Mplify Standard

Mplify 119

Universal SD-WAN Edge Implementation Agreement

June 2025

Disclaimer

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and Mplify Alliance (Mplify) is not responsible for any errors. Mplify does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by Mplify concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by Mplify as a result of reliance upon such information.

The information contained herein is intended to be used without modification by the recipient or user of this document. Mplify is not responsible or liable for any modifications to this document made by any other party.

The receipt or any use of this document or its contents does not in any way create, by implication or otherwise:

a) any express or implied license or right to or under any patent, copyright, trademark or trade secret rights held or claimed by any Mplify member which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor
b) any warranty or representation that any Mplify members will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor
c) any form of relationship between any Mplify member and the recipient or user of this document.

Implementation or use of specific Mplify standards, specifications, or recommendations will be voluntary, and no Member shall be obliged to implement them by virtue of participation in Mplify Alliance. Mplify is a global alliance of network, cloud, cybersecurity, and enterprise organizations working together to accelerate the AI-powered digital economy through standardization, automation, certification, and collaboration. Mplify does not, expressly or otherwise, endorse or promote any specific products or services.

Table of Contents

List of Figures

List of Tables

1 List of Contributing Members

The following members of Mplify participated in the development of this document and have requested to be included in this list.

- AT&T
- Bell Canada
- Colt
- Sparkle
- Verizon
- Versa

2 Abstract

This document defines the Universal SD-WAN Edge (USWE) and specifies the USWE implementation requirements. It also specifies the requirements on the vendor propriety SD-WAN Edge and on SD-WAN Vendor Manager to support the interoperability between these entities and the USWE. A USWE allows an SD-WAN Service Provider (SP) to deploy a single SD-WAN Edge implementation to be deployed at SP common locations. A Universal SD-WAN Edge can participate as an SD-WAN Edge in a Mplify-compliant SD-WAN Service (as specified in MEF 70.1 [42]) with SD-WAN Edges and SD-WAN Vendor Managers provided by other vendors that meet the requirements specified herein.

The Universal SD-WAN Edge included in this specification includes the following:

- Universal Management Plane
    - The set of functions that allows management of the USWE instance.
- Universal Control Plane
    - The set of functions that allows the USWE implementation to exchange routing information with the SD-WAN Vendor control plane.
- Universal Data Plane
    - The set of functions that allows the USWE implementation to exchange data traffic with other SD-WAN Edges within an SD-WAN Service
- Subscriber Routing Domain

- The set of functions that contains all the information about how to route between the Subscriber Network IP Prefixes associated with a given SD-WAN Service

Some of these functions, as described, are required to be supported in both the Universal SD-WAN Edge and the interconnected vendor-proprietary SD-WAN Edges or the SD-WAN Vendor Controller.

3 Terminology and Abbreviations

This section defines the terms used in this document. In many cases, the normative definitions of these terms are found in other documents. In these cases, the third column is used to provide the reference that is controlling, in other Mplify or external documents.

In addition, terms defined in MEF 66 [38], MEF 70.1 [42], and MEF 105 [43] are included in this document by reference and are not repeated in the table below.

Term	Definition	Reference
Advanced Encryption Standard	A specification for the encryption of data	NIST FIPS 197-upd1 [44]
Bidirectional Forwarding Detection	A UDP-based detection protocol that provides a low-overhead method of detecting failures in the forwarding path between two adjacent routers.	IETF RFC 5880 [27]
Control Plane Interface	The network interface that enables the Universal SD-WAN Edge instance to exchange the routing information and other control information with the SD-WAN Vendor Control Plane	This document
Control Tunnel Virtual Connection	A point-to-point forwarding relationship for the Control Plane traffic between the Universal SD-WAN Edge Instance and an SD-WAN Edge or another device connected to that same UCS and terminating the tunnel	This document
Control Tunnel Virtual Connection End Point	The logical construct which terminates a CTVC by performing any encapsulation/encryption and decapsulation/decryption necessary to forward control plane IP Packets over the CTVC.	This document
Fault Monitoring	The function that detects failures of interfaces, operations, or other functions.	This document
Fault Notification	A notification that is sent by the Universal SD-WAN Edge implementation with a specific format to indicate a failure.	This document
Generic Routing Encapsulation	A protocol for encapsulating data packets in order to set up a direct network connection.	IETF RFC 1701 [3]
Multi-Protocol Label Switching	A networking technology that routes traffic based on “labels,” rather than network addresses	IETF RFC 3032[11]
Network Address Translation	A method by which IP addresses are mapped from one realm to another, in an attempt to provide transparent routing to hosts.	IETF RFC 2663 [9]
Point of Presence	A location where the SP has physical equipment deployed.	This document
Routing Domain	A domain (UCS, Subscriber, or Service) that defines the domain within which IP addresses must be uniquely assigned, and packets destined for those IP address are consistently routed.	This document
SD-WAN Vendor	Any entity developing proprietary SD-WAN software and/or hardware for its SD-WAN solution. The SD-WAN Vendor solution includes all the necessary functionalities, such as SD-WAN Edge, Control Plane, Management Plane, Data Plane, among other functions.	This document
SD-WAN Vendor Control Plane	The control plane that is used by the SD-WAN Vendor implementation which connects to the Universal SD-WAN Edge Control Plane Interface.	This document

Term	Definition	Reference
SD-WAN Vendor Manager	The application or function responsible for managing the functions and devices that comprise the SD-WAN Vendor's solution.	This document
SD-WAN Service Routing Domain	The Routing Domain containing and connecting the SD-WAN Edges and other infrastructure used to provide an SD-WAN Service.	This document
Subscriber Routing Domain	The Routing Domain containing and connecting the SD-WAN UNIs and the Subscriber's devices.	This document
UCS Routing Domain	The information about how to route between the End Points associated with a given UCS	This document
Universal Control Plane	The set of capabilities needed to enable route learning and route distribution required for the Universal SD-WAN Edge to interoperate with a compliant SD-WAN Vendor Control Plane.	This document
Universal Data Plane	The set of capabilities needed to enable the forwarding of Subscriber IP traffic between the Universal SD-WAN Edge and SD-WAN Vendor Edges or other Universal SD-WAN Edges.	This document
Universal Management Plane	The set of capabilities needed to configure, monitor, and report management information of the Universal SD-WAN Edge.	This document
Universal SD-WAN Edge	A sub-set of the SD-WAN Edge functionality described in MEF 70.1 [42] with additional functionality including the Universal Control Plane, the Universal Management, and the Universal Data Plane.	This document
Universal Tunnel Virtual Connection	A special implementation of the SD-WAN Tunnel Virtual Connection (MEF 70.1[42]) that uses the standard protocols to support the Universal SD-WAN Edge implementation.	This document
Universal Tunnel Virtual Connection End Point	The logical construct which terminates a UTVC by performing any encapsulation/encryption and decapsulation/decryption necessary to forward IP Packets over the Universal Tunnel Virtual Connection	This document
USWE instance	An instance of a Universal SD-WAN Edge implementation dedicated to a single SD-WAN Service	This document

Table 1 – Terminology

Abbreviation	Definition	Reference
AES	Advanced Encryption Standard	NIST FIPS 140
API	Application Programing Interface	This document
BFD	Bidirectional Forwarding Detection	IETF RFC 5881
CPI	Control Plane Interface	This document
CTVC	Control Tunnel Virtual Connection	This document
CTVC End Point	Control Tunnel Virtual Connection End Point	This document

Abbreviation	Definition	Reference
DHCP	Dynamic Host Configuration Protocol	IETF RFC 2131 [6]
ESP	Encapsulating Security Protocol	IETF RFC 4303
GRE	Generic Routing Encapsulation	IETF RFC 2784
HMAC	Hashed Message Authentication Mode	IETF RFC 4868
iBGP	Internal Border Gateway Protocol	This document
IPsec	Internet Protocol Security	This document
MPLS	Multi-Protocol Label Switching	IETF RFC 4364
PoP	Point of Presence	This document
SLAAC	Stateless Address Auto-Configuration	IETF RFC 4862
SP	Service Provider	This document
USWE	Universal SD-WAN Edge	This document
UTVC	Universal Tunnel Virtual Connection	This document
VPN	Virtual Private Network	This document
VRF	Virtual Routing and Forwarding	This document

Table 2 – Abbreviations

4 Compliance Levels

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 (RFC 2119 [5] RFC 8174 [29] when, and only when, they appear in all capitals, as shown here. All key words must be in bold text.

Items that are **REQUIRED** (contain the words **MUST** or **MUST NOT**) are labeled as **[Rx]** for required. Items that are **RECOMMENDED** (contain the words **SHOULD** or **SHOULD NOT**) are labeled as **[Dx]** for desirable. Items that are **OPTIONAL** (contain the words **MAY** or **OPTIONAL**) are labeled as **[Ox]** for optional**.**

Editor Note 1: The following paragraph will be deleted if no conditional requirements are used in the document.

A paragraph preceded by **[CRa]<** specifies a conditional mandatory requirement that **MUST** be followed if the condition(s) following the "<" have been met. For example, "**[CR1]<**[D38]" indicates that Conditional Mandatory Requirement 1 must be followed if Desirable Requirement 38 has been met. A paragraph preceded by **[CDb]<** specifies a Conditional Desirable Requirement that **SHOULD** be followed if the condition(s) following the "<" have been met. A paragraph preceded by **[COc]<** specifies a Conditional Optional Requirement that **MAY** be followed if the condition(s) following the "<" have been met.

5 Numerical Prefix Conventions

Editor Note 2: This section will be deleted if no numerical prefixes are used in the document.

This document uses the prefix notation to indicate multiplier values as shown in Table 3.

Decimal		**Binary**	
Symbol	**Value**	**Symbol**	**Value**
k	10^3	Ki	2^{10}
M	10^6	Mi	2^{20}
G	10^9	Gi	2^{30}
T	10^{12}	Ti	2^{40}
P	10^{15}	Pi	2^{50}
E	10^{18}	Ei	2^{60}
Z	10^{21}	Zi	2^{70}
Y	10^{24}	Yi	2^{80}

Table 3 – Numerical Prefix Conventions

6 Introduction

SD-WAN Services are at the core of the movement to simplify WAN. An SD-WAN Service is a connectivity service that creates an overlay network over one or more Underlay Connectivity Services as described in MEF 70.1 [42]. Given its benefits, there has been rapid and continued adoption of SD-WAN Services.

For the purposes of this document an SD-WAN Vendor is defined as any entity developing proprietary SD-WAN software and/or hardware for its SD-WAN solution. An SD-WAN Vendor Manager is defined as the application or function responsible for managing the functions and devices that comprise the SD-WAN Vendor's solution. Many SD-WAN Service Providers deploy multiple SD-WAN Vendors' solutions across their networks, each comprising of SD-WAN Edges and an SD-WAN Vendor Manager and using proprietary mechanisms for communication between them. The different SD-WAN Vendor solutions are used by the Service Provider (SP) to support different business requirements that their Subscribers may have.

Traditionally, critical business applications have been hosted in the data center run by the business. However, Subscribers are increasingly moving business-critical resources and services to cloud-based platforms. Therefore, there is a need to connect these Subscribers to a Point of Presence (PoP) (a location where the SP has physical equipment deployed) where such cloud-based platforms can be accessed such as an SP data center, a public cloud, or other organization's PoPs.

Deploying multiple SD-WAN Vendors Edges in SP data center, cloud, or PoP locations to match the SD-WAN Vendors Edges deployed at Subscriber locations may necessitate the SP having multiple deployment configurations for the SP data center, cloud, or PoP locations. This may result in costly management due to differences in the hardware and software required to support SD-WAN Vendor Edges, different management connectivity requirements for different SD-WAN Vendor Edges, and the deployment of different SD-WAN Vendor Edges at SP data center, cloud, or PoP locations.

A Universal SD-WAN Edge (USWE) Implementation is defined as a sub-set of the SD-WAN Edge functionality described in MEF 70.1 [42] with additional functionality including the Universal Control Plane, the Universal Management, and the Universal Data Plane. A USWE as defined within this document can be deployed at SP data center, cloud, or PoP locations to avoid the need to deploy multiple SD-WAN Vendor Edge Instances at these locations, provided that none of the SD-WAN Vendor's proprietary functionality is required. This enables the Service Provider to have a single standard deployment configuration (e.g., hardware requirements, software images and versions, and physical connectivity) for the SP data center, cloud, or PoP locations as opposed to one deployment configuration per SD-WAN Vendor.

This standard achieves this goal by:

- Standardization of the data plane connectivity between the USWE implementation and any compliant SD-WAN Vendor Edge implementations, which enables passing Subscriber data between the USWE instance and any compliant SD-WAN Vendor Edge.

- Standardization of the communication between the USWE implementation and the control plane elements of the SD-WAN Vendor's solution, to enable routing information exchange.

- Standardization of the management plane communication between SD-WAN Vendor Manager implementations and the USWE implementation enabling a common management interface to the USWE implementation and management by different vendors.

The solution, USWE, defined within this document, uses standards and protocols primarily from Mplify and IETF. A USWE implementation does not have to be provided by the same vendor that is used elsewhere in the SD-WAN Service.

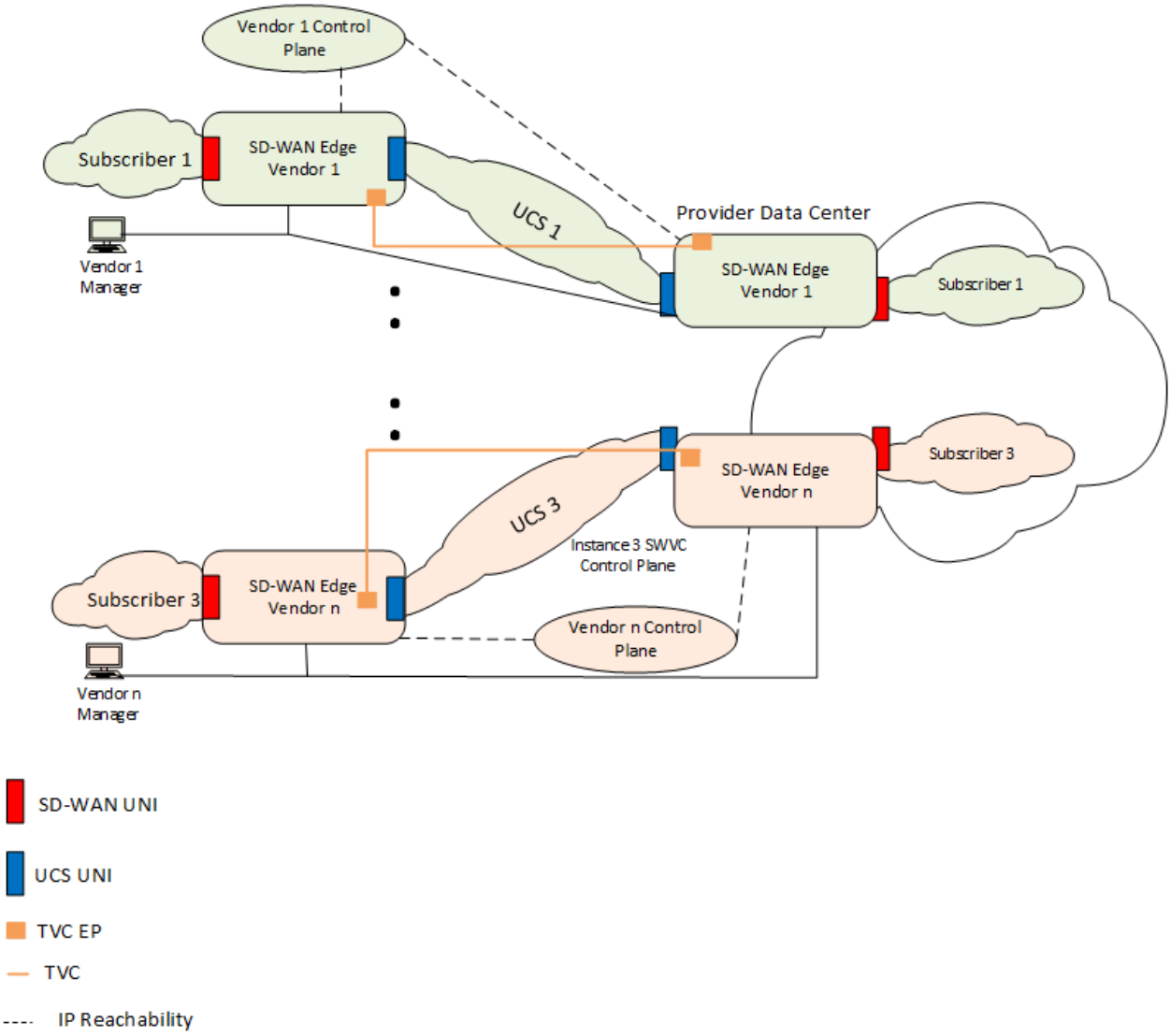


Figure 1 – Current Situation Example

Figure 1 shows the current situation that faces SD-WAN Service Providers. This configuration has challenges associated with it. These challenges include:

- Installation procedure required for each SD-WAN Edge Vendor/software release combination

- May be one time effort per SD-WAN Edge Vendor/software release
- Each SD-WAN Edge Vendor may have different configuration requirements

- If a new SD-WAN Edge Vendor is added at a common location, installation of software is required
  - As the number of SD-WAN Edge Vendors grows, the processes required are exacerbated

To resolve these challenges, the standard has been developed to define the requirements for a Universal SD-WAN Edge. The Universal SD-WAN Edge provides the functionality of an SD-WAN Edge as defined by MEF 70.1 [42]. It supports the MEF 70.1 [42] SD-WAN constructs, including SD-WAN Service, SD-WAN UNI, SD-WAN Virtual Connection (SWVC) End Point, and Underlay Connectivity Service (UCS) components. The distinction is that the Universal SD-WAN Edge provides these functions while interacting with different proprietary SD-WAN Vendor Edges at the other sites within the SD-WAN Service and with the proprietary SD-WAN Vendor Manager. This is shown in Figure 2.

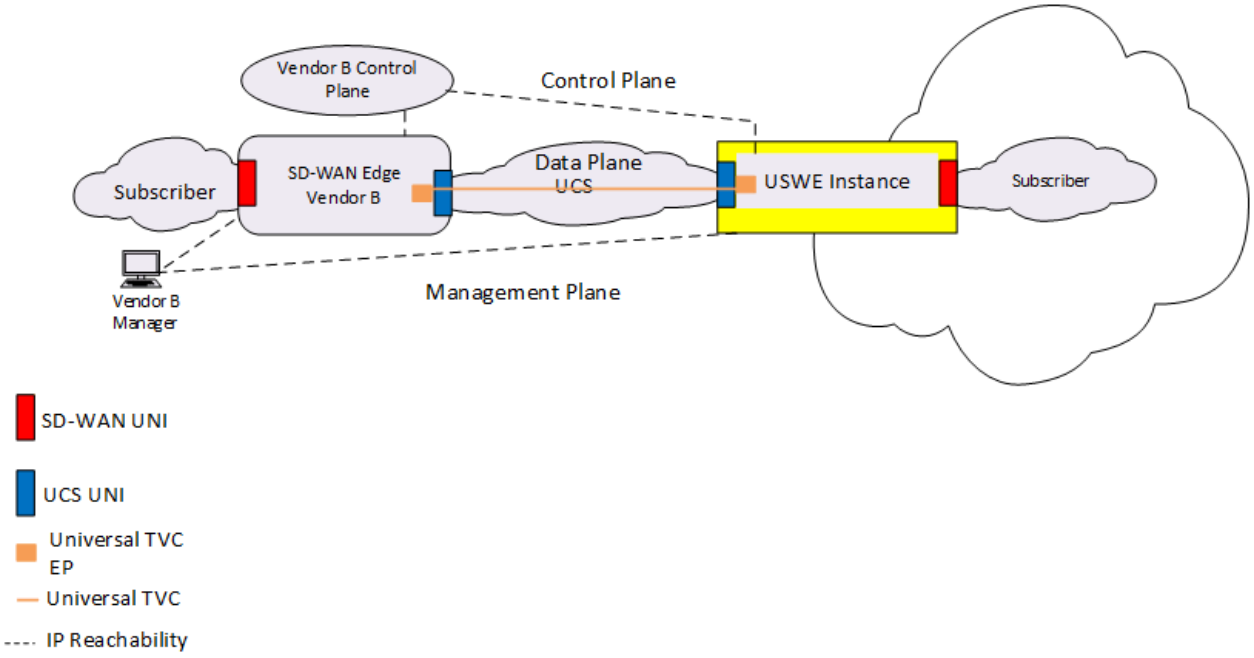


Figure 2 – USWE Implementation with a Single SD-WAN Edge's Vendor Example

In Figure 2, a USWE instance of an implementation produced by Vendor B or a vendor other than Vendor B, is interacting with an SD-WAN Edge and SD-WAN Vendor Manager produced by Vendor B. Support for the subset of features defined within this document is able to be offered to the Subscriber by the SD-WAN Service Provider. This means that SD-WAN Vendor proprietary features are not supported at the USWE instance location. The USWE may be implemented in several ways, including a VNF on a white box, an application on a dedicated hardware platform, or by other methods. How the USWE is implemented is beyond the scope of this document.

A USWE implementation allows providers to equip an SP data center, cloud, or PoP with USWE instances, which can interoperate with different SD-WAN Vendors. The scope of this document is limited to this deployment option. A USWE instance is an instance of a USWE implementation dedicated to a single SD-WAN Service. It replaces the SD-WAN Vendor's SD-WAN Edge in the SP data center, cloud, or PoP. A separate instance of a USWE is used for each SD-WAN Service; this ensures that SD-WAN services are not co-mingled between Subscribers at these locations. Figure 3 reflects the use of the USWE in the data center supporting multiple SD-WAN Edge Vendors. It shows in a yellow box either a single compute instance, separate hardware, or a single monolithic software application that can create multiple distinct instances of a USWE.

