TELECOM INFRA PROJECT

Open BNG

Technical Requirements

Date 16 June 2021

Document version: v2.0

Authors

Konstantinos Antoniou

Senior Researcher, BT

Brendan Black

Network Engineer, Vodafone

Jesús Luis Folgueira Chavarria

Transport Senior Manager, CTIO, Telefónica

Frank Geilhardt

Broadband Access Architect, Deutsche Telekom AG

Paul Gunning

Principal Researcher, BT

Ayman Hamza

Senior Broadband Access Architect, Vodafone

Mario Kind

Research & Development Engineer, Deutsche Telekom AG

Rafael A. Lopez da Silva

Technological Expert, CTIO, Telefónica

Jonathan Newton

Principal Engineer, Vodafone

Rafael Canto Palancar

Transport & IP Network Manager, CTIO, Telefónica

Rosaria Persico

Senior Engineer, Telecom Italia

Peter Willis

Senior Manager Software Based Networks, BT

Copyright © 2021 Telecom Infra Project, Inc.

TIP Document License

By using and/or copying this document, or the TIP document from which this statement is linked, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to copy, display and distribute the contents of this document, or the TIP document from which this statement is linked, in any medium for any purpose and without fee or royalty is hereby granted under the copyrights of TIP and its Contributors, provided that you include the following on ALL copies of the document, or portions thereof, that you use:

1. A link or URL to the original TIP document.
2. The pre-existing copyright notice of the original author, or if it doesn't exist, a notice (hypertext is preferred, but a textual representation is permitted) of the form: "Copyright © 2021, TIP and its Contributors. All rights Reserved"
3. When space permits, inclusion of the full text of this License should be provided. We request that authorship attribution be provided in any software, documents, or other items or products that you create pursuant to the implementation of the contents of this document, or any portion thereof.

No right to create modifications or derivatives of TIP documents is granted pursuant to this License. except as follows: To facilitate implementation of software or specifications that may be the subject of this document, anyone may prepare and distribute derivative works and portions of this document in such implementations, in supporting materials accompanying the implementations, PROVIDED that all such materials include the copyright notice above and this License. HOWEVER, the publication of derivative works of this document for any other purpose is expressly prohibited.

For the avoidance of doubt, Software and Specifications, as those terms are defined in TIP's Organizational Documents (which may be accessed at https://telecominfraproject.com/organizational-documents/), and components thereof incorporated into the Document are licensed in accordance with the applicable Organizational Document(s).

Copyright © 2021 Telecom Infra Project, Inc.

Disclaimers

THIS DOCUMENT IS PROVIDED "AS IS," AND TIP MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THE DOCUMENT ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

TIP WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE DOCUMENT OR THE PERFORMANCE OR IMPLEMENTATION OF THE CONTENTS THEREOF.

The name or trademarks of TIP may NOT be used in advertising or publicity pertaining to this document or its contents without specific, written prior permission. Title to copyright in this document will at all times remain with TIP and its Contributors.

This TIP Document License is based, with permission from the W3C, on the W3C Document License which may be found at https://www.w3.org/Consortium/Legal/2015/doc-license.html.

Copyright © 2021 Telecom Infra Project, Inc.

Table of Contents

Copyright © 2021 Telecom Infra Project, Inc.

Copyright © 2021 Telecom Infra Project, Inc.

List of Figures

Copyright © 2021 Telecom Infra Project, Inc.

List of Tables

Copyright © 2021 Telecom Infra Project, Inc.

1

Introduction

1 Introduction

This document represents the technical requirements for an open and disaggregated broadband network gateway (BNG) device that operators can deploy in current and future networks for the provision of fixed broadband services. It describes the required hardware and proposes non-mutually exclusive software packages for the support of additional services or functionalities.

It includes the role of software-defined networks (SDN) and the desired approach concerning fixed-mobile convergence. And it includes regulatory requirements to deploy Open BNG in networks of operators participating in this requirements document.

This is the second release of the Open BNG requirements document. This version of the document incorporates updates from Open BNG operators, as well as feedback and comments from the Open BNG vendor community. Notable changes since the previous version include:

- Revisions to the System Configurations described in section 4.6.1
- Inclusion of the BNG CUPS software packages in section 8

Other areas have also been updated to provide additional clarity regarding operator requirements, and to provide necessary context to assist HW and SW vendors in developing roadmaps for Open BNG products.

1.1 Why Open BNG?

The project goal is to develop a solution that overcomes some of the most relevant issues operators presently face when deploying access services for fixed customers (e.g., residential, SOHO, SME). A short-term challenge for these services is continuous traffic growth, which not only affects required performance, but also determines the most appropriate network location for BNG functionality (i.e., more centralized vs. more distributed).

Other topics, such as the search for an appropriate fixed-mobile convergence strategy, or the inclusion of SDN methods for improved service provisioning, will also impact future BNG device specifications.

In this environment, operators find that current solutions:

Copyright © 2021 Telecom Infra Project, Inc.

- are based on monolithic platforms that make it extremely difficult to introduce innovation from other vendors in disparate parts of the device stack:
    - Lack of open hardware that can run various software types
    - Lack of open software that permits feature extensibility
    - Lack of fully open APIs that enable external components to interact with a device
- lack standardized (or at least globally agreed) features and tools for zero touch provisioning (ZTP) and initial auto-configuration
- demand per-vendor system integration that affects costs and time-to-market of services
- present a lock-in to same-vendor pluggable modules not based on technology
- represent a strong integration challenge in multi-vendor environments

This set of technical requirements aims to define an open and disaggregated platform that:

- is based on commercial, off-the-shelf components and open software that can perform traditional BNG functions
- reduces deployment and operational costs
- provides the scalability required for multiple scenarios

1.2 Scope of the document

The aim of this document is to describe:

- the desired Open BNG platform architecture—including requirements that will need to be met in relation to hardware and software features
- the end-to-end network architecture where the platform will need to operate, presenting disparate use cases affecting its interface layout, features and functionality, and device capacity
- the management of Open BNG via an SDN controller(s)

Immediately following the publication of this document, a detailed, low-level TRS (technical requirement specification) will be compiled. It will be shared with platform hardware and software vendors as a basis for further technical discussions.

1.3 Document structure

This document is structured as follows:

Copyright © 2021 Telecom Infra Project, Inc.

- **Chapter 1**: Introduction
- **Chapter 2**: Network architecture & Open BNG types
- **Chapter 3**: Platform architecture
- **Chapter 4**: Hardware specifications
- **Chapter 5**: BNG software package (BSW): subscriber management capabilities
- **Chapter 6**: Router software package (RSW): routing capabilities for Open BNG
- **Chapter 7**: Provider Edge software package (PESW): Open BNG as a PE for enterprise services
- **Chapter 8**: BNG CUPS software package
- **Chapter 9**: Open BNG and SDN
- **Chapter 10**: Additional requirements
- **Chapter 11**: Glossary

Copyright © 2021 Telecom Infra Project, Inc.

2

Network Architecture and Open BNG types

2 Network Architecture and Open BNG types

In this section, we introduce the Open BNG deployment models and the most typical network topologies where it will operate. In general, these aspects will have an impact in the hardware layout, the required capacity demand, and the additional functionality required (i.e. software packages).

2.1 Traditional transport networks for fixed services and new trends

There are many different topologies deployed and operated by different network operators. Our intention in this section is not to cover all these in detail. Instead, we start simply with the very typical network architecture, shown in Figure 1, that is subdivided into three segments: Access, Aggregation and Core. We'll use this to describe our reasoning behind the different deployment scenarios for the Open BNG and the differentiated software packages that will be described within this requirements document.

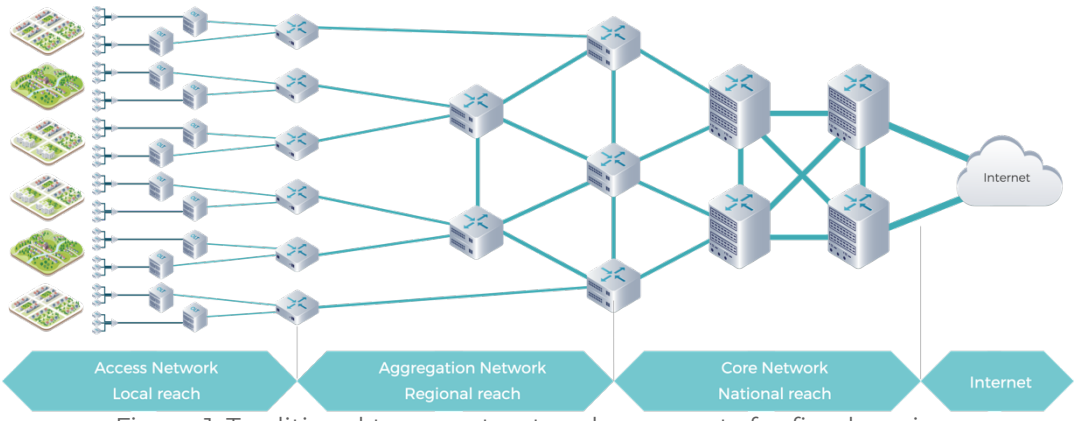

Figure 1. Traditional transport network segments for fixed services

Copyright © 2021 Telecom Infra Project, Inc.

In Figure 1 above, access devices (DSLAM[1] or OLT) in the access segment are connected to a regional aggregation network. The level of aggregation keeps growing upwards and, eventually, traffic is sent to a core 'backbone' network for national forwarding and exchange with external networks.

The technologies used in each network segment varies. While core networks are predominantly IP/MPLS based, aggregation networks present many technology choices: IP/MPLS; MPLS flavours like MPLS-TP; Carrier Ethernet; the growing VxLAN, and more recent trends like Segment Routing. The implication is that the location of the Open BNG functionality particular to each operators' networks has a great impact, not only in the required performance, but also in the type of features that will be required from the Open BNG node.

2.1.1 Scenario BNG + router

The typical scenario historically, back when BNGs were less powerful, is presented in Figure 2.

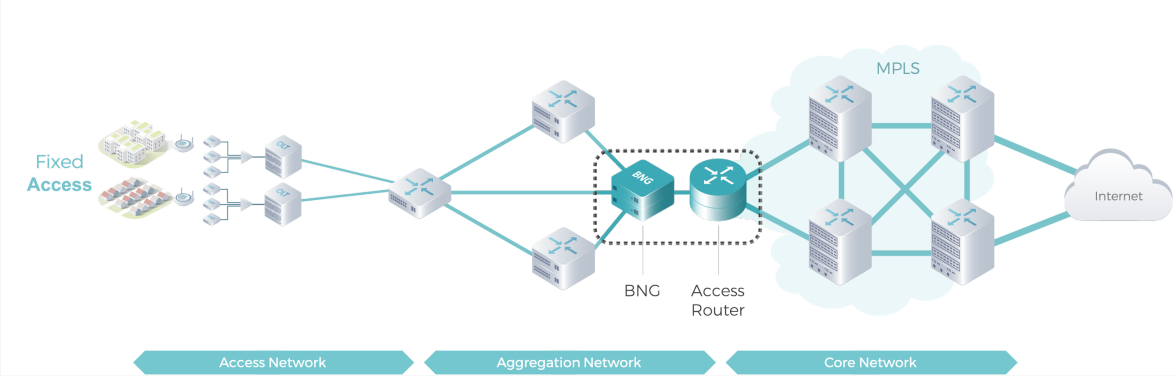

Figure 2. Scenario BNG + router (centralised)

Here, the BNG was more 'centralised' and was located between the aggregation network and the core network to ensure isolation between the two (this is synonymous with the centralised approach that will be described later in section 2.1.3). Indeed, the access-facing interface of the BNG in this historical scenario was normally based on VLANs (both the 1:1 and N:1 VLAN model predominated), and it provided a beneficial segmentation of

[1] For this specification, only IP DSLAMs will be considered. No ATM-related requirements will be demanded from the Open BNG.

Copyright © 2021 Telecom Infra Project, Inc.

the transport protocols. However, the exact location of the BNG depended mainly on its scalability (i.e., the total number of subscribers served).

There were also operators who deployed smaller (decentralised/distributed) BNGs closer to the customers:

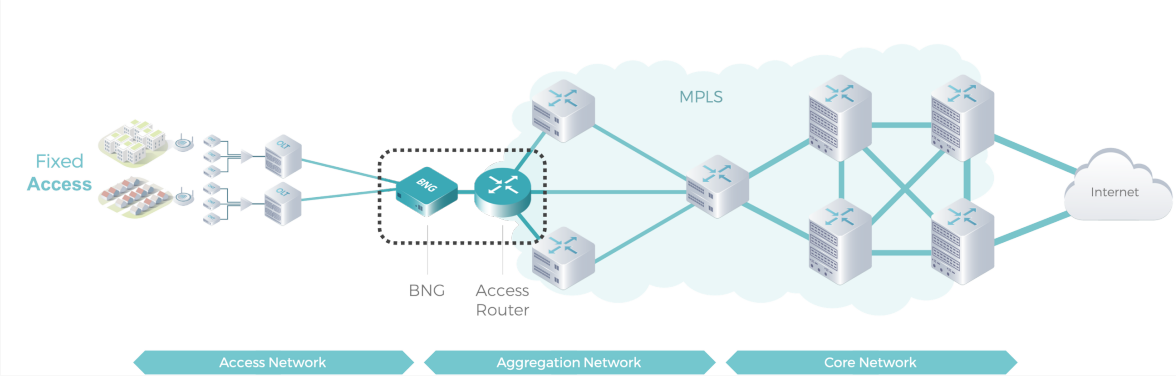

Figure 3. Scenario BNG router (distributed)

As depicted in Figure 3 the aggregation area downstream of the BNG in this distributed case was normally smaller, and there was typically an IP-based regional network upstream towards the national core. However, in essence, these approaches were very similar.

In both cases, the key idea was that BNG devices lacked, at that time, a mature L3 transport protocol stack (i.e., MPLS). So a very common remedy was to deploy, adjacent to the BNG, an L3 Access Router. This router provided the IP/MPLS protocols that the BNG lacked.

Today, this approach is very rare in the industry, as the once separate functionalities (BNG and Router) are combined and supported within a single BNG node in many vendor implementations.

However, it can serve to explain – for when we consider the software requirements for the Open BNG - the separation between the basic subscriber management features (BNG SW package – chapter 5) and the routing requirements (Router SW package – chapter 6). It is also worth mentioning that, in past years, much work has been done at TIP (and the telco ecosystem) to understand the maturity of routing protocols in disaggregated solutions (e.g. TIP's DCSG testing). But perhaps less attention has been focused on the evaluation of subscriber management features. The separation of the two serves to remedy this in the upcoming evaluation of proposals from the industry.

Copyright © 2021 Telecom Infra Project, Inc.

2.1.2 Scenario BNG + router + enterprise PE

In the first scenario described earlier in section 2.1.1, national enterprise services are typically provided by concatenating VPNs across two (or more) regional networks that are interconnected by transiting the core. In the second scenario, shown below in Figure 4, new enterprise Provider Edge (PE) router nodes dedicated to enterprise services are deployed. These PEs are separate and distant from the BNG+Router that they effectively bypass. The national enterprise service that the PEs support therefore do not use the BNG plus router solution. Note also that this situation (distinct enterprise PEs) applies where the BNG and access router functionality is contained within a single node.

