Modeling and Accomplishing the BEREC Network Neutrality Policy[†]

David S. Barreto[1] | Rafael F. Reale[1,2] | Joberto S. B. Martins*[1]

[1]PPGCOMP, Salvador University - UNIFACS, Bahia, Brazil

[2]Federal Institute of Education - IFBA, Bahia, Brazil

Correspondence
*Joberto S. B. Martins, Salvador University - UNIFACS. PPGCOMP, Campus CTN, Salvador, Bahia, Brazil
Email: joberto.martins@gmail.com

Abstract

Network neutrality (NN) is a principle of equal treatment of data in network infrastructures with fairness and universality being the primary outcomes of the NN management practice. For networks, the accomplishment of NN management practice is essential to deal with heterogeneous user requirements and the ever-increasing data traffic. Current tools and methods address the NN problem by detecting network neutrality violations and detecting traffic differentiation. This paper proposes the NN-PCM (Network Neutrality Policy Conformance Module) that deploys the BEREC network neutrality policy using a bandwidth allocation model (BAM). The NN-PCM new approach allocates bandwidth to network users and accomplishes the BEREC NN policy concomitantly. Network neutrality is achieved by grouping users with similar traffic requirements in classes and leveraging the bandwidth allocation model's characteristics. The conceptual analysis and simulation results indicate that NN-PCM allocates bandwidth to users and accomplishes BEREC network neutrality conformance *by design* with transparent, non-discriminatory, exceptional, and proportional management practices.

KEYWORDS:
Network Neutrality; BEREC, Network Neutrality Policy, Network Neutrality by Design; Bandwidth Allocation Model; OpenFlow.

1 | INTRODUCTION

Network neutrality (NN) is a principle of equal treatment of data moving across a network infrastructure. It is a network operation, administration, and management principle in which the traffic should not be discriminated based on its source, destination or content[1][2][3].

The current computer network evolution scenario includes networks such as IoT (Internet of Things), 5G and Cloud/-Fog/Edge computing with a wide variety of services, applications, billions of users, and ever-increasing data traffic. Corporate networks, Internet Service Providers (ISPs), and Content Providers (CPs) play a crucial role in conveying data worldwide. For all these networks, the NN modeling and deployment is a challenging task not yet adequately addressed by the research community due to its heterogeneous traffic characteristics and the complexity of these network ecosystems[4][5].

Many regulatory authorities around the world assumed the task of defending fairness and universality principles for computer networks such as the Internet[6]. These regulatory instances created rules or offered guidelines for traffic discrimination towards network neutrality[7][8][9]. In general, these rules limit the ability of networks to interfere with applications, content, and services, prohibiting undue discriminatory Internet Traffic Management (ITM), also referred to as unreasonable network management for networks in general[10][7]. NN regulatory norms and guidelines were issued and implemented

---

[†]BEREC - Body of European Regulators for Electronic Communications.

at the national level by the USA[8], the European Community(BEREC[1])[7], and Asian and Brazilian regulatory institutions[9][11].

In 2020, network neutrality gains a new push due to the pandemic situation around the world. In effect, the sudden increase of Internet usage by citizens locked in their homes and the need for communication quality and minimum bandwidth allocation assurance points to the need to regulate the Internet and have a neutral, even, and balanced resource allocation policy for networks in general.

Although the regulation defining network neutrality principles and norms have existed and the network neutrality research has been active for a decade, NN tools and technical solutions deployed in networks are under-explored.

Most research efforts and tools available so far are focused on detecting NN violations and providing methods and techniques for traffic differentiation in networks[12]. In addition to that, NN research and discussion have strongly focused on regulatory issues, business models, and network traffic discrimination impact for users and providers[13][14].

In this paper, we propose the tool NN-PCM (Network Neutrality Policy Conformance Module). NN-PCM is a network neutrality policy conformance module based on a Bandwidth Allocation Model (BAM) that accomplishes the BEREC (Body of European Regulators for Electronic Communications) network neutrality non-discriminatory policy for networks.

NN-PCM approach is new in the sense that the BAM model and configuration used to separate network traffic in classes inherently guarantees the BEREC network neutrality non-discriminatory policy for networks. In brief, the modeling approach used to group network users in classes coupled with the leveraging of the BAM model characteristics results in accomplishing the BEREC network neutrality non-discriminatory policy for networks.

Unlike the approaches in current NN tools approaches, the NN-PCM does not detect NN violations or focuses on monitoring traffic differentiation. It directly enforces the NN BEREC policy based on its operation, and that is new and differentiates this solution from the current ones available. As such, it has a new outstanding characteristic that allows NN modeling and NN deployment *by design*[2]. To achieve such a goal, the NN-PCM leverages the characteristics of bandwidth allocation models (BAMs) and uses an SDN/OpenFlow-based architecture to program and control the network.

The organization of the paper is as follows. Section 2 presents an overview of the related works. Section 3 presents the NN-PCM motivation followed by sections 4 and 5 presenting BAM and BEREC basic concepts that serve as the primary background for the following discussion. Section 6 presents NN-PCM architecture, and section 7 develops the analytical formulation of the model and illustrates its configuration. Section 8 discusses the conformance to BEREC ITM requirements with the final considerations following in section 9.

2 | RELATED WORK

Network neutrality may be monitored and evaluated in the network in different ways. Garret[12] and Li[15] present an extensive survey of monitoring techniques and practices for traffic differentiation detection. These techniques can be used for the detection of traffic violations from the perspective of a user. They differ from the proposed NN-PCM solution that addresses the NN problem changing the perspective from the users to the network's side. NN-PCM addresses the NN principles and applies them to network operation and management. A NN solution based on traffic differentiation, as indicated by Garret[12], has enormous challenges to be deployed in networks.

Another way to treat NN in the network is to provide a technical solution or tool that, based on its operation, effectively deploys the defined NN policy. Wójcik[16] proposes a technical solution aligned with the former approach using a QoS architecture. According to the authors, the FAN (Flow-Aware Networking) assures implicit service differentiation based solely on the traffic characteristics without any possibility of undesirable interference by ISPs or Internet users. In this proposal, some control of routers is assumed by using QoS configurations that are not always easy to realize for most practical situations. The NN-PCM tool differs from this solution by deploying neutrality grouping users in classes and allocating bandwidth to them based on the BAM characteristics that, by its turn, result in a neutral operation.

Schewick[2] proposed recently eight possible network neutrality rules, but does not provide details about how these rules are modeled and implemented for networks. One of the proposed rules allows networks to treat classes of applications differently if they treat equally all traffic within each class. This specific rule is aligned with the NN-PCM model for network user grouping in traffic classes for NN conformance.

The works in Garret[12], Ravaiol[17] and Zhang[18] detect network neutrality violations through end-to-end measurements using various techniques like censorship, traffic differentiation and traffic modification. These approaches detect NN violations, but do not effectively deploy the NN police. This is fundamentally different from NN-PCM tool that implements the

---

[1]BEREC - http://berec.europa.eu/
[2]For the scope of this paper, NN, by design, means that the BAM characteristics inherently accomplish the network neutrality.

NN policy *by design* controlling the allocation of bandwidth for network users.

The work in Maltinsky[19] explores the security vulnerabilities of the network neutrality measurements and violations detection techniques as far as they expose certain types of traffic. The NN-PCM NN deployment by design offers an advantage in this respect as far as the traffic is not exposed to any tool.

Mayer[20] discusses the legitimacy of monitoring methods used by ISPs and suggests an open-source framework that explores a certain number of measurements and points out the need for transparency in how ISPs monitor and discriminate user traffic. The NN-PCM provides legitimacy and transparency by exposing and advertising the user's traffic class mapping used in the network. Therefore, the NN-PCM provides configuration visibility for monitoring and auditing purposes for all stakeholders and players involved. This is a fundamental NN-PCM advantage in terms of facilitating NN regulation.

The work in Sivaraman[21] is similar to NN-PCM. It is based on classes of traffic, and for each class, there is an allocated bandwidth. NN-PCM fundamentally differs from this work by allocating bandwidth dynamically on a per-demand basis, resulting from the inherent behavior of the bandwidth allocation model (BAM) used. In summary, the *by design* characteristics of NN-PCM allow a more flexible and dynamic configuration and operation for the network.

Most recently developed works on NN discuss market implications, social impacts, and regulatory issues like innovation, competition, acceptable forms of network management, price and service differentiation, and the importance of traffic management[22,23,24,25,26,13,10,27]. Although highly relevant from the societal point of view, these works also do not discuss or propose any technical solution or tool to handle the network traffic and to provide neutrality.

To the best of our knowledge, there is not yet a proposed solution that models user's traffic and accomplishes the BEREC network neutrality policy in a transparent, non-discriminatory, exceptional, and proportional way.

