





SD-WAN

SD-WAN FAQs

SD-WAN FAQs

Este documento está dedicado a Preguntas Frecuentes relacionadas con la tecnología SD-WAN. En ella se explican conceptos ligados al SD-WAN y su integración en las soluciones Teldat.

Teldat

Índice

1. Escenario y Modelo de Datos

Este apartado describe los principales escenarios de red en los que encaja una solución SD-WAN y resume las principales capacidades y funciones de esta tecnología. Además, detalla cómo se construye el modelo de datos para configurar, gestionar y monitorizar una red WAN corporativa al completo. Algunos de los temas que se abordan aquí son: el tipo de acceso de red, acuerdos sobre el nivel de los servicios, identificación de aplicaciones, calidad de servicio, etc.

1.1. ¿Qué es el "Modelo de Datos"?

Se podría decir que el modelo de datos es la base de datos que contiene la información de la red SDWAN. Es necesario concentrar la definición de la red en un punto, dado que uno de los objetivos principales de SDWAN es la centralización del plano de control en software. En la solución SDWAN Teldat, este plano de control es el "Controller", el cual a partir del "modelo de datos" construye/modifica en tiempo real las configuraciones de todos los equipos de la red.

NOTA: En la configuración "tradicional" de una red, equipo a equipo (CLI), no hay "modelo de datos" como tal, o se podría decir que el modelo de datos está distribuido en los ficheros de configuración de todos y cada uno de los equipos que conforman la red. Aunque también es posible generar y mantener una red SDWAN de esta forma, a lo largo de este documento se asume que no se realizará así, sino que llevará a cabo desde un Controller.

1.2. ¿Cuántas redes de acceso y de que tipo se pueden configurar y utilizar en una red SD-WAN?

Se pueden configurar dos tipos de redes: MPLS e Internet, sin límite en el número de redes de acceso / proveedores de cada tipo. Es necesario diferenciar entre estos dos tipos de red porque las redes MPLS no tienen conectividad entre ellas, y al generar la configuración de conectividad de puntos remotos con concentradores hay que asegurar que pertenecen a una misma red MPLS.

1.3. ¿Cómo se pueden identificar aplicaciones para aplicarles políticas y SLA?

Mediante una lista ordenada de sentencias de análisis de parámetros de nivel 3 (direcciones), 4 (protocolos y puertos) o 7 (Host Name http/https). Dichas sentencias pueden ser inclusivas o exclusivas, por ejemplo, para identificar todo el tráfico excepto el tráfico hacia xxxxx.com, o todo el tráfico TCP excepto el dirigido al puerto X.

1.4. ¿Cuántas aplicaciones se pueden identificar para asignar políticas y SLA?

No hay límite en el número de aplicaciones ni tampoco en el número de políticas. Es posible asociar una política a una aplicación, pero para facilitar la gestión se permite agrupar aplicaciones para aplicar una política común, sin que exista tampoco límite en el número de aplicaciones por grupo.

1.5. ¿Cómo se establece el nivel SLA?

Se generan sondas desde los puntos remotos por todos y cada uno de los accesos y se mide el retardo, variación del retardo (jitter) y tasa de pérdidas en cada acceso.

1.6. ¿Las sondas son activas o pasivas? ¿se pueden parametrizar?

Las sondas son activas, lo cual consume algo de tráfico y CPU, pero en la práctica es despreciable y de esta forma permite disponer de la información de SLA antes de que una aplicación arranque la transmisión. La parametrización de las sondas está incluida en el modelo de datos, de forma que se pueden configurar de forma precisa el ancho de banda utilizado.

1.7. ¿Es posible definir niveles SLA a aplicaciones? ¿Cómo?

Sí. Como se ha comentado antes, es posible asociar umbrales SLAs a aplicaciones o grupos de aplicaciones, es decir, el nivel máximo asumible de retardo, jitter y pérdidas para dicha aplicación(es).

1.8. ¿Cuántos perfiles SLA se soportan?

No hay límite en el número de perfiles SLA que se pueden definir.

1.9. ¿Qué ocurre cuando no se puede mantener el nivel SLA definido de una aplicación?

