aruba 7000 Series Mobility Controllers please refer to:

- ArubaOS Network Operating System Data Sheet (and licenses)
- 7000 Series Mobility Controller
- 7000 Series Ordering Guide
- SD-WAN Data Sheet (and licenses)

aruba
a Hewlett Packard Enterprise company

DS_7000Series_SK_021420 a00059069enw

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

aruba
a Hewlett Packard Enterprise company

DATA SHEET

ARUBA 7200 SERIES MOBILITY CONTROLLERS

Improved network performance, visibility, and control

Aruba 7200 Series Mobility Controllers enhance WLAN performance for high performance, high density enterprise requirements. The 7200 Series centralizes all control functionality for individual Aruba access points (APs) to improve AP utilization, security, and client roaming. Ideally suited for large campuses and high density environments, the 7200 Series can be deployed using Zero Touch Provisioning (ZTP) to simplify deployment.

SIMPLE AND SECURE ACCESS

The 7200 Series serves a key role in Dynamic Segmentation, providing Aruba's Policy Enforcement Firewall (PEF) to enforce policies based on user role, device type, application, and network location - and simplifying and securing wired and wireless network access. Traffic is encapsulated in GRE tunnels for complete encryption all the way from an AP or switch. This feature can be enabled with the ArubaOS PEF license and eliminates the need to manually configure SSIDs, VLANs or ACLs for each new client on the network.

HIGH PERFORMANCE AND RELIABILITY

Each 7200 Series provides connectivity for up to 32,728 concurrent users or client devices, 2,048 access points and over 2 million active firewall sessions. With up to 80 virtual CPUs and 100Gbps of maximum throughput to perform Policy Enforcement Firewall (PEF) features, the 7200 Series are in a class of their own -- ideal for the most demanding enterprise, college, and large public venue requirements.

KEY FEATURES

- Support for new Wi-Fi 6 (802.11ax), WPA3 and Enhanced Open – and existing standards
- Patented ClientMatch technology can now group together Wi-Fi 6-capable devices
- Dynamic Segmentation enforces wired and wireless access policies to simplify and secure the network
- Application awareness for 3,000+ applications without additional hardware
- Built in AI-powered wireless/RF optimization
- Unifies policy enforcement for WLAN, LAN and WAN traffic

For enhanced resiliency and availability, the 7200 Series can be clustered together in a network managed by Aruba Mobility Master.

Front: 7205

Back: 7205

Front: 7210/7220/7240/7240XM

Back: 7210/7220/7240/7240XM

Front: 7280

Back: 7280

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

24/7 MISSION-CRITICAL NETWORKING

Aruba's unique, patented wireless technologies are based on AI-powered machine learning algorithms and integrated directly into ArubaOS. Adaptive Radio Management, AirMatch and ClientMatch (now enhanced with Wi-Fi 6 grouping) provide RF optimization techniques to improve user experience and network health based on changing environmental conditions, correct for noisy or congested RF and resolve sticky client issues during user roaming. RFProtect provides advanced spectrum analysis and wireless intrusion protection (WIPS/WIDS) to help identify and mitigate Wi-Fi and non-Wi-Fi sources of interference, as well as containment of potential security risks. Learn more about Aruba's software features on the ArubaOS datasheet.

When deployed with the Aruba Mobility Master, the 7200 Series can be joined to a controller cluster to increase scale, improve reliability using enhanced High Availability (HA), adopt configurations seamlessly based on hierarchy, support Live Upgrades to reduce maintenance windows and share licenses from a global licensing pool. The 7200 Series also serves a key, policy enforcement role in Aruba's 360 Secure Fabric. For network management, Aruba AirWave provides real-time monitoring, reporting and Wi-Fi location services.

Learn more about the 7200 Series Mobility Controller features in the ArubaOS datasheet.

SD-WAN DEPLOYMENT

For organizations that are now managing multiple WAN connections, the 7200 Series can be connected to Aruba's SD-WAN fabric right out of the box. SD-WAN is a rich WAN management solutions that is used to simplify management of traffic entering and exiting branch sites. Please refer to the SD-WAN datasheet for more information.

MICROSOFT FEATURES

Aruba's integration with Microsoft enables unique application intelligence that detects Microsoft 365, Teams and Skype for Business traffic and then prioritizes them over less critical applications. Through management interfaces on ArubaOS, Aruba Central, and Aruba AirWave, IT can visualize call quality metrics such as MOS, latency, jitter, and packet loss for additional insight.

ENHANCED CAPABILITIES:

Wi-Fi 6 (802.11ax) enhanced with ClientMatch

The latest Wi-Fi standard brings enhanced performance, speed, and efficiency with key features such as OFDMA, 1024-QAM, and bidirectional MU-MIMO. Combined with Aruba's patented ClientMatch technology, 802.11ax clients will now be grouped together to optimize the multi-user experience.

Enhanced wireless security

Support for WPA3 brings stronger encryption and authentication methods, while Enhanced Open brings automatic security to open networks. New WPA2-MPSK feature enables simpler passkey management for WPA2 devices – should the Wi-Fi password on one device need to be changed, no additional key changes are needed for other devices on the network.

Dynamic Segmentation

To simplify and better secure wired and wireless network access, the 7200 Series can enforce per-user and device roles across wired and wireless networks by integrating with ClearPass Policy Manager. This ensures consistent policy regardless of user role and device type, and eliminates the need to configure unnecessary SSIDs, ACLs, VLANs and subnets at every node in the network.

Policy Enforcement Firewall

Enabled by the PEF license, wired and wireless user and application traffic can be tunneled to a stateful firewall on the 7200 Series through GRE tunnels for inspection. Policies are then enforced based on user role, device type, application and location - as described in Dynamic Segmentation.

Application visibility and control

Enabled by the PEF license, application visibility with Deep Packet Inspection (DPI) technology evaluates and optimizes performance and Quality of Service policies for over 3,000 applications - even for encrypted or hidden traffic.

Web content filtering

WebCC is an add-on subscription-based feature that classifies websites by content category and rates them by reputation. It can also block, apply QoS, bandwidth-limit, mirror, and log web content.

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

Unified Communications and Collaboration (UCC)

Visualize and troubleshoot networks based on call quality metrics such as MOS, latency, jitter and packet loss. Supported applications include: Teams, Skype for Business, Wi-Fi Calling, Facetime, SIP, Jabber, Spark and more.

Zero Touch Provisioning

The 7200 Series can be factory-shipped and deployed onsite with cloud-based Aruba Activate. For network-specific requirements, settings can be applied based on hierarchical configuration.

Integrated VPN services

With support for IPSec/SSL VPNs, Aruba Remote APs (RAPs) and Aruba VIA VPN users can establish encrypted sessions without any additional hardware required.

Third-party security integration

For advanced malware or antivirus protection, the 7200 Series can assume the role of an on-premises agent of centrally-hosted firewalls such as those provided by Palo Alto Networks and Check Point Software.

PERFORMANCE AND CAPACITY

Features	7205	7210	7220	7240XM	7280
Maximum campus or remote AP licenses	256	512	1,024	2,048	2,048
Maximum concurrent users/devices	8,192	16,384	24,576	32,768	32,768
Maximum VLANs	4,096	4,096	4,096	4,096	4,096
Active firewall sessions	1 million (M)	2M	2M	2M	2M
Concurrent GRE tunnels	4,096	8,192	16,384	32,768	32,768
Concurrent IPsec sessions	8,192	16,384	24,576	32,768	32,768
Concurrent SSL sessions	4,096	8,192	8,192	8,192	8,192
Firewall throughput (Gbps)	12	20	40	40	100
Wired Bridged Throughput (Gbps)	12	20	40	40	100
Encrypted throughput 3DES (Gbps)	5	7	25	28	57
Encrypted throughput AES-CBC-256 (Gbps)	5	7	22	30	46
Encrypted throughput AES-CCM (Gbps)	5	7	20	29	75
Encrypted throughput AES-GCM-256 (Gbps)	5	7	26	35	70

INTERFACES AND INDICATORS

Features	7205	7210	7220	7240XM	7280
Form factor/footprint	1xRU	1xRU	1xRU	1xRU	1xRU
10/100/1000BASE-T	4xCombo	2xCombo	2xCombo	2xCombo	–
1000BASE-X					
10G Ports (10G or 1G supported)	2xSFP+	4xSFP+	4xSFP+	4xSFP+	8xSFP+
40G Ports	–	–	–	–	2xQSFP+
USB 2.0	2	1	1	1	1
Management/status LEDs	Yes	Yes	Yes	Yes	Yes
LINK/ACT and status LEDs	Yes	Yes	Yes	Yes	Yes
LCD panel and navigation buttons	Yes	Yes	Yes	Yes	Yes
Console port	Micro USB, RJ-45	Mini USB, RJ-45	Mini USB, RJ-45	Mini USB, RJ-45	Micro USB, RJ-45
Out-of-band management port	Yes	No	No	No	Yes

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

PHYSICAL

Features	7205	7210	7220	7240XM	7280
Dimensions (HxWxD)	(H) 4.4 cm x (W) 44.2 cm x (D) 33.4 cm (1.75" x 17.38" x 13.13")	(H) 4.4 cm x (W) 44.5 cm x (D) 44.5 cm (1.75" x 17.5" x 17.5")			(H) 4.4 cm x (W) 44.2 cm x (D) 40.1 cm (1.73" x 17.40" x 15.79")
Weight	4.95 kg (10.19 lbs.)	7.45 kg (16.43 lbs.)			7.9 kg (17.41 lbs)
MTBF (Hours)	129,597 (@40C)	106,536 (@40C)	113,751 (@40C)	116,590 (@40C)	281,896 (@45C)

ENVIRONMENTAL RANGE

Features	7205	7210	7220	7240XM	7280
Operating Temperature	0° C to 40° C				
Storage Temperature	-40° C to 70° C				
Humidity/Storage Humidity	10% to 95%, NC	5% to 95%, NC	5% to 95%, NC	5% to 95%, NC	5% to 95%, NC
Operating Altitude	10,000 feet				
Acoustic Noise[1]	49 dBA	52.9 dBA			47.1 dBA
Maximum Heat Dissipation (BTU/hour)	260	375	427	563	819
Maximum Power Consumption	75.2W	110W	125W	165W	240W
Power Source	Internal power supply	350-watt AC or DC power supply			550-watt power supply

