Independent Submission
Request for Comments: 7297
Category: Informational
ISSN: 2070-1721

M. Boucadair
C. Jacquenet
France Telecom
N. Wang
University of Surrey

July 2014

IP Connectivity Provisioning Profile (CPP)

Abstract

This document describes the Connectivity Provisioning Profile (CPP) and proposes a CPP template to capture IP/MPLS connectivity requirements to be met within a service delivery context (e.g., Voice over IP or IP TV). The CPP defines the set of IP transfer parameters to be supported by the underlying transport network together with a reachability scope and bandwidth/capacity needs. Appropriate performance metrics, such as one-way delay or one-way delay variation, are used to characterize an IP transfer service. Both global and restricted reachability scopes can be captured in the CPP.

Such a generic CPP template is meant to (1) facilitate the automation of the service negotiation and activation procedures, thus accelerating service provisioning, (2) set (traffic) objectives of Traffic Engineering functions and service management functions, and (3) improve service and network management systems with 'decision-making' capabilities based upon negotiated/offered CPPs.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7297.

Table of Contents

1. Introduction

This document describes the Connectivity Provisioning Profile (CPP) and proposes a CPP template to capture IP/MPLS connectivity requirements to be met within a service delivery context (e.g., Voice over IP, IP TV, and VPN services).

In this document, the IP connectivity service is the IP transfer capability characterized by a (Source Nets, Destination Nets, Guarantees, Scope) tuple where "Source Nets" is a group of unicast IP addresses, "Destination Nets" is a group of IP unicast and/or multicast addresses, and "Guarantees" reflects the guarantees (expressed in terms of Quality Of Service (QoS), performance, and availability, for example) to properly forward traffic to the said "Destination". Finally, the "Scope" denotes the (network) perimeter (e.g., between Provider Edge (PE) routers or Customer Nodes) where the said guarantees need to be provided.

1.1. Connectivity Provisioning Interface (CPI)

Figure 1 shows the various connectivity provisioning interfaces covered by CPP: the Customer-Network CPI, the Service-Network CPI, and the Network-Network CPI. Services and applications whose parameters are captured by means of a CPP exchanged through the Service-Network CPI may be provided by the same administrative entity that operates the underlying network or by another entity (for example, a Content Provider).

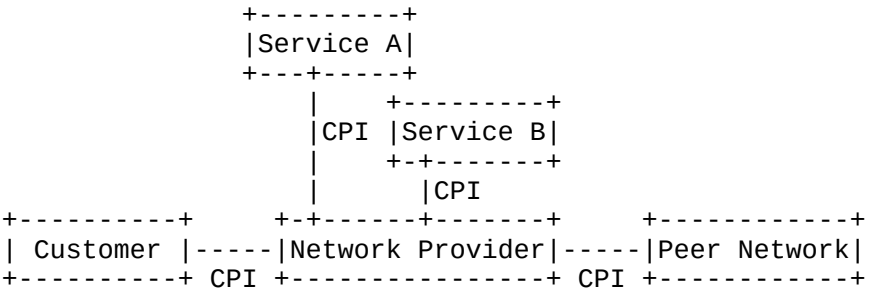

Figure 1: Connectivity Provisioning Interfaces

The interfaces depicted in Figure 1 can be summarized as shown in Figure 2.

The Customer shown in Figure 2 may be another Network Provider (e.g., an IP transit provider), a Service Provider (e.g., an IP telephony Service Provider) that requires the invocation of resources provided by a Network Provider, or an enterprise that wants to interconnect

its various sites by subscribing to a VPN service provided by a Network Provider. The proposed CPP can be used to expose, capture, and facilitate the negotiation of the service parameters between these various entities, thereby presenting a common template for describing the available connectivity services.

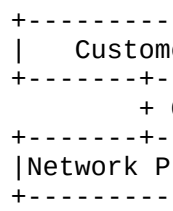

Figure 2: CPP: Generic Connectivity Provisioning Interfaces

In the rest of this document, "Customer" is used as a generic term to denote the business entity that subscribes to connectivity services offered by a Network Provider (see Figure 2).

