

# DNCT704 Network and Cloud Design and Assessment

1 – REPORT AND PRESENTATION  
MURACHI, TAKASHI



Diploma in Applied Network and Cloud Technology (Level 7)

**Cover Sheet and Student Declaration**

This sheet must be signed by the student and attached to the submitted assessment.

<b>Course Title:</b>	<b>DNCT704 Network and Cloud Design and Assessment</b>	<b>Course code:</b>	<b>DNCT704</b>
<b>Student Name:</b>	<b>Takashi Murachi</b>	<b>Student ID:</b>	<b>850000605</b>
<b>Assessment No &amp; Type:</b>	<b>Theory/Practical</b>	<b>Cohort:</b>	<b>DANCT7124C-E/OL</b>
<b>Due Date:</b>	<b>2/8/2024</b>	<b>Date Submitted:</b>	<b>2/8/2024</b>
<b>Tutor's Name:</b>	<b>Vaibhav Fanibhare</b>		
<b>Assessment Weighting</b>	<b>40%</b>		
<b>Total Marks</b>	<b>100</b>		

**Student Declaration:**

I declare that:

I have read the New Zealand School of Education Ltd policies and regulations on assessments and understand what plagiarism is.

I am aware of the penalties for cheating and plagiarism as laid down by the New Zealand School of Education Ltd.

This is an original assessment and is entirely my own work.

Where I have quoted or made use of the ideas of other writers, I have acknowledged the source.

This assessment has been prepared exclusively for this course and has not been or will not be submitted as assessed work in any other course.

It has been explained to me that this assessment may be used by NZSE Ltd, for internal and/or external moderation.

If I am late in handing in this assessment without prior approval (see student regulations in handbook), marks will be deducted, to a maximum of 50%.

**Student signature:**

**Date: 19/7/2024**

**Tutor only to complete**

<b>Assessment result:</b>	<b>Mark</b>	<b>/100</b>	<b>Grade</b>
---------------------------	-------------	-------------	--------------

## Table of Contents

Introduction .....	3
Executive summary: Assessing a network .....	3
Main body .....	3
1. Critical analysis of network design and architecture utilising SDN to achieve high availability and scalability in the current conventional network.....	3
Critical analysis of application and service continuity utilising Fog computing technology to achieve high availability and scalability in the current conventional network. ....	8
The layout of an advanced network architecture that integrates Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Fog computing technologies.....	12
Executive Summary: Technical Advice .....	12
A comprehensive overview of business continuity planning (BCP) and disaster recovery planning (DRP) in hybrid networks .....	12
Outlining their five high-level stages to achieve a logically detailed description of BCP and DRP.....	13
Evaluation of five cost-benefit trade-offs .....	14
Five technical advice on the efficient use of BCP/DRP in a hybrid network, based on five trade-off evaluations. ....	15
Conclusion and recommendations.....	16
Reference lists .....	16

## Introduction

### 100-150 words

Juniper Technologies must conduct a critical analysis of their infrastructure networking in the small to medium IT sector, evaluating their existing hybrid networking system (Figure 1) to ensure its high availability and scalability, to execute business continuity plan (BCP) and disaster recovery plan (DRP) in their budget and needs of their quality of service (QoS). Before and after a disaster, such as COVID-19, a company must evaluate trade-off plans between costs and benefits to ensure that current hybrid networking will be sustainable and cost-effective. To sustain business continuity, this evaluation should incorporate new technologies like software-defined networking (SDN), network function virtualisation (NFV), and fog computing, along with five technical evaluations and advice. The final proposed outcome will be presented by three group members.

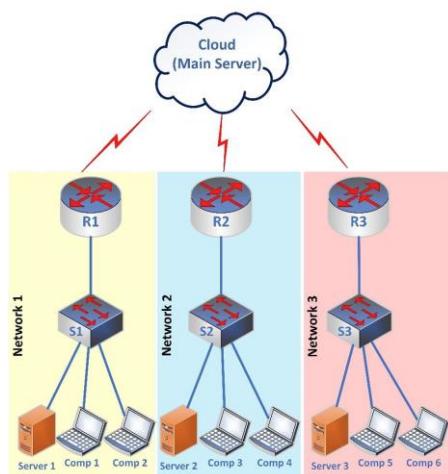


Figure 1: Network topology for Juniper Technologies.

## Executive summary: Assessing a network

### 100-150 words

This paper provides a thorough evaluation of the significant analysis of traditional network problems at Juniper Technologies, a firm of moderate size in the IT services industry. The objective is to improve the architecture by using software-defined networking (SDN), network function virtualization (NFV), and fog computing technologies. The objective is also to enhance their current hybrid cloud networking operation with high availability and scalability. Our proposed new network design layout, which demonstrates both current networking resources and a virtualised software-based architecture design layout as a dynamic and cost-effective business model, will resolve these limitations under the appropriate quality of service (QoS).

## Main body

Critical analysis of network design and architecture utilising SDN to achieve high availability and scalability in the current conventional network.

### Current networking issues contain

1. The lack of dynamic routing

Current networking is set as **static routing** and even implementing dynamic routing using DHCP scope under the physical 3 server machines, so once increasing access point through wireless Lan, there are still limitations for utilising infrastructure resources in upscaling and downscaling.

Configuring the router, switch either manually or using DHCP server allocations for VLAN setting, human errors, malware attacks, less flexibility to find the best forwarding by switch and routing by the router through OSPF, ERGP protocol. For example, between source point A and destination point B, there are three routers C (top), D(middle) and E(bottom) are connected after purchasing a new router for expanding business, but still this physical routing can only communicate the configured router each other. If router C(top) are attacked by malware or does not work, then tomorrow router D is not working, then each time, configure and repair the router, so not easy.

## 2. Inefficient cost performance

Due to the cost of increasing labour costs, customers for small to medium companies can be challenging to do daily operations, such as capitalise cost and operational costs. For example, the business performance for profit and loss will be unpredictable so even if purchasing additional servers, configuration costs, hiring new staff and training costs can easily take all small profits under the flat revenue. If the assigned works are in a remote area, then staff needs to visit on-site until fix the issue which will incur additional costs which will not be a win-win strategy for the client and this company.