3 | MOTIVATION

The primary motivation of the NN-PCM is to fill an existing gap and lack of tools for deploying the BEREC network neutrality policy in networks.

NN-PCM models and enforces BEREC NN. It does not focus on detecting violations or measuring traffic characteristics, and, in effect, it deploys the NN policy while granting bandwidth for network users. These characteristics go beyond the currently available type of tools that have been extensively explored in the domain, and that simply detect NN violations without providing a solution, as to enforce network neutrality rules to accomplish network neutrality.

NN-PCM can be used by corporate networks, ISPs, and Content Providers. It is a tool that groups network users in traffic classes and deploys the network neutrality business model based on the inherent behavior of the bandwidth allocation model (BAM).

Bandwidth allocation models are used to implement the NN-PCM. Therefore, two main questions must be discussed initially:

- How bandwidth allocation models work; and

- How BAM models characteristics are used to implement the NN-PCM and to achieve NN.

These issues are considered in the following sections.

4 | BANDWIDTH ALLOCATION MODELS - SUMMARY

Bandwidth allocation models define a resource allocation and resource sharing method. Reale[28,29] discusses BAM operation, and Figure 1 summarizes all the allocation sharing methods that are possible. With BAM, bandwidth can be private or can be shared between high and low priority users in both directions (LTH - Low to High and HTL - High to Low sharing), depending on the BAM model used.
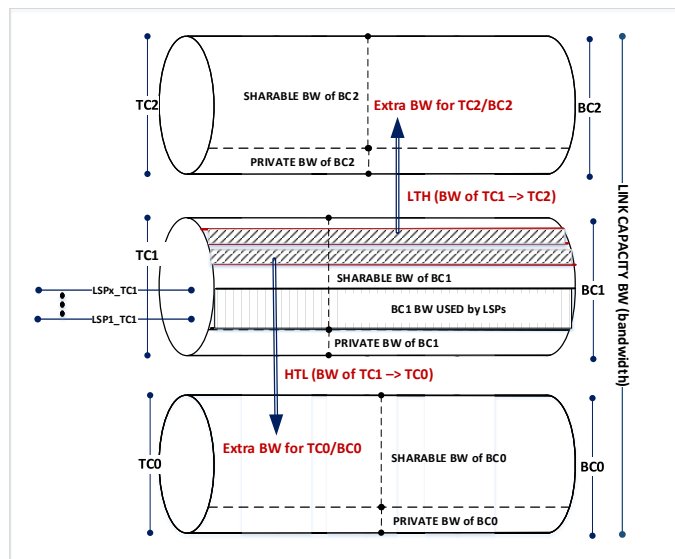

FIGURE 1 BAM generalized bandwidth allocation and sharing methods[29]

The most basic BAM models (MAM - Maximum Allocation Model[30] and RDM - Russian Dolls Model[31]) are resource sharing theoretical models described by RFCs (Request for Comments) that define how to share and to enforce different bandwidth constraints for different classes of traffic aiming traffic engineering. More recently, hybrids of the basic models were proposed[32][33]. The ATCS model (AllocTC-Sharing)[34] is a new basic BAM model that allows resource sharing among all traffic classes and the GBAM model[28] (Generalized BAM) generalizes the deployment of all possible resource sharing strategies for all existing BAM models.

BAMs are deployed nowadays in domains like link bandwidth sharing[35][36], last mile networks[37], 5G networks with virtual network embedding[38] and fiber optic networks[39][40].

BAM is mostly applied to networks in which resources such as link bandwidth and fiber optic slots (lambda circuits) are limited. In this paper, BAMs are used to allocated bandwidth[3] to users in network links.

BAM operation requires 3 main configuration steps (Figure 1)[28][29]:

- The grouping of applications into traffic classes (TCs) with similar network requirements;

- The configuration of the maximum amount of bandwidth (resource) per traffic class (Bandwidth Constraints - BC); and

- The definition of the strategy for bandwidth (resource) sharing among traffic classes (TCs) such as private, LTH (Low-To-High), and HTL (High-To-Low) sharing[29].

There are 3 basic BAM models, described in Reale[28][34] and Neto[33]:

- Maximum Allocation Model (MAM)[30];

- Russian Dolls Model (RDM)[31]; and

- AllocTC-Sharing (ATCS)[34].

Maximum Allocation Model (MAM) allocates bandwidth without any bandwidth sharing between traffic classes (TCs). In summary, MAM traffic classes have exclusive use of their bandwidth resources (BCs).

In the Russian Dolls Model (RDM), it is possible to share bandwidth not used by high priority classes. As such, low priority classes may have access to extra bandwidth in addition to their bandwidth resources (Figure 1) (HTL - High to Low sharing).

Finally, the AllocTC-Sharing model (ATCS) generalizes bandwidth sharing among all classes (low and high priority). In

this case, all unused bandwidth might be shared among classes independently of their priority (Figure 1) (HTL - High to Low and LTH - Low to High sharing).

The ATCS model is adopted in the NN-PCM since it includes and reproduces the operation of all BAM basic models (MAM and RDM) and supports a broader scope of applications[41].

5 | THE BEREC REASONABLE INTERNET TRAFFIC MANAGEMENT

BEREC (Body of European Regulators for Electronic Communication) is the European body that brings together all national regulatory authorities (NRAs) and explores such issues as transparency, competition, quality of service, quality monitoring, and IP interconnection in the context of network neutrality[42].

As discussed in BEREC[7], the BEREC reasonable Internet Traffic Management (ITM) is an acceptable practice that can be used by networks to implement non-discriminatory rules and policies. The so-called reasonable-ITM-exception is discussed in regulatory documents[7][8][9] and studies[22][43][2]. In summary, it is a fair and justifiable deviation from the strict NN non-discrimination rule, where all traffic is absolutely equal in terms of network requirements[44][10].

The reasonable ITM is a concept proposed by Europeans through BEREC[43]. There is a long-term discussion on what network neutrality concept should be used for all actors involved that we consider as out of the scope of this paper. Indeed, we consider BEREC ITM proposal a valid reference for network neutrality based on two main reasons:

- The agnostic approach inherently embedded in the BEREC ITM does not significantly differ from concepts supported by other regulatory institutions; and

- BEREC proposal is based on objective technical requirements[43].

In terms of network neutrality deployment, ITM adopts technical practices and management approaches whose purpose is to maintain, protect, and ensure an efficient network operation[2]. Efficient operation means that the NN solution must take into account that different applications might have different and conflicting network requirements. NN ITM exception considers it acceptable to adopt management practices that deal with different application requirements.

Necessarily, to qualify a management practice as conforming to ITM, it must meet the following requirements[7][45]:

1. Have a legitimate network management purpose;

2. Be transparent;

---

[3]The term **bandwidth**, for the scope of this paper, will mean the **capacity** or **transmission rate** allocated to a user in a link.

3. Be non-discriminatory;

4. Be proportional; and

5. Be exceptional.

The NN-PCM prototype architecture, configuration, and operation that lead to the conformance with these ITM requirements are presented and evaluated next.

6 | THE NN-PCM ARCHITECTURE MODEL

The NN-PCM (Network Neutrality Policy Conformance Module) objective is dual fold:

- To manage the allocation to users of link bandwidth in the network using a bandwidth allocation model (BAM); and

- To accomplish the BEREC Reasonable Internet Traffic Management (ITM) concomitantly.

The main components and interfaces of the NN-PCM prototype architecture is illustrated in Figure 2. They are the NN-PCM module, the controlled network, users generating traffic flows, and a set of interfaces for the network manager and monitoring and controlling the target network. The NN-PCM adopts a centralized network control operation using the OpenFlow protocol under the Software-defined Network (SDN) paradigm[46].

The NN-PCM interacts with the controlled network using two basic functionalities:

- $M()$ for monitoring the network concerning new incoming flows; and

- $C()$ to control the network by programming flows deployment over the set of switches (Figure 2).

The NN-PCM configuration (Figure 2) is another basic element of the NN-PCM architecture. It is the configuration interface that allows the definition of the adopted BAM, its configuration and the grouping of network users in classes of traffic according to their network requirements.