1.2. Rationale

Procedures for the design and the operation of IP services have become increasingly diverse and complex. The time it takes to negotiate service parameters and then proceed with the corresponding resource allocation can thus be measured in days, if not weeks. Yet, experience has shown that the bilateral discussions that usually take place between a Customer and a Network Provider never rely upon some kind of standard checklist where the Customer would be invited to tick all the parameters that apply to its environment. These parameters would then be negotiated with the Network Provider, as a function of the available resources, the Customer’s expectations, the provider’s network planning policy, etc.

The definition of a clear interface between the service (including third-party applications) and the network layers would therefore facilitate the said discussion, thereby improving the overall service delivery procedure by optimizing the design of the network infrastructures. Indeed, the CPP interface aims at exposing and characterizing, in a technology-agnostic manner, the IP transfer requirements to be met when invoking IP transfer capabilities of a network operated by a Network Provider between a set of Customer Nodes (e.g., Multimedia Gateway (Section 11.2.7 of [RFC2805]), Session Border Controller [RFC5853], etc.).

These requirements include: reachability scope (e.g., limited scope, Internet-wide), direction, bandwidth requirements, QoS parameters (e.g., one-way delay [RFC2679], loss [RFC2680], or one-way delay variation [RFC3393]), protection, and high-availability guidelines (e.g., restoration in less than 50 ms, 100 ms, or 1 second).

These requirements are then translated into IP/MPLS-related technical clauses (e.g., need for recovery means, definition of the class of service, need for control-plane protection, etc.). In a later stage, these various clauses will be addressed by the activation of adequate network features and technology-specific actions (e.g., Multiprotocol Label Switching Traffic Engineering (MPLS-TE, [RFC3346]), Resource Reservation Protocol (RSVP, [RFC2205]), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), etc.), by means of CPP-derived configuration information.

For traffic conformance purposes, a CPP also includes flow identification and classification rules to be followed by participating nodes whenever they have to process traffic according to a specific service as defined by the said CPP.

The CPP template aims to capture connectivity needs and to represent and value these requirements in a standardized manner. Service- and Customer-specific IP provisioning rules may lead to a dramatic increase of the number of IP transfer classes that need to be (pre-)engineered in the network. Instantiating each CPP into a distinct class of service should therefore be avoided for the sake of performance and scalability.

Therefore, application-agnostic IP provisioning practices should be recommended, since the requirements captured in the CPP can be used to identify which network class of service is to be used to meet those requirements/guarantees. From that standpoint, the CPP concept is meant to design a limited number of generic classes so that individual CPP documents, by capturing the connectivity requirements of services, applications, and Customers, can be easily mapped to these classes.

CPP may also be used as a guideline for network dimensioning and planning teams of a Network Provider to ensure that appropriate resources (e.g., network cards, routers, link capacity, etc.) have been provisioned. Otherwise, (underlying) transport networks would not be able to meet the objectives expressed in all CPP requests.

Such a generic CPP template:

- Facilitates the automation of the service negotiation and activation procedures, thus improving service delivery times;

- Can help set Traffic Engineering function and service management function objectives, for example, as a function of the number of CPP templates to be processed over a specific period of time; and

- Improves service and network management systems by adding 'decision-making' capabilities based upon negotiated/offered CPPs.

In addition, this CPP abstraction makes a clear distinction between the connectivity provisioning requirements and the associated technology-specific rules that need to be applied by participating nodes and that are meant to accommodate such requirements.

The CPP defines the set of IP/MPLS transfer guarantees to be offered by the underlying transport network together with a reachability scope and capacity needs. Appropriate performance metrics, such as one-way delay or one-way delay variation, are used to characterize the IP transfer service. Guarantees related to availability and resiliency are also included in the CPP.

The CPP can be used in an integrated business environment (where the service and network infrastructures are managed by the same administrative entity) or another business environment (where an administrative entity manages the service while another manages the network infrastructure). In the following sections, no assumption is made about the business environment (integrated or not).

Service differentiation at the network layer can be enforced by tweaking various parameters that belong to distinct dimensions (e.g., forwarding, routing, processing of incoming traffic, traffic classification, etc.). This document does not make any assumption on how network services are implemented within a networking infrastructure.