[1]Sound power per ETSI 300 753 in accordance with ISO 7779

POWER ADAPTER AND SUPPLY SPECIFICATIONS

Features	350-watt AC	350-watt DC	550-watt
Input voltage range	100 VAC to 240 VAC	DC -48V to DC -60V	100 VAC to 240 VAC
Output Voltage	+12VDC, 29.16A	+12VDC, 29.16A	+12VDC, 29.16A
Input frequency	50-60 Hz	50-60 Hz	50-60 Hz
AC line input current (steady state)	5 - 2.5A	5 - 2.5A	7.1 - 3.4A
Operating Temperature	-5o to +55o C	-5o to +55o C	-5o to +55o C
Cooling	Internal fan (Air flow rear to front)	Internal fan (Air flow rear to front)	819 Internal fan (Air flow rear to front)
Weight	1.3 kg (2.8 lbs)	1.3 kg (2.8 lbs)	0.87 kg (1.9 lbs)

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

REGULATORY AND SAFETY COMPLIANCE					
Features	**7205**	**7210**	**7220**	**7240XM**	**7280**
Regulatory SKU information	ARCN7205	ARCN0100	ARCN0101	ARCN0102	ARCN7280
Minimum ArubaOS Release	6.4.3.0	6.2.0.0	6.2.0.0	6.4.4.0	6.5.4.0 or 8.3.0.0
	802.11ax (Wi-Fi 6), AOS 8.4; WI-FI CERTIFIED WPA3™, AOS 8.4; WI-FI CERTIFIED Enhanced Open™, AOS 8.4				
Regulatory and Safety Compliance	FCC Part 15 Class A CE				
	Industry Canada Class A				
	VCCI Class A (Japan)				
	EN 55022 Class A (CISPR 22 Class A), EN 61000-3, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11, EN 55024, AS/NZS 3548				
	UL 60950, EN60950				
	CAN/CSA 22.2 #60950				
	CE mark, cTUVus, CB, C-tick, Anatel, NOM, MIC				
Telco	Common Language Equipment Identifier (CLEI) Code				

SERVICE AND WARRANTY INFORMATION

- Hardware: 1 year parts/labor, can be extended with support contract
- Software: 90 days, can be extended with support contract

ORDERING INFORMATION	
Part Number	Description
Aruba 7205 Series Mobility Controllers	
JW735A	Aruba 7205 (RW) 2-port 10GBASE-X (SFP+) Controller
JW736A	Aruba 7205 (US) 2-port 10GBASE-X (SFP+) Controller
JW737A	Aruba 7205 (JP) 2-port 10GBASE-X (SFP+) Controller
JY852A	Aruba 7205 (EG) 2x 10GBASE-X SFP+ Controller
JW738A	Aruba 7205 (IL) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller
JW739A	Aruba 7205 (RW) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller
JW740A	Aruba 7205 (US) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller
JW741A	Aruba 7205 (JP) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller
JW742A	Aruba 7205 (IL) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

ORDERING INFORMATION

Part Number	Description
Aruba 7210 Series Mobility Controllers	
JW743A	Aruba 7210 (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW744A	Aruba 7210 (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JY853A	Aruba 7210 (EG) 4x 10GBase-x SFP/SFP+ Controller
JW645A	Aruba 7210DC (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW646A	Aruba 7210DC (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW745A	Aruba 7210 (RW) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW746A	Aruba 7210 (US) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW747A	Aruba 7210 (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW647A	Aruba 7210DC (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW748A	Aruba 7210 (IL) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP)
JW749A	Aruba 7210 (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW648A	Aruba 7210DC (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW750A	Aruba 7210 (JP) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
Aruba 7220 Series Mobility Controllers	
JW751A	Aruba 7220 (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW752A	Aruba 7220 (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW649A	Aruba 7220DC (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW650A	Aruba 7220DC (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW753A	Aruba 7220 (RW) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW754A	Aruba 7220 (US) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP)
JW755A	Aruba 7220 (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW651A	Aruba 7220DC (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW756A	Aruba 7220 (IL) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP)
JW757A	Aruba 7220 (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW652A	Aruba 7220DC (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW758A	Aruba 7220 (JP) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP)

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

ORDERING INFORMATION

Part Number	Description
Aruba 7240XM Series Mobility Controllers	
JW784A	Aruba 7240XM (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW830A	Aruba 7240XM (US) FIPS/TAA 16GB DRAM 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JY854A	Aruba 7240XM (EG) 4x 10GBase-x SFP/SFP+ Controller
JW675A	Aruba 7240XMDC (US) 16GB DRAM 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr
JW783A	Aruba 7240XM (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW829A	Aruba 7240XM (RW) FIPS/TAA 16GB DRAM 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW674A	Aruba 7240XMDC (RW) 16GB DRAM 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr
JW786A	Aruba 7240XM (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW832A	Aruba 7240XM (IL) FIPS/TAA 16GB DRAM 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW677A	Aruba 7240XMDC (IL) 16GB DRAM 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr
JW785A	Aruba 7240XM (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW831A	Aruba 7240XM (JP) FIPS/TAA 16GB DRAM 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW676A	Aruba 7240XMDC (JP) 16GB DRAM 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr
Aruba 7240 to 7240XM Series Upgrades	
JW834A	Aruba 7240XM (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW838A	Aruba 7240XM (US) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW842A	Aruba 7240XMDC (US) 4p 10GBase-X/SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr 16GB Upgrade
JW833A	Aruba 7240XM (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW837A	Aruba 7240XM (RW) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW841A	Aruba 7240XMDC (RW) 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr 16GB Upgrade
JW836A	Aruba 7240XM (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW840A	Aruba 7240XM (IL) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW844A	Aruba 7240XMDC (IL) 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr 16GB Upgrade
JW835A	Aruba 7240XM (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW839A	Aruba 7240XM (JP) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW843A	Aruba 7240XMDC (JP) 4p 10GBase-X/SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr 16GB Upgrade

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

ORDERING INFORMATION

Part Number	Description
Aruba 7280 Series Mobility Controllers	
JX910A	Aruba 7280 (US) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX911A	Aruba 7280 (RW) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX912A	Aruba 7280 (JP) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX913A	Aruba 7280 (IL) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX914A	Aruba 7280 (US) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX915A	Aruba 7280 (RW) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX916A	Aruba 7280 (JP) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX917A	Aruba 7280 (IL) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
JZ077A	Aruba 7280 (EG) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JZ078A	Aruba 7280 (EG) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
Controller Accessories	
Aruba 7205/7280 Series Wall/Rack Mount	
JW083A	Aruba SPR-WL2-MNT 7205/7280 - Wall/Rack Mount
Aruba 7210/7220/7240/7240XM Series Wall/Rack Mount	
JW109A	Aruba SPR-WL-MNT 7210/7220/7240/7240XM - Wall/Rack Mount
Aruba 7210/7220/7240/7240XM Redundant Power Supplies and Fan Tray	
JW657A	Aruba PSU-350-AC 7200 Series S3500-24T S3500-48T and S3500-24F 350W AC Power Supply
JW658A	Aruba PSU-350-DC 7200 Series Mobility Controllers 350W DC (-48V DC) Power Supply
JW111A	Aruba HW-7200-FT 7200 Series Fan Tray
Aruba 7280 Redundant Power Supply and Fan Tray	
JZ012A	PSU-550-AC 550W AC Power Supply
JZ013A	Aruba HW-7280-FT 7280 Series Fan Tray

ORDERING INFORMATION

Part Number		7205	7210	7220	7240XM	7280
Transceivers						
JW087A	Aruba 1000BASE-LX LC Connector SFP XCVR	X	X	X	X	X
JW088A	Aruba 1000BASE-SX LC Connector SFP XCVR	X	X	X	X	X
JW089A	Aruba 1000BASE-T RJ45 Connector SFP XCVR	X	X	X	X	X
JW149A	SFP-EX 1000BASE-EX LC SFP XCVR	X	X	X	X	X
JW150A	SFP-ZX 1000BASE-ZX LC SFP XCVR	X	X	X	X	
J4859D	Aruba 1G SFP LC LX 10km SMF Transceiver	X[1]	X[1]	X[1]	X[1]	X[1]
J4858D	Aruba 1G SFP LC SX 500m OM2 MMF Transceiver	X[1]	X[1]	X[1]	X[1]	X[1]
J4860D	Aruba 1G SFP LC LH 70km SMF Transceiver	X[2]	X[2]	X[2]	X[2]	X[2]
J8177D	Aruba 1G SFP RJ45 T 100m Cat5e Transceiver	X[1]	X[1]	X[1]	X[1]	X[1]

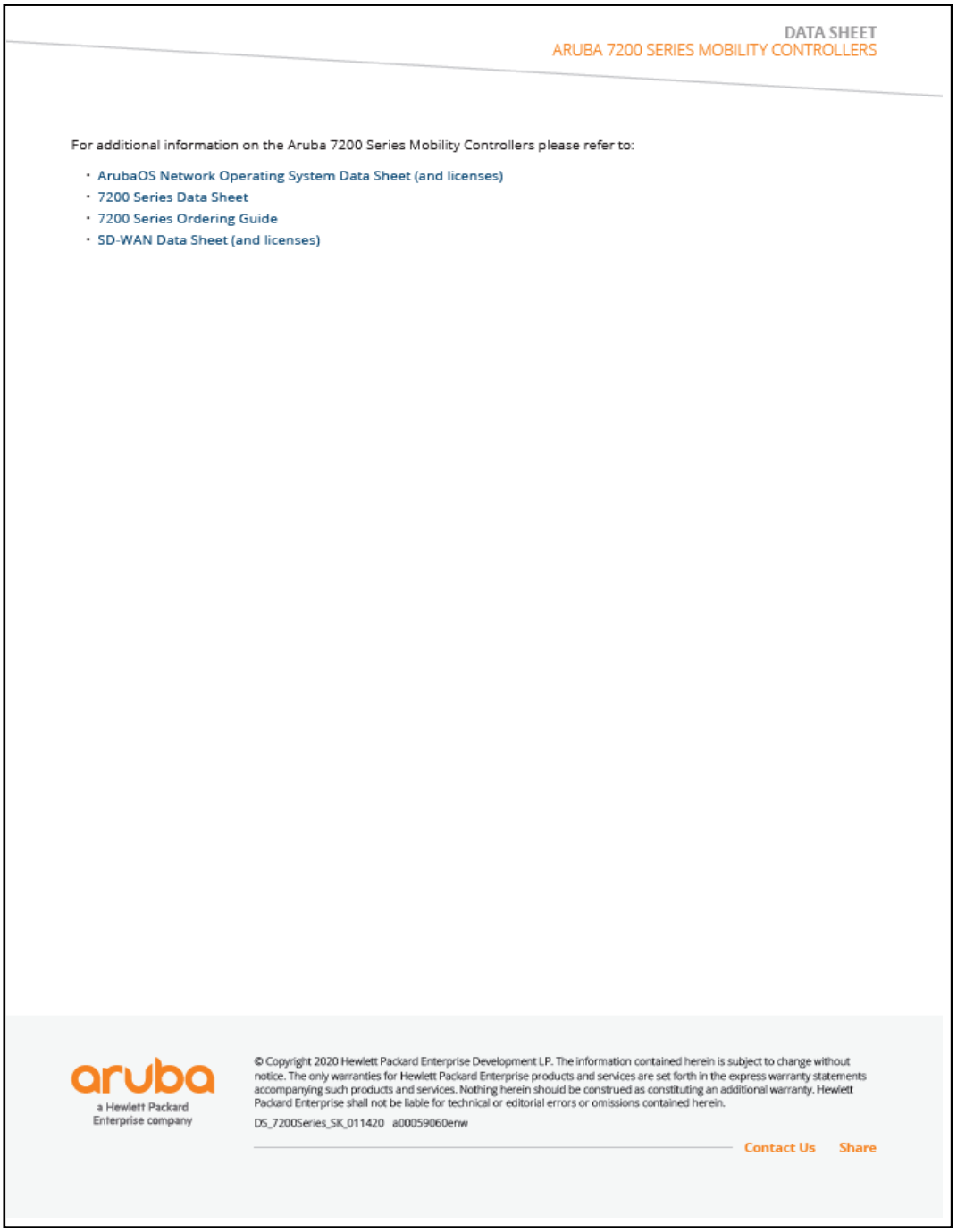
X: Supported transceiver
[1]Default minimum ArubaOS software version is 6.5.3.0 and 8.1.0.0
[2]Minimum ArubaOS software version is 6.5.4.7 and 8.4.0.0