## 3. Unclear or Quality of service (QoS)

When Increasing access to their website, the traffic flow will be expected to be congested. Assumed that this company provide a high level of speed for the finance support, so they cannot stop their business and needs to prioritise the customised bandwidth required, however, management does not know which applications are required to allocate their resources such as load balancer server, which will be also considered as additional budget to request network provider, and setting required networking physical cables, and keep them maintained as additional costs.

## **Introduction SDN**

Software-defined Networking (SDN) is a low-cost, innovative technology to enhances scalability and flexibility by controlling and managing traffic flow congestion in the infrastructure layer from the above layer in one central unit using northbound with application layer and southbound application programming interfaces (APIs) with infrastructure layer dynamically. Open-flow algorithms are most popular in using Ubuntu in Linux environment. This approach enables one application to offer instruction to the entire networking like switching on and off altogether as if we use a remote controller to secure enough resources, managing enhanced security and optimisation for delivering secure data in a virtual environment from any of our chosen cloud vendors. The architecture of Software-Defined Networking (SDN) comprises three layers: the infrastructure layer, the control layer, and the application layer(*Architecture of SDN: DNCT704 Network and Cloud Design and Assessment*, n.d.).The main purpose is to focus on separating the management plan, and control plan from the data plane in software-based networking technologies.

1. Figure 2 shows the top layer of the management strategy, which consists of various programmes that enforce specific network controls. For instance, a range of network environments, from tiny residential networks to large-scale multitenant data centres, employ traffic engineering to detect system errors, load balancing, and firewalls. Compared to the typical network-2 depicted in Figure 2, the implementation of complex management techniques is significantly simpler, relieving users of the burden of purchasing and configuring multiple devices. Applications determine which data should be prioritised under the QoS policy, and shaping the customised wider bandwidth service, and which computer devices have available data storage capacity. This is because network operators like school principals can manage traffic without having to worry about the intricate details of complex control logic with conventional networking as well as sending a request message to the control plane in the lower layers(E & C Engineering Department, National Institute of Technology Srinagar, J & K, 190006 et

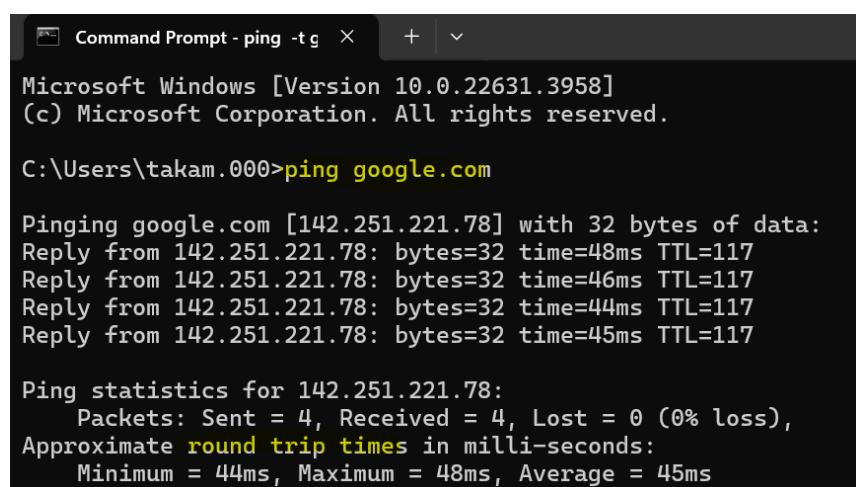
al., 2022, p. 4).

2. The control layer is in the middle of the control plane and is part of the main SDN controller. Its goal is to handle and control all three layers of networking while sending a message to the infrastructure layer, which is at the bottom of the data plane. The control plane, also known as the "core layer," establishes the network control logic and rule policy to link the management and data planes. We can either set up the system with a single centre body or spread it out across many places. The SDN controller ensures that management apps can see the full network structure and know what's happening in real time. This lets them set broad rules for the network without having to worry about the specifics of how it will work at a lower level(E & C Engineering Department, National Institute of Technology Srinagar, J & K, 190006 et al., 2022, p. 4).This layer is a similar layer of our human head containing brain.

The data plane is the distributed-forwarding functional layer. Post office workers, for example, can send data to this layer, and open-flow switches can help identify the optimal router to deliver encrypted packets to the destination, either in software or hardware, with minimal latency, according to the central control plane's rules. The centralized SDN control plane has already received instructions from the rule specifying which data to send to what destination address. Therefore, securely connected routers and switches in the data plane transmit the data to its intended destination. This way can be programmed safely via an open interface, such as OpenFlow protocol to decrypt each piece of encrypted data (E & C Engineering Department, National Institute of Technology Srinagar, J & K, 190006 et al., 2022, p. 3). This layer is a similar layer of our human body containing hands and legs to carry the data based on the instruction of the control plane policy rule.

