

Importance Measures for NFV Data Center: An Availability Evaluation

Rafael Souza¹, Marcelo Santos², Stênio Fernandes¹

¹Centro de Informática – Universidade Federal de Pernambuco (UFPE)
Caixa Postal 181 - CEP 89802-112 – Recife – PE – Brasil

{rrs4, sflf}@cin.ufpe.br

²Instituto Federal do Sertão Pernambucano (IF Sertão-PE)
Caixa Postal 508 - CEP 56000-000 – Salgueiro –PE – Brasil.

marcelo.santos@ifsertao-pe.edu.br

Abstract. *Data center infrastructures need to provide high availability of their services. Unexpected spikes of downtime in data centers lead to financial losses. Besides, there are intangible costs such as damaged reputation, low employee satisfaction, and reduced customer retention. In this context, Network Function Virtualization (NFV) emerged as a paradigm that assists data centers in becoming more dynamic and flexible. This paper presents an availability evaluation and importance analysis under the redundancy of NFV in data centers. The NFV data center component importance is represented by using Reliability Block Diagrams (RBD). The proposed models have identified the availability importance and critical devices in an NFV data center. This research also suggests alternatives for device redundancy to reach higher availability and proposes a new importance measure for analyzing the impact of NFV factors on data center availability. The measure can evaluate the degree of the impact of a failure on the data center, therefore, help to identify the factors with a substantial impact on data center availability.*

1. Introduction

Data centers are composed of a set of technologies and network communications that provide specialized value-added services. These services encompass scalable processing and storage capacity for a myriad of company sizes. These organizations invest heavily in data center planning to avoid, for example, unexpected peaks of data center downtime.

From a planning perspective to a data center, several studies have neglected aspects of dependability regarding availability and fault tolerance [Narten et al. 2014]. Ponemon Institute (Ponemon)¹ claims that several of the data center failure problems occur due to the lack of well-defined fault tolerance strategies. The Ponemon survey states that 81% of failure cases are due to projects conducted with poor resource provisioning or a bad resource allocation plan. The lack of planning increases downtime rates. The same survey shows that the downtime cost doubled — from 2010 to 2016 — from more than \$1 Million USD (United States Dollar) to \$2.4 Million USD. The same study shows that the average cost of data center downtime is about \$9,000 per minute. The traditional technologies of these environments — such as switches and routers — are closed

¹<http://www.ponemon.org/blog/2016-cost-of-data-center-outages>

network appliances. Each vendor uses firmware and software specific to its hardware. Significant capital investment is required when creating or launching a new service. The investment includes space to accommodate new hardware, the integration, and operation of a new complex network appliance. To overcome these barriers, virtualization creates a virtual version of dedicated hardware appliances and network functions. Virtualization mechanisms can lead to more dynamic data centers. It is possible, for example, to carry out process automation, with a reduction in Capital expenditures (CAPEX) and operating expenses (OPEX). NFV is a paradigm that uses the concept of virtualization, inherited from the data center world, to perform network functions, such as firewalls, load balancing and Deep Packet Inspection (DPI). These functions are typically embedded in dedicated network devices, in financial costs [Schaffrath et al. 2009] [Chiosi et al. 2012]. It is important to note that these approaches allow you to manage network resources different from traditional networks. Besides, a survey conducted in 2015 by IHS Markit², estimated investment in NFV solutions would cost close to \$11.6 billion USD by 2020. The same study, states that 100% of the service providers consulted intend to adapt their infrastructures to support NFV; where 81% will achieve that change by the end of 2017.

A solution for redundancy has always been considered a significant way to increase network availability. However, redundancy has a higher financial cost because of the need to add devices and be limited to mission-critical devices. In this context, Importance Measures (IMs) is an advantageous method for designers, manufacturers, and maintenance specialists to identify how a device failure can affect the network operation; thus, determine the weak devices within the network [Si et al. 2009]. This research focuses on establishing availability indexes for critical devices for the entire NFV data center network; including the reliability measure of importance [Birnbaum 1968], [Figueirêdo et al. 2011]. Also, analyzing the significance of the device is useful when faced with cost versus equipment decisions.

Within the IETF, Network Function Virtualization (NFVWG) investigates NFV from several perspectives to identify approaches that can be defined, implemented and used in the short term, as well as identify future research challenges. In particular, Service Function Chain Working Group (SFCWG) main areas of interest include solutions: virtualization, resource allocation and SFC, as well as identification of future research challenges in the area [Khalili et al. 2018] [Xu et al. 2018] [Quinn and Nadeau 2015]. Another group related to this work is the Benchmarking Methodology Working Group (BMWG), research for works also related to performance improvements, among which there are works with a specific focus in the data center [Morton 2017] [Avramov and Rapp 2016] [Avramov 2017]. In this way, we have a contribution the definition of Importance Measures and possible NFV solutions applied to the data center environment. Also, it is expected as a result to contribute to the Internet Draft (I-D) entitled "Analysis of the SFC scalability"³.