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

ORDERING INFORMATION						
Part Number		**7205**	**7210**	**7220**	**7240XM**	**7280**
Transceivers						
JW092A	Aruba 10GBASE-LR LC Connector SFP+ XCVR	X	X	X	X	X
JW091A	Aruba 10GBASE-SR LC Connector SFP+ XCVR	X	X	X	X	X
JW090A	Aruba 10GBASE-LRM LC Connector SFP+ XCVR	X	X	X	X	X
JW100A	SFP+ Direct Attach 0.5M Cable	X	X	X	X	X
JW101A	SFP+ Direct Attach 1M Cable	X	X	X	X	X
JW102A	SFP+ Direct Attach 3M Cable	X	X	X	X	X
JW103A	SFP+ Direct Attach 5M Cable	X	X	X	X	X
JW104A	SFP+ Direct Attach 7M Cable	X	X	X	X	X
JW147A	SFP-10GE-ER 10G LC Cnctr SFP+ XCVR	X	X	X	X	X
JW148A	SFP-10GE-ZR 10G LC Cnctr SFP+ XCVR	X	X	X	X	X
J9150D	Aruba 10G SFP+ LC SR 300m OM3 MMF Transceiver	X[1]	X[1]	X[1]	X[1]	X[1]
J9151E	Aruba 10G SFP+ LC LR 10km SMF Transceiver	X[1]	X[1]	X[1]	X[1]	X[1]
J9152D	Aruba 10G SFP+ LC LRM 220m OM2 MMF Transceiver	X[1]	X[1]	X[1]	X[1]	X[1]
J9153D	Aruba 10G SFP+ LC ER 40km SMF Transceiver	X[1]	X[1]	X[1]	X[1]	X[1]
J9281D	Aruba 10G SFP+ to SFP+ 1m DAC Cable	X[1]	X[1]	X[1]	X[1]	X[1]
J9283D	Aruba 10G SFP+ to SFP+ 3m DAC Cable	X[1]	X[1]	X[1]	X[1]	X[1]
J9285D	Aruba 10G SFP+ to SFP+ 7m DAC Cable	X[1]	X[1]	X[1]	X[1]	X[1]
JH231A	HPE X142 40G QSFP+ MPO SR4 Transceiver					X[1]
JH232A	HPE X142 40G QSFP+ LC LR4 SM Transceiver					X[1]
JH233A	HPE X142 40G QSFP+ MPO eSR4 300M XCVR					X[1]
JH234A	HPE X242 40G QSFP+ to QSFP+ 1m DAC Cable					X[1]
JH235A	HPE X242 40G QSFP+ to QSFP+ 3m DAC Cable					X[1]
JH236A	HPE X242 40G QSFP+ to QSFP+ 5m DAC Cable					X[1]
JH678A	HPE X140 40G QSFP+ LC BiDi 150m MM C-TRX					X[1]
JH700A	HPE X240 QSFP+ 4x10G SFP+DAC Reman C-Cbl					X[1]
JG329A	HPE X240 QSFP+ 4x10G SFP+ 1m DAC Cable					X[1]
JG331A	HPE X240 QSFP+ 4x10G SFP+ 5m DAC Cable					X[1]
JH231A	HPE X142 40G QSFP+ MPO SR4 Transceiver					X[1]
JH232A	HPE X142 40G QSFP+ LC LR4 SM Transceiver					X[1]
JH233A	HPE X142 40G QSFP+ MPO eSR4 300M XCVR					X[1]
JH234A	HPE X242 40G QSFP+ to QSFP+ 1m DAC Cable					X[1]
JH235A	HPE X242 40G QSFP+ to QSFP+ 3m DAC Cable					X[1]
JH236A	HPE X242 40G QSFP+ to QSFP+ 5m DAC Cable					X[1]
JL308A	Aruba 40G QSFP+ LC BiDi 150m MMF XCVR					X[1]

X: Supported transceiver
[1]Default minimum ArubaOS software version is 6.5.3.0 and 8.1.0.0
[2]Minimum ArubaOS software version is 6.5.4.7 and 8.4.0.0

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"



For additional information on the Aruba 7200 Series Mobility Controllers please refer to:

- ArubaOS Network Operating System Data Sheet (and licenses)
- 7200 Series Data Sheet
- 7200 Series Ordering Guide
- SD-WAN Data Sheet (and licenses)

aruba
a Hewlett Packard Enterprise company

DS_7200Series_SK_011420 a00059060enw

Fuente del anexo: https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf
Apartado desde el que se referencia este anexo: "4.1.3.1 Equipos hardware (Gateways) del piloto SD-WAN"

Anexo XVIII

El algoritmo de equilibrio de carga determina cómo se distribuyen las sesiones entre los enlaces ascendentes WAN activos cuando no se han definido políticas de selección dinámica rutas (DPS). El equipo gateway de la sucursal equilibrará la carga del tráfico utilizando uno de los tres tipos de algoritmos que Aruba Central[(1)] ofrece:

- **Round Robin** que distribuye secuencialmente el tráfico saliente entre cada enlace ascendente WAN activo. Este algoritmo es el más fácil de implementar, aunque puede resultar un distribución desigual del tráfico a lo largo del tiempo
- **Algoritmo de recuento de sesiones** que distribuye el tráfico saliente entre los enlaces ascendentes WAN activos en función del número de sesiones administradas por cada enlace. Este algoritmo intenta garantizar un equilibrio entre porcentajes respecto al número de sesiones. Además, permite opcionalmente asignar pesos a cada enlace ascendente, de esta manera, un enlace con peso 80 y otro con peso 20 dará como resultado una relación 4:1, es decir, por cada 4 sesiones enviadas al enlace con un peso 80 solo se enviará una al enlace con peso 20.
- **Algoritmo de utilización de enlace descendente**. Distribuye el tráfico entre los enlaces ascendentes WAN activos. Esta distribución la realiza en función del porcentaje de uso de cada uno de los enlaces, utilizando la velocidad del enlace para realizar el cálculo de uso y definir un umbral máximo de porcentaje de ancho de banda máximo. Cuando ese umbral supera ese porcentaje el enlace ascendente WAN ya no se considera disponible.

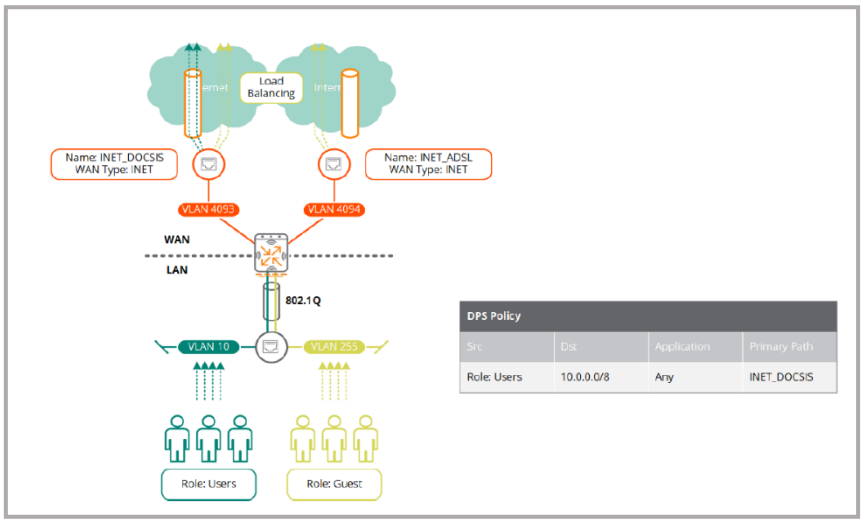


Ilustración 126: Ejemplo de equilibrio de carga sin política DPS[(*)]

[(1)] Se puede encontrar información adicional sobre Aruba Central en el "Anexo XVI"
Contenido del texto de este anexo basado en: *SD-Branch Fundamentals Guide*. (2018). Marshall K. y Tanguay A.
Fuente de la imagen[(*)]: *SD-Branch Fundamentals Guide*. (2018). Marshall K. y Tanguay A.
Apartado desde el que se referencia este anexo: "4.1.4.3 Implementación del piloto SD-WAN"

Aunque, los equipos gateways de Aruba admiten tres algoritmos de carga, de forma predeterminada está seleccionado Round Robin. Aruba recomienda implementar el algoritmo de utilización de enlace descendente para la mayoría de las implementaciones, esto es debido a la implicación de la velocidad del enlace WAN en la selección de la ruta. Sin embargo, cada administrador debe seleccionar el algoritmo de carga apropiado que mejor encaje con las necesidades de su organización.