#### Use of a Decentralised control plan

OpenDaylightm ONOS, Ryu in Linux environment using Python programming, creating many virtual servers and backing up each server to prevent failover of one machine so that a high availability environment can be created for autoscaling such as upscaling and downscaling. The advantage of creating multiple virtual servers over the control layer can minimise the risk of malware attacks and destroy a large network from one main SDN controller. The disadvantage is the complexity of configuration in both physical networking and control load balancer in programming. Automation can be possible with the help of machine learning and deep learning techniques in virtual networks, however, only students can learn with Master's degree (NZQA level 9) and Phd NZQA (level 10).



```
Command Prompt - ping -tg × + ▾
Microsoft Windows [Version 10.0.22631.3958]
(c) Microsoft Corporation. All rights reserved.

C:\Users\takam.000>ping google.com

Pinging google.com [142.251.221.78] with 32 bytes of data:
Reply from 142.251.221.78: bytes=32 time=48ms TTL=117
Reply from 142.251.221.78: bytes=32 time=46ms TTL=117
Reply from 142.251.221.78: bytes=32 time=44ms TTL=117
Reply from 142.251.221.78: bytes=32 time=45ms TTL=117

Ping statistics for 142.251.221.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 44ms, Maximum = 48ms, Average = 45ms
```

```

Microsoft Windows [Version 10.0.22631.3958]
(c) Microsoft Corporation. All rights reserved.

C:\Users\takam.000>tracert google.com

Tracing route to google.com [142.250.71.78]
over a maximum of 30 hops:

 1   1 ms    1 ms    1 ms  192.168.1.254
 2   *         *         * Request timed out.
 3   *         *         * Request timed out.
 4  19 ms    19 ms   18 ms  122.56.119.216
 5  44 ms    *         43 ms  et4-0-5.sgbri3.global-gateway.net.nz [122.56.119.30]
 6  43 ms    43 ms   43 ms  72.14.202.230
 7  45 ms    46 ms   46 ms  192.178.97.91
 8  44 ms    44 ms   47 ms  142.250.234.211
 9  47 ms    44 ms   43 ms  syd1s17-in-f14.1.e100.net [142.250.71.78]

Trace complete.

```

```

C:\Users\takam.000>pathping google.com

Tracing route to google.com [142.250.71.78]
over a maximum of 30 hops:
 0  DESKTOP-78DL9C7.home [192.168.1.70]
 1  192.168.1.254
 2  125-239-56-1-fibre.sparkbb.co.nz [125.239.56.1]
 3  *         *         *

Computing statistics for 50 seconds...
          Source to Here   This Node/Link
Hop  RTT      Lost/Sent = Pct  Lost/Sent = Pct  Address
 0           0/ 100 = 0%        0/ 100 = 0%  DESKTOP-78DL9C7.home [192.168.1.70]
 1     3ms      0/ 100 = 0%        0/ 100 = 0%  192.168.1.254
 2     6ms      0/ 100 = 0%        0/ 100 = 0%  125-239-56-1-fibre.sparkbb.co.nz [125.239.56.1]

Trace complete.

```

## Critical analysis of network design and architecture utilising NFV to achieve high availability and scalability in the current conventional network.

### Current networking issues contain

1. Current networking is static routing and inflexible, which is not true.
2. Failover between switch and PC, so lack of availability of cable.
3. Security threatens

### Introduction of NFV

Network Function Virtualisation (NFV) is an innovative technology that enables the virtualisation of networking functionality by installing special software in the computer server without purchasing, configuring and maintaining physical devices, such as routers, switches and PCs because these are expensive and time-consuming operations and updating them for enhancing the security purpose. Thanks to virtualisation, networking functions can be separated from hardware devices, and to simplify the deployment, administration, and autoscaling, resulting in increasing of flexibility and scalability. Thus, we can avoid purchasing various types of devices and settings. Still, we can set all expected virtual networking based on scalability demands for the long-term or short-term elastic demands. Instead, NFV can have a networking architecture function that injects automation and programmability to enable the implementation of all necessary applications and software into one virtual machine instead of each proprietary hardware. For example, the adaptable and flexible computer in virtualisation of NFV is all inclusively working in virtual networking by installing the updated new service features, such as a firewall to block malware attacks from external networking, load balancer to make equal dataflow from the heavy traffic in bandwidth, VPN to secure

data transmission in a secure tunnel, IDS/IPS to detect and monitor abnormal malware attacks, router to make an optimised the data flow route, switch to deliver the packet to the final destinations(Kaur et al., 2022, p. 3). This NFV can make an effective approach to centralise all usable functions, servers, storage, and switches so that infrastructure and upgrading are easy setting up. However, there are challenge situations regarding equal level of performance in hardware and software in virtualisation, their efficient instantiation, placement, and migration, and the development of new business models and price setting and operational processes

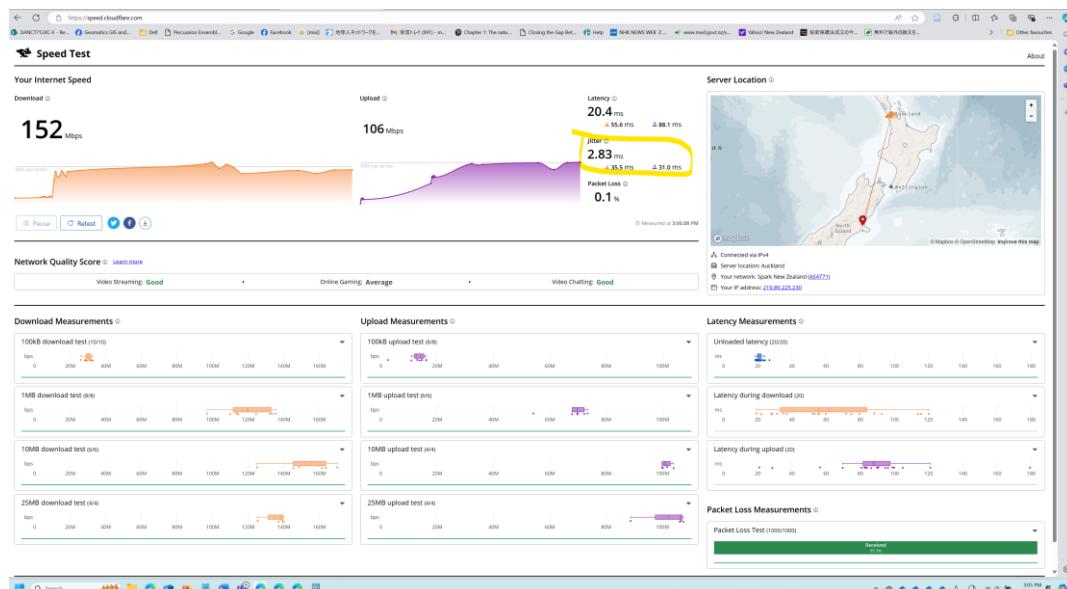
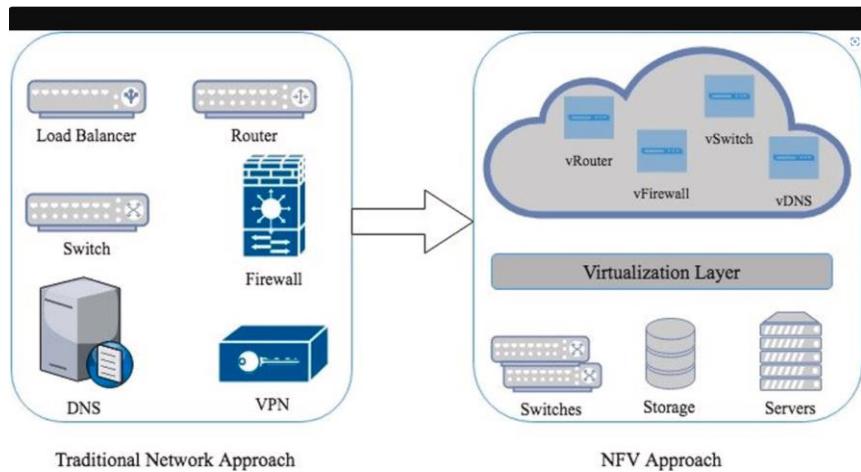
Virtualized network functions (VNFs), NFV infrastructure (NFVI), and the NFV management and orchestration (MANO) system make up the three main parts of the NFV architectural framework. The Network Function Virtualization Infrastructure (NFVI) can execute the Virtualized Network Functions (VNFs), which are software-based representations of network functions. The NFVI refers to the physical and virtual components that together form the infrastructure required for running virtual network functions (VNFs). The MANO system is responsible for administering and coordinating the Virtual Network Functions (VNFs) and **Network Function Virtualization Infrastructure (NFVI)**.

