CERTIFICATION OF APPROVAL

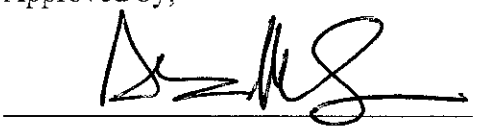
Campus Area Network Simulation using SMLT Architecture

By

Nur Isyatul Mohamed Noor Rosli

A project dissertation submitted to the
Information Communication Technology Programme
Universiti Teknologi PETRONAS in partial fulfillment of the requirement for the
Bachelor of TECHNOLOGY (Hons)
(INFORMATION COMMUNICATION TECHNOLOGY)

Approved by,



(Abdullah Sani Abd Rahman)

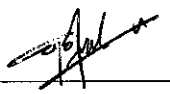
UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK
JULY 2006

t
TK
5105.7
.N974
2006

1) Local area networks (Computer networks)
2) Universities and colleges -- Computer networks

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the reference and acknowledgements, and that the original work contained herein has not been undertaken or done by unspecified sources or persons.



(Nur Isyatul Mohamed Noor Rosli)

ABSTRACT

The objective of this project is to develop a new resilient network structure for Universiti Teknologi PETRONAS (UTP) that can eliminate single points of failure and minimize down time during scheduled network maintenance. UTP has five main residential villages, academic blocks, and management units which are interconnected by the CAN. Currently, network in UTP is not stable, has slow connection speed and encounter many problems. UTP need a better network to run the daily activity smoothly especially in using the SAP and e-learning. The scope of the study is to implement Split Multi-Link Trunking (SMLT) in UTP network. In the new proposed network structure, the access switch in each building in the campus will be connected to two Nortel Passport 8600. The links from the access switch will be split to both Nortel Passport 8600. This new structure will have no single points of failure, all of the available links will be used and increase bandwidth. The new network structure will be simulated using OPNET IT Guru Academic Edition. The proposed network structure will be compared to the current network to find out which network structure is suitable for UTP.

ACKNOWLEDGEMENT

The student would like to thank everyone who has directly or indirectly help in completing this project. Firstly, special thanks to the student's parents for being so supportive and has given lots of encouragement to finish the project. Secondly, the student would like to thank the student's supervisors, Mr. Abdullah Sani Abd Rahman and Mr. Anang Hudaya Muhammad Amin for the assistance and guidance throughout the duration of the project. The advices given really help in completing the project. Gratitude also goes to the iPerintis staffs; Mr. Razif Mohd Rejab, Mr. Razak Salleh, Mr. Safarizal Shuib, Mr. Zahid Izam and Mr. Ku Sani. Their willingness to share valuable knowledge and experience in networking gave great benefits to the student. Besides that, the students also would like to appreciate the student's colleagues and lectures for their cooperation.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

BPS	Business Policy Switch
CAN	Campus Area Network
CPE	Customer Premises Equipment
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISP	Internet Service Provider
IST	Inter Switch Trunk
LAN	Local Area Network
MAC	Media Access Control
MLT	Multi-Link Trunk
POP	Point of Presence
SAP	Systems, Applications and Products
SMLT	Split Multi-Link Trunking
STP	Spanning Tree Protocol
VLAN	Virtual Local Area Network

CHAPTER 1
INTRODUCTION

1.1 Background of Study

Nowadays, application such as IP Telephony, multicast and e-learning gives valuable benefits to an organization. Unplanned network outages can affect all aspects of an organization. An unreliable network does not allow application like the IP telephony and e-learning to provide the benefits that they designed to provide.

Typical resilient Ethernet networks consist of wiring closer switches dual homed to network center aggregation switches in a building or campus. Network servers are being multi-homed to server switches that enable higher bandwidth and improved resiliency. In Internet Service Provider (ISP) environment, Customer Premises Equipment (CPE) devices may be dual-homed to two aggregation switches at a Point of Presence (POP) but this scheme requires the use of Spanning Tree Protocol (STP). STP is used to protect the network against loops but it cannot be used to build redundant network and at the same time fully utilize all the links.

Split Multi-Link Trunking (SMLT) is a new technology introduced by Nortel Network and is an extension to IEEE 802.3ad. SMLT can improve the resiliency of Layer 2 by providing nodal protection, link failure protection and flexible bandwidth scaling. SMLT allows edge switches connects to two SMLT aggregation switches. The two aggregation switches appears as a single device to edge switches. The aggregation switches are interconnected using an Inter-Switch Trunk (IST). IST allows aggregation switches to exchange addressing and state information, permitting rapid fault detection and forwarding path modification. SMLT automatically avoids loops by its enhanced-link-aggregation-control protocol. It is not necessary to use STP in designing a network that uses SMLT.

1.2 Problem Statement

Universiti Teknologi PETRONAS (UTP) has five main residential villages, academic blocks, and management units which are interconnected in a Campus Area Network (CAN). UTP is currently using Fast Ethernet for the Local Area Network (LAN).

Nowadays, UTP network is not stable, has slow connection speed and encounter many problems especially during peak hours (9.00pm until 2.00am). Based on observation, almost every week there will be one network problem for each village. The slow connection speed might be caused by the increasing number of network users as there are new villages opened for students. The other problems may be caused by a certain network design flaws that results in single points of failure and low bandwidth. A single point of failure causes loss of connection between access switch and core switch that will affect the whole network performance. Improper choice of type of link will cause slow network transmission at certain connection and can cause the link to have low bandwidth. Besides that, improper allocation of network devices causes imbalance network between student village and academic complex. The network connection at the academic complex is faster and more stable compared to the student villages. Many students preferred to surf information and download material at the computer labs rather than at their rooms.

1.2.1 Significant of the project

The new network design will be able to encounter all the above-mentioned problems. The network will be fully utilized, eliminate single points of failure, stable, high bandwidth and less down-time. The changes of the network will not give great impact on the current network. By implementing SMLT in the new network structure, the network will have 99% of uptime and approximately only 4ms of down-time.

1.3 Objective and Scope of Study

The objective of this project is to develop a new resilient network structure that can eliminate single points of failure and minimize down time during scheduled network maintenance. Besides that, another objective of this project is to design a network that can support the available hardware and the increasing number of users. With proper network connection and suitable network devices, the new network can provide optimal service that UTP require.

This project is about the simulation of UTP CAN by implementing the SMLT architecture. The new architecture will be simulated using software, OPNET IT Guru Academic Edition to see the performance of the SMLT structure in UTP. The scope of this project is the CAN which consists of the student villages, academic complex and management units. The current network will be redesign with the implementation of SMLT.

1.3.1 The relevancy of the project

There are new residential villages being built in UTP and new application used in the management such as SAP that require high bandwidth and high transfer speed. The network needs to be stable and available all the time. The current network structure needs to be analyzed and improved. SMLT can achieve all the objectives, it is interoperable with the existing server, wiring closet, CPE and edge switches and can be done during working hours. Upgrading the current network to SMLT can save significant amount of money over time.

1.3.2 Feasibility of the project within scope and time frame

This project has been divided into two parts. The first part is the research while the second part is developing the simulation. This project is feasible within the scope and time given.

CHAPTER 2

LITERATURE REVIEW AND THEORY

There are two journals from the Nortel Networks that have been used as a reference. The journals are Eliminate Single Points of Failure and Designing a Resilient Network

2.1 Eliminate Single Points of Failure

In the first journal, Eliminate Single Points of Failure, said that the SMLT improves on the Layer 2 resiliency by providing nodal protection in addition to link failure protection and flexible bandwidth scaling. As network expands, there is an increasing demand for multiple paths from all wiring closet switches into the core of the network to eliminate all single points of failure. The challenge of designing a resilient network not only to eliminate single points of failure but doing it so without ending up with unused and costly capacity. The network must also be able to reroute around failures. SMLT can also solve problems regarding the Layer 2 traffic load sharing and SMLT scaling.

In this paper, SMLT is being compared to the Spanning Tree. SMLT does not have any blocking links, SMLT's IST protocol is used only on a set of two switches and SMLT convergence targets are sub-second in every failure scenario. The Spanning Tree is a good technology to avoid loops but SMLT is better in providing the tools for designing resilient networks, leveraging all installed bandwidth, keeping the VLAN / IP subnet complexity low and allowing for network maintenance during working hours.

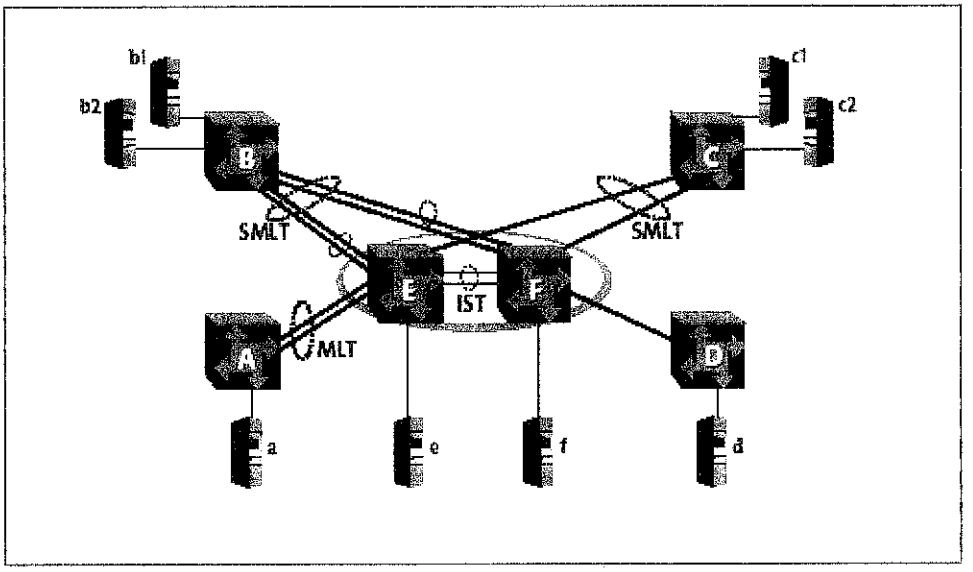


Figure 1: Configuration of two Passport* 8600 Routing Switches

This journal also explained about how SMLT works in Layer 2 of the network. Figure 1 shows the configuration of two Passport* 8600 Routing Switches as link aggregation switch (E and F) and four separate wiring closet switches (A, B, C and D) that can represent any Multi-Link Trunk (MLT) devices such as Passport 8300 Ethernet switch, BayStack* 460 Switch, BayStack 470 Switch and BayStack 5510 Switch. Wiring closet switches B and C are connected to E and F using multi-link trunks that splits between the two aggregation switch. For example, SMLT client switch B may use two parallel links for its connection to E and two additional parallel links to connect with F. SMLT client switch C has only a single link to E and F. A is also configured for MLT but MLT terminates on only one switch in the core network. Switch D has a single connection to the core. Even though both switches A and D can be configured using SMLT but neither one of the switch can gained any benefit from the configuration shown above. Based on the example shown, the implementation of SMLT only requires two SMLT aggregation switch that need to be connected using Inter Switch Trunk (IST). The aggregation switch use this communication ways to confirm that each switch is alive, exchange MAC address information and to forward flooded packets destined for non-SMLT-connected switches.

2.2 Designing a Resilient Network

The second journal, Designing a Resilient Network, explained that SMLT allows two aggregation switches to appear as a single device to dual homed switches. The aggregation switches make use of an IST over which they exchange information, permitting rapid fault detection and forwarding path modification. To achieve network element protection, SMLT extends link aggregation to allow dual homing of IEEE 802.3ad attached devices. Both of the dual homed connected devices are active and pass traffic. This architecture provides twice the available bandwidth of using the Spanning Tree Protocol. SMLT improves the reliability of a Layer 2 network operating between the user access switches in a building and the network centre aggregation switch, as well as with the connections to multi-homed servers. It works by providing load sharing among all available links and fast failover in the case of a link or core switch failure.

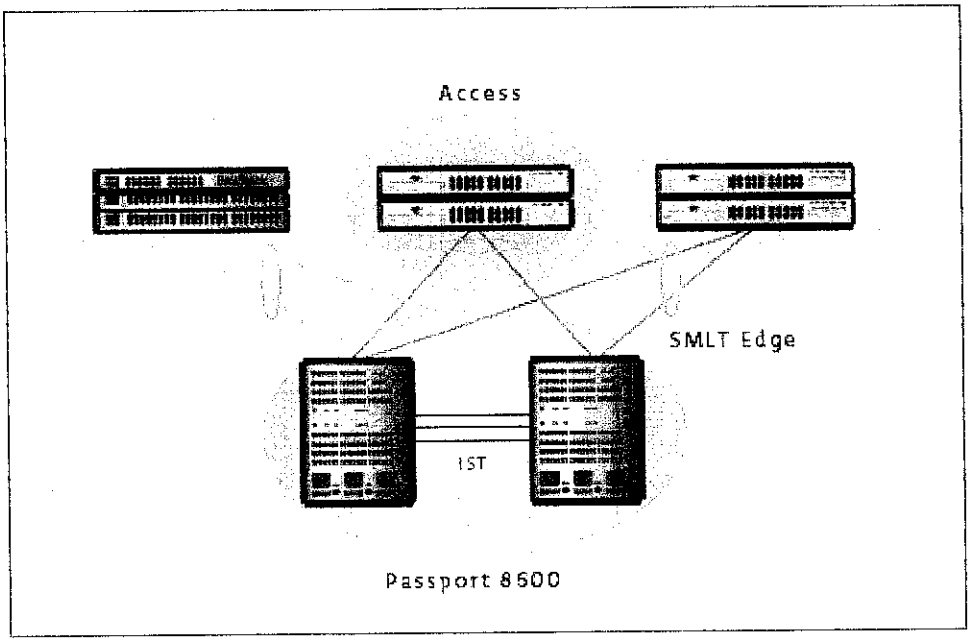


Figure 2: Reliability with SMLT

Figure 2 above shows the basic connection using SMLT. By using SMLT, there will be no single point of failure, no sub-second failover, it is transparent and interoperable.