Contenido del texto de este anexo basado en: *SD-Branch Fundamentals Guide*. (2018). Marshall K. y Tanguay A.
Fuente de la imagen(*): *SD-Branch Fundamentals Guide*. (2018). Marshall K. y Tanguay A.
Apartado desde el que se referencia este anexo: "4.1.4.3 Implementación del piloto SD-WAN"

Anexo XIX

Políticas de selección dinámica de ruta (DPS)

En una red SD-WAN, la mayoría de las sucursales implementarán una o más políticas DPS (selección dinámica de la ruta). Estas políticas determinan, para los usuarios de las sucursales, la forma en que se seleccionarán las rutas WAN de acceso a las aplicaciones y servicios, en la sede central o Internet.

Cada política DPS puede estar configurada para la selección de rutas WAN primarias, secundarias, terciarias..., y pueden ser tanto un solo enlace ascendente WAN o un grupo de ellos. Así, cuando se realiza la selección sobre un grupo de enlaces ascendentes WAN, el equipo gateway de la sucursal realiza un equilibrio de carga mediante el tráfico coincidente, es decir, distribuirá el tráfico coincidente entre los enlaces ascendentes WAN activos en el grupo.

Esta es la forma, en que el algoritmo de carga determina cómo se distribuyen las sesiones entre los enlaces ascendentes WAN activos en el grupo.

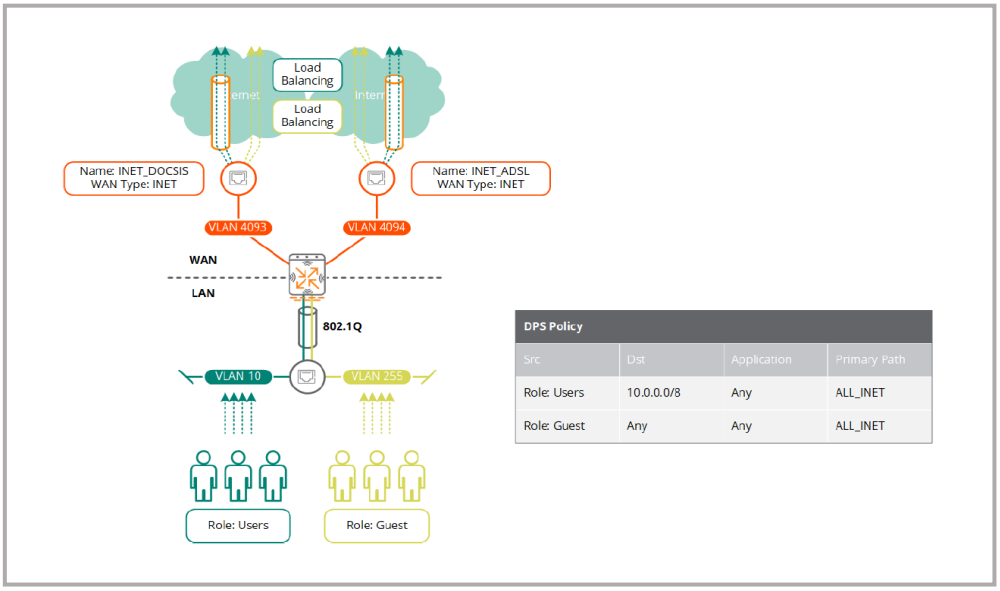


Ilustración 127: Ejemplo de equilibrio de carga con política DPS(*)

Los equipos gateway de Aruba pueden implementar políticas DPS para determinar usuarios, aplicaciones y destinos específicos. La ruta de envío mediante este tipo de políticas podría ser en un solo enlace ascendente WAN o mediante el equilibrio de carga del tráfico en un conjunto de enlaces ascendentes WAN.

Así, la dirección IP de destino del tráfico determinará si el tráfico hay que enviarlo hacía un túnel VPN o se reenvía directamente a Internet, es último caso, no será posible para el caso de implementaciones de túneles completos para el tráfico de superposición en la red subyacente.

Contenido del texto de este anexo basado en: *SD-Branch Fundamentals Guide*. (2018). Marshall K. y Tanguay A.
Fuente de la imagen(*): *SD-Branch Fundamentals Guide*. (2018). Marshall K. y Tanguay A.
Apartado desde el que se referencia este anexo: "4.1.4.3 Implementación del piloto SD-WAN" – "4.1.2 Especificación"

La forma de definir políticas DPS es realizar unas reglas de especificación del tráfico coincidentes según el rol de los usuarios al desplegar la segmentación dinámica de una sucursal. De esta manera para cada sucursal, el tráfico de cada dispositivo se canaliza al gateway SD-WAN de la sucursal donde se le asigna un rol y unas políticas asociadas, lo que simplifica la creación y administración de las políticas DPS al eliminar la necesidad de crear reglas específicas de sucursal que coincidan en direcciones IP o redes de origen.

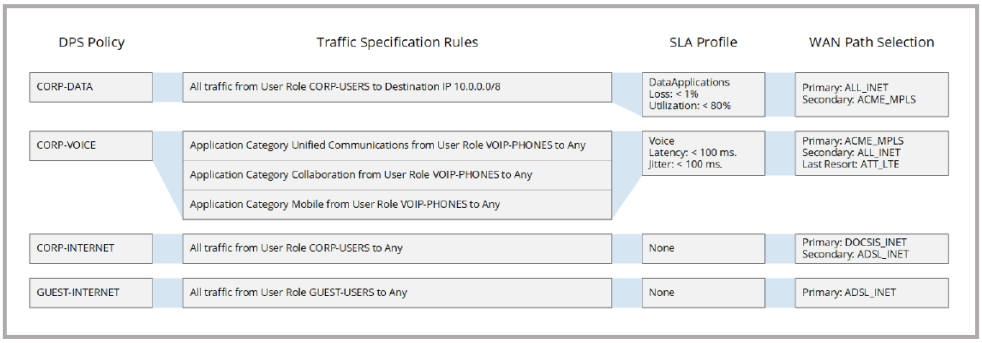


Ilustración 128: Ejemplo de políticas DPS con roles de usuarios(*)

Los perfiles SLA se pueden asignar de manera opcional a cada política. Esta asignación influye en la selección de la ruta para las sesiones nuevas y existentes definidas en cada una de las políticas.

Cuando un perfil SLA es asignado, el equipo gateway supervisará cada una de las rutas WAN definidas en la política para garantizar que el rendimiento de cada enlace ascendente cumpla con los umbrales de características especificadas en cada perfil SLA asignado, como son: latencia, fluctuación, perdida y uso.

Así, el equipo gateway utiliza sondas UDP o ICMP para la cabecera (VPNC) o el FQDN definido por el usuario para monitorear cada ruta WAN, de esta manera, cuando una de las rutas excede en uno o más de los umbrales definidos en el perfil SLA, se considera una violación de la política.

En este caso, tanto las sesiones existentes como las nuevas se moverán de la ruta WAN afectada a otra ruta alternativa que cumpla con los umbrales definidos. En caso de no existir una ruta WAN alternativa que cumpla con los umbrales definidos, entonces el equipo realizará un equilibrio de carga entre las rutas WAN disponibles.

Respecto a la selección de camino, las políticas DPS permiten la asignación de rutas WAN primarias, secundarias y de último recurso.

Este tipo de políticas DPS hay que necesariamente implementar en la red SD-WAN entre la sucursal AL y el nodo principal CR, realizado en el apartado "4.1.4.3 Implementación del piloto SD-WAN" de este documento y así, cumplir con las prioridades respecto al tráfico entre sucursal y cabecera que la institución tiene, tal como se expuso en el apartado "4.1.2 Especificación".

Contenido del texto de este anexo basado en: *SD-Branch Fundamentals Guide*. (2018). Marshall K. y Tanguay A.
Fuente de la imagen(*): *SD-Branch Fundamentals Guide*. (2018). Marshall K. y Tanguay A.
Apartado desde el que se referencia este anexo: "4.1.4.3 Implementación del piloto SD-WAN" – "4.1.2 Especificación"

Desde *Aruba central*, la configuración de políticas DPS se realizar al seleccionar desde el equipo: **DEVICE – WAN – Dynamic Path Steering** y presionar sobre el icono + para crearla.

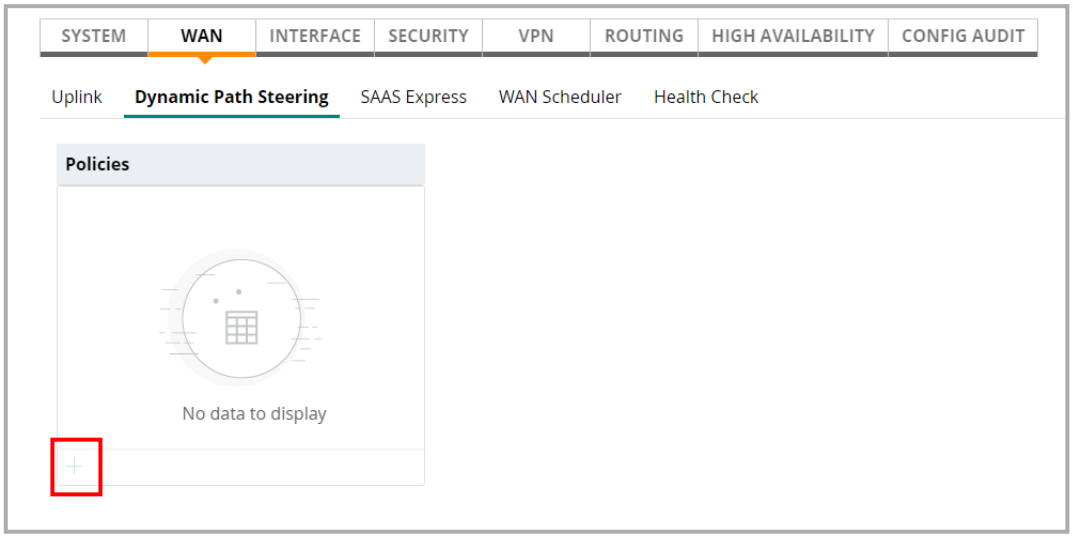


Ilustración 129: Crear políticas DPS en Aruba Central

Apartado desde el que se referencia este anexo: "4.1.4.3 Implementación del piloto SD-WAN" – "4.1.2 Especificación"

Anexo XX

Vista gráfica de las distintas pruebas

- Detalle general del equipo sucursal o cabecera con las características más importantes.