**Virtual Network Functions (VNFs)** enable network services, such as Internet and telephone, to establish efficient connections by utilising immediate resources within a virtual service accessed through a website. This eliminates the need to purchase physical hardware devices, resulting in cost savings. Additionally, VNFs offer easy maintenance and upgrading of resources, enhanced security measures, and simplified data migration.

Physical resources such as servers, storage, and networking equipment make up **NFVI**. Furthermore, the virtualization layer encompasses technologies such as KVM (Kernel-based Virtual Machine), VMware ESXi, and Microsoft Hyper-V. This is analogous to the desks and tables seen in a single classroom within a school. At the virtualization layer, we can install software to establish another virtual network based on the newly created hardware resources at the lower level of the hardware layer. These objects, such as whiteboards and laptops, share similarities with the physical qualities found in our everyday lives.

NFV Management and Orchestration, also known as Management and Network Orchestration (**MANO**), enables the control and coordination of different software and platforms such as OpenStack, VMware vSphere, and Red Hat OpenShift on a Kubernetes-based container platform. It also facilitates networking virtualization via Open vSwitch (OSV) and VMware NSX. Firewall, IDS/IPS, SSL/TLS off-road, performance monitoring, and data analytics tools such as Prometheus, Grafana, and ELK Stack are additional components for enhancing security in virtual networking. In NZSE, both teachers and tutors can oversee and regulate student activities using Canvas. MANO (Management and Orchestration) controls virtual networking using various components. VIM (Virtualized Infrastructure Manager) manages the installation context of Virtual Network Functions (VNFs). The Virtual Network Function Manager (VNFM) monitors the status of VNFs, ascertaining their activation or deactivation within the system. All virtualised VNF network functions, including firewalls and routers, are under the control of NFVO (NFV Orchestrator). According to its instructions, NFVO allocates locations for these functions. The NFVO also establishes the location, usage, and control of VNFs, thereby promoting a well-structured networking environment. NFVO also handles VNF extraction and placement as required. For instance, VNFO can perform many functions, such as deployment, autoscaling, monitoring and administration, resource allocations, and lifecycle controls. When the Network Function Virtualization Orchestrator (NFVO) adds or removes new or old Virtual Network Functions (VNFs), it assumes full responsibility for determining the precise location for evaluation. As the number of users increases, the Virtual Network Function (VNF) must also expand proportionally. By using autoscaling, NFVO can dynamically adjust its capacity based on demand. Occasionally, the NVFO detects a broken VNF and can identify and monitor the extent of damage, as well as pinpoint the specific components that require repair. It can then proceed to fix those sections. By efficiently utilising the hardware resources of the CPU, memory, and storage, NFVO can optimise the allocation of VNFs by ensuring sufficient space in the NFVO. When certain virtual

network functions (VNFs) are no longer needed, the Network Function Virtualization Orchestrator (NFVO) can remove and store those selected VNFs outside of the NFVO(Kaur et al., 2022).



Critical analysis of application and service continuity utilising Fog computing technology to achieve high availability and scalability in the current conventional network.

### Identify Issues:

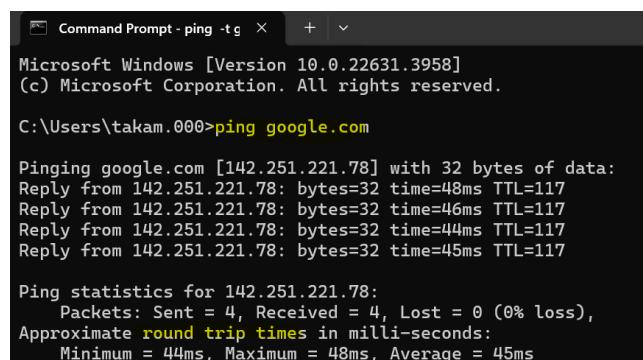
1. High latency in a long packet
2. Hardware failure
3. Jitter