The main contributions of this paper are three-fold: (i) **Availability modeling for the NFV infrastructure in Data Centers**: a representative sample is (in discrete time/continuous time) the stated based models for representing NFV data centers. (ii) **Availability allocation through importance measures in an NFV data center**: identi-

²<http://www.infonetics.com/pr/2015/NFV-Market-Highlights.asp>

³<https://datatracker.ietf.org/doc/draft-ao-sfc-scalability-analysis/>

fying possible hazards is vital for each of the crucial components in the NFV data center. (iii) **Critical availability in NFV data center**, propose critical IMs which rank the components regarding their importance in the NFV data center.

2. Background Concepts

This section presents a summary of the concepts necessary for a better understanding of this research.

2.1. NFV Data Center

NFV is a paradigm that uses the concept of virtualization to perform network functions. NFV separates network functions from proprietary hardware devices with Commercial off-the-shelf (COTS) hardware. COTS hardware focuses on a variety of functions, such as Virtual Private Network (VPN), Firewall, and load balance, among others. As such, it's a concept that uses the technologies of IT virtualization to create entire classes of network nodes, also called Virtual Network Function (VNF). A VNF can define an ordered list of network services (e.g., Network Address Translation (NAT), Firewalls, Cache). These services are then "stitched" together in the network to create a Service Function Chain (SFC) [ISG 2013].

Figure 1 depicts the use of general purpose machines in an NFV data center, it is the virtualization of several different network functions (e.g., Packet Inspection, Firewall, Load Balance, etc.). VNFs are instantiated within the data centers on-demand networks, and they allow flexible virtual machine resource allocation.

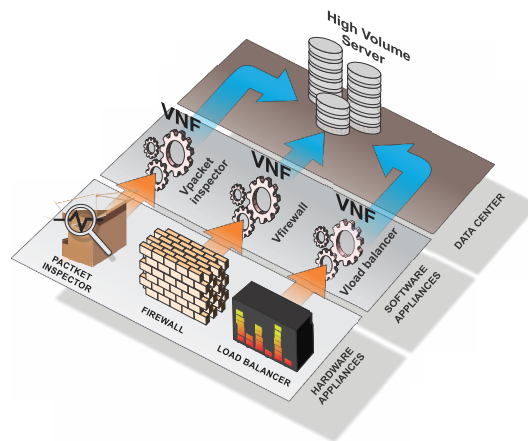


Figure 1. NFV Data Center Overview

2.2. RBD Models

One of the most powerful representations are RBDs. The RBD model consists of two basic elements: devices and links. The devices are represented by blocks, which have several attributes, such as the fault distribution function. The links and nodes are logical constructs to connect the blocks. The links conduct the paths of a network. A path is defined as a continuous path when there is no overlaps from the input to the output ??.

Figure 2(a) shows a RBD in Series and Figure 2(b) represents a parallel RBD. It is possible to represent a physical device in the mode of operation, through a block then estimate the reliability of each block.

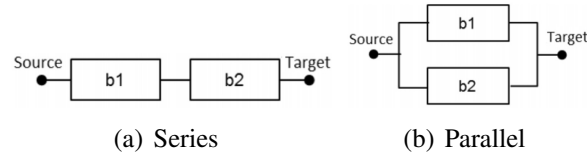


Figure 2. Reliability Block Diagram.

Equation 1 show the probability for the system to be operational.

$$\begin{aligned}
 P \{ \phi (x) = 1 \} &= P \{ \phi (x_1, x_2, \dots, x_i, \dots, x_n) = 1 \} \\
 &= \prod_{i=1}^n P \{ x_i = 1 \} = \prod_{i=1}^n p_i = 1.
 \end{aligned} \tag{1}$$

Therefore, the system reliability is

$$\begin{aligned}
 R_s(t) &= P \{ \phi (x, t) = 1 \} = \prod_{i=1}^n P \{ x_i (t) = 1 \} \\
 &= \prod_{i=1}^n R_i (t),
 \end{aligned} \tag{2}$$

where $R_i(t)$ is the reliability of block b_i . Likewise, the system instantaneous availability is

$$\begin{aligned}
 A_s(t) &= P \{ \phi (x, t) = 1 \} = \prod_{i=1}^n P \{ x_i (t) = 1 \} \\
 &= \prod_{i=1}^n A_i (t),
 \end{aligned} \tag{3}$$

where $A_i(t)$ is the instantaneous availability of block b_i .