Se mueve la aplicación a otra red de acceso en la que el nivel SLA sea mejor. Para cada aplicación y tipo de sede remota, se configuran las prioridades de uso las distintas redes de acceso que tenga disponibles dicha sede.

1.10. ¿Cuántos usuarios y redes IP se soportan?

No hay límite en el número de usuarios y redes IP que se soportan.

1.11. ¿Cuál es el soporte de calidad de servicio (QoS)?

La calidad de servicio se define por cada aplicación o grupo de aplicaciones, y es posible de definir por cada red de acceso:

- Prioridad: Real-time, Alta, Normal y Baja
- Límite en 'bitrate': máximo 'bitrate' que puede usar una aplicación o grupo de aplicaciones
- Peso: porcentaje de ancho de banda que se garantiza a una aplicación o grupo de aplicaciones en caso de que la línea esté saturada.
- Marcado DSCP o ToS: marcado de tráfico con DSCP o ToS
- Longitud de cola para cada categoría de aplicación.

Para facilitar el trabajo de configuración y mantenimiento, la calidad de servicio se configura usando plantillas de oficinas remotas compartiendo la misma configuración de QoS.

1.12. ¿Se soporta salida directa a internet (breakout) desde las sedes remotas?

Sí, se soporta. Para ello basta con identificar en cada sede remota el tipo de tráfico que se ha de enviar directamente a internet. Por ejemplo, todo lo que no sean servicios propios. Para facilitar la configuración y mantenimiento, se soportan perfiles de oficina que tienen una configuración común.

1.13. ¿Se soporta el acceso a servicios "nativos" en la red MPLS (underlay), por ejemplo telefonía sobre IP?

Si, de la misma forma que se soporta el envío de tráfico directo a internet, es posible también seleccionar servicios/aplicaciones y enviarlo directamente por la red MPLS (sin realizar túneles, es decir, en el "underlay").

1.14. ¿Es posible la configuración de equipos de acceso a la red MPLS en SD-WAN Teldat Controller?

Sí, desde CNM Controller se pueden configurar todos los parámetros necesarios para conectar un equipo directamente a la MPLS. En CNM se pueden configurar parámetros como: protocolos de routing, 'peer address', Local AS, Remote AS...

1.15. ¿Necesita el cliente dos equipos, uno de acceso y otro SD-WAN, con Teldat SD-WAN?

No, ya que se soportan los dos escenarios. Si el cliente ya tiene desplegado un equipo de acceso a la red, Teldat puede desplegar un equipo SD-WAN de segundo nivel. Pero si el cliente no tiene un equipo de acceso, Teldat se puede desplegar también como equipo de acceso desde el Controlado SD-WAN.

1.16. ¿Cómo es la conectividad de puntos migrados a SD-WAN y puntos aún no migrados a SD-WAN?

A través del concentrador de VPNs ("Datacenter Edge") es posible conectar puntos migrados y no migrados, ya que dicho elemento mantiene conectividad con los puntos migrados a través de los túneles SDWAN ("overlay") y también conectividad con el resto de la red no migrada ("underlay").

1.17. ¿Se soportan varios Datacenters?

Si, se soportan varios Datacenters sin limitación en el nº de Datacenters ni en en el nº de Datacenter Edges ni Branch Edges que conectan con un Datacenter.

1.18. ¿Se soporta balanceo de tráfico sobre distintos accesos/redes de forma simultánea?

Es posible seleccionar de forma individual para cada aplicación o grupo de aplicaciones el acceso/red a utilizar de forma preferente siempre que se cumpla SLA, de forma que es posible balancear distintas aplicaciones por distintos accesos/redes.

2. Dispositivo en centro de datos

El Centro de Datos es uno de los principales componentes de una red corporativa. Por ello, a la hora de instalar una solución SD-WAN, es esencial que el dispositivo del Centro de Datos reúna una serie de características que se especifican a continuación. En este apartado se resuelven dudas sobre concentradores VPN, alternativas en materia de redundancia y preguntas sobre escalabilidad y demás temas.