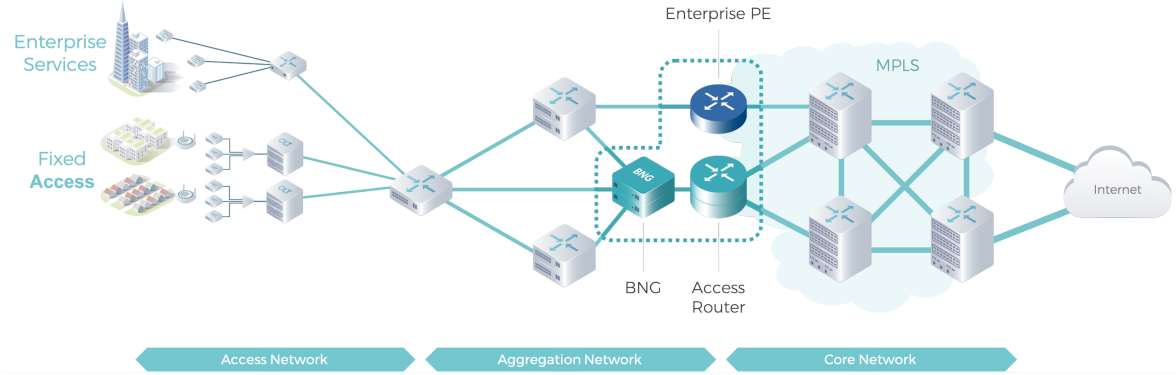

Figure 4. Scenario BNG and separated enterprise PE

2.1.3 Scenario Multi-Service BNG

In the third scenario, require that the separate MPLS PE functionalities should be integrated with the BNG+router functionality, and that all three functions are contained within a single BNG node. Such a 'multi-service BNG' has been described and defined by the Broadband Forum (BBF) in TR-178.

In more centralized deployments, implementing for example Seamless MPLS, the BNG can be considered a Seamless MPLS Service Node, supporting MPLS on both the uplink and downlink. In fact, the encapsulation of subscriber sessions over an MPLS pseudowire is widely deployed. For scalability reasons, operators may easily still choose to provide national VPN services by dividing the VPN in several segments, using the BNG device to do the stitching.

Copyright © 2021 Telecom Infra Project, Inc.

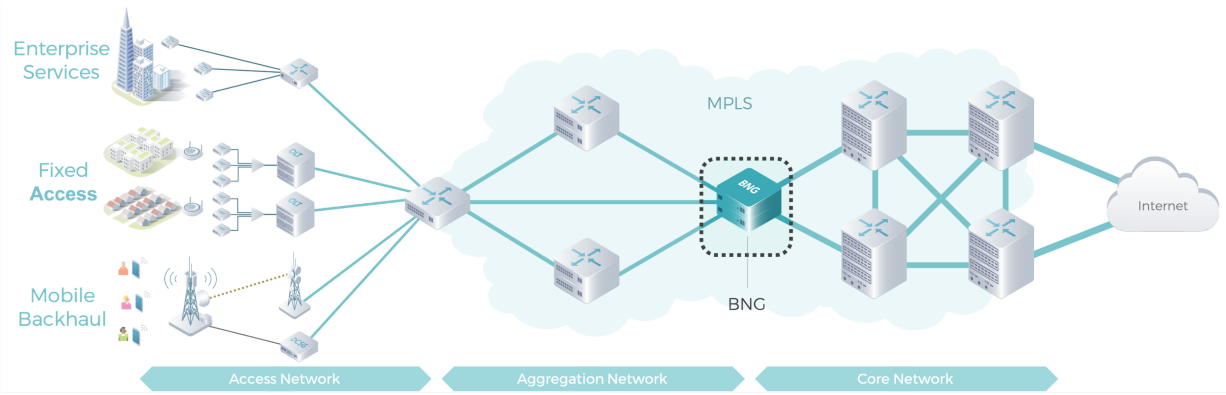

Figure 5. Scenario Multi-Service BNG

Due to the big traffic growth experienced in the last few years, some operators have decided to distribute the BNG function, deploying it closer to the customers. In scenarios like this, it is common that the first aggregation node (i.e., where access nodes are connected) becomes the BNG, and sometimes also the enterprise PE (Figure 6). Furthermore, this node may participate also in the distribution of video services, where multicast capabilities are essential.

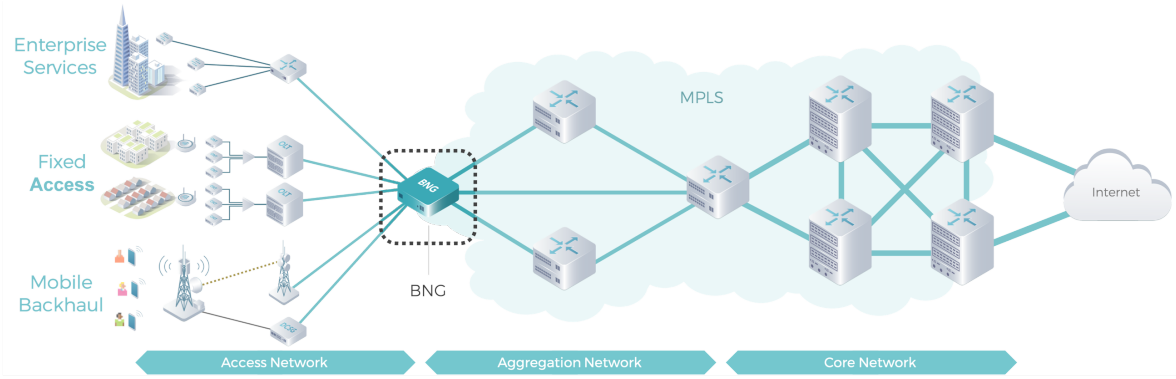

Figure 6. Scenario Multi-service BNG (distributed)

Any of these reasons leads to the definition of the Provider Edge SW package for the Open BNG of this specification (chapter 7).

2.1.4 Regulatory requirements for wholesale and legal intercept

There are two important regulatory requirements for operators where a BNG is of importance. First this is the requirement for granting wholesale access by operators holding significant market power. Typically, this is realised by Layer 2-bit stream access (L2BSA) in various implementation options with VLAN or other tunnelling protocol-based handoff. L2TP is such a tunnelling protocol approach and used as a mechanism to handoff

Copyright © 2021 Telecom Infra Project, Inc.

subscribers from the wholesaler access network to another Operator's service node.

In the L2TP case, the BNG typically provides the LAC function and is responsible for forwarding traffic to wholesale partner networks.

In the L2BSA case, the wholesale service could be implemented by a router in the aggregation network or, if the BNG takes part of it, as a function on the BNG.

Potentially network connections from customers connected via wholesale partner networks are terminated at a BNG or a PE.

Exact accounting might play an important role for wholesale connections.

The other legal requirement is to provide a copy of the traffic of a target customer, as well as the intercept related information (IRI), to a law enforcement agency (LEA). The Lawful Intercept (LI) capability allows LEAs to conduct electronic surveillance as authorized by judicial or administrative order (from competent authorities) to unobtrusively monitor data communications.

LI requires additional functionality like traffic duplication, encryption of traffic, time stamping, etc. It is typically implemented by the operator, close to the BNG or in the BNG, at the point where all traffic of a customer traverses (in contrast to other network locations because of the BNG routing function and redundant network paths between BNG and core network). Similar to wholesale this might be a function implemented in the BNG or as a separate device connected to the BNG.

2.1.5 Fixed/mobile convergence in the aggregation network

There are multiple approaches that operators are following to try and take advantage of convergence techniques between fixed and mobile networks, elements or functions. While core network convergence (also known as WWC) is considered as a long-term objective, convergent transport of fixed and mobile traffic is a common existing requirement for aggregation network.

This means that the BNG, if it plays the role of an aggregator, participates in the mobile backhaul (MBH), or at least stands in the middle of the transmission path for the synchronization signals. The conclusion is that both Sync-E and PTP might be requirements for the Open BNG, the same as for any other node in the MBH. These will be covered in section 4, as they have a demanding impact on the hardware.

2.1.6 Wireless Wireline Convergence

Copyright © 2021 Telecom Infra Project, Inc.

The term "Wireless Wireline Convergence" (WWC) refers to the convergence of the fixed and wireless core networks for those operators who offer services with both kind of accesses and intend to unify their core network. This concept is currently defined in TS 23.316 3GPP and BBF TR-470 & TR-456 specifications, but BBF will be enhancing it further on in the next months introducing for example CUPS for AGF (Access Gateway Function).

WWC is not considered in this document, as the focus here is mainly to pursue implementations of the BNG network function on open hardware, with the possibility to run different software implementations on the same hardware: so in this document the fixed core is assumed to be separated from the mobile core.

However, some operators are considering for the future to offer to wireline users certain services through the mobile core, in order to achieve economies of scale on service platforms, exploit the 5G toolkit to orchestrate services and explore new business models with 3rd parties. One of the most attractive ways to technically achieve the core network convergence is through the transformation of the BNG function into an autosensing BNG/AGF function.

In this sense, any information from vendors about the intentions to develop a multifunction device which is able to work as BNG as well as AGF will be valued.

2.2 Open BNG deployment scenarios

This section describes different deployment scenarios for Open BNG platforms. The first part describes the different flavors of Open BNG, while the second describes locations where Open BNG may be deployed. Both parts describe specific scalability and functionality requirements where appropriate.

2.2.1 Open BNG Types

As described in section 2.1 above, the BNG may serve many functions in addition to subscriber management. As such, we define two types of Open BNG:

Copyright © 2021 Telecom Infra Project, Inc.

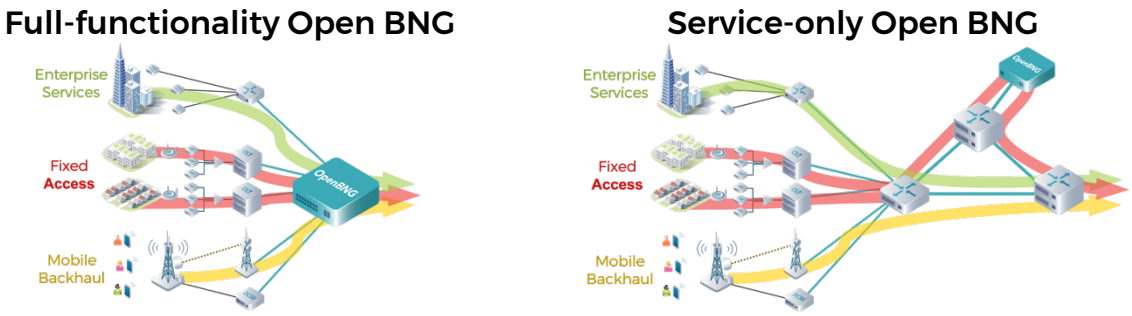

Figure 7. Full-functionality and service-only BNG types

Both types of Open BNG have common requirements for the BNG software, and must comply with the SDN principles provided later on in this specification. In addition to these core requirements, the following sections will describe the key characteristics of each type.

2.2.1.1 Full-functionality BNG

A full-functionality BNG provides both aggregation and subscriber management functions, integrated into the network as a full router.

Access devices may be directly connected to the Open BNG, or may be connected via an aggregation network. In the former case, the Open BNG will typically deal with VLANs towards the access network, while in the latter case other approaches are typically used in addition (e.g. PW encapsulation of these sessions). Both scenarios are depicted in figure 8 below.

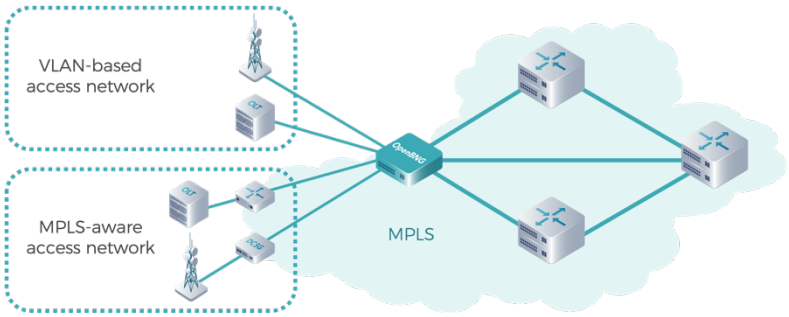

Figure 8. Full-functionality BNG

The Open BNG is deployed physically inline for all traffic, and so it also acts as a PE for enterprise services (e.g. VPN) where these are deployed, thus requiring the PESW package.

Some operators are deploying converged fixed/mobile aggregation networks. Where

Copyright © 2021 Telecom Infra Project, Inc.

there is a master clock device upwards from the Open BNG, this node will have to support equivalent synchronization requirements as those in the MBH.

If the operator provides L2TP based wholesale service, the Open BNG acts as LAC.

2.2.1.2 Service-only BNG

In this deployment case, the BNG does not form an integral part of the aggregation network, instead is running as a dedicated service node for e.g. terminating customers from wholesale partners.

Routing is always required, while PE functionality might be required or not: there is the option of deploying separate Service-only BNG for enterprise (with routing and Enterprise PE functions) and consumer (without Enterprise PE function). Furthermore, PE functionality may be required to terminate sessions into VPNs for other reasons such as wholesale services or operator-internal traffic separation.

As the service-only BNG is not in line with the aggregation network, it is not necessary to support time/phase synchronization for mobile backhaul, as this can instead be passed through the aggregation network.

A service-only BNG is also a candidate for a pure software BNG[2] that is deployed on a general-purpose compute.

2.2.2 Open BNG deployment locations

Operators may choose to deploy BNG in a variety of locations. The decision as to how widely BNG should be distributed depends on subscriber density, operational complexity and cost efficiencies.

[2] TR-345 outlines how a virtualised (BNG) can be instantiated in software as a virtualized network function (VNF). https://www.broadband-forum.org/download/TR-345.pdf

Copyright © 2021 Telecom Infra Project, Inc.

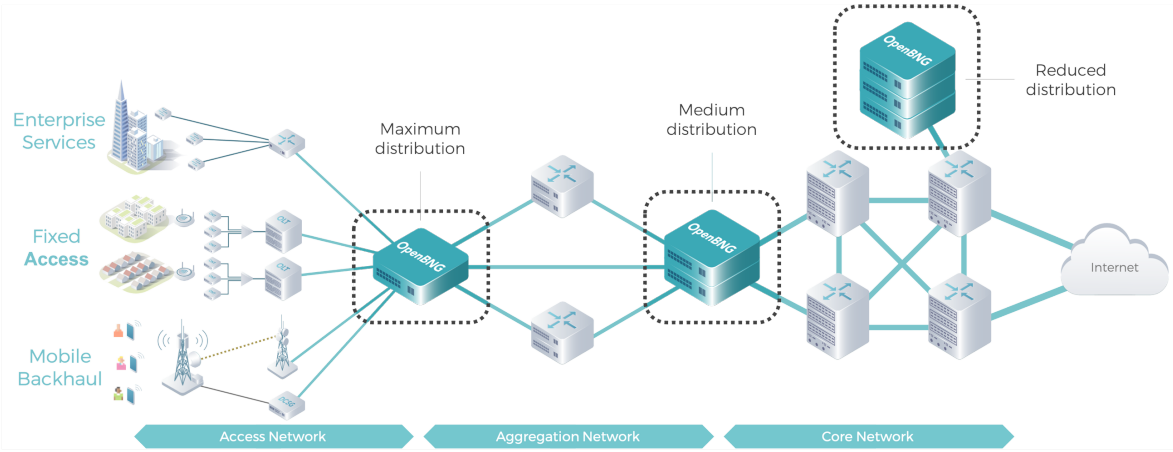

Figure 9. BNG deployment locations

Each deployment location has a different requirement for subscriber density and interfaces count. The characteristics of each location also mean that certain types of Open BNG (full-functionality vs service-only) may be more preferred/suitable. These considerations are explained in the following sections.