2.3. Importance Measures (IM)

Given its dynamic nature, NFV requires high availability in data centers. Data centers must be able to allocate resources within a short time and in the right way.

The aspects of availability require close attention to the network's quality of service. Availability may be instantaneous or stationary. Instant availability represents the probability the network does not fail within a determined time frame. The steady state availability is the percentage of time a device or network can perform its function [Avizienis et al. 2004]. Availability Importance (AI) are mathematical availability analysis tools used to classify network performance [Birnbaum 1968]. However, instead of

using reliability, the metric used is availability, including, in addition to the average time to failure, the recovery time of the devices.

The Critically Availability Importance (CAI) measure is a natural extension of the Birnbaum metric [Birnbaum 1968]. The CAI metric includes the unavailability of devices, while the Birnbaum measure does not [Kuo and Zuo 2003]. A less reliable device receives more attention. Critical measures are useful for prioritizing availability decisions, identifying network node ranking, and weak links. The critical ranking of assets is used to improve maintenance activities.

The following benefits for NFV data center design uses two importance measures: (i) **IM**: is relevant in establishing the direction and prioritization of actions related to an upgrading effort (availability improvement) in NFV data center design. IM also recommends the most efficient way to operate and maintain system status; (ii) **CAI**: prioritizes availability improvement activities, identifies weak-links in the system, and many other uses.

3. Related Works

Based on the literature review, it was observed that no published papers address our specific research problem. There are studies that deal with resource allocation strategies [Thai et al. 2016], [Medhat et al. 2015], [Xia et al. 2015], investigating the SFC, and optimization problems. However, Thai et al. [Thai et al. 2016] and Medhat et al. [Medhat et al. 2015] do not specify the type of optimization algorithms used in their studies. Xia et al. [Xia et al. 2015] proposed two algorithms, one heuristic, and another Integer Linear Program (ILP). This study focused on reducing the consumption of network resources. The heuristic algorithm obtained almost an optimal result.

Other works refer to a SFC, through positioning strategies. Thai et al. [Thai et al. 2016] focused on developing genetic algorithms that control network functions considering dynamic flow changes. Huang et al. [Huang et al. 2015] investigates the problems of SFC and orchestration to intra-chains and inter-chains link contention. Huang et al. sought to satisfy users' Service Level Agreement (SLA) in a software-defined data center network by creating ILP algorithms to evaluate the Orchestrator performance of multiple SFCs. Gupta et al. [Gupta et al. 2015] did not clarify the specific NFV infrastructure used in their Content Delivery Network (CDN).

Therefore, the available related works do not solve the NFV Data Center planning problem. Our research considered aspects of fault tolerance through an availability analysis and evaluation of important measures. To the best of our knowledge, the related studies did not investigate fault tolerance concerning the application of NFV in the data center.

Three assumptions are needed: (i) Device failures are statistically independent. Failure in one device does not affect the outage rate of the other devices; (ii) The time between device interruptions and the repair duration is distributed according to a known exponential distribution system; (iii) Requires a previous calculation of the NFV availability through the operational path and non-operational path.

4. Problem Overview

A complex resource allocation problem exists when virtualized functions are reallocated to provide flexible virtual network services in an NFV based data center. Besides that, unexpected periods of downtime lead to financial losses; as well as, intangible costs such as damaged reputation, low employee satisfaction, and reduced customer retention. In this scenario, fault-tolerance techniques may mitigate these problems.

One of the challenges is to analyze each element of the network infrastructure and estimate which devices are most important in an NFV Data Center scenario based on an availability metric. In an NFV infrastructure, new components and software layers are added when compared to traditional network infrastructures. Determining how to define the set of essential elements is not a trivial task; it demands an advanced level of network management experience.

The lack of a strategy to increase the availability of the network affect the uptime of several services directly. Another factor that must be taken into account is the correct provisioning of network elements to avoid bottlenecks and periods of downtime. The inactive period is a metric that can guide how to establish the direction and prioritization of actions related to an upgrading effort (availability improvement) in system design or suggesting the most efficient way to operate and maintain the system status [Kuo and Zhu 2012]. High availability is crucial to determining whether the availability goals and uninterrupted service are met.

To allocate a set of VNFs, it is necessary to choose a solution between a set of possibilities. Both nodes and substrate links have limited resources. After the deployment process, nodes and links could fail. Redundancy is a conventional technique to guarantee the required performance.

5. Methodology

Figure 3 describes the methodology to adopt an analytical modeling strategy. This methodology employs an integrated approach based on availability and Importance Measures (IM) of the NFV data centers.

