MEF Standard

MEF 69.1

Subscriber IP Service Definitions

February 2022

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 MEF Forum (MEF) is not responsible for any errors. MEF does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by MEF concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by MEF 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. MEF 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 MEF member which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

b) any warranty or representation that any MEF 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 MEF member and the recipient or user of this document.

Implementation or use of specific MEF standards, specifications, or recommendations will be voluntary, and no Member shall be obliged to implement them by virtue of participation in MEF Forum. MEF is a non-profit international organization to enable the development and worldwide adoption of agile, assured and orchestrated network services. MEF 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 the MEF participated in the development of this document and have requested to be included in this list.

- Bell Canada
- China Telecom
- Cisco
- Nokia
- Spirent
- TELUS
- Zayo

2 Abstract

This standard defines Internet Protocol (IP) Services by imposing constraints on certain MEF 61.1 [8] Service Attributes and parameters. An IP Service provides Layer 3 connectivity, the routing of IP Packets, to and from one or more Subscriber sites. Two types of IP Services are defined in this standard, two Internet Access Services (Basic and Advanced), and two Subscriber Internet Protocol Virtual Private Network (IP VPN) Services (Intranet and Extranet). These two service types provide public and private connectivity respectively to Subscribers who purchase these services from Service Providers. This standard supersedes and replaces MEF 69 [10].

3 Terminology and Abbreviations

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

In addition, terms defined in MEF 23.2 [7] and MEF 61.1 [8] are included in this document by reference and are not repeated in the table below.

Term	Definition	Reference
Advanced Internet Access Service	A Subscriber Internet Access service that is typically delivered to business locations and designed for reliability and monitoring.	This document
Basic Internet Access Service	A Subscriber Internet Access service that is typically delivered to Subscriber dwellings, and designed for low-cost, ease of use.	This document
DHCP	Dynamic Host Configuration Protocol.	RFC 2131 [3]
Dynamic Host Configuration Protocol	A protocol that provides a framework for passing configuration information to hosts on a TCP/IP network.	RFC 2131 [3]
Internet Access Service	A connectivity service where a single IPVC is used to connect an IP external interface to the Internet.	This document
Internet Service Provider	A Service Provider that offers Internet Access services.	This document
Internet Protocol Virtual Private Network Service	A connectivity service where a single IPVC is used to interconnect an agreed set of IP external interfaces.	This document
IP VPN	Internet Protocol Virtual Private Network.	This document
ISP	Internet Service Provider.	This document
MPD	Mean Packet Delay.	This document
PDR	Packet Delay Range.	This document
Performance Tier	A set of CPOs and associated parameters that define the expected performance experienced by IP VPN service flows.	This document
PT	Performance Tier.	This document
Subscriber Internet Access Service	An Internet Access Service provided by an ISP to a Subscriber.	This document
Subscriber IP VPN Extranet Service	A connectivity service where a single IPVC is used to interconnect an agreed set of IP UNIs belonging to different Subscribers.	This document
Subscriber IP VPN Intranet Service	A connectivity service where a single IPVC is used to interconnect an agreed set of IP UNIs for a single Subscriber.	This document

Term	Definition	Reference
Subscriber IP VPN Service	A connectivity service where a single IPVC that is provided by a Service Provider to one or more Subscribers is used to interconnect an agreed set of IP UNIs.	This document

Table 1 – Terminology and 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 [2], RFC 8174 [6]) 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**.**

A paragraph preceded by **[CR*a*]<** 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 **[CD*b*]<** specifies a Conditional Desirable Requirement that **SHOULD** be followed if the condition(s) following the "<" have been met. A paragraph preceded by **[CO*c*]<** specifies a Conditional Optional Requirement that **MAY** be followed if the condition(s) following the "<" have been met.

5 Numerical Prefix Conventions

This document uses the prefix notation to indicate multiplier values as shown in Table 2.

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 2 – Numerical Prefix Conventions

6 Introduction

This standard defines IP Services constructed using the Service Attributes defined in MEF 61.1 [8], where certain Service Attribute values have been constrained as per this standard. These services provide public and private connectivity respectively to Subscribers who purchase these services from Service Providers. Four IP Services are defined in this standard. Section 7 provides a description and Section 9 normatively defines two Internet Access Services (Basic and Advanced). Section 8 provides a description and Section 10 normatively defines two Subscriber IP VPN Services (Intranet and Extranet). Appendix A provides informative use cases of IP Services. Appendix A.4 provides guidelines for the use of Fault Management and Performance Management functions in IP VPN services. Appendix B provides an outline of the major changes introduced in this standard superseding MEF 69 [10].

This standard assumes the reader is familiar with MEF 61.1 [8] content that is not repeated here.

7 Subscriber Internet Access Services

This standard defines two Internet Access Services, Basic Internet Access, and Advanced Internet Access which are purchased by a Subscriber from an Internet Service Provider (ISP).

Figure 1 shows an example of an Internet Access Service. A Service Provider (SP) offers connectivity to the Internet to a Subscriber with this service. The SP that offers this service is defined as an Internet Service Provider (ISP). An IPVC used for an Internet Access Service provides the Subscriber with connectivity to the Internet via an IP UNI between the ISP and the Subscriber. The IPVC provides Internet access for the Subscriber Network connected at that UNI.

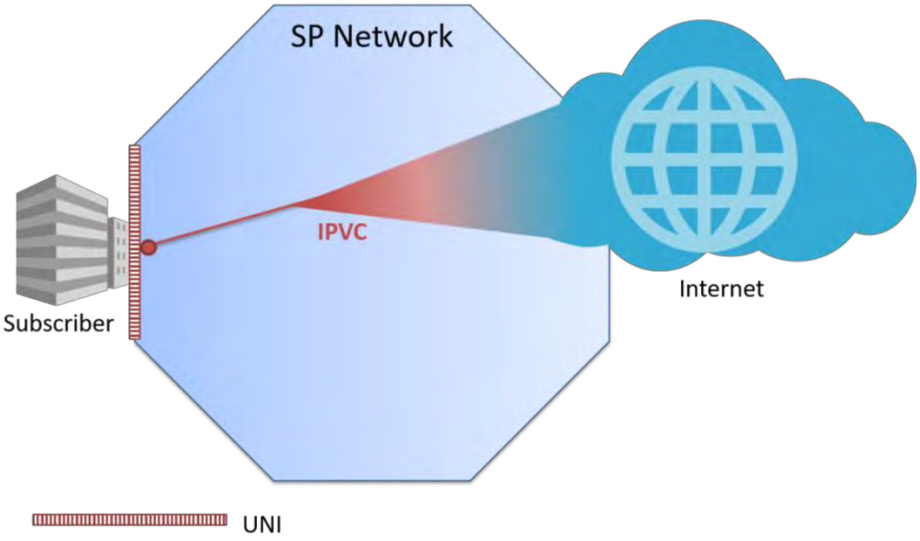

Figure 1 – Subscriber Internet Access Service

Services providing access to the Internet are available in many forms. This standard defines a subset of these services, where:

- The primary service requested by the Subscriber is Internet Access.
- The Internet service is provided to the Subscriber's site, which is a fixed location.

The ISP may offer IPv4 routing, IPv6 routing or both. An Internet access service can include Network Address Translation (NAT) to enable the Subscriber to use private IP addresses within their networks.

Internet Access Services may include a Bandwidth Profile (BWP), defined in MEF 61.1 [8], which governs the temporal properties of IP packets at the UNI. The Subscriber observes the outcome of this BWP as a metering of the traffic rate of IP flows carried by the Internet Access Service. The value of this metering rate is agreed between the Subscriber and ISP and applied by conditioning functions in ISP equipment (e.g., traffic shapers, traffic policers). This is often referred to as the "Service Speed". It may be expressed as two speeds: one in the downstream direction towards the Subscriber, one in the upstream direction from the Subscriber. If a BWP doesn't exist the achievable traffic rate of the service is opaque to the Subscriber, and governed only by the capacity of the media upon which the UNI is constructed, which may not be dedicated to the Subscriber.

MEF 61.1 [8] defines Bandwidth Profile Flows and Bandwidth Profile Envelopes each of which can be used in multiples to produce IP Services with differentiated classes of service. The Internet Access Services defined in this standard have only a single Bandwidth Profile Flow and Bandwidth Profile Envelope, as all traffic flows delivered by the service have equal treatment.

Two types of Internet Access Service can be offered: Basic and Advanced. The possible values for certain Service Attributes differ between these two types. Basic Internet Access is typically delivered to Subscriber dwellings. It may be offered to small/medium businesses. Its service characteristics typically include:

- plug-and-play ease of use
- low-cost
- For IPv4, a few (or shared) publicly routed addresses

Advanced Internet Access is typically delivered to business locations. Its service characteristics include:

- redundancy features
- dynamic routing protocol support (e.g., BGP [4] routing)
- options for Subscriber-supplied IP addressing
- proactive monitoring to support a Service Level Specification (SLS)

Both Basic and Advanced Internet Access Services are normatively defined in Section 9.

8 Subscriber IP VPN Services

A Subscriber IP VPN Service is an Internet Protocol Virtual Private Network Service (IP VPN) service that is provided by a Service Provider to one or more Subscribers.

This standard defines two Subscriber IP VPN Services:

- Subscriber IP VPN Intranet
- Subscriber IP VPN Extranet

For both Subscriber IPVN Intranet and Extranet Services, the SP may offer IPv4 routing, IPv6 routing or both.

8.1 Subscriber IP VPN Intranet Service

A Subscriber IP VPN Intranet Service is a connectivity service where a single IPVC is used to interconnect an agreed set of IP UNIs belonging to a single Subscriber. With this service, a Service Provider (SP) offers connectivity between several parts of a Subscriber Network, typically in different physical locations, to create a single virtual network. It is a private service, where traffic is segregated from other Subscribers and the Internet.

Figure 2 below shows examples of Subscriber IP VPN Intranet Services delivered over a single SP's network. A Subscriber, *Bank of MEF,* has four network locations, one head office, two branch offices and a data center. All branch offices and the data center have connectivity to the head office. IPVC1 allows the two branch offices to communicate with each other and the head office. IPVC2 provides a separate connection to the head office for the data center, ensuring the branch offices and data center cannot communicate directly with each other. A second Subscriber, *Acme Printing*, also subscribes to a Subscriber IP VPN Intranet service, for connectivity between a head office and a branch office shown as "IPVC 3". Connectivity between these two Subscribers is segregated within the SP Network, for security reasons, making it possible for overlapping IP address space to exist between the two Subscribers without routing conflicts.

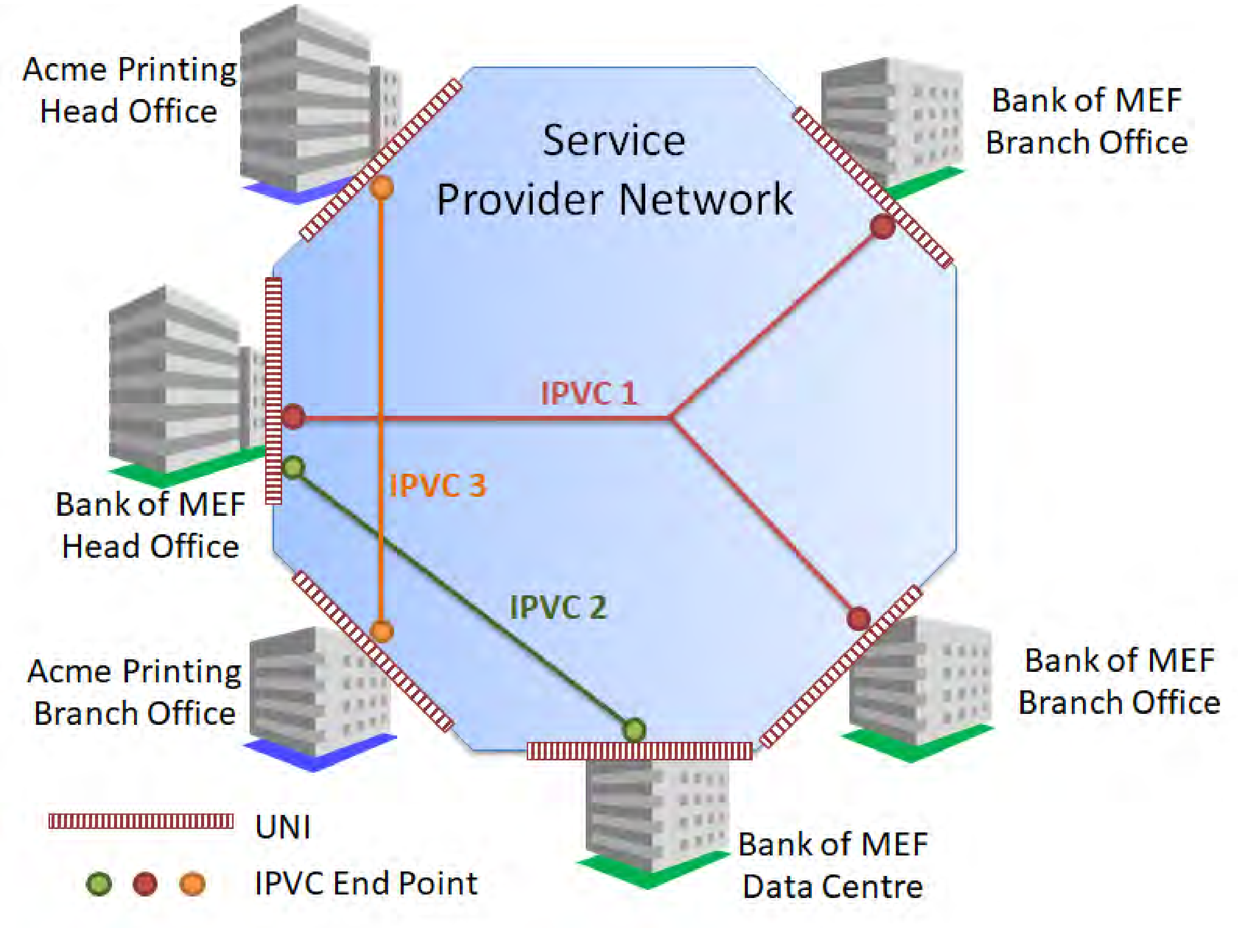

Figure 2 – Examples of Subscriber IP VPN Intranet Services

Subscriber IP VPN Intranet services are Virtual Private Network services constructed using the Service Attributes defined in MEF 61.1 [8] where certain Service Attribute values have been constrained as per this standard.

