Design and Performance Analysis of Complex Switching Networks through VLAN, HSRP and Link Aggregation

Dr.R. Vadivelu and Dr.S. Malathy

Abstract--- *An overview of Layer 2–Switching and its load balancing technique is analyzed in this paper. The work elucidated here gives out the improvement of network performance by decreasing overhead. In this paper it shown that the aggregation and linking is done via Virtual Local Area network (VLAN). Devices of VLAN technology include host, switch and routers Switch used to connect multiple devices in the network. If multicast is not required by a host, then it will not send to that* switch***.** *Switch connects multiple hosts and establish suitable path over the network. Router enables VLAN sharing with external users. Sharing of information is possible in host, switch and router in the network. But quality of service (QoS) is not good as expected. To improve the QoS and performance, link aggregation is performed. Link aggregation is a technology used in combining (aggregating) multiple network connection in parallel to increase throughput beyond what a single connection could sustain and to provide redundancy in case one of the link failure. Layer 2 typically occurs across switch port which can be either physical port or virtual ones managed by VLAN, Hot Standby Router Protocol (HSRP) and link.*

Keywords--- *VLAN, QoS, HSRP, Layer2 Switching, Link Aggregation.*

I. INTRODUCTION

A network is a series of nodes or points that are interconnected by communication paths. Networks can interconnect with other networks that contain sub networks [1]. The most common topology or general configurations of networks include the bus, star, token, ring, and mesh topologies. Networks can also be characterized in terms of spatial distance as local area networks (LANs), Metropolitan Area Networks (MANs), and wide area networks (WANs) [2].Network can also be characterized by the type of data transmission technology and types of physical links such as optical fiber, coaxial cable, and Unshielded Twisted Pair. Large telephone networks and networks using their infrastructure have sharing and exchange arrangements with other devices so that larger networks are created. Internet Protocol Address (or IP Address) is a unique address that computing devices used to identify itself and communicate with other devices in the Internet Protocol network. Any device connected to the IP network must have a unique IP address within its network. An IP address is analogous to a street address or telephone number in that it is used to uniquely identify a network device to deliver mail message, or call a website [3]. Sub netting is the process of creating new networks (or subnets)by stealing bits from the host portion of a subnet mask.

Dr.R. Vadivelu, Associate Professor, Department of Electronics and Communication Engineering, Sri Krishna College of Technology, Kovaipudur, Coimbatore, India. E-mail:r.vadivelu@skct.edu.in

Dr.S. Malathy, Associate Professor, Department of Electronics and Communication Engineering, Sri Krishna College of Technology, Kovaipudur, Coimbatore, India. E-mail:malathy.s@skct.edu.in

There is one caveat: stealing bits from hosts creates more networks but fewer hosts per network. Thus, every time a network is sub netted, addresses are lost. In sub netting, a network is divided into smaller subnets with each subnet having its own subnet address [4].

II. IP ADDRESS CLASSES

Classless inter-domain routing is a method for allocating IP addresses and routing Internet Protocol packets. IP Address consists of two groups of bits in the address. The MSB is the network address which identifies subnet and the LSB is the host identifier that specifies a particular interface of a host on that network.

Network design for IPv4 sized the network address as one or more 8-bit Class full groups, resulting in the blocks of Class A, B, or C addresses. Classless Inter-Domain Routing allocates address space to Internet service providers and end users on any address bit boundary, instead of on 8-bit segments. In IPv6 consist 64 bits [5].

III. EXISTING VLAN TECHNOLOGY

The optimal load balancing in telecommunication networks based on multiple spanning tree routing. This is the case in switched Ethernet networks where the operator configures different routing spanning trees and assigns VLAN to one of the spanning trees [6].

Modeling and solving three load balancing objectives is considered: minimization of the average link load with:

- Guaranteed optimal worst case link load
- Guaranteed optimal average link load, and
- The min-max optimization of link loads.

Both the efficiency and the efficacy of the different solution techniques for optimization criteria are analyzed**.** This observation shows that it is possible to optimize load balancing with a small number of spanning trees, thus, not significantly penalizing the processing overhead in the switches. Virtual Router Redundancy Protocol (VRRP) is developed to fortification the LAN network for single point of failure and not supports the load balancing.