The current network is not suitable for real-time data, such as temperature and rainfall sensor data. Bandwidth in conventional networking is not enough. For instance, consider a scenario where there are two users. For instance, a video call necessitates high bandwidth because one block of data (packets) travels through one lane and reaches the destination every second, whereas the same length of packets travels through three lanes, allowing the first three packets to reach the destination simultaneously, thereby reducing traffic flow delays. Another aspect is that current networking only sets up three routers, resulting in what appears to be static routing. The system will monitor the number of IPs used and configure three servers accordingly. Due to the limited number of routers and switches, excessive access

to the server during peak traffic periods can lead to significant traffic congestion, causing slow motion, floating monitor screens, and a decrease in customer satisfaction. will be downgraded. If an attacker targets an interface located in the middle of a cable line, it will immediately impact the entire network. The packet transmission distance is also a significant issue. The round-trip time from Christchurch, New Zealand, to Sydney, Australia, is approximately 44 to 48 milliseconds. However, if a router malfunctions during this hop, the system switches to a different router to determine the optimal path to Sydney. Such a hardware failure could result in higher costs and a longer preparation time, as a distant location could lead to packet loss or drop. oss or drop could happen.

Time-consuming to execute process the to analyse the data from New Zealand to the nearest data centre in Australia East, which causes high latency.

Suppose the data centre is in Australia. In that case, our business is in New Zealand. All our services including all virtually created resources, such as VM, network, storage, computing courses, and firewalls, will be executed, analysed, and proceed where at the nearest data centre in Australia East. The time is taken from New Zealand to Australia East where the resource in intensive workload will take more time from request to server in Australia East and get a response from the data centre server to New Zealand client machines.



```
Command Prompt - ping -t g × + ▾
Microsoft Windows [Version 10.0.22631.3958]
(c) Microsoft Corporation. All rights reserved.

C:\Users\takam.000>ping google.com

Pinging google.com [142.251.221.78] with 32 bytes of data:
Reply from 142.251.221.78: bytes=32 time=48ms TTL=117
Reply from 142.251.221.78: bytes=32 time=46ms TTL=117
Reply from 142.251.221.78: bytes=32 time=44ms TTL=117
Reply from 142.251.221.78: bytes=32 time=45ms TTL=117

Ping statistics for 142.251.221.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 44ms, Maximum = 48ms, Average = 45ms
```

Therefore, there are uncertain time frame in the distance between New Zealand and Australia. For example, if the partial resources are virtually created near the user of host machine over type 1 hypervisor, then the processing speed will be faster because of the nearest locations in New Zealand through multiple Fog nodes to diversify the risk of malware attacks and load balancing the data frow stream smoothly. Only important information was filtered out either by low pass or high pass filter method to extract the information that we set in quality of service (QoS) for maintaining the quality, availability and responsibility by agreed between cloud provider and users and Service level agreement (SLA) to ensure our company policy and KPI including jitter are all met the updated standards.

Server present at your user's location or near to the user's location is not able to process the intensive workload generated by user due to the data centre having a server is far away. But we use the near server not full fill our workloads and are not able to process that high level of a large volume of data in a main data centre in Australia East, but instead of Australia, near somewhere in New Zealand, we can read the copy of packet near the location in New Zealand.

By the use of Fog computing, initially packets are travelling from source to destination and return to the original point, where edge computing near the collected data point like Christchurch as an example, and Auckland is the Fog computing node area. By diversifying the risk of node(server), it would be better for multiple vietual gateway so that malware attackers could be diversified the risk as well as multiple virtual public load balancer can distribute equally into the fog computing area.

Microsoft's Azure Load Balancer within Fog computing zone is a cloud networking service that spreads network data across various computers in the Azure cloud to improve application speed and uptime. It works at the TCP and UDP protocol level as a layer-4 load balancer, so it can handle a wide range of situations, from simple web services to complicated multi-tier designs. There are three levels of the service: Standard Load Balancer, which moves data between regions and within regions; Gateway Load Balancer, which is a virtual device for service chaining; and Basic Load Balancer, which is best for smaller apps (*Azure Load Balancer*, n.d.).

In this assumed case scenario, Azure Internal Load Balancer is a cloud feature service that allows us to distribute the load of a traffic flow stream across resources in the infrastructure layer, SDN control layer, and application layer. The following functions and qualities are listed below:

### **1. Managing traffic flow.**

Hypervisor type 1 (hyper V) in Microsoft Azure equally reduces workloads for virtual networks, virtual storage, virtual computing cores, and open virtual switches by dynamically increasing or decreasing the number of virtual machines (VMs) on demand. In virtual machines and virtual networking, we achieve this by pre-setting thresholds such as instance, minimum, and maximum. As a result, we no longer must deal with the time-consuming process of downloading and installing software.

### **2. Enhanced security.**

The internal load balancer can serve as the company's internal virtual networking system, which will further enhance security by ensuring a more evenly distributed flow of encrypted data.

### **3. High availability and scalability.**

If damage is done by malware or partial virtual networking, failover networking may happen. However, an AI-integrated SDN controller using the Python Open Flow API can still find the exact locations between the application layers and the SDN control layer, as well as between the infrastructure layer and the SDN control layer. This is possible because anomaly detection-installed applications and DHCP server applications continue to recover the failover area, ensuring high availability and smooth traffic levels. When the data flow surpasses the maximum threshold setting or falls below the minimum threshold setting, the newly established infrastructure layer automatically distributes an optimal amount of data flow to meet the demands. As long as we use the VNF function's resources, Microsoft is responsible for providing them under the Service Level Agreement (SLA) and Quality of Service (QoS) policies. The proposal suggests that internal networking failover will prevent 99.99% or 90% of downtime per week, month, and year, ensuring smooth traffic and high availability. Additionally, it prioritises resources to ensure prompt updates in response to on-demand.

#### **1. Flexible networking structures.**

Even if power outages, disasters, cyber-attacks, or human mistakes occur in the entire zone 1 and cause downtime, an internal load balancer with an alarm function in the application can automatically generate another available zone 2 by copying all information stored in the outage zone 1 (*Azure Load Balancer*, n.d.).