Activating unicast or multicast capabilities to deliver a connectivity service can be explicitly requested by a Customer in a CPP or can be an engineering decision of a Network Provider based on the analysis of the Customer connectivity provisioning requirements.

Examples of CPP usage include the northbound interface introduced by the Application-Based Network Operations (ABNO) framework [NET-OPS] and the technique for exposing network services and their characteristics defined in [RFC7149].

1.3. Reference Architecture

Customer Nodes belong to a Customer (including corporate Customers) or a service infrastructure (see Figure 1). In some contexts, Customer Nodes can be provided and managed by the Network Provider. The connectivity between these Customer Nodes reflects the IP transfer capability implemented thanks to the allocation of a set of IP resources. IP transfer capabilities are considered by higher-layer services (such as transport- and application-layer services) as black boxes. Appropriate notifications and reports would be communicated (through dedicated means) to Customer Nodes to assess the compliance of the experienced IP transfer service against what has been negotiated with the corresponding CPP. These notifications may also be used to assess the efficiency of the various policies enforced in the networking infrastructure to accommodate the requirements detailed in the CPP.

The CPP reference architectures are depicted in Figures 3, 4, and 5.

The Customer infrastructure can be connected over networking infrastructures managed by one or several Network Providers.

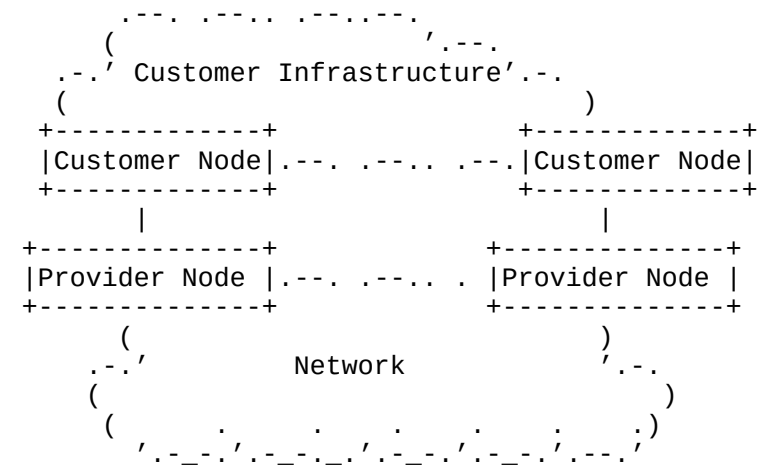

Figure 3: Reference Architecture: Connectivity Service Provided by the Same Network Provider Using Distinct Interconnection Nodes

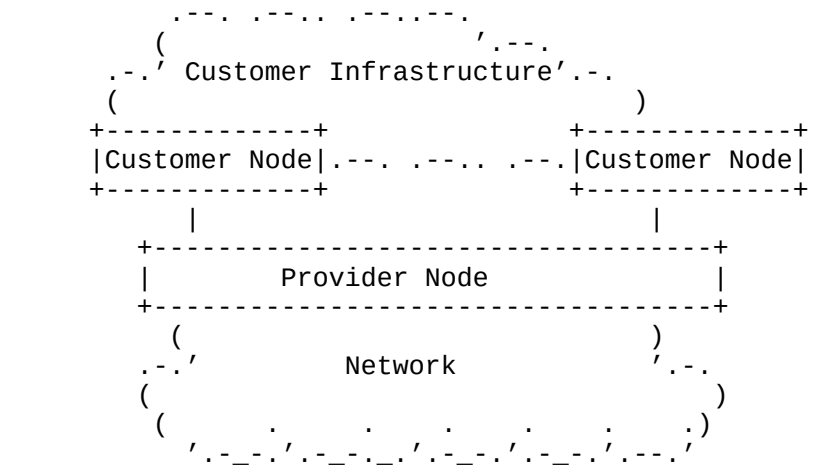

Figure 4: Reference Architecture: Connectivity Service Provided by the Same Network Provider Using a Single Interconnection Node

