



## SD-WAN FAQs

This document is dedicated to FAQs related to SD-WAN and it shows the concepts that are more commonly related with the SD-WAN technology, and how they are implemented in the Teldat solution.

# Index

<b>1. Scenario &amp; Data Model</b>	<b>4</b>
1.1. What is the Data Model?	4
1.2. How many access networks and what kind of them can be set up and used in a SD-WAN network?	4
1.3. How can be indentified applications to apply them policies and SLA?	4
1.4. How many applications can be identified to assign policies and SLA?	4
1.5. How is the SLA level established?	4
1.6. Are the probes active or passive? Can be parameterized?	4
1.7. Is it possible to define SLA levels to applications? How?	4
1.8. How many SLA profiles are supported?	4
1.9. What happens when a defined SLA level in an application cannot be achieved?	5
1.10. How many users and IP networks are supported?	5
1.11. How is quality of service (QoS) supported?	5
1.12. Is direct access to internet (breakout) supported from remote offices?	5
1.13. Are native MPLS services supported, e.g. telephony over IP network?	5
1.14. Does Teldat SD-WAN Controller support the configuration of access devices to MPLS networks?	5
1.15. Need the customer two devices, one for access and other for the SD-WAN capabilities, in Teldat SD-WAN scenario?	5
1.16. How is achieved connectivity between SD-WAN and not yet migrated SD-WAN point?	5
1.17. Are several Datacenters supported?	5
1.18. Traffic balancing over different access/networks simultaneously is supported?	5
<b>2. Data Center Edge</b>	<b>6</b>
2.1. What is and what is the functions of the element "Datacenter Edge"?	6
2.2. What are the possible choices for the "Datacenter Edge"?	6
2.3. Does "Datacenter Edge" supports redundancy?	6
2.4. Does "Datacenter Edge" supports scalability?	6
<b>3. Branch Edge</b>	<b>6</b>
3.1. What is and which is the role of the "Branch Edge" Element?	6
3.2. What are the possible choices for "Branch Edge"?	6
3.3. Is it possible to select the LAN IP address range of each branch office manually?	6
3.4. How are assigned the IP addresses in the LAN in each remote office?	6
<b>4. SD-WAN Controller</b>	<b>7</b>
4.1. What is and which are the functions of the Controller?	7
4.2. Does the Controller support multitenant?	7
4.3. Which is the support of high availability, scalability, and redundancy in the Controller?	7
4.4. What happens if the Controller or its connectivity to the network goes down?	7
4.5. Is the Controller a service or a product?	7
<b>5. Deep Packet Inspection (DPI) / Visibility</b>	<b>7</b>
5.1. Is it possible to use the level 7 data from DPI for routing, QoS, and filtering policies?	7
5.2. What are the possibilities of inspection when SAP is used?	7
5.3. What are the possibilities of inspection when Citrix is used?	7
5.4. Would it be possible to identify applications in the public cloud such as Salesforce, Youtube, Facebook, etc.?	8
<b>6. Self Provision/Configuration Synchronization</b>	<b>8</b>
6.1. What is meand by self-provision?	8
6.2. What does configuration synchronization mean?	8
6.3. Which protocols are used and which is the security level in the communications?	8
6.4. How is ensured that the self-provision is carried out at the specified location?	8

6.5. How can be restricted the use of a Branch Edge in an unsure access network (theft of equipment and subsequent installation in an unauthorized internet access?).....	8
<b>7.Others.....</b>	<b>8</b>
7.1. What licenses are mandatory and which ones are optional?.....	9
7.2. What monitoring options?.....	9
7.3. Is there a Northbound API? What methods are supported?.....	9

# 1. Scenario & Data Model

This section describes which are the principal network scenarios where a SD-WAN solution fits, providing an overview of the main features and functionalities that can be found in SD-WAN. In addition, it's explained how the data model is built to add the capabilities to configure, manage and monitor a complete enterprise WAN network. Some of the topics in this section are the following. Type of network access, SLAs, application identification, QoS...

## 1.1. What is the Data Model?

In some sense, the data model is like a database which contains information from the SDWAN network. It is necessary to unify the network definition because one of the key aspects of SDWAN is the centralization of the entire network control plane in software. In the SDWAN Teldat approach, the control plane is implemented in the "Controller", and from the "data model", it builds / modifies the configurations of all the devices in the network in real time.

