COLLEGE OF APPLIED BUSINESS AND TECHNOLOGY

Gangahity, Chabahil, Kathmandu-7, Nepal

(Affiliated to Tribhuvan University)

Case Study of Workalaya PVT LTD

Submitted by:

Name: Nabin Shrestha
Roll No: 117

Semester: Fourth

Faculty: Science and Technology
Level: Bachelor
Program: CSIT

Submitted to:

Instructor: Tekendra Nath Yogi

July, 2023

Case Study: Workalaya - A Network Service Provider for Subisu ISP

Introduction:
Workalaya is a prominent Network Service Provider (NSP) that offers a wide range of networking services to Internet Service Provider (ISP) Subisu. With a strong commitment to providing reliable, high-speed, and secure connectivity solutions, Workalaya plays a vital role in facilitating seamless internet access for Subisu's end customers. This case study aims to explore the policies and topologies implemented by Workalaya to ensure efficient service delivery and customer satisfaction.

Objective:
The primary objective of this case study is to understand the networking policies and topologies employed by Workalaya in its partnership with ISP Subisu. This study aims to gain insights into how Workalaya manages its network infrastructure, addressing policies, and security measures to provide quality services to Subisu and its end-users.

Topology:
Workalaya deploys a hierarchical network topology to ensure scalability, flexibility, and ease of management. The hierarchical structure comprises three main layers:

a) **Core Layer:** The core layer constitutes the backbone of the network, responsible for high-speed and reliable data transfer between different segments of the network. At this layer, Workalaya implements redundant and fault-tolerant technologies to guarantee uninterrupted connectivity.

b) **Distribution Layer:** The distribution layer acts as an intermediary between the core and access layers. It facilitates routing and filtering of traffic to optimize network performance and ensure efficient utilization of resources.

c) **Access Layer:** The access layer connects end-users and customer premises to the network. Here, Workalaya implements various technologies such as Virtual LANs (VLANs) and Quality of Service (QoS) to segment traffic, prioritize services, and enhance network security.

Addressing Policy:
Workalaya follows a dynamic IP addressing policy for Subisu's network infrastructure. It employs DHCP (Dynamic Host Configuration Protocol) servers to automatically assign IP addresses to devices connected to the network. Dynamic addressing allows efficient utilization of IP resources and simplifies the addition and removal of devices without manual intervention. Workalaya also implements Network Address Translation (NAT) to translate private IP addresses of Subisu's customers into a single public IP address when accessing the internet. This practice ensures improved security by hiding internal network structures from external threats.

Routing Policy:
Workalaya's routing policy ensures efficient network traffic management and optimal data flow:

- Interior Gateway Protocols (IGPs) like OSPF and IS-IS are used for dynamic routing within the network, adapting to changes in network topology.
- Exterior Gateway Protocols (EGPs) like BGP connect Workalaya to external networks and upstream providers, ensuring efficient data exchange and fault tolerance.
- Load balancing evenly distributes traffic across multiple paths, optimizing resource utilization and network performance.
- Quality of Service (QoS) prioritizes critical services like VoIP and video streaming for uninterrupted delivery during peak usage.
- Route summarization reduces routing table size, simplifying routing decisions and conserving router resources.
- Redundant paths through Equal-Cost Multipath (ECMP) routing enhance network resilience and fault tolerance.
- Policy-Based Routing (PBR) customizes routing rules based on specific criteria, providing greater control over traffic flow.
- By adhering to this routing policy, Workalaya ensures optimal data transmission, reduced latency, and improved network reliability for Subisu and its end-users.