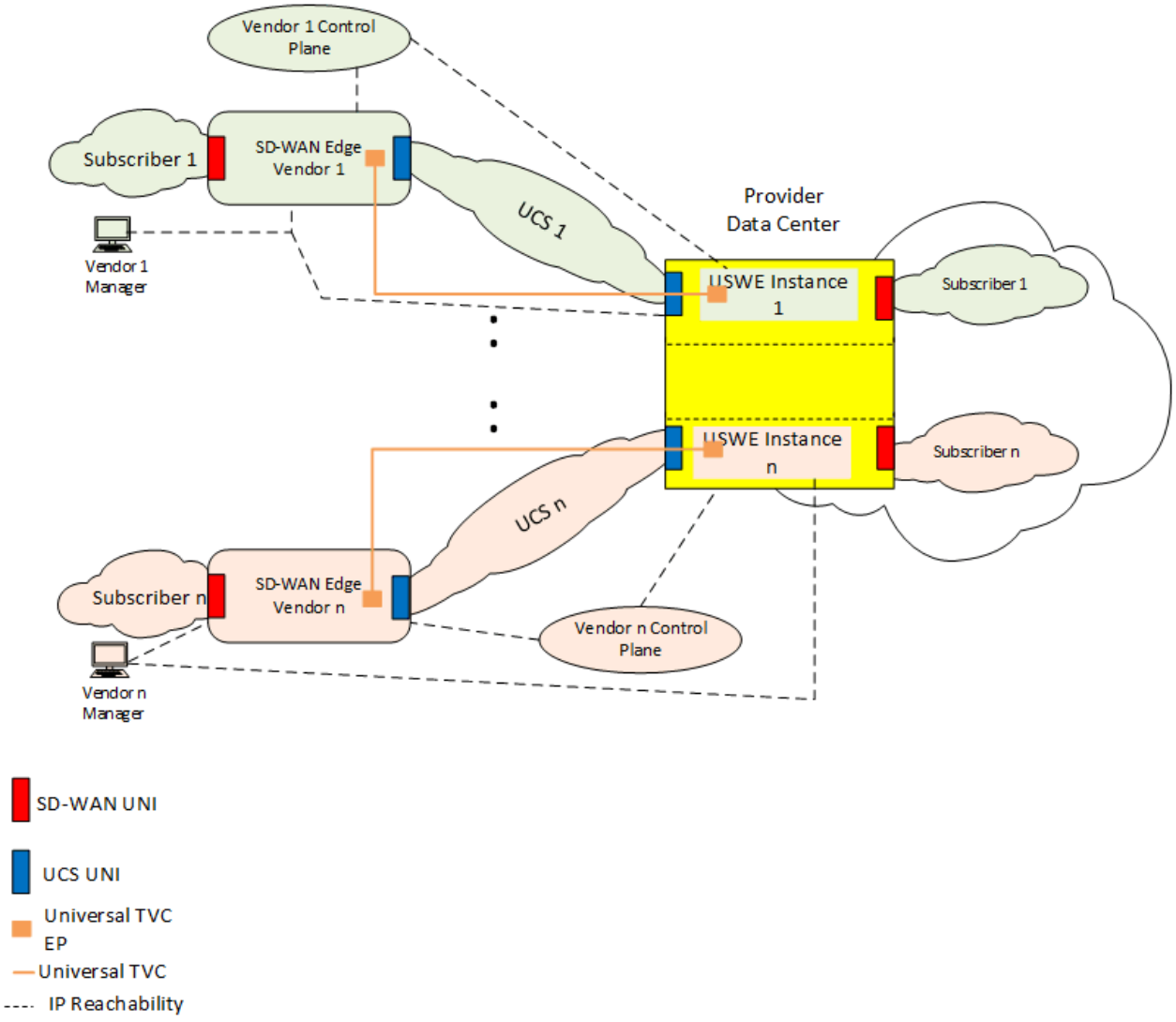


Figure 3 – USWE Deployment with Multiple SD-WAN Vendors Example

As shown in Figure 3, each USWE instance can interact with different SD-WAN Edge Vendors that comply with the requirements in this document. There is a single USWE instance for each SD-WAN Service that has an SD-WAN UNI at a common location. A single USWE Vendor implementation can interact with SD-WAN Vendor 1… n SD-WAN Edges, SD-WAN Vendor Managers, and Universal Control Planes, as shown in the figure. The standard does not require

any changes to the methods used by an SD-WAN Vendor to establish SD-WAN connectivity between an SD-WAN Edge and another SD-WAN Edge from the same Vendor. Only the interaction, within an SD-WAN Service, between a USWE and the SD-WAN Vendor Edges and SD-WAN Vendor Manager is impacted. The SD-WAN Vendor Edges and SD-WAN Vendor Manager must implement the requirements and mechanisms in this standard so as to interoperate with the USWE implementation.

The use case for the USWE, as shown in Figure 2 and Figure 3 connects Subscribers to services that are available at common locations such as Unified Communication as a Service (UCaaS), edge computing, and public cloud access.

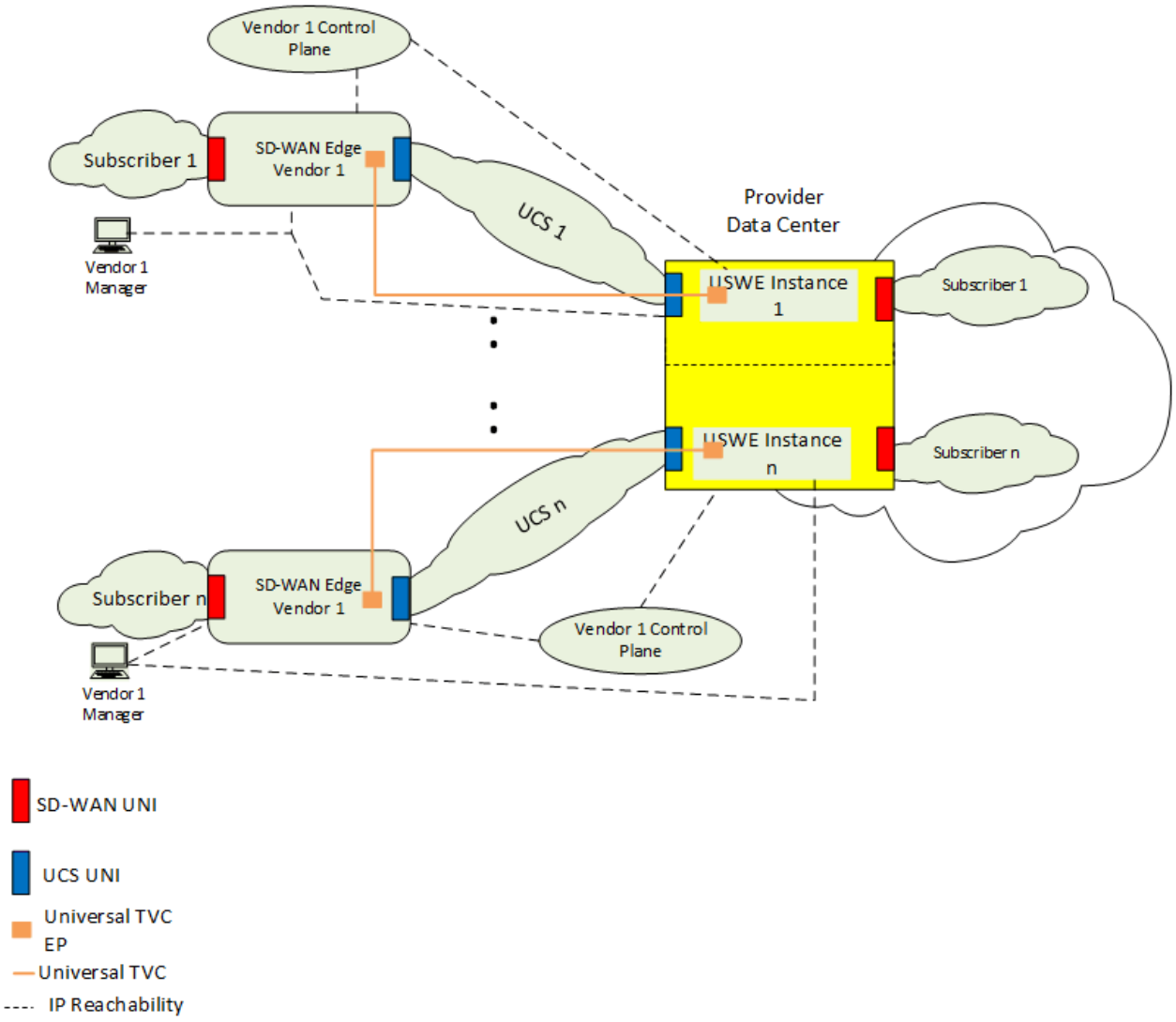


Figure 4 – Example of USWE Deployment with a Single SD-WAN Edge Vendor

Figure 4 shows an example of a single SD-WAN Edge vendor on n different SD-WAN services for n subscribers. This is another possible configuration that is supported by the USWE.

By its placement or pre-staging (installing required hardware and software ahead of an SD-WAN Service order) at the SP data center, cloud, or PoP, the USWE can interoperate with SD-WAN Vendor Edges that comply with this standard by connecting the underlay/Universal Data Plane, Control Plane, and Management Plane to the USWE.

USWE instances can be pre-staged and ready for orders for SD-WAN Services that are enabled at the common location as long as SD-WAN Edges within the SWVC comply with the USWE requirements. While, on the other hand, pre-staging and deploying various SD-WAN Vendor Edges at a location (e.g. a PoP) does not guarantee that a particular Subscriber would have a compatible SD-WAN Service with compatible SD-WAN Vendor Edge (for the same vendor(s)) at its locations. This pre-staging of USWEs can reduce the time it takes to activate services at these common locations.

Deployment of the USWE implementation uses a common configuration rather than a configuration per SD-WAN Edge Vendor. As Subscribers want to add an SD-WAN UNI to connect to services such as UCaaS, edge computing, or public cloud to existing SD-WAN Services, providers can install the USWE instance, make the appropriate connections, and configure the USWE instance including policies to function as a part of the existing SD-WAN Service as long as the SD-WAN Vendor's proprietary features are not required at that location.

New SD-WAN Services using services delivered via a common location can be supported by using a pre-staged USWE instance, making the required connections and configuring the USWE instance which can reduce the time to deliver the services compared to a USWE instance or other SD-WAN Edge that is not pre-staged.

Additional detail on the USWE interaction with an SD-WAN Vendor Edge is provided in section 7.

The document is structured as follows:

- Key Concepts and Overview (section 7)
    - Universal SD-WAN Edge (section 7.1)
    - Universal Control Plane (section7.2)
    - Routing (section 7.3)
    - Universal Data Plane (section 7.4)
    - Universal Management Plane (section 7.5)
    - Compliance with MEF 70.1 (section 7.6)
    - Security Assumptions (section 7.7)
- Universal Control Plane Details and Requirements (section 8)
- Subscriber Routing Details and Requirements (section 9)

- Common TVC Requirements (section 10)
- Universal Data Plane (section 11)
- Universal Management Plane (section 12)
    - Activity flow for USWE (section 12.1)
    - USWE implementation configuration details and requirements (sections 12.2)
    - Fault Monitoring and Detection Details and Requirements (section 12.3)
    - Performance Monitoring Details and Requirements (section 12.4)
    - Enable SD-WAN UNI (section 12.5)
    - Synchronization (section 12.2.2)
    - Notifications (section 12.6)
    - Hardware or Virtual Machine Management (section 12.7)

The key concepts section provides an introduction to the USWE and the associated functions. The subsequent sections define the details and requirements for a USWE implementation, both for an SD-WAN Vendor to interoperate with a USWE implementation, and an SP to deploy the USWE Implementation.

7 The Key Concepts

The key concepts of the Universal SD-WAN Edge (USWE) are described in this section. This includes important terms from MEF 70.1 [42] and a high-level overview of the USWE implementation, the Universal Control Plane, the Universal Data Plane, Subscriber Routing Domain, and the Universal Management Plane. The Universal Control Plane is defined as the set of capabilities needed to enable route learning; route distribution required for the Universal SD-WAN Edge to interoperate with a compliant SD-WAN Vendor Control Plane. The SD-WAN Vendor Control Plane is defined as the control plane that is used by the SD-WAN Vendor implementation, and which connects to the USWE Control Plane Interface. The Universal Data Plane is defined as the set of capabilities needed to enable the forwarding of Subscriber IP traffic between the Universal SD-WAN Edge and SD-WAN Vendor Edges or other Universal SD-WAN Edges. The Universal Management Plane is defined as the set of capabilities needed to configure, monitor, and report management information of the Universal SD-WAN Edge.

7.1 Universal SD-WAN Edge Overview

A USWE implementation is a standardized realization of an SD-WAN Edge. It is an implementation of an SD-WAN Edge that allows it to interoperate with USWE compliant SD-WAN Vendor solutions in a standardized manner. A USWE implementation is deployed at SP data center, cloud, or PoP locations. It is placed on the SD-WAN Service Provider side of the SD-WAN UNI reference point and is based on the SD-WAN Edge functionality defined in MEF 70.1 [41]. In addition to the functionality defined in MEF 70.1 [42], the USWE implementation also supports a set of required functions for the Universal Data Plane, Universal Control Plane, the Subscriber Routing Domain, and Universal Management Plane, as specified in this document. This specification can be used to enable interoperability between the USWE instance and complying SD-WAN Vendor Edges all managed by the same SD-WAN Vendor Manager for a minimum set of SD-WAN attributes and functions (as defined in MEF 70.1 [42]).

A USWE instance is part of the SD-WAN Service Provider Network. A single instance of the USWE implementation is used for each SD-WAN Service. A USWE implementation facilitates access by an SD-WAN Subscriber to resources at a SP data center, PoP, or cloud location over an SD-WAN Service. It is situated between one or more SD-WAN User Network Interfaces (UNIs) on its Subscriber side and Underlay Connectivity Service (UCS) UNIs of one or more UCSs facing the SD-WAN Service. A USWE implementation interoperates with SD-WAN Edges from different compliant SD-WAN Vendors.

A USWE implements functionality, defined in MEF 70.1 [42], that receives ingress IP Packets over the SD-WAN UNI; the USWE implementation determines how they should be handled according to routing information, applicable policies, other service attributes, and information about the UCSs; and if appropriate, forwards them over one of the available UCS UNIs. Similarly, it receives packets over the UCS UNIs and determines how to handle them, including forwarding them over the SD-WAN UNI to the Subscriber Network, if appropriate. Thus, the USWE implements all the data plane functionality of the SD-WAN service that is not provided by a UCS. This includes routing functionality, and the functionality associated with implementing the SWVC End Point and includes the instantiation of any IPsec tunnels.

A USWE implements the functionality needed to connect to the Subscriber Network. It also implements functionality that facilitates connection to the Underlay Connectivity Services.

Since the USWE implementation is required to interoperate with other SD-WAN Vendor implementations, the USWE implementation needs a standardized data plane and control plane to forward packets and to exchange routing information. These also need to be implemented by the other SD-WAN Edges in the service, and by the SD-WAN Vendors' control plane functions. A USWE implementation also requires a standardized management plane so that the USWE can be managed by different SD-WAN Vendor Managers. The SD-WAN Vendor Managers also need to implement this standardized management plane.

Note that the way that a USWE is implemented is not constrained by this document; any implementation is acceptable so long as the externally visible behavior is consistent with the definition and requirements in this document.

Figure 2 shows a specific example of a USWE implementation (other implementations are possible). The example in Figure 2 shows a single USWE instance connected to a single Subscriber. The figure includes the standardized Universal Management Plane, the Universal Control Plane, and the Universal Data Plane.

While it is possible to have a single USWE instance at a data center or cloud access location, the SD-WAN SP is more likely to support multiple USWE instances at that location.

Figure 3 shows an example of multiple USWE instances connected to different SD-WAN Vendor SD-WAN Edges. A number of USWE instances are shown in the yellow box, one per Subscriber. USWE instance 1 supports Subscriber 1 and USWE instance n supports Subscriber n.

Each USWE instance has the following:

- One or more SD-WAN UNIs
- One or more UCS UNIs that connect the USWE instance to one or more SD-WAN Edges within the SD-WAN Service
- One or more Universal Tunnel Virtual Connections (UTVC)
    - Uses standard protocols to support the UTVC implementation
- One or more Control Tunnel Virtual Connections (CTVC)
    - Uses standard protocols to support the CTVC implementation

Each USWE Instance uses the standardized Universal Management, Control, and Data Planes to interconnect to other SD-WAN Vendors. A Universal Tunnel Virtual Connection (UTVC) is defined within this document as a special implementation of the SD-WAN TVC (MEF 70.1[42]) that uses the standard protocols to support the USWE implementation.

The Universal Management Plane is used to connect the USWE instance to the SD-WAN Vendor Manager and allows the management of the USWE instance by the SD-WAN Vendor Manager. The Universal Management Plane provides the following:

- Allows the SD-WAN Vendor Manager to configure the USWE instance with the required attributes for the:
    - Universal Control Plane
    - Universal Data Plane
    - Attributes not included in MEF 70.1 [42]
- Universal Management Plane allows the SD-WAN Vendor Manager to configure values of any attributes associated with the SD-WAN Service
    - UNIs
    - UCSs
    - TVCs
    - Policies
    - Zones
    - Application Flows

Each USWE instance allows routing information to be exchanged between the USWE instance and SD-WAN Vendor control plane.

The Universal Control Plane is defined within this document to provide the following:

- The necessary requirements and functionalities based on the industry-standard protocols that are needed to enable
    - Route learning
    - Route distribution

For interoperability, the SD-WAN Vendor's control plane must also comply with the Universal Control Plane requirements specified in this document.

While MEF 70.1 [42] defines the SD-WAN UNI Routing Protocol Service Attribute, this document expands on this to require support for the Subscriber Routing Domain in the USWE implementation and defines requirements related to the subscriber routing. Subscriber Network routing information such as reachable addresses at a given SD-WAN UNI is obtained by the USWE based on the value of the SD-WAN UNI Routing Protocol Service Attribute.

Note: In this standard, the value of the SD-WAN UNI Routing Protocols Service Attribute [MEF 70.1] is mandated to be a non-empty list with only two possible values *BGP* or *Static.*

A USWE implementation supports a Universal Data Plane that connects one or more USWE instances to one or more vendor-specific SD-WAN Edges within the SD-WAN Service. The interconnection of USWE instances to each other via the Universal Data Plane is beyond the scope of this document. The Universal Data Plane requirements and functionalities are based on industry standards and are described in this document. The Universal Data Plane is configured on the USWE instance and associated with specific UCS UNIs assigned to the specific USWE instance.

The ability to monitor the USWE instance for faults and to send Fault Notifications to the Service Provider and possibly the Subscriber is described in this document. A Fault Notification is defined as a notification that is sent by the USWE instance with a specific format to indicate a failure. Faults of the USWE instance and associated SD-WAN UNIs, UCS UNIs, and UCSs are detected by the USWE instance and reported via the Universal Management Plane.

Monitoring the performance of TVCs and Application Flows is described in MEF 105 [43]. A USWE implementation supports the functionality defined in MEF 105 [43]. This standard defines the tool used to perform measurements between the USWE instance and SD-WAN Vendor SD-WAN Edges.

7.2 Universal Control Plane

The Universal Control Plane is instantiated for each USWE instance. Each USWE instance has Universal Control Plane functionality that communicates with the corresponding Universal Control Plane functionality at the SD-WAN Vendor Control Plane. This connection is carried by the Control Tunnel Virtual Connection. The Control Tunnel Virtual Connection connects the Control Plane Interface to the SD-WAN Vendor Control Plane. The Control Plane Interface is defined as the network interface that enables the USWE instance to exchange the routing information with the SD-WAN Vendor Control Plane. The Control Plane Interface enables the exchange of the SD-WAN routing and control information between the USWE instance and the SD-WAN Vendor Control Plane.

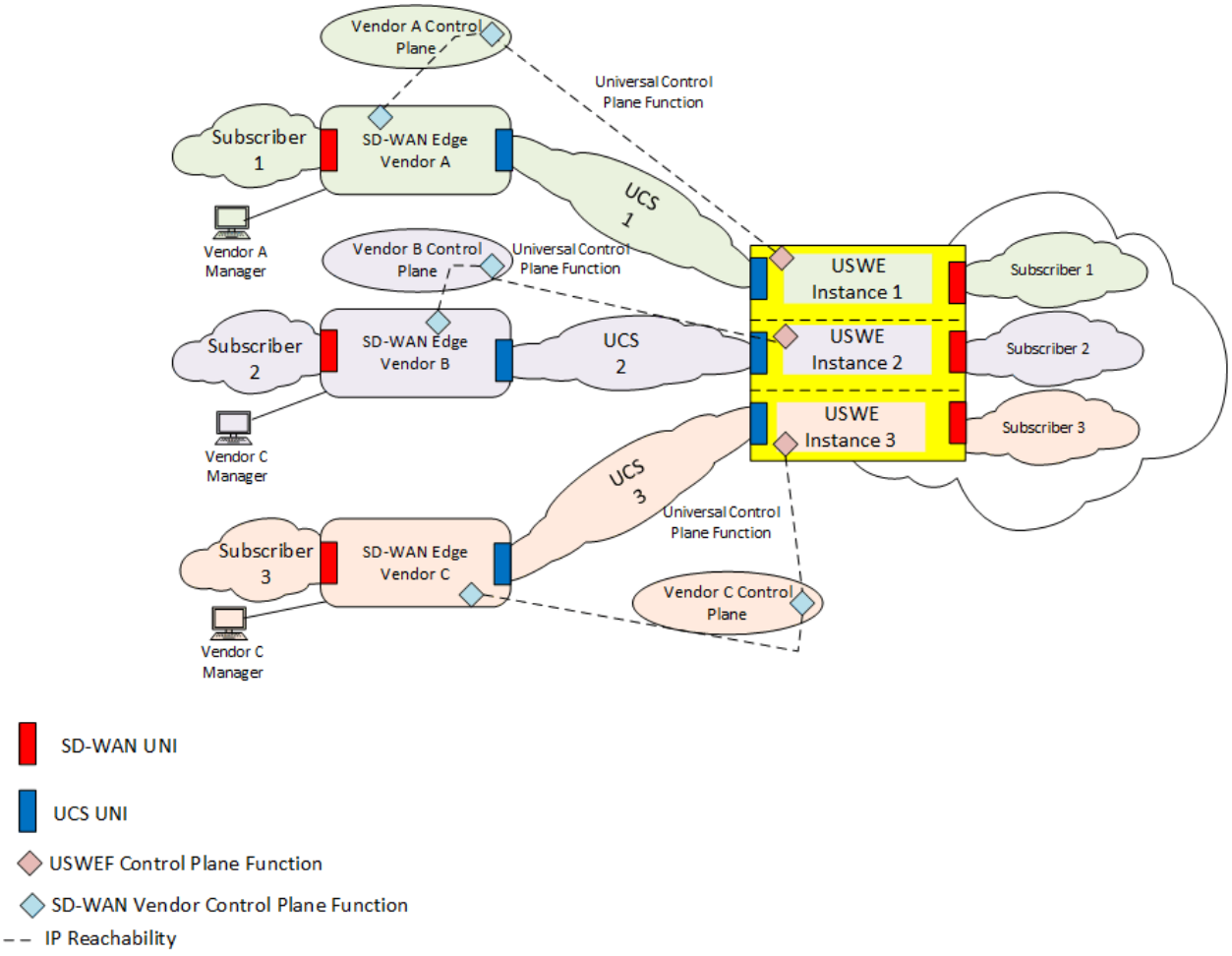


Figure 5 – Example of Universal Control Plane

Figure 5 shows three USWE instances each connecting to an SD-WAN Vendor Control Plane. The Universal Control Plane defined within this document allows the exchange of routing information (e.g., adjacencies, route costs, and attributes) and other control information (e.g., key management or other control attributes).