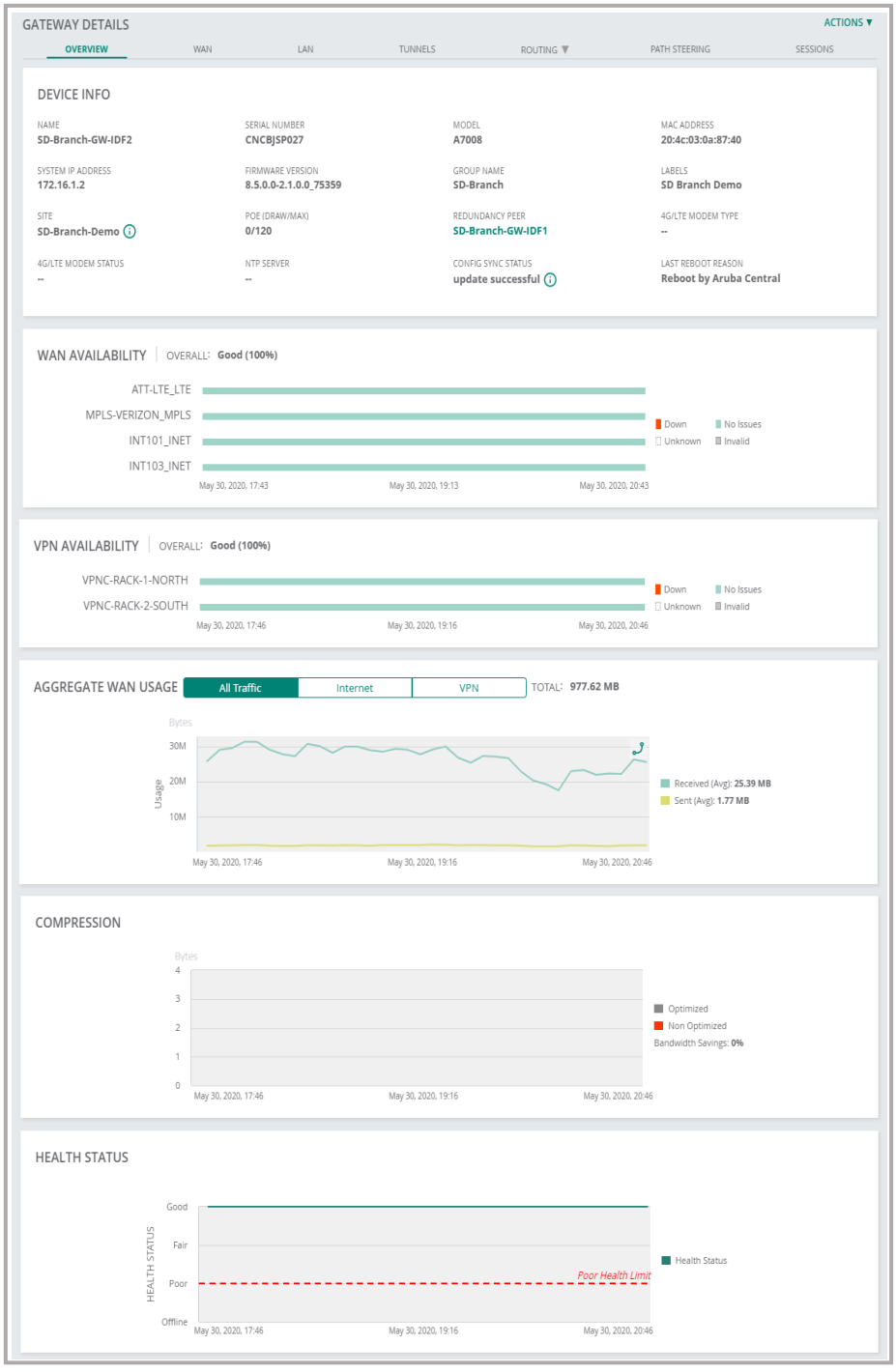


Ilustración 130: Resumen del estado general de gateway SD-WAN

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"

- Detalle de la parte WAN a nivel de equipo donde se pueden ver el estado de puertos, interfaces WAN, tráfico, comprensión, latencia y perdida de paquetes.

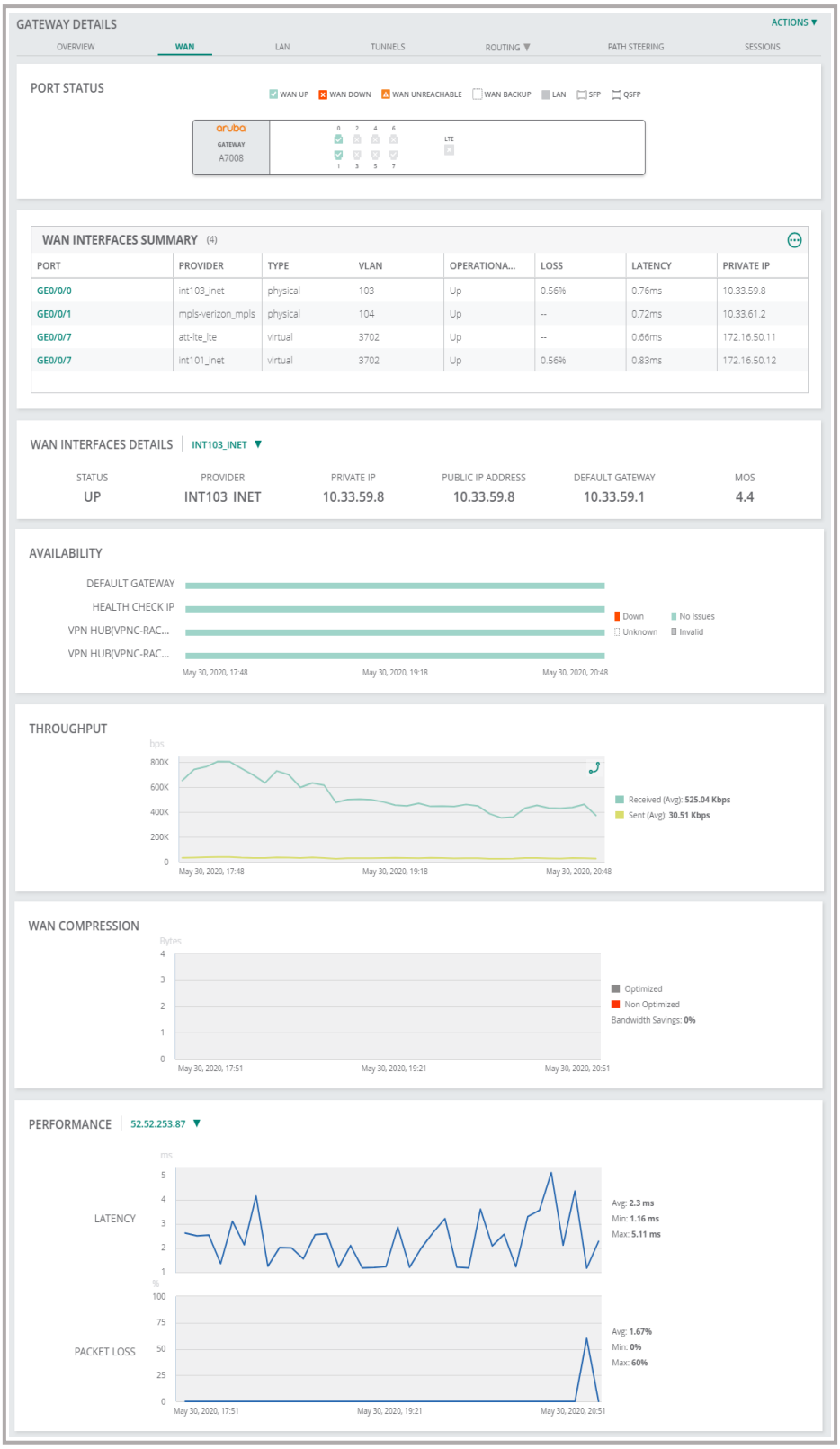


Ilustración 131: Detalle general de la red WAN en gateway SD-WAN

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"

- Detalle de la parte LAN a nivel de equipo donde se pueden ver el estado de puertos, interfaces LAN, interfaces VLAN...

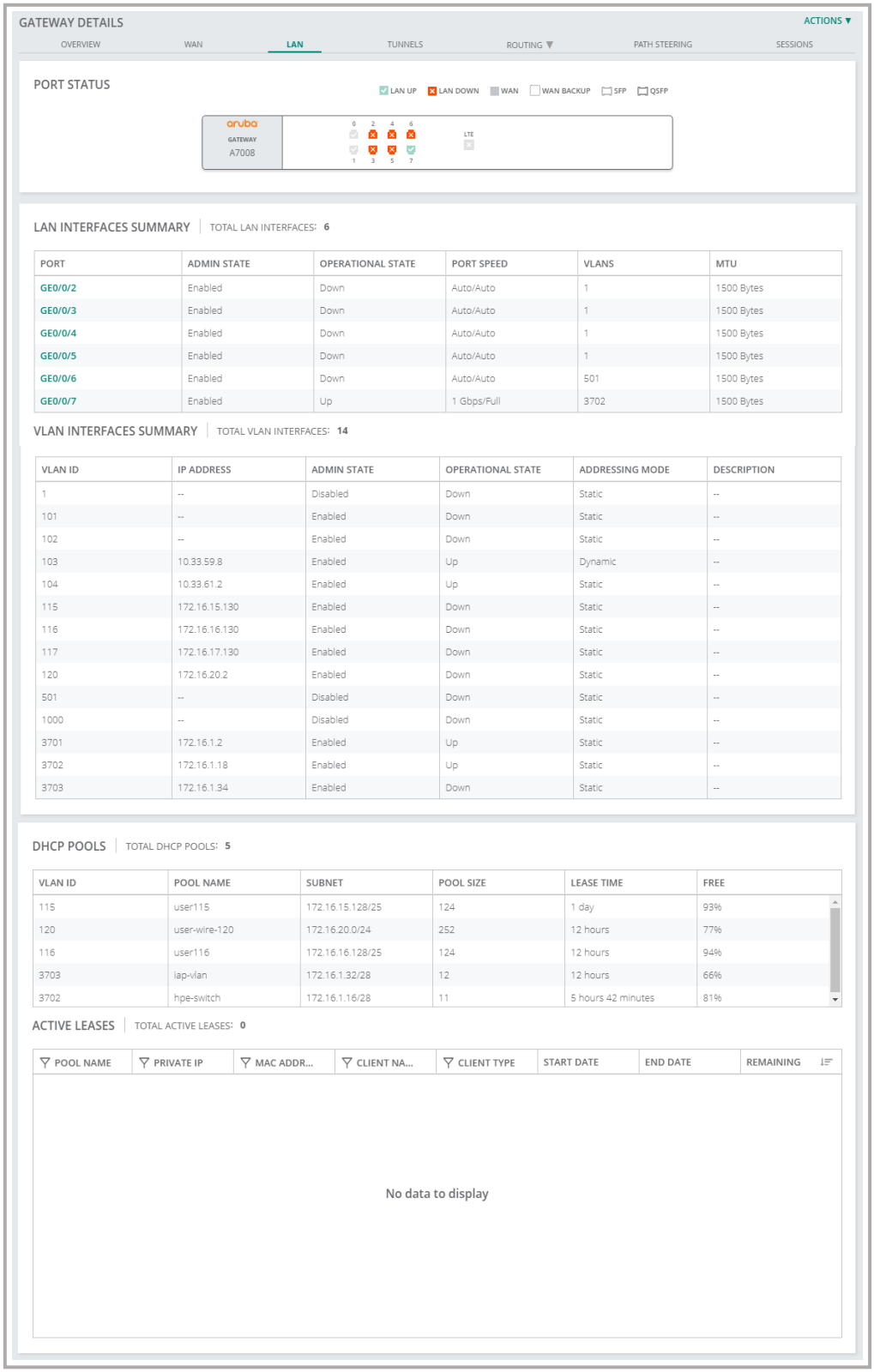


Ilustración 132: Detalle general de la red LAN en gateway SD-WAN

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"