*Note: In the "traditional" networking the configuration is done device by device (CLI), there is no a "data model" as such, and one could say that the data model is distributed in the configuration files of each device and all together make up the network. Although it is also possible to generate and maintain a SDWAN network in this way, throughout this document is assumed that it is not done in this way, instead it is done using the Controller.*

## 1.2. How many access networks and what kind of them can be set up and used in a SD-WAN network?

Two types of networks can be configured: MPLS and Internet, without limit on the number of access networks / suppliers of each type. It is necessary to differentiate between these two types of network since MPLS networks do not have connectivity between them, and to generate the connectivity configuration of remote points with concentrators must be ensured that they belong to the same MPLS network.

## 1.3. How can be indentified applications to apply them policies and SLA?

Using an ordered list of sentences at level 3 (addresses), 4 (protocols and ports) or 7 (Host Name http). These sentences can be inclusive or exclusive, for example, to identify all the traffic except traffic to xxxxx.com, or all TCP traffic except addressed to port X.

## 1.4. How many applications can be identified to assign policies and SLA?

There is not limit on the number of applications, nor the number of policies. It is possible to associate a policy to an application, but to facilitate the management it is possible to group applications to apply a common policy, moreover, there is not limit either in the number of applications per group.

## 1.5. How is the SLA level established?

Probes are generated from the remote points through all networks access, and delay, delay variation (jitter) and loss rate are measured.

## 1.6. Are the probes active or passive? Can be parameterized?

Probes are active, so they consume some traffic and CPU, but in practice it is negligible and thus it is possible to get SLA information before any application starts. Probes parameterization is included in the data model, so the bandwidth consumed can be configured precisely.

## 1.7. Is it possible to define SLA levels to applications? How?

Yes. As mentioned before, it is possible to associate SLA thresholds with applications or groups of applications, i.e. the maximum acceptable level for delay, jitter and loss rate for such application(s).

## 1.8. How many SLA profiles are supported?

There is no limit in the number of SLA profiles that can be defined.

### ***1.9. What happens when a defined SLA level in an application cannot be achieved?***

Application (or group of applications) is (are) moved to another access network where the SLA level is better. (for each application and remote branch type, the preferred access networks available in that branch are configured). The preferred and backup access networks are defined in an application(s) by application(s) basis.

### ***1.10. How many users and IP networks are supported?***

There is no limit in the number of users and IP networks supported.

### ***1.11. How is quality of service (QoS) supported?***

For any application (or group of applications), it is possible to define for each of the network access:

- Priority: Real time, High, Normal and Low
- Bitrate limit: maximum bitrate that can use one or a group of application categories.
- Weight: percentage of throughput that is guaranteed to one or a group of application categories, in case of overload.
- DSCP or ToS marking: mark the traffic with DSCP or ToS
- Queue length for each application category.

To ease the burden of configuration and maintenance, this is configured using templates of remote offices sharing the same QoS configuration.

### ***1.12. Is direct access to internet (breakout) supported from remote offices?***

Yes, it is supported. To do so, simply identify the type of traffic to be sent directly to the internet in each remote site. For example, everything other than their own services. To ease the burden of configuration and maintenance, this is configured using templates of remote offices sharing the same breakout configuration.

### ***1.13. Are native MPLS services supported, e.g. telephony over IP network?***

Yes, in the same way that breakout internet traffic is supported, it is also possible to select services/applications and send them directly through the MPLS network (without tunnels, i.e. in the "underlay").

### ***1.14. Does Teldat SD-WAN Controller support the configuration of access devices to MPLS networks?***

A: Yes, from CNM Controller is possible to configure all the necessary parameters to connect a device directly to the MPLS network. In CNM is possible to configure parameters of the MPLS like: routing protocol, peer address, Local AS, Remote AS...

### ***1.15. Need the customer two devices, one for access and other for the SD-WAN capabilities, in Teldat SD-WAN scenario?***

A: No, the customer has both possibilities. If the customer already has deployed an access device from the carrier, Teldat can deploy the SD-WAN device as a second level device, but if the customer doesn't have it, Teldat devices can be also deployed as an access device with SD-WAN Controller.

### ***1.16. How is achieved connectivity between SD-WAN and not yet migrated SD-WAN point?***

Via the VPNs hub ("Datacenter Edge") is possible to connect remote points migrated and non-migrated since this element keeps connectivity with migrated sites through the SDWAN tunnels ("overlay") and also connectivity with the rest of the network directly ("underlay").