Note: The SD-WAN Vendor Control Plane is shown external to any SD-WAN Edge since the control plane is proprietary and its location may be different for different SD-WAN Edge Vendor implementations.

The Universal Control Plane uses IPsec tunnels and BGP as defined in IETF RFC 4271 [16].

7.3 Routing

A USWE implements Routing Domains so that routing information can be passed within a routing domain and between different routing domains, for underlay, overlay, and Subscriber. A Routing Domain is defined as a domain (UCS, Subscriber, or Service) that defines the domain within which IP addresses must be uniquely assigned, and packets destined for those IP address are consistently routed. Since SD-WAN is an overlay technology, there exists three types of routing domains that need to be considered with respect to a USWE:

- Subscriber Routing Domain
- SD-WAN Service Routing Domain
- UCS Routing Domain

Note: each routing domain can use IP addresses that overlap with IP addresses in anther routing domain and must be treated independently. This is further explained in section 8.

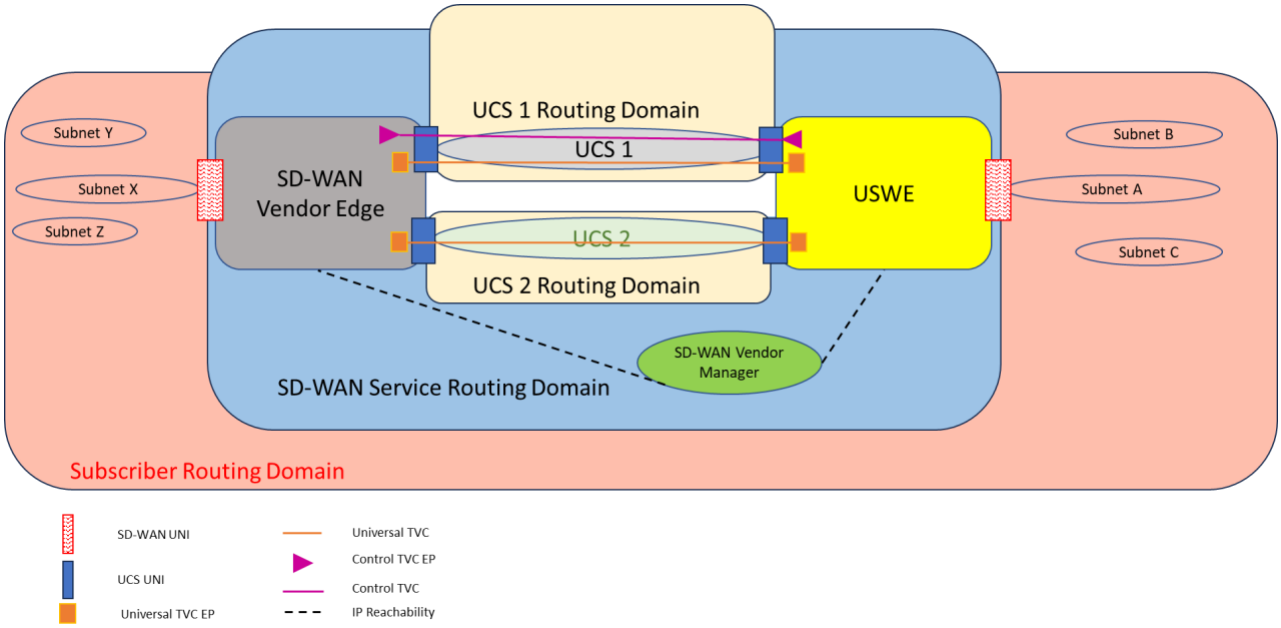


Figure 6 – Example of Routing Domains

The particulars about each routing domain displayed in Figure 6, is described in more detail in the following sections.

7.3.1 Subscriber Routing Domain

The Subscriber Routing Domain contains all the information about how to route between the Subscriber Network IP Prefixes associated with a given SD-WAN Service. The Subscriber Routing Domain is defined as the Routing Domain containing and connecting the SD-WAN UNIs and the Subscriber's devices. The routing information includes the Subscriber Network IP Prefixes reachable via a USWE instance, and the Subscriber Network IP Prefixes reachable via Vendor SD-WAN Edges within a given SD-WAN Service, including the IP addresses for the SD-WAN UNIs.

In the examples shown in Figure 6, the Subscriber routing information contains entries on how to route from Subscriber IP Subnets A, B, and C associated with USWE to Subscriber IP Subnet X, Y, and Z associated with SD-WAN Vendor Edge. Subscriber subnet A is directly connected to the USWE, and the Subscriber advertises subnets B and C to the USWE via Subscriber Routing. The USWE advertises the directly connected subnet A and the Subscriber subnets B and C to the SD-WAN Vendor Control Plane. The Subscriber Routing domain would have routing entries for IP

prefixes that point to the SD-WAN Service, for IP prefixes reachable via the SD-WAN Service, entries for the directly connected IP prefixes at the SD-WAN UNIs, and entries for the IP prefixes reachable via the Subscriber routing. For the directly connected IP prefixes, the next hop would be the SD-WAN UNI interface on the USWE (for any Subscriber subnet associated with the USWE instance). For the IP prefixes reachable via the SD-WAN Service, the next hop would be an SD-WAN Vendor Edge IP address. For the IP prefixes reachable via the Subscriber Routing, the next hop would be an IP address in the directly connected IP prefix (in the case of Static routing) or an IP address in the Subscriber network (in the case of BGP routing). This information is stored in a VRF assigned to the Subscriber with the appropriate route target and MPLS label.

7.3.2 SD-WAN Service Routing Domain

The SD-WAN Service Routing Domain, defined as the Routing Domain containing and connecting the SD-WAN Edges and other infrastructure used to provide an SD-WAN Service, contains all the information about how to route between the SD-WAN Edges associated with a given SD-WAN Service. This would include the SD-WAN Edges (both USWE and Vendor Proprietary), Control Tunnel Virtual Connections (CTVCs), as defined in section 8 and UTVCs, as defined in section 11, associated with the SD-WAN Service.

In section 8, the SD-WAN Service Routing Domain information contains entries on how to route from the USWE to other SD-WAN Edges and the Vendor Control Plane. This would include the entries for the UTVCs from USWE to SD-WAN Vendor Edge, the routing entries for all the other Vendor Edges in the SD-WAN Service (each of which has its own IP Address as described in section 12), and the entry for the CTVC from USWE to the SD-WAN Vendor Edge. This information is stored in an SD-WAN Service VRF with the appropriate route target and MPLS label.

Additionally, since the SD-WAN service supports the concept of Internet Breakout, the default route for Internet Breakout needs to be handled differently than a default route learned via the Subscriber network. Therefore, any default route learned from a UCS (either through static routes or a routing protocol) is stored in its own VRF assigned to the SD-WAN Service with the appropriate route target and MPLS label. This route target and MPLS label is different than that which is assigned to the SD-WAN Service.

7.3.3 UCS Routing Domain

The UCS Routing Domain, defined as the information about how to route between the End Points associated with a given UCS, contains the information about how to route to UCS End Points associated with a given UCS within this domain. In other words, the reachable IP addresses in each UCS Routing Domain are the IP addresses of the UCS UNIs for that UCS.

In the example in Figure 6, the UCS routing information contains entries on how to route from USWE to the SD-WAN Vendor Edge on UCS 1. A different UCS Routing Domain contains the routing information on how USWE can reach the SD-WAN Vendor Edge on UCS 2. Each UCS Routing Domain is stored in its own VRF with the appropriate route distinguisher tag.

7.4 Universal Data Plane

The Universal Data Plane is the collection of UTVCs over one or more UCSs, and the functionality needed to forward traffic across the UTVCs between the USWE and the SD-WAN Vendor Edges. UTVCs, which are configured as described in this document, are TVCs that are defined within this document so that they are interoperable at the UTVC End Points. UTVC End Points are defined as the logical construct which terminates a UTVC by performing any encapsulation/encryption and decapsulation/decryption necessary to forward IP Packets over the Universal Tunnel Virtual Connection. As UTVCs are combined in a single SD-WAN Service Universal Data Plane, passing data between the USWE and SD-WAN Vendor Edges is possible. The Universal Data Plane provides forwarding for all IP Packets including but not limited to Internet-Breakout.

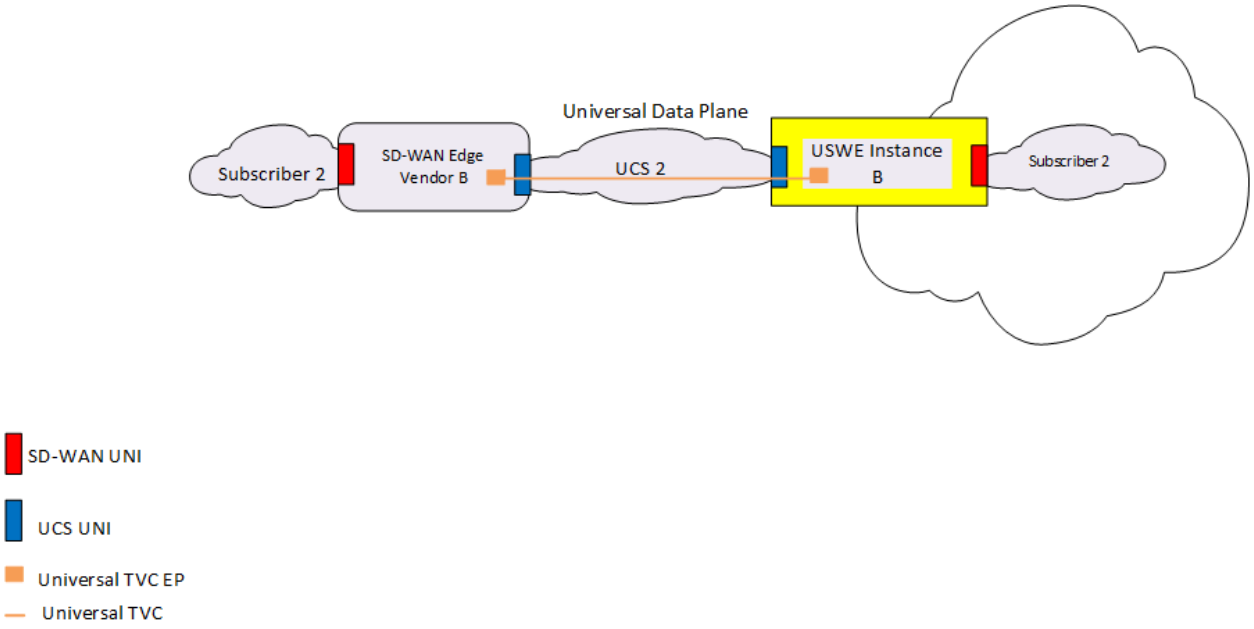


Figure 7 – Universal Data Plane Single SD-WAN Vendor Edge Example

Figure 7 shows an example of the Universal Data Plane between the USWE instance and an SD-WAN Vendor SD-WAN Edge. A UTVC, as defined in section 11, connects the USWE instance with SD-WAN Edge from Vendor B over UCS 2.

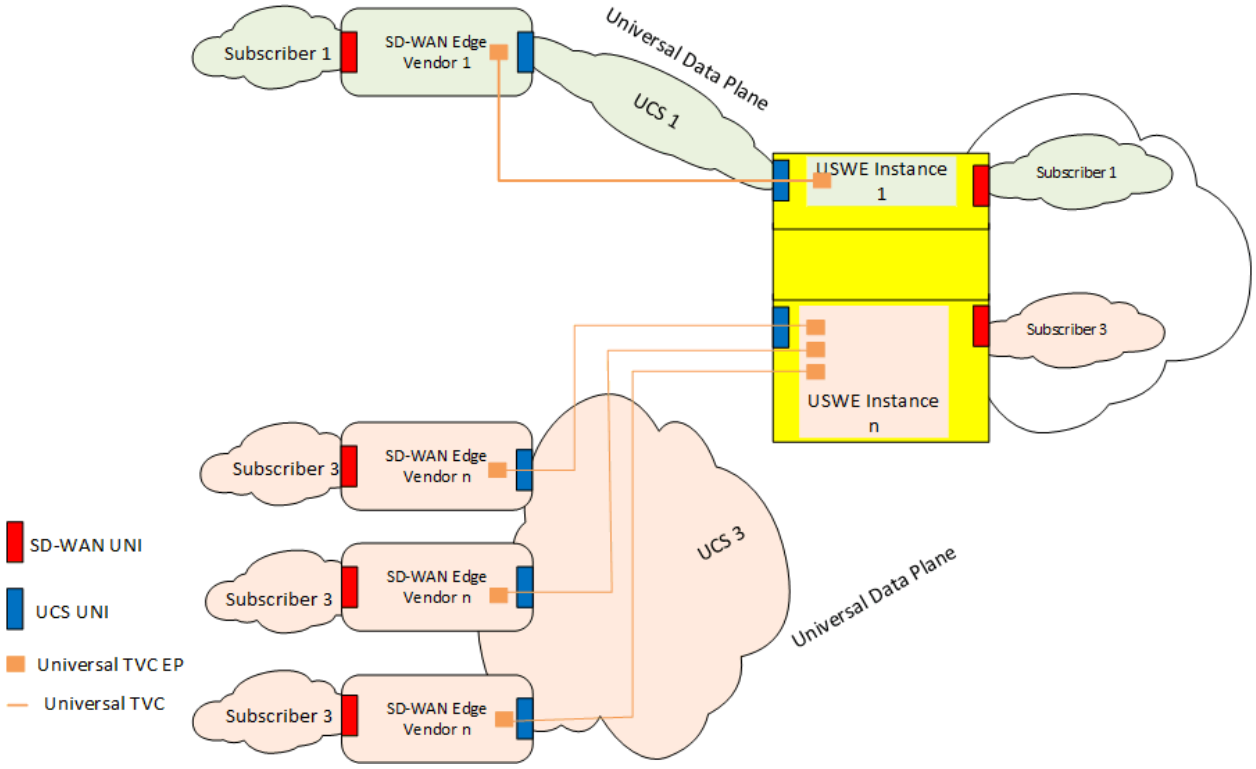


Figure 8 – Universal Data Plane with Multiple SD-WAN Vendors Example

Figure 8 shows the Universal Data Plane connections for multiple sets of USWE instances and SD-WAN Edges within different Subscriber's SD-WAN Services. The Universal Data Plane for each SD-WAN Service connects the USWE instance to the appropriate SD-WAN Edge for each Subscriber over the appropriate UCS.

The Universal Data Plane specified within this document uses existing standards and protocols to avoid any dependency on the development of new protocols. The standards and protocols are detailed in section 11. The Universal Data Plane can include input/output processing, header processing and manipulation, quality of service, queueing, security, etc.

7.5 Universal Management Plane

The Universal Management Plane allows the SD-WAN Vendor Manager to manage the USWE instance. It is used for configuration of the USWE instance and maintenance of the USWE instance. The Universal Management Plane section of this document (section 12) includes a description of the necessary configuration steps that need to be executed to configure the USWE instance the information that need to be exchanged between the SD-WAN Vendor Manager and the USWE instance over the Universal Management Plane. A standardized API is seen as desirable. Having a standard API is expected to reduce the development efforts of SD-WAN SPs who are deploying USWE instances within their network. API development is outside the scope of this document.

The description of the Universal Management Plane in this document focuses on the information passed between the SD-WAN Vendor Manager, a virtual function that can be implemented in

several different ways that are beyond the scope of this document, and the USWE instance. The SD-WAN Vendor Manager communicates with the USWE instance through its standard-based external interface and using the yet to be defined API.

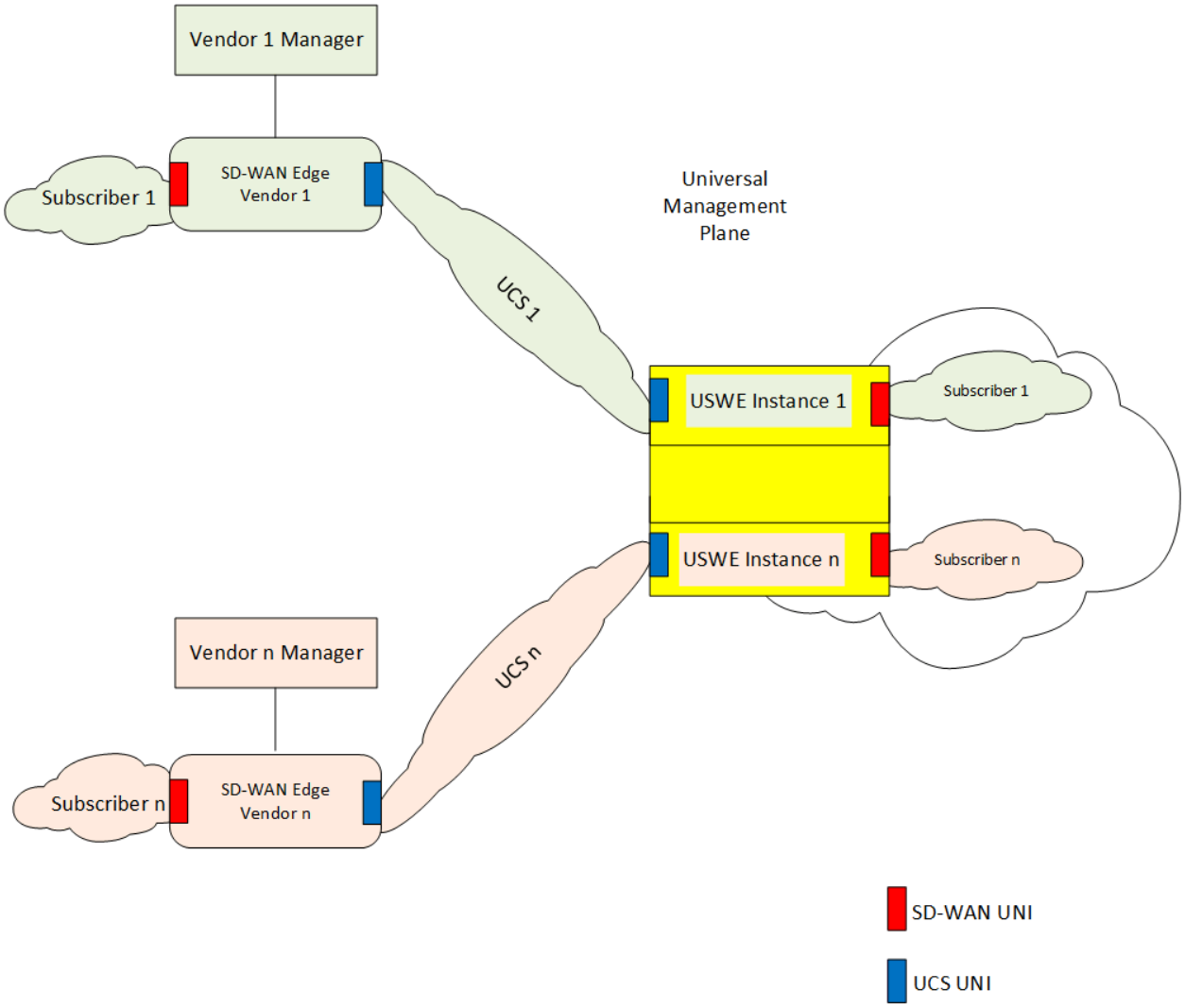


Figure 9 – SD-WAN Edge Vendor Manager Managing USWE Example

Figure 9 illustrates an implementation using each SD-WAN Vendor Manager to manage the USWE instance connected to the SD-WAN Service. In this example, there are three different SD-WAN Vendor Managers, each implementing the SD-WAN Vendor Manager functionality. Each communicates only with the USWE instance that is a part of an SD-WAN Service that they are managing. An implementation requires no additional links between the managers since the scope of management is only a specific USWE instance.

Some method outside the SD-WAN Vendor Manager is likely required to configure the connectivity between a USWE instance and the corresponding SD-WAN Vendor Manager before the USWE instance can be fully configured. How this is done is beyond the scope of this document. This connectivity is a pre-requisite to configuring and using the USWE to carry Subscriber IP Packets.

The Universal Management Plane allows an SD-WAN Vendor Manager to configure parameters on a USWE instance, including the Universal Control Plane attributes, Universal Data Plane attributes, a subset of the SD-WAN UNI, UCS UNI, and UCS attributes, and the Policies required at the USWE instance.

7.5.1 Fault Monitoring

Fault Monitoring is the function that detects failures of interfaces, operations, or other functions. The ability of the USWE implementation to detect fault conditions is defined in section 12.3. This includes faults with the operation of the USWE instance and associated UNIs and UCSs. To detect fault conditions, the USWE implementation is required to have some method of monitoring for faults active at all times. Examples of faults that the USWE implementation might detect are the USWE instance stops forwarding IP packets or an unrecoverable software error occurs that impacts the operation of the USWE instance. This document does not define what is used to perform fault monitoring or how fault detection is implemented.

A USWE implementation also monitors UNIs and UCSs for failures like a loss of incoming signal. This includes the SD-WAN UNIs, UCS UNIs, and all UCSs. Depending on the UCS technology, it may be possible to monitor for other types of failures.

Fault monitoring is configured using the Universal Management Plane. Once a fault is detected, a fault notification is sent as described in section 12.6.

7.5.2 Performance Monitoring

The monitoring of the performance of the components of the SD-WAN Service is a part of the requirements for a USWE implementation. MEF 105 [43] defines Performance Monitoring for SD-WAN. The requirements on USWE implementations and SD-WAN Vendor Control Planes in this document support the functionality in MEF 105. This includes monitoring all UTVCs and selected Application Flows. A USWE instance performs measurements and calculations and passes the metric values to the SD-WAN Vendor Manager.

Performance Monitoring configuration is described as a part of the Universal Data Plane in section 11.4, and the reporting of Performance Metrics is described in section 12.4.

7.5.3 Fault and Performance Notification

The notification of fault conditions from the Universal SD-WAN Edge to the SD-WAN Edge Manager occurs if subscribed to. Fault reporting uses alarms to indicate that a fault has occurred. The type and severity of a fault are included in the alarm notification message.

7.6 Compliance with MEF 70.1

This document relies on MEF 70.1 [42] to define terms and functions used to specify the requirements on a USWE implementation, such as SD-WAN UNIs, UCS UNIs, UCSs, TVCs, and Application Flows. The intention is for the USWE implementation to comply with all required features and functions of an SD-WAN Edge in MEF 70.1[42].

[R1] A USWE implementation **MUST** comply with the SD-WAN Edge definition contained in MEF 70.1 section 7.13.

This means that a USWE implementation has to implement the behavior of an SD-WAN Edge defined in MEF 70.1 [42], including, for example, the behavior of an SWVC End Point, the behavior of interacting with a UCS over a UCS UNI, and the behavior of implementing one end of a TVC.

7.7 Security Assumptions

It is assumed that the USWE instances are securely instantiated in the SPs network for example, using the mechanisms defined in RFC 8572 [33]. This document does not include any requirements or informative text that addresses how this is accomplished. It is also assumed that any Subscribers that are connected to a USWE instance are verified to be the correct Subscribers prior to activating the SD-WAN UNI.