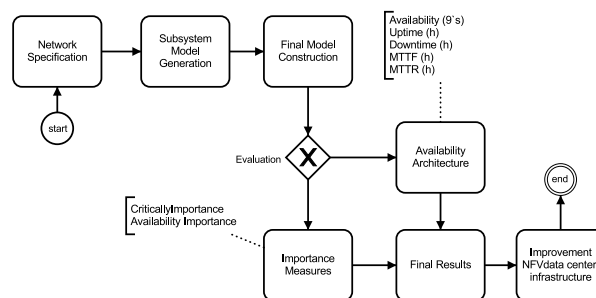


Figure 3. Methodology

The six stages of the methodology are described as follows: (i) Network Specification: Initially, the network was defined as a set of nodes, switches, servers, VMs, and VNFs. The specification can be automatically generated by a tool, such as a mapping algorithm or manually provided by a designer. At this stage, it is essential to clarify the

problem to be analyzed. (ii) Subsystem Model Generation: In this phase, NFV data center subnet models are generated considering their operational mode. At this stage, there are no dependency interactions between devices.

The model provides a logical iteration between system components, defining which active combinations determine the functionality of the network; (iii) Final Model Construction: includes the generation of dependability models; (iv) Evaluation of the Availability Architecture and Importance Measures: At this stage, the impact of device redundancy on the data center availability is quantified. Besides, the most important devices are identified; (v) Final Results: the evaluation results are presented to assist the redesign NFV data center. (vi) Improve NFV data center: The new components are added to the NFV data center to improve availability. Thus, it is possible to know exactly which are the importance and critically components in operation.

Table 1 details the Mean time to failure (MTTF) and the Mean Time To Repair (MTTR) values for each device in the NFV data center infrastructure [Fernandes et al. 2012], [Gill et al. 2011], [Potharaju and Jain 2013]. The time required to perform the availability analysis was 8760 hours (1 year), and it was calculated for the steady state.

Table 1. Input Parameters for the Devices and Links

Devices	MTTF	MTTR
CPU	2500000	1
HD	2000000	1
NIC	6200000	1
Memory RAM	48000	1
VM	2880	2
VNF	2893	0,25
TorSwitch	175200.0	2.9
Aggregation	87600.0	2.1
Core Switch	600000.0	2.1
Link	19996	12

The fat-tree topology is used to inter-connect NFV data center. The baseline architecture (A1) consists of physical devices connected in sequence by 1 Core, 1 Aggregation, 1 Tor switch, 2 Servers. The virtual devices, are Orchestrator, VNF manager, VIM, 3 SFC being SFP1 (Firewall -> Load Balance, Gateway), SFP2 (Cache -> Firewall -> IDS), SFP3 (DPI, Proxy, NAT).

Each server consists of a Central Processing Unit (CPU), Hard disk (HD), Network Interface Card (NIC), Memory, and VM. Next objective is to extract the MTTF and the MTTR from the servers using the following Equation 4.

$$\lambda\mu_{cpu} * \lambda\mu_{hd} * \lambda\mu_{memory} * \lambda\mu_{nic} * \lambda\mu_{vm} \quad (4)$$

where the λ is the MTTF and μ represents the MTTR. The failure of a component (CPU or Mem or HD or NIC or VIM) to perform its required functions can lead to a server error and thus deny the VNF request.

6. Evaluation and Results

The application of redundancy techniques is made compared strategy with IM and without IM. Thus, all variations or suggestions of redundancy have the same amount of additional components. The additional components are a variation of a baseline architecture that is

composed of 1 Core, 1 Aggregation, TorSwitch, 2 Server, 1 Orchestrator, 1 VNF manager, 1 VIM, 9 VNF.

Our evaluation addresses the following questions: **How to decide which device or VNF should be replicated? How to improve the availability at the same time that reduces the cost? How to improve your NFV data center operations?** We evaluate the scenarios where different dependability objectives coexist in the NFV data center network. The contribution of the article is to decide which device is the most important for more efficient planning of availability and fault tolerant. This paper defines the baseline data center architectures (A1) and alternative architectures as created with and without Importance Measures (IM). Figure 4 as shown in NFV Architecture (A1) assumes that there is no redundancy in the data center Fat-Tree topology ($k=1$). The RBD model to represent the architecture A1.

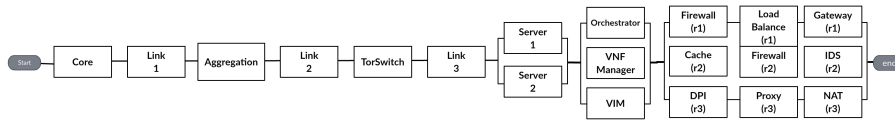


Figure 4. RBD model of Architectures (A1)

6.1. Scenario 1: without Importance Measures (IM)

This section describes the experiments without IM. The objective is estimate the availability of the system when there is not any kind of evidence that indicate which device should be replicated. Table 2 depicts the adopted Topology and Nodes. More specifically, the experiment considers: physical device (topology), virtual device (topology), and number of nodes (node). For each treatment, RBD models are generated.