### ***1.17. Are several Datacenters supported?***

Yes, several Datacenters are supported without limitation in the number of Datacenters or Datacenter Edges. Neither the number of Branch Edges that connect with a Datacenter is limited.

### ***1.18. Traffic balancing over different access/networks simultaneously is supported?***

It is possible to select for each application or group of applications the access/network to use preferentially whenever SLA compliance is achieved, so it is possible to balance different applications for different access/networks.

## 2. Data Center Edge

The Data Center is one of the main components in an enterprise network, and to implement a SD-WAN solution the Data Center Edge device requires some specific characteristics that are explained here. The concept of a VPN hub, the alternatives in the redundancy implementation and other topics such as the scalability are answered.

### ***2.1. What is and what is the functions of the element "Datacenter Edge"?***

It is a "hub of VPNs" where the remote points are connected to it using physical networks ("underlay") and establishing tunnels to build the private network ("overlay").

On the other hand, the Datacenter Edge connects to the internal network of a Datacenter which hosts services/ applications, giving access from remote points to them through the overlay.

### ***2.2. What are the possible choices for the "Datacenter Edge"?***

For small networks, up to 200 remote points and 300Mbps aggregated, is available a solution based on proprietary hardware, Teldat RXL14000. For any size of network, software vRXL is available in ISO format, to run on bare-metal or on a VM on KVM, or AMI format (Amazon Machine Image) to run on Amazon.

### ***2.3. Does "Datacenter Edge" supports redundancy?***

Yes, it is possible to use 2 Datacenters Edges in high availability mode, in active/active configuration, i.e. in a usual situation each one is supporting X remote sites and in case of one of them goes down, the other one assumes its connections (2X connections).

### ***2.4. Does "Datacenter Edge" supports scalability?***

Yes. A Datacenter Edge (or couple of them in redundant mode) provides services to a specific number of sites and supports a specific aggregated throughput, but as many Datacenter Edges (or pairs of them in redundant mode) as desired can be installed.

## 3. Branch Edge

A SD-WAN solution simplifies the configuration, management and monitoring of a network which provides connectivity between branches and/or Data Centers. Thus, the branch edge becomes a key element of the solution. To select the proper branch device, it's necessary to provide the all the technical and commercial information. Topics such as the role of the branch edge device or the possible choices from Teldat portfolio, are covered here.

### ***3.1. What is and which is the role of the "Branch Edge" Element?***

It is the element in the remote point making the nexus between the customer's LAN network and the SDWAN network. The main functions are: connection with the LAN network(s), connection with the WAN network(s), setup the overlay through the Datacenter Edge, generate the probes and measure SLA, identify services/ applications, apply QoS and decide SLA-based on routing policies.

### ***3.2. What are the possible choices for "Branch Edge"?***

The following Teldat routers: Teldat-V, Teldat-M1, Teldat-iM8, Atlas-60, Atlas-i70, Teldat-H2Auto, H2Auto-Teldat + and Teldat-H2Rail.

### ***3.3. Is it possible to select the LAN IP address range of each branch office manually?***

Yes, the user can define from a big IP address range, the group of IP addresses that are assigned to a specific branch office.

### ***3.4. How are assigned the IP addresses in the LAN in each remote office?***

In the remote office template, the user defines which LAN profiles are assigned. A LAN profile is a configuration for the LAN that sets the maximum number of IP addresses that can be assigned to a specific 'User Group' (for example 16 IP addresses for phones and 8 IP addresses for Guest users), if VLANs are used from the router to the LAN and how are the IP address assigned.



CNM allows three different methods to assign the IP addresses to the user devices:

- Manually: there is not DHCP configured in the device.
- By DHCP:
  - o DHCP Server: the DHCP server is in the same network as the devices
  - o DHCP Relay: the DHCP server is not in the same network. In this case, to provide the DHCP server IP address is required.

## 4. SD-WAN Controller

The SD-WAN controller is a new component in the network that comes with any SD-WAN solution. It is an important module to implement new capabilities. The controller works based on the data model to provide basic and advance SD-WAN features as multi-tenancy, high available architectures, reduce point of failures... All these concepts are explained here from a Teldat SD-WAN solution perspective.