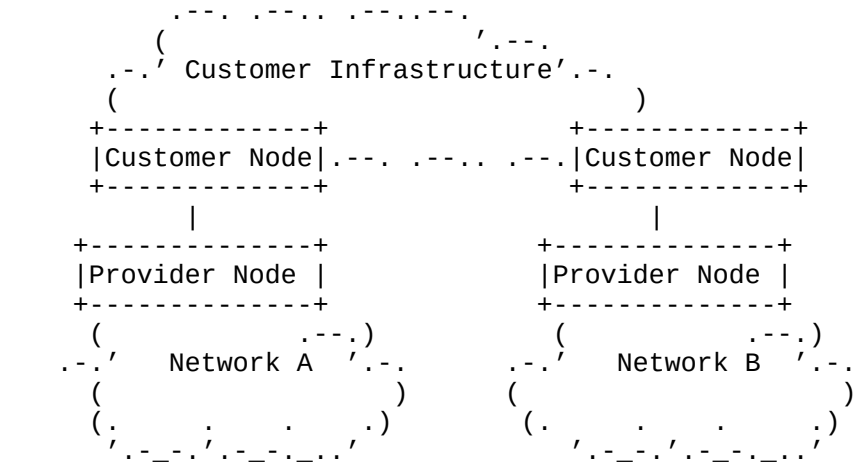

Figure 5: Reference Architecture: Connectivity Services Provided by Distinct Network Providers

2. Scope of This Document

This document details the clauses of the CPP. Candidate protocols (e.g., [CPNP]) that can be used to negotiate and enforce a given CPP are not discussed in this document.

In addition to CPP clauses, other clauses may be included in an agreement between a Customer and a Provider (e.g., contact point, escalation procedure, incidents management, billing, etc.). It is out of the scope of this document to detail all those additional clauses.

Examples of how to translate CPP clauses into specific policies are provided for illustration purposes. It is out of the scope of this document to provide an exhaustive list of the technical means to meet the objectives detailed in a CPP.

CPP was mainly designed to target IP connectivity services. Nevertheless, it can be used for other non-IP transport schemes. It is out of the scope of this document to assess the applicability of CPP to these non-IP schemes.

This document covers both unicast and multicast connectivity services. Both Any-Source Multicast (ASM, [RFC1112]) and Source-Specific Multicast (SSM, [RFC4607]) modes can be captured in a CPP.

3. Connectivity Provisioning Profile (CPP)

A CPP can be seen as the inventory of connectivity provisioning requirements with regard to the IP transfer service. CPP clauses are elaborated in the following sub-sections. The CPP template is provided in Section 4.

3.1. Customer Nodes Map

A CPP must include the list of Customer Nodes (e.g., Customer Edges (CEs)) to be connected to the underlying IP transport network.

These nodes should be unambiguously identified (e.g., using a unique Service_identifier, Media Access Control (MAC) addresses, etc.). For each Customer Node, a border link or a node that belongs to the domain that connects the Customer Nodes should be identified.

This clause can specify geolocation information of Customer Nodes.

Based on the location of the Customer Node, appropriate operations to retrieve the corresponding border link or "Provider Node" (e.g., PE) should be undertaken. This operation can be manual or automated.

A "service site" would be located behind a given Customer Node. A site identifier may be captured in the CPP for the provisioning of managed VPN services [RFC4026], for instance, Site_identifier.

A Customer Node may be connected to several Provider Nodes. Multiple Customer Nodes may be connected to the same Provider Node as shown in Figure 4.

3.2. Scope

The scope clause specifies the reachability of each of the involved Customer Nodes, from both incoming and outgoing traffic perspectives, thereby yielding specific traffic directionality considerations. It is defined as an unidirectional parameter. Both directions should be described in the CPP.

The reachability scope specifies the set of destination prefixes that can be reached from a given Customer site (identified by a group of source prefixes). Both global and restricted reachability scopes can be captured in the CPP. A global reachability scope means that a Customer site can reach any destination in the Internet and can be reached from any remote host. A restricted reachability scope means no global reachability is allowed; only a set of destinations can be reached from a Customer site, and/or only a set of sources can reach the Customer site. Both incoming and outgoing reachability scopes are specified in the CPP.

Both IPv4 and IPv6 reachability scopes may be specified.

The reachability scope clause can include multicast and/or unicast addresses. For SSM, a group of unicast source addresses can be specified in addition to destination multicast addresses.