- Detalle de los túneles VPN y del *routing*, en este caso, orquestado

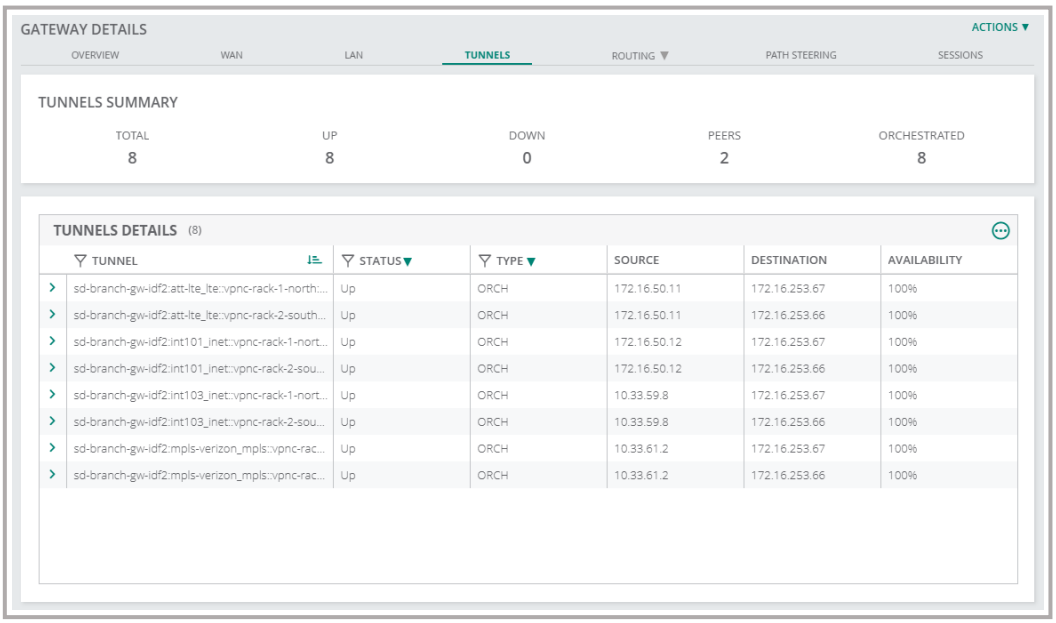


Ilustración 133: Detalle de túneles creados en gateway SD-WAN

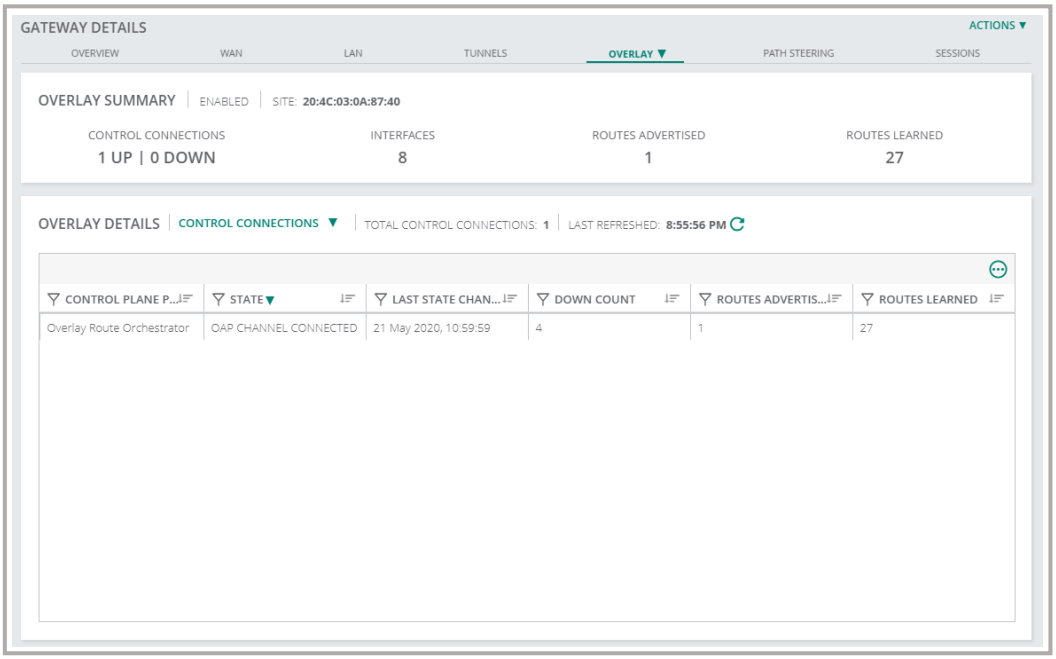


Ilustración 134: Detalle del routing orquestado en gateway SD-WAN

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"

- Detalle de las políticas DPS que se están aplicando, en este caso no hay.

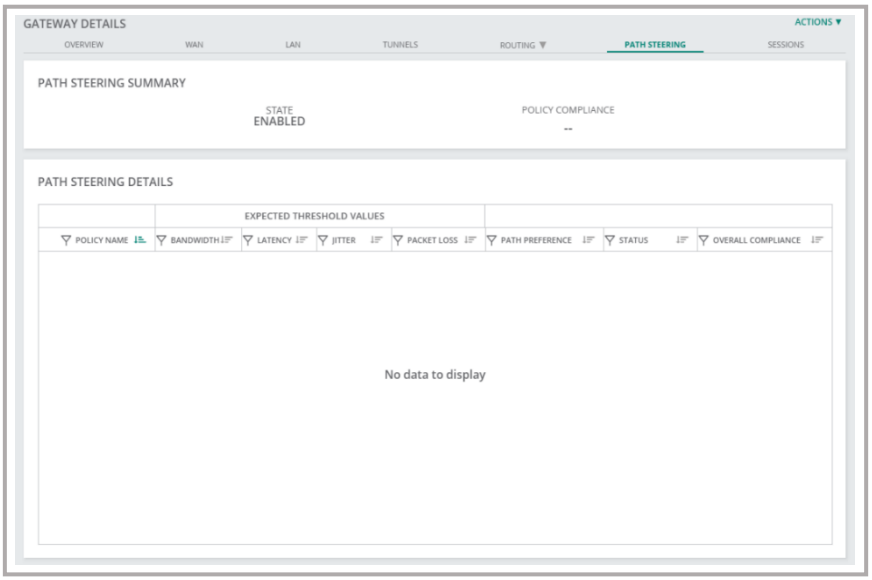


Ilustración 135: Detalle de políticas DPS aplicadas en el gateway SD-WAN

- Información sobre el número de sesiones activas o no

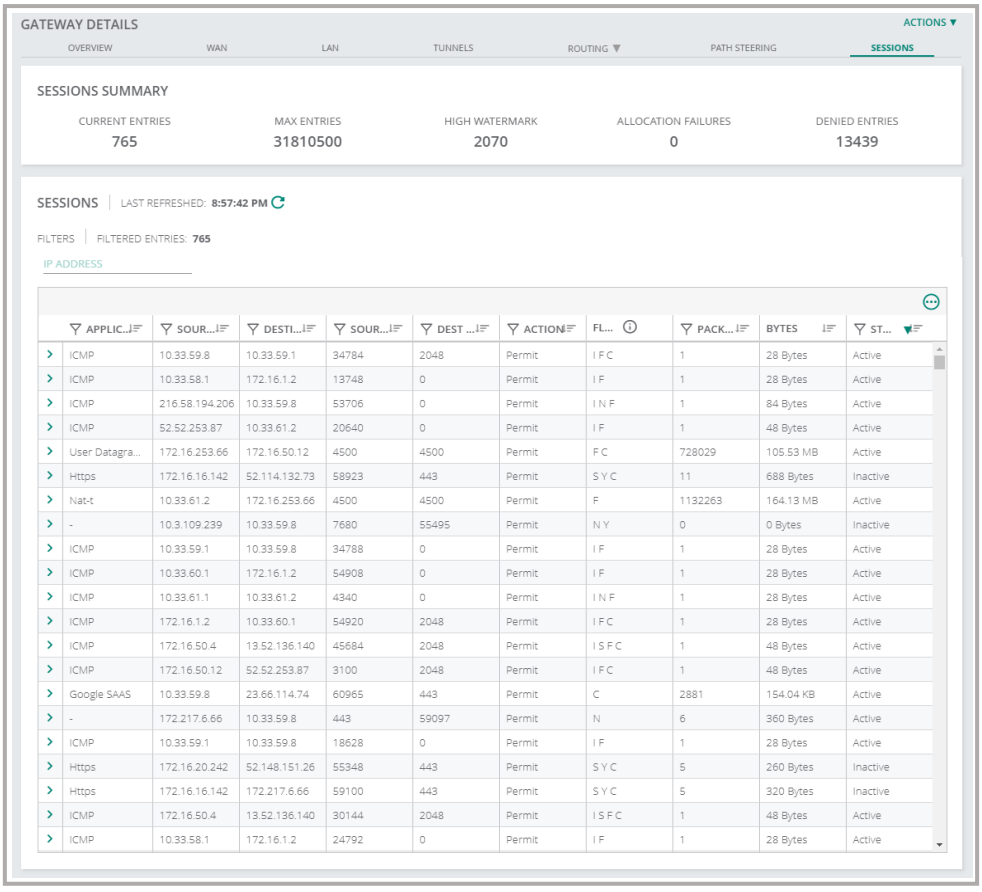


Ilustración 136: Listado de sesiones producidas en un gateway SD-WAN

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"

- Detalle de cualquiera de las sesiones al realizar un selección sobre ella.