### ***4.1. What is and which are the functions of the Controller?***

It is the control point for the SD-WAN. Broadly speaking, it could be said that its functions are 3: a) houses the data model, b) shows a graphical user interface to access / modify the data model and c) synchronize the data model with the network devices.

### ***4.2. Does the Controller support multitenant?***

Yes. Controller is an element of Cloud Net Manager 3.x (CNM), and as such, multi-tenant is supported. There are 2 multitenant levels supported, at service provider level and at the customer level.

### ***4.3. Which is the support of high availability, scalability, and redundancy in the Controller?***

Controller and CNM are build using microservices (based on kubernetes technology), which provides natively high availability, scalability and redundancy.

### ***4.4. What happens if the Controller or its connectivity to the network goes down?***

It would not be possible to apply configuration changes to the network, but the service will not be affected since each device has its copy of the data model and can work autonomously.

### ***4.5. Is the Controller a service or a product?***

Both. Controller is an integral element of CNM3. CNM3 is the Teldat management platform that could be used in service mode (SaaS) or product mode. In the first case, the infrastructure is in a public cloud (Microsoft cloud) and is maintained by Teldat, while in the second case, it runs in a virtual machine in the customer's home environment (VA, Virtual Appliance). In both cases, license for devices to be managed are required.

## 5. Deep Packet Inspection (DPI) / Visibility

Control and visualization of the applications and services that are using our network, is one of the goals for the enterprises. The DPI allows the devices to check and analyze all the network traffic going through them, and provide that information in a user-friendly tool. Furthermore, the identification of application at level 7 is a desirable feature for enterprises, because most of the applications, nowadays, are hosted in the public cloud. How to identify and prioritize this traffic is covered in this area.

### ***5.1. Is it possible to use the level 7 data from DPI for routing, QoS, and filtering policies?***

Yes. Routing, QoS and Policies can be based on parameters of level 3, 4 and 7.

### ***5.2. What are the possibilities of inspection when SAP is used?***

SAP proprietary application uses well known TCP port 3200, so, identification is easy. For SAP in the public cloud, please, see below about identification in public clouds.

### ***5.3. What are the possibilities of inspection when Citrix is used?***

Citrix allows inspection with granularity at two levels, the first level consist in identifying various applications and the second level consists in identifying different levels of priority that may be necessary for transporting

application information within a single application (Citrix provides 4 priority levels: for audio "Very High", "High" for the visual user interface, for MediaStream "Medium" and "Low" for printers and series and parallel ports). This last form of classification is the most interesting, since it provides a higher granularity and guarantees the necessary priority according to the criticality of the data transmitted. This second level is supported by the DPI (note, it requires to configure ICA in Multi-Stream mode, which implies the transmission of each priority level in a different TCP session).

#### ***5.4. Would it be possible to identify applications in the public cloud such as Salesforce, Youtube, Facebook, etc.?***

Applications in public cloud are not easy to identify as they use several simultaneous connections to distribute load and roles in different servers, then it is required to have predefined them. For instance, for Salesforce, identification is done by IP address, as indicated [clicking here](#), for Microsoft365 identification is based on domain names and IP addresses and it is [available here](#), in general, information is usually accessible from sources and third parties, for instance for [Facebook](#).

## **6. Self Provision / Configuration Synchronization**

The centralized management of the devices in a SD-WAN solution, allows to provision them automatically. This process is known as 'Zero Touch Provisioning' (ZTP). ZTP adds the capability to deploy a new branch edge or data center edge device automatically in the network, reducing the necessary expertise of the installer. How this procedure is run in a Teldat SD-WAN solution is explained here.

#### ***6.1. What is meant by self-provision?***

The process whereby a factory setting device (Branch Edge or Datacenter Edge), is able to receive and apply their settings automatically when is connected to the network, without any local action done on the device. This equipment contacts with CNM, identifies itself, and receives its configuration in a secure way.

#### ***6.2. What does configuration synchronization mean?***

Configuration Synchronization is the process in which devices automatically download their configuration from CNM when anything has been changed in the data model. It could be said that the self-provision is a special case of it, since it is occurring the 1st time that the device is installed after leaving the factory.

#### ***6.3. Which protocols are used and which is the security level in the communications?***

HTTPS (SSL/TLS) is used. CNM server is identified by a digital certificate to avoid spoofing and information is authenticated and encrypted in both directions. Optionally HTTP can be used if encryption is not desired or you cannot use port 443 (HTTP uses port 80).