The scope clause can also be used to delimit a topological (or geographical) network portion beyond which the performance and availability guarantees do not apply. A scope may be defined by a set of "Ingress" points and "Egress" points. Several types may be considered, such as:

(1) "1:1" Pipe model. Only point-to-point communications are allowed.

(2) "1:N" Hose model. Only communications from one site towards a set of destinations are allowed.

(3) "1:any" Unspecified hose model. All outbound communications are allowed.

The Ingress and Egress points could be Customer Nodes / Provider Nodes or external nodes, provided that these nodes are unambiguously identified (e.g., IPv6 prefix), or a set of IP destinations.

3.3. QoS Guarantees

QoS guarantees denote a set of IP transfer performance metrics that characterize the quality of the IP transfer treatment to be experienced (when crossing an IP transport infrastructure) by a flow issued from or forwarded to a (set of) "Customer Node(s)".

IP performance metrics can be expressed as qualitative or quantitative parameters (both quantitative and qualitative guarantees cannot be specified in the same CPP). Quantitative guarantees may be specified as an average value, as a maximum bound, or as a percentile over an interval of measurements that should be indicated in the measurement method.

Several performance metrics have been defined, such as:

- Traffic Loss [RFC2680]
- One-way delay [RFC2679]
- One-way delay variation [RFC3393]

These parameters may be specific to a given path or a given scope (e.g., between two Customer Nodes). IP performance metric values indicated in a CPP should reflect the measurement between a set of Customer Nodes or between a Customer Node and a set of Provider Nodes.

Quantitative guarantees can only be specified for in-profile traffic (i.e., up to a certain traffic rate). A CPP can include throughput guarantees; when specified, these guarantees are equivalent to quantitative or qualitative loss guarantees.

The Meta-QoS-Class concept can be used when qualitative metrics are used [RFC5160].

3.4. Availability

This clause specifies the percentage of the time during which the agreed IP performance guarantees apply. The clause can be expressed as a maximum or an average. The exact meaning of the clause value is defined during the CPP negotiation process.

The guarantees cover both QoS deterioration (i.e., IP transfer service is available, but it is below the agreed performance bounds), physical failures, or service unavailability in general. In order to meet the availability guarantees, several engineering practices may be enforced at the border between the Customer and the Network Provider, such as multi-homing designs.

The following mechanisms are provided as examples to show that different technical options may be chosen to meet the service availability objectives:

- When an Interior Gateway Protocol (IGP) instance is running between the "Customer Node" and the "Provider Node", activate a dedicated protocol, such as Bidirectional Forwarding Detection (BFD, [RFC5881][RFC5883]), to control IGP availability and to ensure sub-second IGP adjacency failure detection.

- Use of the Label Switched Path Ping (LSP Ping) capability to detect LSP availability (check whether the LSP is in place or not) [RFC4379][RFC6424][RFC6425][RFC6426][RFC6829].

- Pre-install backup LSPs for fast-reroute purposes when an MPLS network connects Customer Nodes [RFC4090].

- Enable Virtual Router Redundancy Protocol (VRRP, [RFC5798]).

- Enable IP Fast Reroute features (e.g., [RFC5286] or [RFC6981]).

3.5. Capacity

This clause characterizes the required capacity to be provided by the underlying IP transport network. This capacity is bound to a defined "Scope" (see Section 3.2) and IP transfer performance guarantees (see Sections 3.3 and 3.4).

The capacity may be expressed for both traffic directions (i.e., incoming and outgoing) and for every border link. The capacity clause defines the limits of the application of quantitative guarantees.

It is up to the administrative entity, which manages the IP transport network, to appropriately dimension its network [RFC5136] to meet the capacity requirements expressed in all negotiated CPPs.

3.6. Conformance Traffic

When capacity information (see Section 3.5) is included in the CPP, requirements for out-of-profile traffic treatment need to be also expressed in the CPP.

Shaping/policing filters may be applied so as to assess whether traffic is within the capacity profile or out of profile. Out-of-profile traffic may be discarded or assigned another class (e.g., using Lower Effort Per-Domain Behavior (LE PDB) [RFC3662]).

Packet MTU conditions may also be indicated in the CPP.