Enhanced Virtual Router Redundancy Protocol (EVRRP) handle multi load balancing of different subnet. Extended Enhanced Virtual Router Redundancy Protocol (EEVRRP) support load balancing between two or more segment having multiply-node in network on same cluster of router. VLAN ID, VRRP group ID on the interface are binded. Idea of load-balancing between multi subnet made using single VRRP group.

Round-Robin technique introduced for load-sharing between many PC of single network. Normally, security and access control policies rely on features from the host operating system. But we have the necessity to check it is correct. We investigate the feasibility of using the network to enforce these policies. First, a secure VLAN architecture that can be used completely to secure network from unauthorized access is described. Second, IP Telephony is applied.

IV. NETWORK ANALYSIS

Quick Emulator (QEMU) simulator used to construct virtual networks restricted by efficiency and security. Multiple virtual machines (VMs) are connected to the host machine so as to construct an emulated network

environment efficiently and effortlessly. This paper provides the component called Vob sub (VS) Filter for every QEMU guest to forward network packets to the accurate guest system. All the network packets coming from the emulated network card are considered to go through VSFilter, and then delivered to physical network interface. Any disallowed packets are redundant, while allowed packets are forwarded to the selected destination directly. As VSFilter filters packets and only forward allowed packets to the exact destination, VMs process fewer packets than they do when Ethernet tap networking is used separately. Therefore better performance can be expected, especially if the host machine suffers from heavy network traffic. Furthermore, there is only one tap device needed and this reduces the number of virtual network card and the traffic load on the host. VSFilter blocks outgoing packets send to the physical machines by specifying its MAC address. This means VMs cannot steal packets from these physical machines and eavesdrop on physical machines either. Even if some malicious codes are running in VMs, it wouldn't cause any damage to the host machine [7]. Thus, VSFilter can protect the security of the physical machine effectively in the virtual network environment. In this way, security can be better than Ethernet tap network.

V. COMMUNICATION ON VLAN

Advanced Layer-3 switches achieve high-speed IP packet forwarding by storing parts of the header information. Once the IP traffic is congested on an L3 switch, the flow cache is easily exhausted, decreasing the IP packet forwarding performance. VLAN, a virtualization technology at the data-link layer, is widely used in many organizations because it provides design flexibility. Distributed virtual routing, which dynamically controls the packet exchange for each VLAN to suppress the consumption of flow caches. The reduction of the relaying flows through the real network data is evaluated. Dynamic control of redundant traffic is required in VLAN environments. Redundancy is found out by routing point migration mechanism using VRRP. This mechanism can be expected to improve performance and that it is feasible with real network devices. Cisco's VLAN Trunk Protocol (VTP) reduces administration in a switched network. Solutions to both of these issues involve considerable manual re-configuration which transcends from manually changing VTP modes, domain names to manually missing or deleting un-wanted VLANs. The problem of finding the physical layer topology of large, heterogeneous networks that comprises multiple VLANs and may include uncooperative network node. Finding a layer-2 network topology for a given incomplete input is an NP-hard problem even when the network comprises only two VLANs and the network contains one loop is a co-NP-hard problem. An algorithm is designed for wide-spread networks that may contain uncooperative devices. For such networks the algorithm discovers the topology for each VLAN that merges the network topology in O (n3) time, where n is the number of internal network nodes. Another algorithm is designed for smaller, active networks where each device in the network provides access to their MIB and few AFT entries are missing. By implementing VLAN, accurate result is obtained [8].

Flat Network

Flat network is a network without IP subnet planning .Its topology is not divided in to layer or modules. Every station on a flat network receives a copy of every broad cast message sent. The typical architecture for a small LAN is workstations, printers, and servers interconnected to one or more hubs or to a small switch in a flat topology, as illustrated in Figure 1.