CHAPTER 3
METHODOLOGY AND PROJECT WORK

3.1 Procedure Identification

This project is based on a simple waterfall methodology. This methodology was designed as a guide in completing the project. Each phase will be completed one by one. Example, first phase need to be completed before proceeding to the second phase. Figure 3 shows the methodology used in developing this project.

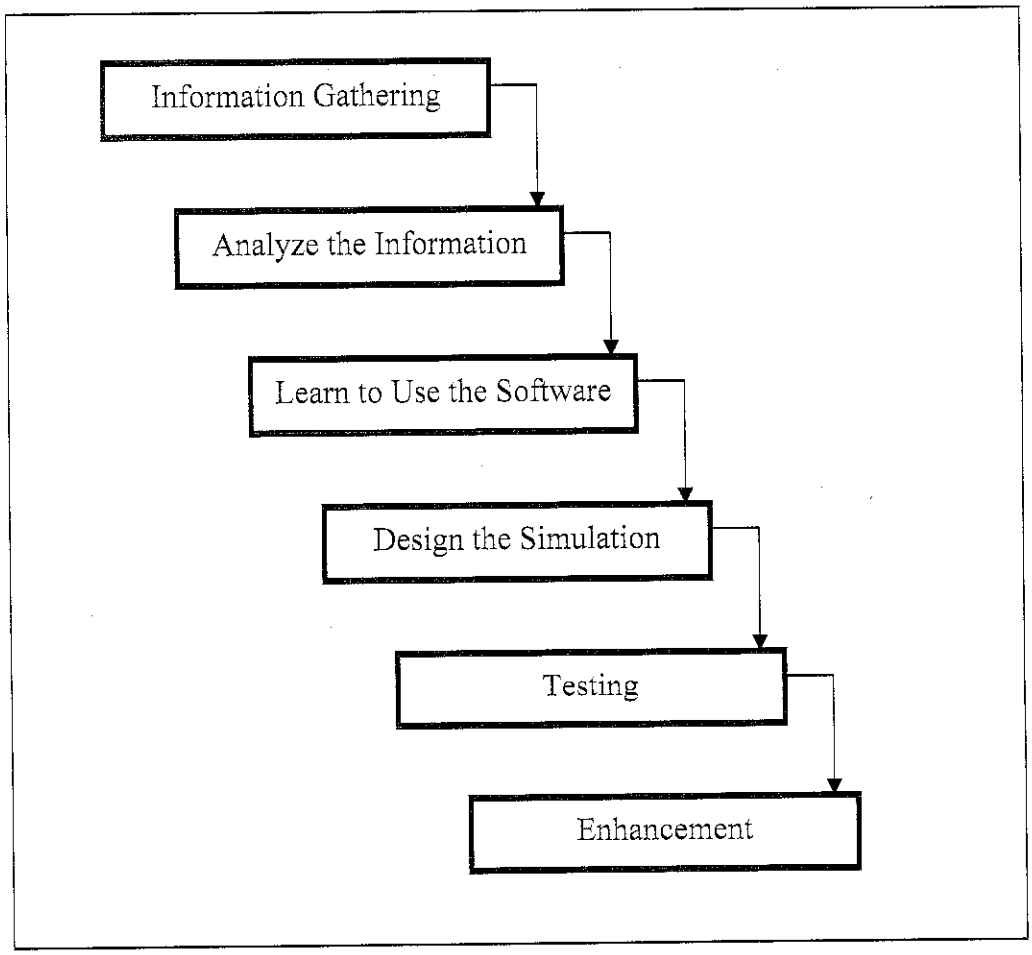


Figure 3: Project Methodology

3.2 Project Methodology

This project begins with the information gathering where all the information required is gathered. The second phase is analyzing the information gathered. The information is being analyzed to identify which information can be used to help in designing the network. The third phase is to learn how to use the software. The fourth phase is to start designing the network using SMLT architecture. The fifth phase is to test the new network design and lastly is the enhancement phase. Any enhancement or modification is done in this phase.

3.2.1 Information gathering

Information Gathering is very important before a project can be executed. Information about SMLT, type of links, suitable software and current UTP network design need to be gathered. The information is used to understand the details of the project. Information is gathered from books, journals, articles, and web pages. The most useful information is from the Nortel Network itself because Nortel Network is the company that introduced SMLT. Another method that can be used to get information is questionnaire. A questionnaire is very helpful in gaining field data from the user. The student has created a simple questionnaire to get user comments about the current network condition.

3.2.2 Analyze the information

All the information gathered has been analyzed to search for details that are relevant for the project. The information gained is used as supporting details to the project. Feedback given by the users through the questionnaire gave general overview of UTP network performance. The feedbacks given by the user has been summarized and has been used as a guide in designing the new network structure.

3.2.3 Learn to use the software

The software used to simulate the network is OPNET IT Guru Academic Edition. Before the network can be designed, it is important to learn how to use the software. User manual has been used as a guide. It is easier to learn and know the tools provided before designing the simulation. The student has saved a lot of time developing the simulation because the student has learnt to use the software in advanced.

3.2.4 Design the simulation

The simulation is done using the OPNET IT Guru Academic Edition. The software consists of the different kinds of network elements that are needed to design a network. All the devices produce by various kinds of manufacturers can be found in the software such as Nortel Networks and Cisco. The devices can functions exactly the same as the real device in the software and be configured according to the network requirements. The network throughput, network delay, packet sent and packet received can be simulated using this software.

3.2.5 Testing

The testing phase needs to be done to ensure that all connection in the simulation works correctly as intended. The testing depends totally on the OPNET IT Guru Software. Any error or problem needs to be corrected before the simulation can be considered successful.

3.2.6 Enhancement

Any enhancement or improvement can be specified in this phase. Future work and new technology can be stated for future development.

3.3 TOOL REQUIRED

3.3.1 Hardware

1. Personal Computer (PC): Pentium-class processor
2. Minimum hard disk space required: 1.5GB
3. Minimum Random Access Memory (RAM): 128MB

3.3.2 Software

1. Platform: Windows XP
2. Software:
    - OPNET IT Guru Software
    - Microsoft Office Excel

CHAPTER 4

RESULT AND DISCUSSION

4.1 Gathering Information from Questionnaire

The simplest way to gather data is by observing the network users. Therefore, questionnaires are distributed to the students, academic and management staff. All the data and comments are used as a guide in designing the new network structure. The results of the questionnaires are presented using pie chart and bar chart.

4.1.1 Condition of UTP network

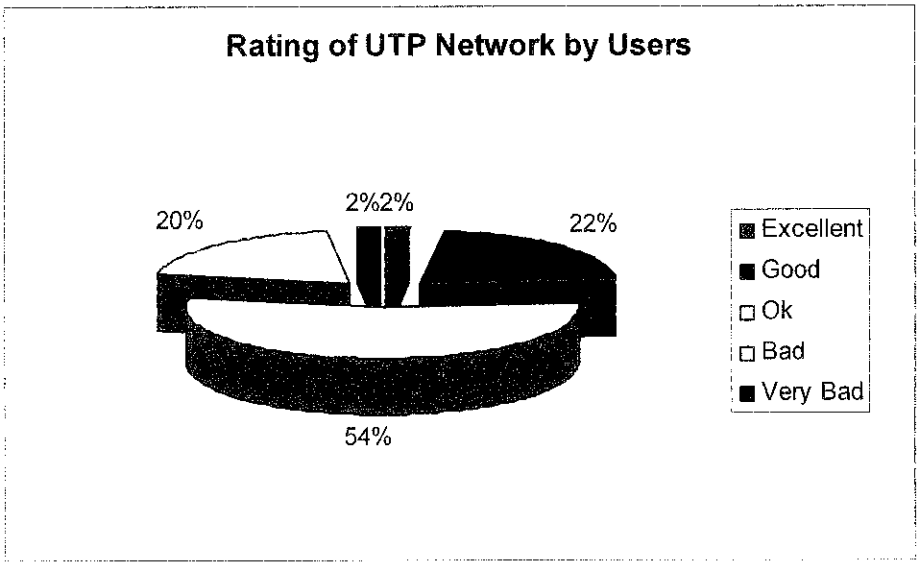


Figure 4: Rating of UTP Network by Users

The pie chart above shows the feedback given by the users about the conditions of current UTP network. 54% of the users said that the network is ok, 22% said it is good, 20% said it is bad, 2% said it is very bad and another 2% said the network is excellent.

4.1.2 Usage of the network connection

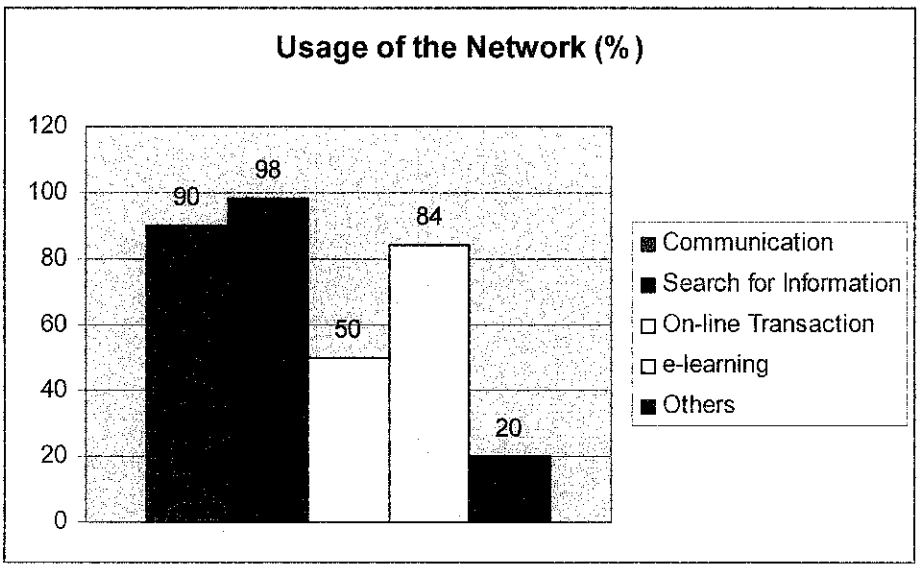


Figure 5: Usage of the Network

All users that answered the questionnaires agreed that the network connection is very important in the daily activities. The users need the network connection for communication (e.g. email, Google Talk, Yahoo! Messenger and Skype), search information using search engine on the net (e.g Google, Yahoo! and MSN), on-line transaction (e.g. BCB and MAYBANK), e-learning and other purposes such as transferring files and read on-line newspaper. The percentage of usage is shown in the bar chart above. 90% of the users uses the connection for communication, 98% used for searching information, 50% used for on-line transaction, 84% used it for e-learning and 20% of the users used it for other purposes.

4.1.3 Difficulty encountered

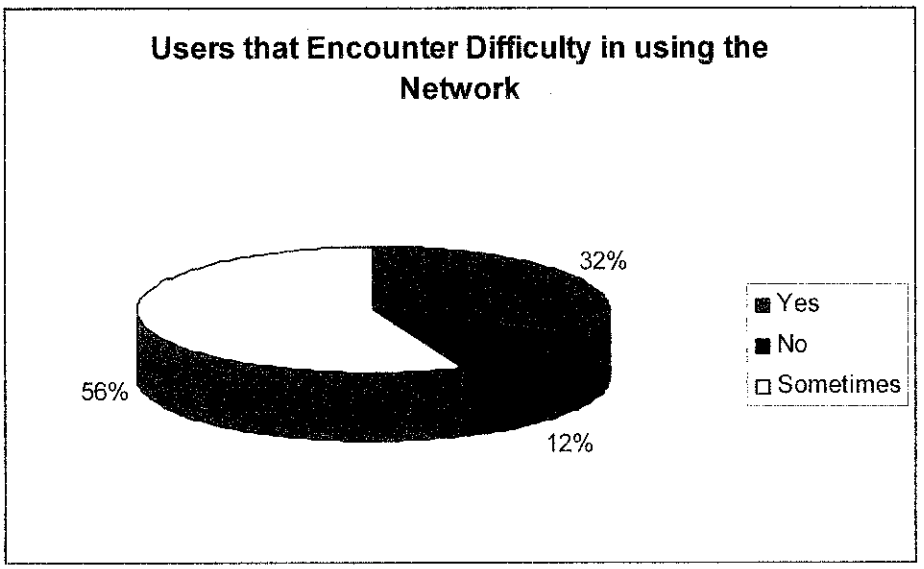


Figure 6: Users that Encounter Difficulty

The pie chart in Figure 6 above shows the percentage of users that faced difficulty in using the current UTP network. 56% of the users said that sometimes they faced difficulty in using the network. 32% of the respondent said that they faced difficulty and another 12% said that they did not face any difficulty.