3.7. Overall Traffic Guarantees

Overall traffic guarantees are defined when the Capacity (Section 3.5) and Conformance Traffic (Section 3.6) clauses are not specified. Or, if they are actually specified, then out-of-profile traffic is assigned another class of service but is not discarded. Such guarantees can only be qualitative delay and/or qualitative loss or throughput guarantees.

If overall traffic guarantees are not specified, best effort forwarding is implied.

3.8. Traffic Isolation

This clause indicates if the traffic issued by or destined to "Customer Nodes" should be isolated when crossing the IP transport network. This clause can also be used to specify additional security protection requirements (including privacy protection requirements).

This clause can then be translated into VPN policy provisioning information, such as the information pertaining to the activation of dedicated tunnels using IPsec, BGP/MPLS VPN facilities [RFC4364], or a combination thereof. The activation of such features should be consistent with the availability and performance guarantees that have been negotiated.

3.9. Flow Identification

To identify the flows that need to be handled within the context of a given CPP, flow identifiers should be indicated in the CPP. Flow identifiers are used for traffic classification purposes. An example of packet classifier is defined in [RFC2475].

A flow identifier may be composed of (but not limited to) the following parameters:

- Source IP address,
- Source port number,
- Destination IP address,
- Destination port number,
- Type of Service (ToS) or Differentiated Services Code Point (DSCP) field,
- Tail-end tunnel endpoint, or
- Any combination thereof.

Distinct treatments may be implemented for elastic and non-elastic traffic (e.g., see the "Constraints on traffic" clause defined in [RFC5160]).

Flow classification rules may be specific to a given link or may be applied for a group or all border links. This should be clearly captured in the CPP.

Some practices such as DSCP re-marking may be indicated in the CPP. Re-marking action is under the responsibility of underlying nodes that intervene to deliver the connectivity service. Re-marking can be enforced for both outgoing and incoming traffic received from or destined to Customer Nodes. These re-marking actions must not alter the service-specific marking integrity (e.g., VPN service).

This clause may specify policies (e.g., DSCP re-marking) to be enforced at the egress nodes on packets received from Customer Nodes. If no such policy is specified, the Network Provider enforces its local policies (e.g., clear DSCP marking) on packets leaving its administrative domain.

3.10. Routing and Forwarding

This clause is used to specify outsourced routing actions, such as installing dedicated routes to convey the traffic to its (service) destination. These dedicated routes may be computed, selected, and installed for Traffic Engineering or resilience purposes. For Traffic Engineering, these paths can be used to intelligently divert traffic away from some nodes/links that may potentially suffer from

congestion or avoid crossing competitors' networks. For resilience, backup paths are typically pre-installed in order to bypass nodes/ links under protection.

This clause is also used to specify intermediate functions that must be invoked in the forwarding path (e.g., redirect the traffic to a firewall, invoke topology hiding features, etc.) or specify geographic routing restrictions.

A requirement for setting up a logical routing topology [RFC4915] [RFC5120] may also be considered, e.g., to facilitate the management of the nodes that are involved in the forwarding of the traffic as defined in the CPP.

This practice should be indicated in the CPP; otherwise, path computation is left to the underlying IP routing capabilities. The forwarding behavior (e.g., Per-Domain Behavior (PDB) [RFC3086]) may also be specified in a CPP but remains optional. If indicated, consistency with the IP performance bounds defined in the CPP should be carefully ensured.

For illustration purposes, a routing policy would avoid satellite links for Voice over IP (VoIP) deployments since this may degrade the offered service.

3.11. Activation Means

This clause indicates the required action(s) to be undertaken to activate access to the IP connectivity service.

Examples of these actions would be the activation of an IGP instance, the establishment of a BGP [RFC4271] or Multiprotocol BGP (MP-BGP) session [RFC4760], Protocol Independent Multicast (PIM, [RFC4601]), etc.

3.12. Invocation Means

Two types are defined:

Implicit: This clause indicates that no explicit means to invoke the connectivity service is required. Access to the connectivity service is primarily conditioned by the requested network capacity.