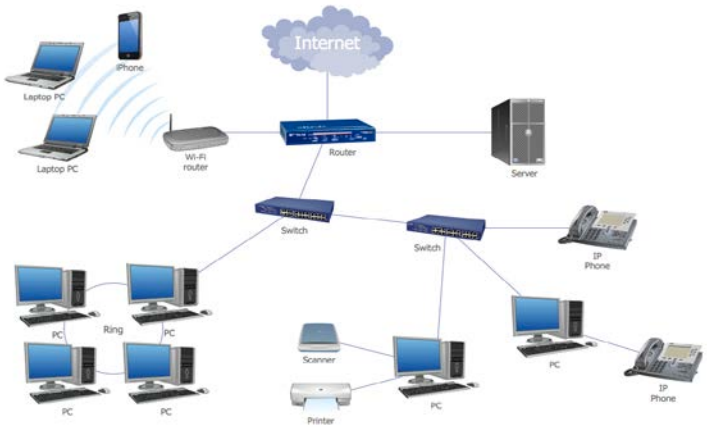

Figure 1: LAN Network

The workstations, printers, and servers here utilize a MAC process, such as Ethernet's carrier sense multiple access collision detect (CSMA/CD), controlling access to the shared bandwidth. These devices are all part of the identical bandwidth and broadcast domain and have the ability to impact the throughput of other devices and cause delay in traffic delivery. For networks with high bandwidth requirements, caused by plentiful users and or traffic-intensive applications, network designers recommend attaching the workstations, printers, and servers to switches rather than hubs. Because hubs work at the physical layer (Layer 1) and switches work at the data link layer (Layer 2), the network is segmented into multiple smaller collision domains [9]. This means that a small number of devices contribute for bandwidth at any one time, rather than a "free-for-all" in which everyone competes for the bandwidth. The number of nodes in a shared-medium LAN and the number of LAN segments are design parameters that should be considered when determining the use and placement of switches or hubs in the network. Because switching is a more expensive solution than using hubs in a shared-medium environment, for some organizations, hubs, or a combination of hubs and switches, might be the best solution. For organizations with high bandwidth and scalability requirements, switches should be used in place of hubs, dedicating each switch port to a single device. The use of switches in this scenario provides dedicated bandwidth to each workstation, printer, or server.

Devices connected Ethernet LANs in a bridged network or switched network are part of the same broadcast domain. Switches forward broadcast frames out all ports (in contrast to routers, which segment networks into separate broadcast domains [10].A single broadcast domain as shown in Figure 2 should be limited to a few hundred devices so that these devices are not plagued by the handing out of broadcast traffic. Introducing hierarchy into a network design by the addition of routers cuts down on the amount of broadcast traffic sent across the network.

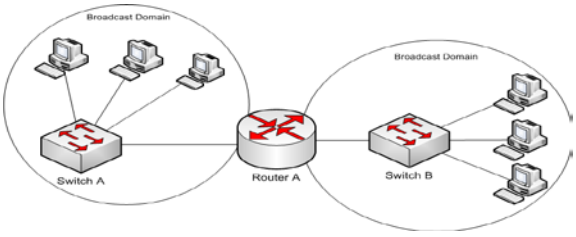

Figure 2: Broadcast Domain

A flat network topology, as illustrated in Figure 1 is adequate for small networks and is implemented using Layer 2 switching. This is no chain of command with a flat network design, and since each network device contained by the topology is performing the same situation, a flat network design can be easy to implement and manage. The flat network topology is not separated into layers or modules and can make troubleshooting and isolating of network faults a bit more challenging than in a hierarchical network. Switched networks by nature will boost performance over shared media devices in use today, first and foremost by reducing the size of collision domains. Grouping users into logical networks will also enlarge performance by preventive broadcast traffic to users performing similar functions or within individual workgroups. Additionally, less traffic will need to be routed, and the latency added by routers will be reduced.

Manual Configuration and Limitation

In the existing system, when there is regular interruption, there is no redundancy in the network setup. This is the main drawback of this system.LAN can communicate and any host can be plugged into any port to access network. Network is less protected. The concerns have to manually divert the traffic to the backup whenever the active link fails. It takes a lot of time and within the period they lose the network time and it eventually reflects in the unconstructive performance of the network.

VLAN Benefits

Switched networks by nature will boost performance over collective media devices in use today, primarily by dropping the size of collision domains. Grouping users into logical networks will also boost performance by limiting broadcast traffic to users performing similar functions or within individual workgroups. Additionally, less traffic will need to be routed, and the latency added by routers will be reduced**.** VLANs provide an easy, flexible, less costly way to modify logical groups in changing environments. VLANs make large networks more manageable by allowing centralized configuration of devices located in physically diverse locations.VLANs provide sovereignty from the physical topology of the network by allowing physically miscellaneous workgroups to be sensibly associated within a single broadcast domain. If the physical infrastructure is already in place, it now becomes a simple matter to add ports in new locations to existing VLANs if a department expands or relocates. These assignments can take place in advance of the move, and it is then a simple matter to move devices with their accessible configurations from one location to another. The old ports can then be decommissioned for future use, or reused by the department for new users on the VLAN [11].