8 Universal Control Plane

The Universal Control Plane, which extends from the USWE to the SD-WAN Vendor Control Plane enables the USWE Control Plane Interface (CPI) to communicate with the SD-WAN Vendor Control Plane. This communication contains routing information. In order for information to be exchanged between the USWE instance and the SD-WAN Vendor Control Plane, the CPI needs to be assigned an IPv4 address, an IPv6 address, or both. Implementations could use either a virtual interface with a unique IPv4 or IPv6 address or a CTVC End Point interface.

[R2] A CPI **MUST** be either:

- A CTVC End Point interface or
- A virtual interface assigned either an IPv4 or an IPv6 address or both.

[R3] Any IP Address (IPv4, IPv6, or both) assigned to the CPI **MUST** be unique within a given SD-WAN Service Routing Domain.

8.1 Universal SD-WAN Edge Control Plane Interface

The USWE Control Plane Interface is the network interface that enables the Universal SD-WAN Edge instance to exchange the routing information and other control information with the SD-WAN Vendor Control Plane. Examples of a Control Plane Interface are a CTVC End Point (if there is only one CTVC) or a loopback interface.

8.2 Control Tunnel Virtual Connection

The communication between the USWE CPI and the SD-WAN Vendor Control Plane traverses one or more Control Tunnel Virtual Connections. A Control Tunnel Virtual Connection (CTVC) is a point-to-point forwarding relationship for the Control Plane traffic between the USWE instance and an SD-WAN Edge or another device connected to the same UCS as the USWE and terminating the tunnel. It associates:

- two UCS End Points in a single Underlay Connectivity Service that is not an Internet Access Service, or
- a UCS End Point in each of two Internet Access Underlay Connectivity Services (such as defined in MEF 69.1 [41])

[R4] For a Control Plane traffic to be forwarded from the USWE instance to the SD-WAN Vendor Control Plane, there **MUST** be at least one CTVC between the USWE instance and another device associated with the SD-WAN Service (e.g. SD-WAN Edge or SD-WAN Vendor Control Plane).

This connection needs to be encrypted and encapsulated such that accidental or malicious exposure can be prevented. The CTVC configuration is based on the UTVC as defined in section 11.

[R5] The Control Tunnel Virtual Connection **MUST** comply with all the requirements of a TVC (see section 10).

[R6] A CTVC **MUST** be encrypted as described in section 10.3.

8.2.1 Control Tunnel Virtual Connection End Point

The Control Tunnel Virtual Connection contains two Control Tunnel Virtual Connection End Points (CTVC End Points). One CTVC End Point is located within the USWE instance, and one is located in the other device which is terminating the CTVC. The CTVC End Point is the logical construct which terminates the CTVC by performing any encapsulation/encryption and decapsulation/decryption necessary to forward control plane IP Packets over a CTVC.

[R7] A given CTVC End Point **MUST** be assigned an IPv4 address, an IPv6 address, or both.

[R8] Any IP Address assigned to a CTVC End Point **MUST** be unique within the SD-WAN Service Routing Domain.

This document does not dictate what type of UCS (e.g., Public or Private) is used to carry the CTVC. Which UCS is used is chosen by the association of the CTVC End Point with the UCS End Point.

For the USWE instance to connect to the other SD-WAN Edges within the SD-WAN Service for exchanging Control Plane information, at least one device must have the logical construct and associated functions that behave as a CTVC End Point. This document does not mandate that the actual construct of CTVC End Point be adopted by the SD-WAN Edge vendor.

For the purposes of this document, the logical construct and associated functions that are performing the functions of the CTVC End Point, in the device terminating the CTVC, will be considered CTVC EPs and these logical constructs must abide by all the requirements in this document.

8.3 CPI Internal Border Gateway Protocol

This communication between a USWE CPI and the SD-WAN Vendor Control Plane uses one or more iBGP sessions as described later in this section.

Since it is critical that the routing and control information be exchanged between the SD-WAN Vendor Control Plane and the USWE instance, many solutions provide for redundancy in the Control Plane.

If redundancy is required in the control plane, the USWE CPI connects to the SD-WAN Vendor Control Plane via two or more iBGP sessions.

[R9] A USWE implementation and the SD-WAN Vendor Control Plane **MUST** support BGP communities as per RFC 1997 [4] .

[R10] A USWE implementation and the SD-WAN Vendor Control Plane **MUST** support BGP extended communities as per RFC 4360 [21].

[R11] A USWE implementation and the SD-WAN Vendor Control Plane **MUST** support securing the iBGP session by using the TCP MD5 signature option as defined by RFC 2385 [7].

[R12] All Universal Control Plane iBGP sessions **MUST** be secured using the TCP MD5.

The need for TCP MD5 is due to the fact that the Universal Control Plane iBGP session may extend beyond the CTVC.

The exact usage of BGP communities and BGP extended communities in the SD-WAN Vendor Control Plane will be at the discretion of the Service Provider.

[R13] A USWE implementation and the SD-WAN Vendor Control Plane **MUST** support four-octet autonomous system numbers per RFC 4893 [26].

Since SD-WAN is an overlay connectivity service, the need to support multiple Virtual Private Networks (VPNs) is a requirement. RFC 4364 defines how VPNs are utilized by Service Providers to create overlay networks.

[R14] A USWE implementation and the SD-WAN Vendor Control Plane **MUST** comply with the requirements of RFC 4364 [22].

Since SD-WAN has multiple Routing Domains (e.g., Subscriber Routing Domain, SD-WAN Service Routing Domain, and UCS Routing Domain), it is important that routes are specifically tagged with unique Route Distinguishers. For example, this enables the USWE implementation to differentiate between a route associated with a 10.1.1.0/24 prefix in the Subscriber Routing Domain from a route associated with 10.1.1.0/24 prefix in the SD-WAN Service Routing Domain. See section 11.1 for more details on how this is addressed.

[R15] The Administrator subfield value of the Route Distinguisher as defined in RFC 4364 [22] for the SD-WAN Service Routing Domain **MUST** be unique for a given Service Provider.

[R16] The Administrator subfield value of the Route Distinguisher for the Subscriber Routing Domain **MUST** be unique for a given Service Provider.

[R17] The Route Target values associated with routes for the SD-WAN Service Routing Domain and the Subscriber Routing Domain **MUST** be different from each other.

Note: support for multiple Subscriber Routing Domains with different Route Targets or MPLS labels is out of the scope of this document.

[R18] The Subscriber Routing Domain **MUST** be associated with a unique MPLS label within the Service Provider Network.

[R19] The SD-WAN Service Routing Domain **MUST** be associated with a unique MPLS label within the Service Provider Network.

Note: for more details on the use of MPLS labels please see section 11.2.

Additionally, SD-WAN supports Internet Breakout. Since the routes to other devices on the Internet, which may include a default route or other routes, might be both in the Subscriber Routing Domain and the UCS Routing Domain, a separate VRF needs to be created to distinguish between the two distinct sets of routes. This also requires a separate MPLS label to be added when there is no local Internet Breakout, so the SD-WAN Data Plane can distinguish between packets that are destined to a SD-WAN UNI via the appropriate routes or via UCS Internet Breakout.

[R20] Internet Breakout **MUST** be associated with a unique MPLS label within the Service Provider Network.

[R21] The SD-WAN Vendor control plane **MUST** store the IPv4 routes learned dynamically or statically from a UCS that supports Internet Breakout or IPv4 routes for Internet Breakout learned from the SD-WAN Vendor Edges in a different VRF within the SD-WAN Service Routing Domain and advertise these routes as VPNv4.

[R22] The USWE **MUST** store the IPv4 routes learned dynamically or statically from a UCS that supports Internet Breakout or IPv4 routes for Internet Breakout learned from the SD-WAN Vendor control plane in a different VRF within the SD-WAN Service Routing Domain.

[R23] The SD-WAN Vendor control plane **MUST** store the IPv6 routes learned dynamically or statically from a UCS that supports Internet Breakout or IPv6 routes for Internet Breakout learned from the SD-WAN Vendor Edges in a different VRF within the SD-WAN Service Routing Domain and advertise these routes as VPNv6.

[R24] The USWE **MUST** store the IPv6 routes learned dynamically or statically from a UCS that supports Internet Breakout or IPv6 routes for Internet Breakout learned from the SD-WAN Vendor control plane in a different VRF within the SD-WAN Service Routing Domain.

[R25] The USWE **MUST** import the IPv4 routes associated with the UNIs to the VRF associated with a UCS that supports Internet Breakout.

[R26] The USWE **MUST** import the IPv6 routes associated with the UNIs to the VRF associated with a UCS that supports Internet Breakout.

Requirements [R20], [R25], and [R26] indicate that in order for the SWVC to support Internet breakout, the IPv4 and IPv6 routes learned for Internet Breakout need to be uniquely encapsulated and stored in a separate VRF within the SD-WAN Service Routing Domain.

[R27] A USWE instance **MUST** advertise all IPv4 routes associated with the addresses of the interfaces associated with the CPI, the CTVC End Point addresses, and UTVC End Point addresses to the SD-WAN Vendor Control

Plane with the appropriate SD-WAN Service Routing Domain Route Target value and the appropriate MPLS label and advertised as VPNv4.

This advertisement would include all the IPv4 Addresses for the TVCs (both UTVCs and CTVC) as well as the CPI IPv4 addresses associated with the USWE instance. This advertisement would not include UNI IPv4 addresses, or any IPv4 prefixes in the Subscriber Routing Domain, nor would this advertisement include any UCS routing information. Since the USWE instance is initiating these advertisements, the next hop address for these routes is the USWE CPI IP address.

[R28] A USWE instance **MUST** advertise all IPv6 routes associated with the addresses of the interfaces associated with the CPI, the CTVC End Point addresses, and UTVC End Point addresses to the SD-WAN Vendor Control Plane with the appropriate SD-WAN Service Routing Domain Route Target value and the appropriate MPLS label and advertised as VPNv6.

This advertisement would include all the IPv6 Addresses for the TVCs (both UTVC and CTVC) as well as the CPI IPv6 addresses associated with the USWE instance. This advertisement would not include UNI IPv6 addresses, or any IPv6 prefixes learned in the Subscriber Routing Domain, nor would this advertisement include any UCS routing information. Since the USWE instance is initiating these advertisements, the next hop address for these routes is the USWE CPI IP address.

[R29] A USWE instance **MUST** advertise all IPv4 routes associated with the Subscriber Routing Domain to the SD-WAN Vendor Control Plane with the appropriate Subscriber Routing Domain Route Target value and the appropriate MPLS label and advertised as VPNv4.

This advertisement would include all the IPv4 Prefixes learned (either dynamically or statically) from the Subscriber via an SD-WAN UNI on a given USWE instance and all of the IPv4 addresses assigned to the given USWE instance SD-WAN UNIs. This advertisement would not include any IPv4 Addresses associated with the USWE UTVCs, CTVCs, or CPI IPs or any UCS routing information. Since the USWE instance is initiating these advertisements, the next hop address for these routes is the USWE CPI IP address.

[R30] A USWE instance **MUST** advertise all IPv6 routes associated with the Subscriber Routing Domain to the SD-WAN Vendor Control Plane with the appropriate Subscriber Routing Domain Route Target value and the appropriate MPLS label and advertised as VPNv6.

This advertisement would include all the IPv6 Prefixes learned (either dynamically or statically) from the Subscriber via an SD-WAN UNI on a given USWE instance and all of the IPv6 addresses assigned to the given USWE instance SD-WAN UNIs. This advertisement would not include any IPv6 Addresses associated with the USWE instance UTVCs, CTVCs, or CPI IPs or any UCS routing information. Since the USWE instance is initiating these advertisements, the next hop address for these routes is the USWE CPI IP address.

[R31] The SD-WAN Vendor Control Plane **MUST** advertise all IPv4 routes associated with the SD-WAN Service Routing Domain to the USWE instance

with the appropriate SD-WAN Service Routing Domain Route Target value and the appropriate MPLS label and advertised as VPNv4.

This advertisement would include all the IPv4 Addresses for the UTVC EPs, CTVC EPs, all SD-WAN Vendor Edge IP addresses, and all iBGP peer IPv4 addresses associated with the SD-WAN Service. This advertisement would not include any IPv4 prefixes learned from the Subscriber or any IPv4 prefixes for subnets directly connected to the Subscriber (i.e., SD-WAN UNI Connection Address subnets) nor would this advertisement include any UCS routing information. Since the SD-WAN Vendor Control Plane is initiating these advertisements, the next hop address for these routes needs to be an IP address reachable by the USWE instance.

[R32] The SD-WAN Vendor Control Plane **MUST** advertise all IPv6 routes associated with the SD-WAN Service Routing Domain to the USWE instance with the appropriate SD-WAN Service Routing Domain Route Target value and the appropriate MPLS label and advertised as VPNv6.

This advertisement would include all the IPv6 Addresses for the UTVC EPs, CTVC EPs, all SD-WAN Vendor Edge IP addresses, and all iBGP peer IPv6 addresses associated with the SD-WAN Service. This advertisement would not include any IPv6 prefixes learned from the Subscriber or any IPv6 prefixes for subnets directly connected to the Subscriber (i.e., SD-WAN UNI Connection Address subnets) nor would this advertisement include any UCS routing information. Since the SD-WAN Vendor Control Plane is initiating these advertisements, the next hop address for these routes needs to be an IP address reachable by the USWE instance.

[R33] The SD-WAN Vendor Control Plane **MUST** advertise all IPv4 routes associated with the Subscriber Routing Domain to the USWE instance with the appropriate Subscriber Routing Domain Route Target value and the appropriate MPLS label and advertised as VPNv4.

This advertisement would include all the IPv4 Prefixes learned (either dynamically or statically) from the Subscriber and all IPv4 prefixes for subnets directly connected to the Subscriber. This advertisement would not include any IPv4 Addresses associated with any of the SD-WAN Edges (UTVC addresses, CTVC addresses or CPI IPs) or any UCS routing information. Since the SD-WAN Vendor Control Plane is initiating these advertisements, the next hop address for these routes needs to be an IP address reachable by the USWE instance.

[R34] The SD-WAN Vendor Control Plane **MUST** advertise all IPv6 routes associated with the Subscriber Routing Domain to the USWE instance with the appropriate Subscriber Routing Domain Route Target value and the appropriate MPLS label and advertised as VPNv6.

This advertisement would include all the IPv6 Prefixes learned (either dynamically or statically) from the Subscriber and all IPv6 prefixes for subnets directly connected to the Subscriber. This advertisement would not include any IPv6 Addresses associated with any of the SD-WAN Edges (UTVC addresses, CTVC addresses or CPI IPs) or any UCS routing information. Since the SD-WAN Vendor Control Plane is initiating these advertisements, the next hop address for these routes needs to be an IP address reachable by the USWE instance.

Figure 10 illustrates an example of the USWE CPI and SD-WAN Vendor Control Plane Connectivity.

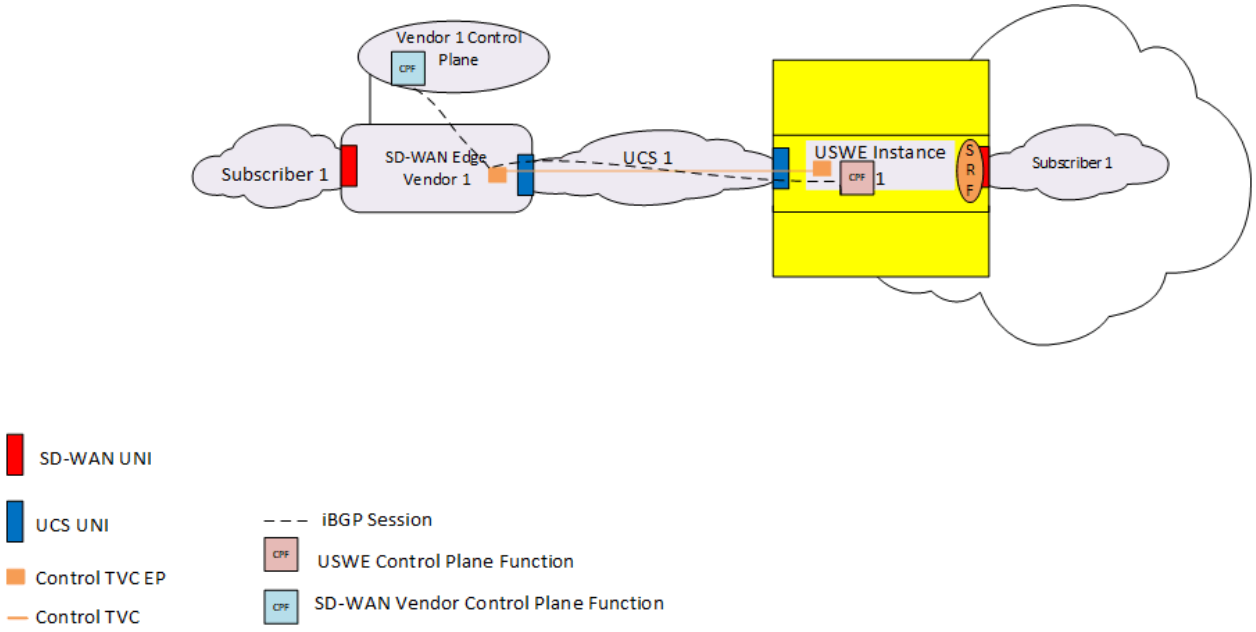


Figure 10 –USWE CPI to SD-WAN Vendor Control Plane Connectivity Example

9 Subscriber Routing Domain

Since the USWE implementation is predicated on MEF 70.1 [42], the routing protocols must adhere to MEF 70.1 [42] for the exchange of Subscriber Network IPv4 and IPv6 Prefixes between the USWE instance and the Subscriber.

The information about Subscriber routes is in a different VRF, as defined by IETF RFC 4364 [22], than the SD-WAN Service routing information.

In particular, this version of the USWE Implementation Agreement mandates that a USWE implementation supports Static and BGP routing at the SD-WAN UNI. Other dynamic routing protocols are not precluded but are beyond the scope of this document.

[R35] A USWE implementation **MUST** support Static and BGP routing in the value of the SD-WN UNI Routing Protocols Service Attribute.

A USWE instance is responsible for advertising the Subscriber Routing Domain IPv4 Prefixes learned via the SD-WAN Vendor Control Plane to the Subscriber via the SD-WAN UNIs at the USWE instance when the Subscriber Routing Protocol for IPv4 is BGP.

[R36] A USWE instance **MUST** advertise to the Subscriber the IPv4 Prefixes in the Subscriber Routing Domain learned from the SD-WAN Vendor Control Plane via any SD-WAN UNI where the value of the SD-WAN UNI Routing Protocols Service Attribute contains a BGP entry for IPv4.

A USWE instance is responsible for advertising the Subscriber Routing Domain IPv6 Prefixes learned via the SD-WAN Vendor Control Plane to the Subscriber via the SD-WAN UNIs at the USWE instance when the Subscriber Routing Protocol for IPv6 is BGP.

[R37] A USWE instance **MUST** advertise to the Subscriber the IPv6 Prefixes in the Subscriber Routing Domain learned from the SD-WAN Vendor Control Plane via any SD-WAN UNI where the value of the SD-WAN UNI Routing Protocols Service Attribute contains a BGP entry for IPv6.

Subscriber IP Packets are routed by the USWE instance only over the Universal Data Plane.

[R38] The Subscriber Routing Domain IP Packets **MUST NOT** be routed over a CTVC.

10 Common UTVC/CTVC Requirements

The common UTVC/CTVC requirements are defined below. These requirements apply to both UTVCs (see section 11.1) and Control Tunnel Virtual Connections (CTVCs) (see section 8.2). Please note that the requirements in this section apply to UTVC or CTVC End Points at the USWE and to UTVC or CTVC End Points located on SD-WAN Vendor Edges.

10.1 UTVC/CTVC End Point

The UTVC/CTVC End Point is a logical construct that terminates the UTVC or CTVC by performing any encapsulation/encryption and decapsulation/decryption necessary to forward IP Packets over a UTVC or CTVC.

[R39] An implementation of a UTVC or CTVC **MUST** support carrying IPv4 (as defined in IETF RFC 791 [1]) and IPv6 (as defined in IETF RFC 4291 [17]) traffic.

Note: [R39] addresses what is carried over the overlay and does not address the abilities of the underlay.

10.2 Common UTVC/CTVC DSCP/PCP Values

The USWE is responsible for correctly using the appropriate DSCP and PCP value for all UTVCs and CTVCs. This value is configured by the SD-WAN Vendor Manager as described in sections 12.2.4.1 and 12.2.5.

[R40] A USWE instance **MUST** use the DSCP and PCP value assigned per [R39] in the outer header of IP packets transmitted over the UTVC or CTVC.

10.3 UTVC/CTVC Encapsulation and Encryption Requirements

IPsec is used in conjunction with the manually configured Security Association to provide secure tunnels between UTVC or CTVC End Points. The following set of requirements define UTVC or CTVC encapsulation and encryption.

IETF RFC 4301 [18] addresses the security architecture for IP.

[R41] An implementation of a UTVC or CTVC **MUST** comply with all mandatory requirements in IETF RFC 4301 [18] unless otherwise noted.

[R42] An implementation of a UTVC or CTVC **MUST** use Tunnel Mode as defined in IETF RFC 4301 [18].

IETF RFC 4303 [19] describes the Encapsulating Security Payload (ESP). ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

[R43] An implementation of a UTVC or CTVC **MUST** comply with IETF RFC 4303 [19].

[R44] An implementation of a UTVC or CTVC **MUST** use extended sequence number (ESN) as defined in IETF RFC 4303 [19] section 2.2.1.

IETF RFC 3948 [13] describes methods to encapsulate and decapsulate IP Encapsulating Security Payload (ESP) packets inside UDP packets for traversing Network Address Translators.

[R45] An implementation of a UTVC or CTVC **MUST** comply with all mandatory requirements of UDP Encapsulation of ESP Packets as specified in IETF RFC 3948 [13].

IETF RFC 4308 [20] specifies optional suites of algorithms and attributes that can be used to simplify the administration of IPsec when used in manual keying mode. IETF RFC 4308 contains no mandatory requirements. This document mandates support for these optional requirements.

[R46] An implementation of a UTVC or CTVC **MUST** comply with all optional requirements specified in IETF RFC 4308 [20].

IETF RFC 8221 [30] describes how to enable ESP and Authentication Header to benefit from cryptography that is up to date while making IPsec interoperable.

[R47] An implementation of a UTVC or CTVC **MUST** comply with all mandatory requirements specified in IETF RFC 8221 [30].

IETF RFC 2451 [8] describes how to use Cipher Block Chaining-mode cipher algorithms with the IPsec ESP Protocol.

[R48] An implementation of a UTVC or CTVC **MUST** comply with all mandatory requirements specified in IETF RFC 2451 [8].