The main blocks and components of the NN-PCM module are illustrated in Figure 3. It is composed by:

- The BAM-broker module;

- The monitoring interface;

- The network control module (NCM); and
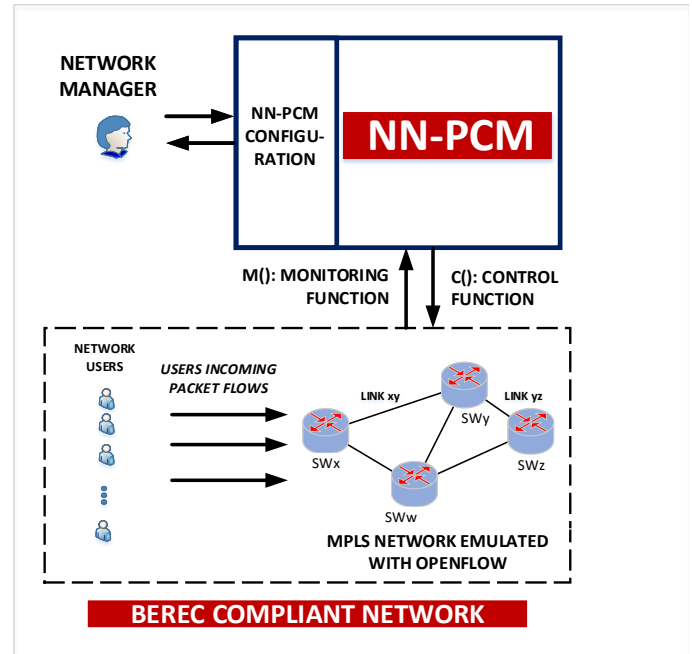
- An interface to allow NN-PCM configuration.

FIGURE 2 NN-PCM architecture main components and interfaces

The BAM module acts as a bandwidth broker and assures the fair and neutral network operation while allocating bandwidth to flows generated by the users. Even when the input traffic fluctuates and bandwidth resources are exhausted, the BAM dynamic behavior allows a neutral distribution of bandwidth under the BEREC policy.

The network monitoring interface (NMI) is responsible for catching and forwarding to the BAM-broker the new bandwidth requests for the new incoming flows in the network. The new input flow is detected by the OpenFlow switches when a packet arrives in the switch, and there is no defined entry for that flow in its flow-table. When this happens, a *PacketIn* OpenFlow message is sent to the NN-PCM that acts as an SDN/OpenFlow network controller.

The network control module (NCM) is the interface through with OpenFlow commands are sent to the network to configure, program, and manage flows in the switch's flow-tables.

The BAM database stores all information concerning the currently configured flows in the network for all users, switches, and paths. It is used by BAM operation to decide on the allocation of bandwidth to new incoming flows in the network.

The internal operation of the OpenFlow switch in the network is monitored and controlled, as illustrated in Figure 4. New flows not yet configured in the switch flow-table generate a *PacketIn* message that is sent to the NN-PCM. A new end-to-end flow (source to destination) is then created for the network
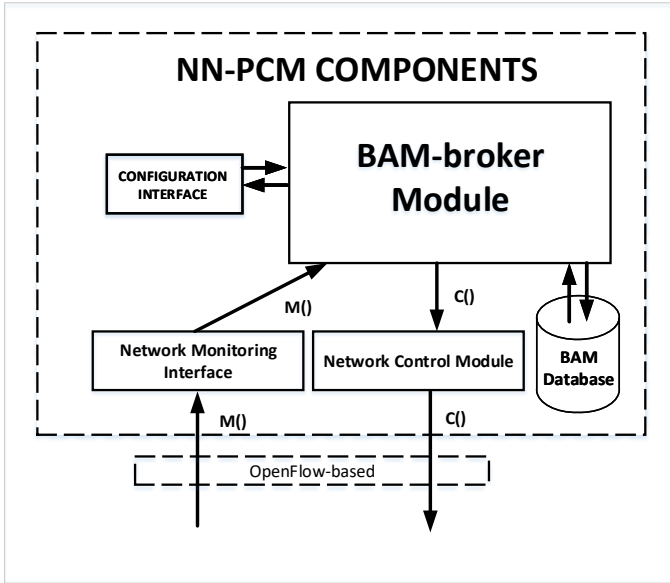
FIGURE 3 The NN-PCM module main blocks and components

by configuring a new flow entry at the flow-table for all the switches in the flow path.
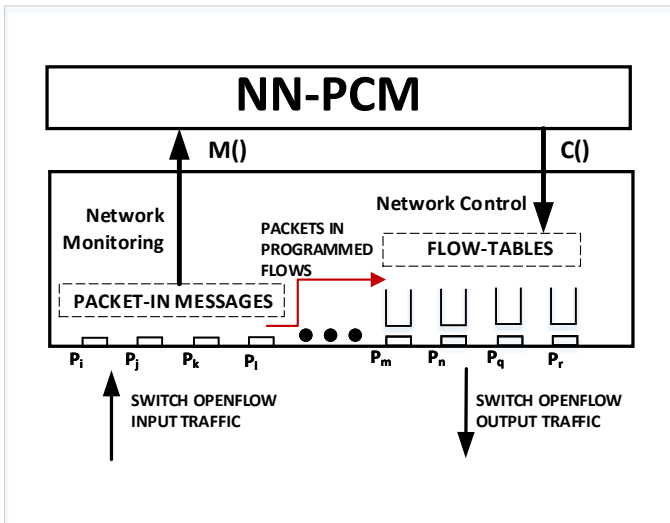

FIGURE 4 OpenFlow switch monitoring and control

The OpenFlow-based centralized monitoring and control of the network allow the NN-PCM to inherit the advantages of an SDN-based deployment. The centralized monitoring and control include a single view of the entire network and the capability to dynamically configure any switch in the network according to the current traffic profile.

The NN-PCM architecture also solves another essential problem present in network neutrality management deployments that is where to place the management control. In NN-PCM, the NN management is effectively positioned at the incoming traffic switch for all switches in the network (Figure 5) (Equation 3). This is achieved by the basic OpenFlow monitoring and programming operation. NN-PCM requires new flow identification, done by the OpenFlow input traffic switches. OpenFlow switch programming includes LSP flows being programmed in terms of bandwidth and queues, and NN-PCM does this for all switches in the LSP path[47].
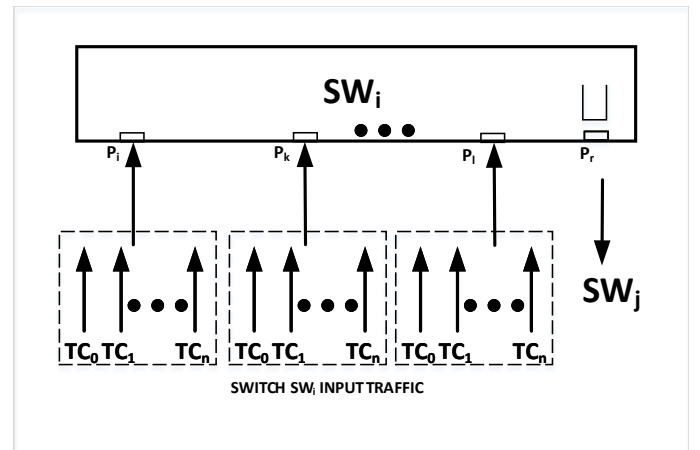

FIGURE 5 BAM operation by switch and by link

The NN-PCM architecture is the base for the analytical NN-PCM description and the BAM behavior simulation analysis discussed in the following sections.

The next question concerning the NN-PCM is how applying the BAM operation to a set of flows and traffic classes in a network conforms (or not) to the BEREC network neutrality policy. This issue is addressed in the following section.

7 | ACCOMPLISHING CONFORMANCE TO BEREC ITM POLICY WITH THE BAM

The fundamental conception premise of the NN-PCM is that the BAM operation does accomplish conformance to the NN BEREC ITM requirements defined in BEREC[7]. Concerning the ITM requirements, this means that:

1. The BAM operation has a **legitimate network management purpose**;

2. Its configuration and operation is **transparent**;

3. It has a **non-discriminatory** behavior concerning network users;

4. It has a **proportional** behavior; and

5. It adopts an **exceptional** behavior when it is acceptably required.

This ITM compliant behavior is evaluated in the next sections but, firstly, we introduce the basic design neutrality principle adopted by the NN-PCM, present an analytical formulation of the BAM operation and illustrate the configuration of NN-PCM operation.

7.1 | NN-PCM Neutrality Model

The general principles used to model a neutral network operation with the NN-PCM are the following:

- The BAM model operation accomplishes a per-link neutral bandwidth allocation; and

- Users with equivalent network requirements are grouped into the same traffic classes (TCs) and are subject to non-discriminatory management.

In addition to the above principles, the following definitions hold for the NN-PCM operation:

- The BAM model manages each link (attached to a switch port) in the physical network independently (Figure 5);

- A network path (LSP from source to destination) is composed of various links. The BAM manages the network path by managing the set of links belonging to the path independently (Equation 3); and

- Accomplishing link neutrality implies accomplishing path neutrality by having the BAM model managing all links belonging to the path independently.

7.2 | NN-PCM BAM Analytical Formulation

The BAM solves effectively a traffic engineering problem and, in the NN-PCM implementation, it is as a centralized controller operating according the SDN paradigm with the OpenFlow protocol.