VLANs have the ability to provide additional safety not available in a shared media network environment. By nature, a switched network delivers frames only to the predictable recipients, and transmits frames only to other members of the VLAN. This allows the network administrator to segment users requiring access to insightful information into separate VLANs from the rest of the general user community in spite ofof physical location. In addition, monitoring of a port with a traffic analyzer will only view the traffic coupled with that particular port, making discreet monitoring of network traffic more difficult [12].In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations. For instance, in a broadcast domain having 10 users, if the broadcast traffic is intended only for 5 of the

users, then placing those 5 users on a separate VLAN can reduce traffic. Compared to switches, routers need more processing of inward traffic. As the volume of traffic passing through the routers increases, so does the latency in the routers, which results in reduced performance. The use of VLAN's reduces the number of routers required, because VLAN's create broadcast domains by switches instead of routers. Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN's be capable of controlling broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion. Switching mechanisms refer to the mechanisms used to eradicate data from an input channel and place it on an output channel. Network latency is highly dependent on the switching mechanism used.

VI. LOAD BALANCING

Load balancing is dividing the amount of work that a computer has to do between two or more computers so that more work gets done in the same amount of time and, in general, all users get served faster. Load balancing can be implemented with hardware, software, or a combination of both. Typically, load balancing is the main reason for computer server clustering [13].On the Internet, companies whose Web sites get a great deal of traffic usually use load balancing. For load balancing Web traffic, there are several approaches. For Web serving, one approach is to route each request in turn to a different server host address in a domain name system table, round-robin fashion. Usually, if two servers are used to balance a work load, a third server is needed to determine which server to assign the work. Since load balancing requires multiple servers, it is usually combined with failover and backup services. In some approaches, the servers are distributed over different geographic locations.Distributed server load balancing products can also provide disaster recovery services by redirecting service requests to a backup location when a catastrophic failure disables the primary site. End-user requests are sent to a load-balancing device that determines which server is most capable of processing the request [14]. It then forwards the request to that server. Server load balancing can also distribute workloads to firewalls and redirect requests to proxy servers and caching.

VII. SAMPLE NETWORK

A basic HSRP network is shown in Figure 3. Router is connected through the gateway and communicates through the internet. In sample network shown, PC's default gateway is configured to IP address 10.1.1.3. However, that IP address doesn't point to a real device; instead, it serves as the virtual IP address for whichever router is the primary.

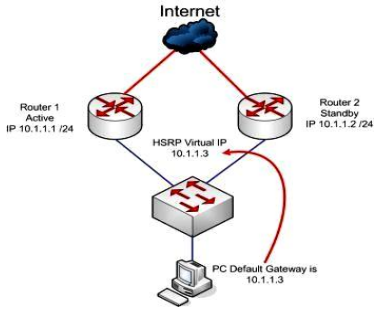

Figure 3: Sample HSRP Network

HSRP Function

When using HSRP, routers can either be primary or standby. If the primary router doesn't send out the HELLO packet to the standby router for a period of time, the standby router assumes the primary router is down and thus takes over. The standby router then assumes responsibility for the virtual IP address and begins responding to the virtual Ethernet MAC address to which the virtual IP address is pointing [15].The primary and standby routers exchange HSRP HELLO packets so that each knows the other router is there. These HELLO packets use multicast 224.0.0.2 and UDP port 1985. The most basic form of HSRP has been available since IOS 10.0, but there have been newer features released in the 11 and 12 versions of the IOS. What determines the active router? First, it can be configured with a priority number to determine it, and then it's by the highest IP address. The default priority number is 100; a higher priority number signifies the preferred router. Of course, when setting up router redundancy, it is not limited to just two routers and can set up groups of routers that work together and have multiple "standby" routers. Configuration of HSRP is accomplished that almost all HSRP configurations in the router's Interface Configuration Mode using the standby command. Let's look at the steps taken to configure the network shown in Figure 4.

For Router 1: Configure the IP address on the Ethernet interface. Configure the standby IP address. Configure standby preempt. (With preempt, Router 1 will always be the primary router as long as it's available.)

For Router 2: Configure the IP address on the Ethernet interface and configure the standby IP address. Configure standby priority to be less than 100.