2.1. ¿Qué es y cuál es la función del elemento "Datacenter Edge"?

Es un "concentrador de VPNs" al que se conectan los puntos remotos utilizando las redes físicas ("underlay") y estableciendo túneles para construir la red privada ("overlay").

Por otro lado, el Datacenter Edge se conecta a la red interna de un Datacenter en el cual se alojan servicios/aplicaciones, dando acceso a los mismos desde los puntos remotos a través del overlay.

2.2. ¿Cuáles son las posibilidades de elección de elementos "Datacenter Edge"?

Para redes pequeñas de hasta 200 puntos remotos y un agregado de 300Mbps está disponible una solución basada en hardware propietario, Teldat RXL14000. Para cualquier tamaño de red, el software vRXL, disponible en formato ISO, para ejecutarse en bare-metal o en una máquina virtual sobre KVM, o en formato AMI (Amazon Machine Image) para ejecutarse en Amazon.

2.3. ¿Se soporta redundancia de "Datacenter Edge"?

Si, se pueden instalar 2 Datacenters Edge en configuración de alta disponibilidad en modo activo/activo, es decir en situación normal cada uno soporta X puntos remotos y si uno de ellos cae, los X puntos remotos que conectaban al Datacenter Edge caído, pasan a conectar con el Datacenter Edge, que por lo tanto daría servicio a 2X puntos remotos.

2.4. ¿Se soporta escalabilidad de "Datacenter Edge"?

Si. Un Datacenter Edge (o pareja de ellos en modo redundante) da servicio a un número determinado de oficinas y soporta un determinado throughput agregado, pero pueden instalarse tantos Datacenter Edges (o parejas de ellos en modo redundante) como se deseen.

3. Dispositivo en sucursal

Las soluciones SD-WAN simplifican la configuración, gestión y monitorización de redes que proporcionan conectividad a sucursales y/o Centros de Datos. Los dispositivos que se instalan en sucursales se convierten, por tanto, en elementos clave de la solución. Para saber cuál se ajusta mejor a sus necesidades, es necesario que facilite toda la información técnica y comercial que pueda. Este apartado también resuelve dudas sobre la función de los dispositivos para sucursales o las distintas opciones presentes en la cartera de productos Teldat.

3.1. ¿Qué es y cuál es la función del elemento "Branch Edge"?

Es el elemento en el punto remoto que hace de nexo entre la red LAN del cliente y la red SDWAN. Las principales funciones son: Conexión con la(s) red(es) LAN, conexión con la(s) red(es) WAN, establecer overlay hacia Datacenter Edge, generar las sondas y medir SLA, identificar servicios/aplicaciones, aplicar QoS y decidir políticas de encaminamiento basadas en SLA.

3.2. ¿Cuáles son las posibilidades de elección de elementos "Branch Edge"?

Los siguientes routers Teldat: Teldat-V, Teldat-M1, Teldat-iM8, Atlas-60, Atlas-i70, Teldat-H2Auto, Teldat-H2Auto+ y Teldat-H2Rail.

3.3. ¿Es posible seleccionar el rango de direcciones IP por cada oficina remota manualmente?

Si, el usuario puede definir de un rango de IPs mayor, un subconjunto de direcciones IP que se asignen a una oficina remota específica.

3.4. ¿Cómo se asignan las direcciones IP en la LAN de cada oficina?

En la platilla de sede remota, el usuario define los perfiles LAN que se configuran. Un perfil LAN es la configuración de la LAN del equipo y define el número máximo de direcciones IP para un grupo específico de usuarios (por ejemplo, 16 direcciones IP para teléfonos y 8 direcciones IP para invitados), si se usan VLAN

desde el router hacia la LAN y como se asignas las direcciones IP.

CNM permite configurar la asignación de direcciones IP de tres maneras diferentes:

- Manualmente: no hay DHCP configurado en el equipo
- Por DHCP
  - o Servidor DHCP: el servidor DHCP es en la misma red que el equipo
  - o DHCP Relay: el servidor DHCP no está en la misma red que el equipo. En este caso, es necesario proporcionar la dirección IP del servidor DHCP.