8.2 Subscriber IP VPN Extranet Service

A Subscriber IP VPN Extranet Service is a connectivity service where a single IPVC is used to interconnect an agreed set of IP UNIs belonging to different Subscribers. With this service an SP offers connectivity between at least two different Subscriber networks. It is a private service, where traffic is segregated from other Subscribers and the Internet.

Figure 3 below shows an example of an IPVC for the Extranet Service. The Extranet IPVC shown in this figure has IPVC EPs at all *Bank of MEF's* UNIs and at the *Acme Printing* head office UNI. In this example, connectivity is constrained for the Extranet IPVC, such that IP packets can only flow between the *Acme Printing's* Head Office IPVC EP and one or more of the *Bank of MEF's* IPVC EPs. This means that connectivity is not allowed between *Bank of*

MEF IPVC EPs associated with the Extranet IPVC. If such connectivity is desired by *Bank of MEF*, then the *Bank of MEF's* IPVC is used.

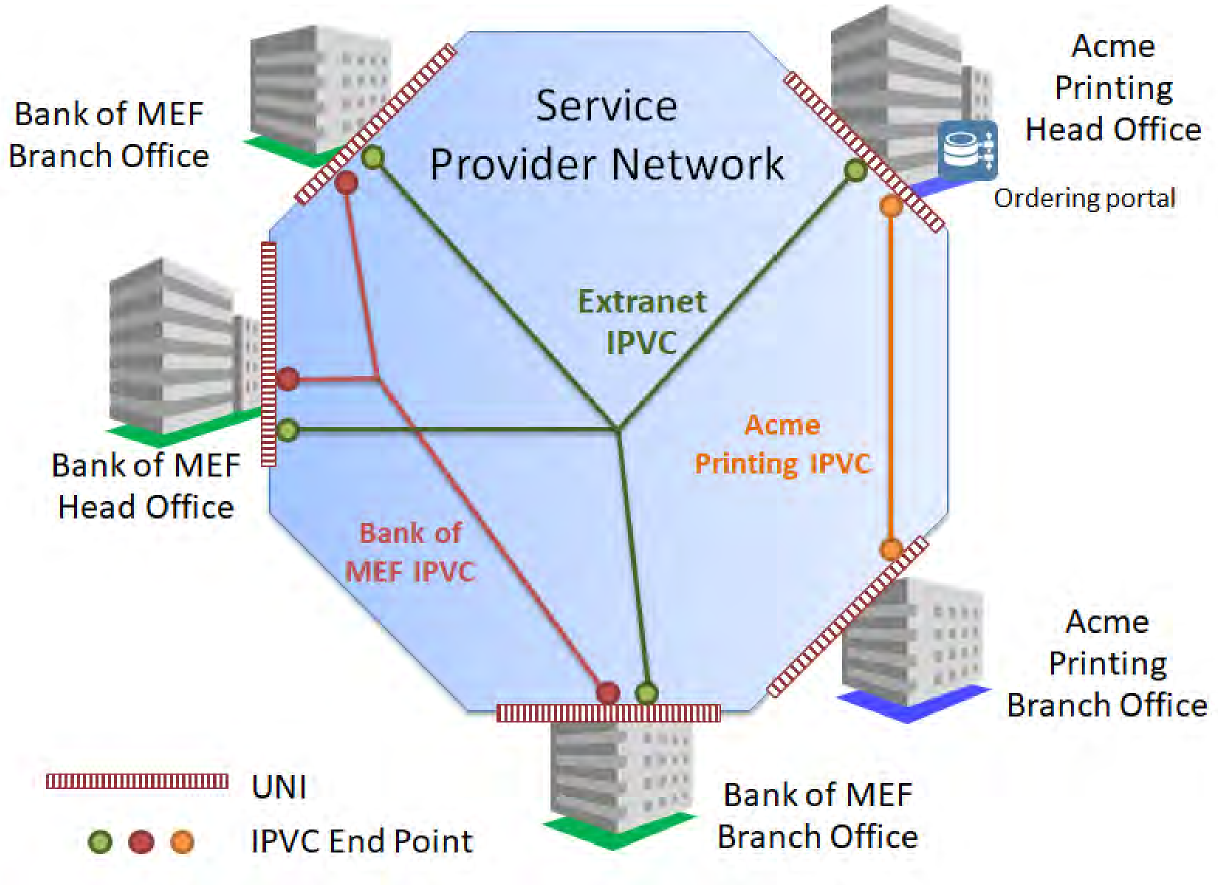

Figure 3 – Example of an Extranet Subscriber IP VPN Service

The Extranet IPVC is not used to provide connectivity between endpoints of the same Subscriber. IP Flows carried across an Extranet IPVC should ingress an IPVC EP belonging to one Subscriber, and egress an IPVC EP belonging to a different Subscriber.

Subscriber IP VPN Extranet services are Virtual Private Network services constructed using the Service Attributes defined in MEF 61.1 [8] where certain Service Attribute values have been constrained as per this standard.

8.3 IP VPN Class of Service Model

MEF 61.1 [8] specifies the IPVC EP Ingress Class of Service Map Service Attribute for associating each ingress packet with a Class of Service Name (CoS Name). This Standard defines three specific CoS Names called Class of Service Labels (CoS Labels). This three CoS Label model is based upon a similar model for Carrier Ethernet as specified in MEF 23.2 [7]. Since Carrier Ethernet services can be used as IP Attachment Circuits, having a similar model could help to achieve consistent treatment of traffic at all IPVC EPs in the IPVC. Additionally, MEF 61.1 [8] suggests avoiding using the standard DSCP names as CoS Names in the IPVC List of Class of Service Names Service Attribute, thus, they are not used as CoS Labels in this standard.

The CoS Label Model provides normative information for three CoS Labels (H, M and L) and a set of CoS Performance Objectives (CPOs) for each CoS Label. An IP VPN SP may choose to offer none, some, or all 3 CoS Labels, as well as their own CoS Names.

CoS Labels H, M and L informally refer to High, Medium and Low, and are differentiated by their performance requirements.

- H – intended for applications that are very sensitive to loss, delay and delay variation such as voice over IP (VoIP) and mobile backhaul control.
- M – intended for applications that are sensitive to loss but more tolerant of delay and delay variation such as near-real-time or critical data applications.
- L – intended for applications that are more tolerant of loss as well as delay and delay variation such as non-critical data applications.

These CoS Labels could apply across a number of Performance Tiers (PTs). A PT is comprised of a unique set of CPOs and associated parameters, for each CoS Label, that define the expected performance experienced by IP VPN service flows in the PT. The derivation of the PT is taken from MEF 23.2 [7]. The application of a PT is independent of the geographical span of the service, as discussed in MEF 23.2 [7].

MEF 61.1 [8] defines a set of performance metrics that can be used to describe the expected performance experienced by the Subscriber. The IPVC Service Level Specification Service Attribute defined in MEF 61.1 [8] section 10.9 is agreed between the SP and the Subscriber and includes performance objectives for these metrics. It is specified to be either *None*, or a four-tuple of the form (*s, T, E, L*) where s is the start time, *T* is a period of time, *E* is a set of SLS entries, and L is a set of locations. MEF 61.1 [8] does not provide recommended values for the *s* and *T* entries of this attribute, nor recommendations for the parameters and performance objectives of the metrics found in the SLS entries.

The entries in Table 4 through Table 9 are either a numerical limit on the parameter or objective value, or "no constraints". The tables apply to entries in an SLS for a Subscriber IP VPN service that are for a CoS Name that is a CoS Label. The interpretation of these entries is as follows:

1. If the SLS includes an objective for a performance metric whose parameter value constraints and objective value constraints are listed in the table with a numerical limit, the SLS is required, or if the entry is in parentheses, recommended, to use parameter values and objective values consistent with the tables.
2. If the SLS includes an objective for a performance metric whose parameter value constraints and/or objective value constraints are listed with “no constraints”, then the value is determined by agreement of the parties and not constrained by this standard.

The CPOs are stated as inequalities, therefore for each objective the SP and Subscriber may agree to a value less than the maximum or more than the minimum.

The following requirements ([R1], [R2], [R3]), specify the required values that apply to CoS Labels:

[R1] If the SLS for a Subscriber IP VPN Service contains at least one entry for a CoS Label, the value of *T* in the SLS **MUST** be less than or equal to 1 calendar month.

[R2] In an SLS for a Subscriber IP VPN Service, each entry for a CoS Label **MUST** use parameter values that are not in parenthesis conforming with Table 3.

[R3] In an SLS for a Subscriber IP VPN Service, each entry for a CoS Label **MUST** use performance objective values that are not in parenthesis for the appropriate Performance Tier conforming with Table 4 through Table 9.

[D1] In an SLS for a Subscriber IP VPN Service, each entry for a CoS Label **SHOULD** use parameter values that are in parenthesis conforming with Table 3.

[D2] In an SLS for a Subscriber IP VPN Service, each entry for a CoS Label **SHOULD** use performance objective values that are in parenthesis for the appropriate Performance Tier conforming with Table 4 through Table 9.

Parameter	Used in Performance Metric	Parameter Values for CoS Label H	Parameter Values for CoS Label M	Parameter Values for CoS Label L
Percentile (p)	PD	≥ 99.9th	≥ 99th	≥ 95th
Difference in the time of arrival of packets (τ)	IPDV	≥ 1sec	≥ (1sec)	no constraints
Percentile (v)		≥ 99.9th	≥ (99th)	no constraints
Percentile (r)	PDR	≥ 99.9th	≥ (99th)	no constraints

Table 3 – CoS Label H, M and L Parameter Values for IP Services

Table 4 through Table 9 provide CPO values for each performance tier.

Performance Metric	CoS Label H	CoS Label M	CoS Label L
PD (ms)	≤ 3	≤ 6	≤ 11
MPD (ms)	≤ 2	≤ 4	≤ 9
IPDV (ms)	≤ 1	≤ (2.5)	no constraints
PDR (ms)	≤ 1.25	≤ (3)	no constraints
PLR (%)	≤ .001% i.e., 10^{-5}	≤ .001% i.e., 10^{-5}	≤ .1% i.e., 10^{-3}
Service Uptime	no constraints	no constraints	no constraints

Table 4 – PT0.3 CPOs

Performance Metric	CoS Label H	CoS Label M	CoS Label L
PD (ms)	≤ 10	≤ 20	≤ 37
MPD (ms)	≤ 7	≤ 13	≤ 28
IPDV (ms)	≤ 3	≤ (8)	no constraints
PDR (ms)	≤ 5	≤ (10)	no constraints
PLR (%)	≤ .01% i.e., 10^{-4}	≤ .01% i.e., 10^{-4}	≤ .1% i.e., 10^{-3}
Service Uptime	no constraints	no constraints	no constraints

Table 5 – PT1 CPOs

Performance Metric	CoS Label H	CoS Label M	CoS Label L
PD (ms)	≤ 25	≤ 75	≤ 125
MPD (ms)	≤ 18	≤ 30	≤ 50
IPDV (ms)	≤ 8	≤ (40)	no constraints
PDR (ms)	≤ 10	≤ (50)	no constraints
PLR (%)	≤ .01% i.e., 10^{-4}	≤ .01% i.e., 10^{-4}	≤ .1% i.e., 10^{-3}
Service Uptime	no constraints	no constraints	no constraints

Table 6 – PT2 CPOs

Performance Metric	CoS Label H	CoS Label M	CoS Label L
PD (ms)	≤ 77	≤ 115	≤ 230
MPD (ms)	≤ 70	≤ 80	≤ 125
IPDV (ms)	≤ 10	≤ (40)	no constraints
PDR (ms)	≤ 12	≤ (50)	no constraints
PLR (%)	≤ .025% i.e., 2.5×10^{-4}	≤ .025% i.e., 2.5×10^{-4}	≤ .1% i.e., 10^{-3}
Service Uptime	no constraints	no constraints	no constraints

