Migration of Data Center VLAN to IPv6 at NITK Surathkal, India

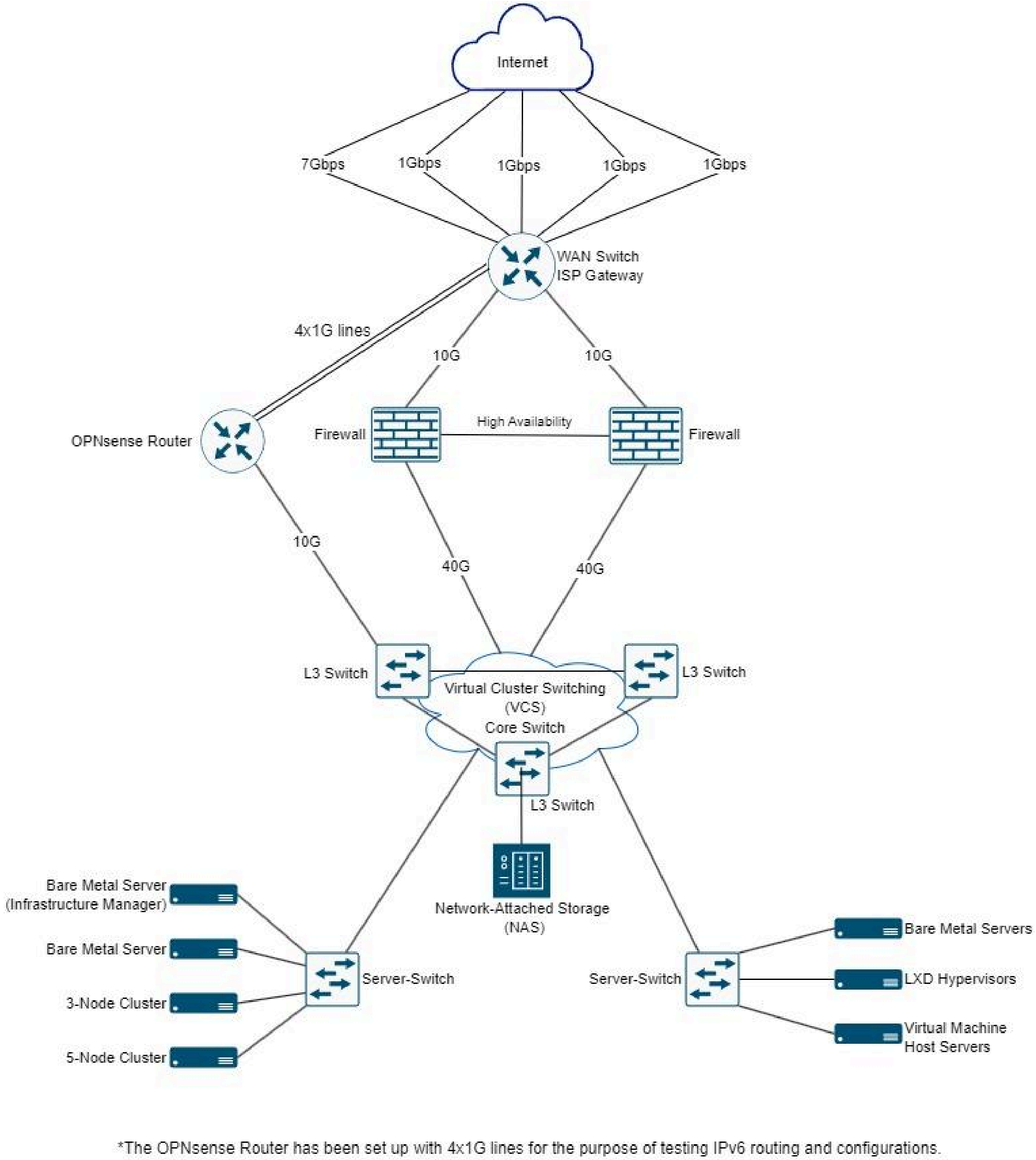
Supported by:

isif asia

Abstract

This document details the process followed to migrate the Data Center (DC) VLAN in National Institute of Technology Karnataka (NITK), Surathkal, India to IPv6. This document also highlights issues encountered during the migration and their corresponding solutions with an aim to serve as a guide for carefully migrating production-level DC VLAN to IPv6. The documentation prefix 2001:db8::/32 has been used throughout this document as per RFC 3849.

1. Data Center VLAN Topology



*The OPNsense Router has been set up with 4x1G lines for the purpose of testing IPv6 routing and configurations.

Figure 1. Topology of NITK Data Center

ISP Gateway: This gateway is provided by an Internet Service Provider (in this case, BSNL), and directs network traffic between the internal NITK network and the external Internet.
In accordance with our IPv6 address plan, the subnet 2001:db8:b0::/50 is statically routed to the IPv6 testbed.

OPNsense router: A security-centric device that manages firewall rules and routing for the NITK network.

Core Switch: A high-capacity switch used to route data between segments, and facilitates connectivity between the distribution switches and the router.