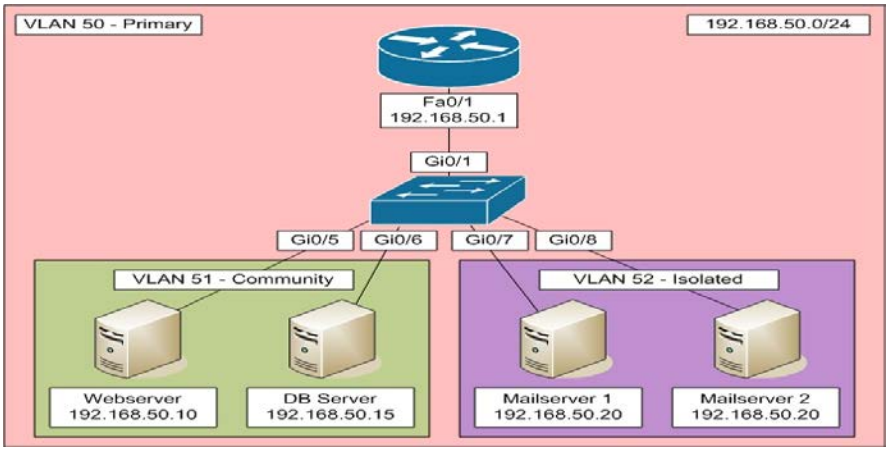

Figure 4: Topology for Proposed VLAN System

Figure 4 shows the proposed system topology. In this topology two switches, two routers and clouds are used. Switches are used for VLAN creation and grouping. Routers are used to communicate the inter VLAN and HSRP is done in the router for The connectivity of the normal LAN network in which all the system in network can communicate with all other system in the network. Due to this, when new systems add to the network it will send broadcast messages to all the systems. Therefore overhead and traffic in the network increases. To reduce the overhead and traffic in load balancing in the network the connectivity checking made on the configured network as shown in Figure 5.

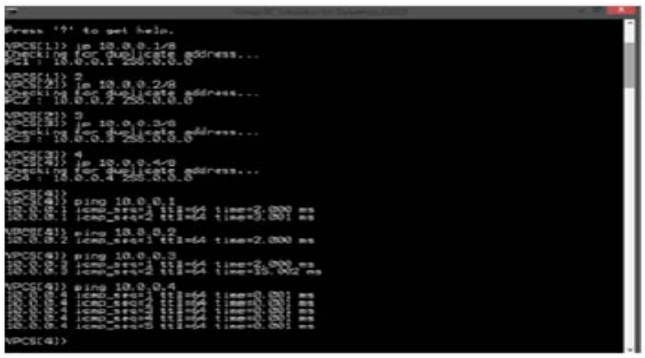

Figure 5: Connectivity Checking

VIII. IMPLEMENTING VLAN INTERFACE

After creating VLAN in the switches, implement them in the interfaces to activate VLAN. After Creating VLAN and activating those in interface only the host from same VLAN can communicate with each other. Host from one VLAN can't communicate with other VLAN. To communicate with different VLANs, layer 3 devices called router is used. After configuring the router for communication between different VLANs, the connectivity of the different VLAN is checked. HSRP should be configured in the router and the status of the router 1 after configuring the HSRP is shown. In this one interface in active and other is standby. This is due the different priority value interface 0/0.1 has 150 value and interface 0/0.2 has 100 value. The status of the router 2 after configuring the HSRP is shown. In this one interface in active and other is standby. This is due the different priority value interface 0/0.1 has 100 value and interface 0/0.2 has 150 value. When one router goes fail then the other router becomes both active. To check this one router is shut down and the status is checked. Hence auto redundancy is achieved. Figure 6. Shows shutting down router2 and Figure 7 shows packet captured on load balancing.