Table 2. Experiment I - without IM

Topology	Nodes
Physical	Core, link, Agregation, Server
Virtual	Firewall, Load Balance, Proxy

Without any criteria, it is possible to define how to deploy additional devices (redundancy) based on the experience of the network operator. However, it can be a wrong choice. In order to show it, Figures 5, presents a Fat-tree topology with redundancy in the Core, Tor Switch and Server devices, but without IM.

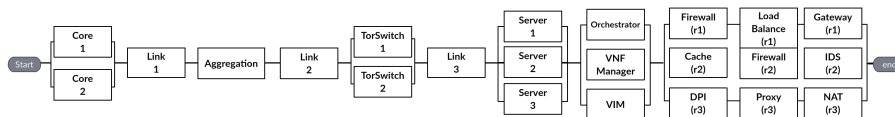


Figure 5. RBD model of Architectures (A2)

Figure 6 shows some models that take into account redundancy in the Virtual devices (Firewall, Cache, DPI), but without IM.

Figure 7 exhibits some models that take into account redundancy in the Virtual devices (Orchestrator, VNF Manager, VIM), but without IM.

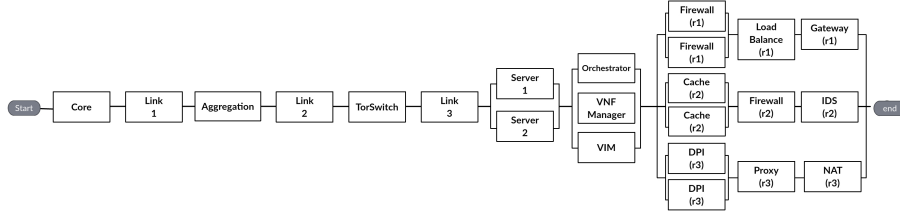


Figure 6. RBD model of Architecture (A3)

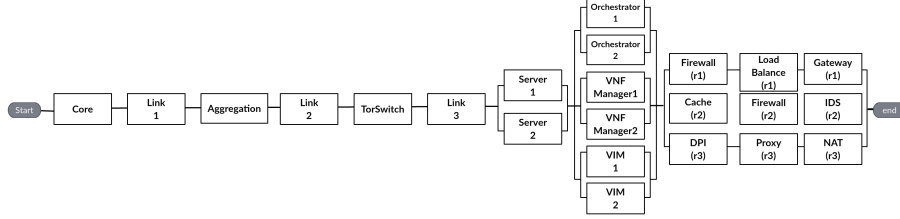


Figure 7. RBD model of Architecture (A4)

6.2. Scenario 2: Importance Measures (IM)

This experiment utilized IM based on availability. The IMs were tested for networks composed of multiple degrading compositions. Here, we first studied the index of importance of different network devices, building a ranking. We then determined how IMs can be used to built redundancy into their deployment process. Equation 5 calculates the component importance for availability.

$$I_A^s = A(1_i, p_i) - A(0_i, p_i) \quad (5)$$

, where I_A^s is the component importance for availability i ; p_i is the availability of component i , and A is the availability of the entire system.

Equation 6 shows how to obtain the normalized form of component importance.

$$I_{ni} = \frac{I_i}{I_x} \quad (6)$$

, where I_{ni} is the normalized index for the i ; The I_i means the non-normalized index value for the device i . The I_x means the value of the highest non-normalized index among the devices.

We performed a second evaluation to understand which are the most critical devices. Equation 7 was used to calculate the impact of the devices.

$$I_{ds}(i; p) = \frac{pi(1_i, p) - A(0_i, p))}{A(p)} \quad (7)$$

The network devices i when operating, is indicated by $I_{ds}(i; p)$, is therefore defined as the probability that the device i works. Device i is critical to the operation of the network since the network is operating.

When i fails, it is denoted by $I_{df}(i; p)$, being defined as the probability that the device i has failed. When the network presents a fault it is expressed by Equation 8.

$$I_{df}(i; p) = \frac{qi(1_i, p) - A(0_i, p)}{1 - A(p)} \quad (8)$$

Table describes the results of availability importance and ranking of each device of architecture A1; This table shows the ranking of the most critical devices of architecture (A1).