The network infrastructure is modeled as a bidirectional physical graph $\aleph^q = (SW^q, L^q)$, where $SW^q = \{sw_1, sw_2, sw_3, ..., sw_n\}$ is the set of OpenFlow switches in the target network q and $L^q = \{l_{ij}\}$, with i and $j = 1, 2, 3, ..., n$, is the set of physical links, with link l_{ij} connecting sw_i to sw_j.

The switch connectivity matrix (SCM) is defined by $C = [c_{ij}]$ with i and $j = 1, 2, 3, ..., n$, and $c_{ij} = 1$ if sw_i is connected to sw_j; 0 otherwise and $c_{ii} = 0 \ \forall i$ by definition.

The link bandwidth matrix (LBM) for the physical network is defined by $LB = [LB_{ij}]$ with i and $j = 1, 2, 3, ..., n$, where

LB_{ij} is the total bandwidth of the link l_{ij} managed by the BAM to allocate all incoming traffic arriving at sw_i to sw_j.

The BAM model defines for each link l_{ij} a set of traffic classes (TC^k), with $k = 0, 1, ..., n$. Each traffic classes TC_{ij}^k belonging to the link l_{ij} has a bandwidth BC^k (Bandwidth Constraint), such that:

$$LB_{ij} \geq \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=1}^{n} BC_{ij}^k \qquad (1)$$

In the BAM operation by switch and by link, $T_{ij} TC^k P_{sw_i}^z$ is the incoming traffic at port z, with $z = 1, 2, .., n$, of sw_i, belonging to traffic class TC^k, with $k = 0, 1, ..., n$, whose destination is sw_j through link l_{ij} (Figure 5).

The traffic class (TC) used bandwidth (TCUB) matrix is defined by $TCUB = [TC^k UB_{ij}]$, with $k = 0, 1, ..., n$, and i and $j = 1, 2, .., n$.

The bandwidth constraint for the traffic classes is:

$$TC^k UB_{ij} \leq BC_{ij}^k \forall k, i, j \qquad (2)$$

A LSP is defined as set of Z 2-switch directed graph $\aleph^Z = (SW^Z, L^Z)$, $Z = 1, 2, ..., z$, where $SW^Z = \{sw_s^z, sw_d^z\}$ are the source and destination switches on the zth LSP section and $L^Z = \{l_{sd}^z\}$ is the link connecting source to destination switches on the zth LSP section with bandwidth allocated $BA_{U_x} TC_{sd}^k LSP_m$ for each link.

For the sake of simplicity to reduce simulation complexity, the LSP path computation is made available to NN-PCM by the LSP connectivity path (LSP_{CP}) matrix:

$$LSP_{CP} = [\sum_{\alpha=1}^{n} \overbrace{(LSP_{seg_{mn}} \parallel \cdots \parallel (LSP_{seg_{yz}})}^{\alpha}] \qquad (3)$$

The LSP has source switch sw_m and destination switch sw_z and is composed by concatenated segments with interconnected switches and links on the path as follows:

$$LSP_{seg_{xy}} = (sw_x, sw_y, l_{xy}) \qquad (4)$$

Computing the LSP path for multiple incoming traffic is a complex traffic engineering optimization problem that has no impact on the evaluation of the network neutrality conformance.

The bandwidth allocated $BA_{U_x} TC_{sd}^k LSP_m$ for the LSP segments $LSP_{seg_{xy}} = (sw_x, sw_y, l_{xy})$ has a fixed value for a given traffic class. This approach is consistent with the principle that users with similar bandwidth requirements are mapped to the same traffic class and have a non-discriminatory treatment.

7.3 | ATCS Model Analytical Formulation

The AllocTC-Sharing (ATCS) model used in the NN-PCM has additional capabilities concerning a basic BAM model:

- Traffic classes (TCs) have a priority; and

- Bandwidth sharing is allowed between all traffic classes, and the amount of bandwidth shared is limited.

The ATCS traffic class priority for all links l_{ij} with $i, j = 1, 2, ..., n$ is:

$$TC_p^0 > TC_p^1 > TC_p^2 > \cdots > TC_p^n \qquad (5)$$

In the BAM convention, traffic class 0 priority (TC_p^0) has the highest value, and traffic class n priority (TC_p^n) the lowest value.

The traffic class priority, as described in Reale[34], is used by the ATCS to:

- Allocate unused bandwidth from other traffic classes; and

- Preempt or return shared bandwidth previously allocated from other traffic classes.

ATCS policy allows each traffic class TC^k to have two bandwidth partitions: private and public. The private bandwidth is exclusively allocated for TC^k users, and the public bandwidth may be allocated by other traffic classes when not used by TC^k users. As such for all l_{ij} with $i, j = 1, 2, ..., n$:

$$TC^k B_{ij} = TC_{pri}^k B_{ij} + TC_{pub}^k B_{ij} \qquad (6)$$

The traffic class used bandwidth (TCUB) matrix for ATCS must then be rewritten as follows for all l_{ij} with $i, j = 1, 2, ..., n$:

$$TC^k UB_{ij} = [TC_{pri}^k UB_{ij} + TC_{pub}^k UB_{ij} \\ + \sum_{z=1}^{n} TC_{pub}^k UB_{ij}] \forall z \neq k \qquad (7)$$

Equation 7 describes the ATCS behavior. ATCS model can allocate unused public bandwidth from other traffic classes. ATCS loan bandwidth from other traffic classes considering the available public bandwidth from the lower to the highest priority TCs.

Users are mapped to traffic classes $\sum_{k=1}^{n} TC^k$ (Figure 6). As such, for all links l_{ij} with $i, j = 1, 2, ..., n$, TC^k has a set of users $\sum_{1=1}^{n} U^i$.

In the NN-PCM current evaluation, each U^i may have any number of LSPs over the network. The limit of LSP setup is only limited by the amount of private and public bandwidth by class and by link.

In summary, for each traffic class TC^k, there is a User LSP matrix (ULSP) with LSPs (Equation 3) conveying user application traffic from source switch sw_s to destination destination sw_d (Figure 6):

$$ULSP = [\sum_{y=1}^{m} U^y \sum_{x=1}^{n} LSP^x] \forall TC^k, k = 0, 1, \ldots, n. \qquad (8)$$
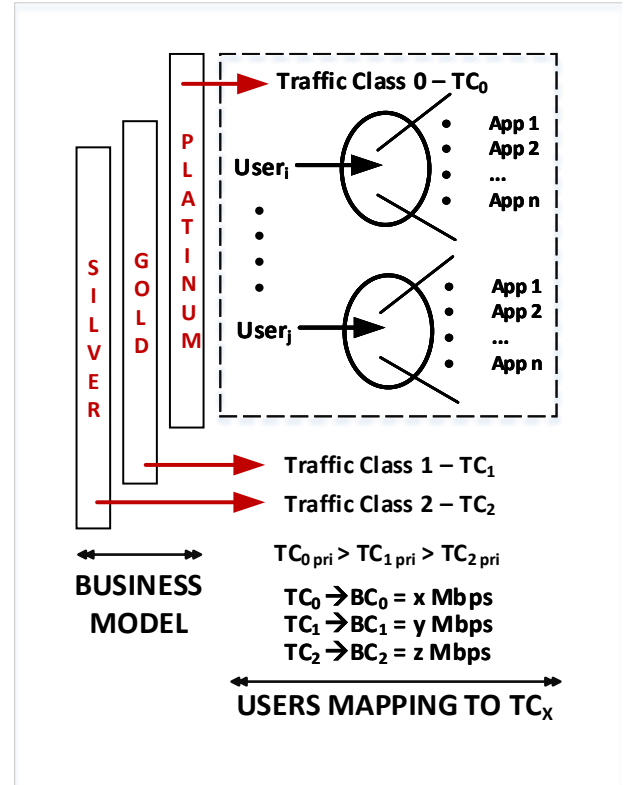

FIGURE 6 NN-PCM network neutrality model and BAM configuration

7.4 | NN-PCM Configuration

The NN-PCM is configured by mapping network users, services, and applications, from now on, generically referred as **users**, into a set of BAM traffic classes (TCs) (Figure 6).

There are various alternatives to map users to traffic class and this mapping strongly depends on the business model adopted by the network owner. Just as an illustration, Figure 6 shows 3 TCs (platinum, gold, and silver) where platinum has the highest and silver has the lowest priority (Equation 5).

From the network neutrality perspective, to group users into classes allows:

- To have users with equivalent bandwidth requirements in the same class; and

- To have users with either distinct bandwidth requirements or distinct priorities in different classes.

From the network manager perspective, the mapping of users into traffic classes (TCs), has to consider two essential aspects:

- The user bandwidth requirement for the application or service execution; and

- The network policy ruling its business, managerial practices, and legal constraints.