4.1.4 Types of difficulties encountered

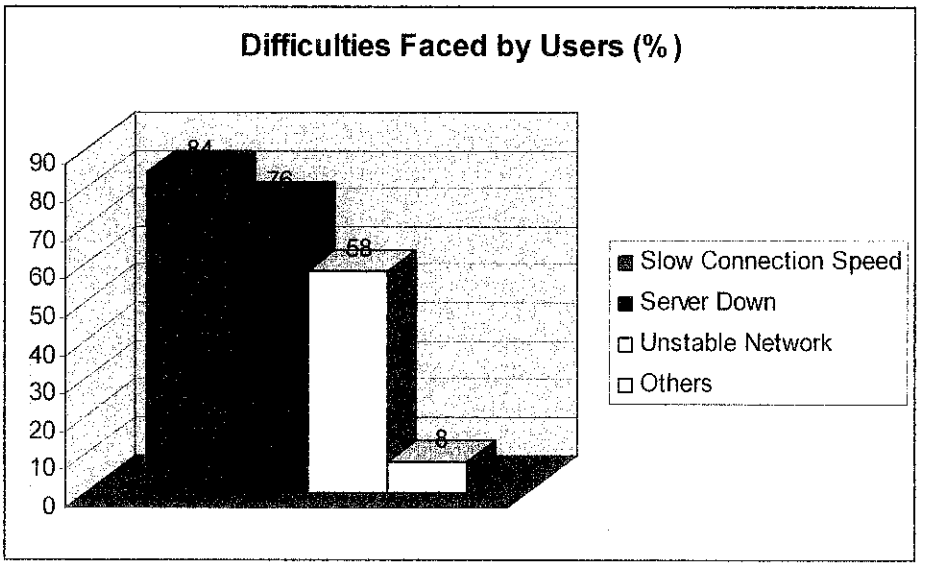


Figure 7: Types of Difficulties

Figure 7 shows the types of difficulties that the respondent faced in using the UTP network. Three main problems usually occurred which is slow connection speed, server down and unstable network. 84% of the users said that the connection speed of the network is slow, 76% said the server is always down, 58% said the network is unstable and another 8% responded that they faced other problem such as network suddenly disconnected.

4.1.5 User recommendations

Majority of the users recommend increasing the bandwidth and speed of the current network. The network connection also should be stable and available all the time. Any problem with the network can interrupt the daily activities especially in using e-learning and SAP.

4.2 Gathering Information about SMLT

SMLT is Nortel Networks architecture that helps eliminate single points of failure and creates multiple paths from user access switches to the core of the network. SMLT does more than preventing from the network loops. SMLT provides the architecture to design resiliency directly into the network. It also has the advantage to reroute failures as quickly as possible. SMLT give faster convergence time than the STP which is typically one second versus 30-60 seconds. SMLT also eliminates the blocking of ports that will increase the network bandwidth because all the trunks between switches can be fully utilized for user traffic. There are five main components in SMLT which is the SMLT aggregation switch, Inter Switch Trunk (IST), SMLT, SMLT Client and SMLT ID. Spanning Tree Protocol is not use in the SMLT because it is being disabled on the SMLT ports. SMLT code is supported on Passport 8600 Routing Switches.

4.3 Gathering Information about Types of Links

The Ethernet network runs at the speed of 10/100/100Mbps. There are several types of links that can support this network medium speed. The 10 Base T can carry 10 Mbps (Twisted Pair Ethernet). The 100 Base T link is the networking standard for twisted-pair cabling that capable of carrying data at 100Mbps (Fast Ethernet). The 100 Base FX is the networking standard for fiber-optic cabling capable of carrying data at 100Mbps. The 1000 BASE SX carried data at 1000Mbps (max) over short haul multimode after fiber optic cabling.

4.4 Gathering Information from Interview

4.4.1 Current network structure in UTP

The student has met Mr. Arfaishah, UTP Network Engineer to get some information about UTP network structure. Mr. Arfaishah has briefly explained the structure of current network. Basically, the network is arranged in Star Topology (as shown in Figure 8). It is divided into five parts which are Village Core Network, Academic Core Network, Central Core Network and Server Farm (also known as Data Center), Internet and Corporate Network. For this project, the student only focused on two parts; Village Core Network and Academic Core Network that makes up the CAN.

Briefly, Mr. Arfaishah told the student that at Layer 2, UTP is using Business Policy Switch (BPS) while at Layer 3, UTP use Nortel Passport 8600. BPS has 24-Port Ethernet Switch. The connection between Layer 2 switch and Layer 3 switch is using Multi-Link Trunk (MLT). MLT means there are two links connected between Layer 2 switch and Layer 3 switch. One link is the main link while the other one is the backup link. If the main link has problem, the backup link can take the responsibility to make sure the network connection is still available. Mr. Arfaishah also told that UTP is using Fast Ethernet.

For every village, there is one Nortel Passport 8600 and each building in the village has one access switch (BPS). For example, Village 1 (V1) has four blocks. So, there are four BPS and one Nortel Passport 8600. Each block has one BPS. The BPS is connected to the Nortel Passport 8600 through MLT link. Only Village 5 (V5) has two Nortel Passport 8600 because there are 11 blocks in this village. The number of users is large.

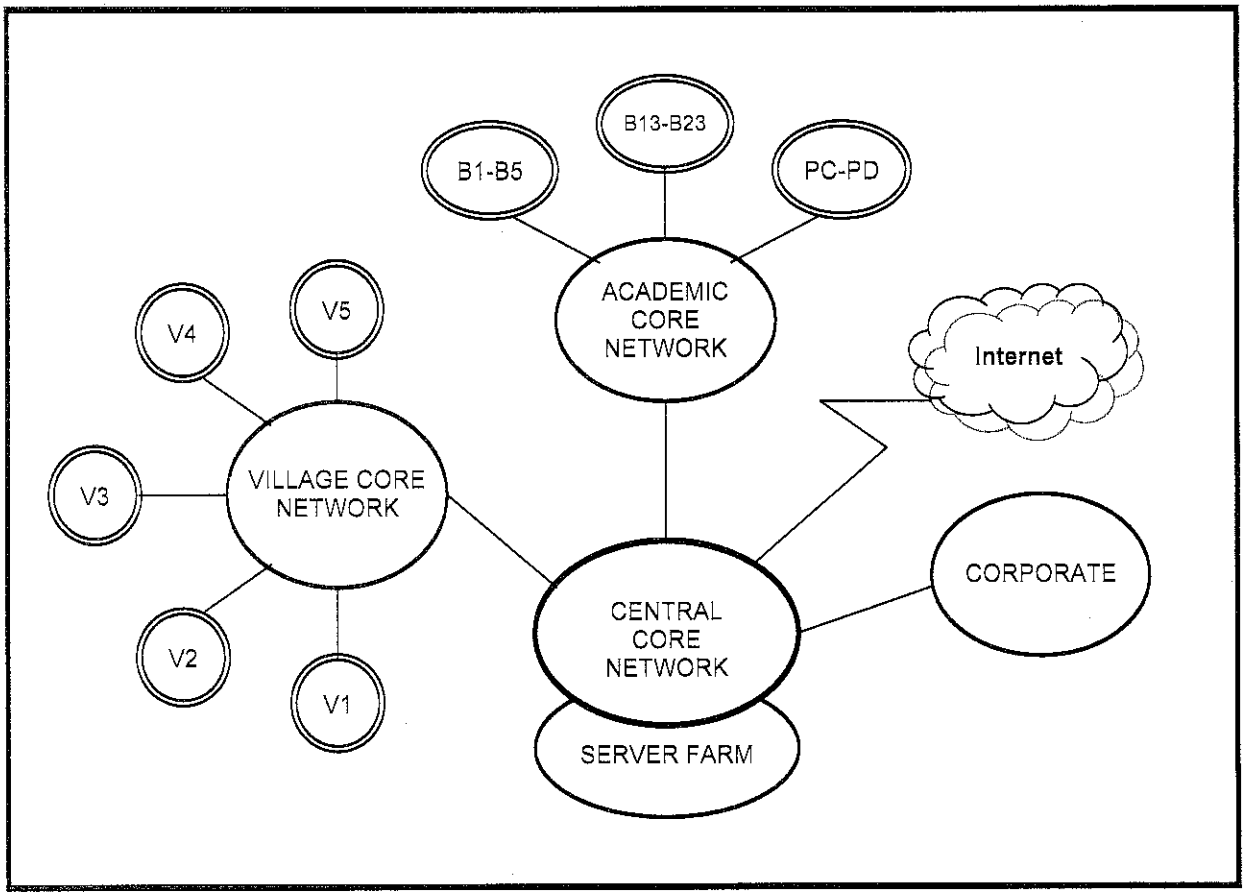


Figure 8: Overall Network Diagram of UTP

Figure 8 above shows the overall network diagram for UTP. The network structure is divided into five main parts. First part is the Village Core Network that manages the connection between Village 1 (V1), Village 2 (V2), Village 3 (V3), Village 4 (V4) and Village 5 (V5). Second part is the Academic Core Network that manages the network flows in the new academic complex (Building 1 – Building 23, Pocket C and Pocket D). Another three parts are the Core Network and Server Farm, Corporate Network and Internet.

4.5 Designing the Current Network in OPNET IT Guru

4.5.1 Village 1 (V1)

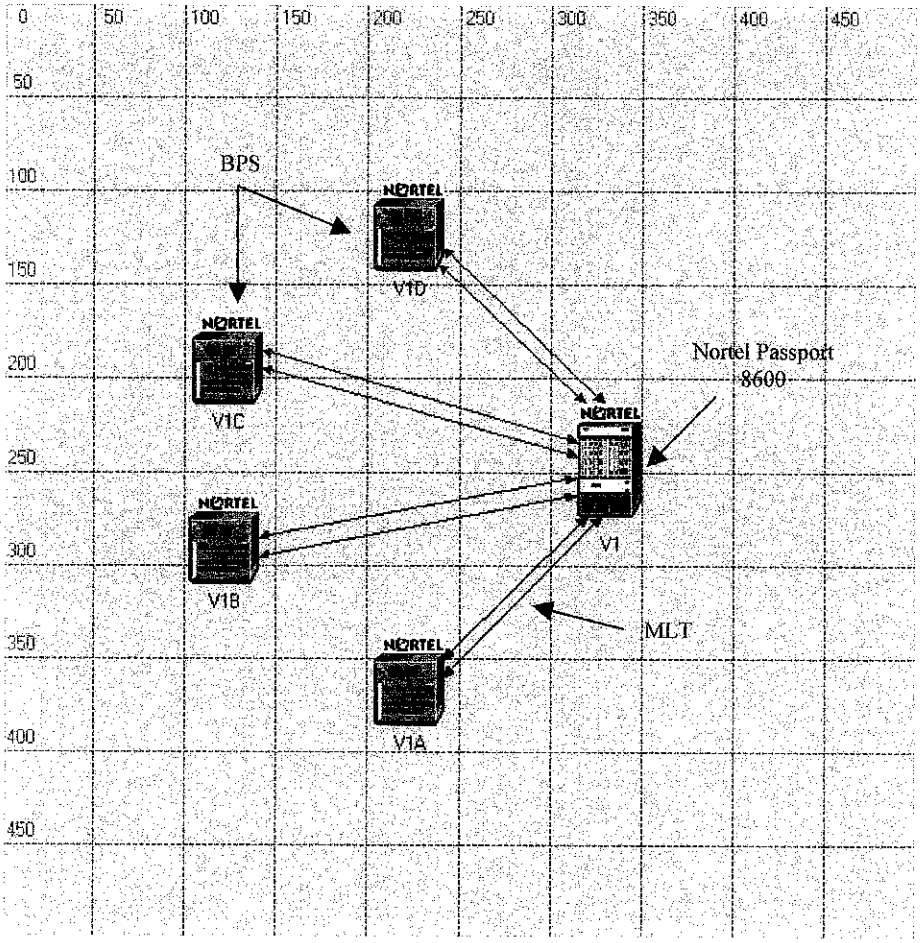


Figure 9: Current Village 1 Network

Based on the information given by Mr. Arfaishah, the student has designed the current network in OPNET IT Guru. Figure 9 shows the network for V1. There are four BPS and one Nortel Passport 8600 connected through MLT links. The pair of MLT links is shown by the colored arrow. For example, the connection from V1B to the Nortel Passport 8600, has two links. If one link broken, V1B will still be able to connect to V1 through the other link. Lost of connection will only happen if both MLT link broken and the access switch has problem. The worst case is when the Nortel Passport 8600 itself has problem. If that happens, V1 network will be isolated from the whole UTP network.

