Research Paper Engineering

Automation and Analysis of Enterprise Campus Network Design

Tushar Krishna Yaratha	School of Electronics Engineering Vellore Institute of Technology Vellore, India
Archisman Banerjee	School of Electronics Engineering Vellore Institute of Technology Vellore, India
Arun M	School of Electronics Engineering Vellore Institute of Technology Vellore, India

ABSTRACT

Internet is the need of the hour these days. Every enterprise has to be connected to the internet 24*7 to optimize its performance. However with the growing demand for internet, ensuring connectivity is becoming a major challenge and concern these days.
A flat enterprise network is the one where all the PCs, servers and IP Phones are connected to a single switch. A flat network does not also have subnets. All devices on the subnet are on the same broadcast domain. This adds to a lot of network congestion. Therefore, we employ a hierarchical network design.
The network design has to be scalable and redundant as well. The objective of this project is to design an industry standard hierarchical layout of a campus networking topology using various routing and switching protocols like OSPF, BGP, EIGRP, STP, HSRP, VTP, etc. in accordance to customer/enterprise requirements. Few tedious tasks need to be automated in a network. This was done using various tools.

KEYWORDS OSPF, EIGRP, Embedded Event Manager, Network Architecture, GNS3

Introduction

A flat enterprise network is the one where all the PCs, servers and IP Phones are connected to a single switch. A flat network does not also have subnets. All devices on the subnet are on the same broadcast domain. This adds to a lot of network congestion. Therefore, we employ a hierarchical network design. The objective of this project is to design a hierarchical layout of a campus networking topology. Some of the analysis which is done on this network design can be automated. This automation will be useful in making the monotonous analysis of networks easier.

Design

In GNS3, we have simulated a flat topology using 5 hosts and a switch. They are in the same broadcast domain. The image of the flat topology is appended below in Fig1.

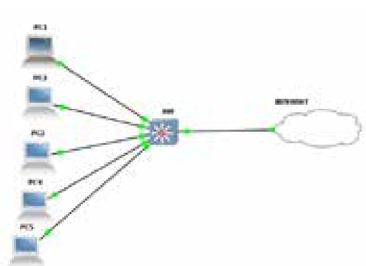

Fig1. Flat Topology

The hierarchical topology has been configured with a 3 layer topology. The three layers are Core, Distribution and Access Layers. The Core and Distribution Layers have routers. While, the access layer has switches. The broadcast domains are neatly segregated in this type of design. The image of the Hierarchical Network Design is appended below in Fig2.

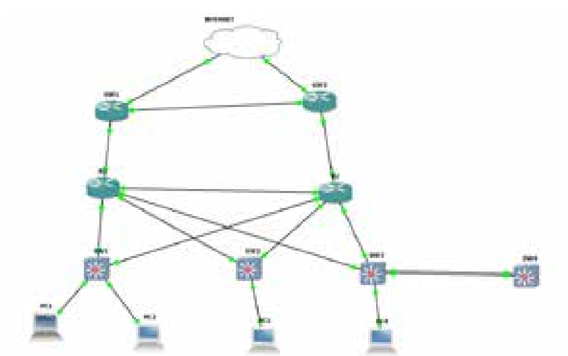

Fig2. Hierarchical Topology

IMPLEMENTATION AND OBSERVATIONS

In the flat topology, the network congestion was observed to be really high. Fig3 proves the same.

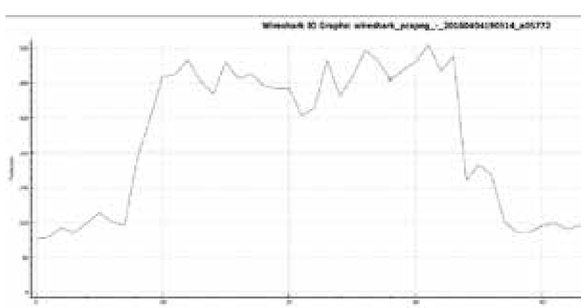

Fig3. Packets/s in flat topology

ISSN - 2250-1991 | IF : 5.215 | IC Value : 77.65

The average Round Trip Time(RTT) was observed to be 38 ms. The packets/s were observed to be 560 approximately. This is quite a lot of traffic and the congestion might sometimes cause undesirable consequences.