Note that the interface numbers in this section only describe aggregation requirements, which are driven by the number of downstream access platforms. The approach to dimensioning capacity is covered later in section 2.2.3.

2.2.2.1 Maximum distribution

In this case (figure 10), the Open BNG is totally distributed (i.e. in a local PoP or central office). The full-functionality BNG is most typically deployed here, and the BNG provides aggregation for downstream access nodes. Enterprise CE nodes and MBH (or more generically mobile x-haul) may also be connected where these services are present.

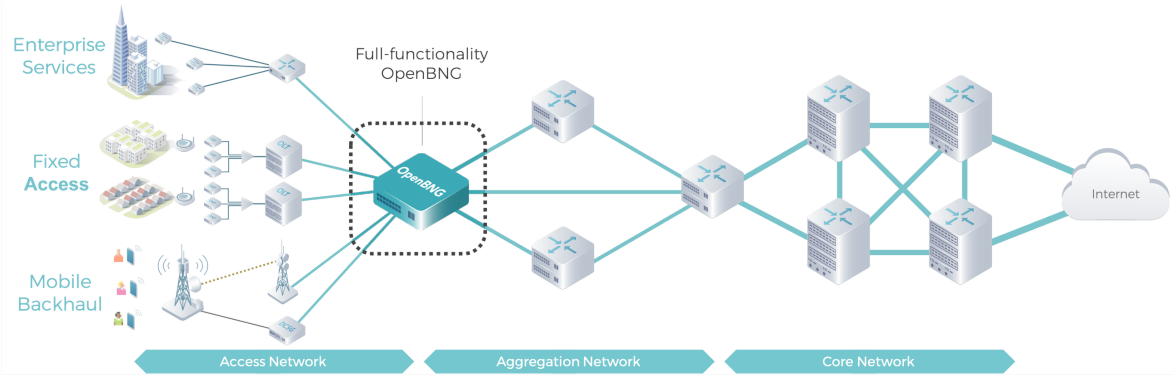

Figure 10. BNG with maximum distribution

Since the BNG is distributed deep into the network, the subscriber density and traffic volume for these locations are relatively low, although a large number of 1GE/10GE ports

Copyright © 2021 Telecom Infra Project, Inc.

are required for local aggregation. The required scalability for these locations is:

- Typically up to 32k dual-stack subscribers (although may be as high as 100k in some extreme cases)
- Typically 80*1GE/10GE/25GE ports for downstream access aggregation (although may be as high as 400 ports in some extreme cases)
- 100GE ports for upstream connectivity (scaled according to traffic volumes)

Note that these scalability numbers refer to the entire location; the deployment shall be in the form of a single device or a fabric. . Multiple devices are expected to be needed where these scalability targets cannot be met by the single device.

2.2.2.2 Medium distribution

In this case, the Open BNG is less distributed (i.e. in a regional PoP) and there are a greater density of subscriber sessions to terminate. Operators may deploy a full-functionality BNG or a service-only BNG to these locations.

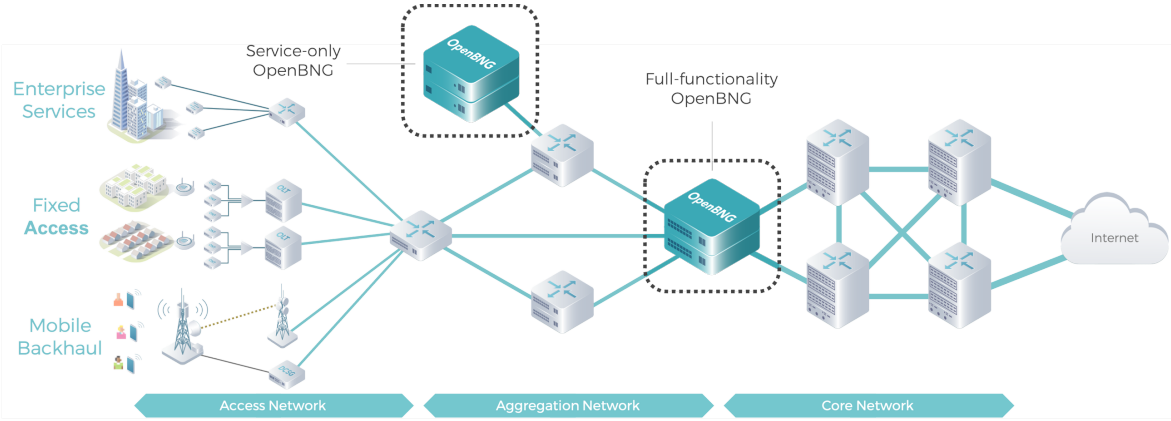

Figure 11. BNG with medium distribution

Medium distribution locations will typically scale up to 128k subscribers (dual stack), and upstream connectivity is provided using 100GE ports. In the case where a full-functionality BNG is deployed, up to 80*1GE/10GE/25GE ports will be required for downstream aggregation, and additional scalability (up to 10*100GE ports) may be needed to cover the needs of upcoming mobile x-hauling. Additional scalability might also be needed for wholesale, legal intercept or existing and upcoming mobile network requirements.

While existing BNG solutions may allow these requirements to be met using a single device, we acknowledge that this may be unachievable for an Open BNG, and in any case operators may prefer to spread the load across multiple devices to reduce the size

Copyright © 2021 Telecom Infra Project, Inc.

of their failure domains. Since operators would expect to deploy multiple devices to these locations, we provide more specific guidance regarding deployment in section 2.2.3 below.

2.2.2.3 Reduced Distribution

In this case, the Open BNG is deployed at a centralised PoP (e.g. core location). Operators expect to deploy service-only BNG to these locations.

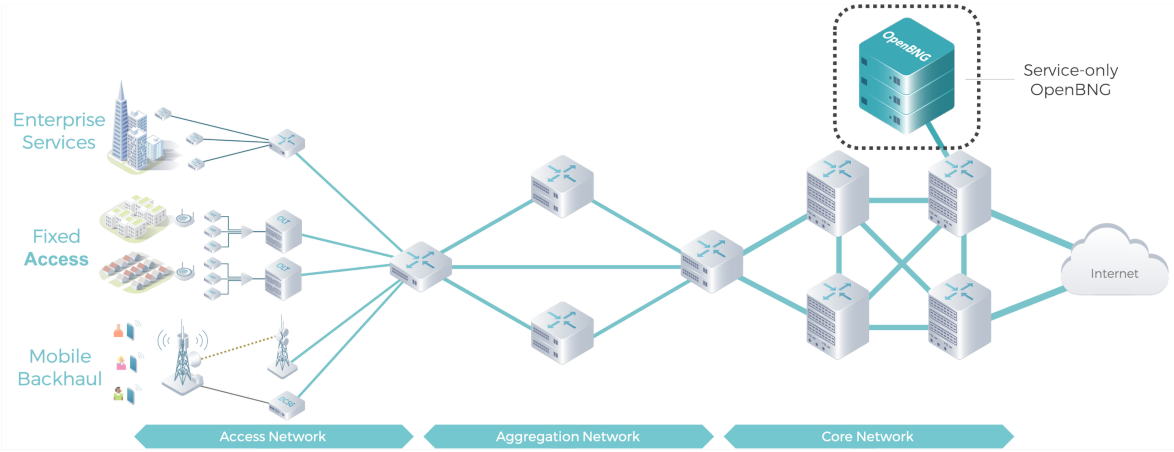

Figure 12. BNG with reduced distribution

The density for these locations may scale well beyond 128k subscribers, so TIP operators expect to meet such requirements by the deployment of multiple devices.

2.2.3 Open BNG deployment models

As described in the previous section, subscriber densities for some deployment locations may grow to very large numbers. In many cases, operators may need to deploy multiple devices to meet these requirements, allowing them to:

- Constrain the size of failure domains and associated 'blast radius' of any failures, to protect service levels and appetite for risk
- Scale in a modular and linear fashion, accepting that meeting these numbers may be quite a challenge considering current state-of-the-art
- Provide resiliency to accommodate failure of one or more devices to be recovered using redundant capacity

Where multiple devices are deployed, any capabilities that can simplify the complexity of working with multiple devices are valued (e.g. techniques that permit managing the multi-chassis solution as a single node).

Copyright © 2021 Telecom Infra Project, Inc.

This section describes the expected deployment models for Open BNG devices, which would meet the deployment scenarios already described.

Note that the deployment models described in this section are not specific to any particular deployment scenario (e.g. service-only vs full-functionality, maximum vs medium vs reduced distribution).

2.2.3.1 Standalone Open BNG

Figure 13. Standalone Open BNG

The simplest scenario, where Open BNGs are deployed as standalone devices. Each location may have just one node, or multiple Open BNG nodes may be deployed. The deployment of multiple nodes would typically be to reduce failure domains, or for scalability reasons, but in both cases these multiple nodes operate independently of each other. There is no capability to recover service in the event an Open BNG device fails, and there is no resilience other than uplink connectivity, fans and power redundancy.

Where multiple nodes are deployed, links towards downstream access nodes are divided evenly between standalone Open BNGs, as are subscriber sessions. Accordingly, each Open BNG serves a subset of the downstream access network.

Uplink capacity for each device is dimensioned according to the total number of subscribers connected to that device (plus any additional transit traffic from other services – e.g. MBH).

2.2.3.2 Clustered Open BNG

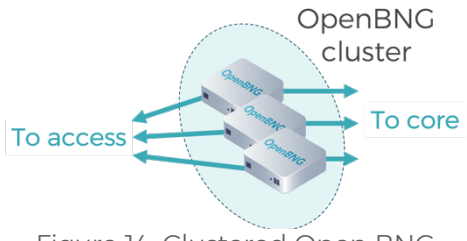

Figure 14. Clustered Open BNG

In the clustered scenario, multiple Open BNG nodes are deployed in a notional cluster. Downstream access networks are physically connected to two or more Open BNG

Copyright © 2021 Telecom Infra Project, Inc.

devices, which provide resiliency for each other; in the event one Open BNG device fails, services can be handed over or recovered on another Open BNG.

When proposing solutions that would form part of a clustered deployment, software vendors should consider that many Open BNG deployments will be providing multiple services. As such, any failover capabilities will need to consider failover scenarios for multiple services – e.g. BNG sessions, PE services, timing/synchronization, etc. In the specific case of BNG sessions, the availability of stateful (hot-standby or warm-standby) failover is valued to minimise customer impact. Such failover may be achieved through CUPS, or via other local clustering techniques like VRRP.

Uplink capacity for each device is dimensioned according to the total number of subscribers terminating on that device under failure conditions, plus any local cross-connect needed to implement the clustering solution.

2.2.3.3 Leaf-spine Open BNG

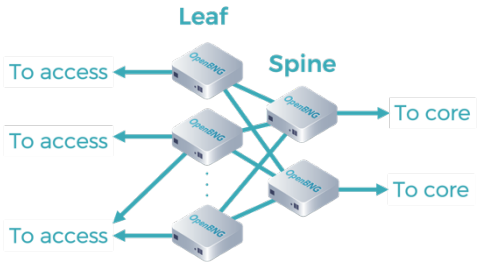

Figure 15. Leaf-spine Open BNG

This design follows the fabric idea of typical data center architectures. Multiple Open BNG nodes are deployed, with Open BNG leaf devices aggregating customers and provide connectivity towards downstream access networks, and Open BNG spine devices providing connectivity towards the core network. Leaf and spine nodes are interconnected using n*100GE LAG, with fabric capacity dimensioned non-blocking according to the demand for each leaf node and potential east-west traffic forwarded between leaf nodes. Downstream access networks may be single-homed or multi-homed to multiple Open BNG devices.

Devices in the leaf-spine model might be functionally specific. That is to say, BNG based subscriber edge services like residential, business, wholesale or MBH might be terminated on the leaf nodes. If functionalities are available on another leaf node only, e.g. a business L3VPN service or wholesale connectivity to other operators, customers on one node are transparently forwarded to the respective service node.

Copyright © 2021 Telecom Infra Project, Inc.

MPLS and PE services might be used in different ways in the fabric design:

- Core network connections are typically MPLS based and PE services must be terminated on the spine nodes. As such, the BSW package is not needed for the spine nodes, and HW solutions should be specified accordingly.
- MPLS is used inside the fabric for transparent forwarding between leafs and leaf-spines
- PE services might be used to for access networks and are terminated at leaf nodes
- Customer specific MPLS based services (e.g. L3VPN) terminated at the leaf nodes or at a specific leaf node in the fabric as indicated before

Extensibility and flexibility are the key drivers for the fabric design of the leaf-spine Open BNG. It is expected that in the future additional demand like edge computing might be handled here as well. The support of 25G ports shall provide this extensibility for e.g. attaching servers to the OpenBNG leaf nodes of the fabric. The specific requirements beyond this interface support are for the time being out of scope of this specification.

Copyright © 2021 Telecom Infra Project, Inc.

3

Open BNG Platform Architecture

3 Open BNG Platform Architecture

The main modules/components of the Open BNG platform are depicted in Figure 16 below.

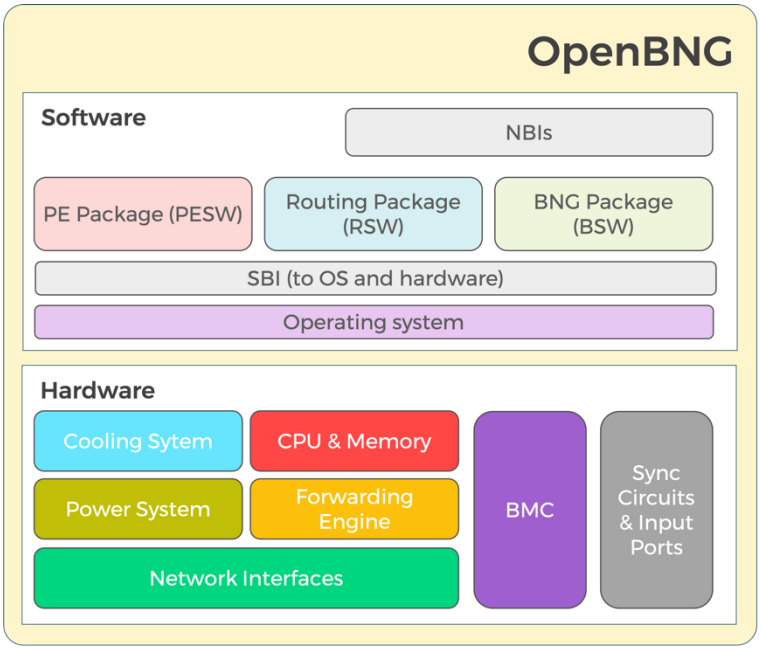

Figure 16. Open BNG platform architecture

The Open BNG node consists of:

- Commercial off-the-shelf (COTS) hardware with an open, programmable northbound interface (NBI). *Hardware requirements are described in section 4 below.*
- Open software (network operating system – NOS) with an open, programmable NBI. *Software requirements are described in sections 5-8 below, and SDN interfaces are described in section 9 below.*

Note that this specification does not define a strict position on how or where the software (or part of it) has to run (e.g. in the device, in an external VM). This is considered an implementation decision to be taken by vendors and network operators.

3.1 Openness

The 'open' in Open BNG does not imply 'open-source', but rather no 'hidden' or 'restricted' APIs that preferentially benefit the hardware vendor; or the NoS vendor; or the OS selected. Open BNG operators should be able to 'swap out' or replace any one of the

Copyright © 2021 Telecom Infra Project, Inc.

three without affecting the other two.