4. Controlador SD-WAN

El controlador SD-WAN es un nuevo componente de red que se entrega junto con cualquier solución SD-WAN. Se trata de un módulo esencial para poner en marcha las nuevas capacidades. El controlador trabaja, en función del modelo de datos, para proporcionar funciones SD-WAN básicas y avanzadas (como tenencia múltiple, arquitecturas

4.1. ¿Qué es y cuáles son las funciones del Controller?

Es el punto de control de la red SD-WAN. A grandes rasgos se podría decir que las funciones son tres:

a) aloja el modelo de datos

b) presenta un interfaz de usuario gráfico para acceder/modificar el modelo de datos

c) sincroniza el modelo de datos con los dispositivos de la red.

4.2. ¿Se soporta multitenant en el Controller?

Si. Controller es un elemento de Cloud Net Manager 3.x (CNM), y como tal soporta multitenant, tanto a nivel de distintos clientes como a nivel de distintos proveedores los cuales a su vez dan servicio a sus clientes.

4.3. ¿Cuál es el soporte de alta disponibilidad, escalabilidad y redundancia del Controller?

Controller y CNM están construidos mediante microservicios (usando tecnología kubernetes), lo que proporciona de forma nativa alta disponibilidad, escalabilidad y redundancia.

4.4. ¿Qué sucede si cae el Controller o la conexión del mismo a la red?

No será posible realizar cambios en la configuración de la red, pero el servicio no se verá afectado puesto que cada dispositivo tiene su copia del modelo de datos y es capaz de trabajar de forma autónoma.

4.5. ¿Cuáles son las modalidades de venta del Controller?

Controller es un elemento integrante de CNM3. CNM3 es la plataforma de gestión Teldat que pude contratarse en modo servicio (SaaS) o en modo producto. En el primer caso la infraestructura reside en una nube pública (nube Microsoft) y es mantenida por Teldat, mientras que, en el segundo caso, se aloja en un entorno de máquina virtual en domicilio del cliente (VA, Virtual Appliance). En ambos casos, se requiere licencia para los dispositivos a gestionar.

5. Inspección Profunda de Paquete (DPI) / Visibility

Uno de los principales objetivos de las empresas es controlar y visualizar qué servicios y aplicaciones usan sus redes. La DPI permite a los dispositivos verificar y analizar todo el tráfico de red que pasa por ellos, y facilitar esta información a través de una herramienta fácil de utilizar. Además, poder identificar la aplicación en la capa 7 es una función útil para las empresas porque, a día de hoy, la mayoría de aplicaciones se almacenan en nubes públicas. Este apartado también explica cómo identificar y priorizar el tráfico.

5.1. ¿Es posible utilizar la información de nivel 7 obtenida por el DPI para establecer políticas de encaminamiento, QoS y filtrado?

Si. Las políticas se pueden realizar en función de parámetros de nivel 3, 4 y 7.

5.2. ¿Qué posibilidades de inspección son posibles si se usa SAP?

La aplicación propietaria SAP utiliza un puerto conocido (3200), de forma que es sencillo identificarla. Para SAP en modo servicio, ver la pregunta más adelante acerca de la identificación de aplicaciones en nubes públicas.

5.3. ¿Qué posibilidades de inspección son posibles si se usa Citrix?

Citrix permite inspección con una granularidad a dos niveles, el primer nivel consiste en identificar las distintas

aplicaciones y el segundo nivel consiste en identificar dentro de una misma aplicación los distintos niveles de prioridad que puedan ser necesarios para transportar información de dicha aplicación (Citrix proporciona 4 niveles de prioridad: "Very High" para el audio, "High" para la interface visual de usuario, "Medium" para MediaStream y "Low" para impresoras y puertos serie y paralelo). Esta última forma de clasificación es la más interesante, pues proporcionar una mayor granularidad y garantiza la prioridad necesaria según la criticidad de los datos transmitidos. Este segundo nivel es soportado por el DPI (nota, requiere configurar ICA en modo Multi-Stream, lo cual implica la transmisión de cada nivel de prioridad en una sesión TCP distinta).