In the implementation of the hierarchical network topology, various protocols such as VLAN Trunking Protocol (VTP), Dynamic Host Configuration Protocol (DHCP), Open State Path First (OSPF), Network Address Translation (NAT), Virtual Router Redundancy Protocol (VRRP) and Border Gateway Protocol (BGP) were used. The network congestion was observed to be a lot lesser in this topology. Fig4 proves the same. The network congestion was observed to be approximately 180 packets/s. The Round Trip Time (RTT) was observed to be 33 ms.

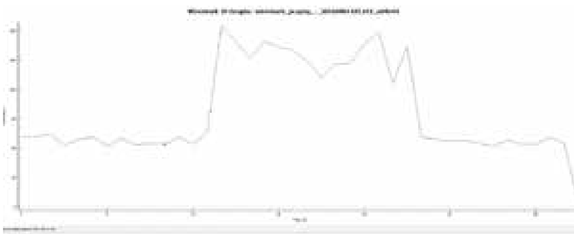

Fig4. Packets/s in hierarchical topology

Few additional features such as syslog, Embedded Event Manager (EEM), Role Based CLI Access and Tool Code Language (TCL) were tested in the hierarchical topology of the network.

Syslog is a method to collect messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. A SYSLOG service simply accepts messages, and stores them in files or prints them. We have used KIWI Syslog Server for this purpose.

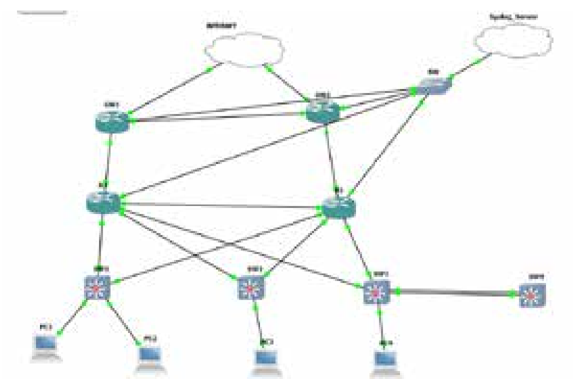

Fig5. Network Topology with Syslog Server

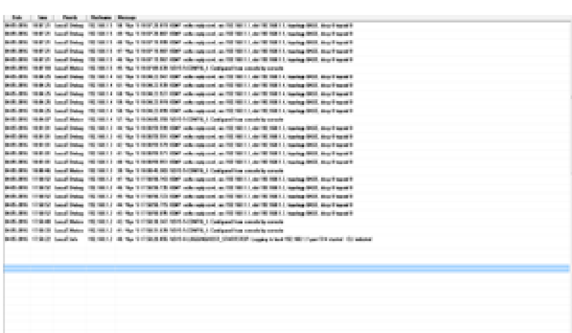

Fig6. Sample output of the logs

Fig6 shows the results of the logs which have been populated on the Syslog Service. These logs are the debug ICMP packets.

A packet analysis of the link between R1 and GW1 has been analyzed. This was done using two protocols i.e. Open State Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP). We observe in Fig7 that in EIGRP, there are frequent updates. Therefore, the traffic is a lot more as compared to OSPF. In Fig8, we observe that the traffic is lot lesser.

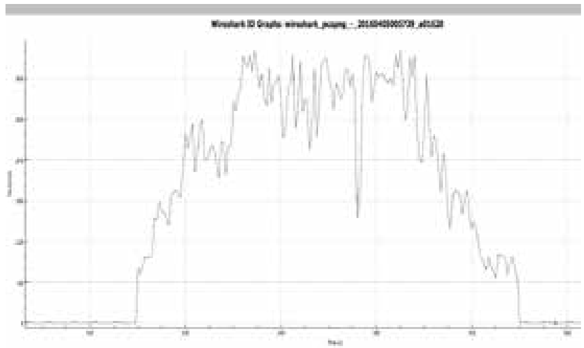

Fig7. EIGRP packet analysis

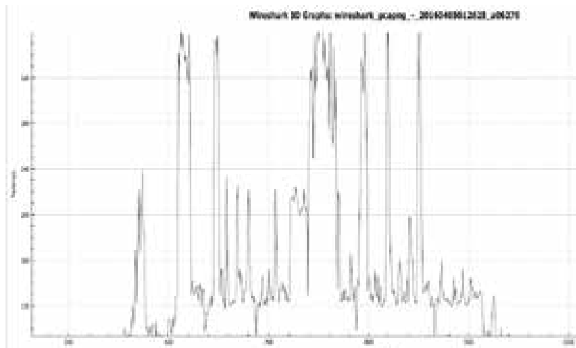

Fig8. OSPF packet analysis

Cisco IOS Embedded Event Manager (EEM) is a powerful and flexible subsystem that provides real-time network event detection and automation. It gives you the ability to adapt the behavior of your network devices to align with the needs of the network. We have incorporated various features of the EEM in the project such as getting the interface up if its shutdown and not allowing debugs as it consumes a lot of processing.