Figure 6: Shutting Down Router 2

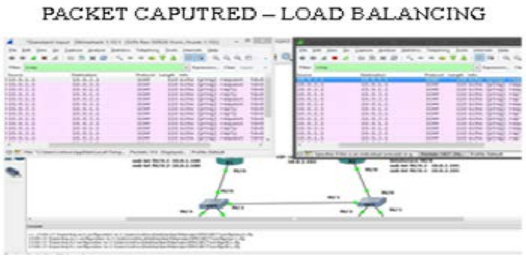

Figure 7: Packet Captured and Load Balancing

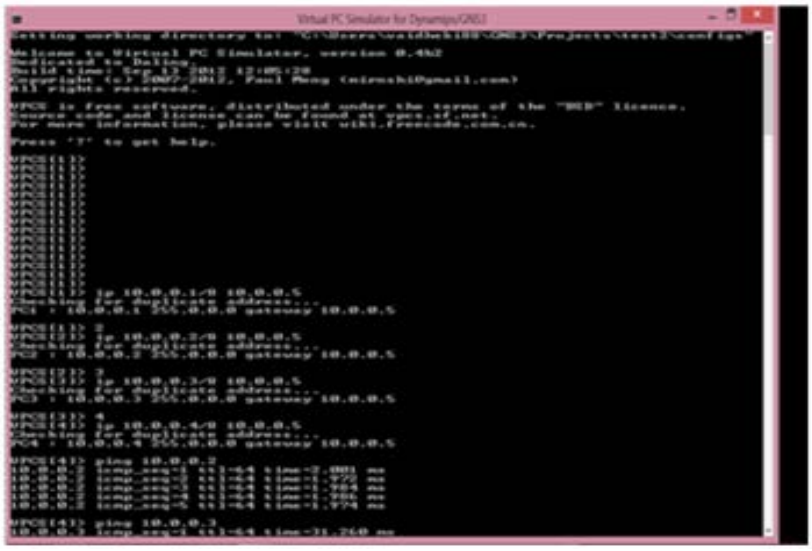

Figure 8: VPCS Output

IX. RESULT AND CONCLUSION

The Virtual PC simulator output for the VLAN concept is depicted in Figure 8.In that ping of the data is occurring and viewed. A common gateway is there and the data transmission occurs in the network through that gateway to the different network. Dynamic control of redundant traffic occurring in VLAN environments is discussed and the effect of redundancy in actual networks is measured and, through experiments, the effects on transmission of a routing point migration mechanism using HSRP is shown. It is understood clearly that the mechanism improves the performance and that it is feasible with real network devices. Experiments on larger scale networks that include more complex topologies are subjected to futurework.

REFERENCES

[1] M. Ajtai, J. Komlos and E. Szemeredi, “An O (nlogn) sorting network”, Proc. 15th ACM Symp. Theory Comput., Pp. 1–9, 1983.

[2] IEEE Computer Society LAN Man Standard Committee, “Wireless LAN Medium Access Control (MAC) and Physical Layer Specification”, IEEE Standard 802.11. IEEE New York.

[3] K.J. Negus, A.P. Stephens and J. Lansford, “Home RF: Wireless Networking for the Connected Home”, 2000.

[4] A. Ferreira, A. Goldman and J. Monteiro, “Performance evaluation of routing protocols for MANETs with known connectivity patterns using evolving graphs”, Wireless Networks, Vol. 16, No. 3, Pp. 627–640, 2009.

[5] S. Deering and R. Hinden, “RFC 2460: Internet Protocol”, Version 6 (IPv6) Specification, 1998.

[6] S. Salam and A. Sajassi, “Provider Backbone Bridging and MPLS: Complementary Technologies for Next-Generation Carrier Ethernet Transport”, IEEE Communications Magazine, 2008.

[7] M.K. Chowdhry and R. Boutaba, “Network Virtualization: State of the Art and Research Challenges”, Communication Magazines, Vol. 47, No.7, Pp. 20-26, 2009.

[8] D. Fedyk and D. Allan, “Ethernet Data Plane Evolution for Provider Networks”, IEEE Communications Magazine, 2008.

[9] M. Norris, “Gigabit Ethernet - Technology and applications”, Artech House, 2003.

[10] M. Robert Metcalfe and R. David Boggs, “Ethernet: distributed packet switching for local computer networks”, Commun. ACM, Vol. 19, No. 7, Pp. 395–404, 1976.

[11] ETNA Consortium, “Ethernet Transport Networks, Architectures of Networking”, Work Package 2 Deliverable 2.1. Network Architecture, 2008.
[12] I.A. Alimi and A.O. Mufutau, “Enhancement of Network Performance of an Enterprises Network with VLAN”, American journal of Mobile Systems, applications and Services, Vol. 1, No. 2, Pp. 82-93, 2015.
[13] J. Quittek, T. Zseby, B. Claise and S. Zander, RFC 3917: Requirements for IP Flow Information Export (IPFIX), 2004.
[14] P. Kobierský, J. Koˇrenek and A. Hank, “CESNET technical report 33/2006”, Traffic Scanner, 2006.
[15] Cisco ME 3400E Ethernet Access Switch Software Configuration Guide.