IETF RFC 3602 [12] describes the use of the Advanced Encryption Standard Cipher Algorithm in Cipher Block Chaining Mode, with an explicit Initialization Vector, as a confidentiality mechanism within the context of the IPsec Encapsulating Security Payload (ESP).

[R49] An implementation of a UTVC or CTVC **MUST** comply with all mandatory requirements specified in IETF RFC 3602 [12].

IETF RFC 4106 [15] describes the use of the Advanced Encryption Standard (AES), defined as a specification for the encryption of data, in Galois/Counter Mode (GCM) as an IPsec Encapsulating Security Payload (ESP) mechanism to provide confidentiality and data origin authentication.

[R50] An implementation of a UTVC or CTVC **MUST** comply with all mandatory requirements specified in IETF RFC 4106 [15].

IETF RFC 4868 [25] describes the use of Hashed Message Authentication Mode (HMAC) in conjunction with the SHA-256, SHA-384, and SHA-512 algorithms in IPsec.

[D1] An implementation of a UTVC or CTVC **SHOULD** comply with all mandatory requirements specified in IETF RFC 4868 [25].

Hashing and Encryption are used by the Universal Data Plane and the Control Plane Interface to provide a secure means to forward Subscriber's packets and to eliminate the ability of a party other than the Subscriber from determining what data is being passed between SD-WAN Edges.

10.4 UTVC/CTVC Key Exchange

Key Exchange is done via a manually configured Security Association. In order for UTVC or CTVC encryption to remain secure, the encryption keys need to be rotated as to not allow for inappropriate disclosure of the encryption keys and to prevent brute force identification of the encryption keys. This is defined as the key Lifetime in section 12.2.4 for CTVCs and section 12.2.5 for UTVCs. The initial key pair is generated by the USWE instance, and the public key is communicated to the SD-WAN Vendor Manager via the Management Plane. When the key Lifetime reaches its half-life, the USWE instance generates a new key pair and communicates the new public key to the SD-WAN Vendor Manager. Similarly, the SD-WAN Vendor Manager passes the public keys from the other SD-WAN Edges to the USWE instance via the Management Plane. Switching from the existing key pair to the new key pair requires coordination between the USWE instance and the SD-WAN Vendor Manager. The date and time that the new key pair becomes active is communicated between the USWE instance and the SD-WAN Vendor Manager by the SD-WAN Vendor Manager. This is described in section 12.2.5.

[R51] When a UTVC or CTVC is encrypted, the UTVC or CTVC key pair **MUST** support binary keys as described in NIST 800-56A-Rev 3 [45].

[R52] When a UTVC or CTVC is encrypted, the UTVC or CTVC key pairs **MUST** be randomly generated.

[R53] The private key **MUST** be stored securely in the SD-WAN Edge or other UTVC or CTVC terminating device where it is generated, and not transmitted or revealed to any entity outside that device.

Note: recommendations for manual key distribution are defined in NIST SP 800-57, Part 1, Rev 5 [44]. While manual keying is not recommended in NIST SP 800-77 [47], the below text from NIST SP 800-77 [47], has influenced the decision to use manual keying.

"The only time that manual keying might be acceptable is if another trusted entity, such as a security controller in the SDWAN paradigm, assumes these responsibilities. Another example is the 3GPP protocol, which negotiates the IPsec parameters between a cell tower and handset using a non-Internet Key Exchange protocol."

[R54] When a UTVC or CTVC is encrypted, an implementation of UTVC or CTVC key generation and distribution **MUST** comply with the recommendations in NIST SP 800-57, Part 1, Rev 5 [44].

[R55] When a UTVC or CTVC is encrypted, an implementation of a UTVC or CTVC **MUST** support the following encryption and hashing algorithms:

- AES256
- SHA1

While other encryption and hashing algorithms can be supported, these are specified so that both ends of the UTVC have at a minimum these in common. If addition algorithms are supported at both the USWE and the SD-WAN Vendor Edge, they can be utilized as determined by the SP.

[R56] An implementation of a SD-WAN Vendor Manager **MUST** support notifying the USWE instance when rekeying is required when one or more UTVCs or CTVCs are encrypted.

[R57] A USWE implementation **MUST** support generation of initial and subsequent keys when one or more UTVCs or CTVCs are encrypted.

Note: the initial and subsequent keys are distributed via the Universal Management Plane. Time of Day synchronization between the USWE instance and the remote SD-WAN Vendor Edge is necessary to avoid traffic loss at the time of key switchover. See section 12.2.2 for details.

10.5 Monitoring UTVCs or CTVCs for Faults

It is mandated that all UTVCs or CTVCs be monitored for faults. Bidirectional Forwarding Detection (BFD), defined as a UDP-based detection protocol that provides a low-overhead method of detecting failures in the forwarding path between two adjacent routers, is the selected method for monitoring connectivity of UTVCs or CTVCs.

[R58] A USWE implementation **MUST** support single hop Bidirectional Forwarding Detection in compliance with section 7.2.1.2 of MEF 66 [38].

[R59] The USWE **MUST** monitor each UTVC or CTVC using BFD.

[R60] The USWE **MUST** declare a fault whenever a fault is recognized by BFD monitoring.

11 Universal Data Plane

The Universal Data Plane is defined in this section. The Universal Data Plane is a collection of UTVCs between the USWE instance and other SD-WAN Edges within an SD-WAN Service. UTVCs, which are defined within this document, are a special type of TVC that meet the forwarding relationship requirements defined in MEF 70.1 [42]. The additional requirements for UTVCs are defined in the following sections of the document. These requirements represent the minimum set of requirements that must be met for interoperability. Additional functionality may be provided, and that additional functionality is outside the scope of this document.

11.1 Universal Tunnel Virtual Connection

As stated above, a UTVC is a type of TVC that represents a forwarding relationship between a USWE instance and an SD-WAN Vendor Edge. A UTVC always is point to point and always provides authentication. The UTVC uses IPsec protocol with or without encryption. Authentication is always done regardless of whether there is encryption.

The UTVC supports several functions that are specified in detail within this document to provide interoperability. These characteristics are:

- Point to Point Connectivity
- Authentication
- Privacy via optional encryption

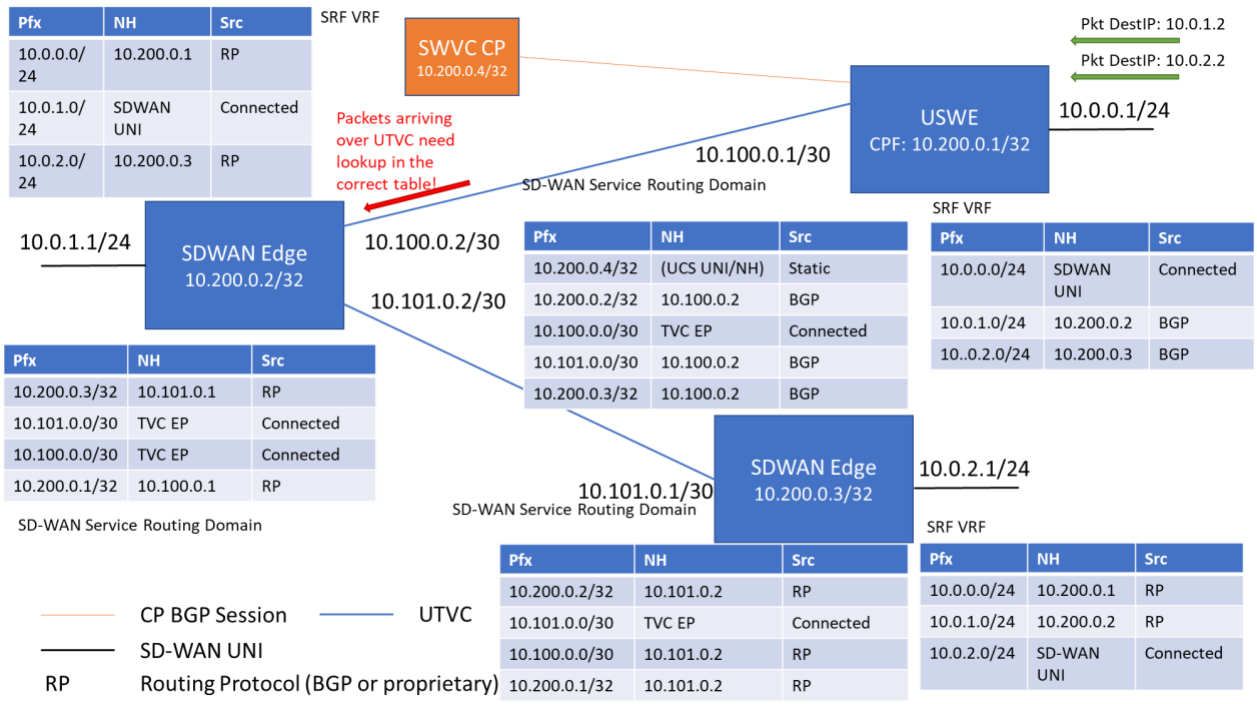
The UTVC supports only IPv4 and IPv6 unicast packets as payload. The UTVC provides privacy through the use of IPsec tunnel.

Note: IP Multicast is beyond the scope of this document since it is not addressed in MEF 70.1 [42].

The UTVC has two end points, and each end point is assigned an IP Address, either IPv4, IPv6, or both.

11.2 Routing Domains and Data Plane Forwarding

An SD-WAN Edge implementation needs the ability to identify which routing domain an ingress IP Packet belongs to so that it looks in the correct route table in the correct routing domain to correctly forward the IP Packet. If the routing domain cannot be identified, it can result in IP Packets being discarded and never reaching the target domain. Figure 11 shows an example of the issue.



Pfx	NH	Src
10.0.0.0/24	10.200.0.1	RP
10.0.1.0/24	SDWAN UNI	Connected
10.0.2.0/24	10.200.0.3	RP

Pfx	NH	Src
10.200.0.4/32	(UCS UNI/NH)	Static
10.200.0.2/32	10.100.0.2	BGP
10.100.0.0/30	TVC EP	Connected
10.101.0.0/30	10.100.0.2	BGP
10.200.0.3/32	10.100.0.2	BGP

Pfx	NH	Src
10.0.0.0/24	SDWAN UNI	Connected
10.0.1.0/24	10.200.0.2	BGP
10..0.2.0/24	10.200.0.3	BGP

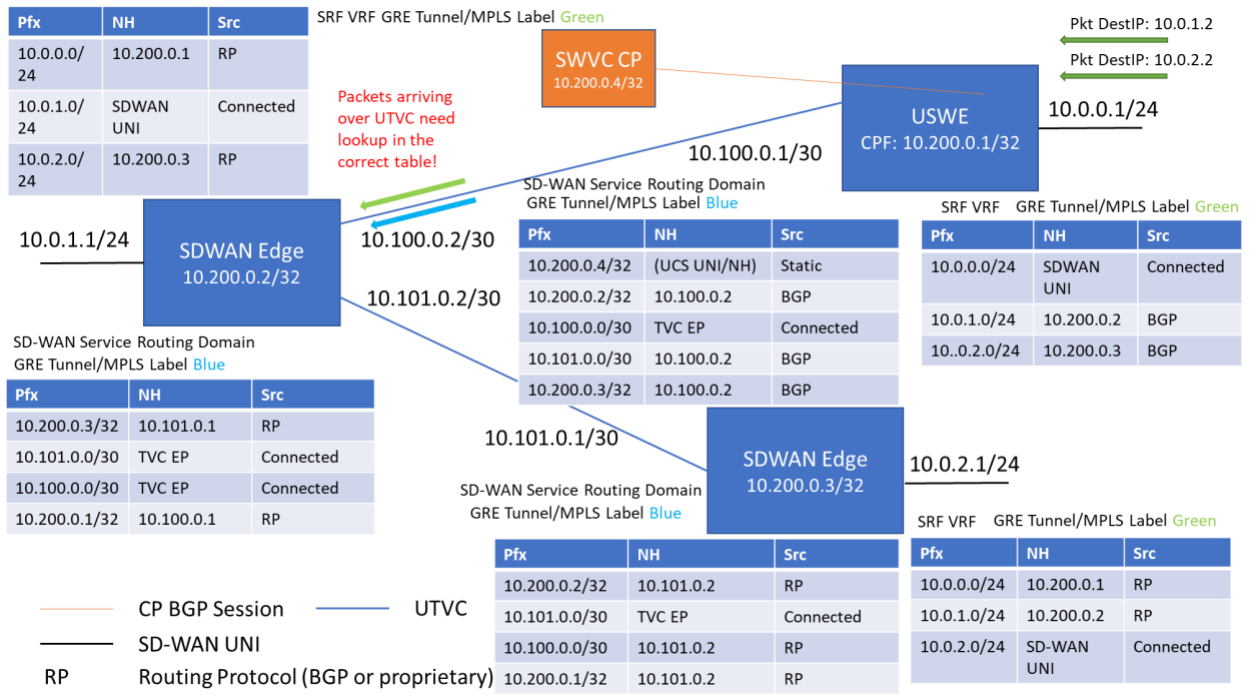
Pfx	NH	Src
10.200.0.3/32	10.101.0.1	RP
10.101.0.0/30	TVC EP	Connected
10.100.0.0/30	TVC EP	Connected
10.200.0.1/32	10.100.0.1	RP

Pfx	NH	Src
10.200.0.2/32	10.101.0.2	RP
10.101.0.0/30	TVC EP	Connected
10.100.0.0/30	10.101.0.2	RP
10.200.0.1/32	10.101.0.2	RP

Pfx	NH	Src
10.0.0.0/24	10.200.0.1	RP
10.0.1.0/24	10.200.0.2	RP
10.0.2.0/24	SD-WAN UNI	Connected

Figure 11 – IP Address Example

In Figure 11 there are two Routing Domains reflected, the SD-WAN Service Routing Domain and the Subscriber Routing Domain. The SD-WAN Service Routing Domain reflects the Control Plane, and the Subscriber Routing Domain reflects Subscriber packets. When an IP Packet arrives at the SD-WAN Vendor Edge there must be a decision made on which domain the packet should be forwarded to. There is no way to determine if the packet is intended for the SD-WAN Service Routing Domain or the Subscriber Routing Domain. This means in this example the packet may be dropped. The SP needs to address these issues for a SD-WAN Service to work with the USWE. The solution is shown in Figure 12. To support this, a combination of a Generic Routing Encapsulation (GRE) header and a Multi-Protocol Label Switching (MPLS) Label have been selected.



Pfx	NH	Src
10.0.0.0/24	10.200.0.1	RP
10.0.1.0/24	SDWAN UNI	Connected
10.0.2.0/24	10.200.0.3	RP

Pfx	NH	Src
10.200.0.4/32	(UCS UNI/NH)	Static
10.200.0.2/32	10.100.0.2	BGP
10.100.0.0/30	TVC EP	Connected
10.101.0.0/30	10.100.0.2	BGP
10.200.0.3/32	10.100.0.2	BGP

Pfx	NH	Src
10.0.0.0/24	SDWAN UNI	Connected
10.0.1.0/24	10.200.0.2	BGP
10..0.2.0/24	10.200.0.3	BGP

Pfx	NH	Src
10.200.0.3/32	10.101.0.1	RP
10.101.0.0/30	TVC EP	Connected
10.100.0.0/30	TVC EP	Connected
10.200.0.1/32	10.100.0.1	RP

Pfx	NH	Src
10.200.0.2/32	10.101.0.2	RP
10.101.0.0/30	TVC EP	Connected
10.100.0.0/30	10.101.0.2	RP
10.200.0.1/32	10.101.0.2	RP

Pfx	NH	Src
10.0.0.0/24	10.200.0.1	RP
10.0.1.0/24	10.200.0.2	RP
10.0.2.0/24	SD-WAN UNI	Connected

Figure 12 – GRE Tunnel and MPLS Label within IPsec Tunnel Example

The GRE tunnel is used to encapsulate each IP packet. This changes the IP Address and MAC address in the SD-WAN Service Domain. An MPLS label is added within the GRE tunnel that represents the domain the packet belongs to. A USWE instance and SD-WAN Edges can then use the MPLS label to determine the domain that the packet belongs to and forward the packet to the correct domain. In this example packets from the SD-WAN Service Routing Domain and the Subscriber Routing Domain are received at a SD-WAN Vendor Edge interface. By using the MPLS label, the USWE instance or the SD-WAN Vendor Edge can determine which domain the packet is intended for. The correct forwarding path can then be discovered without incorrect routing or dropped packets. The following requirements apply to both the USWE instance and the SD-WAN Vendor Manager.

[R61] All IP Packets that traverse the IPsec Tunnel **MUST** contain an MPLS Label as defined in IETF RFC 3032 [11] which uses the Label to identify the Routing Domain and a standard GRE header as defined in IETF RFC 2784 [10] that indicates that the contents contains an MPLS Label.

[R62] The device, USWE instance or SD-WAN Vendor Edge, that receives the IP Packets **MUST** use the GRE header and MPLS Label to determine which routing domain the IP Packet belongs to.

[R63] The GRE implementation **MUST** use a Protocol Type of 0x8847 to indicate that there is an MPLS Label within the GRE tunnel.

[R64] The MPLS implementation **MUST** use a unique Label, as specified in [R18] and [R19], to indicate the Routing Domain that the IP packet belongs to as described in IETF RFC 4023 [14].

Note: The Label used is determined by the SP and does not need to be shared with the Subscriber.

[R65] Any IP Packet that is forwarded by the USWE via Internet Breakout **MUST** be forwarded based on routing information in the VRF for Internet Breakout (see [R20]).

[R66] Any IP Packet that is forwarded by the USWE for the purposes of Internet Breakout at a different SD-WAN Vendor Edge **MUST** be encapsulated in GRE with a unique MPLS label, as defined in [R20], i.e., different to the labels used for the Subscriber and SD-WAN Service Routing Domains.

Requirement [R66] dictates that the IP packets which by Policy are directed to remote Internet Breakout need to be encapsulated in GRE with a specific MPLS Label. This enables the SD-WAN Data Plane to distinguish between a packet following a route via the SD-WAN Service to another SD-WAN UNI or being sent to the internet via a UCS which supports Internet Breakout.

MEF 70.1 [42] defines Internet Breakout as "The forwarding of IP Packets in Application Flows, based on Policy, to Internet destinations via Internet Access UCSs," and Local Internet Breakout as "Internet Breakout in which Ingress IP Packets are forwarded over Internet Access UCSs connected to the SD-WAN Edge where the Ingress SD-WAN UNI is located." In the context of the USWE, Application Flows which by Policy should be forwarded over Internet Access UCSs, may breakout on the USWE or an SD-WAN Vendor Edge. Since the IP packets which are forwarded from the USWE to another SD-WAN Vendor Edge need to include the markings for Internet Breakout, these packets need to be encapsulated in GRE so that the receiving SD-WAN Vendor Edge understands to forward these IP packets over the Internet Access UCS and not over another TVC. However, if the receiving SD-WAN Vendor Edge does not have a connected Internet Access UCS, the IP Packets are forwarded over another TVC to an SD-WAN Vendor Edge that has a connected Internet Access UCS. In this case, the IP Packets would still be encapsulated in GRE. However, once the IP Packets are received by an SD-WAN Vendor Edge with a connected Internet Access UCS, the GRE encapsulation is removed, and the IP packet is forwarded to the Internet Access UCS. IP Packets received from the Internet at an SD-WAN Vendor Edge and destined for an SD-WAN UNI located at a USWE are encapsulated in GRE and have an appropriate MPLS label added to them by the SD-WAN Vendor Edge.

11.3 Fault Management

Fault Management for the USWE instance is defined in this section. This includes monitoring the operation of the USWE instance (e.g., the application operation of the instance) and faults on an interface to a UCS UNIs and the SD-WAN UNI. The monitoring of the hardware platform that hosts the USWE instance is outside the scope of this document.

11.3.1 UCS UNI and SD-WAN UNI Fault Management

Faults may occur with a UCS UNI or SD-WAN UNI. A USWE instance monitors UCS UNIs and SD-WAN UNIs for faults and declares that a fault exists. Faults that are detected on a UCS UNI or SD-WAN UNI include:

- Loss of incoming signal at an interface

- Remote failure indication if supported by the underlay technology

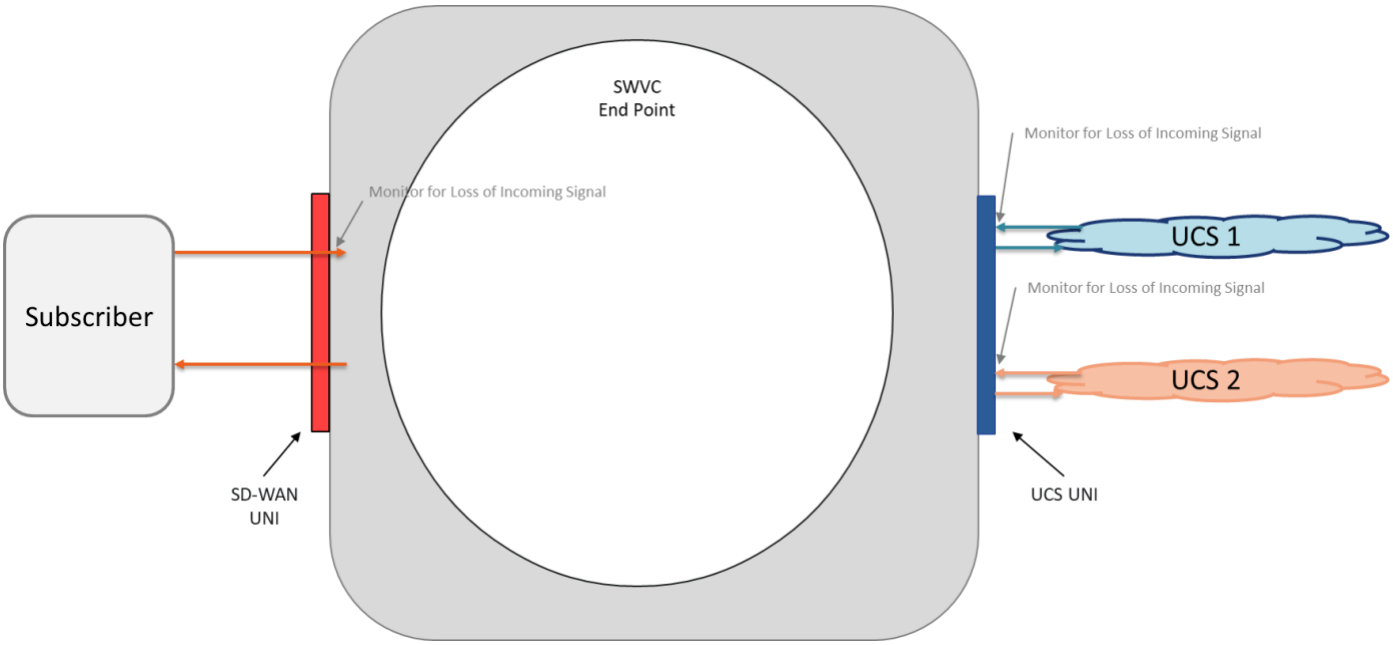


Figure 13 – Monitoring Interfaces

Figure 13 shows the monitoring of UCS UNIs and SD-WAN UNIs for a loss of incoming signal. How this monitoring is performed and what is monitored for may differ depending on the UCS type or the SD-WAN UNI type. This may also impact if any remote failure can be detected. For example, a Layer 1 UCS might support remote failure indications, whereas an Ethernet underlay may not.