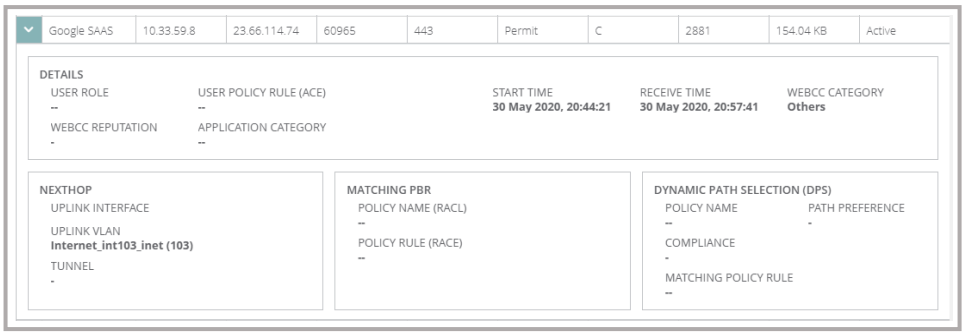


Ilustración 137: Detalle de una sesión en un equipo SD-WAN

- Cantidad y lista de clientes conectados

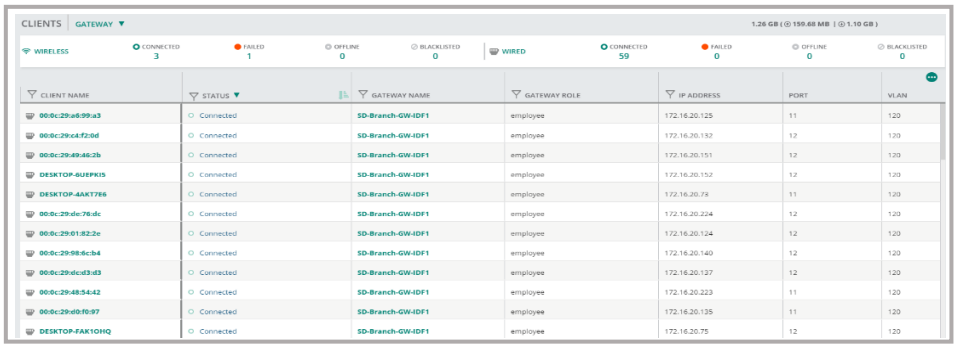


Ilustración 138: Lista de clientes conectados en un gateway SD-WAN

- Resumen de cualquira de los clientes al realizar una selección sobre él, así como de las sesiones que tiene o ha tenido activas.

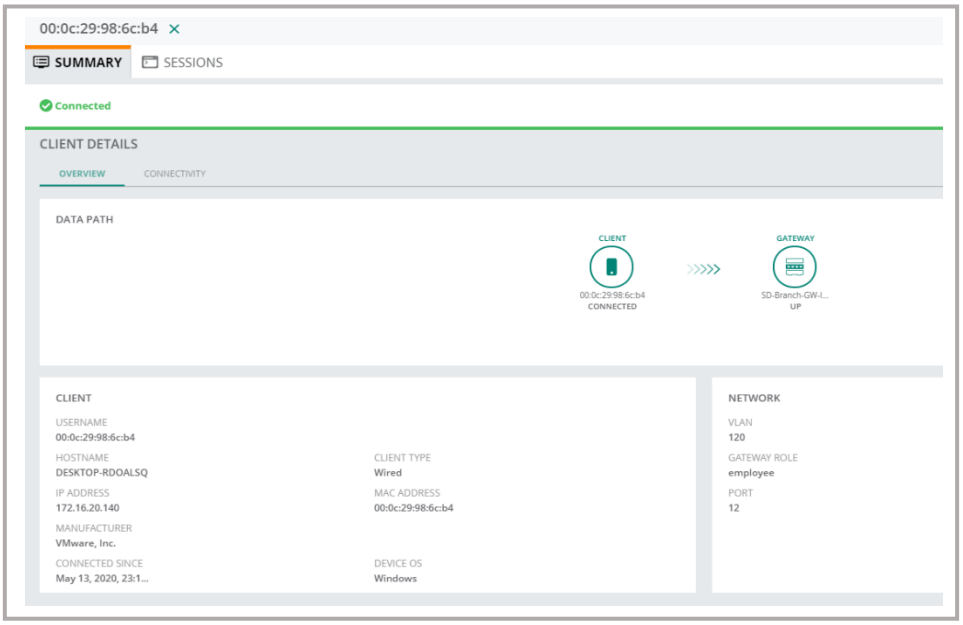


Ilustración 139: Resumen de datos de un cliente del gateway SD-WAN

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"

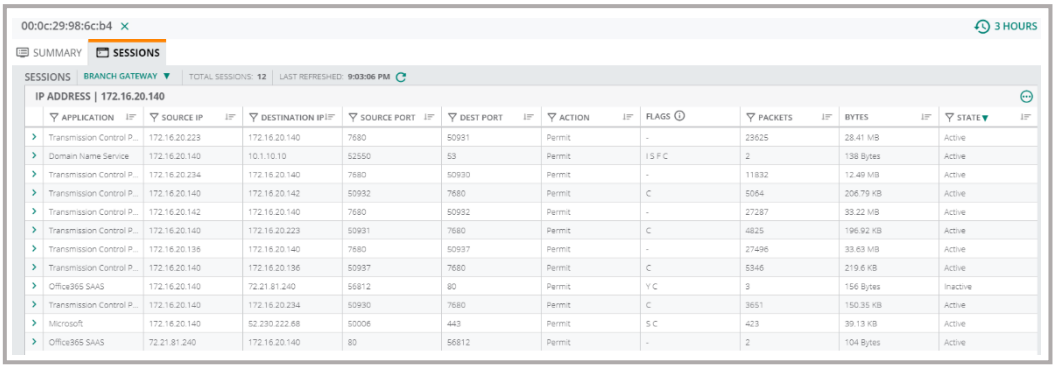


Ilustración 140: Lista y detalles de cualquier sesión de un cliente

- Incluso, el detalle de cualquiera de las sesiones de un cliente

Ilustración 141: Destalle específico de las sesiones de un cliente

- Listado, respecto a un usuario, de aplicaciones y categorización de los sitios web, así como el detalle de una aplicación concreta.

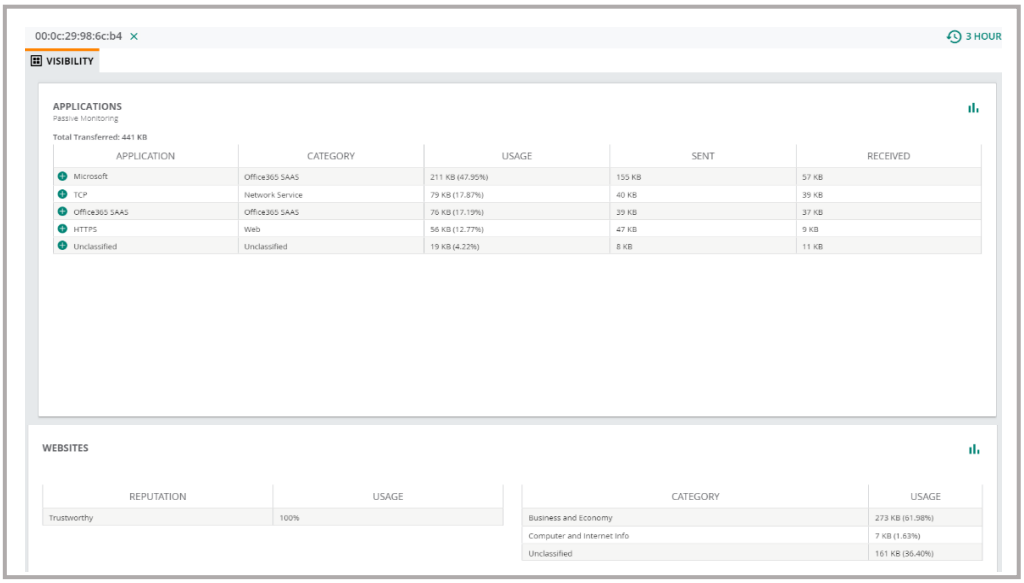


Ilustración 142: Resumen de aplicaciones y sitios web de un cliente

---

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"

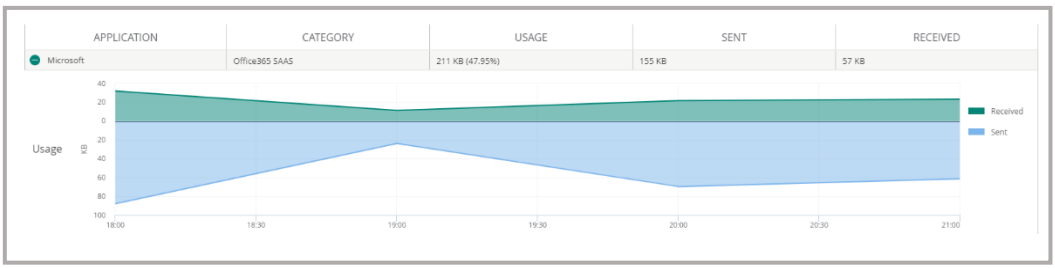


Ilustración 143: Detalle de uso, por parte de un cliente, de una aplicación

- Lista de aplicaciones y categorización de sitios web visitados, por red o equipo