4.5.2 Village 2 (V2)

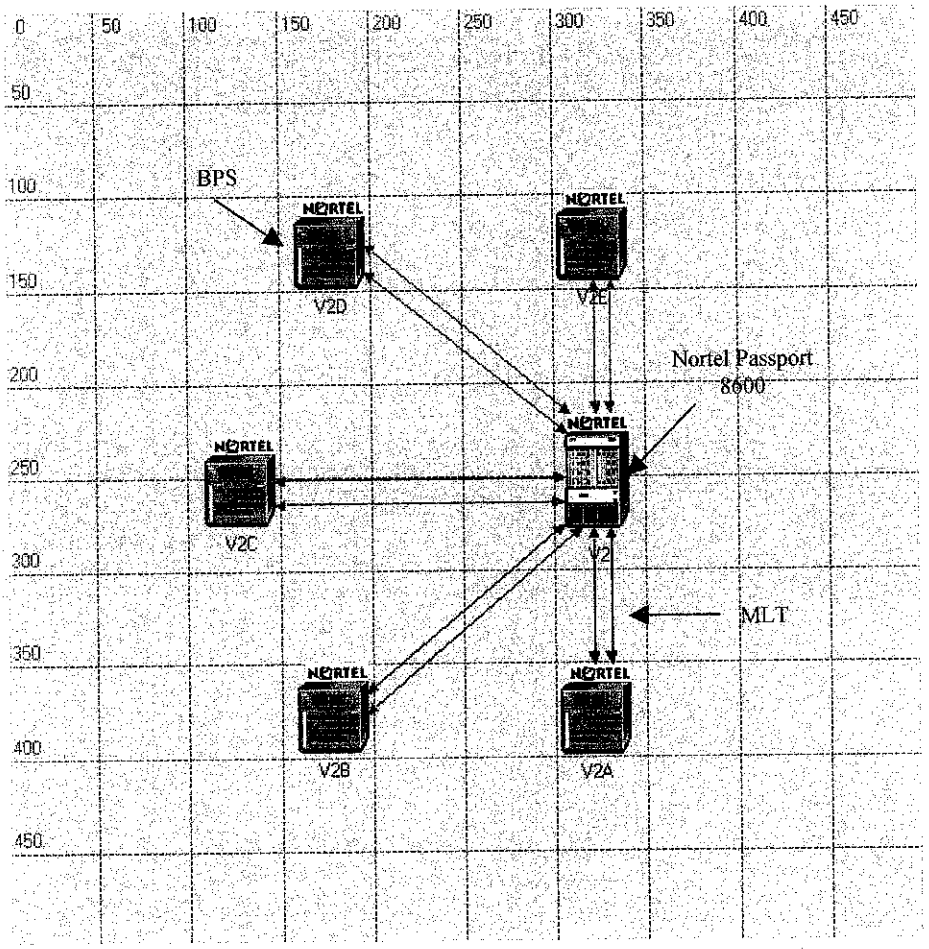


Figure 10: Current Village 2 Network

Figure 10 shows the current V2 network. This network is almost the same as V1 network structure. The only different is that V2 has five blocks which means there are five access switches in this network. The access switches are the BPS. There is only one Nortel Passport 8600. For easy notification in this report, all the Nortel Passport 8600 in each village is named according to the village where it is located. For example, in V2 network diagram, Nortel Passport 8600 is named V2.

4.5.3 Village 3 (V3)

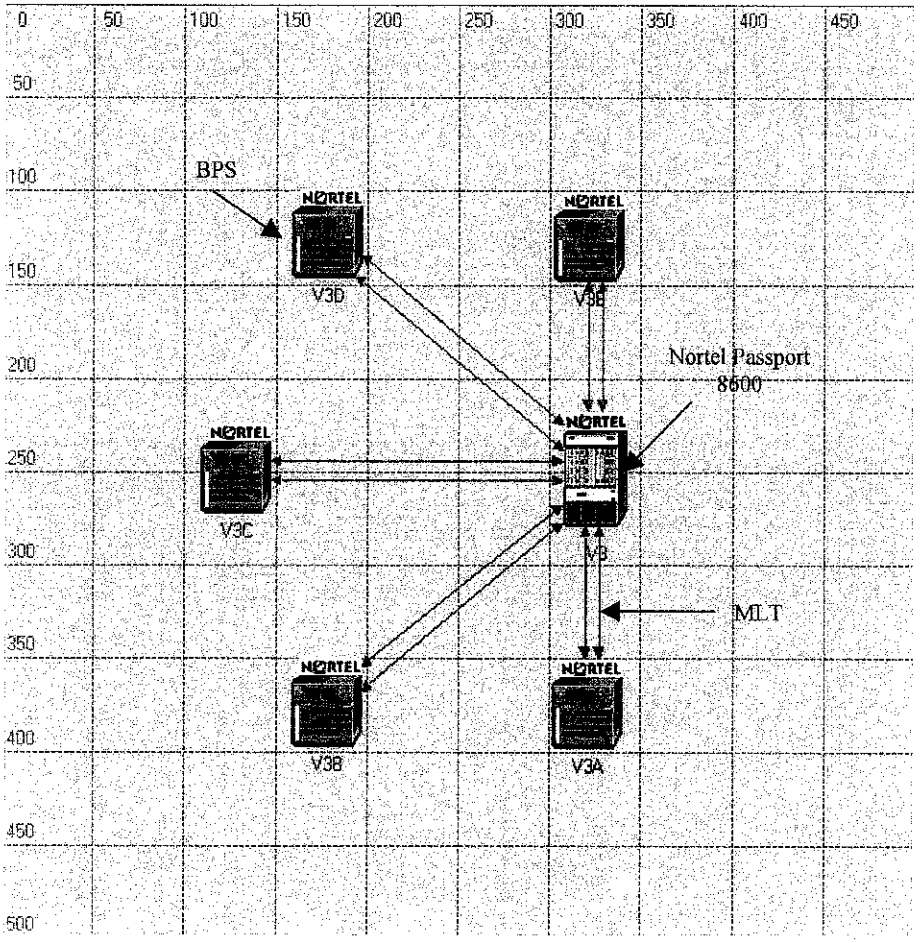


Figure 11: Current Village 3 Network

Figure 11 shows the current V3 network as being constructed in OPNET IT Guru Software. There are five blocks in this village which means there are five BPS and one Nortel Passport 8600 available in this village. The network structure is still the same as V1 and V2. MLT is used to connect the access switches to Nortel Passport 8600. If one link broken, another link can be use. The connection will be lost if both MLT links fail and access switch encounter problem. The worst case is when the Nortel Passport 8600 failed to function.

4.5.4 Village 4 (V4)

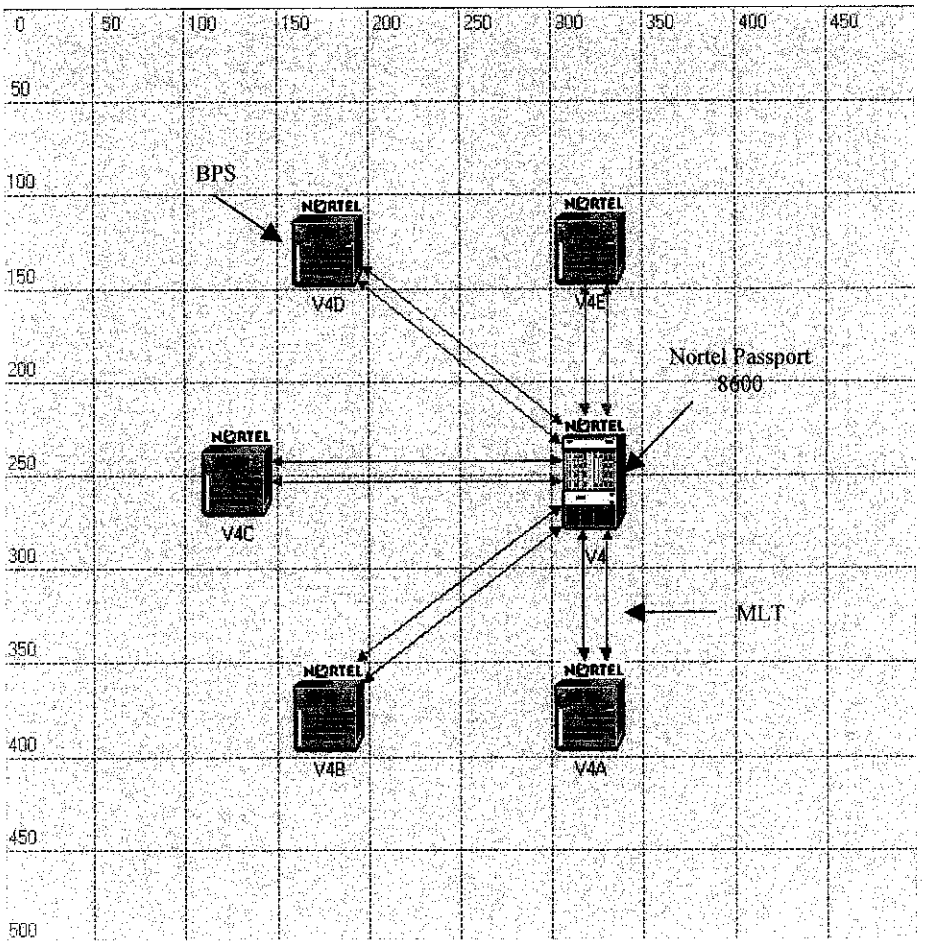


Figure 12: Current Village 4 Network

Figure above shows the current V4 network. V4 network is exactly the same as V3 network. The design of the building is also the same. The only different is in term of physical location.

4.5.5 Village 5 (V5)

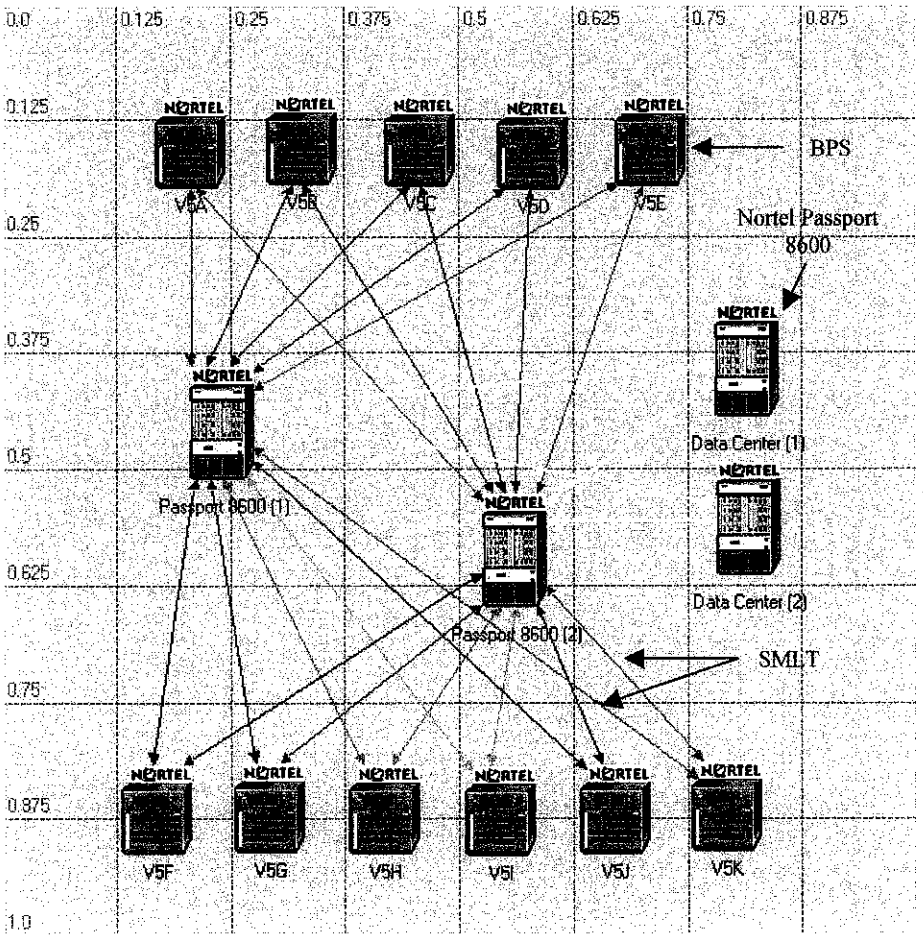


Figure 13: Current Village 5 Network

Village 5 network is totally different from the other villages. Figure 13 shows the current V5 network. There are 11 access switches in this network as there are 11 block occupied by the students. There are two Nortel Passport 8600 for V5 to cater for the large number of network users. The connection from BPS to Nortel Passport 8600 is not MLT but SMLT. The links from access switches are split to two Nortel Passport 8600. The two Nortel Passport 8600 are then connected to two Nortel Passport 8600 at the Data Center using SMLT. There are no single points of failure in this network structure. For this project, V5 will be excluded because V5 has already being implemented with SMLT.