We used Cisco's EEM to keep the interfaces always up. So, whenever we try to shut an interface, it comes back up again. In Fig9 we observe that when we try to shut down one of the interfaces, it comes back again due to EEM.

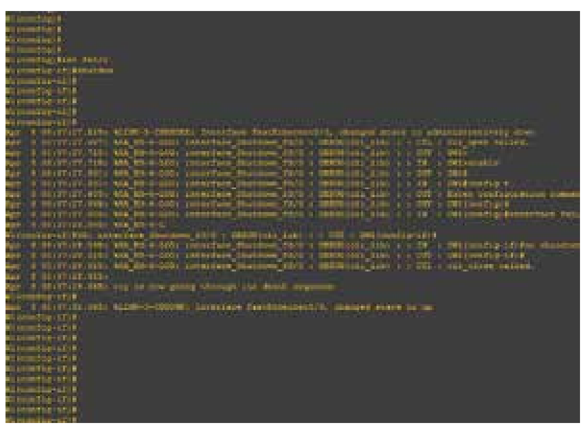

Fig9. Interfaces are always kept up

Debugs are really CPU intensive. To prevent it, we have used EEM to prevent the debug command by automatically selecting the no option. Fig10 shows the same.

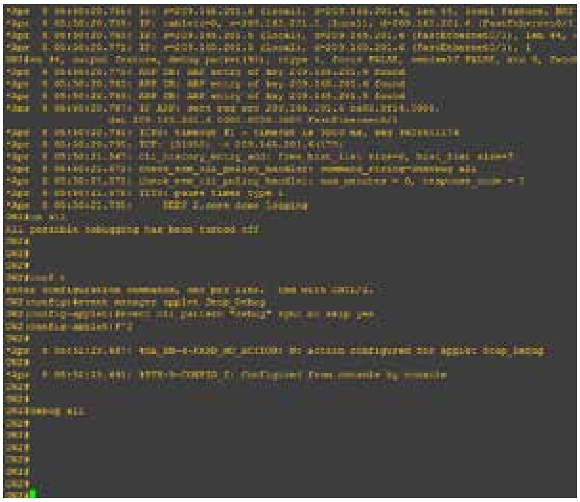

Fig10. Preventing the debug command

We observe in Fig11 that the PC is not able to ping for a while as the port was shut down due to heavy traffic. The interface at the gateway is marked down when the traffic increases considerably. This was also done using EEM.

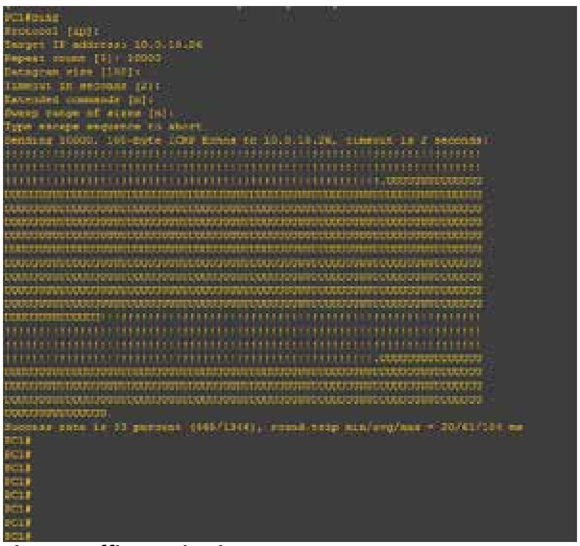

Fig11. Traffic Monitoring

We observe in Fig11 that the gateway is unreachable for a while as the traffic load was too high.

The "reload" command in Cisco devices will lead to the loss of the Running Configuration present on the Cisco devices. Therefore, the reload command was disabled using EEM. Fig12 shows that the reload command is being entered, but we observe a syslog message which says that the reload command is disabled.

Fig12. Prevention of the Reload Command

Another script was used to create loopbacks. The script which is run automatically creates loopbacks based on the input given i.e. number of loopbacks. Fig13 shows that 3 loopbacks were created with their ip addresses.