To this end, the hardware system must not impose any restriction that limits the software that can run on it. In other words, the system must allow operators to install any operating system, even if its implementation comes from a third party. To ensure compatibility, it is highly recommended that Network Operating Systems for this platform are provided in the form of binary installers compatible with the Open Network Install Environment (ONIE) specification, as defined by the Open Compute Project (OCP). Equivalently, the Open BNG hardware will be equipped with ONIE.

If the platform provides the capability to verify the signature (via a particular certificate or a cryptographic key) of the software, it must be possible to disable such verification at any time, through software or firmware configuration, without the need for any specific or additional license. Moreover the hardware must be accompanied with a comprehensive toolkit of maintenance, configuration, diagnostic and repair information to facilitate modifications.

3.2 Forwarding Engine Implementations

One key element of the TIP Open BNG initiative is to ensure a viable ecosystem for disaggregated solutions. To this end, is is acknowledged that there are a variety of options for how the forwarding engine function could be implemented (e.g. ASIC, FPGA, SmartNIC, VNF, etc). It may also be necessary to integrate multiple forwarding elements or technologies to meet the packet processing, traffic management and other scalability demands of the BNG function. The requirements in this document are intended to be agnostic to this implementation choice, and Open BNG operators expect the development of solutions based on a diverse range of forwarding technologies to encourage a diverse supply chain. In addition, Open BNG operators expect that there will be competition between the approaches as well as between the open chipset suppliers themselves, in order to ensure a healthy ecosystem in all parts.

3.3 Software Packages

Open BNG requirements are defined using a number of software packages, each of which describes a discrete set of functionality:

- RSW, defines core routing plane functions
- PESW, defines functions to deliver L2VPN and L3VPN services

Copyright © 2021 Telecom Infra Project, Inc.

- BSW, defines BNG subscriber management functions

Section 8 describes an alternative approach to the BSW package, where the package is split into separate BSW-UP and BSW-CP packages in accordance with BBF TR-459.

The primary objective of this modular approach is to group common requirements rather than to express any requirement to 'mix-and-match' different software components, and vendor NOS should implement the functionality for the packages in combination (e.g. RSW, PE-SW, and the relevant BSW package). However, as described in section 2.2 above, different deployment scenarios may require only a subset of functionality, so a modular approach to licensing of each package will be valued. Licensing considerations are covered in more detail in section 10.4 below.

This modular approach is also necessary to enable alternative implementations for a given set of functionality. For example, the single BSW package vs the multiple CUPS BSW packages. In this case, vendors may wish to propose a unique NOS build for each.

Note, to avoid creating overlapping requirements, each function is generally described under only a single SW package. For example, QoS functions are described as part of the BSW package (since the BSW H-QoS implementation is the most complex), even though some aspects of QoS are relevant to all packages.

3.3.1 HW/SW Abstraction

Regardless of the underlying system architecture, a core principle of Open BNG is to enable the disaggregation of hardware and software in a sustainable fashion. This sustainability objective means solutions must be interoperable to avoid a proliferation of disparate implementations. Indeed, since more than one vendor can be positioned for any given function, it is important to ensure interoperability between each component of the solution (HW and SW packages).

To this end, further vertical separation of the software stack to strengthen the abstraction between HW and SW solutions is valued, as are solutions that mitigate the operational complexities of managing a large estate of Open BNG devices (e.g. IP address management, SW upgrades, etc). One solution aspect to these problems is CUPS, and another one is the establishment of an abstraction layer between the drivers or SDK representing the forwarding engine and the SW package. A CUPS based approach does not necessarily exclude the other. Figure 17 below provides a simplified representation of how CUPS and/or a HW abstraction layer could be implemented to

Copyright © 2021 Telecom Infra Project, Inc.

reduce the volume and complexity of required integrations.

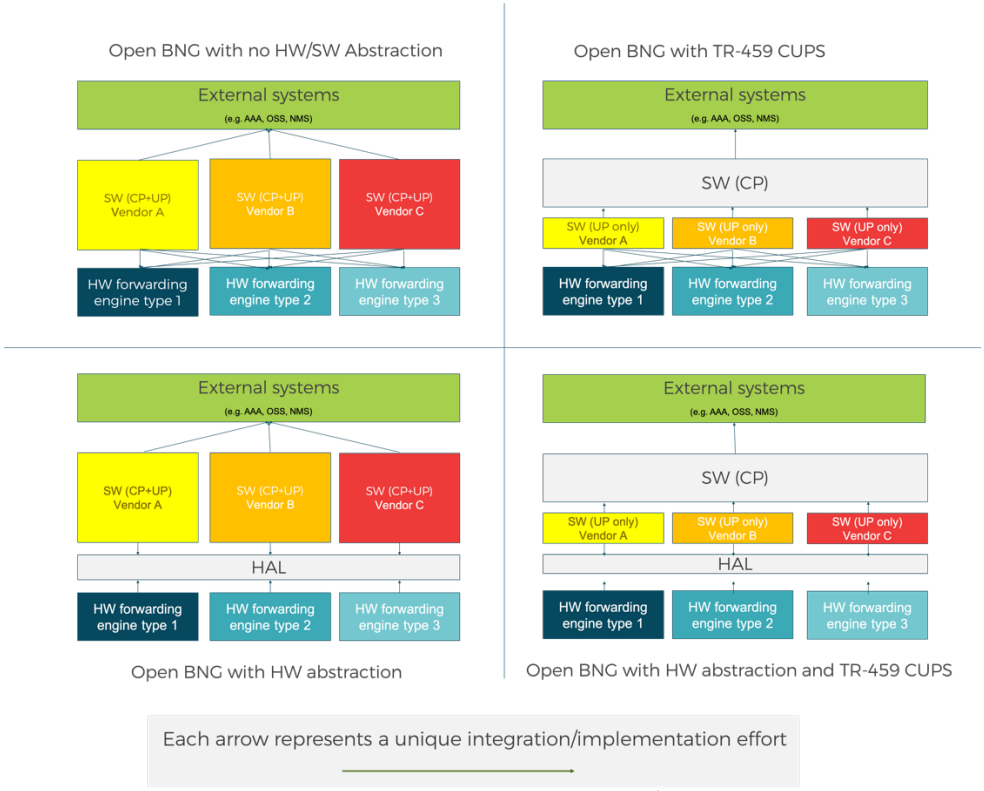

Figure 17. Open BNG approaches to HW/SW abstraction

For those vendors implementing CUPS, it is recommended that the TR-459 standard is followed, The requirements and implementation of solutions based on TR-459 CUPS is further detailed in section 8.

When considering HW abstraction, some solutions are already available in the data centre market (e.g. Switch Abstraction Interface - SAI), but in the case of BNG there is currently a lack of open solutions to this problem. One approach tackling this abstraction is currently developed in the ONF TASSEN project based on P4/gNMI. Considering this is an ongoing area of research, this document does not mandate such an abstraction layer but would value proposals to enable HW independence. In any case, solutions that make use of an abstraction layer should not suffer of sub optimizations due to the fact that the HAL exposes only a subset of the HW forwarding engine.

Copyright © 2021 Telecom Infra Project, Inc.

4

Hardware Specifications

4 Hardware Specifications

The following sections describe the requirements of Open BNG hardware platforms, including environmental characteristics, performance expectations and timing/synchronisation requirements.

4.1 Hardware Solution form factor and environmental conditions

Open BNG hardware platform will be deployed exclusively in Central Offices. Installation will be done in standard 19'' racks, typically 600mm or 800mm wide, and 800mm or 1000mm deep. The Open BNG hardware form factor is expected to be optimised for limited space consumption and thermal/power efficiency. Smaller form factors are preferred.

The equipment shall conform to, or exceed, ETSI standard ETS 300 019-1-3 requirements (Class 3.1), in particular with regards to temperature (from -5˚C to +45˚C).

The equipment shall also conform to all applicable standards regarding mechanical, electrical and safety conditions, and must comply with all directives and certifications required in the countries where it will be deployed. In particular, solutions that improve the energy efficiency of the node will be extremely valued.

4.2 Hardware Platform CPU and Forwarding Engine

The CPU of the Open BNG hardware platform shall be compliant with the ONIE switch hardware requirements[3], and shall support the ability to run a variety of NOS.

The forwarding engine shall support line-rate forwarding across all ports according to an IMIX traffic profile and without any limitations. Hardware platforms shall be non-blocking and the forwarding capacity of the platform shall be able to support all interfaces at full rate with no limitations. The forwarding engine shall support all the features and packet types defined in the software sections (or as a less preferred, not prevent the implementation of such features purely in software). Extensively, there shall

[3] https://opencomputeproject.github.io/onie/design-spec/hw_requirements.html

Copyright © 2021 Telecom Infra Project, Inc.

be no limitations in the hardware to support any of the defined SW packages.

Programmability features of the forwarding engine will be valued. Redundancy of these components will also be valued.

4.3 Hardware Platform power supply and cooling requirements

The Open BNG hardware platform will include redundant power supplies and cooling components (fans); and replaceable filters to capture airborne dust and particulate matter from air intake and exhaust portals. It must be possible to substitute any of these with the device still in operation (hot swapping).

The equipment must support both DC power supplies, and the availability of AC power supplies as an option would be valued . In the event of a single power feed failure, the system shall be capable of maintaining full-service operation, without traffic loss. Associated alarms shall be generated for the duration of the fault.

The equipment must also include variable speed blowers, to adapt the cooling capacity to the exact demand. In general, the airflow in the Open BNG will be from front to back. Alternative mechanisms may be discussed. Again, associated alarms shall be generated in case of any fault in the cooling system.

4.4 Hardware Platform management

The Open BNG hardware must include, as a minimum, one console and one management port (both RJ45) and one USB 3.0 port, for local configuration and debugging. Nonetheless, it must be possible to remotely disable the console and/or the management port and/or the USB port. It is therefore mandatory that the platform also supports in-band management.

The hardware platform must include status indicators, including per port LEDs.

4.5 Hardware Platform Synchronization requirements

As stated in section 2, the Open BNG hardware may be used to aggregate MBH. In these cases, the Open BNG shall be able to propagate synchronization signals to other network elements directly or indirectly connected to it. Furthermore, it may also need to provide

Copyright © 2021 Telecom Infra Project, Inc.

frequency, time and phase synchronization to 2G/3G/4G/5G base stations directly connected.

The following are the mandatory synchronization requirements:

- Support of IEEE 1588 profile as defined in ITU-T G.8275.1 (full-timing support; Telecom - Boundary Clock) and Sync-E for holdover purposes and Grandmaster redundant sources support. The requirement corresponds to the support of IEEE1588v2 – Precision Time Protocol – profile for telecoms (multicast mode preferred) and includes Sync-E in Ethernet interfaces as per ITU-T G.8261 (section 9.2.1), G.8262 and G.8264.
- Network quality model (microsecond precision) according to ITU-T G.8271.1.
- Node performance (noise generation, tolerance, transfer and holdover) according to ITU-T G.8273.2 (sections 7.1/7.2/7.3/7.4).
- Node performance (upon wander, failure and holdover) according to ITU-T G.8273.2 (sections 7.2/7.3/annex). Clock type class B (minimum) or C (desirable), as defined in ITU-T G.8273.2.
- Support of IEEE 1588 profile as defined in ITU-T G.8275.2 (partial-timing support).
- Network quality model (microsecond precision) according to ITU-T G.8271.2.
- Node performance (noise generation, tolerance, transfer, wander, failure and holdover) according to ITU-T G.8273.4 (sections 7 & 8). Clock type class B, as defined in ITU-T G.8273.4.
- Support for G.8262.1 (eSEC) desirable.

The electronics used to build the synchronization regeneration capabilities are to be selected by the platform manufacturer (ensuring full performance compliance with standards), but detailed information should be shared within TIP. Hardware SKUs should include at least 2 time synchronization solutions to allow software (SW) providers to implement the above mentioned features using their preferred SW stack.

Finally, the hardware platform must include, at least, one GPS signal input interface (which may be based on SFP) and one 1PPS interface for external synchronization. These will be used in scenarios where the synchronization signals cannot be received from the network, and there are base stations directly connected. It may also be possible to select one signal among several (by means of a BMCA, desirably hardware implemented), in case there are multiple sources.

Note: These requirements are not applicable in scenarios where the BNG is a service only

Copyright © 2021 Telecom Infra Project, Inc.

device (not being part of the aggregation network), and may not be applicable for certain full-functionality deployments. As such, the ability to make synchronisation capabilities optional at the point or order (or via licensing) is valued.

4.6 Hardware SKU network interfaces and forwarding capacity

The required capacity and the interfaces layout in the hardware platform heavily depend on the specific Open BNG scenario (i.e. platform type, deployment location and deployment model) that is being considered. General requirements will be included first, with specifics per scenario defined later.

The solution must be able to support electrical and optical interfaces as per IEEE 802.3, and they shall be configurable to work either as UNI or as NNI. Pluggable optics will be preferred to fixed format connectors: they shall be able to operate at the same temperature ranges as the node, and it will be possible to configure them at different speeds (e.g. 1G/10G with SFP+) without reboot. There will be no limitations on the type of connectors that are used (SR, LR, etc.; LAN/WAN PHY), and the platform must be fully interoperable with third party optics. Additionally, the system shall be compatible with third-party coloured WDM pluggable optics (tuneable & fixed).

All physical network interfaces in the proposed platform must support multiple services simultaneously, independently on whether they are: multiple PWs each with its own set of VLANs; multiple VLANs associated to VRFs, VPLS, E-VPN, etc.; multiple native VLANs or VLANs associated with core interfaces (those configured with IS-IS, OSPF, LDP, etc.); multiple VLANs associated with BNG services (i.e., transporting PPPoE/IPoE sessions). Similarly, ethernet LAG interfaces must support the same type of services as single physical interfaces.

4.6.1 System Configurations

Accommodation of all the Open BNG flavours in a single SKU or chassis type will be extremely valued. If not possible, efforts will be done to limit the number of different SKUs. According to the details provided in section 2.2, the following standard configurations (SC) are envisioned:

Copyright © 2021 Telecom Infra Project, Inc.

	SC-1	SC-2	SC-3 leaf	SC-3 spine
Downstream ports	64*1G/10G/25G	4*10G/25G	32*1G/10G/25G	4*10G/25G 20*100G
Upstream ports	8*100G	16*100G	8*100G	4*100G
BNG subscribers	32,000	32,000	20,00	n/a

Table 1. OpenBNG Standard Configurations

SC-1 primarily addresses full-functionality deployments. Multiple SC-1 Open BNG nodes will be deployed to meet the increased subscriber/interface requirements for larger locations. As such, SC-1 nodes may be deployed according to any deployment model (standalone, clustered, or as a leaf node)

SC-2 primarily addresses service-only BNG requirements and may be deployed singly or multiply depending on required scale. The use of 400GE ports might be considered to reduce the numerosity of ports.

SC-3 specifically addresses the leaf-spine configuration described in section 2.2.3.3 (hence there is no BNG traffic requirement for this device). In case of a redundancy or development cost optimizations, SC-1 might be applicable as SC-3 leaf. In all other cases, the number of interfaces and supported subscribers of a leaf node can be reduced.

In the case where the BNG is deployed as a software function on a general-purpose server, it is anticipated that any number of high-speed NIC Cards can be used up to the capacity of the server. However, it is accepted that it may be unfeasible to address these system configurations given the interface and/or forwarding plane capacity of a single server. Hardware acceleration from the NIC cards is a valid option to improve performance (although acceleration must be made available to the BNG in a standard abstracted form).