4.5.6 Academic Complex

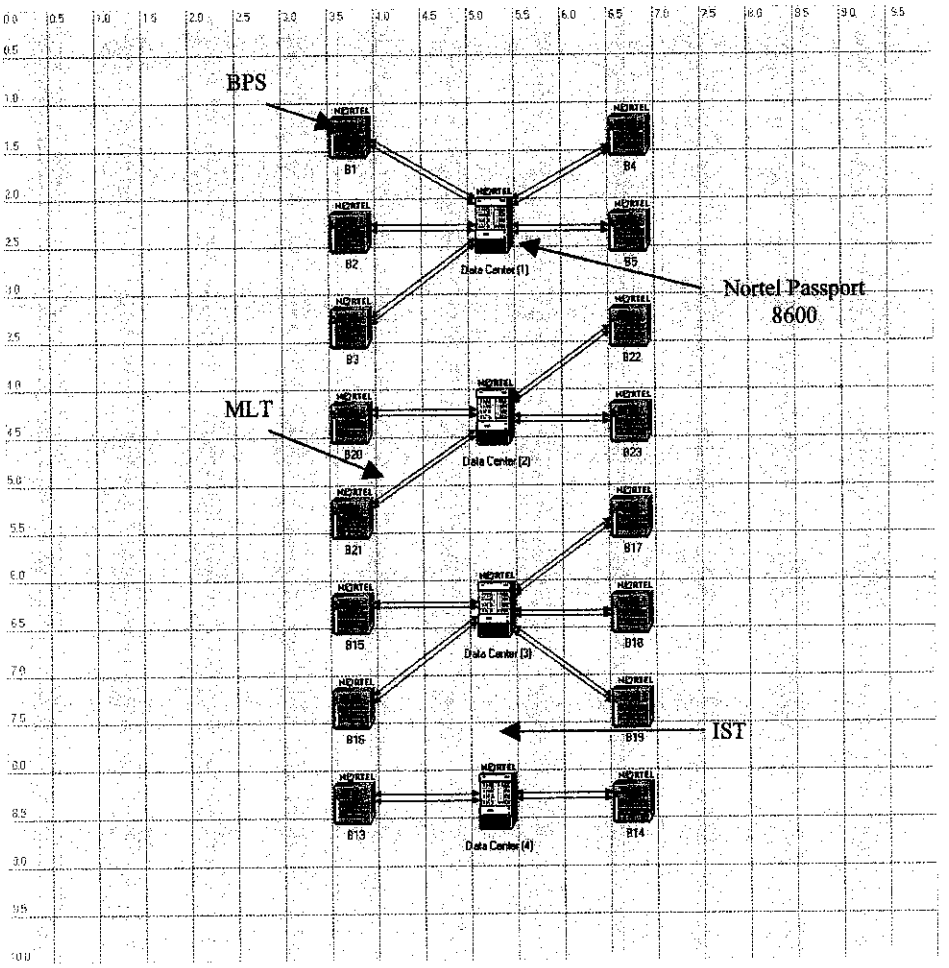


Figure 14: Current Academic Complex Network

Figure 14 above shows the current academic complex network. There are 16 blocks currently being built at the academic complex. Each blocks have own BPS. There are four Nortel Passport 8600 to manage the connection. One connects with access switches from Building 1 to Building 5; second connects with access switches from Building 20 – Building 23; third connects with Building 15 – 19; fourth connects to Building 13 – 14. All the connection from Layer 2 to Layer 3 switches are MLT. Each Nortel Passport 8600 can communicate with each other through IST link.

4.5.7 Pocket C and Pocket D

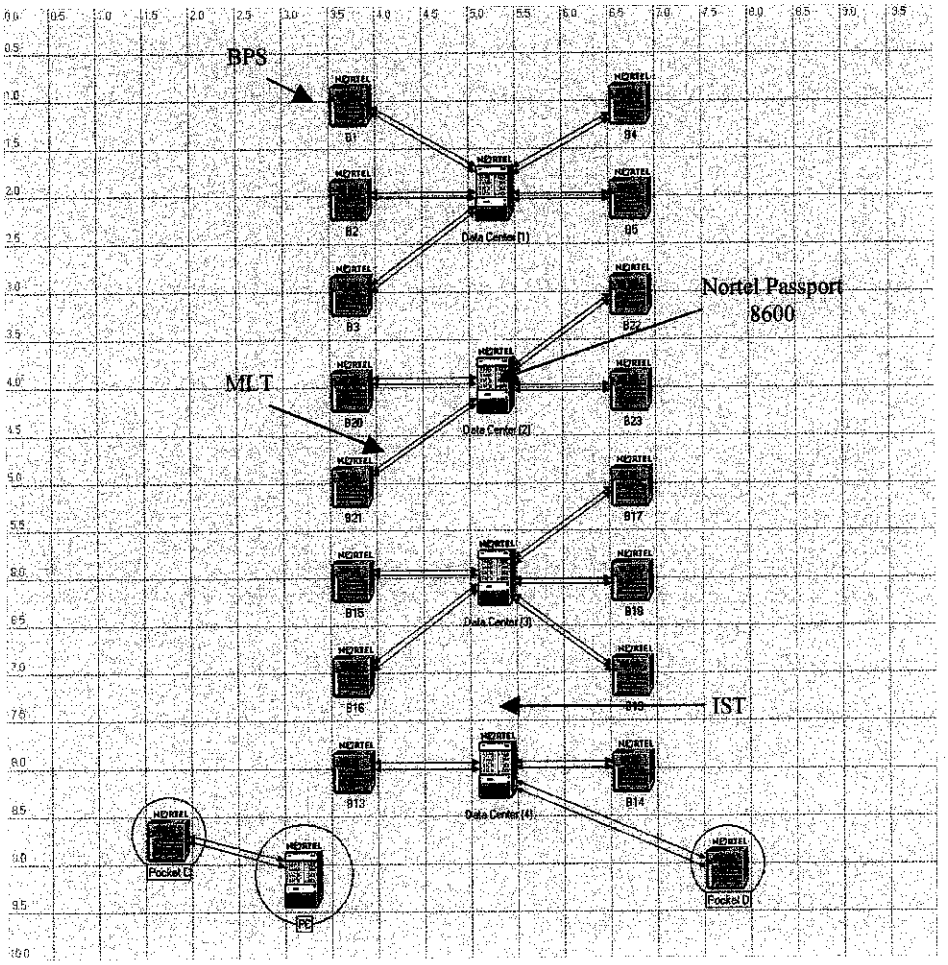


Figure 15: Current Pocket C and Pocket D Network

Figure 15 shows the current Pocket C (PC) and Pocket D (PD) network. PC has own BPS and Nortel Passport 8600. Access switch at PC is connected to Nortel Passport 8600 through MLT and then connected to Nortel Passport 8600 at the Data Center by MLT. There is no Nortel Passport 8600 for PD. PD access switch is directly connected to Nortel Passport 8600 at the Data Center through MLT.

4.6 Designing the New Network (with SMLT) in OPNET IT Guru

4.6.1 Village 1 (V1)

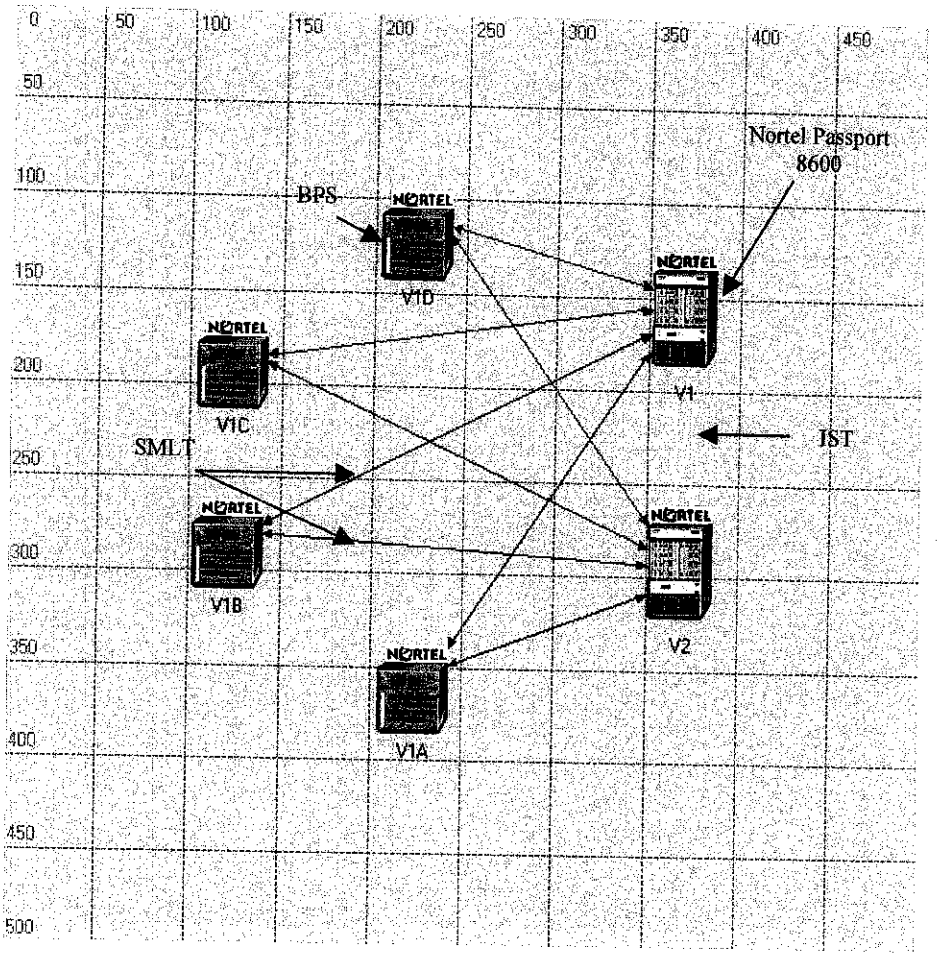


Figure 16: New Village 1 Network

Figure 16 shows the new V1 network that has been implemented with SMLT structure. There are still four BPS and one Nortel Passport 8600. The different is that the connection between access switch to Nortel Passport 8600 is now using SMLT not MLT. Access switch is linked to two Nortel Passport 8600 (aggregation switch). Nortel Passport 8600 for V1 is linked to Nortel Passport 8600 at V2. Both aggregation switches are connected together using and IST. IST allows the switches to communicate and share information. There are no single points of failure in this scheme except for the failure of both Nortel Passport 8600.

4.6.2 Village 2 (V2)

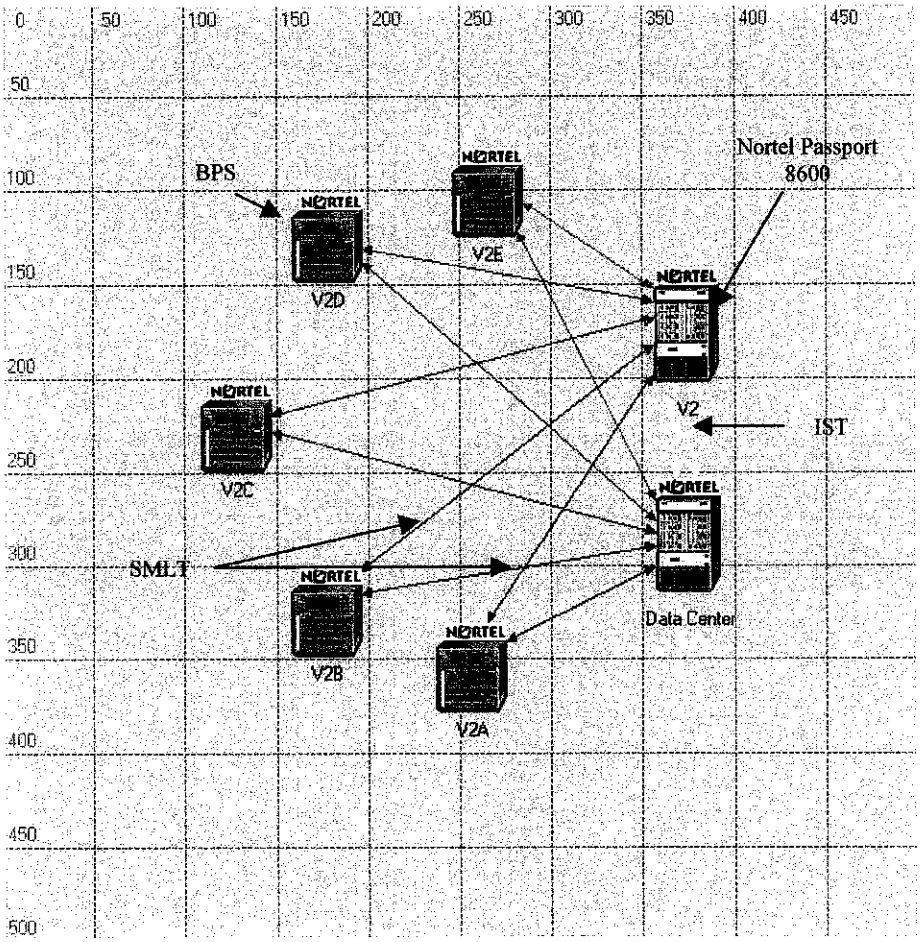


Figure 17: New Village 2 Network

Figure 17 shows the new V2 network. There are five BPS and one Nortel Passport 8600. The link connection is changed from MLT to SMLT where one access switch is connected to two Nortel Passport 8600. Previously, for V1, the Nortel Passport 8600 is connected to Nortel Passport 8600 at V2. For V2, the available aggregation switch is connected to Nortel Passport 8600 at the Data Center. This means that V1 network connects to V2 and then connects to the Data Center. (*In this report, the term Nortel Passport 8600 is sometime referred as aggregation switch and BPS is sometime called access switch*)