Table 3. Importance Measurement (A1)

Devices	I_1^d	Rank	$I_{df}(i; p)$	Rank
Core1	0.982138	5	0.9999	2
Link1	0.988039	2	0.9999	2
Agregation	0.985158	3	1.0	1
Link2	0.988039	1	1.0	1
TorSwitch1	0.982151	4	1.0	2
Link3	0.988039	1	1.0	1
Server1	0	n/a	0	n/a
Server2	0	n/a	0	n/a
Orchestrator	0	n/a	0	n/a
VNF Manager	0	n/a	0	n/a
VIM	0	n/a	0	n/a
SFP1 (Firewall, Load Balance and Gateway)	0	n/a	0	n/a
SFP2 (Cache, Firewall and IDS)	0	n/a	0	n/a
SFP3 (DPI, Proxy, NAT)	0	n/a	0	n/a

The parameters are presented in decreasing order of the IM index. The highest ranked devices are Agregation, Link2, and Link3. This technique helps us to identify the parameters with significant impact on system steady-state availability. The IM ranking obtained will also enable us to justifiably ignore parameters that have less impact on the measure of interest.

The models indicated that three devices cause the greatest impact on data center availability: Agregation, Link2, and Link3. A new Architecture 5 (A5) was defined. Figure 8 presents the RBDs related to A5.

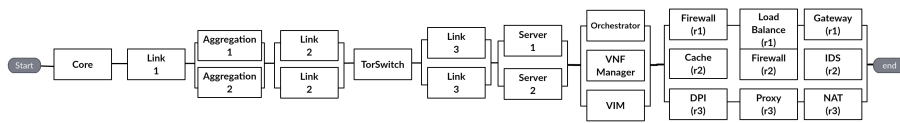


Figure 8. RBD model of Architecture (A5)

An important consideration is the device failing mode. It is possible to identify the devices with greatest impact on data center availability. Availability is computed by Equation 9. Availability of a system is expressed through the relation between MTTF and the MTTR [Ebeling 2004].

$$A \lim_{t \rightarrow \infty} A = t = \frac{MTTF}{MTTF + MTTR} \quad (9)$$

The number of nines (9's) is a way to represent availability and it can be calculated according to Equation 10. The number 100 represents the maximum level of availability that the network system can reach. The variable A means the availability of the network system.

$$N = 2 - \log(100 - A) \quad (10)$$

Figure 9 shows the graphical results of evaluation dependability of NFV data center with and without Importance Measure.

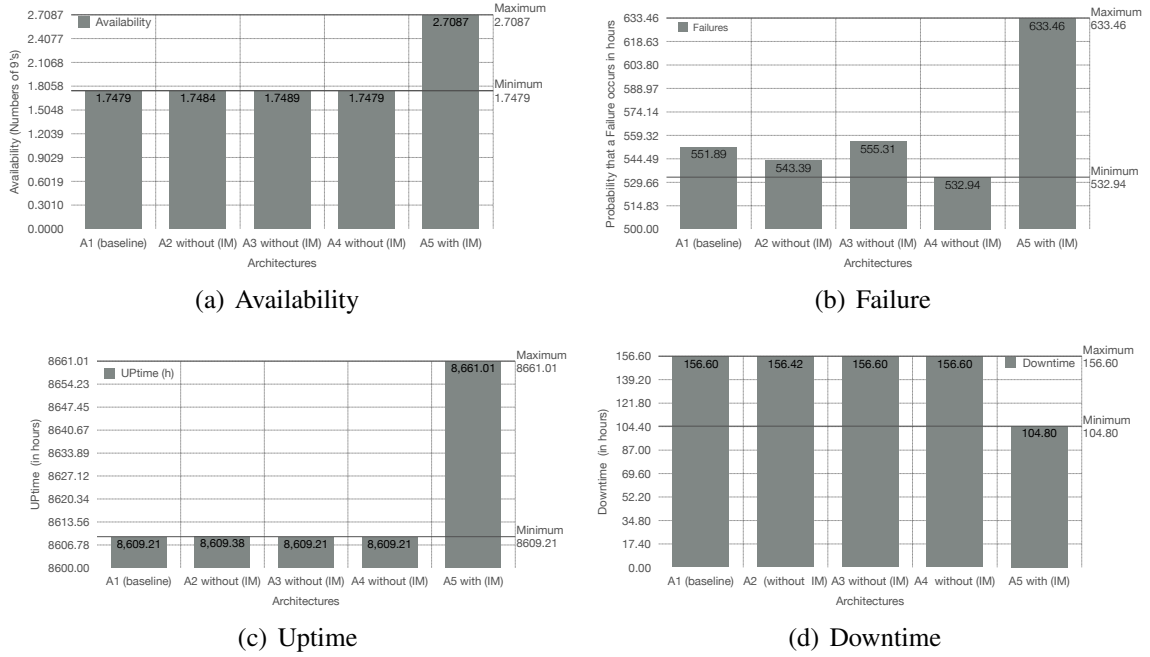


Figure 9. Evaluation Dependability

Figure 9(a) summarizes the results of the five architectures. The availability limits are presented with the availability in number of nines. As we can see, there were few improvements using the without IM strategy of availability to plan the best NFV application in the data center. The architectures A2, A3, and A4 had a small percentage increase in availability to A1. However, our proposal is based on measurements of the importance of availability and critically. This solution shows significant increases in availability, is easier to operate and is practical. When compared to A1, A5 increased by 96%. However, it is important to note that even after all the improvements, the system has not reached the 5 9's because of the device quantity for the reduction. Our search was limited to a maximum of 24 devices in both scenarios. The use of the IM technique allows obtaining exact and efficient 59s with the addition of more components.