It is worth mentioning that the previous definition of standard configurations does not prevent the inclusion of additional variants with a higher number of ports, or higher capacities, to account for the future or for an increased resiliency. As already said in section 2.2.3.2, the option of clustering could be considered to achieve this, considering the required interfaces to connect the Open BNG devices in a cluster.

Copyright © 2021 Telecom Infra Project, Inc.

When considering the forwarding capacity of the Open BNG for one of the above system configurations, or for alternative SKUs (based on dedicated HW or general-purpose servers), vendors should base any calculations on the peak average consumption per user from the table below:

	2021	2023	2025
Peak average per user (mbps)	4	7	11

Table 2. Peak average bandwidth dimensioning guidelines

Note that the refresh cycle for the BNG function is typically at least 7 years, and the lifespan for Open BNG devices is expected to extend to 2030 (and beyond). While traffic projections beyond 2025 inherently contain many unknowns, any Open BNG solution should be dimensioned to accommodate traffic growth of between 20%-30% year-on-year for this period.

4.6.2 Interface requirements

The 1G/10G/25G Ethernet port cages should support both short-reach (SR) or long-reach (LR, ZR, ER) pluggable optical transceivers, and direct attach copper (DAC) transceiver-cable assemblies. In addition to downstream connections to access nodes, it is expected that a number of these ports will be used (1G/10G/25G) for local connections to servers hosting control and management plane as well as other services like wholesale interfaces or legal intercept connections. The use of breakout cable to provide these ports is discouraged as these would limit the flexibility to support different configurations of optical transceivers

For 100G/400G ports, again there is a mixture of interfaces for short-reach (SR) and longer distances (LR, ZR, ER). These interfaces provide connections between the leaf and spine switch (100G) as well as connections to the network core (100G/400G).

With regards to the forwarding capacity, the main requirement is to present non-blocking forwarding architectures, as already commented in section 3.2. *Note: Oversubscription of the spine is expected, as leaf nodes will be run with less capacity for redundancy reasons.*

Copyright © 2021 Telecom Infra Project, Inc.

5

BNG Software Package (BSW)

Subscriber management capabilities

TELECOM INFRA PROJECT

5 BNG Software package (BSW)

The requirements for the BNG Software package are primarily based in the following Technical Report from the Broadband Forum: TR-101 Issue 2 (2011) – Migration to Ethernet-Based Broadband Aggregation. Any Open BNG platform proposal must provide a very high degree of compliance with such Technical Report and its list of requirements. Several of these will be explicitly mentioned in this specification for clarification; however, that does not exclude the needed compliance with the rest.

Together with TR-101, these three additional Technical Reports must be supported:

- TR-059 (2003): DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services
- TR-092 (2004): Broadband Remote Access Server (BRAS) Requirements Document
- TR-146 (2013): Subscriber Sessions

As derived from TR-101, the main access technology will be Ethernet. In particular, the Open BNG must support IEEE 802.1Q frames, and VLAN stacking (QinQ) mechanisms as per IEEE 802.1ad. It must be noted that QinQ must be supported even if the ethertype of the outer VLAN is 0x8100 instead of the standard 0x88A8.

It shall be possible to assign automatically one (or more) IP address to all subscribers in the Open BNG. These addresses may be assigned by one of the following mechanisms:

- Fixed defined by AAA server
- Dynamic from a pool configured in the Open BNG and referenced by AAA server
- Dynamic from a pool provided by AAA server

5.1 Encapsulation methods and protocols

5.1.1 PPPoE encapsulation

The platform must support PPP protocol as per RFC1661 (and later updates), permitting both PAP or CHAP authentication. Per-session keep-alive messages must be supported, with parameters like the interval time or the timeout being configurable.

Incoming PPP sessions will be encapsulated over Ethernet, either with one or with two VLAN headers.

5.1.2 IPoE plus DHCP service

Copyright © 2021 Telecom Infra Project, Inc.

The platform must support DHCP in combination with IPoE subscribers, as described in TR-101. It must also support the DHCP Relay Agent functionality, with the possibility to configure redundant DHCP Servers, and supporting Option 82 (DHCP Relay Agent Information Option).

Mechanisms to control the DHCP load (requests rate, filters, etc.) shall be implemented.

5.1.3 L2TP

Open BNG will also participate in wholesale scenarios, typically solved using L2TP. Therefore, the node must comply with the L2TP Access Concentrator (LAC) and L2TP Network Server (LNS) functionalities as per RFC2661.

According to this, it shall be possible to i) configure PPPoE subscribers and encapsulate their sessions over L2TP, and ii) terminate PPPoE subscribers that are encapsulated over L2TP. In the first scenario, regarding the decision on whether to terminate the session or encapsulate it, it must be possible either to configure it statically, or receive it dynamically via RADIUS, on a per session basis. In any case, it shall be possible to activate RADIUS accounting for these L2TP LAC services.

L2TP tunnels in which Open BNG participates must be able to support multiple PPPoE sessions, and it must be possible to have redundant L2TP tunnels.

5.1.4 VPN

It must be possible to map dynamically PPPoE or IPoE sessions on top of a VPN, via RADIUS control.

5.1.5 PPPoE/IPoE over PW

The support of incoming PPPoE/IPoE sessions over MPLS PW will be highly valued. This requirement may be of special importance in environments like that in section 2.2.2.2, in which MPLS end-to-end strategies can be applied. Moreover, active-standby PW support will be also appreciated, including the ability to synchronise the status of PW and BNG state. This could enable interesting resilience schemes, especially in conjunction with CUPS implementation.

5.2 IPv6

The Open BNG must support both dual stack (IPv4 and IPv6) access and IPv6 only access over PPP. Some requirements for the BNG functionality concerning IPv6 are:

Copyright © 2021 Telecom Infra Project, Inc.

- Wholesale model using L2TP must also be supported for IPv6 and IPv4/IPv6 sessions
- Prefix delegation (delegating router role) must be supported
- Support of DHCPv6 and DHCPv6 Relay is required
- The platform shall be able to interact with AAA servers including all IPv6-related attributes, in particular those dealing with prefix delegation
- In dual-stack environments, it shall be possible to steer IPv4 traffic from subscribers to external CG-NAT platforms, using for example VPN mechanisms.

5.3 Authentication, Authorization and Accounting (AAA)

Primary protocol for AAA in Open BNG will be RADIUS. Alternatively, support of DIAMETER will be valued. For those reasons, support of the most relevant RADIUS and DIAMETER RFCs will be requested. Some details for clarification are provided below.

In general, all subscriber and service profiles will reside in the AAA server. During the establishment of a subscriber session, the Open BNG will apply the specific profile(s) to the session. The Open BNG will also receive the IP address information from the AAA server.

It shall be possible to configure separate AAA servers for the different AAA processes, and it shall be possible to have redundancy for any of them. Similarly, to DHCP, it shall be also possible to configure control mechanisms in the AAA traffic, like specific rates, filters, etc.

It shall be possible to base the authentication mechanisms on four subscriber identifiers, each univocally identifying a subscriber:

- By the attributes NAS-Port (or NAS-Port-ID) plus NAS-IP-Address[4]
- By username and password
- By domain and/or agent_remote_id
- By Circuit and Remote Id

NAS-Port will typically code the physical port ID, plus the VLAN tag values in the QinQ.

[4] NAS-IP-Address must be a configurable parameter.

Copyright © 2021 Telecom Infra Project, Inc.

The information that identifies the subscriber must appear in the form of attribute in all authentication and accounting packets: Auth-req, Acc-req, Acc-Start, Acc-Update and Acc-Stop.

There are two different philosophies on how to deal with subscriber profiles.

The simplest design is based on an access parameterized profile, which is applied to the BNG logical interface where the subscriber is attached, containing all session and services parameters: these parameters, when a subscriber logs in, are assigned by the BNG the values indicated in the Radius Access-Accept message; in case the Radius server does not indicate a value for a specific parameter, the BNG will apply a default value, defined locally. As example of parameters that can be controlled via Radius the following can be mentioned: input/output filters, shaping rate, scheduler, classifier, rewrite rule, PPP authentication option (e.g. PAP, CHAP), routing-instance, etc.

Potentially, AAA can dynamically modify active sessions via Change-of-Authorization (CoA) messages. CoA messages can instruct BNG to create, modify, or terminate a subscriber service, or to set or modify usage thresholds (volume, time) for current subscriber services. Not all the Operators use CoA to dynamically modify sessions.

The sophisticated design is required by operators who seek more control or expect additional service activations by customers on the fly without interruption of the session. Here, the profile is separated into subscriber and service session part, where the service part might exist multiple times depending on the number of services, for example captive portals, an IPTV channel package or parental control. Based on this separation, the underlying implementation must support additional mechanisms, e.g. resolution in case of overlapping identifiers in service profiles. An illustration of the two design philosophies is given in Figure 18 below.

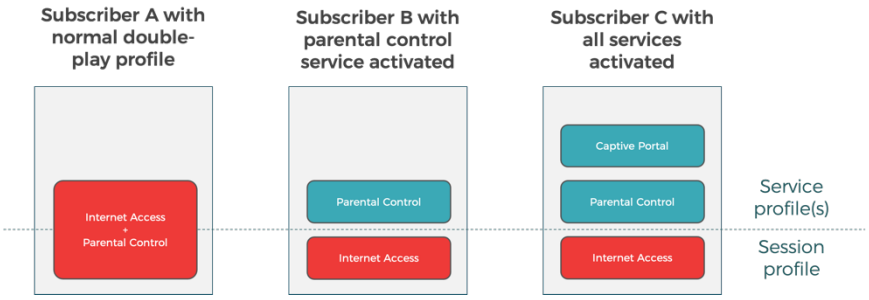

Figure 18. Simple vs stacked RADIUS profiles

In case of accumulation of a series of Radius requests to activate multiple services, it is important to mention that the platform will generate as many accounting sessions as

Copyright © 2021 Telecom Infra Project, Inc.

profiles/services are applied to a subscriber. In the simple design, Subscriber A of Figure 18 will have only one subscriber profile represented by single subscriber session accounting. In contrast, Subscriber C of Figure 18, for example, will have one accounting session for the subscriber session (as a whole), and then three additional accounting sessions, one for each of the applied service profiles (service session accounting). Each service accounting session will only take into account the traffic to which the associated profile has been applied.

Where multiple service profiles are applied, these would be stacked based on associated priorities to avoid conflicts so that it is clear how they apply at any moment. An example for service sessions is provided in Figure 18. Service profiles shall be executed consecutively, unless one profile determines otherwise (e.g. a captive portal for defaulting customers).

In both the approaches described above, with or without multiple services applied via Radius to the session, it shall possible to modify parameters on the fly without impact on the subscriber session itself or interruption on other service sessions. This might range from adaptation of the bandwidth of schedulers or shapers until fine granular configuration of ACLs. Irrespective of the parameters, the modifications shall be applied by using Change of Authorization (CoA) messages.

Accounting ON/OFF messages shall also be implemented. Together with a clear record of the allocation/withdrawal of IPv4, IPv6 and IPv4/v6 addresses.

5.4 Quality of Service

In multi-service nodes like the flavours of Open BNG that are being proposed, Quality of Service applies to all of the described services. However, requirements associated with the Internet Access are possibly the most complex, due to the strict hierarchical scheme that is demanded. This is why the QoS section is included as part of the BNG SW package.

It must be noted that Open BNG will not work with a single QoS header. Client interfaces are normally Ethernet based, so the platform will have to cope with Ethernet headers. On the contrary, network interfaces are normally IP/MPLS, so the node shall be able to interact at both levels, and to translate flexibly between them.

The number of required traffic classes is max 8 (eight). The platform shall be able to discriminate traffic and manipulate it based on the definition of those eight classes. The

Copyright © 2021 Telecom Infra Project, Inc.

platform must also be able to match the internally generated traffic (for example, routing protocols traffic and access side signalling such as PPPoE, DHCP, PPP traffic) to any of these traffic classes, based on configuration.

In this section, we will start from the simpler features (classification, marking, scheduling, etc.), and later on we will describe the H-QoS scheme required for the Open BNG.

5.4.1 Classification

In the ingress direction, the platform will perform two main processes[5]: classification and assignment to ingress queues. The platform shall be able to classify and assign incoming traffic based on at least one, or the combination of, the following parameters: physical/logical port, VLAN IDs (including VLAN stacking), Ethernet CoS value, MAC source/destination address, IPv4/IPv6 source/destination prefix, TCP/UDP port values, IP DSCP/Precedence value and MPLS EXP value.

The above classification must be possible not only at the physical port level, but also at the sub-interface (or VLAN, or logical port, etc.) level.

In addition, the platform shall be able to re-classify packets in the egress direction, before assigning an egress-queue, based on the same parameters as above (except for physical and logical port).

5.4.2 Marking

For each of the traffic classes defined in the node, the platform shall be able to re-write the priority values at the following headers: Ethernet CoS (at any VLAN tag), IP DSCP/Precedence and MPLS EXP. This re-writing will be based on specific rules defined by configuration. If not required to re-write the priority values at IP level, the platform shall leave them unchanged.

The platform shall also implement inheritance mechanisms, by which a certain header maps the QoS value of another header. The minimum requirement is that the QoS value of the IP Precedence header can be mapped both towards the Ethernet and MPLS QoS headers.

[5] Potential ingress policing will be described in a later section.

Copyright © 2021 Telecom Infra Project, Inc.

5.4.3 Scheduling

Similarly, to the classification process, the scheduling must also be possible at different levels, in particular, to individual logical connections (not only per port).

It is required that schedulers in the Open BNG can support up to 8 (eight) queues, with at least 2 (two)[6] different behaviours (priorities); it shall be possible for the highest priority to be configured as strict priority. The remaining queues shall support at least one weighted mechanism that ensures committed rates per queue (e.g. WFQ, WRR, etc.). Such committed rates may be defined either by numeric values, or by weights (percentages) of the total scheduler throughput.

An improved approach with regards to the number of queues and schedulers, which will be highly valued, is that each scheduler optimizes the usage of queues. In other words, each scheduler will only consume the number of queues that it requires (number that will be determined automatically and dynamically), and furthermore, if that number is not two or higher, the scheduler itself may not be needed[7].

With regards to exceeding traffic, it shall be possible to assign the remaining throughput to those queues that can still consume capacity beyond their committed rates, if available. It shall be possible to control the assignment of exceeding capacity for each traffic class. It shall also be possible to limit the maximum throughput that is assigned to the strict priority queue.

For dropping criteria, it shall be possible to define one of these policies on a per queue basis: Tail Drop (Weighted Tail Drop valued) or Weighted RED (with a minimum of two drop priorities).

As a result of the above description, each queue in the scheduler will be defined by the following parameters: priority, CIR, PIR, exceeding traffic policy (typically EIR) and drop policy.

5.4.4 Traffic rate limit

In general, shaping will be preferred over policing for limiting subscribers' traffic rates, both in the uplink and in the downlink.

[6] More than two priorities per scheduler will be valued.
[7] For example, if shaping is implemented at the scheduler itself, then the scheduler will be needed.

Copyright © 2021 Telecom Infra Project, Inc.

Shaping may be applied either as part of the schedulers or as a separate function. Independently of the implementation method, it must be possible to apply shaping to individual logical connections, not only on the physical port. The shaping rates and schedulers shall be controlled via Radius parameterised attributes.

It shall be possible to define CIR and PIR (or EIR, where PIR = CIR + EIR). The possibility to define CBS and EBS will be valued.

Two items must be noted:

- It shall be possible to apply shaping to those subscribers that will be later on tunnelled via L2TP.
- Per subscriber shaping values are part of the AAA policies.