Explicit: This clause indicates the need for explicit means to access the connectivity service. Examples of such means include the use of RSVP [RFC2205], RSVP-TE [RFC3209], Internet Group Management Protocol (IGMP, [RFC3376]), or Multicast Listener Discovery (MLD, [RFC3810]). Appropriate admission control procedures [RFC6601] would have to be enforced, e.g., to check whether the capacity actually used is not above the agreed threshold.

3.13. Notifications

For operation purposes (e.g., supervision) and service fulfillment needs, management platforms need to be notified about critical events that may impact the delivery of the service.

The notification procedure should be indicated in the CPP. This procedure may specify the type of information to be sent, the interval, the data model, etc.

Notifications can be sent to the management platform by using Simple Network Management Protocol (SNMP, [RFC3416]), Syslog notifications [RFC5424], Connectivity Provisioning Negotiation Protocol (CPNP) signals [CPNP], Network Configuration Protocol (NETCONF) Event Notifications [RFC5277], or a phone call!

4. CPP Template

Figure 6 provides the Routing Backus-Naur Form (RBNF, [RFC5511]) format of the CPP template.

A CPP document includes several connectivity provisioning components; each of these is structured as a CPP. The CPP may include additional optional information elements such as metrics used for Service Assurance purposes, activation schedule, etc.

```
<CONNECTIVITY_PROVISIONING_DOCUMENT> ::=
                            <Connectivity Provisioning Component> ...
<Connectivity Provisioning Component> ::=
                            <CONNECTIVITY_PROVISIONING_PROFILE> ...
<CONNECTIVITY_PROVISIONING_PROFILE> ::=
                            <Customer Nodes Map>
                            <Scope>
                            <QoS Guarantees>
                            <Availability>
                            <Capacity>
                            <Traffic Isolation>
                            <Conformance Traffic>
                            <Flow Identification>
                            <Overall Traffic Guarantees>
                            <Routing and Forwarding>
                            <Activation Means>
                            <Invocation Means>
                            <Notifications>
                            <Optional Information Element> ...
<Customer Nodes Map> ::=  <Customer Node> ...
<Customer Node> ::=  <IDENTIFIER>
                     <LINK_IDENTIFIER>
                     <LOCALIZATION>
```

Figure 6: CPP Template

The description of these clauses is provided in Section 3.

The CPP may also include a Customer’s administrative information, such as a name and other contact details. An example of the RBNF format of the Customer’s information is shown in Figure 7.

```
<Customer Description> ::= <NAME> <Contact Information>
<Contact Information> ::=  <EMAIL_ADDRESS> [<POSTAL_ADDRESS>]
                           [<TELEPHONE_NUMBER> ...]
```

Figure 7: Customer Description Clause

The CPP may include administrative information of the Network Provider too (name, Autonomous System number(s), and other contact details). An example of the RBNF format of the provider’s information is shown in Figure 8.

```
<Provider Description> ::= <NAME><Contact Information>[<AS_NUMBER>]
<Contact Information> ::=  <EMAIL_ADDRESS> [<POSTAL_ADDRESS>]
                           [<TELEPHONE_NUMBER> ...]
```

Figure 8: Provider Description Clause

5. Security Considerations

This document does not define an architecture or specify a protocol. Yet, the means to provide guarantees about the identity of a Customer and its ability to expose connectivity requirements to a Network Provider through a CPP need to be investigated. Likewise, the means to provide guarantees about the identity of a Network Provider and the ability to expose its capabilities, let alone capture the requirements of a Customer through a CPP, should be carefully studied.

CPP documents should be protected against illegitimate modifications (e.g., modification, withdrawal); authorization means should be enabled. These means are deployment-specific.

The Network Provider must enforce means to protect privacy-related information captured in a CPP document [RFC6462]. In particular, this information must not be revealed to external parties without the consent of Customers. Network Providers should enforce policies to make Customer fingerprinting more difficult to achieve. For more discussion about privacy, refer to [RFC6462] and [RFC6973].

6. Acknowledgements

Some of the items in this document are the result of several discussions with E. Mykoniati and D. Griffin. Special thanks to them.

Many thanks to P. Georgatsos for the discussions and the detailed review of this document.

Thanks to S. Shah, G. Huston, D. King, and S. Bryant for reviewing the document and providing useful comments.