Table 7 – PT3 CPOs

Performance Metric	CoS Label H	CoS Label M	CoS Label L
PD (ms)	≤ 230	≤ 250	≤ 390
MPD (ms)	≤ 200	≤ 220	≤ 240
IPDV (ms)	≤ 32	≤ (40)	no constraints
PDR (ms)	≤ 40	≤ (50)	no constraints
PLR (%)	≤ .05% i.e., 5×10^{-4}	≤ .05% i.e., 5×10^{-4}	≤ .1% i.e., 10^{-3}
Service Uptime	no constraints	no constraints	no constraints

Table 8 – PT4 CPOs

Performance Metric	CoS Label H	CoS Label M	CoS Label L
PD (ms)	≤ 370	≤ 450	≤ 600
MPD (ms)	≤ 300	≤ 350	≤ 470
IPDV (ms)	≤ 50	$\le (75)$	no constraints
PDR (ms)	≤ 75	$\le (125)$	no constraints
PLR (%)	$\le 1.0\%$ i.e., 10^{-2}	$\le 1.0\%$ i.e., 10^{-2}	no constraints
Service Uptime	no constraints	no constraints	no constraints

Table 9 – PT5 CPOs

The performance objective values specified in Table 4 through Table 9 apply to unicast IP Data Packets that are Qualified Packets, as defined in section 10.9.2 of MEF 61.1 [8], and as further specified in the following requirements in MEF 61.1 [8]:

- R27 (One-way Packet Delay Percentile Performance Metric),
- R29 (One-way Mean Packet Delay Performance Metric),
- R31 (One-way Inter-Packet Delay Variation Performance Metric),
- R33 (One-way Packet Delay Range Performance Metric), and
- R35 (One-way Packet Loss Ratio Performance Metric).

As described in MEF 61.1 [8], when a Service Level Specification (SLS) is specified for an IPVC, each entry in the SLS applies to a specific CoS Name and a set of ordered pairs of SLS Reference Points (SLS-RPs) that are agreed between the SP and the Subscriber, for which performance objectives apply. Each ordered-pair of SLS-RPs in the set *S* can be a pair of IPVC EPs, pair of Locations, or one IPVC EP and one location. These can be used in the following methods:

- IPVC EP pairs are typically used to specify end-to-end performance (e.g. from CE-to-CE)
- Location-pairs are typically used to specify performance of the core network (e.g. from city-to-city or PE-to-PE)
- IPVC EP + Location pairs are typically used to specify performance of the access network (e.g. from CE-to-PE)

The set S can be formed from a combination of these three methods. Each of the pairs within the set S is assigned a PT agreed by the SP and the Subscriber.

An SLS objective typically applies to both directions, hence S would include two entries for each pair of SLS-RPs, e.g., {SLS-RP$_1$- SLS-RP$_2$, SLS-RP$_2$- SLS-RP$_1$}.

Recall that a CoS Label is a standardized CoS Name. There can be performance objectives for several CoS Names in the SLS.

Note that an SP and a Subscriber can agree on an SLS that contains entries for CoS Names that are not CoS Labels, and such entries do not need to conform with the values in Table 4 through Table 9.

The IPVC EP Ingress Class of Service Map Service Attribute and the IPVC EP Egress Class of Service Map Service Attribute are used to map between CoS Names and CoS Labels. Table 10 shows the DSCP values that are recommended to be used by the SP when mapping received packets to CoS Labels and transmitting packets towards the Subscriber. This mapping is agreed between the SP and the Subscriber using the IPVC EP Ingress Class of Service Map Service Attribute and IPVC EP Egress Class of Service Map Service Attribute defined in MEF 61.1 [8] section 11.9 and 11.10.

CoS Label	DSCP Values
H	46 (EF), 44 (VA)
M	26 (AF31), 28 (AF32), 30 (AF33)
L	10 (AF11), 12 (AF12), 14 (AF13), 0 (Default)

Table 10 – The relationship between CoS Label and DSCP values (DSCP Names)

Note: the DSCP Name, e.g., EF, is included for informational purposes. The mapping of DSCP values to CoS Labels in Table 10 matches the mapping found in MEF 23.2 [7] Table 4.

An SP and a Subscriber can agree to a Subscriber IP VPN Service that uses fewer than three CoS Labels. Table 11 below provides a suggested mapping of DSCP values to CoS Labels at an IPVC EP that supports two or more of the three H, M and L CoS Labels. The mapping is agreed between the SP and the Subscriber using the IPVC EP Ingress Class of Service Map Service Attribute defined in MEF 61.1 [8] section 11.9. Note: this table matches the mapping of DSCP labels to CoS Label combinations found in MEF 23.2 [7] table 43. These two tables are intentionally made identical to facilitate seamless operation of Carrier Ethernet services providing underlying transport for IPVCs.

MEF CoS Combination Supported at an IPVC End Point	DSCP Mapping per Class of Service		
	H	M	L
{H + M + L}	40-47	16-39, 48-63	0-15
{H + M}	40-47	0-39, 48-63	n/a
{H + L}	40-47	n/a	0-39, 48-63
{M + L}	n/a	16-63	0-15

Table 11 – Example DSCP Mapping for Multi-CoS IPVCs Supporting Only Standard Classes of Service at the UNI

The CPOs defined in this standard are for the delivery of unicast packets only, as delivery of multicast and broadcast are outside the scope of MEF 61.1 [8], and hence out of scope of this standard as well.

8.4 IP VPN Bandwidth Profile

Subscriber IP VPN Services include a Bandwidth Profile (BWP), defined in MEF 61.1 [8], which governs the temporal properties of IP packets at the UNI. The Subscriber observes the outcome of this BWP as a metering of the traffic rate of IP flows carried by the Subscriber IP VPN Service. The value of this metering rate is agreed between the Subscriber and SP and applied by conditioning functions in the SP's equipment (e.g., traffic shapers, traffic policers). This is often referred to as the "Service Speed". At a given UNI, there may be two BWPs: one in the egress direction towards the Subscriber, one in the ingress direction toward the SP. These two BWPs can have different parameter values. MEF 61.1 [8] defines Bandwidth Profile Flows and Bandwidth Profile Envelopes each of which can be used in multiples to produce IP Services with differentiated classes of service. A Subscriber IP VPN Service defined in this standard may have one or more Bandwidth Profile Flows and Bandwidth Profile Envelopes. When a single Bandwidth Profile Flow and Bandwidth Profile Envelope is used, all traffic flows delivered by the service have equal treatment in a single Class of Service (CoS). When multiple Bandwidth Profile Flows in one or more Bandwidth Profile Envelopes are used, traffic flows are separated into distinct Classes of Service, allowing for differentiated treatment.

9 Subscriber Internet Access Service Requirements

This section specifies the requirements for Subscriber Internet Access Services. Unless otherwise specified, the requirements apply to both Basic and Advanced Internet Access Services.

9.1 Subscriber Internet Access Service: IPVC Requirements

Table 12 contains the subset of the MEF 61.1 [8] IPVC Service Attributes that are constrained for Subscriber Internet Access Services. For all other IPVC Service Attributes described in MEF 61.1 [8], there are no additional constraints for an Internet Access Service - in other words, any of the values specified in MEF 61.1 [8] for these Service Attributes can be agreed between the SP and the Subscriber, subject to the requirements in MEF 61.1 [8]. The first column lists the IPVC Service Attribute, and the second column specifies the requirements.

IPVC Service Attribute	IPVC Requirements
IPVC Topology	**[R4]** For an Internet Access Service, IPVC Topology **MUST** be *Cloud Access*
IPVC End Point List	**[R5]** For an Internet Access Service, IPVC End Point List **MUST** have exactly one entry.
IPVC Packet Delivery	**[R6]** For a Basic Internet Access Service, IPVC Packet Delivery **MUST** be *Standard Routing*. Note: Redundancy for Advanced Internet Access Service is for further study.
IPVC DSCP Preservation	**[D3]** For an Internet Access Service, IPVC DSCP Preservation **SHOULD** be *Disabled*.
IPVC List of Class of Service Names	**[R7]** For an Internet Access Service, IPVC List of Class of Service Names **MUST** have exactly one entry.
IPVC Fragmentation	**[R8]** For an Internet Access Service, IPVC Fragmentation **MUST** be *Enabled*. Note: Fragmentation is necessary for an Internet Access Service as the Subscriber has no control over the size of packets received from the Internet. IPVC Fragmentation *Enabled* ensures the ISP will not discard any packets destined to the Subscriber that exceed the allowable IPVC MTU size.

IPVC Service Attribute	IPVC Requirements
IPVC Cloud	**[R9]** For an Internet Access Service, IPVC Cloud **MUST** be *Internet Access*. **[R10]** For an Internet Access Service, Cloud Ingress Class of Service Map (*F*, *M*, *D*), map *M* **MUST** be empty. **[R11]** For an Internet Access Service, Cloud Ingress Class of Service Map (*F*, *M*, *D*), default CoS name, *D*, **MUST NOT** be *Discard*. Note that the combination of [R7], [R10] and [R11], along with R50 in MEF 61.1 [8], mean that all IP Packets received from the Internet are mapped to a single Class of Service Name. **[R12]** For a Basic Internet Access Service, Cloud DNS **MUST NOT** be *None*. Note: Cloud DNS provided by the ISP to the Subscriber fulfills one aspect of the plug-and-play characteristics of a Basic service. For an Advanced Internet Access Service, a value of *None* for Cloud DNS is not precluded. **[R13]** For an Internet Access Service, if the Cloud DNS parameter of the IPVC Cloud Service Attribute is *Static*, the associated list of DNS Servers **MUST** have at least one entry. **[D4]** For an Internet Access Service, if the Cloud DNS parameter of the IPVC Cloud Service Attribute is *Static*, the associated list of DNS Servers **SHOULD** contain at least two DNS servers.
IPVC Reserved Prefixes	**[R14]** For an Internet Access Service, IPVC Reserved Prefixes **MUST** be either empty, or free from any public address prefixes.

Table 12 – Internet Access IPVC Service Attributes Requirements

9.2 Subscriber Internet Access Service: IPVC End Point Requirements

Table 13 contains the subset of the MEF 61.1 [8] IPVC EP Service Attributes that are constrained for Internet Access Services. The first column lists the IPVC EP Service Attribute, and the second column specifies the requirements. For all other IPVC EP Service Attributes described in MEF 61.1 [8] there are no additional constraints for an Internet Access Service - in other words, any of the values specified in MEF 61.1 [8] for these Service Attributes can be agreed between the SP and the Subscriber, subject to the requirements in MEF 61.1 [8].

IPVC End Point Service Attribute	IPVC End Point Requirements
IPVC EP EI	**[R15]** For a Basic Internet Access Service, the UNI Identifier specified in the IPVC EP EI Service Attribute **MUST NOT** exist in the IPVC EP EI Service Attribute of any other IP Service.
IPVC EP Role	**[R16]** For an Internet Access Service, IPVC EP Role **MUST** be *Root*.
IPVC EP Ingress Class of Service Map	**[R17]** For an Internet Access Service, IPVC EP Ingress Class of Service Map (*F*, *M*, *D*), map *M* **MUST** be empty. **[R18]** For an Internet Access Service, IPVC Ingress EP Class of Service Map (*F*, *M*, *D*), default CoS name, *D*, **MUST NOT** be *Discard*. Note that the combination of [R7], [R17] and [R18], along with R50 in MEF 61.1 [8], mean that all Ingress IP Packets for the Internet Access Service are mapped to a single Class of Service Name.
IPVC EP Ingress Bandwidth Profile Envelope	**[D5]** For a Basic Internet Access Service, the IPVC EP Ingress Bandwidth Profile Envelope **SHOULD** be *None*.
IPVC EP Egress Bandwidth Profile Envelope	**[D6]** For a Basic Internet Access Service, the IPVC EP Egress Bandwidth Profile Envelope **SHOULD** be *None*. Note that [D5], [D6], [D12] and [D13] constrain Basic Internet Access Service to allow only one ingress and/or egress Bandwidth Profile at the UNI. This defines the simple nature of this Basic Internet Access service, in that it is incapable of supporting additional Connectivity Services across the same UNI.
IPVC EP Prefix Mapping	**[R19]** For a Basic Internet Access Service, the IPVC EP Prefix Mapping **MUST** be Empty.

Table 13 – Internet Access IPVC EP Service Attributes Requirements

9.3 Subscriber Internet Access Service: UNI Requirements

Table 14 contains the subset of the MEF 61.1 [8] UNI Service Attributes that are constrained for Internet Access Services. The first column lists the UNI Service Attribute, and the second column specifies the requirements. For all other UNI Service Attributes described in MEF 61.1 [8], there are no additional constraints for an Internet Access Service - in other words, any of the values specified in MEF 61.1 [8] for these Service Attributes can be agreed between the SP and the Subscriber, subject to the requirements in MEF 61.1 [8].