We can easily increase speed and accessibility by using the DNS system application, which can connect to multiple access points across different regions where the data centre has been set up for Azure virtual machines, Web applications, cloud services, and external non-Azure endpoints. This implies that we can use Azure Traffic Manager to regulate the internet's data flow.

Here is a list of the following tasks and qualities:

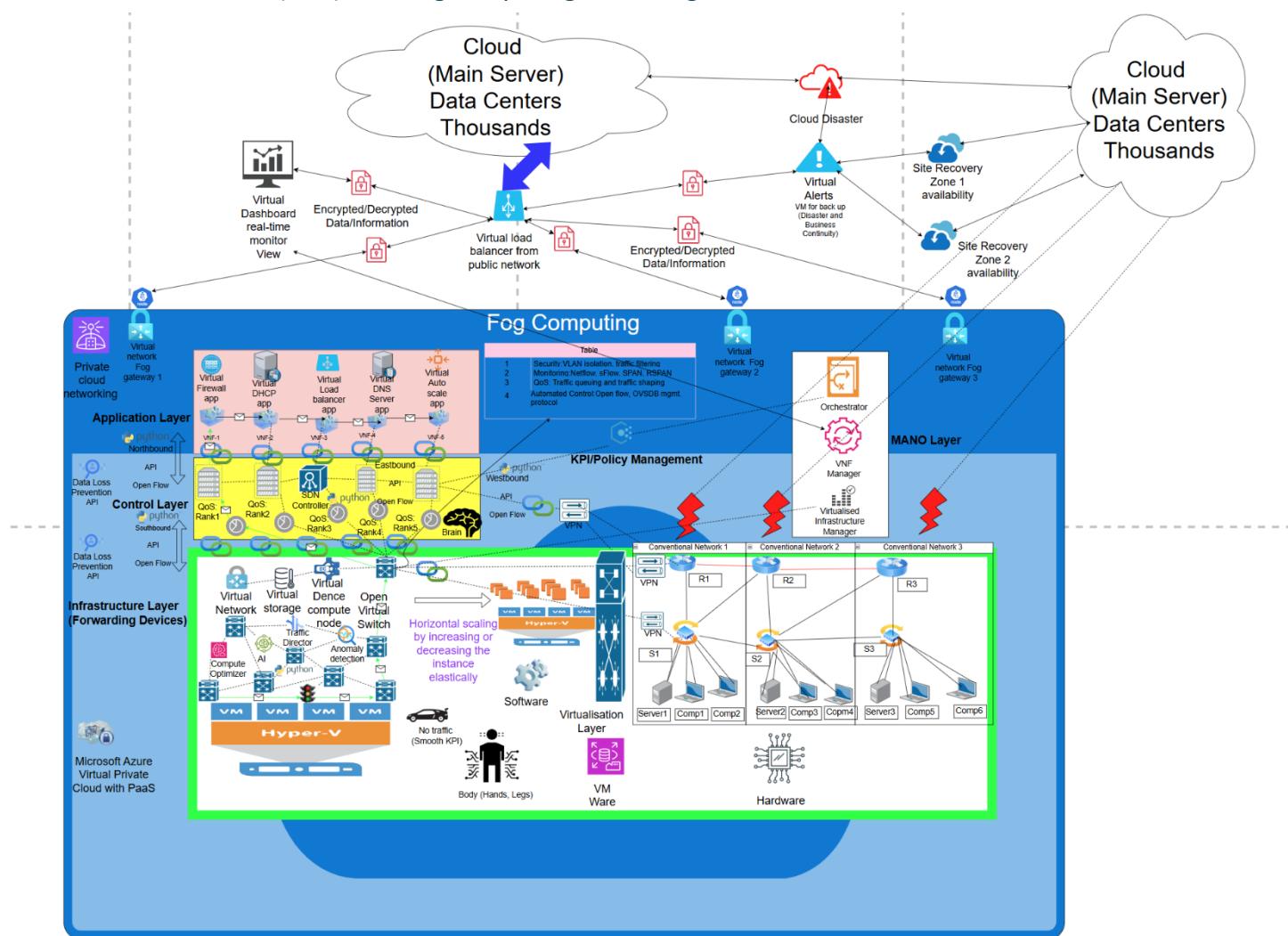
#### **1. Global distribution of load balances**

Because the end customers are located all over the world, the longer distance between the data centre and the user locations may result in significant delays. The traffic manager can, however, find

the closest entry point by optimising the traffic path. That reduces latency, and users can feel at ease with a smooth internet exchange and a positive user experience(Bhagat, 2019).

2. There are multiple routes available.
  - In each area, the QoS setting will optimise the traffic path according to the specific target's traffic rules.
  - The priority route enables us to locate the most direct path to Microsoft's data centres across various global regions.
  - The multivalve route tool can show customers all their options, allowing them to choose the best data centre spot.
3. The backup plan ensures high uptime during disasters.  
Even if a natural disaster destroys one data centre, the traffic manager can still route traffic to a backup data centre(*Azure Load Balancer*, n.d.).
4. Check up on your health.  
When people visit a website through HTTP and HTTPS, the health probe in Traffic Manager can fully check to see if there are any problems with launching the website. This makes sure that the website is stable. When we send an email over TCP, the health probe will turn on the regular functions on the application layer(mbender-ms, 2023).
5. Compatibility and building in Azure Traffic Manager can connect to and work with Azure services like the Azure App Service, virtual machines, and cloud services. It can also work with services that aren't Azure.

The layout of an advanced network architecture that integrates Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Fog computing technologies.



## Executive Summary: Technical Advice

Juniper Technologies focuses on the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) because both on-premises and cloud networking are feasible enough to prepare for future disaster resilience in the ongoing COVID-19. This report offers a comprehensive assessment and detailed description of the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) in hybrid networking. It highlights five high-level stages that aim to set middle points to balance cost and benefits, and it evaluates and provides advice on five technical aspects that justify why the benefits of BCP and DRP provide effective benefits in Juniper Technologies. These criteria can assist in making decisions about resilience and their respective enterprises based on cost-effective and sustainable business in hybrid networking.