As another example to illustrate users mapping alternatives, certain users need guaranteed minimum bandwidth, while others do not. Besides, some users take advantage of additional bandwidth, if available, to improve its user experience. These criteria are used by the network manager to map users with similar requirements in the same class.

It is relevant to indicate that the mapping of users on a traffic class (TC) does not guarantee bandwidth for all TC users. Network resources are, in most real cases, scarce and disputed. The NN-PCM supports bandwidth disputes under congestion, with the BAM model assuring that the NN principle is preserved.

The NN-PCM configuration can be summarized as follows:

- Map users with similar network requirements on a set of traffic classes (TCs);

- Configure the available bandwidth per class (bandwidth constraints) for each TCs; and

- Choose the BAM model (MAM, RDM, ATCS, other) that defines the behavior for bandwidth sharing among TCs.

In practice, there are various possibilities to group users into TCs and configure the TCs bandwidth (BCs). The evaluation of these alternatives is out of the scope of this paper.

Table 1 illustrates one of many possible users grouping into classes. This grouping is based on the association of QoS classes as proposed in ITU-T Recommendation Y.1541 and the transfer capabilities requirements extracted from ITU-T Recommendation Y.1221 [48] [49].

8 | BAM CONFORMANCE TO ITM REQUIREMENTS - DISCUSSION AND PROOF-OF-CONCEPT

In this section, we demonstrate how the NN-PCM operating with a BAM model does conform to the 5 previously defined criteria for BEREC reasonable Internet Traffic Management (ITM).

As presented in Reale [28], the BAM models have two types of behavior [4]:

- BAM general behavior; and

- BAM specific behavior.

The general behavior corresponds to the set of BAM operational characteristics that are valid for all BAM models. The specific BAM behavior, as the name suggests, corresponds to the individual operational characteristics of each BAM model.

As an example, MAM and RDM have specific behaviors, since MAM does not share resources while RDM does.

In summary, the general BAM behavior certifies conformance to ITM requirements 1, 2, 3, and the specific BAM behaviors certify conformance to ITM requirements 4 and 5.

The conformance to ITM requirements 1, 2, 3 is based on the interpretation of the ITM requirements in relation to the general behavior of BAM models. The conformance to ITM requirements 4 and 5 depends on the evaluation of BAM specific behavior by simulation. As such, we first present the simulation scenario used, followed by the conformance analysis to all ITM requirements.

An inference generalization holds for the NN-PCM ITM conformance evaluation. In effect, it is necessary to evaluate the ITM conformance just for one network link. That is so because the BAM model manages bandwidth allocation for all links of the network independently. In a network with N links, N independent BAM instances manage the available resources, one for each link. This means that the same general and specific behaviors exist for all links in the network if the same BAM model is configured for all links.

Based then on the premises that the BAM control links independently and the same BAM model is used for all links of the network, the simulation, and verification of the NN-PCM ITM conformance for any link of the network, leads to the conclusion that it conforms for all links and conform for any path of the network. Consequently, the NN-PCM is ITM conform for the entire network.

8.1 | Simulation Network for BAM Behavior Analysis

The simulated network is an MPLS (MultiProtocol Label Switching) network in which users request circuits (LSP - Label Switched Path) passing through network links (Figure 7). The requested resource in all links over the LSP path is the bandwidth required by the requested LSP. The requested LSP belongs to a user, configured by the manager in a traffic class (TC0, TC1 or TC2).

From the user (external) point of view, the NN-PCM acts as a broker that emulates an MPLS network. That means, in summary, that users get an LSP that is fully emulated by the NN-PCM through its SDN/OpenFlow-based control functions ($M()$ and $C()$) (Figure 3) with no need to use MPLS signaling protocols.

The basic simulation definitions are:

- The simulator used is the BAMSim (BAM Simulator) [28]; and

- NN-PCM uses the AllocTC-Sharing (ATCS) BAM model [34].

---

[4] The BAM behavior is the set of characteristics that the BAM model has when it allocates bandwidth for users

TABLE 1 Example of Users to Traffic Class (TC) Mapping

USERS	TC	TRAFFIC
Medical images, virtual reality, emergency, ...	TC0	Critical and emergency
Audio/video, real-time applications, ...	TC1	Real time; bandwidth intensive
Web applications, browsing, file transfer, ...	TC2	Best effort; non real-time

BAMSim has features to simulate various BAM behaviors using the NSF (National Science Foundation) benchmark topology with 14 nodes and 42 bidirectional links. For the scope of NN-PCM specific ITM conformance evaluation, the link 0-1 is considered (Figure 7).

The simulation runs use two network traffic scenarios.

- The first scenario uses random input traffic requesting LSPs and evaluates whether the NN-PCM achieves a non-discriminatory resource distribution in a proportional way (ITM requirement 4).

- The second scenario uses a previously established (non-random) input traffic profile to test whether the NN-PCM operation is exceptional (ITM requirement 5).

The simulation configuration parameters are:

- The network link simulated (Figure 7) has a total bandwidth of 1000 Mbps between nodes 0 and 1 of the topology;

- Sharing limit: 100% of BC; and

- 3 Traffic Classes: TC0 with BC0 = 25%, TC1 with BC1 = 35% and TC2 with BC2 = 40% of the total link bandwidth.

The simulation (scenarios 1 and 2) runs for 5 hours with 5 phases of 1 hour. Other simulation parameters are:

- LSP bandwidth randomly distributed between 5 and 15 Mbps;

- Interval of LSP arrival requests modeled exponentially;

- Exponentially modeled LSP time life - average of 300 seconds; and

- Halting criteria - 5 hours.

8.2 | ITM Requirement 1 Conformance Accomplishment - Legitimate Management Purpose

ITM requirement 1 defines that the network management practice must have a **legitimate network management purpose**.
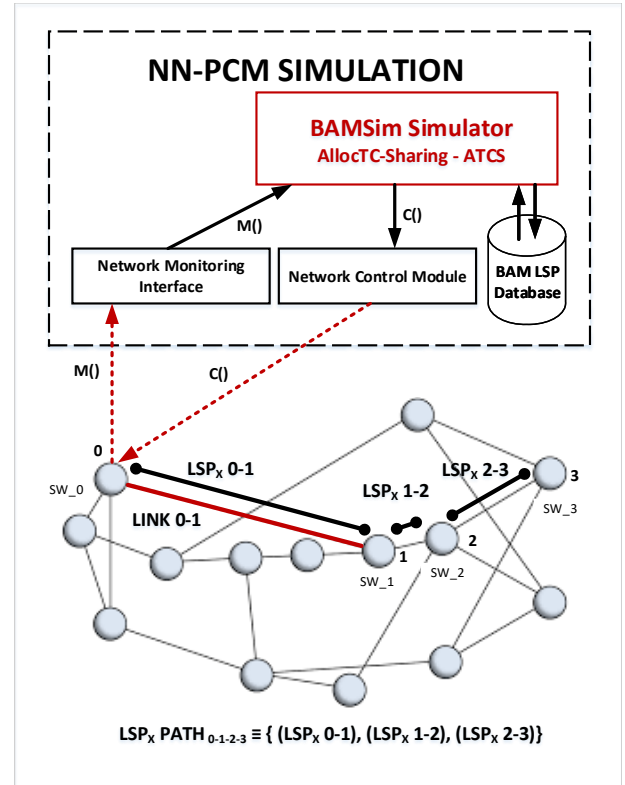
FIGURE 7 NN-PCM simulation set-up

By legitimate network management purpose, it is meant that the applied management has to be designed to maintain, protect, and ensure an efficient network operation.

The NN-PCM, being based on any BAM, is conform to ITM requirement 1 due to the BAM's general behavior. The BAM's general behavior has a legitimate network management purpose because it maintains and protect bandwidth for traffic classes (TCs) and, also, allows efficient use of the available bandwidth, responding to different technical requirements of specific categories of traffic configured in different traffic classes (TCs)[41].

In summary, each TC has its bandwidth maintained, protected from other external users, and, in exceptional circumstances, it is allowed bandwidth sharing leading to efficient network operation[41].

8.3 | ITM Requirement 2 Conformance Accomplishment - Transparency

The ITM requirement 2 defines that traffic management measures should be transparently included in the contract and published with a clear and comprehensive explanation of traffic management measures applied.

The ITM **transparency** requirement is accomplished by publishing or making public the NN-PCM configuration parameters. This, in practice, corresponds to the network neutrality policy implementation being defined for the target network by the manager. Various NN configuration parameters that can be made public and transparent, such as:

- The number of traffic classes (TCs), the mapping of users, the bandwidth available per traffic class, and the limit for bandwidth sharing.

This information can be made transparent for users, stakeholders, partners, and regulators.