UNI Service Attribute	UNI Requirements
UNI List of UNI Access Links Service Attribute	**[R20]** At a UNI with an IPVC EP for a Basic Internet Access Service, the UNI List of UNI Access Links **MUST** contain exactly one entry. Note: In the case where a Subscriber is provided both Wifi and Ethernet connectivity with their Basic service, typically that is a single subnet, and is viewed as a single common UNI on a single UNI Access Link.
UNI Ingress Bandwidth Profile Envelope	**[D7]** At a UNI with an IPVC EP for a Basic Internet Access Service, if the UNI Ingress Bandwidth Profile Envelope is not *None*, it **SHOULD** have Bandwidth Profile Flows that contain all Ingress IP Data Packets at the UNI that are mapped to any of a given set of IPVC EPs (as defined in MEF 61.1 [8] Table 28). Note: Note that a consequence of [D5] and [D12], along with [R103], [R104] and [R176] from MEF 61.1 [8], is that if an Ingress Bandwidth Profile is used, it is recommended to be specified using the UNI Ingress Bandwidth Profile Envelope.
UNI Egress Bandwidth Profile Envelope	**[D8]** At a UNI with an IPVC EP for a Basic Internet Access Service, if the UNI Egress Bandwidth Profile Envelope is not *None*, it **SHOULD** have Bandwidth Profile Flows that contain all Egress IP Data Packets at the UNI that are mapped to any of a given set of IPVC EPs (as defined in MEF 61.1 [8] Table 28). Note: Note that a consequence of [D6] and [D13], along with [R105], [R106] and [R177] from MEF 61.1 [8], is that if an Egress Bandwidth Profile is used, it is recommended to be specified using the UNI Egress Bandwidth Profile Envelope.

UNI Service Attribute	UNI Requirements
UNI List of Control Protocols	**[D9]** At a UNI with an IPVC EP for an Internet Access Service, if the UNI has at least one UNI Access Link where the UNI Access Link IPv4 Connection Addressing is not *None*, the UNI List of Control Protocols **SHOULD** include ICMP with a list of applicable ISP IP addresses. **[D10]** At a UNI with an IPVC EP for an Internet Access Service with at least one UNI Access Link where the UNI Access Link IPv6 Connection Addressing is not *None*, the UNI List of Control Protocols **SHOULD** include ICMPv6 with a list of applicable SP IP addresses.
UNI Routing Protocols	**[R21]** At a UNI with an IPVC EP for a Basic Internet Access Service, the UNI Routing Protocols list **MUST** be empty.
UNI Reverse Path Forwarding	**[D11]** At a UNI with an IPVC EP for an Internet Access Service, UNI Reverse Path Forwarding **SHOULD** be *Enabled*.

Table 14 – Internet Access UNI Service Attributes Requirements

9.4 Subscriber Internet Access Service: UNI Access Link Requirements

Table 15 contains the subset of the MEF 61.1 [8] UNI Access Link Service Attributes that are constrained for Internet Access Services. The first column lists the UNI Access Link Service Attribute, and the second column specifies the requirements. For all other UNI Access Link Service Attributes described in MEF 61.1 [8], there are no additional constraints for an Internet Access Service - in other words, any of the values specified in MEF 61.1 [8] for these Service Attributes can be agreed between the SP and the Subscriber, subject to the requirements in MEF 61.1 [8].

UNI Access Link Service Attribute	**UNI Access Link Requirements**
UNI Access Link IPv4 Connection Addressing	**[R22]** At a UNI Access Link in a UNI with an IPVC EP for an Advanced Internet Access Service, UNI Access Link IPv4 Connection Addressing **MUST** be *Static* or *None*. **[R23]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, UNI Access Link IPv4 Connection Addressing **MUST** be *DHCP* or *None*. Note: The value of Unnumbered for UNI Access Link IPv4 Connection Addressing is intentionally excluded as Unnumbered interfaces render most of the common troubleshooting and performance monitoring tools unusable. **[R24]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, if the UNI Access Link IPv4 Connection Addressing is *DHCP*, the UNI Access Link IPv4 Connection Addressing Secondary Subnet List parameter **MUST** be empty. **[R25]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, if the UNI Access Link IPv4 Connection Addressing is *DHCP*, the UNI Access Link IPv4 Connection Addressing Primary Subnet parameter **MUST** contain only a single Service Provider IPv4 Address.

UNI Access Link Service Attribute	**UNI Access Link Requirements**
UNI Access Link IPv6 Connection Addressing	**[R26]** At a UNI Access Link in a UNI with an IPVC EP for an Advanced Internet Access Service, UNI Access Link IPv6 Connection Addressing **MUST** be *Static* or *None*. Note: The value of LL-only for UNI Access Link IPv6 Connection Addressing is intentionally excluded as LL-only interfaces render most of the common troubleshooting and performance monitoring tools unusable. **[R27]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, UNI Access Link IPv6 Connection Addressing **MUST** be *DHCP* or *SLAAC* or *None*. **[R28]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, if the UNI Access Link IPv6 Connection Addressing is *DHCP* or *SLAAC*, the UNI Access Link IPv6 Connection Address Subnet List parameter **MUST** contain a single entry. **[R29]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, if the UNI Access Link IPv6 Connection Addressing is *DHCP* or *SLAAC*, the UNI Access Link IPv6 Connection Addressing Subnet List parameter **MUST** contain only a single Service Provider IPv6 Address. Note: The UNI Access Link IPv6 Connection Addressing Service Attribute consists of a list of subnets each containing a list SP IPv6 addresses. [R28] and [R29] ensure that only a single SP IPv6 address exists for a Basic Internet Access Service.
UNI Access Link DHCP Relay	**[R30]** If at a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, where the UNI contains only a single IP Service, the UNI Access Link DHCP Relay **MUST** be empty.
UNI Access Link BFD	**[R31]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, UNI Access Link BFD **MUST** be *None*.

UNI Access Link Service Attribute	**UNI Access Link Requirements**
UNI Access Link Ingress Bandwidth Profile Envelope	**[D12]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, UNI Access Link Ingress Bandwidth Profile Envelope **SHOULD** be *None*.
UNI Access Link Egress Bandwidth Profile Envelope	**[D13]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, UNI Access Link Egress Bandwidth Profile Envelope **SHOULD** be *None.*
UNI Access Link Reserved VRIDs Service Attribute	**[D14]** At a UNI Access Link in a UNI with an IPVC EP for a Basic Internet Access Service, UNI Access Link Reserved VRIDs Service Attribute **SHOULD** be *None*. Note: The use of VRRP by the ISP is discouraged in the Basic Internet Access Service, as it requires coordination of VRID resources between the Subscriber and ISP, which compromises the simplicity and plug-and-play nature of this service type.

Table 15 – Internet Access UNI Access Link Service Attributes Requirements

10 Subscriber IP VPN Service Requirements

This section specifies the requirements for Subscriber IP VPN Services. Unless otherwise specified, the requirements apply to both Intranet and Extranet Subscriber IP VPN Services.

10.1 Subscriber IP VPN Service: IPVC Requirements

Table 12 contains the subset of the MEF 61.1 [8] IPVC Service Attributes that are constrained for Subscriber IP VPN Services. For all other IPVC Service Attributes described in MEF 61.1 [8], there are no additional constraints for a Subscriber IP VPN Service - in other words, any of the values specified in MEF 61.1 [8] for these Service Attributes can be agreed between the SP and the Subscriber, subject to the requirements in MEF 61.1 [8]. The first column lists the IPVC Service Attribute, and the second column specifies the requirements.

IPVC Service Attribute	IPVC Requirements
IPVC Topology	**[R32]** For a Subscriber IP VPN Service, IPVC Topology **MUST** be either *Multipoint* or *Rooted Multipoint*. **[R33]** If an Extranet IPVC has two or more IPVC EPs for the same Subscriber, and one or more of them is at a UNI that also has an IPVC EP for an Intranet IPVC, the IPVC Topology Service Attribute for the Extranet IPVC **MUST** be set to *Rooted Multipoint*. Note: The purpose of [R33] is to help ensure that when both Intranet and Extranet IPVCs share the same UNI, only the Intranet IPVC is used for connectivity between IPVC EPs of the same Subscriber. This is required to conform with MEF 61.1 [8] R80.
IPVC End Point List	**[R34]** For a Subscriber IP VPN Intranet Service, the IPVC End Point List **MUST** contain only IPVC EPs that reside on UNIs belonging to a single Subscriber. **[R35]** For a Subscriber IP VPN Extranet Service, the IPVC End Point List **MUST** contain IPVC EPs that reside on UNIs belonging to at least two Subscribers.
IPVC Packet Delivery	**[R36]** For a Subscriber IP VPN Service, IPVC Packet Delivery **MUST** be *Standard Routing*.
IPVC Maximum Number of IPv4 Routes	**[R37]** For a Subscriber IP VPN Service, IPVC Maximum Number of IPv4 Routes **MUST NOT** be *Unlimited.*

IPVC Service Attribute	IPVC Requirements
IPVC Maximum Number of IPv6 Routes	**[R38]** For a Subscriber IP VPN Service, IPVC Maximum Number of IPv6 Routes **MUST NOT** be *Unlimited.* **[R39]** For a Subscriber IP VPN Service, IPVC Maximum Number of IPv4 Routes and IPVC Maximum Number of IPv6 Routes **MUST NOT** both be equal to zero.
IPVC DSCP Preservation	**[D15]** For a Subscriber IP VPN Intranet Service, IPVC DSCP Preservation **SHOULD** be *Enabled*.
IPVC List of Class of Service Names	**[D16]** For a Subscriber IP VPN Service, at least one CoS Label as listed in Table 10 **SHOULD** be used in the IPVC List of Class of Service Names Service Attribute. **[D17]** For a Subscriber IP VPN Service, each Class of Service Name listed in the IPVC List of Class of Service Names Service Attribute **SHOULD** have a Packet Loss Ratio entry in the IPVC Service Level Specification. **[D18]** For a Subscriber IP VPN Service, each CoS Name listed in the IPVC List of Class of Service Names Service Attribute **SHOULD** have entries in the IPVC Service Level Specification that include objectives for at least one of the following pairs of Performance Metrics: (PD, IPDV), (PD, PDR) or (MPD, PDR).
IPVC Path MTU Discovery	**[D19]** For a Subscriber IP VPN Service, IPVC Path MTU Discovery **SHOULD** be *Enabled*.
IPVC Cloud	**[R40]** For a Subscriber IP VPN Service, IPVC Cloud **MUST** be *None*.
IPVC Reserved Prefixes	**[R41]** For a Subscriber IP VPN Service, IPVC Reserved Prefixes **MUST** include all IP prefixes used by the SP to manage the service.

Table 16 – Subscriber IP VPN Service IPVC Attributes Requirements

10.2 Subscriber IP VPN Service: IPVC End Point Requirements

Table 17 contains the subset of the MEF 61.1 [8]. IPVC EP Service Attributes that are constrained for Subscriber IP VPN Services. The first column lists the IPVC EP Service Attribute, and the second column specifies the requirements. For all other IPVC EP Service Attributes described in MEF 61.1 [8] there are no additional constraints for a Subscriber IP VPN Service - in other words, any of the values specified in MEF 61.1 [8] for these Service Attributes can be agreed between the SP and the Subscriber, subject to the requirements in MEF 61.1 [8].

IPVC End Point Service Attribute	IPVC End Point Requirements
IPVC EP Role	**[R42]** For a Subscriber IP VPN Service, IPVC EP Role **MUST** be *Root* or *Leaf*.
IPVC EP Maximum Number of IPv4 Routes	**[R43]** For a Subscriber IP VPN Service, IPVC EP Maximum Number of IPv4 Routes **MUST NOT** be *Unlimited*
IPVC EP Maximum Number of IPv6 Routes	**[R44]** For a Subscriber IP VPN Service, IPVC EP Maximum Number of IPv6 Routes **MUST NOT** be *Unlimited* **[R45]** For a Subscriber IP VPN Service, IPVC EP Maximum Number of IPv4 and IPVC EP Maximum Number of IPv6 Routes **MUST NOT** both be equal to zero.
IPVC EP Ingress Class of Service Map	**[D20]** For a Subscriber IP VPN Service, the SP **SHOULD** support *IP DS* in the list *F* in the value of the IPVC EP Ingress Class of Service Map Service Attribute. Note: [D20] does not prevent the SP and Subscriber from agreeing on the use of other fields (e.g., IP addresses, Layer 4 ports) **[CD1]**<[D16] For a Subscriber IP VPN Service, either the map *M* or *D* in the value of the IPVC EP Ingress Class of Service Map Service Attribute **SHOULD** contain a CoS Label. **[CD2]**<[CD1] If a CoS Label is included in the IPVC List of Class of Service Names, the values of *M* and *D* in the IPVC EP Ingress Class of Service Map Service Attribute **SHOULD** be such that the DSCP values listed in Table 10 for that CoS Label are mapped to the CoS Label. Note: R86 in MEF 61.1 [8] enforces CoS alignment across the IPVC and IPVC EP.