4.6.3 Village 3 (V3)

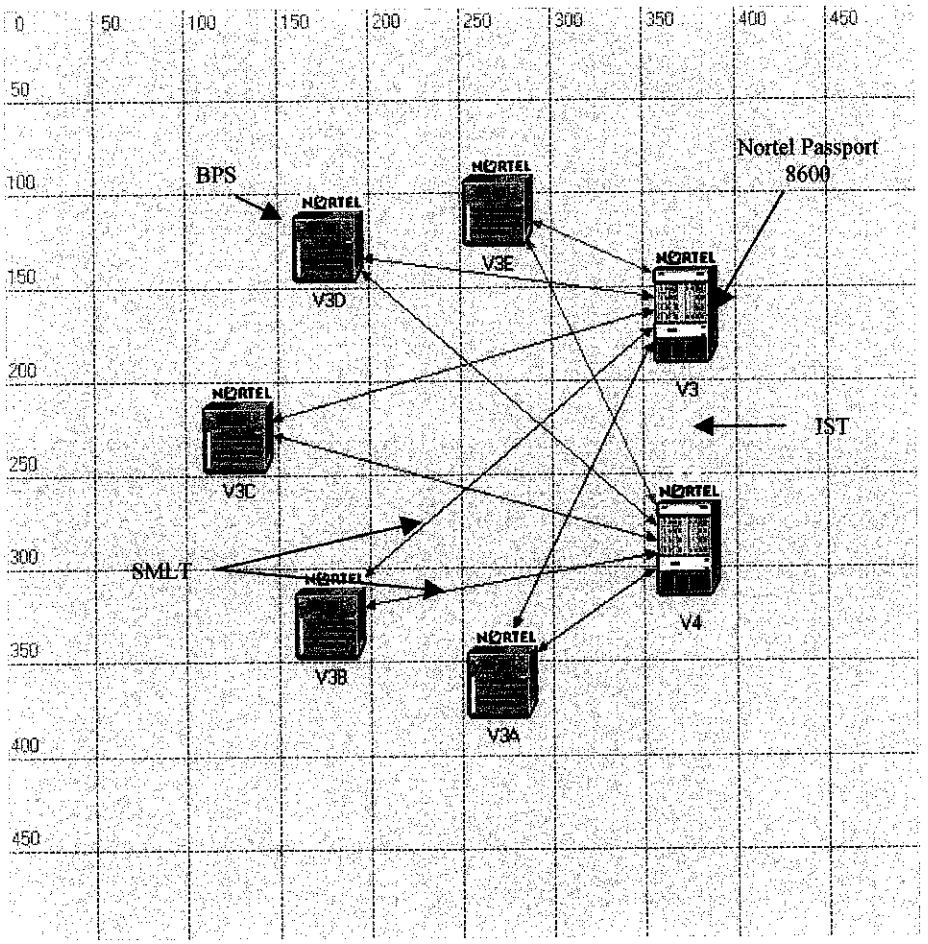


Figure 18: New Village 3 Network

The structure of V3 and V4 new network are the same. Figure 18 shows the new V3 network while Figure 19 shows the new network for V4. The MLT used before is changed to SMLT. The only different in these two networks is that Nortel Passport 8600 for V3 is connected to Nortel Passport 8600 at V4. For V4, the available Nortel Passport 8600 is connected to the Data Center.

4.6.4 Village 4 (V4)

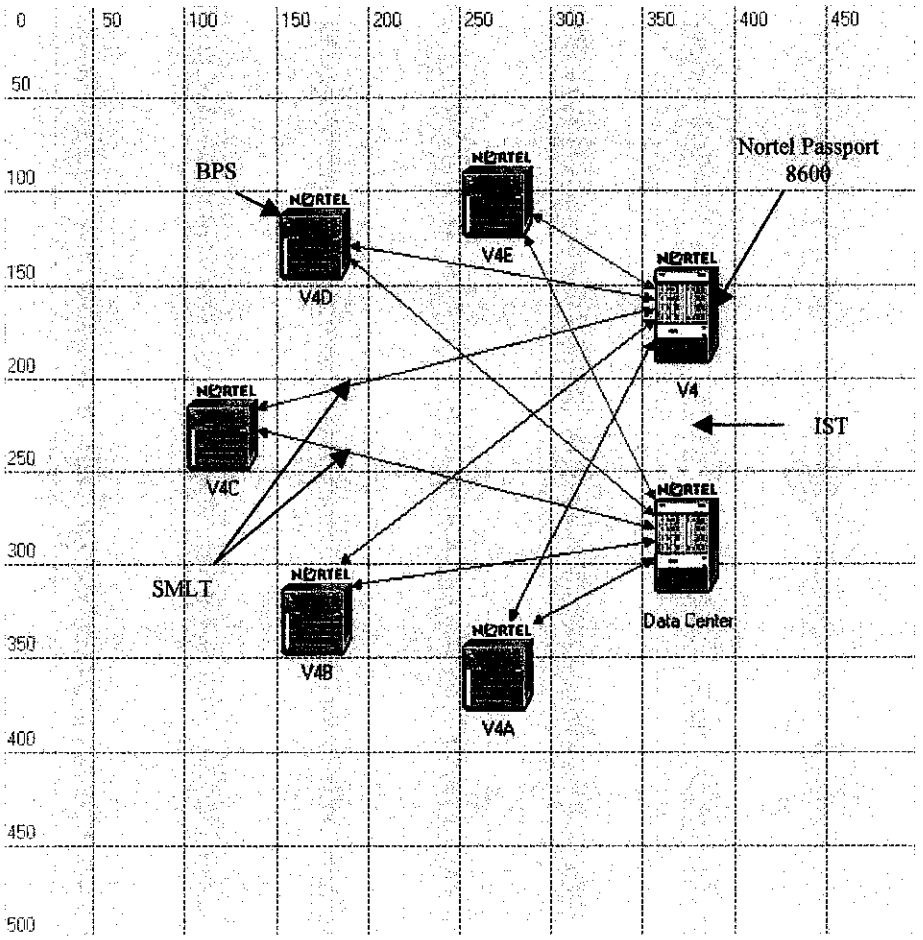


Figure 19: New Village 4 Network

SMLT allow the access switches to be connected to two aggregation switches. The two aggregation switches will appear as a single switch for the access switch. This structure will have no single points of failure, high availability and high bandwidth. In MLT design, if the Nortel Passport 8600 at the village has problem, the whole network for that village will lost connection. But, in SMLT design, if one aggregation switch has problem, there is another aggregation switch that can replace the existing switch. If one link down, there is another backup link. The worst case is when both aggregation switches failed to function that is rarely happened.

4.6.5 Academic Complex

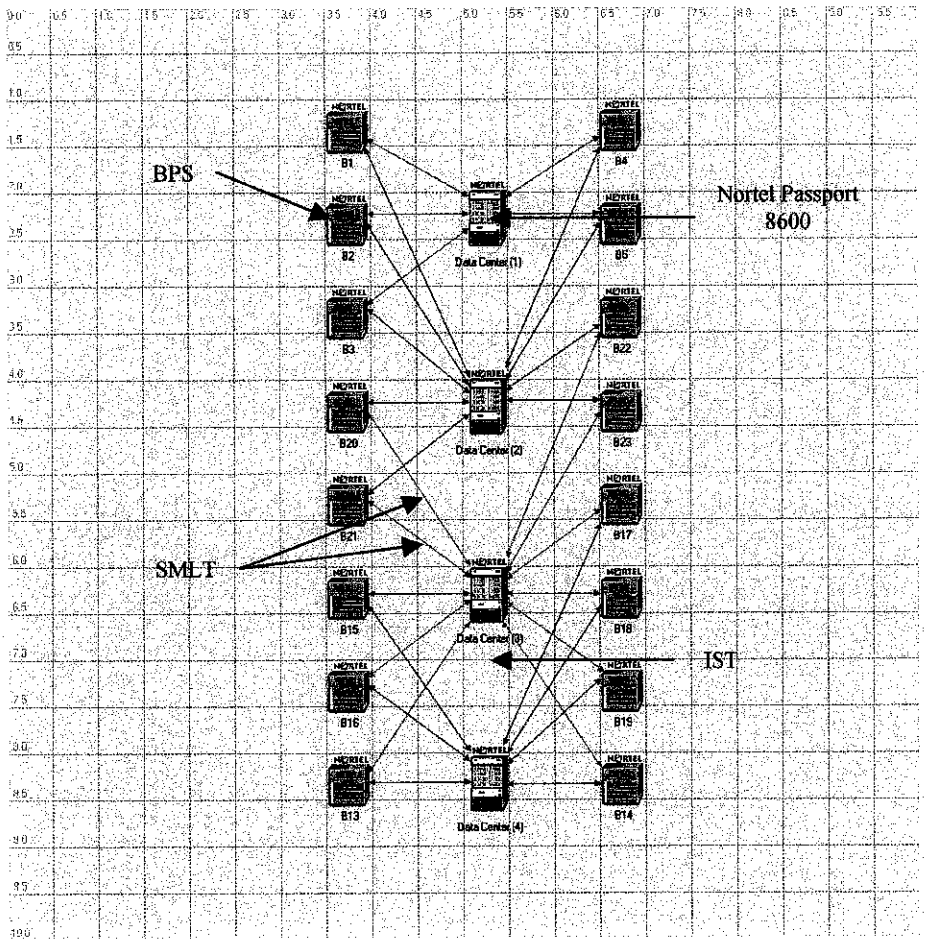


Figure 20: New Academic Complex Network

Figure 20 above shows the new network for academic complex. The number of BPS and Nortel Passport 8600 is still the same as the current design. In this design, there is no MLT between BPS and Nortel Passport 8600. All links from the access switch is split to two aggregation switches. Based on figure above, there are four aggregation switches which is located at the data center. For easy recognition, the switches are named Data Center (1) to Data Center (4). Links from access switches for Building 1 until Building 5 are split to Data Center (1) and Data Center (2); links for access switches for Building 20 to 23 are split to Data Center (2) and Data Center (3); links for access switches for Building 13 to 19 are split to Data Center (3) and Data Center (4). Each aggregation switches have almost the same load.

4.6.6 Pocket C and Pocket D

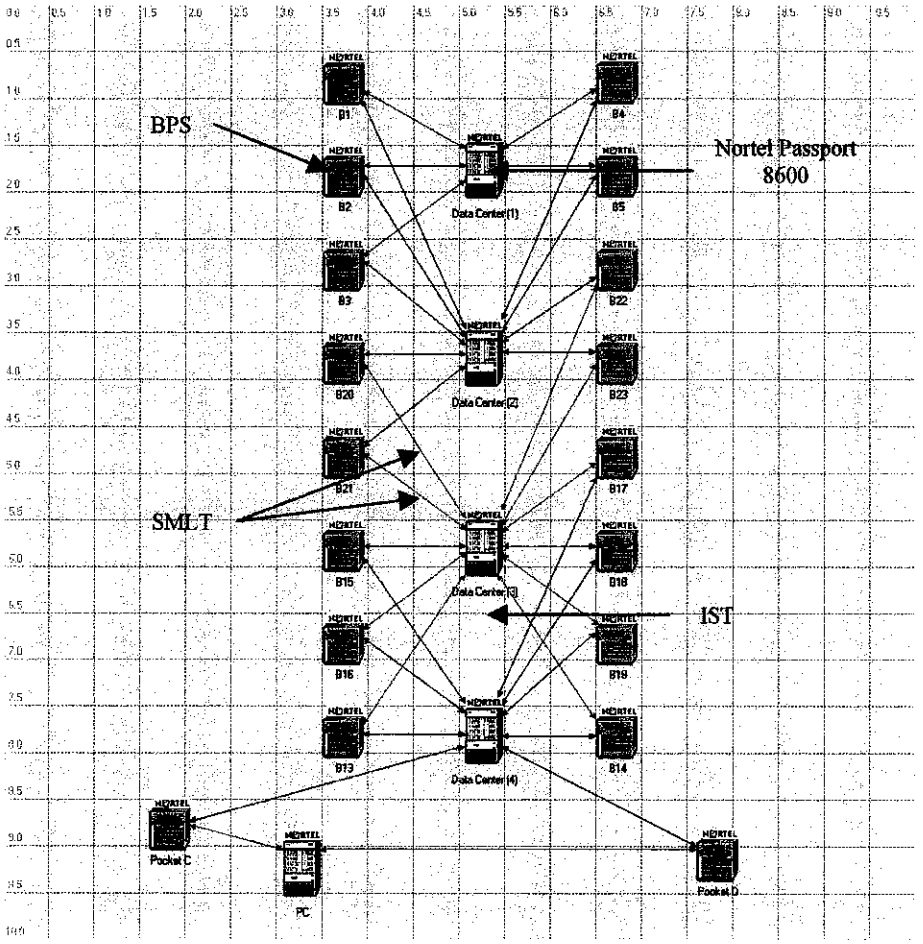


Figure 21: New Pocket C and Pocket D Network

Figure 21 shows the new network structure for Pocket C and Pocket D. Access switch at Pocket C and Pocket D is connected to Data Center (4) and PC by SMLT. Data Center (4) can communicate and exchange MAC addresses with Nortel Network 8600 at Pocket C through an IST.