It shall be possible to modify these values (e.g. speed upgrade operation) without the need to restart the session.

Independently of the support of shaping, policing must also be supported, both at the ingress and at the egress. Even if shaping is preferred for conditioning of subscribers traffic, many control mechanisms can still be implemented with policers. For that, it shall be possible to apply it to individual logical connections.

The following policer types will be required: i) single rate, two colours, and ii) two rate, three colours. Support of single rate, three colour policers will be valued. Actions applicable to policers will include, at least: forward, drop, re-classify, re-write and increment an associated counter.

5.4.5 Hierarchical QoS

The platform must permit the application (in cascade) of QoS policies at different hierarchical levels. Capabilities in each of these levels must be equivalent to those included in the sections above, and it shall be possible to configure the specifics of each level separately.

The H-QoS hierarchy can be expressed using the following three domains:

- Subscriber QoS, which implements subscriber-specific behaviours against individual subscribers, services, or groups thereof
- Network QoS, which implements subscriber-agnostic behaviours to model capacity constraints in the downstream access or transport network
- Interface QoS, which implements behaviours specific to physical or logical interfaces on the Open BNG itself

Copyright © 2021 Telecom Infra Project, Inc.

The Open BNG QoS model should be flexible enough to support a variety of configurations; indeed, while all deployments are expected to implement a variant of subscriber QoS, the configuration of network or interface QoS is expected to be specific to operator deployment scenarios.

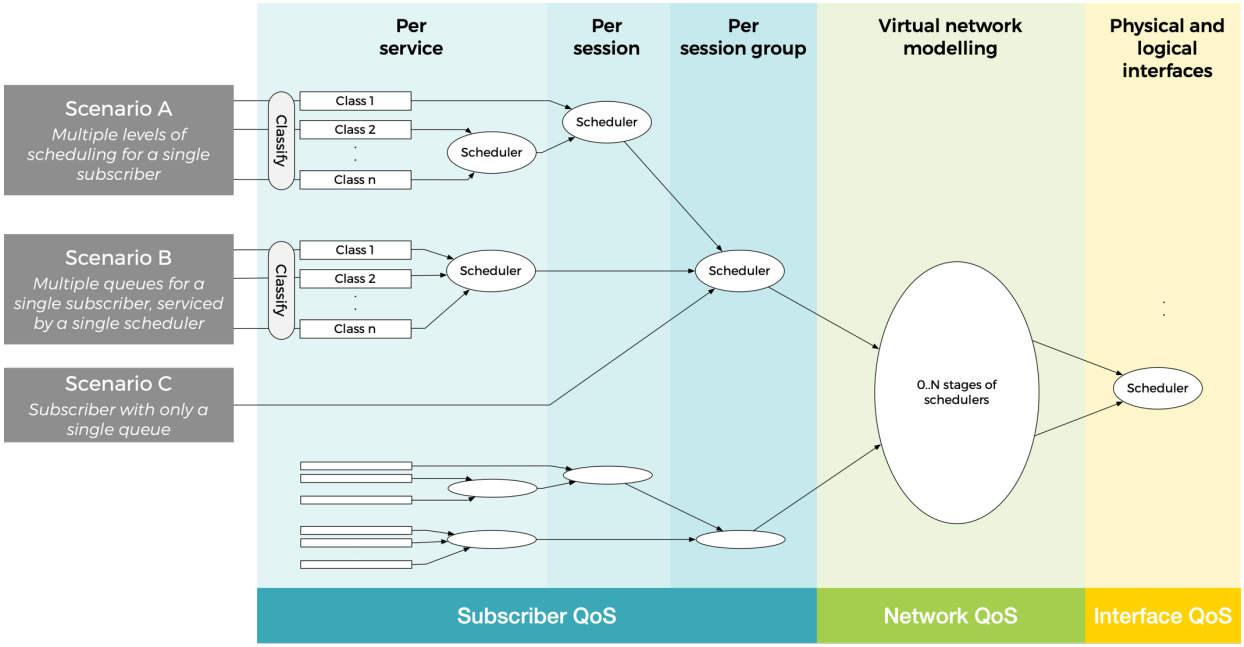

Figure 19. Indicative H-QoS hierarchy

Figure 19 above provides an indicative view of how downstream H-QoS could be configured on an Open BNG. In this instance, a number of levels are defined:

- **Per-service scheduling**. As described in section 5.4.3 above, the Open BNG should allow for up to 8 classes of service per subscriber, and with a variety of scheduling mechanisms to manage resource allocation for each class.
- **Per-session scheduling**, providing further scheduling of aggregated services for an individual subscriber. Session in this context is defined as an IPoE or PPPoE session with single or dual-stack. Multiple sessions may be associated with a single subscriber or household.
- **Per-session-group scheduling**, providing the ability to limit the overall bandwidth assigned to a group of users. User groupings may be based on transport identifiers (e.g. VLAN ID, PW), or may be assigned arbitrarily by RADIUS.
- **Virtual network modelling**, providing the ability to model downstream transport and access network components (e.g. a backhaul link or a PON segment). There

Copyright © 2021 Telecom Infra Project, Inc.

number of levels of scheduling at this level typically varies from 0 (no network QoS requirements) to 2 (access network and backhaul/transport network)

- **Interface scheduling**, governing queue and scheduler behaviours for physical/logical interfaces and sub-interfaces.

A minimum of three levels of subscriber H-QoS is required, although four or more are valued.

5.4.5.1 Shared Shaper

In H-QoS it's a valid business case that the SP provide a compound bandwidth for multiple services (e.g. High Speed Internet & VOIP/Gaming) to be shaped at a specific rate deducted from the total aggregate bandwidth sold or provided to the subscriber. To achieve this use case, a shared shaper is used to control the total consumed bandwidth for multiple services in the contention moments with other services that might need more bandwidth at this moment of contention instance.

For example: Suppose an end subscriber is provisioned a total aggregate bandwidth of 30Mb/s for the following services: High Speed Internet, VOIP, Gaming, & IPTV (HD) for one TV. The service provider will shape the HSI, VOIP, Gaming to specific bandwidth to allow and guarantee a bandwidth of HD channel to be transmitted to the subscriber at the moment of bandwidth contentions when all these services are running at the same time.

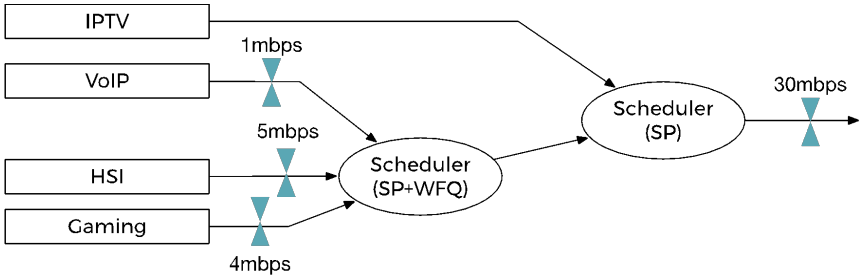

Figure 20. Shared shaper worked example

As depicted figure 20 above, the device will share shape different services at the following rates:

- HSI to 5Mb/s (WFQ)
- VOIP to 1Mb/s (with high priority queueing)
- Gaming to 4Mb/s (WFQ with higher Weight than HSI)

The rest of the total aggregate bandwidth will be allocated to the HD channel (e.g. 20Mb/s).

Copyright © 2021 Telecom Infra Project, Inc.

5.5 Multicast

The BNG SW package must be able to handle source specific multicast (SSM) per subscriber and provide replication mechanisms according to the used encapsulation and protocols (PPPoE/IPoE and IPv4/v6). A special attention shall be paid to the use of IGMP controlled multicast with PPPoE encapsulation. In addition to SSM, the support for commonly used any-source multicast with IGMPv2 must be given in order to handle existing and widely deployed CPE implementations.

While the BNG and the Router SW package (see section 6) must interwork, it must be based solely on source specific multicast and other variants must be adopted accordingly.

A special case is the deployment of a leaf-spine fabric and the distribution of the BNG and Router SW package in different nodes of the fabric. Here an additional network segment must support multicast and the preferred option is based on multicast support in L3VPN (RFC 6514).

Where multicast packet replication is performed external to the Open BNG – for example downstream within a separate head-end, or layer 2 switch - a dynamic policy control mechanism is required to shape (or police) unicast and multicast traffic flows that are distinguished by CVLAN. The requirement serves to maintain the contracted bandwidth ceiling that is applied to each end-user: the aggregated sum of the unicast and multicast traffic flows is dynamically clamped. In operation the policy control mechanism would decrement the unicast bandwidth allocated to the end-user to exactly match and rebalance each corresponding multicast bandwidth increment. The Open BNG control plane on receipt of an IGMP join/leave datagram from an end-user (multicast receiver) would invoke the policy control mechanism – yet maintain a sufficient unicast bandwidth floor to maintain voice services.

Details about the multicast capabilities for routing are given in section 6.

5.5.1 Call Admission Control

Where multicast is deployed, operators adopt many mechanisms to deliver the multicast traffic. In some cases, it may be necessary to implement CAC to enable the Open BNG to feedback the MSAN as well as the subscriber's STB if there is enough bandwidth for the requested Multicast IPTV channel. When the Open BNG receives an IGMP join message from the MSAN (while the MSAN is configured with IGMP snooping)

Copyright © 2021 Telecom Infra Project, Inc.

and there is no bandwidth available for the requested IPTV channel; Open BNG will send a Deny CAC protocol message to the MSAN which will switch it to the subscriber's STB. In case the MSAN is configured with IGMP proxy, the CAC message sent by the Open BNG will be sent to the MSAN which will in turn forward it to the subscriber's STB.

5.6 Lawful Interception

The Lawful Interception mechanism supported by the Open BNG must be compliant with ETSI specifications like ETSI TR 101 943 (2004) and ETSI TR 102 528 (2006), in particular with regards to Reference Points INI1, INI2 and INI3 (X1, X2 and X3 in 3GPPP standards). The proposed platform must implement the Internal Intercept Function (IIF), while access and control of this function will only be possible from an Administration Function (ADMF). This access will be done ensuring that:

- There is a single dedicated user profile, duly authenticated, with features not accessible to any other user profile (not even administrator). LI related configurations will only be visible for this profile.
- Connectivity is limited to a single IP and port, with only one concurrent user, which is the ADMF.

Requirements for the IIF at the Open BNG include:

- Same availability as any other node feature.
- It shall be synchronized via NTP.
- Any audit data will be generated and sent to an external safe-keeping node. This communication will be encrypted. The Open BNG will not store any of the audit data.
- Audit data may be sent in-band or out-of-band. In particular, it shall be possible to send it over a VPN.
- There will be no actions by the IIF that permits the target to learn that it is being intercepted.
- It shall be possible to apply LI to PPPoE and IPoE subscribers, even those tunneled using L2TP (in this case it's the LNS that plays the role of IIF).
- Identification of the target subscriber will be done based on any of the parameters that may govern the subscriber authentication (as defined in section 5.3) and/or by 5-tuple match (source/destination IP address, protocol, and source/destination port)

Copyright © 2021 Telecom Infra Project, Inc.

- Reboot of the Open BNG shall not affect the LI operation and configuration.

Copyright © 2021 Telecom Infra Project, Inc.

6

Router Software Package (RSW)

Routing capabilities for Open BNG

TELECOM INFRA PROJECT

6 Router Software package (RSW)

The following list of requirements is included to ensure that the Open BNG platform will be able to work in any type of network scenario potentially deployed in the production networks of the participating operators. Some of these requirements may be considered as prerequisites for the support of VPN services (i.e., pre-requisites for the Open BNG operating as a PE). Examples of these may be MP-BGP or T-LDP. However, they will be included here to avoid too much dispersion in the location of requirements.

6.1 IP/MPLS routing

Firstly, it is important to note that the Open BNG must support dual stack (IPv4 and IPv6), or IPv6 only, in all its network interfaces[8]. In fact, for all the protocols mentioned below, it will be understood that they must support the applicable IPv6 extensions (when applicable).

The high-level list of routing protocols is the following:

- Static routing.
- IS-IS, including extensions for Traffic Engineering.
- OSPFv2/v3, including extensions for Traffic Engineering.
- BGP-4, including multiprotocol extensions, capabilities advertisement (RFC5492), communities (RFC1997), BGP-LU (RFC3107), deterministic-med (RFC 4721), graceful restart / non-stop Forwarding (RFC 4724), extensions for 4-byte AS number (RFC4893), confederations (RFC3065), route reflection (RFC4456), error-handling (RFC 7606), peer tracking (RFC 7854) and prefix-Independent Convergence (PIC)[9].

With regards to these protocols, the proposed platform must support distributing routes between any of them, based on defined policies, and also distributing local and static routes. It must also support modifying the priority (administrative distance) of the

[8] Requirements for interfaces towards the CE, when the Open BNG acts as a PE node, are defined in section 7.

[9] Bashandy, A., Ed., Filsfils, C., and Mohapatra, P.: "BGP Prefix Independent Convergence", Work in Progress, https://datatracker.ietf.org/doc/html/draft-ietf-rtgwg-bgp-pic-13, February 2021.

Copyright © 2021 Telecom Infra Project, Inc.

different routing protocols when populating the active FIB. Any mechanism for mutual authentication must support at least MD5 authentication.

MPLS must be supported as well, with at least four MPLS labels in the label stack. Signalling of MPLS labels must be possible both using:

- LDP, including T-LDP and IGP and LDP synchronization.
- RSVP-TE, with the capability of path computation based on CSPF and supporting FRR mechanisms.

Finally, other features that are required include:

- ECMP
- Entropy-label-based load balancing[10]
- IP LFA FRR mechanism
- VRRP
- Multicast capabilities, both for IPv4 and IPv6, for L3VPNs outlined in RFC6514 as the preferred option
- Policy Based Routing (this will be described further below)
- PWE3

Policy based routing (PBR) must be supported and capable of being implemented to forward all subscriber traffic to an ISP gateway. The PBR mechanisms are required to prevent any local turnaround of subscriber traffic. This is particularly apposite for peer-to-peer traffic. The PBR mechanism must therefore:

- support the forwarding of PBR traffic to an indirect next hop i.e. using a route in the routing table;
- where there is no route in the routing table assigned as the PBR address, then the default route, if present, should be used;
- support the ability to set exceptions to the PBR policy for particular destination IP addresses, so that traffic to those destination IP addresses ignores the PBR policy and uses the routing table.

[10] Akiya, N., Swallow, G., Pignataro, C., Malis, A., and Aldrin, S.: Label Switched Path (LSP) and Pseudowire (PW) Ping/Trace over MPLS Networks Using Entropy Labels (ELs); https://datatracker.ietf.org/doc/html/rfc8012, November 2016.

Copyright © 2021 Telecom Infra Project, Inc.

Segment Routing (and other mechanisms like TI-LFA) shall be supported, using MPLS encapsulation (SR-MPLS) and associated OSPF/IS-IS extensions. Support for alternative segment routing technologies (e.g. SRv6) would be valued. If segment routing is not supported, then proposals complying with this specification must demonstrate a clear roadmap to implement Segment Routing. Policy-based routing will be required to eliminate forwarding to non-adjacent next-hops i.e. a mechanism to prevent subscriber-to-subscriber traffic flow. On the other hand, the Open BNG must support PCEP and BGP-LS, to account for the deployment of PCE nodes together with RSVP-TE.

Finally, and despite the strong focus on layer-3 functionalities, support of layer-2 Ethernet switching is also required in the Open BNG.