IPVC End Point Service Attribute	IPVC End Point Requirements
IPVC EP Egress Class of Service Map	**[CD3]<**[D16] For a CoS Label, if the value of *D* in the IPVC EP Egress Class of Service Map Service Attributes is not *None*, it **SHOULD** map the CoS Label to one of the DSCP values as per Table 10. **[R46]** For a Subscriber IP VPN Service, the value of *D* in the IPVC EP Egress Class of Service Map **MUST NOT** be *None* when IPVC DSCP Preservation is *Disabled*.
IPVC EP Ingress Bandwidth Profile Envelope	**[R47]** For an IP VPN IPVC EP, exactly one of the following statements **MUST** hold: • The value of the IPVC EP Ingress Bandwidth Profile Envelope Service Attribute is not *None*. • The value of the UNI Ingress Bandwidth Profile Envelope Service Attribute is not *None* for the UNI where the IPVC EP is located. • The value of the UNI Access Link Ingress Bandwidth Profile Envelope Service Attribute is not *None* for all of the UNI Access Links in the UNI where the IPVC EP is located. **[R48]** For a Subscriber IP VPN Service, if the IPVC EP Ingress Bandwidth Profile Envelope contains a Bandwidth Profile Flow that uses CoS Label H, the Bandwidth Profile Flow **MUST** have the Burst Behavior parameter set to the value of "*Optimize-Delay*".

IPVC End Point Service Attribute	IPVC End Point Requirements
IPVC EP Egress Bandwidth Profile Envelope	**[R49]** For an IP VPN IPVC EP, exactly one of the following statements **MUST** hold: • The value of the IPVC EP Egress Bandwidth Profile Envelope Service Attribute is not *None*. • The value of the UNI Egress Bandwidth Profile Envelope Service Attribute is not *None* for the UNI where the IPVC EP is located. • The value of the UNI Access Link Egress Bandwidth Profile Envelope Service Attribute is not *None* for all of the UNI Access Links in the UNI where the IPVC EP is located. **[R50]** For a Subscriber IP VPN Service, if the IPVC EP Egress Bandwidth Profile Envelope contains a Bandwidth Profile Flow that uses CoS Label H, the Bandwidth Profile Flow **MUST** have the Burst Behavior parameter set to the value of "*Optimize-Delay*".

Table 17 – Subscriber IP VPN Service IPVC EP Attributes Requirements

10.3 Subscriber IP VPN Service: UNI Requirements

Table 18 contains the subset of the MEF 61.1 [8] UNI Service Attributes that are constrained for Subscriber IP VPN Services. The first column lists the UNI Service Attribute, and the second column specifies the requirements. For all other UNI Service Attributes described in MEF 61.1 [8], there are no additional constraints for a Subscriber IP VPN Service - in other words, any of the values specified in MEF 61.1 [8] for these Service Attributes can be agreed between the SP and the Subscriber, subject to the requirements in MEF 61.1 [8].

UNI Service Attribute	UNI Requirements
UNI Ingress Bandwidth Profile Envelope	**[R51]** At a UNI with an IPVC EP for a Subscriber IP VPN Service, if there is an ingress Bandwidth Profile Flow for that IPVC EP that uses CoS Label H, within the UNI Ingress Bandwidth Profile Envelope, the ingress Bandwidth Profile Flow **MUST** have the Burst Behavior parameter set to the value of "*Optimize-Delay*".

UNI Service Attribute	UNI Requirements
UNI Egress Bandwidth Profile Envelope	**[R52]** At a UNI with an IPVC EP for a Subscriber IP VPN Service, if there is an egress Bandwidth Profile Flow for that IPVC EP that uses CoS Label H, within the UNI Egress Bandwidth Profile Envelope, the egress Bandwidth Profile Flow **MUST** have the Burst Behavior parameter set to the value of "*Optimize-Delay*".
UNI List of Control Protocols	**[R53]** At a UNI with an IPVC EP for a Subscriber IP VPN Service, if the UNI has at least one UNI Access Link where the UNI Access Link IPv4 Connection Addressing is not *None*, the UNI List of Control Protocols **MUST** include ICMPv4 with addressing information of *SP/Operator Addresses*. **[R54]** At a UNI with an IPVC EP for a Subscriber IP VPN Service, if the UNI has at least one UNI Access Link where the UNI Access Link IPv6 Connection Addressing is not *None*, the UNI List of Control Protocols **MUST** include ICMPv6 with addressing information of *SP/Operator Addresses*.
UNI Routing Protocols	**[R55]** At a UNI with an IPVC EP for a Subscriber IP VPN Service, if the UNI Routing Protocols Service Attribute includes BGP, the UNI Routing Protocols BGP Subscriber AS Number **MUST** be a Private AS Number or a Public AS Number assigned to the Subscriber.
UNI Reverse Path Forwarding	**[D21]** At a UNI with an IPVC EP for a Subscriber IP VPN Service, UNI Reverse Path Forwarding **SHOULD** be *Enabled*.

Table 18 – Subscriber IP VPN UNI Service Attributes Requirements

10.4 Subscriber IP VPN Service: UNI Access Link Requirements

Table 19 contains the subset of the MEF 61.1 [8] UNI Access Link Service Attributes that are constrained for Subscriber IP VPN Services. The first column lists the UNI Access Link Service Attribute, and the second column specifies the requirements. For all other UNI Access Link Service Attributes described in MEF 61.1 [8], there are no additional constraints for a Subscriber IP VPN Service - in other words, any of the values specified in MEF 61.1 [8] for these Service Attributes can be agreed between the SP and the Subscriber, subject to the requirements in MEF 61.1 [8].

UNI Access Link Service Attribute	UNI Access Link Requirements
UNI Access Link Connection Type	**[R56]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, UNI Access Link Connection Type **MUST** support a value of *P2P*.
UNI Access Link IPv4 Connection Addressing	**[D22]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, UNI Access Link IPv4 Connection Addressing **SHOULD NOT** be *Unnumbered*. **[R57]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, the SP **MUST** process any ICMPv4 Echo packets addressed to one of the Service Provider Addresses listed in the UNI Access Link IPv4 Connection Addressing Service Attribute and generate an ICMPv4 echo reply as specified in RFC 792 [1].
UNI Access Link IPv6 Connection Addressing	**[D23]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, UNI Access Link IPv6 Connection Addressing **SHOULD NOT** be *LL-only*. **[R58]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, the SP **MUST** process any ICMPv6 Echo Request packets addressed to one of the Service Provider Addresses listed in the UNI Access Link IPv6 Connection Addressing Service Attribute and generate an ICMPv6 echo reply as specified in RFC 4443 [5].

UNI Access Link Service Attribute	UNI Access Link Requirements
UNI Access Link BFD	**[D24]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, the UNI Access Link BFD Service Attribute **SHOULD NOT** be *None*. **[D25]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, the value of the Transmission Interval parameter in the UNI Access Link BFD Service Attribute **SHOULD** be 100ms. **[D26]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, the value of the Detect Multiplier parameter in the UNI Access Link BFD Service Attribute **SHOULD** be 3. Note: [D25] and [D26] attempt to make the BFD parameters uniformly set across IP VPN Service offerings, in an effort to streamline the number of parameters negotiated between the SP and Subscriber. **[D27]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, if the SP supports a value of the UNI Access Link BFD other than *None*, the SP **SHOULD** support all possible values for the Active End parameter. **[D28]** At a UNI Access Link with an IPVC EP for a Subscriber IP VPN Service, if the value of the UNI Access Link BFD Service Attribute is not *None*, the Active End parameter of the UNI Access Link BFD Service Attribute **SHOULD** be set to *Subscriber*. Note: The Subscriber equipment is best suited for the Active End of the BFD session, as message processing resources are more difficult to scale in Service Provider equipment serving many Subscriber IPVCs.
UNI Access Link Ingress Bandwidth Profile Envelope	**[R59]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, if there is an ingress Bandwidth Profile Flow for that IPVC EP that uses CoS Label H within the UNI Access Link Ingress Bandwidth Profile Envelope, the ingress Bandwidth Profile Flow **MUST** have the Burst Behavior parameter set to a value of "*Optimize-Delay*".

UNI Access Link Service Attribute	**UNI Access Link Requirements**
UNI Access Link Egress Bandwidth Profile Envelope	**[R60]** At a UNI Access Link in a UNI with an IPVC EP for a Subscriber IP VPN Service, if there is an egress Bandwidth Profile Flow for that IPVC EP that uses CoS Label H within the UNI Access Link Egress Bandwidth Profile Envelope, the egress Bandwidth Profile Flow **MUST** have the Burst Behavior parameter set to the value of "*Optimize-Delay*".

Table 19 – Subscriber IP VPN Service UNI Access Link Service Attributes Requirements

11 References

[1] IETF RFC 792, *Internet Control Message Protocol*, by Dr. Jon Postel, September 1981.

[2] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, by Scott Bradner, March 1997.

[3] IETF RFC 2131, *Dynamic Host Configuration Protocol*, by Dr. Ralph Droms, March 1997.

[4] IETF RFC 4271, *A Border Gateway Protocol 4 (BGP-4),* by Dr. Yakov Rekhter, January 2006. Copyright © The Internet Society (2006). All Rights Reserved.

[5] IETF RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*, by Alex Conta, Mar 2006. Copyright © The Internet Society (2006). All Rights Reserved.

[6] IETF RFC 8174, *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words*, by Barry Leiba, May 2017. Copyright © 2017 IETF Trust and the persons identified as the document authors. All Rights Reserved.

[7] MEF 23.2, Carrier Ethernet Class of Service IA, Phase 3, Aug 2016.

[8] MEF 61.1, *IP Service Attributes*, May 2019.

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

[10] MEF 69, Subscriber IP Service Definitions, Nov 2019.

Appendix A Use Cases (Informative)

The following use cases provide practical examples of Subscriber Internet Access Services and Subscriber IP VPN Services.

A.1 Subscriber Residential Internet Access Use Case

This residential Internet use case is based on the Basic Internet Access Service as described earlier in this standard. It offers an easy-to-use, plug-and-play, low-cost Internet connectivity solution delivered to Subscriber dwellings. It is the most common example of fixed Internet Access Service. A residential Internet service is illustrated in Figure 4.

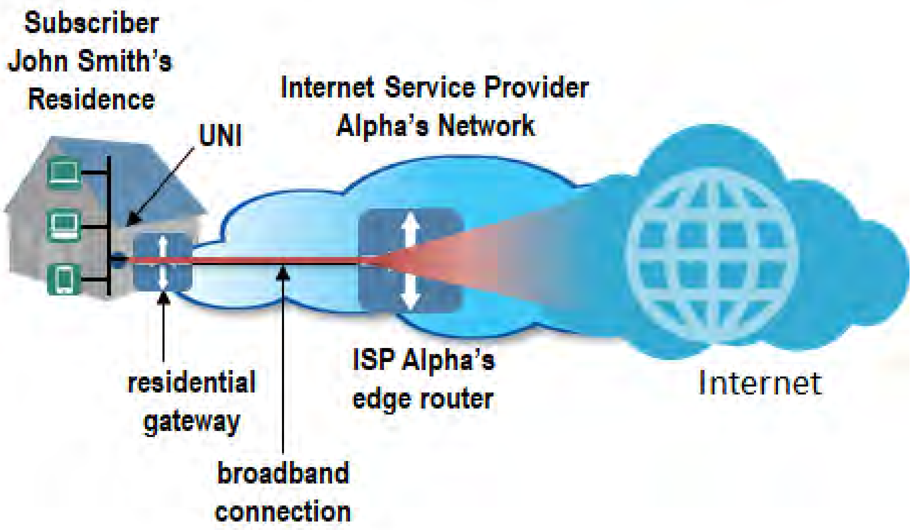

Figure 4 – Example of the Residential Internet Use Case

The Subscriber, *John Smith*, requires Basic Internet access at his residence, and asks Internet Service Provider, *ISP Alpha*, to offer a solution. *John* has several devices in the home that require Internet connectivity: a smartphone, laptop and a desktop computer. The smartphone and laptop are also used outside the home, where they make use of Internet Access Services provided by other ISPs (e.g., his workplace, coffee shops, etc). *John* cannot be inconvenienced with reconfiguration of IP addressing and related parameters on these mobile devices each time they are reconnected to different Internet Access Services, so the service at his residence must support a plug-and-play user experience.

ISP Alpha constructs a broadband network facility or circuit from the ISP POP (point of presence) to *John's* residence, providing a media over which the final segment of the Internet IPVC is carried. The broadband connection is terminated on a residential gateway owned and provided by *ISP Alpha*. This is captured by agreeing to a value of the UNI Management Type Service Attribute of *Provider-Managed*.

John's devices utilize either wired media (e.g., Ethernet) or wireless media (e.g., Wifi) to connect to the Internet Access Service. The Internet Access Service UNI exists across both of these media (wired and wireless).