A comprehensive overview of business continuity planning (BCP) and disaster recovery planning (DRP) in hybrid networks

**Business continuity:** Business continuity refers to the ongoing and strategic preparation and procedures implemented to ensure that critical business processes can continue to function daily, even in the event of natural disasters and cyberattacks. For instance, the New Zealand government implemented COVID-19 restrictions. However, if employees have access to remote work options or can promptly replace a deceased

staff member, businesses can continue operating by using another system and human resources as an alternative backup.

**Disaster recovery:** Business continuity primarily concentrates on the recovery planning of information technology systems and their associated data. The primary objective is to restore damaged infrastructure and recover lost data to their original standard level, enabling daily normal company operations that rely on information and technology. For instance, a corporation already possesses well-documented, sequential procedures that indicate the assigned individuals and the appropriate contact information for efficiently recovering all relevant IT resources.

Outlining their five high-level stages to achieve a logically detailed description of BCP and DRP.



**The BCDR process, from high-level policy to technical infrastructure, consists of multiple layers**

(*Introduction to BCDR: DNCT704 Network and Cloud Design and Assessment*, n.d.)

**1. Business Impact Analysis:**

The alert system, which can set instance, minimum, and maximum thresholds, highlights a detailed reference list of all related risk assessment level criteria, such as high (red), medium (yellow), and normal (green).

**2. Policy and strategy development:**

Based on regular internal discussions with various departments, management can determine the minimised amount of data loss and the downtime between the last updated backup time and the restored time after the disaster, considering the company budget, planned human and information technology-related resources, and prioritising applications that used in clients at most based on the last 12 months.

**3. Set up emergency guidance:**

In the event of power outages, emergency guidance could provide multiple access points using emergency slice technology through access points provided by drones and radio access networks.

#### **4. Training internal staff or consult with external experts:**

Provide the special training that can provide comprehensive training related to emergency and disaster resilient training annually that includes first aid certification.

#### **5. Validation and testing:**

Regular emergency training can provide ample confidence and prompt action in the event of a disaster. Such a high frequency of trial training fosters professional development enhances self-awareness of risk and updates their feedback into the newly documented references.

### Evaluation of five cost-benefit trade-offs

#### **1. Managing different sites and making copies of backup data**

**Cost:** The cost will include additional cloud storage, a service fee, a new SLA, and QoS.

**Benefits:** Regular backups, such as every 7 p.m., which is outside of business hours after data migration from on-premises to the cloud, help to minimise downtime.

**Trade-off:** analyse the historical usage ratio of the top 5 applications on the website, migrate them as a priority under the new SLA, and prioritise high bandwidth as the top priority parameter (99.99%) in QoS due to recent heavy web browser usage.

#### **2. Training cost for selected staff or outsourcing cost vs Outsourcing cost for DRP/BCP**

**Cost:** NZ\$10,000 per year for outsourcing will be charged to the company.

**Benefits:** The company can get specific and prompt advice from an outsourcing company with results and reports. The company can have the opportunity to learn new skills as professional development that make motivates to work and increase productivity with support from experienced work visa holders.

**Trade-off:** Although the initial cost of NZ\$10,000 per year will be expensive, internal staff will be educated by experienced staff with work visas can gain all necessary skills for 3 to 5 years and finally internal specialists can share teaching with other staff in a documented procedure.

#### **3. Cloud service subscription cost vs scalability and flexibility**

**Cost:** The continuous cloud service fee and the storage fee will increase daily as long as increase the storage demand and set the budget as NZ\$60,000 per year using a threshold alert and monitoring system in cloud service.

**Benefits:** Scale up and down under SDN and VNF technology over the type 1 hypervisor can bring scalability to meet the on-demand such as a sudden increase the demand or decrease in the demand and back up the site replication in other zones sites by using load balancer application that can bring risk diversification.

**Trade-offs:** Only minimum required cloud service that is related to the highest rank of QoC, and set alarm that is close to the target budget. application and keep the expense as low as possible. Before using cloud service, management can set the threshold as NZ\$65,000 per year. If an emergency event has happened, utilising cloud service for an assumed 5 times a year of the event, so 1 one-time event can save NZ\$10,000 times 5 events so a total of NZ\$50,000 can be saved with minimum downtime.

#### **4. Regular maintenance and upgrading of the networking system.**

**Cost:** Physical hardware and software license fees and updated security fees will be increased annually, as will training and hiring costs, because administrators need to control all risks, including regular downtime during the maintenance server.

**Benefits:** Networking performance will increase and mitigate sudden downtime because monitoring the anomaly behaviour in real-time will prevent the spread of the entire network.

**Trade-off:** Instead of increasing the downtime period, optimise the number of downtimes by using data analytics with data visualisation, to minimise the downtime time and cost.

#### **5. QoS setting priority**

**Cost:** Set the QoS policy agreement will take the time-consuming to read and determine in the entire organisation. Having the updated knowledge and skills are necessary to renew the QoS, so such professional development fees will incur additionally.

**Benefits:** Enhance the speed and security level, and user experience review on our website will increase customer satisfaction and increase sales with this review.

**Trade-off:** As a trade-off, instead of looking at all criteria for risk assessment, only the most important or high-risk criteria can be chosen as top-priority services in QoS, like bandwidth checks, so as not to stop the main application and to change each parameter gradually.

Five technical advice on the efficient use of BCP/DRP in a hybrid network, based on five trade-off evaluations.

##### **1. Managing different sites and making copies of backup data**

Backup data in virtual networking over the different geographically separate or different zones in the same region are option. However, the company size is small to medium so still save confidential information related privation information are saved in both on-premises servers as well as in the Microsoft Azure Virtual Private Cloud setting, because it can contribute to New Zealand access storage, which offers PaaS (Jeffery Mitchell, 2023) and easy to migrate into Microsoft Azure once data centres start operating in 2025 in New Zealand (*Azure Virtual Private Cloud - Guide - Whizlabs Blog*, 2021). This will benefit to indigenous Māori documents and personal information to meet the Private Act.