#### ***6.4. How is ensured that the self-provision is carried out at the specified location?***

This is an important issue if 'public' access to internet are used for a corporate SDWAN network, since a malicious installer could use a fake internet access to gain access to the internal network. To avoid this, it is possible to disable automatic self-provision of devices in CNM, and only when CNM manager verifies that installation is safe using any method (for example, confirming by phone with the remote branch staff), and once secured, just to enable in CNM the self-provision of the device by clicking on the interface.

#### ***6.5. How can be restricted the use of a Branch Edge in an unsure access network (theft of equipment and subsequent installation in an unauthorized internet access?)***

This is an important issue if 'public' access to internet are used for a corporate SDWAN network, since a malicious installer could use a fake internet access to gain access to the internal network. To avoid this, it is possible to disable automatic self-provision of devices in CNM, and only when CNM manager verifies that installation is safe using any method (for example, confirming by phone with the remote branch staff), and once secured, just to enable in CNM the self-provision of the device by clicking on the interface.

## **7. Others**

Some other questions related with the SD-WAN features or the Teldat license model are answered. Capabilities such



as the device monitoring or the integration with third party elements (through API) are some of the topics which are covered in this section.

### ***7.1. What licenses are mandatory and which ones are optional?***

In the device:

1. IPSec or IPSec hardware license (depending on model): mandatory
2. Acceleration (UP, UP1 and UP2) license: optional
3. ZTP enable license: to self-provision (this license is only available at manufacturing time)

In CNM (license per device to be managed):

1. Base license: to manage the device and self-provision.
2. Controller license: to generate and manage the settings in the data model.
3. Visualizer license: for traffic visibility (in development). Alternatively, you can use the platform Teldat Visualizer for the visibility of traffic (requires device license) separately from CNM

### ***7.2. What monitoring options?***

When devices are managed by CNM, vital signs and connectivity can be monitored and alarms can be raised from CPU status, memory status, flash status, or in case of incorrect firmware release (CIT+BIOS+FW).

### ***7.3. Is there a Northbound API? What methods are supported?***

Yes. Methods related to provisioning and configuration are supported.






# FLEXIBLE COMMUNICATIONS SOLUTIONS THAT GROW WITH YOU.



The Teldat SD-WAN solution allows customers to gradually migrate from a traditional access device to a fully operative SD-WAN network. Because our architectural solution is based on individually licensed products, customers can configure customized solutions to meet their specific needs and transition plan. The addition of an enormous variety of interfaces with Teldat edge devices providing the underlay, has produced a unique and flexible SD-WAN solution at the same time as being powerful yet scalable: a true bonus for our customers.

Moreover, Teldat has just relaunched a new version of its SD-WAN solution called CNMv3, which has a new modern interface for users and it has an improved responsive screen, that adapts perfectly to different screen types and sizes. Additionally, the core computing is new and based on microservices. This offers Teldat's SD-WAN solution a higher level of availability and scalability.

A Northbound API has been included to enable the integration of external platforms and their management within the SD-WAN network, including registration, modifications, queries and withdrawals of devices, users, groups, etc. Another important new feature of Teldat's SD-WAN platform CNMv3, is the ability to now manage the network based on a new the concept, projects. So the client can establish different networks within it's SD-WAN software platform, enabling the devices and templates of each project to work independently.

 <b>BASE</b>	Initial software platform that manages the distributed intelligence of the WAN and integrates the different networks into a single platform.
 <b>PROVISIONER</b>	Enables edge devices to be installed at branch level using ZTP. Makes deployment immensely simple and reduces related
 <b>VISUALIZER</b>	Entire network visibility of services and applications for monitoring and analysis at different levels. From a whole network level to branch level.
 <b>CONTROLLER</b>	Defines and configures the network in a simple, intuitive and automated format, considerably reducing dedicated network management.
 <b>SERVICER</b>	Offer additional services to a standard SD-WAN solution such as enhanced security, WAN optimization, NAS and more. It also offers an advanced management application system.



GROUP

Headquarters

#### Spain

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

#### Germany

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



©2018 Teldat SA | This document shall be used only for information purposes. Teldat reserves the right to modify any specification without prior notice. All trademarks mentioned in this document are the property of their respective owners. Teldat accepts no responsibility for the accuracy of the information from third parties contained on this document.  
Publish Date: Mayo, 2018

Our sales offices contact details are on [www.teldat.com](http://www.teldat.com)