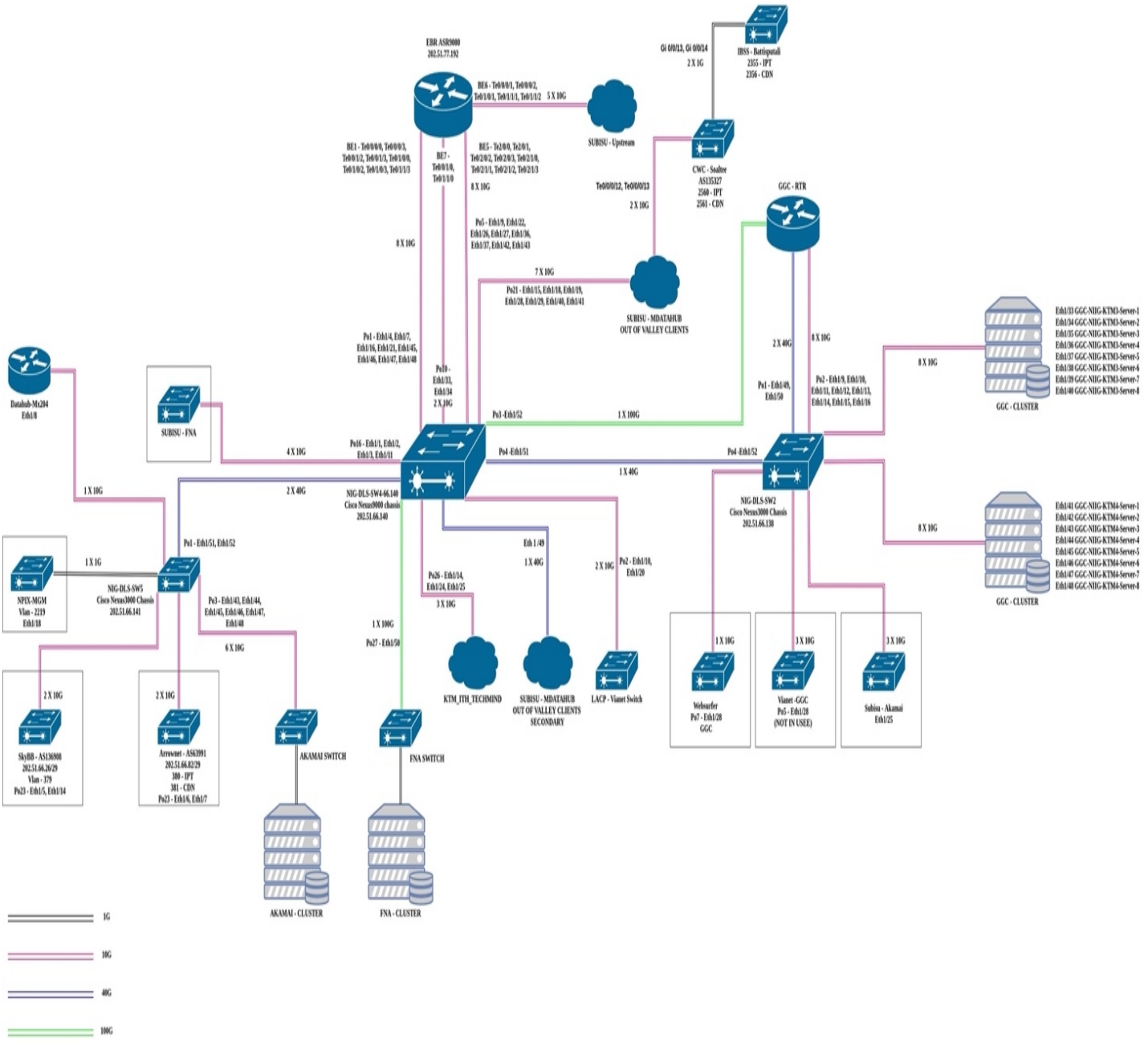
Security Policy:
Security is of paramount importance to Workalaya's network operations. To protect Subisu's infrastructure and customer data, several security policies and measures are employed:
a) Firewalls: Workalaya deploys state-of-the-art firewalls at the network's perimeter and between different network segments to filter and monitor incoming and outgoing traffic. This helps in mitigating potential threats and unauthorized access attempts.

b) Intrusion Detection and Prevention Systems (IDPS): IDPS are implemented to detect and block suspicious activities, such as network intrusion attempts, malware attacks, and DoS (Denial of Service) attacks.

c) Virtual Private Networks (VPNs): Workalaya uses VPN technology to establish secure and encrypted communication channels between Subisu's headquarters, data centers, and remote sites. This ensures the confidentiality and integrity of data transmitted over the network.

d) Regular Audits: Workalaya conducts periodic security audits and vulnerability assessments to identify and address potential weaknesses in the network infrastructure.

Conclusion:
Workalaya's efficient network policies and topologies play a significant role in enabling Subisu to provide reliable and high-quality internet services to its customers. The hierarchical network topology ensures seamless connectivity, while the dynamic addressing policy and NAT support efficient IP resource management. Additionally, the robust security measures safeguard Subisu's network infrastructure and customer data from potential threats.