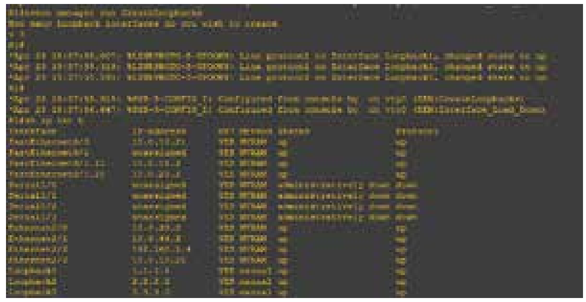

Fig13. Script to create loopbacks

The Tool Control Language (TCL) script was used to test the reachability to other network devices. In Fig14, we see that three addresses are reachable.

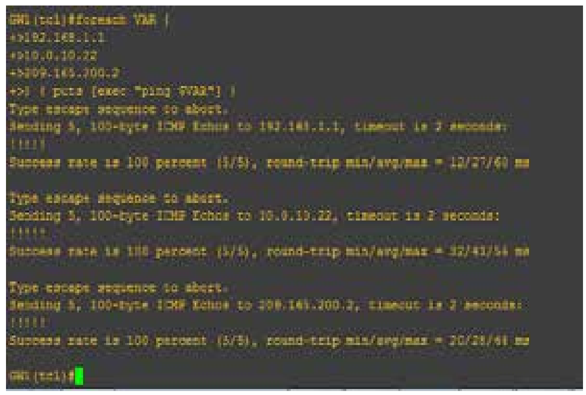

Fig14. TCL script to test the reachability

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration.

Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible.

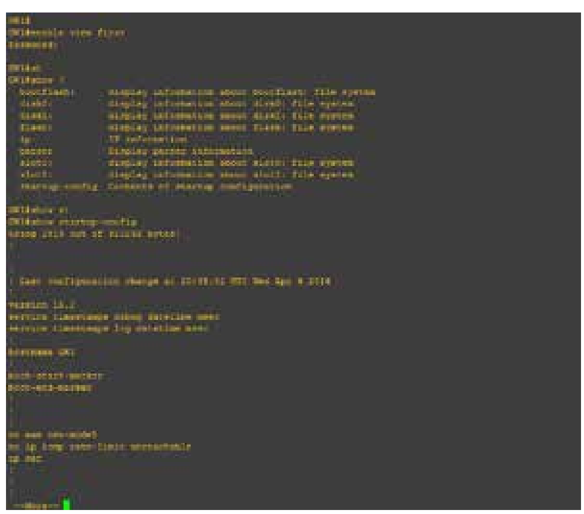

Fig15. First User

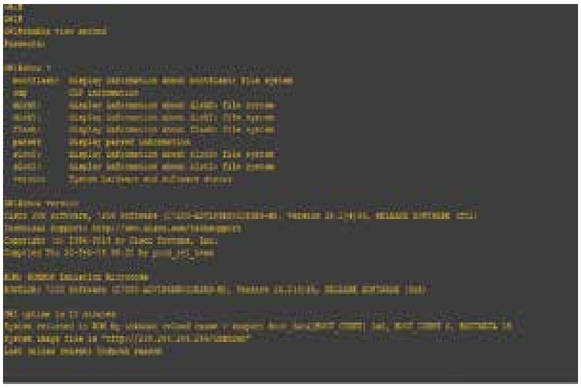

Fig16. Second User

In Fig15, we observe that the first user is given access only to the “show ip interface brief” and the “show startup-config” commands. While in Fig15, we observe that the user is given access to “show cdp neighbours” and “show version” commands. In this way the network administrator can give preferential access to the users.

IV.CONCLUSION

The difference between the flat topology and the hierarchical topology was analyzed with the help of GNS3 and Wireshark. The network congestion was observed to be pretty low in the case of the hierarchical network design as compared to the flat topology. Therefore, the hierarchical topology is preferred in most of the cases.

Problems like the interfaces of a network device going down, the debugs are a huge problem in a network. Therefore, EEM was used to tackle these problems. TCL was used to test the reachability to multiple devices. Role Based CLI Access on the other hand gives preferential access to the user.

These methods, if employed on a real time network, will be really useful in administering the network.

V.REFERENCES

[1] Enterprise Networking Planet
[2] Official GNS3 Documentation
[3] RFC 2328
[4] RFC 4271
[5] RFC 1541
[6] Cisco Documents on various protocols