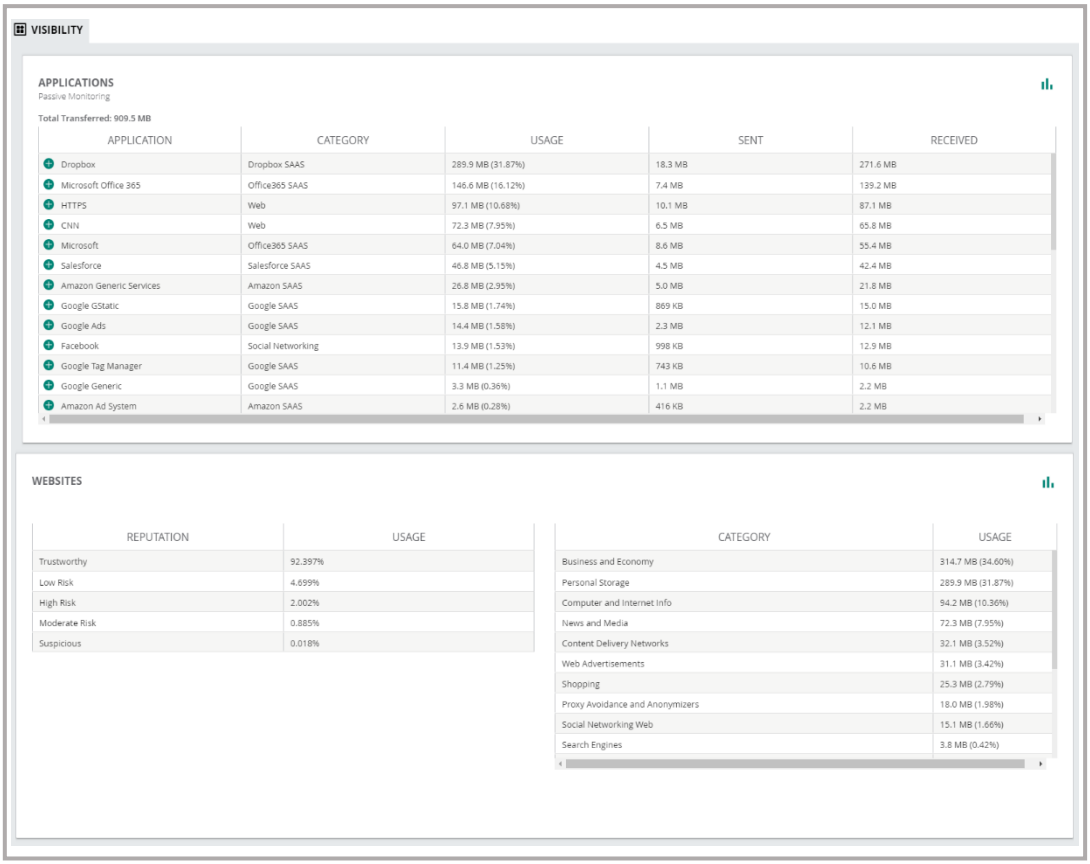


Ilustración 144: Resumen de aplicaciones y sitios web del sitio SD-WAN

- Detalle del uso de una aplicación determinada por ubicación o red

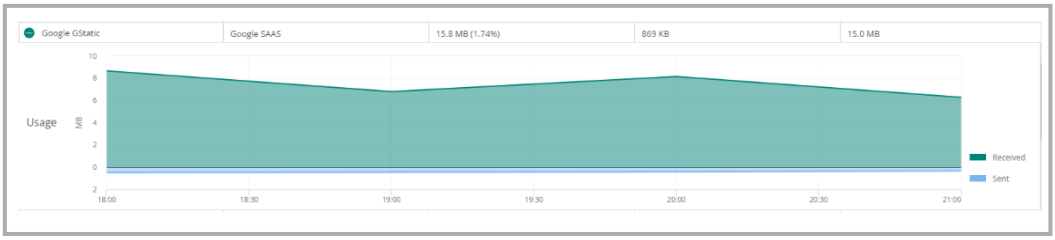


Ilustración 145: Detalle de uso de una aplicación por sitio SD-WAN

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"

- Listado de alertas y eventos sobre la red

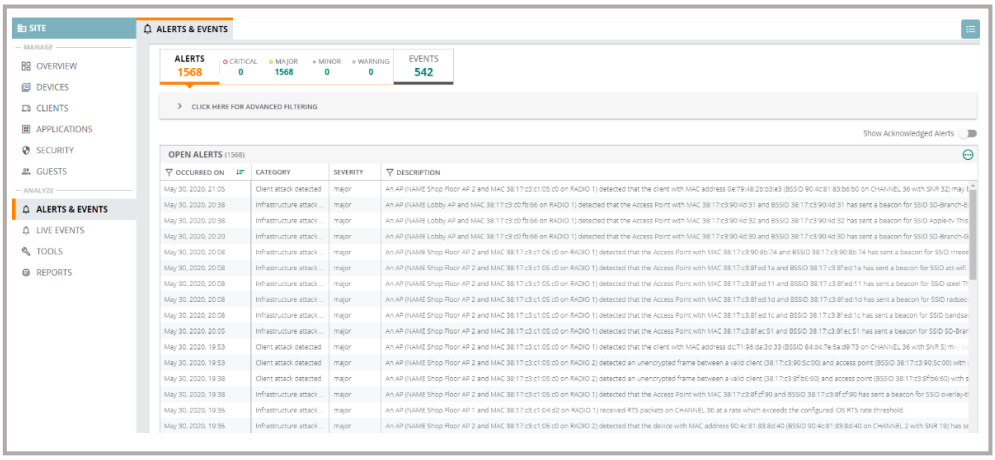


Ilustración 146: Listado de alertas por sitio en red SD-WAN

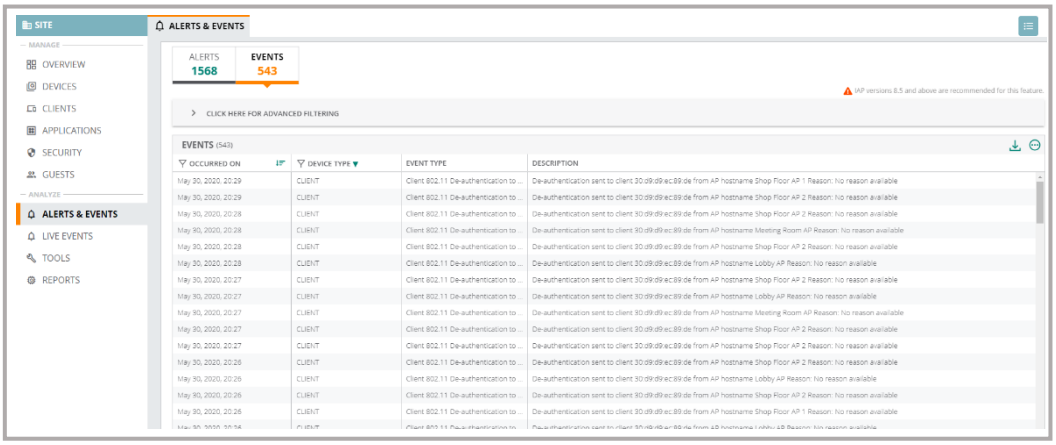


Ilustración 147: Listado de eventos por sitio en red SD-WAN

- Disponibilidad de distintas herramientas de chequeo y de comandos

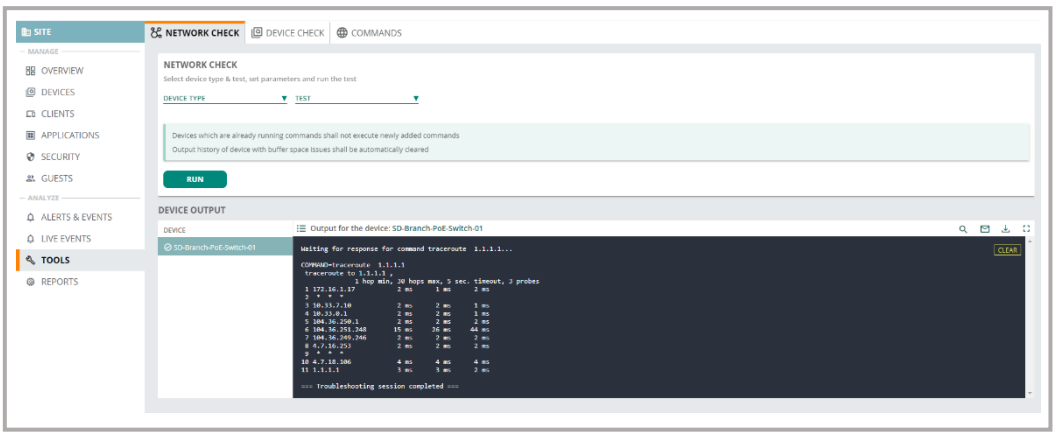


Ilustración 148: Disponibilidad de herramientas para chequeo de la red

---

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"

- Programación de informes por secciones y selección de cualquiera de ellos, incluyendo el envío por email o la exportación PDF.

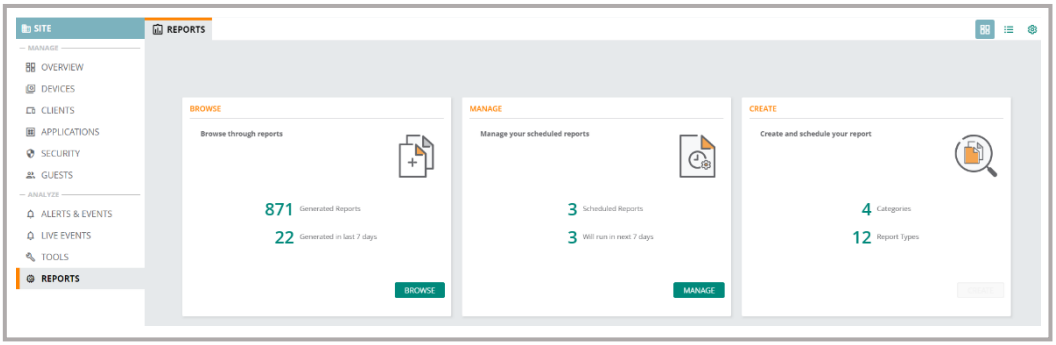


Ilustración 149: Resumen de contenedores de informes

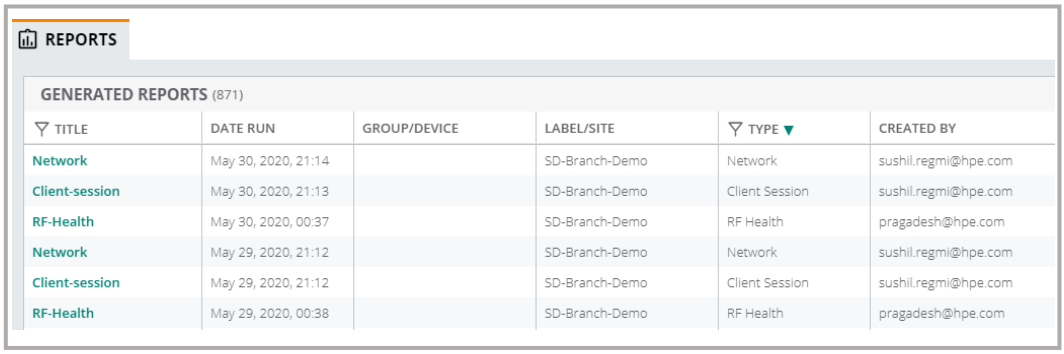


Ilustración 150: Listado de informes generado de una sección

Apartado desde el que se referencia este anexo: "4.1.5 Pruebas"