EBR ASR9000
202.51.77.192
BE6 - Te0/0/0/1, Te0/0/0/2,
Te0/1/0/1, Te0/1/1/1, Te0/1/1/2 5 X 10G
SUBISU - Upstream
Gi 0/0/13, Gi 0/0/14
2 X 1G
IBSS - Battisputali
2355 - IPT
2356 - CDN
CWC - Soaltee
AS13527
2560 - IPT
2561 - CDN
Te0/0/0/12, Te0/0/0/13
2 X 10G
BE1 - Te0/0/0/0, Te0/0/0/3,
Te0/0/1/2, Te0/0/1/3, Te0/1/0/0,
Te0/1/0/2, Te0/1/0/3, Te0/1/1/3
BE7 -
Te0/0/1/0,
Te0/1/1/0
BE5 - Te2/0/0, Te2/0/1,
Te2/0/2, Te0/2/0/3, Te0/2/1/0,
Te0/2/1/1, Te0/2/1/2, Te0/2/1/3
8 X 10G
8 X 10G
Po5 - Eth1/9, Eth1/22,
Eth1/26, Eth1/27, Eth1/36,
Eth1/37, Eth1/42, Eth1/43
7 X 10G
Po21 - Eth1/15, Eth1/18, Eth1/19,
Eth1/28, Eth1/29, Eth1/40, Eth1/41
SUBISU - MDATAHUB
OUT OF VALLEY CLIENTS
GGC - RTR
2 X 40G
8 X 10G
Po1 - Eth1/49,
Eth1/50
Po2 - Eth1/9, Eth1/10,
Eth1/11, Eth1/12, Eth1/13,
Eth1/14, Eth1/15, Eth1/16
8 X 10G
GGC - CLUSTER
Eth1/33 GGC-NIIG-KTM3-Server-1
Eth1/34 GGC-NIIG-KTM3-Server-2
Eth1/35 GGC-NIIG-KTM3-Server-3
Eth1/36 GGC-NIIG-KTM3-Server-4
Eth1/37 GGC-NIIG-KTM3-Server-5
Eth1/38 GGC-NIIG-KTM3-Server-6
Eth1/39 GGC-NIIG-KTM3-Server-7
Eth1/40 GGC-NIIG-KTM3-Server-8
Po1 - Eth1/4, Eth1/7,
Eth1/16, Eth1/21, Eth1/45,
Eth1/46, Eth1/47, Eth1/48
Po10 -
Eth1/33,
Eth1/34
2 X 10G
Po3 -Eth1/52
1 X 100G
Datahub-Mx204
Eth1/8
SUBISU - FNA
4 X 10G
Po16 - Eth1/1, Eth1/2,
Eth1/3, Eth1/11
Po4 -Eth1/51
Po4 -Eth1/52
1 X 40G
1 X 10G
2 X 40G
NIG-DLS-SW4-66.140
Cisco Nexus9000 chassis
202.51.66.140
NIG-DLS-SW2
Cisco Nexus3000 Chassis
202.51.66.138
8 X 10G
Eth1/41 GGC-NIIG-KTM4-Server-1
Eth1/42 GGC-NIIG-KTM4-Server-2
Eth1/43 GGC-NIIG-KTM4-Server-3
Eth1/44 GGC-NIIG-KTM4-Server-4
Eth1/45 GGC-NIIG-KTM4-Server-5
Eth1/46 GGC-NIIG-KTM4-Server-6
Eth1/47 GGC-NIIG-KTM4-Server-7
Eth1/48 GGC-NIIG-KTM4-Server-8
GGC - CLUSTER
Po1 - Eth1/51, Eth1/52
1 X 1G
NPIX-MGM
Vlan - 2219
Eth1/18
NIG-DLS-SW5
Cisco Nexus3000 Chassis
202.51.66.141
Po3 - Eth1/43, Eth1/44,
Eth1/45, Eth1/46, Eth1/47,
Eth1/48
6 X 10G
Eth 1/49
1 X 40G
2 X 10G
Po2 - Eth1/10,
Eth1/20
Po26 - Eth1/14,
Eth1/24, Eth1/25
3 X 10G
1 X 100G
Po27 - Eth1/50
KTM_ITH_TECHMIND
SUBISU - MDATAHUB
OUT OF VALLEY CLIENTS
SECONDARY
LACP - Vianet Switch
1 X 10G
Websurfer
Po7 - Eth1/28
GGC
3 X 10G
Vianet -GGC
Po5 - Eth1/28
(NOT IN USEE)
3 X 10G
Subisu - Akamai
Eth1/25
2 X 10G
SkyBB - AS136908
202.51.66.26/29
Vlan - 379
Po23 - Eth1/5, Eth1/14
2 X 10G
Arrownet - AS63991
202.51.66.82/29
380 - IPT
381 - CDN
Po23 - Eth1/6, Eth1/7
AKAMAI SWITCH
FNA SWITCH
AKAMAI - CLUSTER
FNA - CLUSTER
1G
10G
40G
100G