Figure 9(b) summarizes the results of the five architectures. The probability that a failure will occur is considered in a one year interval time. We noticed, compared to the baseline architecture A1, that the A5 architecture is more fault tolerant than A2, A3 and A4. Therefore, the use of IM is essential for NFV data center fault tolerant planning.

Figure 9(c) summarizes the uptime of the five architectures. It represents the available operating time during space time in 8760 hours (one year). The results show the usual uptime for a higher than normal period occurs between the architectures when using the IM methodology. Compared to A1, the Uptime level is high in the A5 architecture.

Figure 9(d) we present the results of the downtime at the NFV data center. The

results show the efficiency in reducing the period of downtime between the architectures when using the IM methodology. The downtime is 104.80 hours for the A5 architecture compared to the A1 (156,600 hours).

Table 4 summarizes the results of the five architectures.

Table 4. Summary Results of Architectures

Architectures	MTTF	MTTR	Availability	Uptime(h)	Downtime(h)
A1	528.037680	9.605030985	0.9821349182	8609.21	156.60
A2	543.397214	9.873055170	0.9821550954	8609.38	156.42
A3	555.312656	10.10116412	0.9821349182	8609.21	156.50
A4	532.944419	9.694284812	0.9821349182	8609.21	156.50
A5	633.460555	7.665113223	0.9980442889	8661.01	104.80

From the evaluation of our research, we were able to answer the questions: How to decide which device or VNF should be replicated? How to improve the availability at the same time that reduces the cost? How to improve your NFV data center operations?. So our answer is that the Importance Measure (IM) with the main goal of assessing the critical points for improvements in the NFV data center. This technique helps us to identify the parameters with significant impact on system steady-state availability. The following observations can be made based on the experiment results. Architecture A5 have higher availability compared to Architecture A1. This occurs because they have redundant devices like Aggregation, Link2, and Link3, which reduces the bottleneck of network availability. In general, the results demonstrate the significant impact of distinct devices on the availability of the respective physical device. Both RBD models are valuable tools for NFV data center designers during architectural planning.

Introducing redundancy in physical devices turns the virtual devices reliable based on the two evaluated scenarios. If the goal is to assist network designers in reducing bottlenecks, the measure of importance is adequate.

Network infrastructure planning consists of many devices. Exploring every possible combination is needed to maximize the availability of the NFV data center. However, with the application of the important and critical parameters evidence shows an optimized process with mathematical indicators. The process is based on the index to perform redundancy for each element of the NFV data center.

7. Conclusions

This paper presented models to assess the availability in NFV data center environments. The work was conducted based on distinct analytical RBD models to evaluate the impact of different redundancy strategies to increase availability. Critical and Importance are used to define a device redundancy policy.

The results show that adding redundancy without any criteria may result in a low availability of the network and unnecessary cost. Availability importance can be used to identify good candidates that lead to improved NFV data center availability. The importance measure of critically can be used to prioritize maintenance actions. Besides that, the results show that network availability can be improved efficiently by focusing on a reduced set of factors, thereby, producing a substantial increase in availability. Specifically,

in the context of NFV data center, the results show that components as the Orchestrator, VMs and VNFs are less relevant than other physical devices when the objective is to maximize the general availability. Through the use of IM, it is possible to increase the uptime of the NFV Data Centers more than 100 hours in a year when compared to a scenario without any redundancy or based on bad choices of redundant devices.

Future research will include the development of an exact algorithm based on the branch and bound approach. The research will identify a heuristic algorithm to solve the problem of mapping of SFC in the NFV data center. The heuristic algorithm can be used in real-time decision making supporting the importance measures. The algorithm will consider various ways to improve dependability requirements of one or more data center NFV devices. For example, traffic variation can reduce the availability and reliability of virtual and physical links within a data center.