##### **2. Training cost for selected staff or outsourcing cost vs Outsourcing cost for DRP/BCP**

Investing in internal staff is critical, as outsourcing costs approximately NZ\$70 per hour, which is more than twice the market wage depending on your financial planning in the short, mid, and long term. However, you can still benefit from the return on investment and gradually transition from external to internal staff. The teaching methods include remote class training and face-to-face teaching classes to motivate staff for professional development, which can hugely benefit company growth with staff learning speed (*Cost of Training Employees*, n.d.).

##### **3. Cloud service subscription cost vs scalability and flexibility**

Organisations, being small to medium-sized companies focused on day-to-day operations, require on-demand services or the ability to reduce demand without incurring significant initial costs. For instance, to minimise the downtime interval between RPO and RTO on the cloud platform, Infrastructure as a Service (IaaS) models serve as essential infrastructure. This necessitates the hiring of

experienced staff, who then utilise IaaS models to access all resources, thereby fulfilling the company's decision-making policy requirements for availability, reliability, and scalability. This model will be agile and pay-as-you-go, allowing for cost savings and improved problem-solving solutions that are easier to manage while monitoring activity (*Cloud Computing 101*, 2020).

#### **4. Regular maintenance and upgrading of the networking system.**

Regular updates and visualisation with regulatory compliance are crucial because improve productivity and easily identify issues and resolve issues by prioritising the QoS service for security over other parameters(*developer*, 2023). For instance, integrating data visualisation with analytics is a proactive strategy to reduce downtime. This paper explores the potential of visual analytics in optimising manufacturing processes, focusing on part quality, machine downtime, and component life. It emphasises the importance of using machine data to make informed decisions and provide cost-effective solutions (*Engineering Proceedings / Free Full-Text / Visual Analytics Enabling Optimisation of Downtime*, n.d.).

#### **5. QoS setting priority**

The company cannot meet all parameters; therefore, management needs to decide which parameters should be prioritised. For example, QoS technology enables network engineers to prioritise latency-sensitive traffic flows, generating valuable data for monitoring and optimising traffic in hybrid networking environments. Network teams need to deploy, monitor, and adjust policies, collect crucial metrics, provide clear reports, and integrate with other network management systems for optimal performance(*Quality of Service (QoS) in Computer Networks*, n.d.).

### **Conclusion and recommendations**

Juniper Technologies can enhance networking agility and benefits by integrating new technologies like SDN, VNF, and fog computing while adhering to regulatory requirements. By determining the optimal time and data allocation during downtime under BCP and DRP strategies, Juniper Technologies can reduce costs and increase returns on investment. After evaluating risk assessment procedures, they can determine the midpoint of cost and benefits for a sustainable business model based on five technical recommendations and their evaluation results.

### **Reference lists**

- *Architecture of SDN: DNCT704 Network and Cloud Design and Assessment*. (n.d.). Retrieved 13 July 2024, from [https://nzseg.instructure.com/courses/809/pages/architecture-of-sdn?module\\_item\\_id=41529](https://nzseg.instructure.com/courses/809/pages/architecture-of-sdn?module_item_id=41529)
- *Azure Load Balancer: Features, Pricing, and Best Practices*. (n.d.). Spot.io. Retrieved 26 July 2024, from <https://spot.io/resources/azure-automation/azure-load-balancer-features-pricing-and-best-practices/>

- Azure Virtual Private Cloud—Guide—Whizlabs Blog. (2021, May 4).  
<https://www.whizlabs.com/blog/azure-virtual-private-cloud-guide/>
- Bhagat, A. (2019, September 14). Azure Load Balancing: Petabutz.  
<https://medium.com/petabutz/azure-load-balancing-f91a18d15668>
- Cloud Computing 101: Scalability, Reliability, and Availability. (2020, November 9). Lucidchart.  
<https://www.lucidchart.com/blog/reliability-availability-in-cloud-computing>
- Cost of training employees: Clear breakdown & saving tips. (n.d.). Retrieved 2 August 2024, from  
<https://www.lingio.com/blog/cost-of-training-employees>
- developer. (2023, June 13). The Importance of Regular Network Maintenance and Upgrades. *Networking Gurus*. <https://www.networking-gurus.co.nz/the-importance-of-regular-network-maintenance-and-upgrades/>
- E & C Engineering Department, National Institute of Technology Srinagar, J & K, 190006, Ahmad, S., & Hussain Mir, A. (2022). SDN Interfaces: Protocols, Taxonomy and Challenges. *International Journal of Wireless and Microwave Technologies*, 12(2), 11–32.  
<https://doi.org/10.5815/ijwmt.2022.02.02>
- Engineering Proceedings | Free Full-Text | Visual Analytics Enabling Optimisation of Downtime. (n.d.). Retrieved 2 August 2024, from <https://www.mdpi.com/2673-4591/65/1/6>
- Introduction to BCDR: DNCT704 Network and Cloud Design and Assessment. (n.d.). Retrieved 1 August 2024, from [https://nzseg.instructure.com/courses/809/pages/introduction-to-bcdr?module\\_item\\_id=41296](https://nzseg.instructure.com/courses/809/pages/introduction-to-bcdr?module_item_id=41296)
- Jeffery Mitchell. (2023, May 25). Connectivity to Azure PaaS services—Cloud Adoption Framework. <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/connectivity-to-azure-paas-services>

- Kaur, K., Mangat, V., & Kumar, K. (2022). A review on Virtualized Infrastructure Managers with management and orchestration features in NFV architecture. *Computer Networks*, 217, 109281.  
<https://doi.org/10.1016/j.comnet.2022.109281>
- mbender-ms. (2023, November 6). *Azure Load Balancer health probes*.  
<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview>
- *Quality of Service (QoS) in Computer Networks: Boosting Performance*. (n.d.). Retrieved 2 August 2024, from <https://www.networkcomputing.com/enterprise-connectivity/quality-of-service-qos-in-computer-networks-boosting-performance>