8.4 | ITM Requirement 3 Conformance Accomplishment - Non-discriminatory

ITM requirement 3 defines that the network management practice adopted has to be non-discriminatory concerning users. As discussed in Belli[43] and Schewick[2], non-discriminatory means basically that the management practice is application-agnostic. As stated in Schewick[2], "the management practice may have information about the application but does not make any distinction among data packets based on this information ". Likewise, the ITM concept establishes that traffic and users may be grouped into categories that should reflect their technical requirements[7][43].

In the NN-PCM, users with similar network requirements receive similar treatment. In other words, users with similar requirements are handled agnostically in the same traffic class (application-agnostic operation). Likewise, users with distinct network requirements are handled by distinct traffic classes (TCs).

As such, the operation of the NN-PCM for all possible BAM models is non-discriminatory. It is non-discriminatory because it always grants (or not) bandwidth for a group of users organized into classes with common or similar requirements. This assertive is discussed and reinforced again in the following sections when simulating the operation of the NN-PCM with a specific BAM model (AllocTC-Sharing - ATCS[34]).

8.5 | ITM Requirement 4 Conformance Accomplishment - Proportionality

The ITM proportionality requirement defines that we should have pieces of evidence that the network management practice

reaches its defined purpose, and the actions must be necessary to reach the purpose, interfering as less as possible[7].

As a practical example in the context of the NN-PCM, ITM proportionality requires that blocking, preemption, and devolution events must be proportional, that is, should not occur more than necessary to reach the purpose of allocating bandwidth to users according to their requirements as well to optimize network performance.

An ITM management practice is considered proportional when there is no less interfering and equally effective alternative to manage user's demand with the available network resources[7].

In the FRFS bandwidth allocation management practice, users share the link bandwidth without any class grouping or priorities with no interference at all among them. FRFS is the best possible approach in terms of non-interfering criteria.

Based on the above ITM proportionality definition, we evaluated the NN-PCM proportionality conformance comparing the NN-PCM with the FRFS method as follows:

- NN-PCM allocates bandwidth using AllocTC-Sharing BAM (ATCS) using simulation scenario 1; and

- The First-Requested First-Served (FRFS) allocates bandwidth using the same simulation scenario 1 for comparison.

The ITM proportionality requirement is evaluated using two network performance parameters: i) link utilization; and ii) blocking rate. The simulation results for these parameters are presented in Table 2.

Table 2 shows that the NN-PCM and the FRFS perform with equivalent efficiency in terms of link utilization. On the other hand, the NN-PCM performs better for TC1 and TC2 and worse for TC0. TC0 worse performance reflects the fact that it has the lowest priority among all classes in the NN-PCM class configuration mapping, and, due to that, higher priority classes TC1 and TC2 benefit from the ATCS sharing behavior. In conclusion, we verify that, as far as the utilization performance parameter is concerned, the NN-PCM is approximately equivalent to FRFS in terms of the proportionally ITM requirement.

The NN-PCM presents a much better result in terms of blocking users. This result shows that it enforces a proportional policy since it gets to the same network result (additional LSPs established and equivalent link utilization performance) interfering as less as possible with users.

TABLE 2 ITM Proportionality Simulation Results Summary - NN-PCM vs FRFS

PARAMETER	NN-PCM	FRFS
Utilization TC0	78,06%	86,94%
Utilization TC1	89,41%	87,01%
Utilization TC2	93,10%	86,92%
Mean utilization	86,86%	86,96%
Block rate TC0	8,72%	10,68%
Block rate TC1	4,75%	10,61%
Block rate TC2	3,36%	10,69%
Mean block rate	5,61%	10,66%

8.6 | ITM Requirement 5 Conformance Accomplishment - Exceptionality

The ITM exceptionality requirement defines that the management practice may temporarily and exceptionally throttle bandwidth-greedy users.

As an example, during congestion, bandwidth-greedy users can be exceptionally throttled. In the NN-PCM specific case, when congestion occurs, the traffic classes stop sharing bandwidth, and any previously shared bandwidth among classes is reclaimed back to its configured class.

The simulation results for evaluating the ITM exceptionality for traffic scenario 2 is presented in Figure 8. Let's first consider the NN-PCM behavior for all phases in sequence and then, identify the exceptional NN-PCM conformance.

Figure 8.a illustrates the link utilization during the operation of the NN-PCM for simulation scenario 2. In phase 1 (low bandwidth demand), the blocking rate is null since there is an excess of available bandwidth for the link, and ATCS model shares the not used bandwidth among all users. In phases 2 to 4 (medium bandwidth demand), there is a high demand for classes 0, 1, 2 alternatively. In these phases, LSP block rate is higher due to the high occupation of the link, and the sharing among class is less frequent. In phase 5 (high bandwidth demand for all class - near congestion), the block rate is high for all TCs. This is because bandwidth demand is higher than its availability for all classes. The sharing stops, and each class tends to use its resources (Figure 8.b).

LSP preemption and devolution rates have similar behavior, as illustrated in Figures 8.c and 8.d.

The exposed NN-PCM behavior for the link allows us to conclude that the trigger for applying the differentiated treatment among users is the occurrence of congestion, i. e., the LSP block, preemption, and devolution events occur only when bandwidth demand is beyond class or link availability. As such,

the NN-PCM using the ATCS BAM assures not only an exceptional but also a temporary management practice, as required by ITM exceptionality.

During congestion, the NN-PCM has a non-discriminatory behavior. That is so because, during congestion, each class uses its predefined resources, and there is no discrimination among users belonging to the same class.

8.7 | NN-PCM Network Neutrality with ATCS - Results Summary

In summary, the simulation results indicate as a proof-of-concept that the NN-PCM operation with ATCS accomplishes conformance by design to the BEREC network neutrality requirements, which are legitimate network management purpose, transparency, non-discrimination behavior, proportional behavior, and exceptional behavior.

Network neutrality is enforced inherently by the NN-PCM operation, with the network bandwidth being allocated to users grouped into traffic classes. The ATCS BAM model used in the NN-PCM manages the bandwidth allocation operation and the bandwidth sharing when traffic class resources become exhausted.

8.8 | ITM Requirement Conformance Accomplishing for Other BAM Models

There are 3 basic BAM models (MAM, RDM, and ATCS) and several hybrids[28]. This leads to the following question: Does the NN-PCM conformance result obtained for the ATCS model holds for other BAM models?

The non-discriminatory behavior (ITM requirement 3) of the NN-PCM holds for all models, as previously demonstrated (Section 8.4).

The NN-PCM conformance to exceptionality requirement using other BAM model than ATCS can be intuitively derived from previous ATCS simulation results. In effect, if the BAM
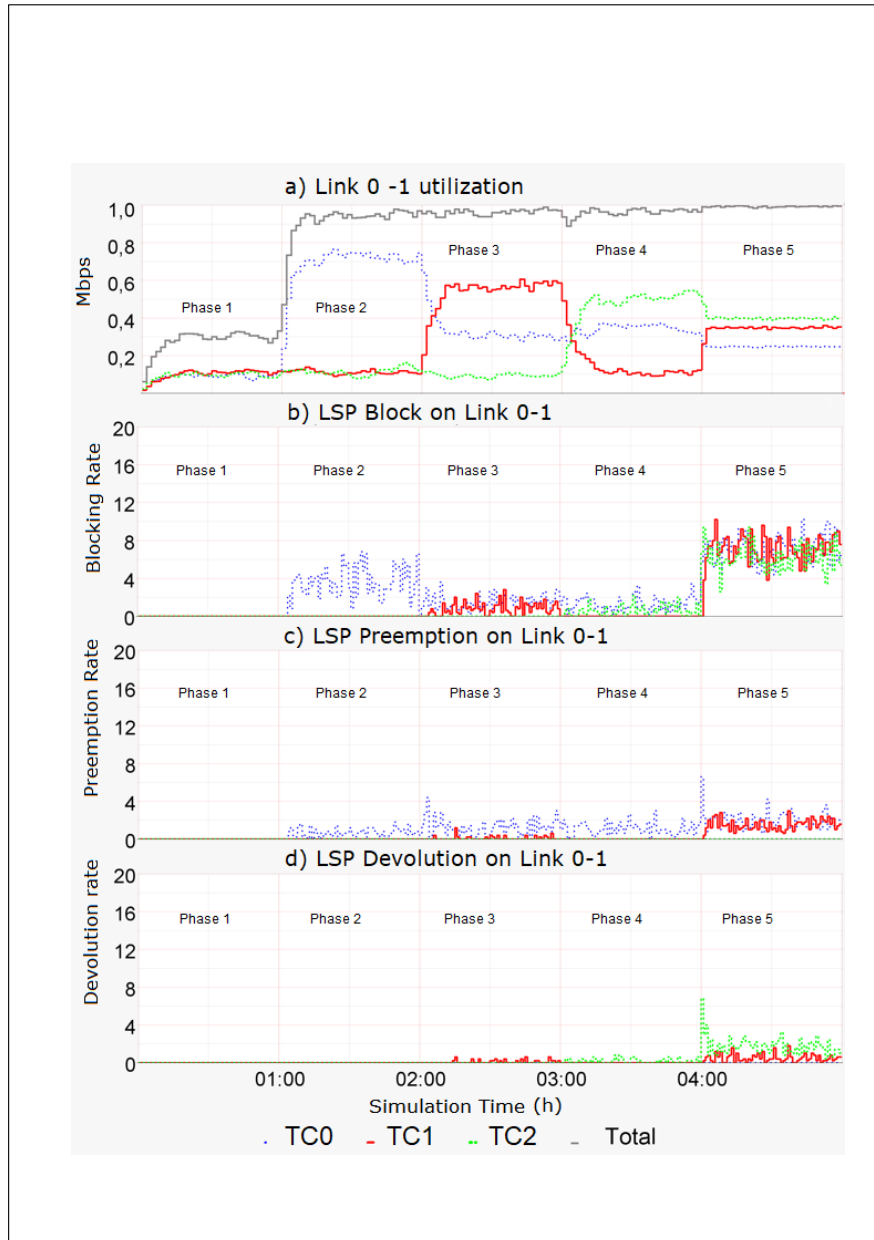
FIGURE 8 NN-PCM simulation with ATCS - Scenario 2 - ITM Exceptionality Conformance accomplishment