References

- Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1):11–33.
- Avramov, L. (2017). Data Center Benchmarking Methodology. RFC 8239.
- Avramov, L. and Rapp (2016). Data Center Benchmarking Methodology. Internet-Draft draft-ietf-bmwg-dcbench-methodology-03, Internet Engineering Task Force. Work in Progress.
- Birnbaum, Z. W. (1968). On the importance of different components in a multicomponent system. Technical report, Washington Univ Seattle Lab of Statistical Research.
- Chiosi, M., Clarke, D., Willis, P., Reid, A., Feger, J., Bugenhagen, M., Khan, W., Fargano, M., Cui, C., Deng, H., et al. (2012). Network functions virtualisation: An introduction, benefits, enablers, challenges and call for action. In *SDN and OpenFlow World Congress*, pages 22–24.
- Ebeling, C. E. (2004). *An introduction to reliability and maintainability engineering*. Tata McGraw-Hill Education.
- Fernandes, S., Tavares, E., Santos, M., Lira, V., and Maciel, P. (2012). Dependability assessment of virtualized networks. In *Communications (ICC), 2012 IEEE International Conference on*, pages 2711–2716. IEEE.
- Figueirêdo, J., Maciel, P., Callou, G., Tavares, E., Sousa, E., and Silva, B. (2011). Estimating reliability importance and total cost of acquisition for data center power infrastructures. In *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*, pages 421–426. IEEE.
- Gill, P., Jain, N., and Nagappan, N. (2011). Understanding network failures in data centers: measurement, analysis, and implications. In *ACM SIGCOMM Computer Communication Review*, volume 41, pages 350–361. ACM.
- Gupta, A., Habib, M. F., Chowdhury, P., Tornatore, M., and Mukherjee, B. (2015). On service chaining using virtual network functions in network-enabled cloud systems. In *Advanced Networks and Telecommunications Systems (ANTS), 2015 IEEE International Conference on*, pages 1–3. IEEE.

- Huang, P.-H., Li, K.-W., and Wen, C. H.-P. (2015). NACHOS: Network-aware chains orchestration selection for nfv in sdn datacenter. In *Cloud Networking (CloudNet), 2015 IEEE 4th International Conference on*, pages 205–208. IEEE.
- ISG, N. (2013). Network functions virtualisation (NFV) virtualisation requirements.
- Khalili, R., Despotovic, Z., Hecker, A., Purkayastha, D., Rahman, A., and Trossen, D. (2018). Optimized Service Function Chaining. Internet-Draft draft-khalili-sfc-optimized-chaining-00, Internet Engineering Task Force. Work in Progress.
- Kuo, W. and Zhu, X. (2012). Some recent advances on importance measures in reliability. *IEEE Transactions on Reliability*, 61(2):344–360.
- Kuo, W. and Zuo, M. J. (2003). *Optimal reliability modeling: principles and applications*. John Wiley & Sons.
- Medhat, A. M., Carella, G., Lück, C., Corici, M.-I., and Magedanz, T. (2015). Near optimal service function path instantiation in a multi-datacenter environment. In *Network and Service Management (CNSM), 2015 11th International Conference on*, pages 336–341. IEEE.
- Morton, A. (2017). Considerations for Benchmarking Virtual Network Functions and Their Infrastructure. RFC 8172.
- Narten, T., Gray, E., Black, D., Fang, L., Kreeger, L., and Napierala, M. (2014). Problem statement: Overlays for network virtualization. Technical report.
- Potharaju, R. and Jain, N. (2013). When the network crumbles: An empirical study of cloud network failures and their impact on services. In *Proceedings of the 4th annual Symposium on Cloud Computing*, page 15. ACM.
- Quinn, P. and Nadeau, T. (2015). Problem Statement for Service Function Chaining. RFC 7498.
- Schaffrath, G., Werle, C., Papadimitriou, P., Feldmann, A., Bless, R., Greenhalgh, A., Wundsam, A., Kind, M., Maennel, O., and Mathy, L. (2009). Network virtualization architecture: proposal and initial prototype. In *Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures*, pages 63–72. ACM.
- Si, S., Liu, F., and Cai, Z. (2009). Failure importance analysis models based on bayesian network. In *Industrial Engineering and Engineering Management, 2009. IE&EM'09. 16th International Conference on*, pages 151–154. IEEE.
- Thai, M.-T., Lin, Y.-D., and Lai, Y.-C. (2016). A joint network and server load balancing algorithm for chaining virtualized network functions. In *Communications (ICC), 2016 IEEE International Conference on*, pages 1–6. IEEE.
- Xia, M., Shirazipour, M., Zhang, Y., Green, H., and Takacs, A. (2015). Network function placement for nfv chaining in packet/optical datacenters. *Journal of Lightwave Technology*, 33(8):1565–1570.
- Xu, Q., chun Zhou, H., Li, T., Li, G., and Li, G. (2018). A Method for Service Orchestration in hSFC. Internet-Draft draft-xu-sfc-hierarchical-orchestration-02, Internet Engineering Task Force. Work in Progress.