7. Informative References

[CPNP] Boucadair, M., Jacquenet, C., and D. Zhang, "Connectivity Provisioning Negotiation Protocol (CPNP)", Work in Progress, June 2014.

[NET-OPS] King, D. and A. Farrel, "A PCE-based Architecture for Application-based Network Operations", Work in Progress, February 2014.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

[RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[RFC2679] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Delay Metric for IPPM", RFC 2679, September 1999.

[RFC2680] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, September 1999.

[RFC2805] Greene, N., Ramalho, M., and B. Rosen, "Media Gateway Control Protocol Architecture and Requirements", RFC 2805, April 2000.

[RFC3086] Nichols, K. and B. Carpenter, "Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification", RFC 3086, April 2001.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3346] Boyle, J., Gill, V., Hannan, A., Cooper, D., Awduche, D., Christian, B., and W. Lai, "Applicability Statement for Traffic Engineering with MPLS", RFC 3346, August 2002.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[RFC3393] Demichelis, C. and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", RFC 3393, November 2002.

[RFC3416] Presuhn, R., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002.

[RFC3662] Bless, R., Nichols, K., and K. Wehrle, "A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services", RFC 3662, December 2003.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC4026] Andersson, L. and T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026, March 2005.

[RFC4090] Pan, P., Swallow, G., and A. Atlas, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, May 2005.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

[RFC4379] Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", RFC 4379, February 2006.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.

[RFC4915] Psenak, P., Mirtorabi, S., Roy, A., Nguyen, L., and P. Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC 4915, June 2007.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, February 2008.

[RFC5136] Chimento, P. and J. Ishac, "Defining Network Capacity", RFC 5136, February 2008.

[RFC5160] Levis, P. and M. Boucadair, "Considerations of Provider-to-Provider Agreements for Internet-Scale Quality of Service (QoS)", RFC 5160, March 2008.

[RFC5277] Chisholm, S. and H. Trevino, "NETCONF Event Notifications", RFC 5277, July 2008.

[RFC5286] Atlas, A. and A. Zinin, "Basic Specification for IP Fast Reroute: Loop-Free Alternates", RFC 5286, September 2008.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.

[RFC5511] Farrel, A., "Routing Backus-Naur Form (RBNF): A Syntax Used to Form Encoding Rules in Various Routing Protocol Specifications", RFC 5511, April 2009.

[RFC5798] Nadas, S., "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 5798, March 2010.

[RFC5853] Hautakorpi, J., Camarillo, G., Penfield, R., Hawrylyshen, A., and M. Bhatia, "Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments", RFC 5853, April 2010.

[RFC5881] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881, June 2010.

[RFC5883] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for Multihop Paths", RFC 5883, June 2010.

[RFC6424] Bahadur, N., Kompella, K., and G. Swallow, "Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels", RFC 6424, November 2011.

[RFC6425] Saxena, S., Swallow, G., Ali, Z., Farrel, A., Yasukawa, S., and T. Nadeau, "Detecting Data-Plane Failures in Point-to-Multipoint MPLS - Extensions to LSP Ping", RFC 6425, November 2011.

[RFC6426] Gray, E., Bahadur, N., Boutros, S., and R. Aggarwal, "MPLS On-Demand Connectivity Verification and Route Tracing", RFC 6426, November 2011.

[RFC6462] Cooper, A., "Report from the Internet Privacy Workshop", RFC 6462, January 2012.

[RFC6601] Ash, G. and D. McDysan, "Generic Connection Admission Control (GCAC) Algorithm Specification for IP/MPLS Networks", RFC 6601, April 2012.

[RFC6829] Chen, M., Pan, P., Pignataro, C., and R. Asati, "Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6", RFC 6829, January 2013.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

[RFC6981] Bryant, S., Previdi, S., and M. Shand, "A Framework for IP and MPLS Fast Reroute Using Not-Via Addresses", RFC 6981, August 2013.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, March 2014.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes 35000
France

EMail: mohamed.boucadair@orange.com

Christian Jacquenet
France Telecom
Rennes 35000
France

EMail: christian.jacquenet@orange.com

Ning Wang
University of Surrey
Guildford
UK

EMail: n.wang@surrey.ac.uk