At service ordering time, *ISP Alpha* allows *John* to select one or both of two versions of IP protocol the Internet Access service supports: IPv4 and IPv6. His selection populates the parameters of the UNI Access Link IPv4 and IPv6 Connection Addressing Service Attributes. He selects the DHCP option for both protocols. *John's* devices (smartphone, laptop, desktop computer) will use the DHCP protocol [3] to peer with *ISP Alpha's* residential gateway to obtain IP configuration information dynamically (plug-and-play).

ISP Alpha offers *John* a selection of Internet speeds supported by the broadband circuit delivered to his home. John selects the "100Mbps downstream, 50Mbps upstream" Internet service speed option, which is populated into service attributes:

- UNI Egress BWP Envelope Service Attribute MaxIR parameter = 100Mbps.
- UNI Ingress BWP Envelope Service Attribute MaxIR parameter = 50Mbps.

ISP Alpha offers *John* a selection of monthly traffic volume plans. *John* selects the "500G down, 100G up" option. This plan allows *John* to consume up to 500 Gigabytes of data in the downstream direction, and up to 100 Gigabytes of data in the upstream direction throughout the monthly billing cycle without incurring additional charges. Should either of these thresholds be exceeded, *ISP Alpha* applies an additional charge to *John's* bill. *John* is billed for this service by *ISP Alpha* at the beginning of each month. This monthly usage cap is expressed in the IPVC Cloud Service Attribute Cloud Data Limit parameter 4-tuple as follows:

- S_{cdl} = starting at time 00:00, 1st day of the month
- T_{cdl} = 1 month duration
- u_{cdl} = 100,000,000,000 octets
- d_{cdl} = 500,000,000,000 octets

The meaning of the parameters of the 4-tuple are as follows:

- S_{cdl} specifies the start time
- T_{cdl} specifies the time duration
- u_{cdl} specifies the amount of IP traffic transmitted towards the Internet Access service (from the Subscriber)
- d_{cdl} specifies the amount of IP traffic transmitted from the Internet Access service (to the Subscriber)

A.2 Subscriber Business Internet Access Use Case

The Business Internet use case is based on the Advanced Internet Access Service as described earlier in this standard. It offers a premium Internet connectivity solution delivered to business locations (e.g., office towers). It includes Service Attribute values required to deliver a more highly available and reliable service than Basic Internet Access Service, suitable for delivering Commercial applications. The Business Internet use case is illustrated in Figure 5.

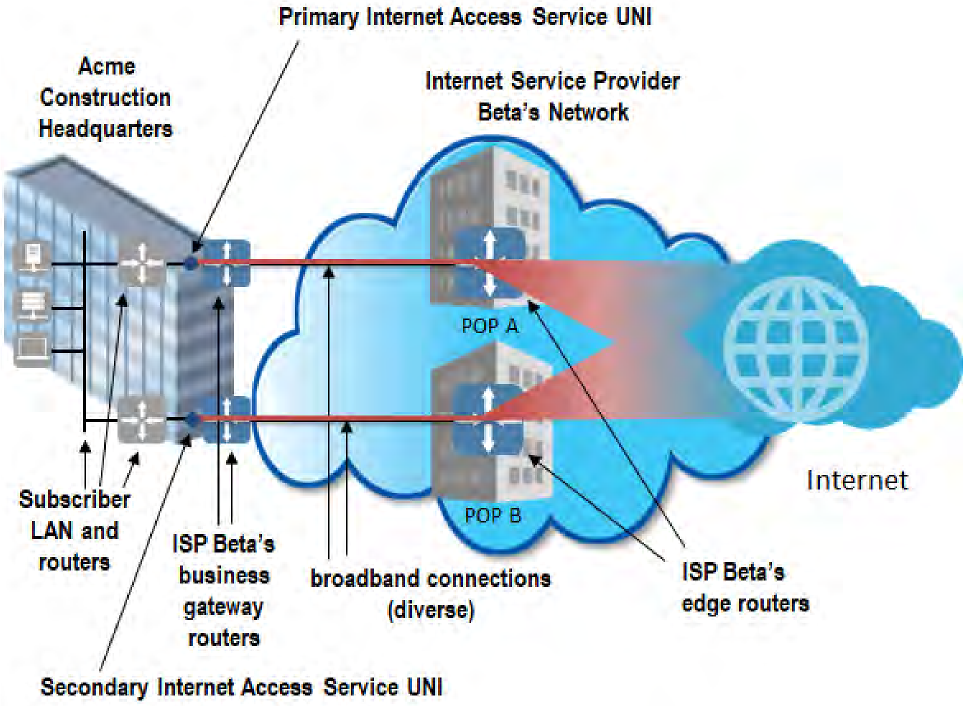
Primary Internet Access Service UNI
Acme Construction Headquarters
Internet Service Provider Beta's Network
POP A
POP B
Internet
Subscriber LAN and routers
ISP Beta's business gateway routers
broadband connections (diverse)
ISP Beta's edge routers
Secondary Internet Access Service UNI

Figure 5 – Example of the Business Internet Use Case

A Subscriber, *Acme Construction*, requires Advanced Internet Access at their corporate headquarters, and asks Internet Service Provider, *ISP Beta*, to offer a solution. This service is required for the following business needs:

- Email
- Web Browsing
- Corporate website hosting

Numerous devices at *Acme Construction* will utilize this service, including employee IT devices, (smartphones, tablets and laptops) and corporate email and web hosting servers. Reliability of the Internet access is critical for Acme Construction's operations. *Acme Construction* is prepared to pay a premium for a service that is resilient to failures.

ISP Beta offers *Acme Construction* two redundant Advanced IP Access Services to meet the reliability requirements. Each IP Access Service requires a broadband network facility or circuit from an *ISP Beta* POP to the *Acme Construction* headquarters location, providing a media over which the final segment of the Internet IPVC is carried. These two services are delivered via different *ISP Beta* POPs. The two broadband circuits are physically diverse, ensuring the alternate service survives a facility "cut" of any form (e.g., backhoe breaks the fiber). Each broadband connection is terminated on a business gateway owned and provided by *ISP Beta*, in other words, the UNI Management Type Service Attribute is *Provider-Managed*.

Acme Construction has an existing IPv4 and Ethernet network at the headquarters location. The two *ISP Beta* business gateways connect to *Acme Construction* network routers with Gigabit

Ethernet links. The Internet Access Service UNIs exist on these Gigabit Ethernet links that connect the two companies. The corporate network does not yet have IPv6 capability.

Acme Construction has its own publicly routable IPv4 address space, 203.0.113.0/24, which it would like to use on these new IP Access Services from *ISP Beta*. *Acme Construction* may in the future subscribe to another Advanced Internet Access Service from a different ISP, to further improve the resiliency of their connectivity to the public Internet. *Acme Construction* apportions two subnets of their address space to be used on the Gigabit Ethernet links that connect to *ISP Beta* business gateways, 203.0.113.0/30 and 203.0.113.4/30. The two companies agree that *ISP Beta* routers will use the lower numbered IP host on the subnet.

The UNI Access Link IPv4 Connection Addressing value is set as follows for the first Internet Access Service:

(Type: Static,
Primary IPv4 Prefix: 203.0.113.0/30,
Primary SP IPv4 Addresses: [203.0.113.1],
Primary Subscriber IPv4 Address: 203.0.113.2,
Primary Reserved Prefixes: [ ],
Secondary Subnets: [ ]
)

The UNI Access Link IPv6 Connection Addressing value is set to *None*.

To facilitate redundancy between the two Internet Access Services, *Acme Construction* and *ISP Beta* exchange reachability information using the BGP routing protocol. *ISP Beta* allows its Subscribers to use the ICMP [1] protocol to test connectivity to business gateway routers. Therefore, the UNI List of Control Protocols Service Attribute value for these services is set as follows:

[(Protocol: ICMP, Addressing: SP Addresses, Reference: RFC 792),
(Protocol: BGP, Addressing: SP Addresses, Reference: RFC 4271),
]

Acme Construction has its own BGP Autonomous System (AS) number, 64496. *ISP Beta* has BGP AS 64511. Therefore, the UNI Routing Protocols Service Attribute value AS parameters for these services is set as follows:

Subscriber’s AS Number = 64496
SP’s AS Number = 64511

Alignment on the setting of the service parameters above provides clarity to both parties on how the service is to be configured.

A.3 Subscriber IP VPN Intranet Service Use Case

This Intranet use case is based on the Subscriber IP VPN Intranet Service as described earlier in this standard.

A *Subscriber Acme* has five locations, one Headquarters (HQ) office, one data center (DC) and three branch offices. *Acme* purchases an IP VPN Intranet service from *Service Provider Alpha* for this connectivity between these locations. The *Acme* network must be kept separate from other Subscribers on the *Alpha* Network.

Subscriber Acme has special connectivity requirements between locations. Only the HQ location is permitted to communicate with the DC location. Also, the Branch offices use IPv4 address space that is in duplicate to the IPv4 address space used in the DC. *SP Alpha* provides this separation of *Acme's* Intranet by offering two IPVCs, one for HQ and Branch connectivity, the other for HQ and DC connectivity. The use of two IPVCs also allows for unique BWPs to be applied to flows to the Branch location and to the DC location.

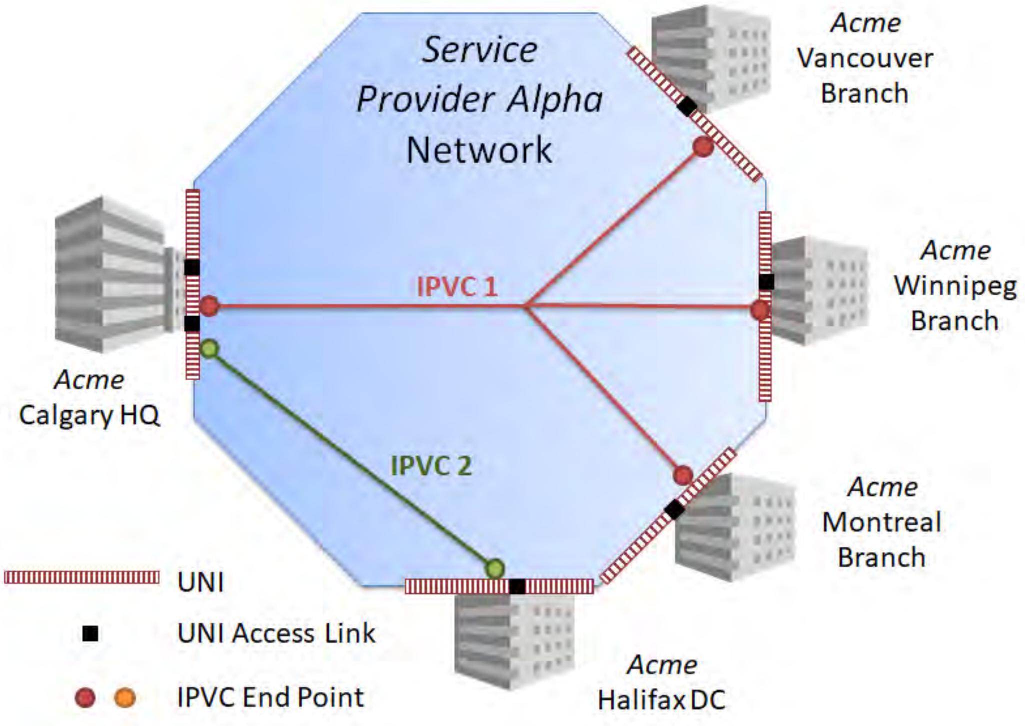

Figure 6 – Example of the IP VPN Intranet Use Case

SP Alpha offers *Subscriber Acme* intuitive human-readable names for UNI Identifiers. The name of each *Acme* location is embedded into the UNI Identifier text, as follows:

List of UNI Identifiers:

- ACME_Calgary_HQ
- ACME_Winnipeg_Branch
- ACME_Vancouver_Branch
- ACME_Montreal_Branch
- ACME_Halifax_DC

SP Alpha offers two models for management of the CE. *SP Alpha* can supply and manage the CE device, or will allow the Subscriber to own and be responsible for the CE. *Subscriber Acme* has a small team of IT support staff, so prefers a solution where the Service Provider manages all aspects of WAN routing. *Acme* selects the Provider-Managed value for the UNI Management Type Service Attribute to choose this option.

Each of the Branch and DC sites have a single UNI Access Link Identifier, again defined with intuitive human-readable names as follows:

- UNIAL.ACME_Winnipeg_Branch.01
- UNIAL.ACME_Vancouver_Branch.01
- UNIAL.ACME_Montreal_Branch.01
- UNIAL.ACME_Halifax_DC.01

Each of the UNI Access Link Identifiers above form a single-entry list for the "UNI List of UNI Access Links Service Attribute" for the UNI of each site.

The HQ site has two IPVCs and two UNI Access Links. The two UNI Access Link Identifiers for the HQ site are as follows:

- UNIAL.ACME_Calgary_HQ.01
- UNIAL.ACME_Calgary_HQ.02

These two UNI Access Link Identifiers above form a two-entry list for the "UNI List of UNI Access Links Service Attribute" for the HQ site UNI.