4.7 Combining Network for All Villages in OPNET IT Guru

4.7.1 Current Network (without SMLT)

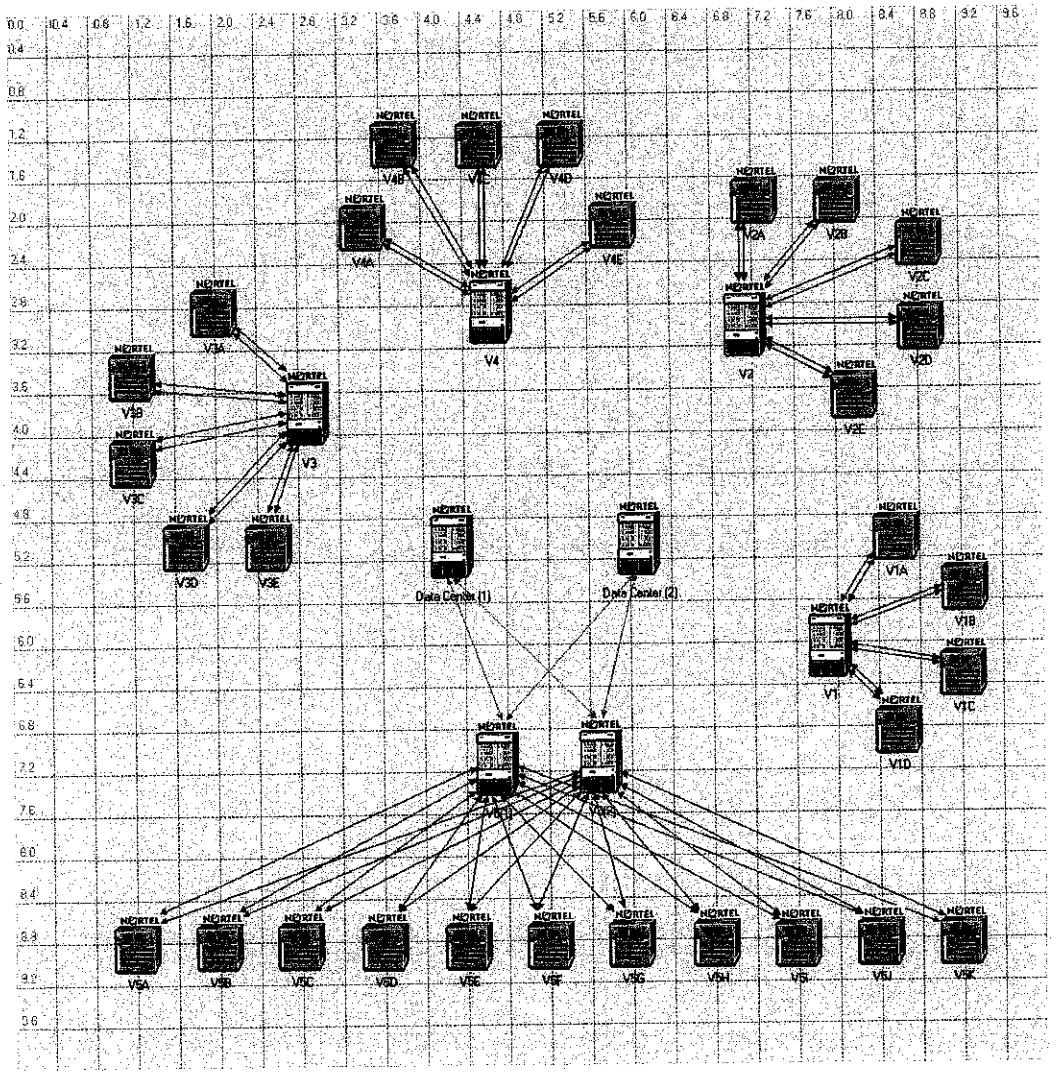


Figure 22: Current Village Network

Figure 22 shows the entire village network currently used. Only V5 has been implemented with SMLT architecture. The other villages are using MLT architecture. The main disadvantage of this network is that if the Nortel Passport for any villages except V5 failed, that village will be isolated from the whole UTP network. Another weakness is if the links between V2 and V4 is broken, V1 and V2 will automatically disconnect from the network.

4.7.2 New Network (with SMLT)

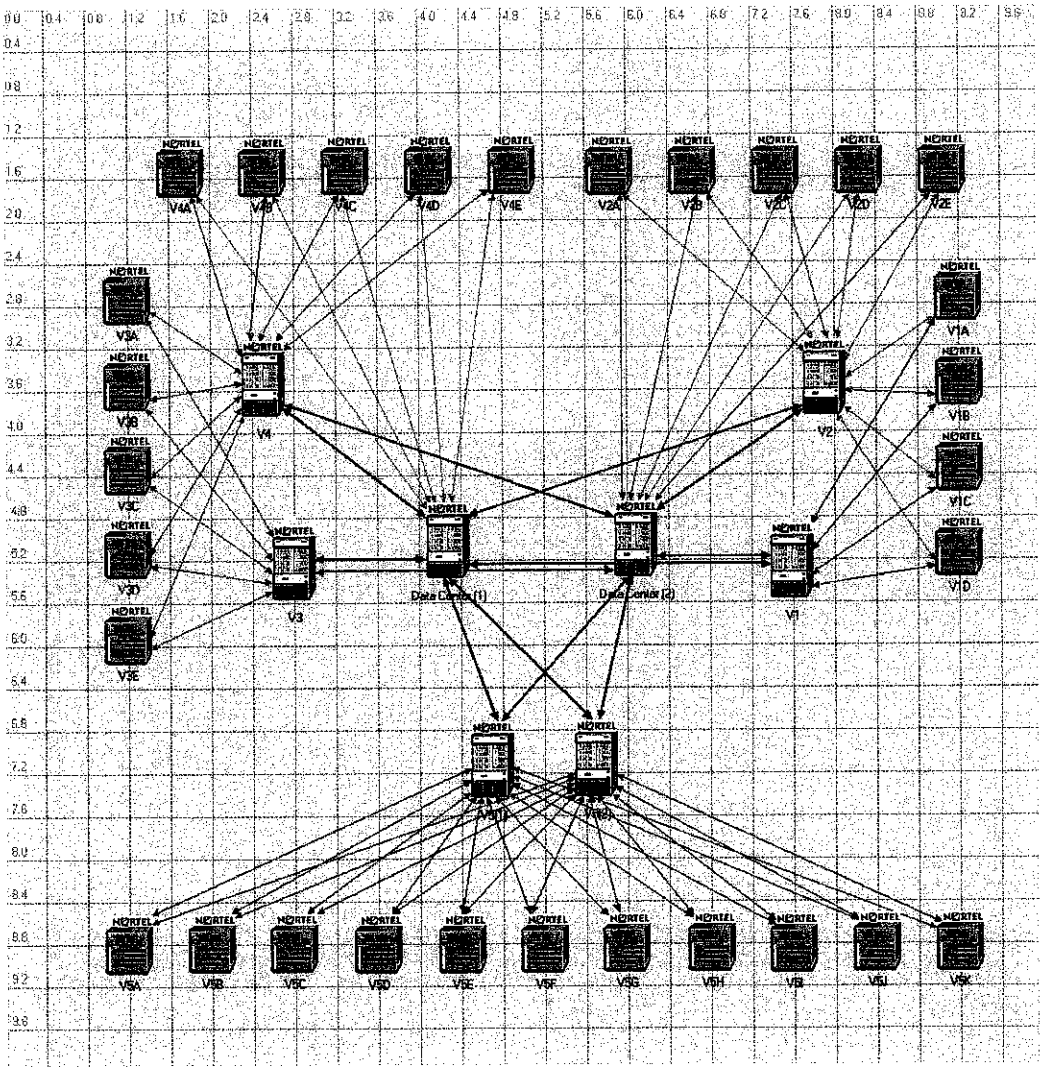


Figure 23: New Village Network

Figure 23 shows the entire new village network. All the villages have been implemented with SMLT architecture. Compared to the previous network, the new network will not have single point of failure. The network will be available all the time. The changes made to the current network did not incur any additional cost because there is no new device needed to upgrade MLT to SMLT. The available network devices can be use in SMLT architecture.

4.8 Results of the Simulation

Results of the simulation are being presented in graph. The current network and new network are being evaluated in term of bit error rate, Ethernet delay, processing delay, throughput and utilization.

In each graph, the current network is presented by blue line while the new network is presented in red line. The x-axis is the bit or packet while the y-axis is the time (second).

The simulation is done for an hour (1hr. 0min. 0sec.). Time elapsed is 1 second. The average speed of the simulation is about 8000 to 15000 per seconds.

The results given are for V1, V2 and academic complex only. V3 and V4 have the same output as V2 so the student does not display the results for V3 and V4 in this report. Pocket C, Pocket D and the whole village network cannot be simulated in this software because OPNET IT Guru can only handle 20 nodes.

4.8.1 Bit error rate

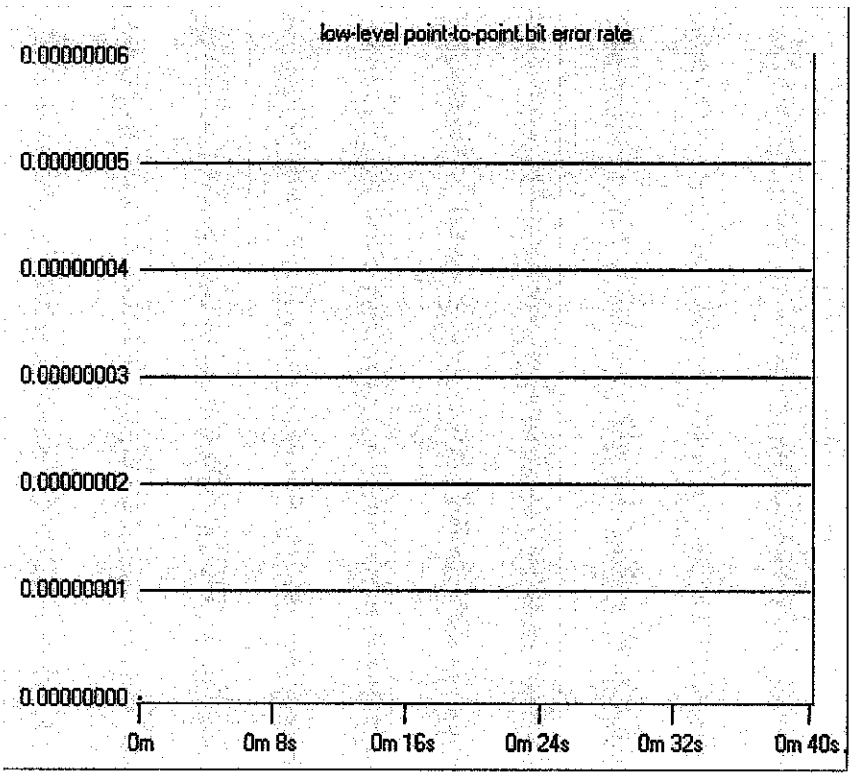


Figure 24: Bit error rate

Figure 24 above shows the bit error rate. All new network simulated in OPNET IT Guru Academic Edition has the same output. It can be assumed that there is not bit error rate because the number is too small. On paper, the bit error rate is not obvious. But, in real scenario, the result may be differs due to external factors such as virus, worm and hackers.