6.2 Link aggregation

The proposed platform must support aggregating several physical ports into a single logical interface, based on LACP protocol as defined in IEEE 802.1ax. Both LACP active-active and active-standby shall be supported.

Schemes for balancing the load among the different ports that achieve a balanced share will be preferred. It shall also be possible to determine by configuration the number of interfaces within a LAG that determine the failure status of the whole logical interface (e.g. 1 out of 3, 2 out of 2...).

All the IP/MPLS, QoS, synchronization, OAM and Performance Monitoring functionalities shall work on logically aggregated interfaces.

The traffic balancing algorithm must be based on MAC over L2 links and on IP flow over L3 links.The support of multi-chassis LAG, meaning that a single device can connect using LACP, in a dual-home active/standby scheme to two ports in two different Open BNGs, will be valued.

6.3 BFD

The proposed platform must support Bi-directional Forwarding Detection (BFD) for failure detection as described in RFC5880. In particular, it is required to support BFD in Ethernet interfaces, and in LACP interfaces as described in RFC7130. It is also required to support BFD in the signalling protocols listed in section 6.1, and in MPLS LSPs.

Copyright © 2021 Telecom Infra Project, Inc.

7

Provider Edge Software Package (PESW)

Open BNG as a PE for enterprise services

TELECOM INFRA PROJECT

7 Provider Edge Software package (PESW)

The following is a summary of the requirements for the Open BNG acting as a PE of L2 and L3 VPN services. As commented before, this summary relies on the support of certain transport protocols which are described in section 6.

A Multi-Service BNG is defined in the Broadband Forum Technical Report: TR-178 Issue 2 (2017) – Multi-service Broadband Network Architecture and Nodal Requirements. Any Open BNG platform proposal must provide a very high degree of compliance with such Technical Report and its list of requirements.

7.1 L2VPN

In the provision of L2 services for enterprise customers, the Open BNG shall be MEF 2.0/3.0 compliant, at least with regards to E-LAN and E-LINE services. E-TREE services will be valued. It will be very beneficial that the proposed platform is certified accordingly.

In particular, the platform must support the implementation of E-LINE services based on VLL technology, and E-LAN services based on VPLS. Support of H-VPLS topologies will also be valued.

Requirements below have already been tackled in previous sections, but they are included here as well for specific clarification of their usage in a L2VPN environment.

- The proposed platform must be able to forward traffic into the L2VPN at least based on the following encapsulations: no tagging, VLAN tagging (IEEE 802.1q), VLAN double tagging (IEEE 802.1ad) and MACinMAC (IEEE 802.1ah). For double tagging, the TPID value must also admit 0x8100 in the outer VLAN, together with the standard 0x88A8.
- The proposed platform will permit the establishment of CIR, EIR, CBS and EBS parameters over the L2VPN service and/or each specific L2VPN client connection.
- The proposed platform will permit configuring specific Layer-2 based filters per each L2VPN client connection. Other standard security measures shall be supported as well.
- For E-LAN (and E-TREE, in case they are supported) services, it must be possible to configure in the proposed platform a different rate limit per each type of BUM traffic (one for broadcast, one for unknown unicast and one for multicast). It must

Copyright © 2021 Telecom Infra Project, Inc.

also be possible to configure limits in the number of learnt MAC addresses per service and client interface, and the lifetime for these learnt MAC addresses.

Finally, redundancy mechanisms, loop detection mechanisms and OAM functionalities shall be included in the proposed platform. IGMP snooping must also be supported.

7.2 L3VPN

Full-mesh and Hub & Spoke models of BGP/MPLS L3VPN must be supported for IPv4 and IPv6. In particular, the proposed platform must support the establishment of a L3VPN over multi-AS backbones.

The non-exclusive set of protocols outlined in Section 6.1 (RIP, IS-IS, OSPF and BGP-4) including static routing, must be supported in the CE/PE link. BFD associated with these protocols and DHCP Relay must also be included.

With regards to the rest of the features, like QoS, multicast, filtering, redundancy, etc., the same requirements as listed in sections 5 and 6 for IP environments must be supported, both in the client and network interfaces. Additionally, control plane control mechanisms (e.g. BGP dampening) shall be available.

7.3 E-VPN

The proposed platform must support E-VPN services. All the requirements specified above for MPLS based VPN services shall apply as well to corresponding E-VPN variants.

E-VPN must be supported with single and multi-homing (with single-active and all-active modes supported for the latter case).

Copyright © 2021 Telecom Infra Project, Inc.

8

BNG CUPS

Control and User Plane Separation

TELECOM INFRA PROJECT

8 BNG CUPS: Control and User Plane Separation

As described in section 3, the core focus of the Open BNG initiative is to open and disaggregate the BNG function. While much of this document describes the decoupling of BNG HW and SW, there are also opportunities to further disaggregate the SW stack.

While the BSW package described in section 5 provides both control plane and user plane functions, the following sections describe an alternative approach involving separation of control plane and user plane functions as introduced in section 3.3.1 above. BSW-CUPS can be deployed instead of the BSW package in the case where operators are looking to deploy a CUPS-based solution.

Note, while this section focuses primarily on CUPS, any opportunities to improve the level of convergence, openness and disaggregation will be valued. Of great importance for fixed access solutions, however, is to make sure that no solution for convergence has an impact on the current complexity and cost of fixed services. Proposals that modify the architecture and processes of fixed broadband to assimilate mobile paradigms will be strongly discouraged, unless fully justified economically.

8.1 Operator drivers for CUPS

Broadband Forum TR-459 defines a mode of disaggregation of a BNG that separates the subscriber control plane from the user plane.

Copyright © 2021 Telecom Infra Project, Inc.

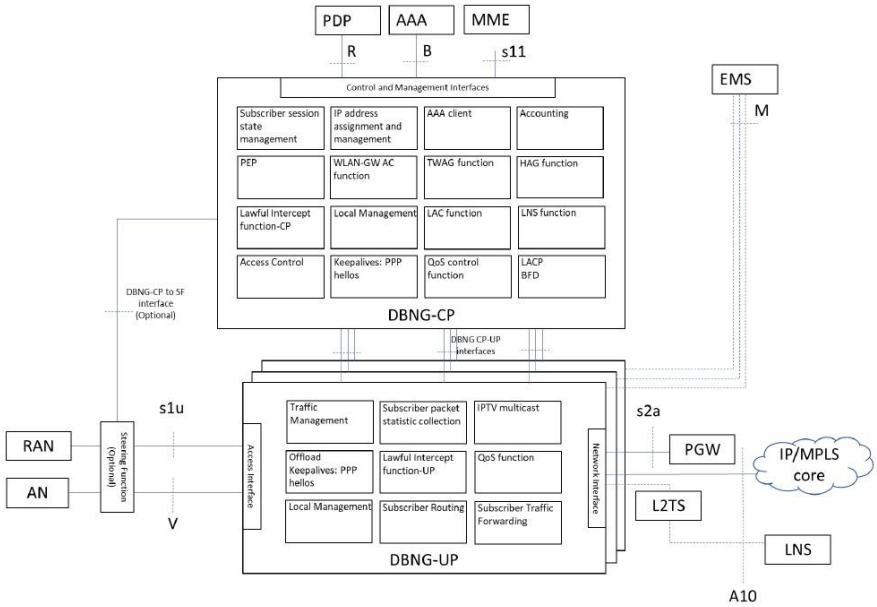

Figure 21. TR459 Disaggregated BNG Architecture (source: Broadband Forum)

As shown in Figure 21, all of the responsibility for subscriber signalling, session state, and interfaces to policy systems is maintained in the Control Plane in the TR459 architecture. The User Plane is simplified such that it mainly performs the forwarding and queueing functions, as well as running a local routing control plane to support fast convergence in response to network changes.

Whilst an Open BNG can benefit from hardware disaggregation (where the hardware and the software that runs on it can be provided by different suppliers), TR459 does not have any inherent view on Hardware Disaggregation, instead focusing on the separation of subscriber control and user plane. The User Plane of a TR-459 dBNG is still required to maintain a number of control plane aspects (such as routing and keepalive generation).

Potential drivers for an operator to deploy TR-459 based disaggregated BNG:

- Reducing the complexity of the Physical User Plane.
- Centralized Subscriber State for enhanced geographic resilience.
- Automated, on demand, distribution of IP address blocks.
- Control Plane can benefit from cloud paradigm such as scaling, robustness and continuous deployment.
- Convergence of User Plane across Fixed Broadband, Cable, and Fixed Mobile (through the CUPS approach for Wireless Wireline Convergence)

Copyright © 2021 Telecom Infra Project, Inc.

- Support for unique or innovative subscriber management or authentication approaches without needing to upgrade software across a large user-plane deployment.

Where Open BNG operators are looking to deploy TR-459 based disaggregated solutions, these drivers are expected to map to the following outcomes:

- Independent Control and User Plane scaling and life-cycle management.
- Geographic separation of Control Plane and User Planes, with User Planes distributed in sites closer to subscribers to exploit local Service Platforms for low latency and high bandwidth services.
- A Centralized Control Plane facilitates the use of well-tailored User Planes, possibly small and numerous, without increasing Operational costs. This opens up to User Plane SW solutions too, which can be brought online rapidly in response to network failures or short term scaling requirements.
- Fast introduction of other Vendors' User Plane technologies under the control of an already deployed Control Plane, keeping control and management interfaces towards external systems (such as PDP, AAA, OSS,...) unchanged.
- Use of specialized User Planes, where the chipset resources are tailored and optimized for a particular type of customers or sessions (e.g. sessions dedicated to premium video).

8.2 OpenBNG CUPS Architecture

An Open BNG implementation with TR-459 will affect the 'BNG software package', effectively splitting it into two separate functions.

- The TR-459 Control Plane, which moves the subscriber control-plane aspects into the cloud where they can be implemented in a cloud-native approach allowing enhanced scaling, resiliency and the ability to be upgraded seamlessly, without customer impact.
- The TR-459 User Plane, which is responsible for terminating the TR459-defined interfaces from the control-plane and ensuring the required forwarding and QoS rules are implemented into the forwarding plane, as well as passing the required subscriber prefixes to the routing package for advertisement.

The Routing and PE packages are not affected.

Copyright © 2021 Telecom Infra Project, Inc.

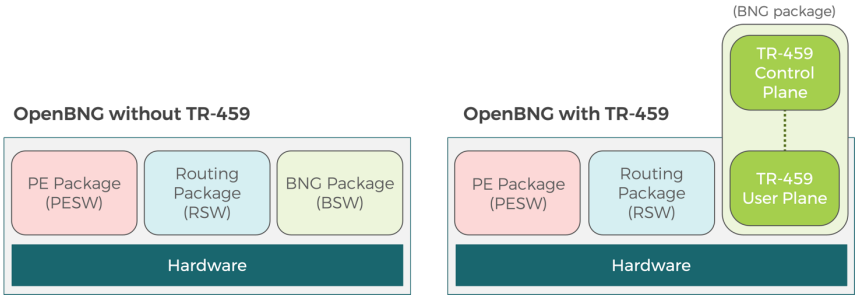

Figure 22. Open BNG with and without TR-459

Whilst the deployment model is at operator's discretion, a TR-459 control plane is expected to support many millions of subscribers distributed across hundreds of user planes, possibly of different sizes and optionally with some being deployed as pure software forwarding planes.

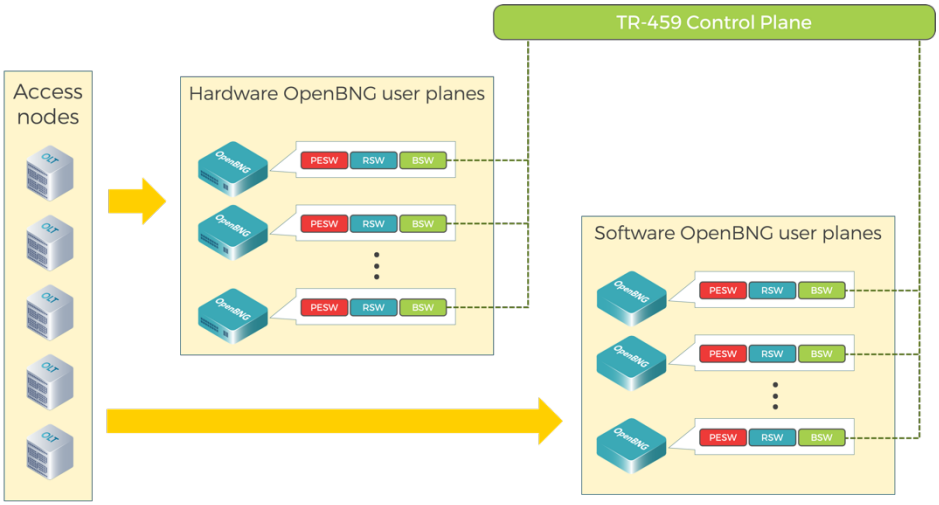

Figure 23. TR459 Control Plane across multiple Open BNG User Planes

The option of supporting Open BNG with software forwarding planes under the same subscriber control plane may also provide the option to forward a subset of subscribers that require complex services or scheduling that is not possible on particular hardware solutions to a different User Plane. This approach means that an operator does not need to deploy hardware across the board that covers the superset of all subscriber requirements.

The standardization of the TR459 interfaces will also enable deployment of Open BNG User Plane elements alongside more traditional BNG User Plane in the same system. This may enable easier and incremental integration of Open BNG solutions into an operator network.

Copyright © 2021 Telecom Infra Project, Inc.

8.3 Minimum Open BNG requirements for a TR-459 UP

The 'TR-459 User Plane' Package will support the following for a minimum viable solution:

- Two simultaneous PFCP associations with the following features:
  - PPPoE
  - IPoE
  - LCP Keepalive Offload
  - L2TP LAC
  - L2TP LNS (desirable, but not mandatory)
  - NAT-CP (from WT-459.2, where the underlying forwarding plane supports NAT)
- Forwarding of subscriber control plane traffic into the GTP-u Control Packet Redirection Interface (under direction of the TR-459 CP, with the required NSH header and metadata added.
- To support named QoS profiles that can be referenced by a session establishment.
- To support subscriber sessions on physical interfaces
- To support subscriber sessions on logical interfaces that can be created through basic configuration (i.e. VLAN sub-interface)
- To support subscriber sessions on the logical interfaces that can be created through the routing package (i.e. Ethernet within an outer tunnel such as an MPLS Pseudowire)
- To pass relevant prefix information (in particular Address Pools and Framed Routes) to the Routing package running on the UP.
- To support resiliency scenarios based on moving from a UP to another groups of subscribers, associated by a common prefix announcement, in case of failures.

Copyright © 2021 Telecom Infra Project, Inc.

9

Open BNG management, programmability and security

9 Open BNG management, programmability and security

The following section describes requirements for the management and monitoring of Open BNG devices, as well as security considerations affecting the management, control and forwarding plane.

9.1 Management

As stated in section 4.4, both out-of-band and in-band management must be supported. For this, mechanisms based on SSH, CLI and Netconf will be preferred to those based on web browser.

The CLI will permit the configuration of different access profiles, at different levels and with different permissions (e.g. operator, monitoring…). It will also permit the login of multiple concurrent users.

The following protocols shall be supported:

- SNMPv2c/v3, for management and configuration purposes
- Netconf for management and configuration purposes
- NTP, for time synchronization with the rest of the network
- SCP or SFTP, for file transfer (e.g. configuration files or software upgrade versions)

9.2 Monitoring

SNMP may also be used for monitoring purposes. In that sense, the platform shall support the required MIBs for monitoring of the main activated functionalities, and it must be possible to send monitoring traps to multiple destinations.