[R67] A USWE instance **MUST** monitor each UCS UNI for any loss of incoming signal and declare a fault if one is detected.

[R68] If the underlay technology supports remote failure indications, a USWE instance **MUST** monitor each UCS for a remote failure indication received from a far-end or the next hop of the UCS and declare a fault if one is detected.

[R69] A USWE instance **MUST** monitor each SD-WAN UNI for any loss of incoming signal and declare a fault if one is detected.

[R70] A USWE instance **MUST** monitor the status of each interface (physical or logical) and declare a fault if the status indicates a failure condition has occurred.

11.3.2 Types of Faults

Examples of fault types are defined in Table 4 and are used to indicate the category of fault that has occurred.

Fault Type	Definition
Interface Down	A loss of incoming signal or Remote Defect Indication is detected at a physical or virtual interface on the USWE instance
BFD Fault	A loss of forwarding between two UTVC or CTVC end points. See section 10.5.
BGP Neighbor State	An indication that a BGP neighbor is down
CPU Resource in Use	An indication that the amount of CPU in use has reached a percentage that is considered a threat to the proper operation of the USWE instance
Memory Resource in Use	An indication that the amount of memory in use has reached a percentage that is considered a threat to the proper operation of the USWE instance
Storage Resource in Use	An indication that the amount of storage in use has reached a percentage that is considered a threat to the proper operation of the USWE instance

Table 4 – Example Fault Types

11.3.3 Fault Notification

The requirements for Fault Notification are defined in this section.

[R71] A USWE implementation **MUST** provide the ability to generate a notification of the occurrence of any configured fault or clearance of a fault within 10 seconds of the occurrence or clearance.

Note: generating a notification can be as simple as logging to syslog.

10 seconds has been selected as the value since it is believed that this value can be supported by the majority of SD-WAN Vendors at the current time.

A fault notification is generated when any interface experiences a fault as described in section 11.3.1.

[R72] A fault notification **MUST** include the following as defined in Table 5:

- Fault Date/Time

- Fault Type
- Fault Description
- Severity

The fault notification attributes are defined in Table 5. There is no USWE identifier in the fault notification. The Source IP Address for the USWE Management Plane is used to identify the USWE sending the notification to the SD-WAN Vendor Manager.

Notification Attribute	Description	Format	Comments
Fault Date/Time	The date and time that the fault was detected or cleared by the USWE instance.	Date and Time (ISO 8601-1:2019 [36])	This is the detected/clearance time, not the reported time.
Fault Type	A classification of the fault	String	Specified by the USWE implementation
Fault Description	A brief textual description of the fault.	String	The specific text to be used is implementation specific.
Severity	The severity of an Alarm.	One of: Warning Minor Major Critical Cleared	Note: the severity of a fault is determined by the implementation.

Table 5 – Fault Notification Attributes

11.4 Performance Monitoring

Performance Monitoring at the USWE instance, as defined in this standard, includes monitoring the performance of the overlay (TVCs and Application Flow MIR) and the underlay (UCSs). Performance Monitoring of the overlay is defined in MEF 105 [43]. Performance Monitoring of

underlay is defined in MEF 66 (IP) and MEF 35.1 (Ethernet) depending on the type of underlay. Monitoring of Application Flow performance is out of scope.

MEF 105 [43] defines an architecture and set of requirements for Performance Monitoring for SD-WAN. The calculated Performance Metrics are defined, Measurement Points where measurements are performed, including their logical location are defined, reporting of Performance Metrics is described, and Threshold Crossing Alerts (TCAs) are defined. This section does not restate the requirements and architecture from MEF 105 [43], instead, it provides a high-level overview of what is defined in MEF 105 [43]. MEF 105 [43] should be used as the source document to define most of the PM requirements in a USWE implementation.

MEF 105 [43] specifies that all TVCs are monitored. The Performance Metrics that are monitored for UTVCs are:

- One-way Mean Packet Delay
- One-way Mean Inter-Packet Delay Variation
- One-way or Two-way Packet Loss Ratio (see below)

The Performance Metrics are calculated at the interval defined as the Performance Metric Calculation Interval for TVCs. They are reported at some regular interval that is a multiple of the Performance Metric Calculation Interval defined as the Performance Metric Report Interval.

Threshold Crossing Alerts (Stateful or Stateless) are described in MEF 105 [43] as optional functions that may be supported. TCAs provide notifications when a specified Performance Metric Value is less than, equal to, or greater than a specified threshold value.

Monitoring the performance of TVCs is defined in MEF 105 [43]. The requirements in MEF 105 [43] do not specify what tool or method is used to perform measurements. This is because MEF 105 [43] is based on the SD-WAN Service described in MEF 70.1 [42] and is assumed to include a single SD-WAN Vendor. Since a USWE implementation may interact with different SD-WAN Vendors' Edges, this section defines Ping as the mandatory method to perform the measurements and STAMP as an optional method to perform the measurements.

A USWE implementation performs some Performance Metric calculations and some measurements that are passed to the SD-WAN Vendor Manager for calculation. The USWE performs the following measurements and calculations:

- One-Way Mean Packet Delay
- One-Way Mean Inter-Packet Delay Variation
- Two-Way Packet Loss Ratio

These three measurements are performed using pings which result in two-way measurements of packet delay and packet loss. The two-way Packet Delay values are divided in half to result in one-way values in each direction. It is understood that these values are not as accurate as true one-

way measurements but a compromise between accuracy and ease of implementation has been made.

In addition, the USWE performs MIR measurements of the following as defined in MEF 105 [43]:

- Ingress number of bytes received
- Egress number of bytes transmitted

These are collected and passed by the USWE to the SD-WAN Vendor Manager where they are used to calculate Ingress and Egress Mean Information Rates. Performing the calculation of MIR by the SD-WAN Vendor Manager places the complexity in the vendor manager and not within the USWE.

11.4.1 USWE Implementation Performance Monitoring Requirements

The requirements for PM for the USWE implementation are defined in this section.

[R73] When using ping to perform measurements, a USWE implementation or SD-WAN Vendor Edge implementation **MUST** support calculating and reporting Performance Metrics (One-Way Mean Packet Delay, One-Way Mean Inter-Packet Delay Variation, as described in MEF 105 [43] section 7.2.4, and Two-Way Packet Loss Ratio which is not described in MEF 105 [43]).

[CR1]<[O3] When using STAMP to perform measurements, a USWE implementation or SD-WAN Vendor Edge implementation **MUST** support calculating and reporting Performance Metrics (One-Way Mean Packet Delay, One-Way Mean Inter-Packet Delay Variation, and One-Way Packet Loss Ratio as described in MEF 105 [43] section 7.2.4).

Note: When Ping is used as the measurement tool, One-Way Mean Packet Delay and One-Way Mean Inter-Packet Delay Variation are calculated by dividing two-way measurements in half. Two-Way Packet Loss Ratio encompasses both near-far and far-near paths in the metric value.

[R74] A USWE implementation or SD-WAN Vendor Edge implementation **MUST** support Byte Counters as described in MEF 105 [43] section 7.2.4.

[O1] A USWE implementation or SD-WAN Vendor Edge implementation **MAY** support Stateless TCA reporting as defined in MEF 105 [43] section 7.4.

[CR2]<[O1] If Stateless TCA reporting is supported, the USWE implementation or SD-WAN Vendor Edge implementation **MUST** support the damping factor set to 1.

[CO1]<[O1] If Stateless TCA reporting is supported, the USWE implementation or SD-WAN Vendor Edge implementation **MAY** support the damping factor set to >1.

[O2] A USWE implementation or SD-WAN Vendor Edge implementation **MAY** support Stateful TCA reporting as defined in MEF 105 [43] section 7.4.

The One-way Mean Packet Delay and One-way Mean Inter-Packet Delay Variation measurements are derived by halving Two-way Mean Packet Delay and Two-way Mean Inter-Packet Delay Variation measurements. Packet Loss Ratio is a two-way measurement rather than a one-way measurement required in MEF 105 [43]. These differ from MEF 105 [43] due to the limitations of performing only two-way measurements that a Ping using ICMP messages has.

[R75] A USWE implementation or SD-WAN Vendor Edge implementation **MUST** support the use of Ping with ICMP messages, either IPv4 as defined in IETF RFC 792 [2] or IPv6 as defined in IETF RFC 4443 [23] depending on the end point address type, IPv4 or IPv6, to perform delay and packet loss measurements (for calculating One-Way Mean Packet Delay, One-Way Mean Inter-Packet Delay Variation, and Two-Way Packet Loss Ratio).

[R76] A USWE implementation or SD-WAN Vendor Edge implementation **MUST** use a unicast DA for synthetic packets generated as part of a Ping using ICMP messages.

[R77] A USWE implementation or SD-WAN Vendor Edge implementation **MUST** support a time interval between the transmissions of Ping using ICMP messages of 100ms.

[D2] A USWE implementation or SD-WAN Vendor Edge implementation **SHOULD** support a time interval between transmissions of Ping using ICMP messages of less than 100ms.

[R78] A USWE implementation or SD-WAN Vendor Edge implementation of Ping **MUST** allow the number of Ping using ICMP messages to be transmitted to be selected.

[R79] A USWE implementation or SD-WAN Vendor Edge implementation of Ping **MUST** be capable of transmitting Ping using ICMP messages indefinitely.

[R80] A USWE implementation or SD-WAN Vendor Edge implementation of Ping **MUST** allow for configuration of the packet length of the Ping using ICMP message to any value in the range of 64-1500 Bytes.

[D3] A USWE implementation or SD-WAN Vendor Edge implementation of Ping **SHOULD** allow for configuration of the packet length of the Ping using ICMP message to any value in the range of 1501-10000 Bytes.

The Ping function was selected as the mechanism to perform PM Measurements because it is widely supported by multiple SD-WAN Vendor Edge implementations. STAMP is shown as optional because it has not been widely implemented but does provide superior measurements to Ping.

[O3] A USWE implementation or SD-WAN Vendor Edge implementation **MAY** use STAMP as defined in IETF RFC 8762 [34] to perform delay and packet loss measurements (for calculating One-Way Mean Packet Delay, One-Way Mean Inter-Packet Delay Variation, and One-Way Packet Loss Ratio).

[CR3]<[O3] A unicast DA **MUST** be used as the DA when performing PM measurements using STAMP.

[CR4]<[O3] A USWE implementation or SD-WAN Vendor Edge implementation **MUST** support a time interval between the transmissions of STAMP messages of 100ms.

[CD2]<[O3] A USWE implementation or SD-WAN Vendor Edge implementation **SHOULD** support a time interval between transmissions of STAMP messages of less than 100ms.

[CR5]<[O3] A USWE implementation or SD-WAN Vendor Edge implementation of STAMP **MUST** allow the number of STAMP messages to be transmitted to be selected.

[CR6]<[O3] A USWE implementation or SD-WAN Vendor Edge implementation of STAMP **MUST** be capable of transmitting STAMP messages indefinitely.

[CR7]<[O3] A USWE implementation or SD-WAN Vendor Edge implementation of STAMP **MUST** allow for configuration of the packet length of the STAMP message to any value in the range of 64-1500 Bytes.

[CR8]<[O3] A USWE implementation or SD-WAN Vendor Edge implementation of STAMP **SHOULD** allow for configuration of the packet length of the STAMP message to any value in the range of 1501-10000 Bytes.

11.4.2 SD-WAN Vendor Manager Performance Monitoring Requirements

From a Performance Monitoring perspective, the SD-WAN Vendor Manager has responsibility for collecting byte-counter values that are reported by the USWE instance and calculating the MIR on appropriate Application Flows. A USWE instance reports byte-counters and the SD-WAN Vendor Manager performs the MIR calculations.

[R81] The SD-WAN Vendor Manager **MUST** calculate the Ingress and Egress MIR as specified in MEF 105 [43] section 7.2 from byte-counter values provided by the USWE instance.

11.4.3 USWE Underlay Performance Monitoring Requirements

The requirements in this section apply to the Underlay versus the Overlay.

[R82] If the Underlay is Ethernet, the USWE Implementation **MUST** support all mandatory requirements from MEF 35.1 [38].

[R83] If the Underlay is Ethernet, the SD-WAN Vendor Edge Implementation **MUST** support all mandatory requirements in MEF 35.1 [38].

[R84] If the Underlay is IP, the USWE implementation **MUST** support all mandatory requirements defined in MEF 66 [40].

[R85] If the Underlay is IP, the SD-WAN Vendor Edge Implementation **MUST** support all mandatory requirements defined in MEF 66 [40].

12 USWE Universal Management Plane

The Universal Management Plane is a connection between the SD-WAN Vendor Manager and the USWE instance. The requirements for the information passed over this connection are detailed in this section. The API that is used to communicate over this connection is not defined in this document. The USWE Universal Management Plane is shown in Figure 14 .

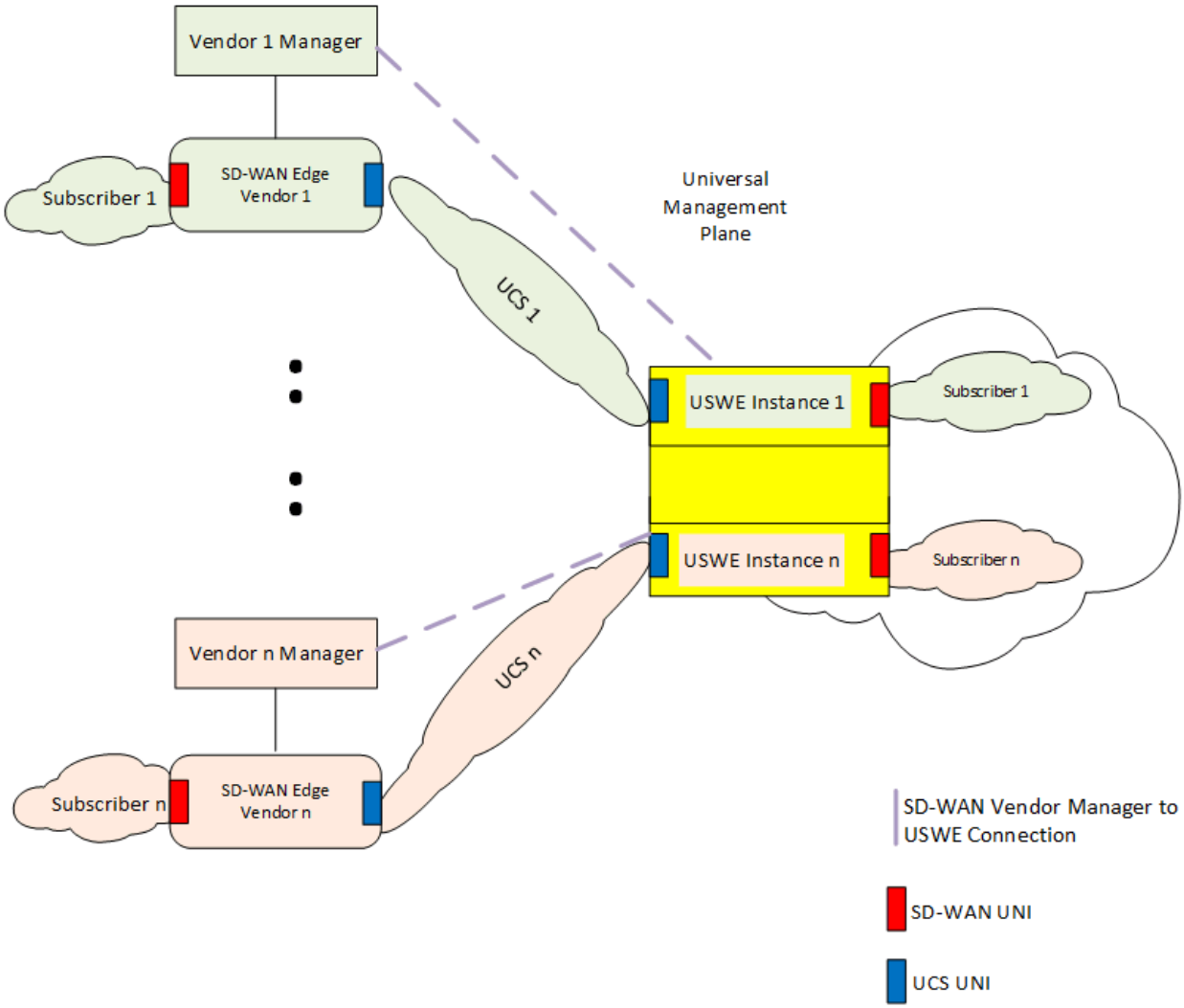


Figure 14 – USWE Universal Management Plane – Multiple SD-WAN Vendor Managers

The Universal Management Plane, connecting the SD-WAN Vendor Manager to the USWE instance, is responsible for configuring the USWE instance by the SD-WAN Vendor Manager sending the configuration details to the USWE instance. The SD-WAN Vendor Manager also receives from the USWE instance, notifications, including Fault Alarms and Performance Monitoring results.

The Universal Management Plane supports the following:

- The configuration of the USWE instance by the SD-WAN Vendor Manager including
    - the configuration and connectivity of the Universal Control Plane
    - the configuration and connectivity of the Universal Data Plane
- The passing of notifications from the USWE instance to the appropriate SD-WAN Vendor Manager

This section includes the steps taken to configure, associate, or manage the USWE instance, the SD-WAN Service with associated UNIs, Policies, Application Flows, and the Control and Data Plane Connectivity. It does not specify the APIs used to manage the USWE instance.

This section assumes that any actions required to instantiate or "spin up" the USWE instance are completed before any USWE instance configuration by the Universal Management Plane is performed. Initial management configuration (so that the USWE instance is reachable and authenticated by the SD-WAN Vendor Manager) is assumed to be done via an out of band connection to the USWE instance. Details on loading the initial configuration are out of scope but an out of band connection to the USWE instance is assumed to exist. It is also assumed that a USWE instance can contact the SD-WAN Vendor Manager when it is activated.

It is assumed that a secure channel exists between the SD-WAN Vendor Manager and the USWE instance. This secure channel is created between the USWE and the SD-WAN Vendor Manager. It provides secure communications where the USWE and the SD-WAN Vendor Manager each authenticate the other and confidentiality and integrity of data passed over the channel is ensured.

There are four operation terms defined for the Universal Management Plane, *Create*, *Modify*, *Delete*, and *Retrieve*. The functions operate as follows where the SD-WAN Vendor Manager is responsible for the action:

- *Create* operation supports the initial instantiation or configuration of an entity.
- *Modify* operation supports changing values of existing attributes or setting values for optional attributes.
- *Delete* operation supports deleting an existing entity.
- *Retrieve* operation supports retrieving the values of all attributes of an entity

[R86] An implementation of the SD-WAN Vendor Manager or the USWE **MUST** support the *Create*, *Modify*, *Delete*, and *Retrieve* functions as described above.

The SD-WAN Vendor Manager sends the configuration data for connectivity for both the Control Plane and Data Plane.

[R87] An instance of the USWE **MUST** store on the USWE instance all configuration data received from the SD-WAN Vendor Manager.

[R88] An instance of the USWE **MUST** provide the ability for the SD-WAN Vendor Manager to retrieve all configuration data stored on the USWE instance.

12.1 Activity Flow for USWE

A step-by-step example of the flow of actions for configuring a USWE instance is described in this section as an activity flow. The remaining sections in section 12 describe each step in the activity flow in detail.

For this activity flow to begin, the connection between the SD-WAN Vendor Manager and the USWE instance must exist. The connection of UCSs to physical or virtual interfaces on the USWE instance is assumed to have been completed, and the information about which interface on the USWE is connected to which UCS is assumed to be available to the SD-WAN Vendor Manager. Similarly, the connection of the Subscriber to physical or virtual interfaces on the USWE instance that will act as SD-WAN UNIs is assumed to have been completed.

A USWE instance contains a number of physical or logical network interfaces, that might be configured by the SD-WAN Vendor Manager so as to act in various different roles, e.g. as UCS UNIs, UCS End Points, SD-WAN UNIs, CTVC End Points, UTVC End Points, etc. The SD-WAN Manager does not pass information about the role of a given network interface to the USWE instance; rather, it uses its own knowledge of the intended role of each network interface to pass appropriate configuration for that interface to the USWE instance, e.g. the appropriate IP address and VRF information. Each network interface on the USWE instance is assumed to have a unique interface identifier.

How the SD-WAN Vendor Manager determines the appropriate configuration for each interface on the USWE is beyond the scope of the document. It may use information about the SD-WAN Service Attribute values that the SP has agreed with the Subscriber (e.g. the IP Connection addresses at an SD-WAN UNI); information from other internal sources within the SP (e.g. which UCSs are connected to which network interfaces on the USWE instance); and information generated within the SD-WAN Vendor Manager itself (e.g. IP addresses assigned for each UTVC).

Once the prerequisites have been completed, the configuration of the USWE instance by the SD-WAN Vendor Manager can begin. How the SD-WAN Vendor Manager determines the required configuration parameter values to pass to the USWE instance is beyond the scope of the document. A high-level description of the recommended sequence of configuration steps is described in this section.