model shares bandwidth, independently of the style and volume of bandwidth shared, it only blocks, preempts, or return resources when bandwidth demand is beyond class or link availability. Consequently, BAM behavior assures an exceptional and temporary management practice. The MAM model is a specific case in which there is no bandwidth sharing at all. In this case, there is no provision for exceptional or temporary practices, and users only dispute the available bandwidth per class.

The conformance with the proportionality requirement for other BAM models follows the same line of reasoning. In effect, bandwidth sharing results in outperforming the FRFS

bandwidth allocation method. Consequently, other BAM models using distinct bandwidth sharing approaches do conform to proportionally ITM requirement. The MAM model without any sharing behavior is nearly equivalent to FRFS in terms of resource grant. In this case, eventual advantages or disadvantages concerning FRFS depend on the traffic input pattern, and, as such, we cannot guarantee that, specifically for MAM model, it will be fully compliant and always conform to ITM proportionality requirement.

In summary, all BAM models and hybrids, except for MAM, are compliant with the ITM requirements and do accomplish the BEREC network neutrality policy. The MAM model does

not specifically conform to the proportionality ITM requirement 3.

8.9 | NN-PCM Quality of Service Related Considerations

The current evaluation is a proof-of-concept that NN-PCM does achieve a neutral operation allocating bandwidth to users belonging to different traffic classes. The allocations remain neutral even if the bandwidth, as a resource, becomes scarce.

Looking from a different perspective, the neutral operation of the NN-PCM does not guarantee that all users in all classes will always get the bandwidth they want when they request it. That is so because resources (i.e., link capacity) are typically under-provisioned by network operators. Consequently, under traffic spike conditions, the bandwidth will probably not be available for all requesting users. Neutrality, as demonstrated, will be kept by the NN-PCM, but the NN-PCM operation can not necessarily maintain the quality of service (QoS) the users obtain in normal traffic conditions (non-congested). In this scenario, the lack of resources impacts all users, and the impact is inversely proportional to the priority they have (TC priority). Anyhow, from the QoS perspective, all users will experience a smaller or more significant impact. The NN-PCM effectively shares the scarcity of resources neutrally among users.

This work has not focused on evaluating the impact of bandwidth scarcity in the QoS obtained by users with a neutral operation. Future work will consider the analysis and evaluation of the quality of service parameters like packet loss and delay that can be effectively obtained for users with the network submitted to peaks of traffic or, equivalently, with the network deliberately using under-dimensioned links.

It is also important to highlight that multiple solutions can be achieved with the NN-PCM (BAM) that can keep an equilibrium between network neutrality and QoS impact. As an example, a simple and straightforward approach for the operator business model would be to have a highly prioritized traffic class that, with congestion, uses the extra bandwidth of low priority classes by design. In other words, it means that the network operator can define its classes of traffic in such a way that, for some users, QoS will be less impacted and in a previously simulated range. The NN-PCM operation based on a BAM allows this kind of previous simulated configuration. In brief, the NN-PCM neutral operation does not necessarily maintain QoS, but it allows countermeasures and the possibility to design a contingency solution previously.

9 | FINAL CONSIDERATIONS

The NN-PCM is an innovative network neutrality tool based on a BAM model. The NN-PCM network neutrality accomplishment of the European BEREC reasonable Internet Traffic Management (ITM) practices was modeled and validated through the analysis of BAM models behavior and simulations. The results demonstrate that NN-PCM using the ATCS BAM model is legitimate, transparent, non-discriminatory, proportional, and exceptional.

A relevant operational aspect of the NN-PCM is its capability to accomplish network neutrality by design. In effect, the conformance to the BEREC ITM policy results from the inherent BAM behavior associated with the grouping of users in classes. In other words, NN by design means that the network manager chooses the BAM, configure it, and, following that, the NN-PCM operation allocates bandwidth to users in conformance with the BEREC network neutrality policy. To the best of our knowledge, network neutrality by design is unexplored by other NN technical deployments that focus mainly on detecting NN violations, reacting to them, and discriminating traffic.

Transparency concerning the business model adopted by network management is another positive aspect achievable by the NN-PCM. The business model in this paper corresponds to the allocation of users in classes and the definition of how much bandwidth is allocated to each class. The NN-PCM allows users to know two pieces of information about the business model. Firstly, it is possible to advertise to users the amount of resources they collectively have that technically corresponds to the minimum bandwidth constraint per class. Secondly, the users may know how the network will manipulate the available bandwidth per class and among classes. This second point corresponds to the configured BAM model operation and behavior. Whenever this information is made public, the NN-PCM accomplishes transparency by exposing to users what they have as resources and how these resources are allocated among them. By exposing the BAM configuration information, the NN-PCM contributes to solving a current network neutrality deployment problem, which is why most NN deployments have opaque policies that are hard to perceive or not perceived at all by the users.

The focus of the NN-PCM development is to demonstrate that, whether the available bandwidth configured for each class is under or over-dimensioned, the allocation of bandwidth to the user remains neutral and respects the BEREC requirements for network neutrality. This result was achieved, and, in summary, it means that the NN-PCM does accomplish BEREC network neutrality conformance with a neutral allocation of bandwidth among all users, regardless of their classes.

References

1. Stocker V, Smaragdakis G, Lehr W. The State of Network Neutrality Regulation. *ACM SIGCOMM Computer Communication Review* 2020; 50(1): 45–59.

2. Schewick Bv. Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like. *Stanford Law Review* 2015; 67(1): 1–129.

3. Wu T. Network Neutrality, Broadband Discrimination. *Journal of Telecom. and High Technology Law* 2005; 2: 141–180.

4. Maille P, Simon G, Tuffin B. Toward a Net Neutrality Debate That Conforms to the 2010s. *IEEE Communications Magazine* 2016; 54(3): 94–99.

5. Valletti T, Peitz M, Greenstein S. Net Neutrality: A Fast Lane to Understanding the Trade-offs. Working Paper 16-01, University of Mannheim; : 2016.

6. Webb M. Net Neutrality: A Regulatory Perspective. In: ITU; 2012; Sri Lanka.

7. BEREC . Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.; 2016. BoR (16) 127.

8. Commission FC. Protecting and Promoting the Open Internet. Tech. Rep. 15-24, ; Washington: 2015.

9. Brazil CD. Decreto No 8.771.; 2016.

10. Belli L, Bergen vM. A Discourse-Principle Approach to Network Neutrality: A Model Framework and its Application. tech. rep., ; : 2013.

11. Marsden C. Comparative Case Studies in Implementing Net Neutrality: A Critical Analysis of Zero Rating. *SCRIPTed* 2016; 13(1): 1–39.

12. Garrett T, Setenareski LE, Peres LM, Bona LCE, Duarte EP. Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection. *IEEE Communications Surveys Tutorials* 2018: 1–1.

13. Bourreau M, Kourandi F, Valletti T. Net Neutrality with Competing Internet Platforms. *The Journal of Industrial Electronics* 2015; 63(1): 30–73.

14. Peitz M, Schuett F. Net Neutrality and Inflation of Traffic. *Int. Journal of Industrial Organization* 2016; 46: 16–62.

15. Li F, Niaki AA, Choffnes D, Gill P, Mislove A. A Large-Scale Analysis of Deployed Traffic Differentiation Practices. In: Proceedings of the ACM Special Interest Group on Data Communication - SIGCOMM. ; 2019; Beijing, China: 130–144.