The support of SYSLOG is also a requirement for logging redirection: all relevant system events must generate SYSLOG messages, which may be sent to multiple SYSLOG servers.

Performance indicators such as Netflow/IPFIX are also a requirement for the Open BNG. It must be possible to define by CLI the sampling criteria (one out of “n” packets sent), and the vendor must ensure the values of “n” which will not affect the performance. It shall be possible to activate Netflow/IPFIX on a per interface basis, and to define several collectors for the exporter.

Finally, for monitoring of quality of service, support of Y.1731, CFM 802.1ag, Y.1564, PNPM,

Copyright © 2021 Telecom Infra Project, Inc.

IPSLA or RPM, OWAMP and TWAMP mechanisms is requested.

9.3 SDN and Programmability

As explained in previous sections, we encourage more modern and advanced management mechanisms and protocols with improved programmability and SDN support. The intention is to have a (centralised) control entity (an SDN Controller) managing Open BNG in a smart and automatic way.

The SDN controller could be centralised and connected to the Open BNG in an out- or in-band management connection. Alternatively, the SDN controller could be collocated to the Open BNG, especially in fabric designs. We appreciate deployments where the Open BNG domain may be orchestrated in common with adjacent domains e.g. access/regional aggregation domain, IP/MPLS backbone domain etc. to provision and maintain an end-to-end service. Also, there are situations where optical line termination (OLT) elements are incorporated within a combined OpenOLT / Open BNG domain. But it is emphasised that regulatory oversight or market conditions can mandate that the Open BNG is managed separately and distinctly from other network elements.

The SDN controller shall manage and optimize the Open BNG domain in order to perform SLA fulfilment and service provisioning (Figure 23). All the configuration and management of the Open BNG shall be done using industry wide well accepted protocols like Netconf (RFC7803) or gNMI. Netconf connections could be encrypted using Transport Layer Security (TLS) [RFC5246] or Secure Shell (SSH) [RFC4251], with TLS being the preferred option. gNMI should use TLS secured HTTPS connections.

BGP-LS (IETF RFC 7752), the PCE architecture (PCEP protocol) (IETF RFC 4655 e IETF RFC 5440) and Stateful PCE will be also valued.

Copyright © 2021 Telecom Infra Project, Inc.

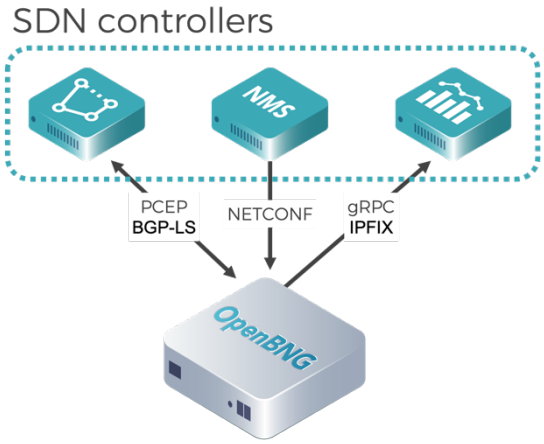

Figure 24. SDN controller and management interfaces

The Open BNG will be compliant with OOPT MUST TIP SBI specification for the use cases applicable to the Open BNG. Current OOPT MUST TIP SBI specification, version 1.0, was released in February 2021 and is available in TIP website. The specification is updated quarterly to incorporate additional use cases. For the Open BNG use cases not yet covered by MUST TIP SBI specification 1.0, operators will work to augment MUST TIP SBI specification with them, and if there exist no YANG models by any standards organization covering these use cases, operators will work to augment the applicable YANG models to support these use cases. These extensions will be taken to the relevant standard/industrial bodies, being Openconfig the favored choice for that purpose.

9.4 Network Telemetry

Open BNG shall support advanced monitoring and telemetry features, in particular:

- gRPC Network Management Interface (gNMI), gPB (Google Protocol Buffers) proto3 for encoding, and data exported (modelling) based on YANG models
- YANG push (RFC 8639, RFC 8640, RFC 8641, RFC 8650) with support for YANG QoS models[11]

Those will be used by the SDN controller (Figure 24) in order to monitor the status of the platform and the different services instantiated in the node.

[11] Choudhary, A., Ed., Jethanandani, M., Strahle, N., Aries, E., and I. Chen, "YANG Model for QoS", Work in Progress, draft-ietf-rtgwg-qos-model-03", February 2021.

Copyright © 2021 Telecom Infra Project, Inc.

9.5 Security

The following is a non-strict list of requirements having to do with security of the platform. Participating operators strongly encourage vendors to keep these capabilities up to date, incorporating new mechanisms as soon as they become available.

The proposed platform must be capable of implementing segment, packet and frame PDU filters in any physical or logical interface, and in the incoming and/or outgoing directions simultaneously with fine-grained – per subscriber - granularity. Filters will be able to take into account any combination of the following arguments: source/destination IP address, source/destination port, protocol, source/destination MAC address, VLAN, TCP flags, fragmentation flags, ICMP type and packet size. There must be counters available for each rule in the filter, increasing with each matching packet, and available for consultation via SNMP.

With regards to management operations, the platform must support the following:

- TACACS+ for authentication and authorization of the CLI features.
- Logging of all the commands executed by all the operators, for audit purposes.
- SSH sessions with 3DES encryption – and not preclude options to use more advanced encryption methods e.g. AES-128 or AES-256.
- Restriction of the management access only to a defined subset of IP addresses.

In the data plane, the platform must support Unicast Reverse Path Forwarding (URPF), as defined in RFC3704. Further, for PPP Termination and Aggregation (PTA) sessions, uRPF must be applied per subscriber. It must also be capable of limiting the maximum number of MAC addresses and limiting the BUM (broadcast, unknown unicast and multicast) traffic per physical or logical interface.

Protection mechanisms against Denial of Service (DoS) attacks is also required, at least for the following list: Tear Drop, Ping of Death, Smurf, Fraggel, UDP Flood and SYN-ACK.

Mechanisms to moderate control protocol (e.g. LCP) traffic load per subscriber (requests rate, filters, etc.) shall be implemented. Finally, the proposed architecture must ensure the maximum possible isolation between the control and management planes, and the data plane.

9.5.1 IPSec

The Open BNG must support IPSec RFC4835 (updated by RFC7321 and later by RFC8221)

Copyright © 2021 Telecom Infra Project, Inc.

defines the encryption and authentication algorithms that should be supported. The primary use cases for IPSec are to protect control and management plane traffic, and for the protection of other critical data in transit (e.g. lawful interception flows).

The implementation solution for IPSec must try to minimize the impact on the CPU usage and the introduced latency. HW-supported implementations will be permitted, although implementations that result in external specific components should be avoided (e.g. specific network cards).

IPSec must be compatible both with IPv4 and IPv6.

9.5.2 Access security and Anti-Theft

In general, the solution must support the necessary security mechanisms to authenticate and encrypt communications between the network element and its management system or controller.

The Open BNG must offer the possibility of enabling this traffic only after it has been authenticated by the management platform/controller.

The system should also offer the possibility to enable anti-theft mechanisms that prevent the use of the equipment in any other environment than the one it was conceived for.

Copyright © 2021 Telecom Infra Project, Inc.

10

Additional requirements

10 Additional requirements

To finish this specification, the following sections include additional requirements which do not fit any of the software packages defined above, but that are mandatory independently on the Open BNG flavour.

10.1 Port mirroring

The proposed platform must support mirroring capabilities, transparent (i.e., not impacting) to the rest of the Open BNG functionalities. In particular, specification of characteristics like the source granularity (LAG, port, VLAN, etc.), the source direction (RX, TX, both) and the destination (port, IP address, tunnel) is required. Mirrored traffic must be capable of redirection and appropriate encapsulation over physical or logical interfaces to nominated destinations.

It must be possible to activate multiple concurrent mirroring sessions, and to send the mirrored traffic to multiple destinations at the same time.

Port mirroring capabilities must coexist simultaneously, and will not interfere, with those for Lawful Interception.

10.2 Configuration and versions management

It shall be possible to modify the node configuration by means of configuration files accessible or directly copied in the node disk (via SFTP or SCP). Processes of file transfer, loading of a target configuration, and activation of the target configuration shall be three different processes. None of this shall require a reboot of the node, nor will affect its operational status.

It will be valued that more than two (active and target) configuration versions are accessible to the operator. This will be achieved by storing more than one target configuration in the node. It shall be possible to activate any target configuration from those stored.

Prior to the activation of a target configuration, the device will check its coherence, and will warn the operator of any incompatibility.

For configuration changes based on CLI:

- No configuration change will require a reboot of the system for its activation

Copyright © 2021 Telecom Infra Project, Inc.

- It will be valued that the introduction of the command, and its activation, are two different processes (e.g. using “save configuration” or “commit” commands).

On the other hand, notwithstanding automated procedures for Zero-Touch Provisioning as described in section 10.3, it shall also be possible to transfer a software package to the node for a version update or downgrade. Again, the process of transferring the file, and activating it, must be two different processes, and none must require a reboot or affect its operational status. Indeed, it is strongly encouraged that, even for those proposals that are built using a pizza-box approach, and do not implement redundancy of the control board, ISSU is supported.

10.3 Zero-Touch Provisioning

Zero-Touch Provisioning (ZTP) is the process to deploy a Network Operating System (NOS) and a base configuration in a network element, so it can enter in production environment without any human configuration. ZTP process is executed for the first time when the device is turned on in the network.

Periodically, system vendors release new versions of their NOS; a very similar process can be done for upgrade scenarios. Nowadays, the NOS upgrade process is a vendor-dependent process, which differs between each vendor solution. The ZTP and upgrade mechanisms should evolve to generate a common procedure for open white-box scenarios.

This procedure will influence the requirements with regards to configuration management. The ZTP platform or the SDN controller will have to maintain the NOS images and a pointer for the current configuration files that the network element requires.

10.4 Licensing

It is not the goal to define a strict licensing agreement at this stage, but some important ideas, in line with the disaggregation philosophy, would include:

- With regards to SW packages defined in sections 5 to 8, it should be possible to differentiate between licenses associated with each of these packages. The figure of an “all included” license should also exist.
- Upgrades to features existing in one of the packages should not affect the cost of other SW packages.

Copyright © 2021 Telecom Infra Project, Inc.

- The platform shall be compatible with a pay-as-you-grow model not only from the hardware point of view, but also as defined by software licenses.

10.5 Local regulation compliance

Again, it is not a goal to include in this section the full list of local regulations that would apply to the commercialization of an Open BNG. It is worth mentioning, however, a few of them.

The solution shall be compliant with EU GDPR regulation: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

For the Brazilian market, the solution must have a Certificate of Conformity issued by a Designated Certification Body and approved/homologated by ANATEL.

Copyright © 2021 Telecom Infra Project, Inc.

11Glossary Example

AAA	Authentication, Authorization and Accounting
AC	Alternating Current
ADMF	Administration Function
AGF	Access Gateway Function
API	Application Programming Interface
AS	Autonomous System
ASIC	Application-Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
BBF	BroadBand Forum
BFD	Bidirectional Forwarding Detection
BGP-4	Border Gateway Protocol 4
BGP-LS	BGP Link State
BGP-LU	BGP Labelled Unicast
BMCA	Best Master Clock Algorithm
BNG	Broadband Network Gateway
BRAS	Broadband Remote Access Server
CAC	Call Admission Control
CBS	Committed Burst Size
CE	Customer Edge
CG-NAT	Carrier Grade Network Address Translation
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate
CLI	Command Line Interface
CoA	Change of Authorization
CoS	Class of Service
CPU	Central Processing Unit
CUPS	Control and User Plane Separation
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DSCP	DiffServ Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
E-VPN	Ethernet VPN
EBS	Excess Burst Size

Copyright © 2021 Telecom Infra Project, Inc.

ECMP	Equal Cost Multi Path
EIR	Excess Information Rate
ER	Extended Reach (optics)
EXP	MPLS EXPerimental bits
FIB	Forwarding Information Base
FPGA	Field-Programmable Gate Array
FRR	Fast Reroute
gNMI	gRPC Network Management Interface
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
gRPC	gRPC Remote Procedure Call
H-QoS	Hierarchical Quality of Service
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IIR	Internal Intercept Function
IP	Internet Protocol
IPSLA	Internet Protocol Service Level Agreement
IRI	(lawful) Interception Related Information
IS-IS	Intermediate System to Intermediate System
L2BSA	Layer 2 BitStream Access
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LAC	L2TP Access Concentrator
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LDP	Label Distribution Protocol
LEA	Law Enforcement Agency
LED	Light Emitting Diode
LFA	Loop Free Alternate
LI	Lawful Intercept
LNS	L2TP Network Server
MAC	Media Access Control
MBH	Mobile Backhaul
MPLS	Multiprotocol Label Switching
MPLS-TP	MPLS Transport Profile

Copyright © 2021 Telecom Infra Project, Inc.

NAS	Network Access Server
NBI	North-Bound Interface
NIC	Network Interface Card
NNI	Network-Network Interface
NOS	Network Operating System
NTP	Network Time Protocol
OAM	Operations, Administration and Management
OCP	Open Compute Project
OLT	Optical Line Termination
ONIE	Open Network Install Environment
OSPF	Open Shortest Path First
OWAMP	One-Way Active Measurement Protocol
PAP	Password Authentication Protocol
PBB	Provider Backbone Bridge
PCEP	Path Computation Element Protocol
PE	Provider Edge
PIC	(BGP) Prefix Independent Convergence
PIR	Peak Information Rate
PNPM	Passive Network Performance Monitoring
PPP	Point to Point Protocol
PTP	Precision Time Protocol
PW	Pseudowire
PWE3	PW Emulation Edge to Edge
QinQ	802.1Q Tunnelling
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RED	Random Early Detection
RFC	Request For Comments
RIP	Routing Information Protocol
RSVP-TE	Reservation Protocol – Traffic Engineering
SC	Standard Configuration
SCP	Secure Copy Protocol
SDN	Software Defined Networks
SFP	Small Form-factor Pluggable
SR	Short Reach (optics)
SKU	Stock Keeping Unit
SLA	Service Level Agreement
SME	Small or Medium Enterprise

Copyright © 2021 Telecom Infra Project, Inc.

SNMP	Simple Network Management Protocol
SOHO	Small Office, Home Office
SSH	Secure Shell
STB	Set-Top Box
T-BC	Telecom Boundary Clock
T-LDP	Targeted LDP
TACACS	Terminal Access Controller Access Control System
TCP	Transport Control Protocol
TI-LFA	Topology Independent LFA
TLS	Transport Layer Security
TWAMP	Two-Way Active Measurement Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
UPF	User Plane Function
URPF	Unicast Reverse Path Forwarding
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VLL	Virtual Leased Line
VM	Virtual Machine
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
VxLAN	Virtual Extensible Local Area Network
WAN	Wide Area Network
WFQ	Weighted Fair Queueing
WRR	Weighted Round Robin
WWC	Wireless Wireline Convergence
ZR	Extended Reach (optics)
ZTP	Zero-Touch Provisioning

Copyright © 2021 Telecom Infra Project, Inc.

Copyright © 2021 Telecom Infra Project, Inc. A TIP Participant, as that term is defined in TIP's Bylaws, may make copies, distribute, display or publish this Specification solely as needed for the Participant to produce conformant implementations of the Specification, alone or in combination with its authorized partners. All other rights reserved.

The Telecom Infra Project logo is a trademark of Telecom Infra Project, Inc. (the "Project") in the United States or other countries and is registered in one or more countries. Removal of any of the notices or disclaimers contained in this document is strictly prohibited.