5.4. ¿Es posible identificar aplicaciones en nube pública como Salesforce, Microsoft365, Facebook, Youtube, etc.?

La identificación de esas aplicaciones tiene cierta complejidad porque suelen realizar varias conexiones simultáneas para repartir los procesos, donde las direcciones IP y nombres de dominio a los que se conectan son variados y hay que tenerlos identificarlos todos. Por ejemplo, en el caso de Salesforce, la identificación se realiza a nivel IP para los distintos servicios del proveedor, según se indica en **este enlace**, para Microssoft365 la identificación basada en nombres de dominios e IP y está disponible en **este enlace**, y en general la información está disponible en las mismas fuentes y en terceros, a modo de ejemplo, el tráfico **Facebook**.

6. Autoaprovisionamiento / Sincronización de configuración

La gestión centralizada de dispositivos en una solución SD-WAN permite su aprovisionamiento automático. A este proceso se le conoce con el nombre "Zero Touch Provisioning" (ZTP). ZTP permite instalar nuevos dispositivos en sucursales o centros de datos y conectarlos automáticamente a la red, sin que el instalador deba tener conocimientos técnicos muy avanzados. En este apartado se explica cómo funciona este proceso en las soluciones SD-WAN de Teldat.

6.1. ¿Qué se entiende por autoprovisión?

El proceso por el cual un dispositivo (Branch Edge o Datacenter Edge) de fábrica, es capaz de recibir y aplicar su configuración de forma automática al conectarse a la red, sin que para ello se haya realizado localmente sobre el mismo ninguna acción previa adicional. Para ello el equipo contacta con CNM, se identifica, y recibe su configuración de forma segura.

6.2. ¿Qué se entiende por sincronización de configuración?

La automatización en el envío de configuración desde CNM cuando se cambia el modelo de datos en Controller. Se podría decir que la autoprovisión es un caso especial de la sincronización, dado que es el que ocurre la 1ª vez que el equipo se instala tras salir de fábrica.

6.3. ¿Qué protocolos se utilizan y cuál es el nivel de seguridad en las comunicaciones?

Se utiliza HTTPS (SSL/TLS). El servidor CNM se identifica mediante un certificado digital para evitar suplantaciones y la información se autentica y cifra en ambos sentidos. Opcionalmente se puede utilizar HTTP si no se desea cifrar o no se puede utilizar el puerto 443 (HTTP usa el puerto 80).

6.4. ¿Cómo se asegura que la autoprovisión se realiza en la ubicación especificada?

Este es un tema importante si se utilizan accesos "públicos" de internet para una red SDWAN corporativa, ya que bastaría la posesión de un equipo para autoprovisionarlo en un acceso cualquiera de internet emulando ser el punto remoto y consiguiendo así acceso a la red interna. Para evitarlo, es posible deshabilitar la autoprovisión automática de los equipos al darlos de alta en CNM hasta que el operador de CNM se asegura por otro canal que la instalación se está realizando en la ubicación correcta (por ejemplo confirmándolo telefónicamente con el personal de la oficina), una vez asegurado, basta habilitar en CNM la autoprovisión de dicho equipo mediante un clic en el interfaz.

6.5. ¿Cómo se evita la conectividad de un Branch Edge en un acceso de red distinto al que le corresponde (robo de equipo y posterior instalación en un acceso a internet no autorizado)?

En desarrollo diversos mecanismos para evitar este caso. Una posibilidad es detectar si un punto remoto se mantiene más de un determinado tiempo desconectado de la red (lo cual podría significar que el equipo remoto está siendo trasladado a otro lugar), para deshabilitar la conectividad del mismo a la red; en caso de

falsa alarma se activaría tras una intervención manual en CNM.

7. Otros

Aquí se resuelven otras preguntas relativas a las funciones SD-WAN o el modelo de licenciador Teldat. Funciones como la monitorización del dispositivo, o su capacidad de integración con componentes pertenecientes a terceros (a través de la interfaz de programación de aplicaciones), son otros de los temas que aborda este apartado.