1. The SD-WAN Vendor Manager instantiates a VRF on the USWE instance for each UCS that the USWE instance is connected to, for the Service Routing Domain, Internet Breakout, and the Subscriber Routing Domain.
2. The SD-WAN Vendor Manager configures Network Timing Protocol on the USWE.
3. The SD-WAN Vendor Manager instantiates UCS UNIs on the USWE instance by passing the following information to the USWE instance.
    a. Physical/virtual interface identifier
    b. Ethernet Attributes
    c. IP attributes
        i. Static IP per UCS UNI (when IP underlay) or per UCS End Point (when Ethernet underlay) or configure to use DHCP/SLAAC Per UCS UNI or UCS End Point.
        ii. The VRF for the interface (i.e., the VRF for the UCS with which the UCS UNI or UCS End Point is associated)

iii. Any UCS UNI routing protocol needed (internet default route, MPLS BGP)

d. Enable UCS UNIs and UCS End Points

4. The SD-WAN Vendor Manager enables the Universal Control Plane on the USWE instance using the following steps:
   a. Create the SD-WAN Service VRF
   b. Create the Internet Breakout VRF
   c. Create one or more CTVCs by passing the following information for each one:
      i. CTVC End Point (IPsec tunnel)
         1. CTVC End Point Identifier
         2. VRF for the interface (i.e. the SD-WAN Service VRF)
         3. CTVC End Point IP address (IPv4, IPv6, both)
         4. IP prefix length
         5. Manual SA information:
            a. Key exchange information (key length policy and key lifetime)
            b. Public key for the remote end of the CTVC Authentication Method
         6. Privacy Method
      ii. Association of CTVC End Point to UCS End Point i.e., the interface identifier for the network interface on the USWE which the CTVC should traverse - this will be an interface corresponding to a UCS UNI or UCS End Point.
      iii. Destination IP address for the UCS End Point for the other end of the CTVC
   d. A USWE instance generates a key pair to use for each CTVC and passes the public key for each CTVC to the SD-WAN Vendor Manager.
   e. If the CPI interface is not a CTVC End Point then the SD-WAN Vendor Manager instantiates the CPI by passing the following information to the USWE instance
      i. Interface identifier for the interface that will act as the CPI
      ii. CPI interface to SD-WAN Service VRF
      iii. CPI interface IP address (IPv4, IPv6, both)
      iv. IP prefix length
   f. The SD-WAN Vendor Manager defines attributes for each Control Plane iBGP session, by passing the following information to the USWE instance for each one:
      i. BGP parameters for the BGP connection between the USWE instance and the SD-WAN Vendor Control Plane
      ii. IP address that are of the BGP peer
      iii. Static route for SD-WAN Vendor Control Plane IP Address via remote CTVC End Point IP address
      (Note that SD-WAN Vendor Control Plane must be configured, along with all necessary SD-WAN Service devices, with the reachability to USWE CPI. See section 8 for detailed requirements.
      iv. Add static routes for local Internet Breakout
      v. iBGP sessions become active and advertise/receive routes for the SD-WAN Service routing domain VRF

5. The SD-WAN Vendor Manager enables the Universal Data Plane on the USWE instance using the following steps:
    a. Create one or more UTVCs by passing the following information for each one:
        i. UTVC End Point (IPsec tunnel)
            1. VRF for the interface (i.e. the SD-WAN Service VRF)
            1. UTVC End Point IP address (IPv4, IPv6, both)
            2. IP prefix length
            3. Manual SA information:
                a. key exchange information (key length policy and key lifetime) if encrypted
                b. Public key for the remote end of the CTVC Authentication Method (if encrypted)
            4. Privacy Method (if encrypted)
        ii. Association of UTVC End Point to UCS End Point i.e., the interface identifier for the network interface on the USWE which the UTVC should traverse - this will be an interface corresponding to a UCS UNI or UCS End Point.
        iii. Destination IP address for the UCS End Point for the other end of the UTVC
    b. A USWE instance generates a key pair to use for each UTVC and passes the public key for each UTVC to the SD-WAN Vendor Manager.
    c. Configure GRE Tunnels/MPLS Labels
        i. Configure GRE Tunnel per UTVC
        ii. Configure MPLS Label associated with SD-WAN Service Routing VRF
        iii. Configure MPLS Label associated with Subscriber Routing VRF
        iv. Configure MPLS Label associated with Internet Breakout
6. The SD-WAN Vendor Manager configures each SD-WAN UNI on the USWE instance by passing the following information:
    a. Physical/virtual interface identifier
    b. Ethernet Attributes
    c. The IP addresses for the SD-WAN UNI, assigned according to the value of the SD-WAN UNI IPv4/IPv6 Connection Addressing Service Attribute.
    d. The maximum L2 frame size for the SD-WAN UNI, determined according to the value defined in the SD-WAN UNI Maximum L2 Frame Size Service Attribute.
    e. SD-WAN UNIs are left *Disabled*

    Note: An SD-WAN UNI includes a logical SD-WAN Service End Point as defined in MEF 70.1.
7. The SD-WAN Vendor Manager configures Subscriber Routing using the following steps
    a. Create Subscriber Routing VRF
    b. Add the network interfaces corresponding to each SD-WAN UNI to Subscriber Routing VRF
    c. If the value of the SD-WAN UNI Routing Protocol Service Attribute is Static Routing populate static routes in Subscriber Routing VRF
    d. If the value of the SD-WAN UNI Routing Protocol Service Attribute is BGP configure BGP peering with Subscriber in the Subscriber Routing VRF

   e. Configure USWE CPI BGP sessions to carry Subscriber Routing VRF routing information as VPNv4 or VPNv6 routes. This includes configuring the Route Distinguishers, import and export Route Targets and MPLS labels.
8. Create Application Flow Specifications
   a. The SD-WAN Vendor Manager passes *AFName, AFCritList,* (defined in MEF 70.1 [42] sec 9.12) to the USWE instance for each Application Flow Specification
9. Configure Zone Matching Criteria
   a. The SD-WAN Vendor Manager passes Zone Matching Criteria (defined in MEF 70.1 [42] sec 9.6) to the USWE instance for each Zone
10. Configure SD-WAN Service End Point Policy Map
   a. For each SD-WAN UNI, Zone Name, and Application Flow Specification, the SD-WAN Vendor Manager passes the *list of UTVC End Point Interface Identifiers for Ingress (filled or empty*) in the order of preference, and the values of *Internet Breakout (T/F), Allowed Destination Prefixes (either 0/0 or a list of IP prefixes), Block-Source* to the USWE instance (see section 12.2.11 for details)
11. The SD-WAN Vendor Manager configures Fault Management on the USWE instance by passing the following information:
   a. Enable fault reporting for each interface on the USWE instance corresponding to an SD-WAN UNI or UCS UNI, and for the USWE instance itself.
   b. The BFD configuration for each UTVC and CTVC is passed by the SD-WAN Vendor Manager to the USWE instance.
   c. Note: Alarm Severity is configured on each USWE instance but may not be able to be configured by the SD-WAN Vendor Manager since Alarm Types supported may be different per USWE implementation.
12. The SD-WAN Vendor Manager configured Performance Monitoring on the USWE instance by passing the following information.
   a. The SD-WAN Vendor Manager passes the values for *Monitored* Entity (UTVC EP, and Performance Metric), *Performance Metric Calculation Instance* and *Performance Metric Calculation Instance Duration Set,* as described in MEF 105 [43] and ping or STAMP parameters as specified in section 12.4 to the USWE instance
13. Enable SD-WAN UNI
   a. The SD-WAN Vendor Manager enables all interfaces that correspond to SD-WAN UNIs on the USWE instance

The SD-WAN Vendor Manager passes the values of a subset of the SD-WAN Service Attributes defined in MEF 70.1 [42] to the USWE instance. Not all the attributes are required to be configured on the USWE instance.

12.2 USWE Configuration Requirements

The USWE configuration, as described above and detailed within this section, includes configuring the USWE physical interfaces, virtual interfaces, and protocol (including routing and IPsec) information for each interface. The USWE is only aware of the configuration of the interfaces and is not aware of what role a given interface is serving in the SD-WAN Edge. Likewise, the information passed from the SD-WAN Vendor Manager to the USWE is expressed in terms of interfaces and protocols and not SD-WAN constructs. In each case, the SD-WAN

Vendor Manager identifies the interface that needs to be configured including creating a logical interface if necessary.

The only exception to what is stated above, is regarding SD-WAN specific attributes such as Application Flow Specifications or SD-WAN Policies.

12.2.1 Create VRFs (Step 1)

The requirements for the instantiation of the UCS, Service Domain, Internet Breakout, and Subscriber Routing Domain on the USWE are defined below.

[R89] An Instance of the SD-WAN Vendor Manager **MUST** pass the UCS VRF attributes to the USWE for each UCS VRF.

[R90] An Instance of the SD-WAN Vendor Manager **MUST** pass the Service Domain VRF attributes to the USWE.

[R91] An Instance of the SD-WAN Vendor Manager **MUST** pass the Internet Breakout VRF attributes to the USWE.

[R92] An Instance of the SD-WAN Vendor Manager **MUST** pass the Subscriber Routing Domain VRF attributes to the USWE.

12.2.2 Synchronization (Step 2)

If synchronization is required by the USWE, the SD-WAN Vendor Manager configures Network timing Protocol (NTP) on the USWE via the Management Plane.

[R93] An instance of the SD-WAN Vendor Manager **MUST** send the NTP configuration to the USWE via the Management Plane to include:

- NTP Server IP Address

It should be noted that in normal operation the USWE requires synchronization for time of day to allow key rollover between the USWE and SD-WAN Edges and alarm correlation. It is not required for notifications since it sends all notifications and PM Metrics to the SD-WAN Vendor Manager where they are expected to be time stamped upon arrival. That time stamp is used for research and reporting.

12.2.3 UCS UNI Interface Configuration (Step 3)

The requirements for the configuration of UCS UNIs on a USWE instance via the Universal Management Plane are defined below.

12.2.3.1 UCS UNI Interface Attribute

The UCS UNI Interface Attribute contains two parameters (Interface Identifier, Interface State) that are supported by the Management Plane. These are not defined in MEF 70.1 [42].

[R94] An Instance of the SD-WAN Vendor Manager **MUST** pass the following UCS UNI interface parameters to the USWE instance:

- Interface Identifier specified as a string e.g., shelf/slot/port, shelf/port/VLAN or sub-interface
- Interface Type
- If a sub-interface is used, the mapping of that sub-interface (including the VLAN Identifier(s)) to the parent-interface
- Interface State
  - *Disabled*

If the interface is Ethernet, the following requirements apply.

[R95] An instance of the SD-WAN Vendor Manager **MUST** pass the following UCS End Point interface parameters to the USWE instance:

- Interface Identifier specified as a string e.g., shelf/slot/port, shelf/port/VLAN or sub-interface
- If a sub-interface is used, the mapping of that sub-interface (including the VLAN Identifier(s)) to the parent-interface
- Interface State
  - *Disabled*

[R96] An instance of the SD-WAN Vendor Manager **MUST** pass the following values of Service Attributes defined in MEF 10.4 [38] section 9.4 to the USWE instance:

- Subscriber UNI List of Physical Links
- Subscriber UNI Maximum Service Frame Size
- Subscriber UNI Maximum Number of EVC EPs
- Subscriber UNI Maximum Number of C-Tag VLAN IDs per EVC EP
- Subscriber UNI Token Share
- Subscriber UNI Envelopes
- EVC EP MAP
- Subscriber UNI Layer 2 Control Protocol Address Set

- Subscriber UNI Layer 2 Control Protocol Peering

In addition to the MEF 10.4 attributes, Auto-Negotiation is specified. This is addressed in the following requirement.

[R97] An instance of the SD-WAN Vendor Manager **MUST** pass the following values for Auto-Negotiation to the USWE instance:

- *Enabled*
- *Disabled*

12.2.3.2 UCS UNI Interface/UCS End Point IPv4 Attributes

The UCS UNI interface IPv4 Attributes that are supported by the Management Plane are defined in this section. The UCS UNI Interface IP Address allocation method is used to describe if the IPv4 Address assigned to the UCS UNI Interface is Static or Dynamic (includes DHCP). If Static, the IPv4 Address of the UCS UNI Interface is passed by the SD-WAN Vendor Manager to USWE instance. If Dynamic and IPv4, the UCS UNI Interface is configured to obtain an IP Address using DHCP. If the UCS is Ethernet, then this text applies to the UCS UNI EPs.

[R98] If the UCS UNI Interface IPv4 Address Type is Static an Instance of the SD-WAN Vendor Manager **MUST** pass the following attributes to the USWE instance:

- Static IP Address (IPv4)
- Subnet Mask
- Default Gateway

[R99] If the UCS UNI Interface IPv4 Address Type is Dynamic, an implementation of the SD-WAN Vendor Manager **MUST** pass the following attributes to the USWE instance:

- DHCP Enabled

A USWE instance then obtains an IPv4 Address for the UCS UNI Interface using DHCP.

12.2.3.3 UCS UNI Interface/UCS End Point IPv6 Attributes

The UCS UNI interface IPv6 Attributes that are supported by the Management Plane are defined in this section. The UCS UNI Interface IP Address allocation method is used to describe if the IPv6 Address assigned to the UCS UNI Interface is Static or Dynamic (includes DHCP and SLAAC,). If Static, the IPv6 Address of the UCS UNI Interface is passed by the SD-WAN Vendor Manager to USWE instance. If Dynamic and IPv6, the UCS UNI Interface is configured to obtain an IP Address using DHCP or SLAAC.

[R100] If the UCS UNI Interface IPv6 Address Type is Static an implementation of the SD-WAN Vendor Manager **MUST** pass the following attributes to the USWE instance:

- Static IP Address (IPv6)
- Subnet Mask
- Default Gateway

[R101] If the UCS UNI Interface IPv6 Address Type is Dynamic, an implementation of the SD-WAN Vendor Manager **MUST** pass the following attributes to the USWE instance:

- DHCP Enabled or
- SLAAC Enabled

A USWE instance then obtains an IPv6 Address for the UCS UNI Interface using DHCP or SLAAC.

12.2.3.4 UCS VRF Assignment

If the UCS is using some type of routing protocol and a VRF for the UCS has been created, the VRF is included in the UCS UNI/UCS EP configuration.

[R102] An implementation of the SD-WAN Vendor Manager MUST pass the VRF assignment for each UCS UNI/UCS EP that is configured.

12.2.3.5 UCS UNI/UCS End Point Interface Routing Protocol Configuration

If the UCS is using some type of routing protocol, the protocol is configured by the SD-WAN Vendor Manager.

[R103] An implementation of the SD-WAN Vendor Manager **MUST** pass the routing protocol attributes (or configuration) for each UCS UNI/UCS EP Interface as agreed on by the Subscriber and the SD-WAN SP to the USWE instance.

12.2.3.6 Enable UCS UNI/UCS EPs

After the UCS UNI Interfaces are configured, the UCS UNI Interfaces are placed into service. If UCS EP interfaces have been configured, they are placed into service also.

[R104] An implementation of the SD-WAN Vendor Manager **MUST** place the UCS UNI Interfaces into service.

12.2.4 Control Plane Configuration (Step 4)

The requirements for the configuration of the Control Plane on a USWE instance via the Universal Management Plane are defined below.

12.2.4.1 Control Tunnel Virtual Connection Interface Configuration

The CTVC, as defined in section 8.2, is configured to carry Control Plane traffic. One or more CTVCs are configured. This process is repeated for each CTVC.

[R105] For each CTVC, an implementation of the SD-WAN Vendor Manager **MUST** pass the following information used for each CTVC to the USWE Instance:

- Interface Identifier specified as a string e.g., shelf/slot/port, shelf/port/VLAN or IPsec Tunnel
- If a sub-interface is used, the mapping of that sub-interface (including the VLAN Identifier(s)) to the parent-interface
- Interface Type is IPsecTunnel
- Interface State
  - *Enabled*

[R106] For each CTVC, an implementation of the SD-WAN Vendor Manager **MUST** pass the value of the CTVC End Point IP Address and prefix length to the USWE instance.

[R107] For each CTVC, an instance of the USWE **MUST** pass the value of the Security Association (SA) (defined in NIST SP 800-77 [47]) key to the implementation of the SD-WAN Vendor Manager.

[R108] For each CTVC, an implementation of the SD-WAN Vendor Manager **MUST** pass the following values of the security parameters (defined in NIST SP 800-77 [47]) to the USWE instance:

- Authentication Method
- Privacy Method
- Key length policy
- Key lifetime

Note: further details on the Authentication Method, Privacy Method, key length policy and key lifetime are found in section 10.

[R109] For each CTVC, an implementation of the SD-WAN Vendor Manager **MUST** send the encryption and hashing algorithms of the CTVC to the USWE instance.

[R110] For each CTVC, the USWE instance **MUST** generate a key pair initially and upon the half-life of the Key Lifetime as notified by the SD-WAN Vendor Manager.

[R111] For each CTVC, the USWE instance **MUST** communicate the public key and the interface name to the SD-WAN Vendor Manager via the Management Plane so that the appropriate SD-WAN Edges can be updated.

[R112] If the UTVC is to be encrypted, upon receipt of a key, the SD-WAN Vendor Manager **MUST** communicate to the USWE the date and time the key will become active (see section 12.2.2 for details about Synchronization), the Interface Name, and the Key Hash

[R113] For each CTVC, an implementation of the SD-WAN Vendor Manager **MUST** pass the UCS UNI interface identifier or the UCS End Point interface identifier for each CTVC interface to the USWE instance.

The DSCP and PCP values are used by the USWE when sending IP Packets for the TVC over the UCS so as to ensure they are mapped to the correct UCS CoS Name as described in section 10.2.

[R114] The SD-WAN Vendor Manager **MUST** pass the DSCP and PCP Value for each CTVC interface to the USWE instance.

Note: other mechanisms that are used to determine the UCS CoS name are out of scope for this version of the Standard.

[R115] The SD-WAN Manger **MUST** pass, for each CTVC interface, the IP Address of the UCS End Point or UCS UNI at the remote end of the CTVC.

[R116] An implementation of the SD-WAN Vendor Manager **MUST** pass the SD-WAN Service VRF to be used for each CTVC End Point to the USWE instance.

12.2.4.2 CPI via Virtual Interface Configuration

If the CTVC End Point is not acting as the CPI, the CPI needs to be created.

[R117] If the CTVC End Point is not acting as the CPI, an implementation of the SD-WAN Vendor Manager **MUST** pass the following information for that interface to the USWE instance:

- Interface Identifier specified as a string e.g., shelf/slot/port, shelf/port/VLAN or sub-interface
- Interface Type

- Interface State
    - *Enabled*

[R118] If the CTVC End Point is not acting as the CPI, an implementation of the SD-WAN Vendor Manager **MUST** pass the SD-WAN Service VRF that the CPI is assigned to the USWE instance.

[R119] If the CTVC End Point is not acting as the CPI, an implementation of the SD-WAN Vendor Manager **MUST** pass the value of the CPI IP address and prefix length to the USWE instance.

12.2.4.3 Define Control Plane iBGP

The SD-WAN Vendor Manager passes the following information regardless of where the CPI is located (CTVC End Point or virtual interface).

[R120] An implementation of the SD-WAN Vendor Manager **MUST** pass the BGP Router ID to the USWE.

[R121] An implementation of the SD-WAN Vendor Manager **MUST** pass to the USWE the Route Distinguisher value for the following VRFs:

- SD-WAN Service Domain VRF
- Subscriber Routing

In the SD-WAN service, there is only one SD-WAN Service Domain VRF, one Subscriber Routing VRF, and a single Internet Breakout VRF. For each of these VRFs, a BGP Route Distinguisher and associated VRF need to be assigned so the USWE can distinguish the routes and IP Packets for each of these VRFs.

[R122] An implementation of the SD-WAN Vendor Manager **MUST** pass to the USWE the following attribute values associated with each VRF:

- BGP AS Number
- Import Route Targets
- Export Route Targets
- Import Route Policy
- Export Route Policy

The Import Route Policy from [R122] is needed to allow for routes to be redistributed from the Forwarding Information Base (FIB).

The Export Route Policy from [R122] is needed to provide which routes from the VRF can be instantiated in the FIB.

[R123] An implementation of the SD-WAN Vendor Manager **MUST** pass the MPLS for each VRF to the USWE.

[R124] An implementation of the SD-WAN Vendor Manager **MUST** pass to the USWE the following values associated with the BGP Peers:

- Peer IP address
- Peer Remote BGP AS-Number
- Peer TCP MD5 Encryption
- Peer Password
- PEER TCP MSS
- Peer Address Families
- Peer VRF Association
- BGP Import Route Policy
- BGP Export Route Policy
- BGP Community Policy
- BGP Path Attributes Policy

The Import Route Policy from [R124] is needed to allow for routes to be accepted from BGP peers.

The Export Route Policy from [R124] is needed to provide which routes from the VRF can be advertised to BGP peers.

The BGP Community Policy and BGP Path Attribute Policy from [R124] are needed so the routes received or exported to BGP Peers can have the appropriate BGP Parameters modified or added.

The BGP parameters and attributes are shown to be set on each individual BGP peer. However, the BGP manageability RFCs 8349 [31] and 8529 [32] show that these can be assigned using Peer Groups. The usage of Peer Groups is not precluded but also not required by this specification.

[D4] The SD-WAN Vendor manager and the USWE **SHOULD** support the BGP attributes and parameters as defined by RFCs 1997 [4], 2385 [7], 4271 [16], 4360 [21], 4364 [22], 4684 [24], and 4893 [26].

There are numerous BGP parameters and attributes defined in RFCs 1997 [4], 2385 [7], 4271 [16], 4360 [21], 4364 [22], 4684 [24], and 4893 [26] which allow for the control of BGP route

advertisement exchange process. Therefore, the SD-WAN Vendor Manager and the USWE need to agree on the parameters that are passed and as such should support the options as defined in the RFCs 1997 [4], 2385 [7], 4271 [16], 4360 [21], 4364 [22], 4684 [24], and 4893 [26].

[R125] An implementation of the SD-WAN Vendor Manager **MUST** use a static route to the USWE CPI IP Address for the SD-WAN Vendor Control Plane.

[R126] An implementation of the SD-WAN Vendor Manager **MUST** pass the static routes to the USWE for the BGP peering addresses of the SD-WAN Vendor Control Plane.

[R127] The SD-WAN Vendor Control Plane **MUST** support securing the iBGP session by using the TCP MD5 signature option as defined by RFC 2385 [7].

[R128] All Universal Control Plane iBGP sessions **MUST** be secured using the TCP MD5.

12.2.5 Universal Tunnel Virtual Connection Configuration (Step 5)

The requirements for the configuration of a UTVC on a USWE instance via the Universal Management Plane are defined below. These requirements are based on the Universal Data Plane description in section 11.

One or more UTVCs are configured. This process is repeated for each UTVCs.

[R129] For each UTVCs, an implementation of the SD-WAN Vendor Manager **MUST** pass the following information used for each UTVCs to the USWE Instance:

- Interface Identifier specified as a string e.g., shelf/slot/port, shelf/port/VLAN or IPsec Tunnel
- If a sub-interface is used, the mapping of that sub-interface (including the VLAN Identifier(s)) to the parent-interface
- Interface Type is IPsecTunnel
- Interface State
  - *Enabled*

[R130] For each UTVCs, an implementation of the SD-WAN Vendor Manager **MUST** pass the value of the UTVCs End Point IP Address and prefix length to the USWE instance.

[R131] If encrypted, for each UTVCs an instance of the USWE **MUST** pass the value of the Security Association (SA) (defined in NIST SP 800-77 [47]) key to the implementation of the SD-WAN Vendor Manager.

[R132] If encrypted, for each UTVC an implementation of the SD-WAN Vendor Manager **MUST** pass the following values of the security parameters (defined in NIST SP 800-77 [47]) to the USWE instance:

- Authentication Method
- Privacy Method
- Key length policy
- Key lifetime

Note: further details on the Authentication Method, Privacy Method, key length policy and key lifetime are found in section 10.

[R133] If encrypted, for each UTVC an implementation of the SD-WAN Vendor Manager **MUST** send the encryption and hashing algorithms of the UTVC to the USWE instance.

[R134] For each CTVC, the USWE instance **MUST** generate a key pair initially and upon the half-life of the Key Lifetime as notified by the SD-WAN Vendor Manager.