16. Wójcik R. *Net Neutral Quality of Service Differentiation in Flow-Aware Networks*. PhD thesis. AGH University of Science and Technology, Kraków, Poland; 2011.

17. Ravaioli R, Urvoy-Keller G, Barakat C. Towards a General Solution for Detecting Traffic Differentiation at the Internet Access. In: Proceedings of the 27th International Teletraffic Congress (ITC). ; 2015: 1–9

18. Zhang Z, Mara O, Argyraki K. Network Neutrality Inference. In: SIGCOMM '14. Association for Computing Machinery; 2014; Chicago, Illinois, USA: 63–74.

19. Maltinsky A, Giladi R, Shavitt Y. On Network Neutrality Measurements. *ACM Transactions on Intelligent Systems and Technology* 2017; 8(4): 56:1–56:22.

20. Mayer W, Schreiber T, Weippl E. A Framework for Monitoring Net Neutrality. In: Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES); 2018; Hamburg, Germany: 1–10.

21. Sivaraman V, Madanapalli SC, Kumar H, Gharakheili HH. OpenTD: Open Traffic Differentiation in a Post-Neutral World. In: SOSR '19. Association for Computing Machinery; 2019; San Jose, CA, USA: 119–126.

22. Stocker V, Smaragdakis G, Lehr W. The State of Network Neutrality Regulation.; 2020.

23. Bauer JM, Knieps G. Complementary Innovation and Network Neutrality. *Telecommunications Policy* 2018; 42(2): 172 – 183.

24. Glass V, Tardiff T. A New Direction for the Net Neutrality Debate. *Telecommunications Policy* 2019; 43(3): 199 – 212.

25. Abiteboul S, Stoyanovich J. Transparency, Fairness, Data Protection, Neutrality: Data Management Challenges in the Face of New Regulation.; 2019.

26. Ma RT, Misra V. Routing Money, Not Packets: A Tutorial on Internet Economics. In: SIGMETRICS '17 Abstracts. Association for Computing Machinery; 2017; Urbana-Champaign, Illinois, USA: 69–70.

27. Choi JP, Jeon DS, Kim BC. Net Neutrality, Business Models, and Internet Interconnection. *American Economic Journal: Microeconomics* 2015; 7(3): 104–141.

28. Reale R, Bezerra R, Martins J. G-BAM: A Generalized Bandwidth Allocation Model for IP/MPLS/DS-TE Networks. *International Journal of Computer Information*

Systems and Industrial Management Applications 2014; 6: 635–643. doi: 10.5281/zenodo.1292771

29. Reale RF. *Orquestração Cognitiva e Dinâmica da Alocação de Recursos para Redes MPLS/DSTE*. PhD thesis. Salvador University - UNIFACS, Salvador, Brazil; 2019.

30. Faucher FL, Lai W. Maximum Allocation Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering. Request for Comments RFC 4125, IETF; : 2005.

31. Le Faucheur F, Boyle J, Kompella K, Townsend W, Nadeau TD, Skalecki D. Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering. Request for Comments - RFC RFC 4127, Internet Engineering Task Force - IETF; : 2005.

32. Tata C, Kadoch M. CAM: Courteous bandwidth constraints allocation model. In: Proceedings of the 20th International Conference on Telecommunications - ICT; 2013: 1–5

33. Neto WCP, Martins JSB. Adapt-RDM - A Bandwidth Management Algorithm suitable for DiffServ Services Aware Traffic Engineering. In: IEEE/IFIP Network Operations and Management Symposium; 2008: 975–978.

34. Reale RF, Neto WCP, Martins JSB. AllocTC-Sharing: A New Bandwidth Allocation Model for DS-TE Networks. In: Proceedings of the VII Latin American Network Operations and Management Symposium; 2011; Quito, Equador: 1–4

35. Bahnasse A, Louhab FE, Oulahyane HA, Talea M, Bakali A. Smart Bandwidth Allocation for Next Generation Networks Adopting Software-Defined Network Approach. *Data in Brief* 2018; 20: 840–845. doi: 10.1016/j.dib.2018.08.091

36. Oliveira EM, Reale RF, Martins JSB. Cognitive Management of Bandwidth Allocation Models with Case-Based Reasoning - Evidences Towards Dynamic BAM Reconfiguration. In: Proceedings of the IEEE International Symposium on Computers and Communications (ISCC); 2018; Natal, Brazil: 1–7

37. Sadon SK, Din NM, Al-Mansoori MH, et al. Dynamic Hierarchical Bandwidth Allocation Using Russian Doll Model in Epon. *Computers & Electrical Engineering* 2012; 38(6): 1480–1489. doi: 10.1016/j.compeleceng.2012.05.002

38. Trivisonno R, Guerzoni R, Vaishnavi I, Frimpong A. Network Resource Management and QoS in SDN-Enabled 5G Systems. In: Proceedings of the IEEE Globecom; 2015: 1–7.

39. Durães G, Reale R, Bezerra R, Fontinele A, Soares A, Martins JSB. Evaluating the Applicability of Bandwidth Allocation Models for EON Slot Allocation. In: Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEEANTS); 2017; Bhubaneswar, Odisha, India: 1–6.

40. Hesselbach X, Dantas J, Amazonas JR, Botero JF, Piney JR. Management of Resources under Priorities in EON Using a Modified RDM Based on the Squatting-Kicking Approach. In: IEEE; 2016; Trento, Italy: 1–5

41. Reale RF, Bezerra RM, Martins JSB. Analysis of Bandwidth Allocation Models Reconfiguration Impacts. In: Proceedings of the III International Workshop on ICT Infrastructures and Services (ADVANCE); 2014; Florida, US: 67–76

42. BEREC . All You Need to Know about Net Neutrality Rules in the EU.; 2020.

43. Belli L. *Net Neutrality Reloaded: Zero Rating, Specialised Service, Ad Blocking and Traffic Management*. Fundação Getulio Vargas - Direito . 2016.

44. Belli L, De Filippi P. The Value of Network Neutrality for the Internet of Tomorrow. tech. rep., CERSA - Centre d'Etudes et de Recherches de Sciences Administratives et Politiques; : 2013.

45. Barreto D, Reale R, Martins J. Neutralidade de Rede com Modelos de Alocação de Banda e Comportamentos G-BAM Análise de Compatibilidade. In: Proceedings of the XXXV Computer Networks and Distributed Systems Brazilian Symposium (SBRC); 2017; Belém, Brazil: 702–715.

46. Kreutz D, Ramos FMV, Verissimo P, Rothenberg CE, Azodolmolky S, Uhlig S. Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE* 2014; 103(1): 14–76.

47. Mendiola A, Astorga J, Jacob E, Higuero M. A Survey on the Contributions of Software-Defined Networking to Traffic Engineering. *IEEE Communications Surveys Tutorials* 2017; 19(2): 918–953.

48. ITU-T . Y.1541: Network Performance Objectives for IP-Based Services.; 2002.

49. ITU-T . Y.1221: Traffic Control and Congestion Control in IP-Based Networks.; 2002.

AUTHORS BIOGRAPHY

M. Sc. David S. S. Barreto. Bachelor in Electrical Engineering by Faculdade AREA1 and Masters Degree in Computer Science at Salvador University (UNIFACS). David is a member of IPQoS Research Group and RePAF Project (Resource Allocation Framework for MPLS, Elastic Optical Networks and IoT) at UNIFACS and currently works at ANATEL (Brazilian Telecommunications Regulatory Agency). His research interests include Network Neutrality, Coverage and Quality measurements in mobile networks, Performance, QoS and QoE.

Prof. Dr. Rafael F. Reale. Professor at Institute Federal of Bahia (IFBA). Ph.D. in Computer Science with DMCC (UFBA/UNIFACS/UEFS), MSc. in Computer Systems by Salvador University - UNIFACS (2011) and bachelor in Informatics by Universidade Católica do Salvador (2005). Professor at Instituto Federal da Bahia (IFBA). His current research interests include Bandwidth Allocation Model, MPLS, DS-TE, Autonomy, QoS, Future Internet Architectures, Software-Defined Networks and Cognitive Networks.

Prof. Dr. Joberto S. B. Martins. Ph.D. in Computer Science at Université Pierre et Marie Curie - UPMC, Paris (1986), PosDoc at ICSI/ Berkeley University (1995), and PosDoc Senior Researcher at Paris Saclay University - France (2016). International Professor at Hochschule für Technik und Wirtschaft des Saarlandes - HTW (Germany) (since 2004) and Université d'Evry (France). Full Professor at Salvador University (UNIFACS) on Computer Science, Director of NUPERC and IPQoS research groups with research interests on Cognitive Management, Resource Allocation, Machine Learning, SDN/ OpenFlow, Internet of Things, Smart Grid and Smart Cities.