7.1. ¿Qué licencias son obligatorias y que licencias son opcionales?

En el equipo:

1.Licencia IPSec o IPSec hardware (según el modelo): Obligatoria

2.Licencia de aceleración (UP, UP1 o UP2): Opcional

3.Licencia habilitación ZTP: Para autoprovisión (esta licencia solo está disponible en tiempo de fabricación)

En CNM (licencia por cada equipo a gestionar):

1.Licencia Base: Para poder gestionar el equipo en CNM y autoprovision.

2.Licencia Controller: Para generar y administrar la configuración en el modelo de datos.

3.Licencia Visualizer: Para visibilidad del tráfico (en desarrollo). Alternativamente se puede usar la plataforma Teldat Visualizer para la visibilidad del tráfico (requiere licencia por equipo) de forma separada de CNM.

7.2. ¿Cuáles son las opciones de monitorización?

Cuando el equipo es gestionado por CNM, se monitoriza y se pueden generar alarmas a partir de la conectividad con CNM, la versión de software (CIT+BIOS+FW), CPU, memoria y disco.

7.3. ¿Existe un Northbound API? ¿Qué métodos soporta?

Si. Se soportan los métodos relacionados con la provisión y configuración.

SOLUCIONES
DE COMUNICACIÓN FLEXIBLES
QUE CRECEN CON USTED.

La solución SD-WAN de Teldat permite a los clientes la migración gradual a una red SD-WAN con funcionalidad completa desde un equipo de acceso tradicional. Esto es así porque la arquitectura de nuestra solución se basa en productos que se licencian independientemente de forma que el cliente puede configurarse una solución a medida de las necesidades de su negocio, en función de su plan de transición. Si a esto se añade la enorme variedad de interfaces con el underlay que presentan los edges de Teldat, la solución SD-WAN que ofrecemos a nuestros clientes es única en cuanto a flexibilidad, potencia y escalabilidad.

Teldat acaba de relanzar una nueva versión de su solución para SD-WAN (CNMv3). Ésta cuenta con una interfaz de usuario mucho más moderna y sensible, lo que le permite adaptarse a los distintos tipos y tamaños de pantalla. Además, gracias a la nueva computación basada en microservicios, la solución SD-WAN de Teldat ofrece mayor disponibilidad y escalabilidad.

La integración de un API Northbound, permitiendo así el uso de plataformas externas y su gestión desde la red SD-WAN, incluyendo registros, modificaciones, consultas, retiradas de dispositivos, manejo de usuarios, grupos, etc. La nueva solución CNMv3 también permite gestionar la red en base a un nuevo concepto: los proyectos. El cliente puede configurar así redes por proyectos y los equipos de cada proyecto son independientes, cada proyecto con sus plantillas individuales.

cnm BASE	Plataforma inicial de software que gestiona la inteligencia distribuida de la WAN e integra distintas redes en una única plataforma.
cnm PROVISIONER	Permite la instalación automática de dispositivos en sucursales. Facilita enormemente la puesta en marcha y reduce los costes asociados.
cnm VISUALIZER	Visualiza todos los servicios y aplicaciones de la red con el fin de efectuar controles y análisis a distintos niveles. Ofrece una visión panorámica completa a nivel de red y por sucursales.
cnm CONTROLLER	Define y configura la red usando un formato sencillo, intuitivo y automatizado (lo que reduce considerablemente el tiempo empleado en la gestión de la red).
cnm SERVICER	Ofrece servicios adicionales a soluciones SD-WAN estándar (como mayor seguridad, optimización de la WAN, almacenamiento conectado en red, etc.). También proporciona un sistema avanzado de gestión por aplicaciones.

Teldat GROUP | Sedes

España
Teldat S.A.
Parque Tecnológico de Madrid
Tres Cantos – 28760
Madrid (Spain)
Phone:+34 91 807 6565
info@teldat.com

Alemania
bintec elmeg GmbH
Suedwestpark 94. 90449
Nuremberg (Germany)
Phone: +49 911 9673 0
info@bintec-elmeg.com

Datos de contacto de nuestras oficinas comerciales en www.teldat.com