The IPVC between the HQ and Branch sites have the following IPVC Endpoints:

- IPVCEP.ACME_Calgary_HQ.01
- IPVCEP.ACME_Winnipeg_Branch.01
- IPVCEP.ACME_Vancouver_Branch.01
- IPVCEP.ACME_Montreal_Branch.01

The IPVC between the HQ and DC sites have the following IPVC Endpoints:

- IPVCEP.ACME_Calgary_HQ.02
- IPVCEP.ACME_Halifax_DC.01

Acme groups its business applications into three categories based on network performance requirements: voice, general data, backups. *Acme's* voice-over-IP (VOIP) application has stringent network delay and loss requirements. High quality voice conversations are an important aspect in *Acme's* business, justifying a premium cost for connectivity services that guarantee the required performance for this application. The VOIP gateway resides at the HQ site. VOIP traffic is required between the branch and HQ sites only; not the DC site. Employees of *Acme* work with large data files, requiring relatively frequent backups across the network at any time of the day. These backups are to receive best-effort performance from the network, not impacting the performance of any other application traffic flow. All other applications used by *Acme* fall into the category of "general data", having similar, modest performance requirements. All applications in this category are hosted at the *Acme* HQ site. These *Acme* application groupings are used in the selection of class-of-service (CoS) service options from *SP Alpha*. *SP Alpha* customers can select from four Bandwidth Profile (BWP) Flow options; per UNI, per UNI AL, per IPVC EP, and per CoS. *Acme* selects the "per CoS" BWP Flows option.

SP Alpha offers up to four CoS to Subscribers: High, Medium, Low, Best Effort. These four CoS are CoS Names, and these CoS Names map to standard CoS Labels as follows:

SP Alpha CoS Name	MEF 69.1 CoS Label
High	H
Medium	M
Low	no match
Best Effort	L

Table 20 – Mapping of *SP Alpha* CoS Name to MEF 69.1 CoS Label

Acme selects High CoS for its VOIP application, Medium CoS for general data, and Best Effort CoS for backups.

The IPVC List of Class of Service Names Service Attribute is set to the following for IPVC1:
[High, Medium, Best Effort]

The IPVC List of Class of Service Names Service Attribute is set to the following for IPVC2:
[Medium, Best Effort]

Acme estimates a need for 80Mb/s of peak traffic capacity at each branch office, 600Mb/s at the HQ site, and 200Mb/s at the DC site. 5Mb/s of committed capacity is required for VOIP at each branch and the HQ site. The remainder of committed capacity is required for general applications. The backup application will use any remaining available capacity at the site, with no performance commitment. Should the backup application introduce traffic that contends for network capacity with any other *Acme* application traffic, it is acceptable that the backup application be starved (e.g., the application will automatically reattempt after a time delay). These traffic capacity requirements apply to both directions (ingress and egress at each location).

The IPVC EP Ingress Bandwidth Profile Envelope Service Attribute and IPVC EP Egress Bandwidth Profile Envelope Service Attribute are set to the following to express the traffic requirements listed above for the Calgary HQ Site:

```
( MaxIR_E: 600Mb/s,
  T_E: 2 ms,
  Flows: [
   ( Flow Identifier: 1,
     Flow Definition:
       { ( IPVCEP.ACME_Calgary_HQ.01, High ) },
     CIR: 5,
     MaxIR: 5,
     Weight: 0,
     Burst Behavior: Optimize-Delay ),
   ( Flow Identifier: 2,
     Flow Definition:
       { ( IPVCEP.ACME_Calgary_HQ.01, Medium ) },
     CIR: 595,
     MaxIR: 600,
     Weight: 0,
     Burst Behavior: Optimize-Throughput ),
   ( Flow Identifier: 3,
     Flow Definition:
       { ( IPVCEP.ACME_Calgary_HQ.01, Best-Effort ) },
     CIR: 0,
     MaxIR: 600,
     Weight: 0,
     Burst Behavior: Optimize-Throughput ) ] )
```

Acme desires a Service Level Agreement that covers the greatest extent of the connectivity service provided by the Service Provider. This includes the measurement of the performance of the broadband circuit that connects *Acme* buildings *to SP Alpha* buildings. The selection of a Provider-Managed value for the UNI Management Type Service Attribute facilitates this requirement, as *SP Alpha* owns and manages the CE equipment and can place a measurement point on the CE.

SP Alpha offers a Service Level Agreement for the High class, guaranteeing performance for One-way Packet Loss Ratio and One-way Packet Delay metrics. *SP Alpha* guarantees 77 millisecond one-way packet delay performance at 95th percentile, and 0.025% one-way packet loss ratio for traffic between pairs of *Subscriber Acme* locations. This matches CPO values found Performance Tier 3 (PT3) of Table 7. Both metrics are measured monthly, starting from the date the two parties agreed the service was successfully delivered; on January 1st, 2019.

The IPVC Service Level Specification Service Attribute is set as following to express the SLS above:

```
( s: 00:00:00 on 1 January 2019,
  T: 1 Calendar Month,
  E: { ( Metric: One-way Packet Loss Ratio,
         C: High,
         S: {(IPVCEP.ACME_Calgary_HQ.01,
              IPVCEP.ACME_Winnipeg_Branch.01),
             (IPVCEP.ACME_Winnipeg_Branch.01,
              IPVCEP.ACME_Calgary_HQ.01),
             (IPVCEP.ACME_Calgary_HQ.01,
              IPVCEP.ACME_Vancouver_Branch.01),
              (IPVCEP.ACME_Vancouver_Branch.01,
               IPVCEP.ACME_Calgary_HQ.01),
             (IPVCEP.ACME_Calgary_HQ.01,
              IPVCEP.ACME_Montreal_Branch.01),
              (IPVCEP.ACME_Montreal_Branch.01,
                IPVCEP.ACME_Calgary_HQ.01)
            },
        $\hat{F}$: 0.025%
      ),
      ( Metric: One-way Packet Delay,
         C: High,
         S: {(IPVCEP.ACME_Calgary_HQ.01,
              IPVCEP.ACME_Winnipeg_Branch.01),
             (IPVCEP.ACME_Winnipeg_Branch.01,
              IPVCEP.ACME_Calgary_HQ.01),
             (IPVCEP.ACME_Calgary_HQ.01,
              IPVCEP.ACME_Vancouver_Branch.01),
              (IPVCEP.ACME_Vancouver_Branch.01,
               IPVCEP.ACME_Calgary_HQ.01),
             (IPVCEP.ACME_Calgary_HQ.01,
              IPVCEP.ACME_Montreal_Branch.01),
              (IPVCEP.ACME_Montreal_Branch.01,
               IPVCEP.ACME_Calgary_HQ.01)
           },
         $p$: 95,
      $\hat{d}$: 77 ms,
     ) },
  L: {}
)
```

The *Acme* network has accurately marked the DS QoS field packets for only the VOIP application, using decimal value 46. All other applications, including backups, may have any DS value (other than decimal value 46). The backup application can be identified by the backup server IP address: 192.168.1.200. No other application makes use of this server.

The following IPVC EP Ingress Class of Service Map Service Attribute setting is used at the Calgary_HQ location:

- *F* = [*IP DS, Destination IP Address*]
- *M* = [
  (46, 0/0) → "High",
  (0,192.168.1.200/32) → "Best-Effort",
  (1,192.168.1.200/32) → "Best-Effort",
  (2,192.168.1.200/32) → "Best-Effort",
  (3,192.168.1.200/32) → "Best-Effort",
  (4,192.168.1.200/32) → "Best-Effort",
  (5,192.168.1.200/32) → "Best-Effort",
  (6,192.168.1.200/32) → "Best-Effort",
  (7,192.168.1.200/32) → "Best-Effort",
  (8,192.168.1.200/32) → "Best-Effort",
  (9,192.168.1.200/32) → "Best-Effort",
  (10,192.168.1.200/32) → "Best-Effort",
  (11,192.168.1.200/32) → "Best-Effort",

(12,192.168.1.200/32) → “Best-Effort”,
(13,192.168.1.200/32) → “Best-Effort”,
(14,192.168.1.200/32) → “Best-Effort”,
(15,192.168.1.200/32) → “Best-Effort”,
(16,192.168.1.200/32) → “Best-Effort”,
(17,192.168.1.200/32) → “Best-Effort”,
(18,192.168.1.200/32) → “Best-Effort”,
(19,192.168.1.200/32) → “Best-Effort”,
(20,192.168.1.200/32) → “Best-Effort”,
(21,192.168.1.200/32) → “Best-Effort”,
(22,192.168.1.200/32) → “Best-Effort”,
(23,192.168.1.200/32) → “Best-Effort”,
(24,192.168.1.200/32) → “Best-Effort”,
(25,192.168.1.200/32) → “Best-Effort”,
(26,192.168.1.200/32) → “Best-Effort”,
(27,192.168.1.200/32) → “Best-Effort”,
(28,192.168.1.200/32) → “Best-Effort”,
(29,192.168.1.200/32) → “Best-Effort”,
(30,192.168.1.200/32) → “Best-Effort”,
(31,192.168.1.200/32) → “Best-Effort”,
(32,192.168.1.200/32) → “Best-Effort”,
(33,192.168.1.200/32) → “Best-Effort”,
(34,192.168.1.200/32) → “Best-Effort”,
(35,192.168.1.200/32) → “Best-Effort”,
(36,192.168.1.200/32) → “Best-Effort”,
(37,192.168.1.200/32) → “Best-Effort”,
(38,192.168.1.200/32) → “Best-Effort”,
(39,192.168.1.200/32) → “Best-Effort”,
(40,192.168.1.200/32) → “Best-Effort”,
(41,192.168.1.200/32) → “Best-Effort”,
(42,192.168.1.200/32) → “Best-Effort”,
(43,192.168.1.200/32) → “Best-Effort”,
(44,192.168.1.200/32) → “Best-Effort”,
(45,192.168.1.200/32) → “Best-Effort”,
(47,192.168.1.200/32) → “Best-Effort”,
(48,192.168.1.200/32) → “Best-Effort”,
(49,192.168.1.200/32) → “Best-Effort”,
(50,192.168.1.200/32) → “Best-Effort”,
(51,192.168.1.200/32) → “Best-Effort”,
(52,192.168.1.200/32) → “Best-Effort”,
(53,192.168.1.200/32) → “Best-Effort”,
(54,192.168.1.200/32) → “Best-Effort”,
(55,192.168.1.200/32) → “Best-Effort”,
(56,192.168.1.200/32) → “Best-Effort”,
(57,192.168.1.200/32) → “Best-Effort”,
(58,192.168.1.200/32) → “Best-Effort”,
(59,192.168.1.200/32) → “Best-Effort”,

(60,192.168.1.200/32) → "Best-Effort",
(61,192.168.1.200/32) → "Best-Effort",
(62,192.168.1.200/32) → "Best-Effort",
(63,192.168.1.200/32) → "Best-Effort"
]

- *D* = "Medium"

The following IPVC EP Ingress Class of Service Map Service Attribute setting is used at the Halifax_DC location:

- *F* = [*Source IP Address*]
- *M* = [(192.168.1.200/32) → "Best-Effort"]
- *D* = "Medium"

A.4 Subscriber IP VPN Extranet Service Use Case

Section 8.2 outlines the Subscriber IP VPN Extranet Service and provides a simple example topology. This appendix provides a more advanced use case, with two possible solutions that could be implemented by an SP.

A Subscriber *Acme Printing* has two locations, one office on 4th Street, another office on 8th Avenue. These provide two locations for customers to send and pickup document printing orders. Another Subscriber *Bank of MEF* has three locations, a branch office, head office and data center. *Bank of MEF* requires highly reliable connectivity to *Acme Printing* for printing transactions. *Bank of MEF* purchases an IP VPN Extranet service from SP *Alpha* for connectivity between all its locations to the two *Acme Printing* locations. *Acme Printing* has purchased an IP VPN Intranet service from SP *Alpha* between its 4th Street and 8th Avenue locations.

SP *Alpha* could design the IP VPN service used to interconnect these Subscribers in different ways. A single IPVC could be used, as shown in Figure 7 below. An IPVC with IPVC Topology Service Attribute set to *Rooted Multipoint* is used to provide extranet connectivity between these two Subscribers. The IPVC EP Role Service Attribute for *Bank of MEF* IPVC EPs is set to *Leaf*. The IPVC EP Role Service Attribute for *Acme Printing* IPVC EPs is set to *Root*. The IPVC EP Prefix Mapping Service Attribute is used for both the Intranet and Extranet IPVC EPs in Acme Printing, to ensure that different IP Prefixes are exposed in the Intranet vs the Extranet. This is necessary to comply with MEF 61.1 [8] R80.