[R135] If encrypted, for each UTVC the USWE instance **MUST** communicate the public key and the interface name to the SD-WAN Vendor Manager via the Management Plane so that the appropriate SD-WAN Edges can be updated.

[R136] If the UTVC is to be encrypted, upon receipt of a key, the SD-WAN Vendor Manager **MUST** communicate to the USWE the date and time the key will become active (see section 12.2.2 for details about Synchronization), the Interface Name, and the Key Hash

[R137] For each UTVC, an implementation of the SD-WAN Vendor Manager **MUST** pass the UCS UNI interface identifier or the UCS End Point interface identifier for each UTVC interface to the USWE instance.

The DSCP and PCP values are used by the USWE when sending IP Packets for the TVC over the UCS so as to ensure they are mapped to the correct UCS CoS Name as described in section 10.2.

[R138] The SD-WAN Vendor Manager **MUST** pass the DSCP and PCP Value for each UTVC interface to the USWE instance.

Note: other mechanisms that are used to determine the UCS CoS name are out of scope for this version of the Standard.

[R139] The SD-WAN Manger **MUST** pass, for each UTVC interface, the IP Address of the UCS End Point or UCS UNI at the remote end of the UTVC.

[R140] An implementation of the SD-WAN Vendor Manager **MUST** pass the UCS VRF to be used for each UTVC End Point to the USWE instance.

Note: Each UTVC that is a part of a single SD-WAN Service may have a different configuration. The following requirements apply to each UTVC.

12.2.6 GRE Tunnel Configuration

The Interface Name, GRE Tunnel, GRE Protocol Type = 0x8847 and MPLS Label associated with the SD-WAN Service Routing and the Subscriber Routing Domain are passed to the USWE instance by the SD-WAN Vendor Manager.

[R141] An implementation of the SD-WAN Vendor Manager MUST pass the GRE Tunnel Identifier, the GRE Tunnel IP Address and prefix, and the GRE Protocol Type = 0x8847.

[R142] An implementation of the SD-WAN Vendor Manager **MUST** pass the UTVC Interface Name, the GRE Interface Name, and MPLS Label associated with the SD-WAN Service Routing Domain to the USWE instance.

[R143] An implementation of the SD-WAN Vendor Manager **MUST** pass the Interface Name, the GRE Interface Name, and MPLS Label associated with the Subscriber Routing Domain to the USWE instance.

[R144] An implementation of the SD-WAN Vendor Manager **MUST** pass the Interface Name, the GRE Interface Name, and MPLS Label associated with the Internet Breakout Routing Domain to the USWE instance.

12.2.7 SD-WAN UNI Configuration (Step 6)

The requirements for the configuration of an SD-WAN UNI on a USWE instance via the Universal Management Plane are defined below.

12.2.7.1 SD-WAN UNI Interface Attributes

The SD-WAN UNI interface configuration is defined in this section.

[R145] An implementation of the SD-WAN Vendor Manager **MUST** pass the following interface attributes values to the USWE instance for each SD-WAN UNI interface:

- Interface Identifier specified as a string e.g., shelf/slot/port, shelf/port/VLAN or sub-interface
- If a sub-interface is used, the mapping of that sub-interface (including the VLAN Identifier(s)) to the parent-interface
- Interface State
  - *Disabled*

[R146] An implementation of the SD-WAN Vendor Manager **MUST** send to the USWE instance the value for the following SD-WAN UNI Interface Service Attributes:

- SD-WAN UNI L2 Interface
- SD-WAN UNI Maximum Frame Size

12.2.7.2 SD-WAN UNI Interface IPv4 Attributes

The SD-WAN UNI interface IPv4 Attributes that are supported by the Management Plane are defined in this section. The SD-WAN UNI Interface IP Address allocation method is used to describe if the IPv4 Address assigned to the SD-WAN UNI Interface is Static or Dynamic (includes DHCP, SLAAC, and None). If Static, the IPv4 Address of the SD-WAN UNI Interface is passed by the SD-WAN Vendor Manager to USWE instance. If Dynamic and IPv4, the SD-WAN UNI Interface is configured to obtain an IP Address using DHCP.

[R147] If the SD-WAN UNI Interface IPv4 Address Type is Static an implementation of the SD-WAN Vendor Manager **MUST** pass the following attributes values to the USWE instance:

- Static IP Address (IPv4)
- Subnet Mask
- Default Gateway IP Address

[R148] If the SD-WAN UNI Interface IPv4 Address Type is Dynamic, an implementation of the SD-WAN Vendor Manager **MUST** pass the following attributes to the USWE instance:

- DHCP Enabled

A USWE instance then obtains an IPv4 Address for the SD-WAN UNI Interface using DHCP.

12.2.7.3 SD-WAN UNI Interface IPv6 Attributes

The SD-WAN UNI interface IPv6 Attributes that are supported by the Management Plane are defined in this section. The SD-WAN UNI Interface IP Address allocation method is used to describe if the IPv6 Address assigned to the SD-WAN UNI Interface is Static or Dynamic (includes DHCP, SLAAC, and None). If Static, the IPv6 Address of the SD-WAN UNI Interface is passed by the SD-WAN Vendor Manager to USWE instance. If Dynamic and IPv6, the SD-WAN UNI Interface is configured to obtain an IP Address using DHCP or SLAAC.

[R149] If the SD-WAN UNI Interface IPv6 Address Type is Static an implementation of the SD-WAN Vendor Manager **MUST** pass the following attributes values to the USWE instance:

- Static IP Address (IPv6)
- Subnet Mask
- Default Gateway IP Address

[R150] If the SD-WAN UNI Interface IPv6 Address Type is Dynamic, an implementation of the SD-WAN Vendor Manager **MUST** pass the following attributes to the USWE instance:

- DHCP Enabled or
- SLAAC Enabled

A USWE instance then obtains an IPv6 Address for the SD-WAN UNI Interface using DHCP or SLAAC.

12.2.8 Subscriber Routing Configuration (Step 7)

After the Subscriber Routing Domain VRF has been added, the Subscriber Routing configuration includes the following steps and requirements.

The requirements for including each SD-WAN UNI in the Subscriber Routing Domain are below.

[R151] The SD-WAN Vendor Manager **MUST** pass the Interface ID for each SD-WAN UNI to the USWE to be included in the Subscriber Routing Domain VRF.

If the routing is static, the requirements for the configuration of static Subscriber routing are defined below.

[R152] When configuring a static route, the Subscriber Routing Domain VRF **MUST** be configured with the following:

- IP Prefix
- Nexthop Interface ID or IP address
- Admin distance

If the routing is BGP, the requirements for the configuration of BGP Subscriber routing are defined below.

[R153] An implementation of the SD-WAN Vendor Manager **MUST** pass to the USWE the following values associated with the Subscriber Routing Domain BGP Peers:

- Peer IP address
- Peer Remote BGP AS-Number
- Peer TCP MD5 Encryption
- Peer Password

- PEER TCP MSS
- Peer Address Families
- Peer VRF Association
- BGP Import Route Policy
- BGP Export Route Policy
- BGP Community Policy
- BGP Path Attributes Policy

12.2.9 Application Flow Specification (Step 8)

The requirements for the configuration of an Application Flow Specifications on a USWE instance via the Universal Management Plane are defined below.

[R154] The SD-WAN Vendor Manager **MUST** pass to the USWE the list of *<AFName, AFCritList>* pairs corresponding to the value of the Service Attribute in MEF 70.1 [40].

12.2.10 Zone (Step 9)

The requirements for the configuration of Zones on a USWE instance via the Universal Management Plane are defined below.

[R155] The SD-WAN Vendor Manager **MUST** pass Zone Name and Zone Prefixes (defined in MEF 70.1 [40] sec 9.6) to the USWE instance for each Zone.

12.2.11 Configure SD-WAN Service End Point Policy Map (Step 10)

The values for each SD-WAN Service Policy Map are passed to the USWE instance by the SD-WAN Vendor Manager.

The SD-WAN Vendor Manager evaluates the attributes and policy criteria and uses those to determine which UTVCs the Application Flow can be forwarded over. Some policy criteria can only be evaluated by the USWE and values for these are passed to the USWE by the SD-WAN Vendor Manager. The passed policy criteria values include Internet Breakout, Allowed Destination IP Prefixes, Bandwidth Limits, and Block-Source. Other policy criteria and their values are not passed to the USWE and are implemented within the SD-WAN Vendor Manager. Each of the policy criteria that are passed to the USWE are discussed below.

Internet Breakout is a Boolean that indicates if it is *ENABLED* (IP packets in the Application Flow are routed to the Internet) or *DISABLED* (IP packets in the Application Flow are not routed to the Internet). The SD-WAN Vendor Manager determines whether each Application Flow should be forwarded towards the Internet or towards another SD-WAN UNI.

Note: If Internet Breakout is set to *ENABLED*, the Internet Breakout VRF is used for the lookup for local or remote Internet Breakout. For remote Internet Breakout, the Data Plane uses the MPLS Label received from the Vendor Control Plane that indicates that the IP Packet is using the Internet VRF. If Internet Breakout is set to False the Subscriber VRF is used for the lookup and the MPLS Label indicates that the IP Packet is using the Subscriber VRF.

Allowed Destination Zones identify the Zones that an ingress IP packet can be delivered to. The SD-WAN Vendor Manager determines which Zones the Application Flow needs to be able to forward IP packets to and passes the destination Zone Name(s) to the USWE.

Note: The Block-Source is shown as a Boolean for the purposes of this document. The Block Source value is set to *TRUE* if either of the following conditions hold; otherwise it is set to *FALSE*:

- The Zone name for the Egress Application Flow to which the Policy is being applied is the reserved value *Internet* and the Block-Source Policy Criterion as defined in MEF 70.1 [42] includes the value *INTERNET*

- The Zone name for the Egress Application Flow to which the Policy is being applied is not the reserved value *Internet* and the Block-Source Policy Criterion as defined in MEF 70.1 [42] includes the value *UNI*

The list of UTVC EPs identifies a list of UTVCs that the Application Flow may use to transit to another SD-WAN Edge. The acceptable list of UTVC End Points is passed by the SD-WAN Vendor Manager to the USWE.

[R156] An Instance of the SD-WAN Vendor Manager **MUST** pass the values of the following attributes and policy criteria for each Application Flow to the USWE instance:

- Three tuple identifying the Application Flow (*SD-WAN UNI Interface* i.e., the interface identifier of the interface acting as an SD-WAN UNI, *Application Flow Specification* specifically, one of the AFName values passed in section 12.2.8, *Zone Name* specifically, one of the Zone Names passed in section 12.2.10)

- List of *UTVC Interface IDs* that can be used for forwarding this Application Flow. This may be provided in order of preference if a performance policy criteria is applied to this Application Flow.

- *Internet Breakout (Boolean)*

- *Allowed Destination Zones*

- *Bandwidth limit on Application Flow*

- *Block-Source (Boolean)*

[R157] The SD-WAN Vendor Manager **MUST** pass the *irduration* value from the SWVC Performance Time Intervals Service Attribute to the USWE.

Note: The SD-WAN Vendor Manager determines if an Application Flow is meeting the Performance Criteria defined for the Application Flow and if a UTVC is not meeting performance criteria, it updates the list of *UTVC Interface IDs* to change the preference of UTVCs.

Bandwidth sharing between AFs, which is based on Application Flow Groups, is outside the scope of this document.

12.3 Fault Management (Step 11)

Fault Management, defined in section 11.3, addresses managing faults that occur on the USWE instance. Fault Management includes areas such as detecting faults on the USWE instance and software, Loss of Signal on UCSs and SD-WAN UNIs, and Bidirectional Forwarding Detection.

[R158] An Instance of the SD-WAN Vendor Manager **MUST** subscribe to all severity levels of alarms that are sent by the USWE from the severities shown below:

- *Warning*
- *Minor*
- *Major*
- *Critical*

Note: the definition of each severity is found in ITU-T X.733 [37].

[R159] An implementation of the SD-WAN Vendor Manager **MUST** configure BFD parameters on each UTVC or CTVC interface as defined below:

- BFD Transmission Interval – 100-300ms
- Detect Multiplier – 3
- DSCP Value – Match UTVC DSCP settings
- Severity – as defined by the SP

12.3.1 Fault Retrieval

The SD-WAN Vendor Manager has the ability to retrieve current and historical faults from the USWE instance.

[R160] The USWE **MUST** provide the SD-WAN Vendor Manager with the ability to retrieve faults from the USWE.

[R161] When retrieving faults, the SD-WAN Vendor Manager **MUST** provide the start date, end date, fault type (zero or more), and fault severity (zero or more) to the USWE instance.

[R162] A USWE instance **MUST** include the Fault Notification Attributes shown in 11.3 for each fault returned in response to the SD-WAN Vendor Manager's request.

[D5] A USWE instance **SHOULD** store faults and their associated attributes for at least 24 hours.

12.4 Performance Monitoring (Step 12)

The requirements for the configuration of Performance Monitoring (PM) on a USWE instance via the Universal Management Plane are defined below.

[R163] An Instance of the SD-WAN Vendor Manager **MUST** send the list of (UTVC Interface ID, Performance Metric) pairs to be monitored to the USWE instance.

[R164] An Instance of the SD-WAN Vendor Manager **MUST** send the values of the Performance Metric Calculation Interval Duration, as described in MEF 105 [43], to the USWE instance.

[R165] For each UTVC being monitored an Instance of the SD-WAN Vendor Manager **MUST** pass the following Ping values to the USWE instance:

- Unicast Destination Address of remote TVC End Point
- Time Interval between Ping messages
- Ping packet length
- Number of packets (integer or indefinitely)

[R166] For each UTVC being monitored using STAMP, An Instance of the SD-WAN Vendor Manager **MUST** pass the STAMP values defined in MEF 66 [40] to the USWE instance.

The SD-WAN Vendor Manager collects PM Metric values or byte-counter values from the USWE and generates reports based on the values collected. Threshold Crossing Alerts are also generated by the SD-WAN Vendor Manager based on PM Metric values received from the USWE.

The retrieval of SD-WAN Performance Monitoring Metrics and byte-counters is the responsibility of the SD-WAN Vendor Manager. The SD-WAN Vendor Manager retrieves the metric values and values of the counters from the USWE instance.

[R167] For each UTVC being monitored, the SD-WAN Vendor Manager **MUST** retrieve the PM Metric values and/or the byte-counter values from the USWE instance.

Threshold Crossing Alerts (TCAs) are Performance Monitoring based notifications of events that have occurred when Performance Metrics either exceed a specified threshold which causes the event to be declared or are below a specified threshold which causes the event to be cleared. The processing of Performance Metrics to generate or clear TCAs is the responsibility of the SD-WAN Vendor Manager based on data received by the SD-WAN Vendor Manager from the USWE.

[R168] The SD-WAN Vendor Manager **MUST** have the ability to support TCAs as defined in MEF 105 [43].

The configuration of the SD-WAN Vendor Manager to support TCAs is beyond the scope of this document.

12.5 Enable SD-WAN UNI (Step 13)

The SD-WAN Vendor Manager enables all SD-WAN UNIs on the USWE after all other steps are completed.

[R169] An Instance of the SD-WAN Vendor Manager **MUST** send to the USWE instructions to enable each interface on the USWE that is acting as an SD-WAN UNI.

12.6 Notifications

Notifications include Fault Notifications and Performance Notifications. Notifications are pushed from the USWE to the SD-WAN Vendor Manager via the Management Plane.

The SD-WAN Vendor Manager subscribes to notifications.

[R170] The SD-WAN Vendor Manager **MUST** subscribe to notifications on the USWE instance providing the following information:

- Notification Type (*Fault Notification, Public Key Notification*)

The method used to deliver notifications to the SD-WAN Vendor Manager is outside the scope of this document.

[R171] If the Notification Type *is Fault Notification*, then the USWE **MUST** send the fault as defined in section 11.3.

[R172] If the Notification Type is *Public Key Notification*, the notification sent to the SD-WAN Manager **MUST** include the following:

- *UTVC/CTVC Identifier*
- *Public Key*

12.7 Hardware or Virtual Machine Management

While the USWE application does not specifically need to manage the hardware or virtual machine platform it is configured on, the SD-WAN Vendor Manager may need to configure the hardware or virtual machine platform. It is recommended that IETF RFC 7317 [28] be reviewed and supported for these tasks.

13 References

[1] IETF RFC 791, *Internet Protocol*, by J. Postel, September 1981

[2] IETF RFC 792, *Internet Control Message Protocol*, by J. Postel, September 1981

[3] IETF RFC 1701, *Generic Routing Encapsulation*, S. Hanks, T. Li. D. Farinacci, P. Traina, October 1994

[4] IETF RFC 1997, *BGP Communities Attributes*, by R. Chandra, P. Traina, T. Li, August 1996

[5] IETF RFC 2119, *key words for use in RFCs to Indicate Requirement Levels*, by S. Bradner, March 1997

[6] IETF RFC 2131, *Dynamic Host Configuration Protocol*, R. Droms, March 1997

[7] IETF RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*, A. Heffernan, August 1993, Copyright (C) The Internet Society (1998). All Rights Reserved

[8] IETF RFC 2451, *The ESP CBC-Mode Cipher Algorithms*, by R. Pereira, R. Adams, November 1998, Copyright (C) The Internet Society (1998). All Rights Reserved

[9] IETF RFC 2663*, IP Network Address Translator (NAT) Terminology and Considerations*, P. Sirsuresh, M. Holdrege, August 1999, Copyright (C) The Internet Society (1999). All Rights Reserved.

[10] IETF RFC 2784, *Generic Routing Encapsulation (GRE)*, D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, March 2000, Copyright (C) The Internet Society (2000). All Rights Reserved.

[11] IETF RFC 3032, *MPLS Label Stack Encoding*, by E. Rosen, D. Tappan, G. Federkow, Y. Rekhter, D. Farinacci, T. Li, A. Contra, January 2001, Copyright (C) The Internet Society (2001). All Rights Reserved.

[12] IETF RFC 3602, *The AES CBC-Cipher Algorithm and Its Use with IPsec*, by S. Frankel, R. Glenn, S. Kelly, September 2003, Copyright (C) The Internet Society (2003). All Rights Reserved.

[13] IETF RFC 3948, *UDP Encapsulation of IPsec ESP Packets*, by A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg, January 2005, Copyright (C) The Internet Society (2005).

[14] IETF RFC 4023, *Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)*, by T. Worster, Y. Rekhter, E. Rosen, Ed., March 2005, Copyright (C) The Internet Society (2005).

[15] IETF RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulation Security Protocol (ESP)*, by J. Viega, D. McGrew, June 2005, Copyright (C) The Internet Society (2005).

[16] IETF RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*, by Y. Rekhter, T. Li, S. Hares, January 2006, Copyright (C) The Internet Society (2006).

[17] IETF RFC 4291, *IP Version 6 Addressing Architecture*, by R. Hinden, S. Deering, February 2006, Copyright (C) The Internet Society (2006)

[18] IETF RFC 4301, *Security Architecture for the Internet Protocol*, by S. Kent, K.Seo, December 2005, Copyright (C) The Internet Society (2005).

[19] IETF RFC 4303, *IP Encapsulating Security Payload (ESP)*, by S. Kent, December 2005, Copyright (C) The Internet Society (2005).

[20] IETF RFC 4308, *Cryptographic Suites for IPsec*, by P. Hoffman, December 2005, Copyright (C) The Internet Society (2005).

[21] IETF RFC 4360, BGP Extended Communities Attribute, by S. Sangli, D. Tappan, Y. Rekhter, February 2006, Copyright (C) The Internet Society (2006).

[22] IETF RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*, E. Rosen, Y. Rekhter, February 2006, Copyright (C) The Internet Society (2006).

[23] IETF RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*, by A.Conta, S. Deering, M. Gupta, March 2006, Copyright (C) The Internet Society (2006).

[24] IETF RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*, P. Marques, R. Bonica, L. Fang, L. Martini, R. Razsuk, K. Patel, J. Guichard, November 2006, Copyright (C) The IETF Trust (2006)

[25] IETF RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*, by S. Kelly, S. Frankel, May 2007, Copyright (C) The IETF Trust (2007).

[26] IETF RFC 4893, *BGP Support for Four-octet AS Number Space*, Q. Vohra, E. Chen, May 2007, Copyright (C) The IETF Trust (2007)

[27] IETF RFC 5880, *Bidirectional Forwarding Detection*, D. Katz, D. Ward, June 2010, Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

[28] IETF RFC 7317, *A YANG Data Model for System Management*, A. Bierman, M. Bjorklund, August 2014, Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

[29] IETF RFC 8174, *Ambiguity of Uppercase vs Lowercase in RFC 2119 key Words*, by B. Leiba, May 2017, Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

[30] IETF RFC 8221, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*, by P. Wouters, D. Migault, J. Mattsson, Y. Nir, T. Kivinen, October 2017, Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

[31] IETF RFC 8349, *A YANG Data Model for Routing Management (NMDA Version)*, by L. Lhotka, CZ. NIC, A. Lindem, Y. Qu, March 2018, Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

[32] IETF RFC 8529, *YANG Data Model for Network Instances*, by L. Berger, C. Hopps, A. Lindem, D. Bogdanovic, X. Liu, March 2019, Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

[33] IETF RFC 8572, *Secure Zero Touch Provisioning (SZTP)*, by K. Watsen, I. Farrer, M. Abrahamsson, April 2019, Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

[34] IETF RFC 8762, *Simple Two-way Active Measurement Protocol (STAMP)*, by G. Mirsky, G. Jun, H. Nydell, R. Foote, March 2020, Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

[35] IETF RFC 9026, *Multicast VPN Fast Upstream Failover*, T. Morin, Ed., R. Kebler, Ed., G. Mirsky, April 2021

[36] ISO 8601-1:2019, *Date and time — Representations for information interchange — Part 1: Basic rules*

[37] ITU-T Recommendation X.733, *Information technology – Open Systems Interconnection – Systems Management: Alarm reporting function*, March 1999

[38] MEF 10.4, *Subscriber Ethernet Service Attributes*, December 2018

[39] MEF 35.1, *Service OAM Performance Monitoring Implementation Agreement*, May 2015

[40] MEF 66, *SOAM for IP Services*, July 2020

[41] MEF 69.1, *Subscriber IP Service Definitions*, February 2022

[42] MEF 70.1, *SD-WAN Service Attributes and Service Framework*, November 2021

[43] MEF 105, *Performance Monitoring and Service Readiness Testing for SD-WAN*, April 2024

[44] NIST FIPS 197 upd1, *Advanced Encryption Standard (AES)*, May 9, 2023

[45] NIST SP 800-56A, Revision 3, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, April 2018

[46] NIST SP 800-57, Part 1, Revision 5, *Recommendation for key Management: Part 1-General*, May 2020

[47] NIST SP 800-77, *Guide to IPsec VPNs*, June 2020

Appendix A Acknowledgements (Informative)

Mike **BENCHECK**

Neil **DANILOWICZ**

Federica Maria **MANINI**

Basil **NAJEM**

Jack **PUGACZEWSKI**

Ettore **PULIERI**

Richard **TAYLOR**