2. Migration Plan

- Enable routing on DC VLAN by configuring IPv6 routing at the core switch.
- Update firewall rules on the NITK OPNsense router to allow incoming traffic for the specific VLAN.
- The router advertisements are set to Router-Only mode. We chose not to allow SLAAC as all the servers in the Data Center VLAN would suddenly get IPv6 addresses and potentially interfere with our observations.
- According to the IPv6 address plan, we chose the allocated prefix for the Data Center VLAN to be 2001:db8:80:c00::/56.
- Once Router Advertisements (RAs) are observed, IPv6 routing must be verified, and the working of applications must be tested:
    - To ensure that IPv6 routing was correct, we created a virtual machine to check connectivity for both outgoing and incoming traffic.
    - Services such as DNS and DHCPv6 operate in the data center VLAN. These applications are to be migrated to IPv6.

Note:

- The infrastructure in the Central Computing Center and containers provisioned for students should ideally be in different subnets. However, due to the current design, it is not possible to separate critical infra traffic from provisioned containers. This issue will be revisited in the future and resolved.

3. Core Switch Configuration

3.1 Commands

The following commands are executed on the core switch (`10.5.0.1)`. These commands are specific to Brocade.

```
# configure
# rbridge-id 1
# interface Ve 367
# ipv6 nd prefix 2001:db8:80:c00::/56
# ipv6 address 2001:db8:80:c00::1/56
# exit
# exit
# copy running-config startup-config
```

3.2 Explanation

- `interface Ve 367`
  - This specifies the ID of the VLAN that we make modifications to. In this case, the Data Center VLAN has an ID of 367.
- `ipv6 nd other-config-flag`
  - If this option is used, the DHCPv6 server gives configuration information (such as the DNS server), excluding the IP address information.
  - This option was skipped during the migration of the Data Center VLAN, as routing may be impacted when DHCPv6 is missing.
  - We plan to use a container to test and observe different Router Advertisement modes.
- `ipv6 nd prefix 2001:db8:80:c00::/56`
  - The router advertisement messages advertise a prefix of 2001:db8:80:c00::/56

4. Troubleshooting

4.1 Verification

- Check that the configuration in `/etc/netplan/01-netcfg.yaml` matches the requirements.
- Check the routing table with `route -6 -n`. This should show that the gateway is set. However, we also observed that the route table contained stale information.
- Verify that IPv6 Neighbor Discovery is enabled on the VLAN interface (ID 367) using `show ipv6 nd interface ve 367`.
- Check the IPv6 neighbors on the VLAN interface (ID 367) using `show ipv6 neighbor ve 367`.

4.2 Ping and Traceroute Testing

- Attempted to ping the IRIS Gateway (2001:db8:80:c000::1), which failed.
- Successfully pinged 2001:db8:80:c00::1.
- Pinging an external domain (eg. ipv6.google.com) also fails.
- Edited /etc/netplan/01-netcfg.yaml to add the gateway manually (2001:db8:80:c00::1). The route and next-hop destination are explicitly specified through this.
- Confirmed successful ping to 2001:db8:80:c000::1 after updating the network configuration.
- Attempted to ping ipv6.google.com, which failed, indicating a potential firewall issue.

4.3 Analysis

4.3.1 Analysis on Data Center VLAN - Interface ID 367

- The live logs on the firewall showed that packets were not being forwarded from the core switch.
- Identified a potential issue with incorrect routes learned from previous configurations. Available options were to:
    - Shut down and restart the interface to reset the incorrectly learned routes, which was done while migrating the IRIS VLAN. However, this solution is impractical for Data Center VLAN.
    - Configure IPv6 on the Central Computing Center (CCC) Lab VLAN (interface ID 302). This would allow us to experiment with potential solutions without disrupting services that run on the Data Center VLAN.

4.3.2 Analysis on CCC Lab VLAN - Interface ID 302

- Successfully pinged addresses internal to NITK, but encountered issues reaching external addresses.
- The route for 2001:db8::/36 was disabled on the NITK OPNsense router.
- Resolved the problem by enabling the route, allowing successful pings to external domains from the CCC Lab VLAN.

4.3.3 Verification on Data Center VLAN

- Removing the static gateway resulted in the inability to access external domains but successful pings to the core switch interface and IRIS.
- We have temporarily added the IPv6 gateway manually in order to ensure connectivity.
- Restarting the interface allowed IPv6 routing to work without specifying the gateway explicitly. However, this might not be practical for all cases, and needs to be investigated further.

5. IPv6 Address Modification for Services

5.1 Public and Private Services

We use the following address patterns for public and private services:

- Public Services - 2001:db8:80:c00:**10:17:0:208**/56
- Private Services - 2001:db8:80:c00:**0:17:0:208**/56

In case we do not wish to modify the IP address, a firewall rule may be added to permit incoming connections. However, it is important to note that this may result in a large number of firewall rules. It is recommended to use an address pattern to distinguish between public and private services.

5.2 Directly Exposed Services

- The server should be running UFW.
- The load balancers currently do not support IPv6. As the Data Center VLAN has now been migrated to IPv6, we can enable IPv6 on load balancer machines and add these IP addresses to DNS.
- For web servers:

- The recommended method is to use load balancers. In case this is not possible, provide a public IPv6 address.
- It is possible to use raw TCP on Nginx, which was followed in IRIS to provide connections to the development server.
- However, there is a challenge in involving external port number changes, potentially limiting compatibility for some applications.