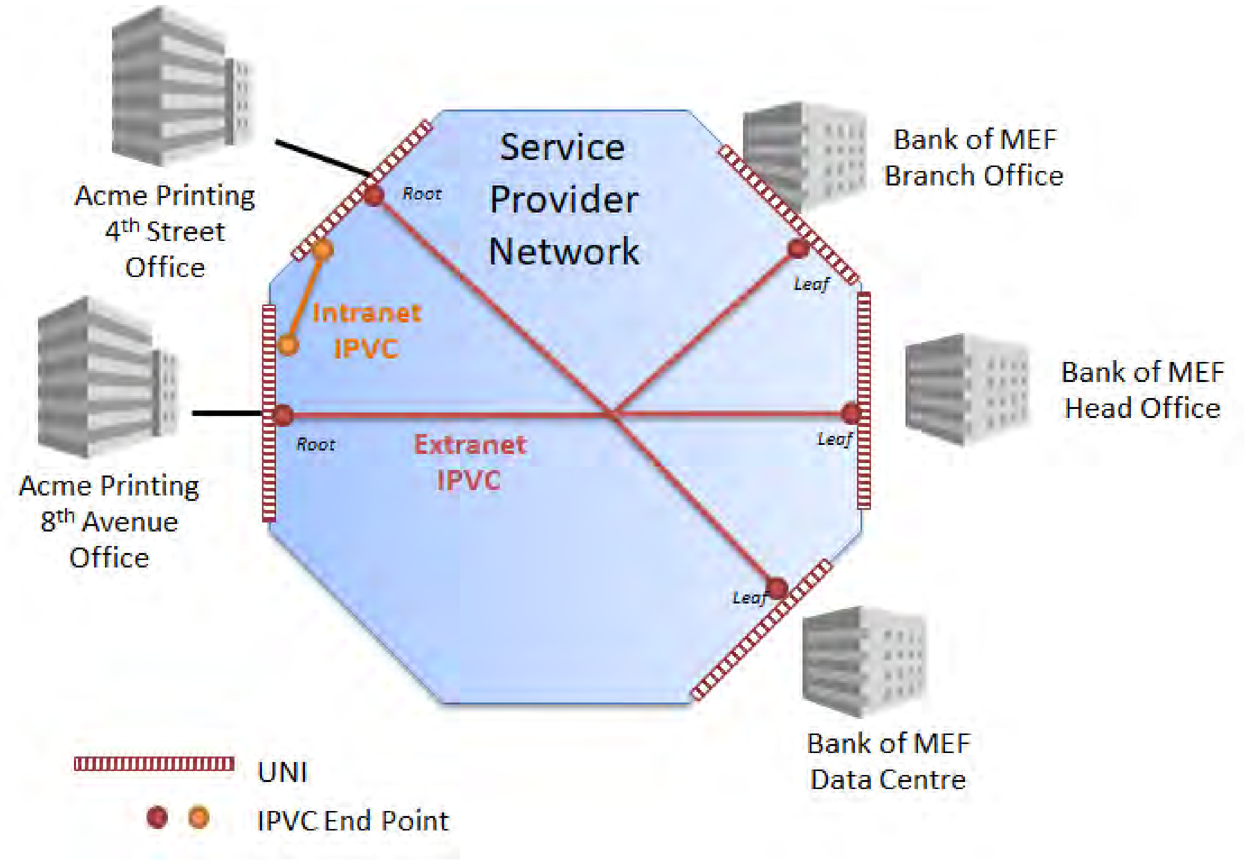

Figure 7 – IP VPN Extranet IPVC with two roots

A multiple IPVC design could also be used, as shown in an example in Figure 8 below. A pair of IPVCs each with IPVC Topology Service Attribute set to *Rooted Multipoint* is used. The IPVC EP Role Service Attribute for *Bank of MEF* IPVC EPs is set to *Leaf*. The IPVC EP Role Service Attribute for *Acme Printing* IPVC EPs is set to *Root*.

In both examples, one of the Subscribers has all IPVC EPs with the IPVC EP Role Service Attribute set to *Root*. The other Subscriber has all IPVC EPs with the IPVC EP Role Service Attribute set to *Leaf*. Both examples support Extranet services with more than two Subscribers. Where more than two Subscribers exist in an Extranet service, only a single Subscriber in the service has IPVC EPs with the IPVC EP Role Service Attribute set to *Root*. All other Subscribers in the Extranet service have IPVC EPs with the IPVC EP Role Service Attribute set to *Leaf*. The multiple IPVC example can be extended to support more than two locations with IPVC EP Role Service Attribute set to *Root* for the same Subscriber.

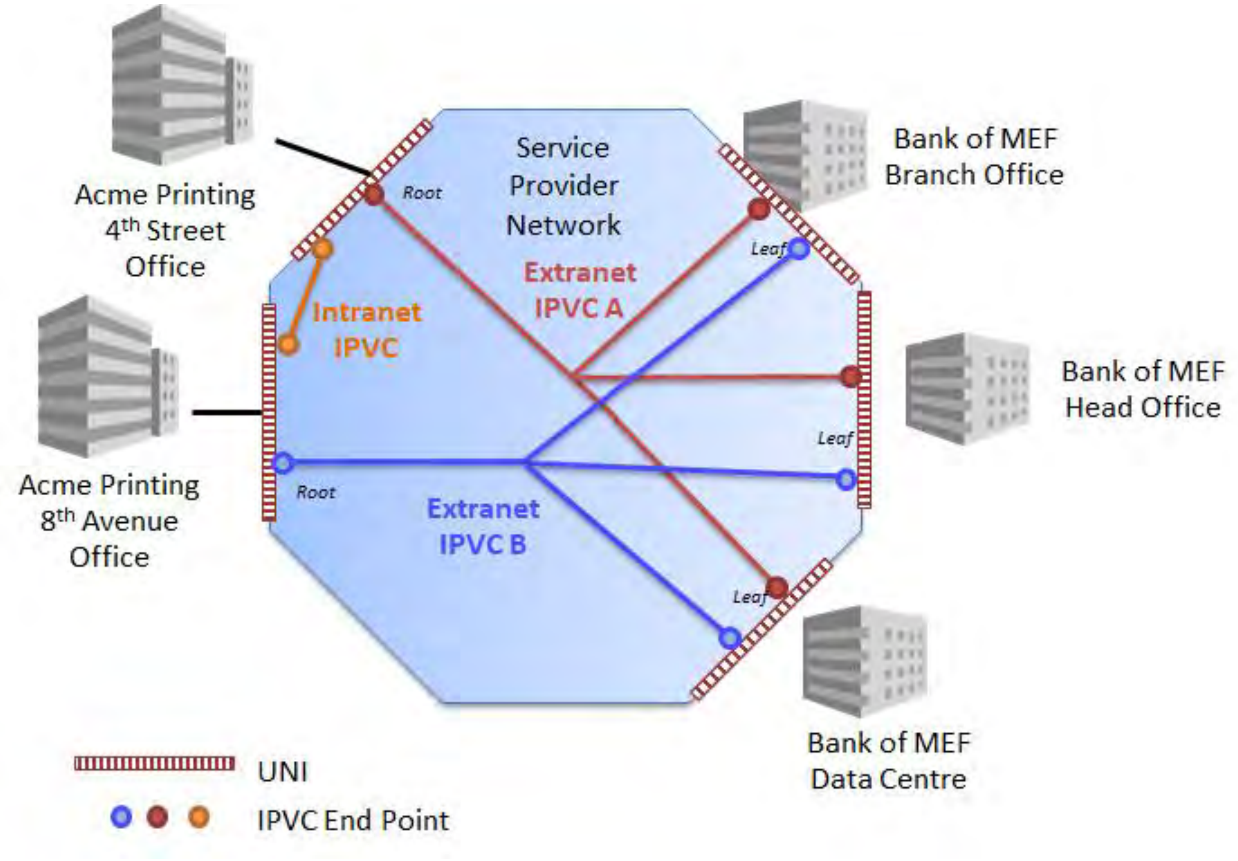

Figure 8 – Two IP VPN Extranet IPVCs

The single Extranet IPVC example has the following advantages:

- requires a minimal set of attributes to deliver the service (e.g., one IPVC, one IPVC endpoint per location, one ingress and one egress Class of Service map per location, etc)
- the addition of a new leaf or root to the service requires only a single IPVC endpoint and its associated attributes

The multiple Extranet IPVC example has the following advantages:

- intuitive traffic flow between locations of the same Subscriber. For the single IPVC design outlined in Figure 7 traffic between *Acme Printing* locations could traverse either the Intranet IPVC or the Extranet IPVC. The two IPVC design clearly segregates flows for Extranet service and Intranet service.
- allows for flexibility of applying different CoS Maps per IPVC EP

A.5 SOAM for Subscriber IP VPN Services

IP Services require a set of management tools for validating and maintaining the intended connectivity and performance delivered by the SP to the Subscriber. Fault Management (FM) tools are provided by the SP for use by the Subscriber to troubleshoot and isolate connectivity impairments. Performance Monitoring (PM) protocols are used within the SP network to validate the Subscriber IP VPN service is operating within performance objectives outlined in the SLS (Service Level Specification). A consistent implementation and provisioning of these tools and protocols on SP and Subscriber equipment is required to effectively utilize them for assurance tasks. MEF 66 [9] provides a set of implementation requirements to achieve this.

A.5.1 Fault Management

BFD and ICMP are two examples of FM tools. The BFD (Bidirectional Fault Detection) protocol is an important part of Subscriber IP VPN Services, ensuring faults that occur on the UNI Access Link are discovered and possibly mitigated in a timely fashion. BFD provides an alert to the SP and Subscriber that connectivity has been lost and may also be used to influence routing protocols to recover from the fault. When BFD is applied on the UNI Access Link, its messages are exchanged between Subscriber and Service Provider network equipment. Table 19 includes a set of constraints for Subscriber IP VPN Services that ensure the intended operation of this protocol, and provide guidelines to streamline provisioning.

ICMP is an important FM tool for network assurance, allowing either the SP or Subscriber to isolate the location and cause of interruptions in IP connectivity. It supports a Traceroute tool for validating the hop-by-hop network path Subscriber packets traverse and a Ping tool for validating connectivity to a particular hop or end IP destination. The requirements for peering different ICMP packets are described in MEF 66 [9] section 7.2.2, RFC 792 [1], and RFC 4443 [5]. These requirements provide the structure used to construct data models for APIs important for operational tasks performed by the SP and Subscriber.

When an ICMPv4 Echo or ICMPv6 Echo Request is sent from the Subscriber to SP, the ICMP Echo Response should use the DSCP value marked in the ICMP request. Subscribers should also support this capability, for ICMP packets initiated by the SP.

The Active End parameter of the UNI Access Link BFD Service Attribute for an IP Service identifies which equipment of the two parties, SP and Subscriber, that is responsible for the generation and reception of BFD packets. The equipment responsible for the Active End of BFD requires additional processing resources compared to the opposing end, as it must generate packets even when the BFD session is not established. SP equipment aggregates numerous Subscribers and IPVCs. Applying the Active End on SP equipment for all IP Services introduces a scalability challenge, requiring a significant amount of processing resources. For this reason, for IP Services, it is recommended that the Subscriber equipment be the Active End in requirement [D28]. If the Subscriber equipment is unable to support the Active End of the BFD, then the SP equipment should support the Active End.

A.5.2 Performance Monitoring

Performance Monitoring (PM) is the active measurement of the performance of IP Services. An SP uses PM tools to actively measure that the IP Service offered to a Subscriber is meeting the agreed upon performance objectives. Performance Monitoring is an important aspect of Subscriber IP VPN Services, providing a mechanism to continuously validate the quality of the service meets the requirements of Subscriber applications. MEF 66 [9] defines use cases, tool requirements and deployment guidelines used in the implementation of PM for IP Services. MEF 66 [9] identifies three PM tools in section 9.4: TWAMP, TWAMP-Lite and STAMP.

If the Subscriber IP VPN service offered to the Subscriber includes a CoS with performance objectives in the SLS, the SP should implement PM for that CoS Name and provide reports to the Subscriber. A SP could choose to offer CoS performance objectives without implementing PM, but would experience difficulties in managing Subscriber inquiries for performance violations that occurred in the past.

MEF 66 [9] in section 9.1 defines two methods for active PM Measurement: Location to Location or IPVC Monitoring. The SP should identify to the Subscriber which of these two methods are being used for the SLS. A clear understanding between the two parties of the method chosen by the SP's PM implementation is useful in the design of the Subscriber's own PM solution, and for performance-related assurance activities.

Appendix B Major Changes from MEF 69 to MEF 69.1

The following list represents the major changes in this standard, MEF 69.1, from the previous version, MEF 69 [10]:

- Added the Subscriber IP VPN Service (Sections 8 and 10)
- Added Subscriber IP VPN Service use cases (Appendix A.3 and A.4)
- Clarified the terminology:
    - Internet Access Service -> Subscriber Internet Access Service
- Added [D3] recommending IPVC DSCP Preservation be *Disabled* for the Internet Access Service (Section 9.1)
- Added [R15] requiring the UNI Identifier in the IPVC EP EI attribute be unique across all Basic Internet Access Services (Section 9.2)
- Added [D11] recommending UNI Reverse Path Forwarding be *Enabled* for the Internet Access Service (Section 9.3)
- Removed the Summary of Constrained Attributes appendix