4.8.2 Ethernet delay

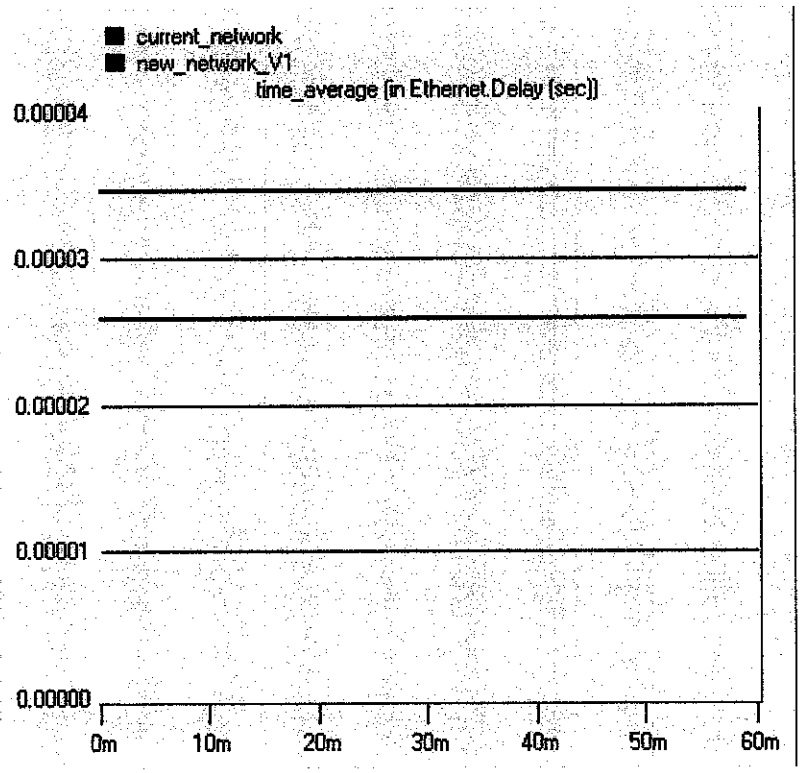


Figure 25: Ethernet delay for V1

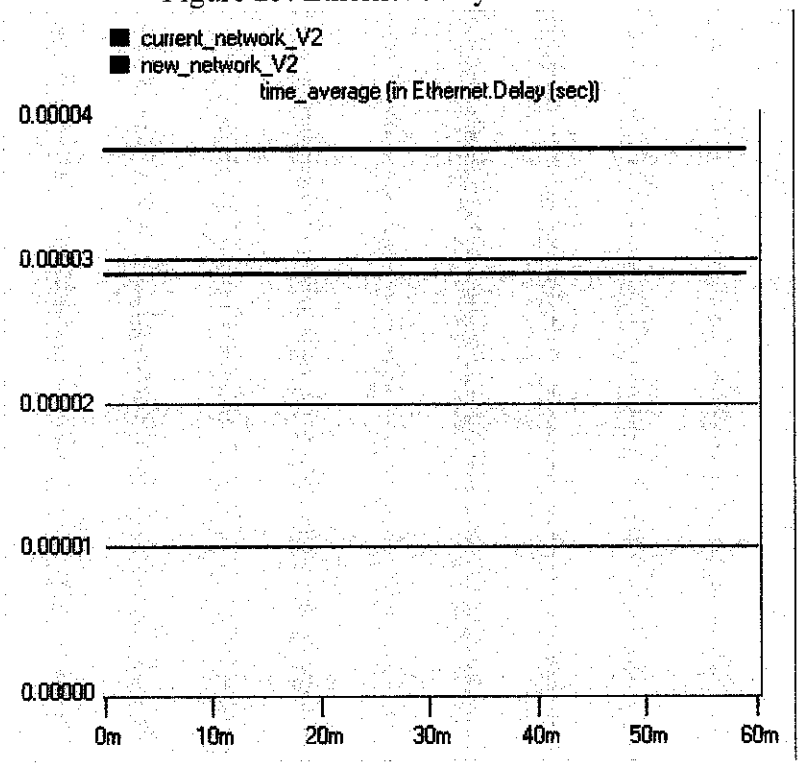


Figure 26: Ethernet delay for V2

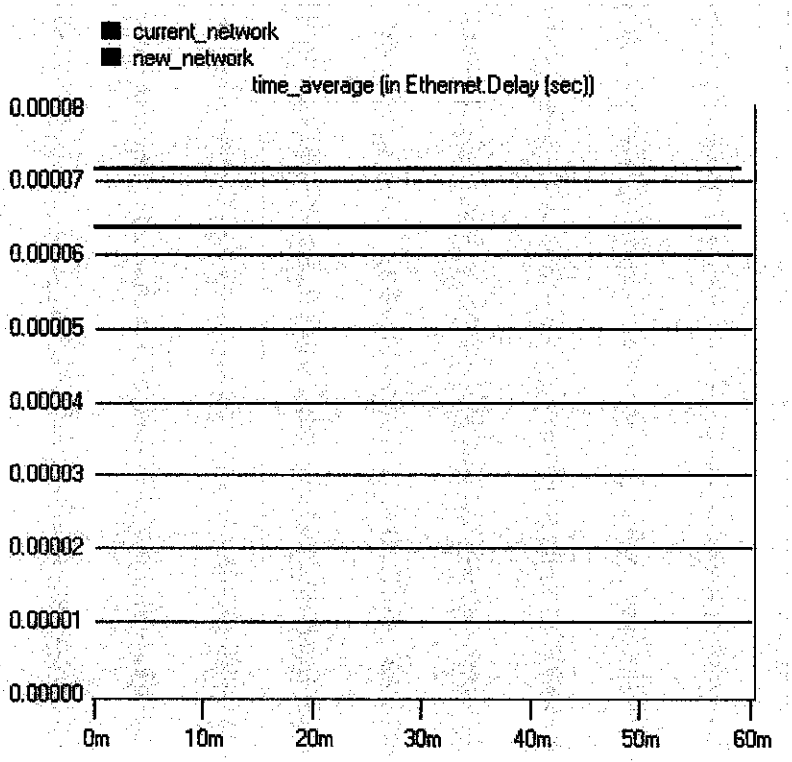


Figure 27: Ethernet delay for academic complex

4.8.3 Processing delay

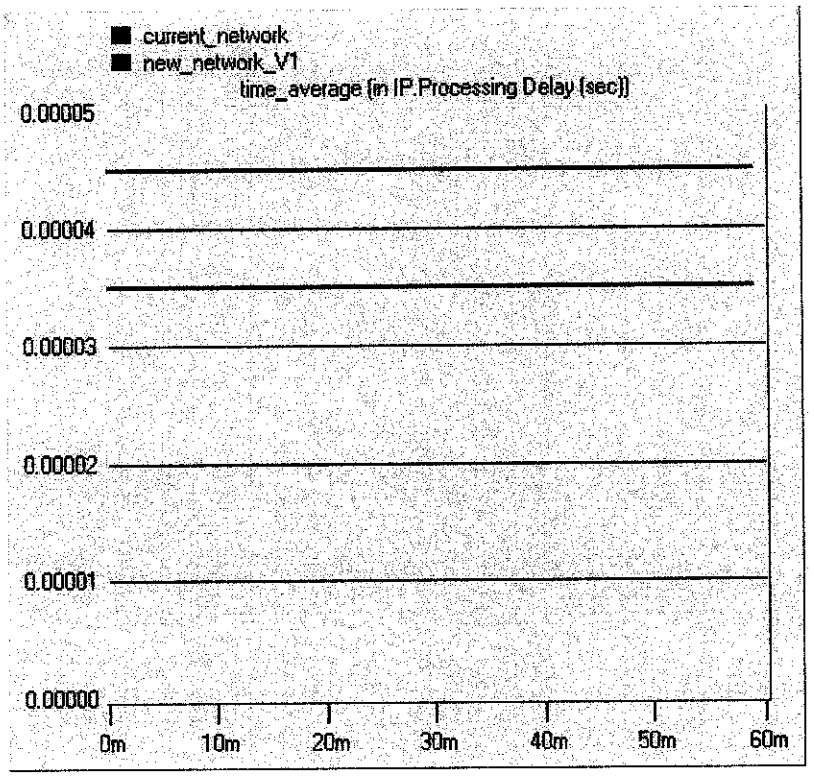


Figure 28: Processing delay for V1

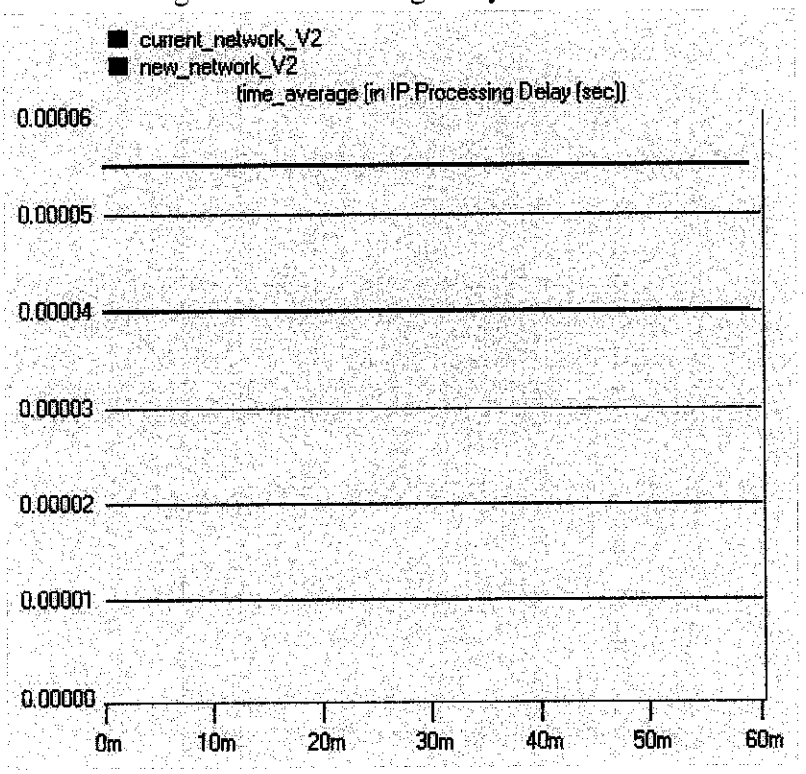


Figure 29: Processing delay for V2

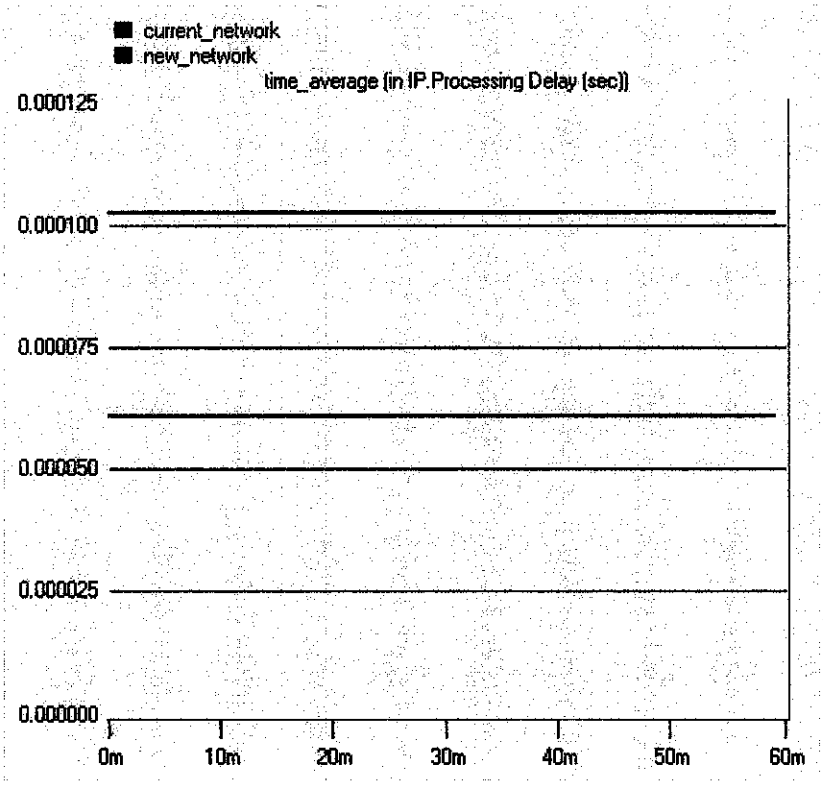


Figure 30: Processing delay for academic complex

4.8.4 Throughput

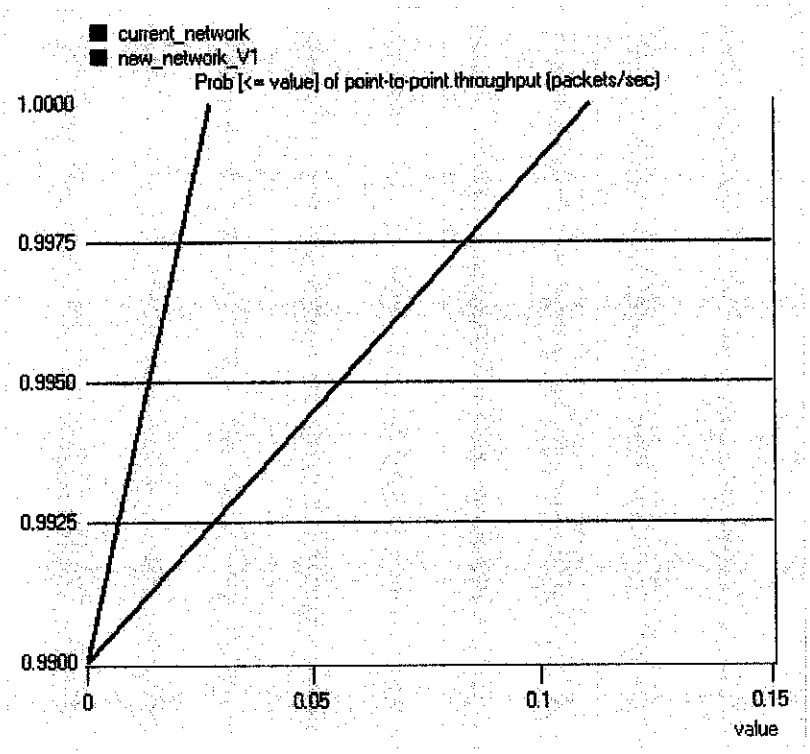


Figure 31: Throughput for V1

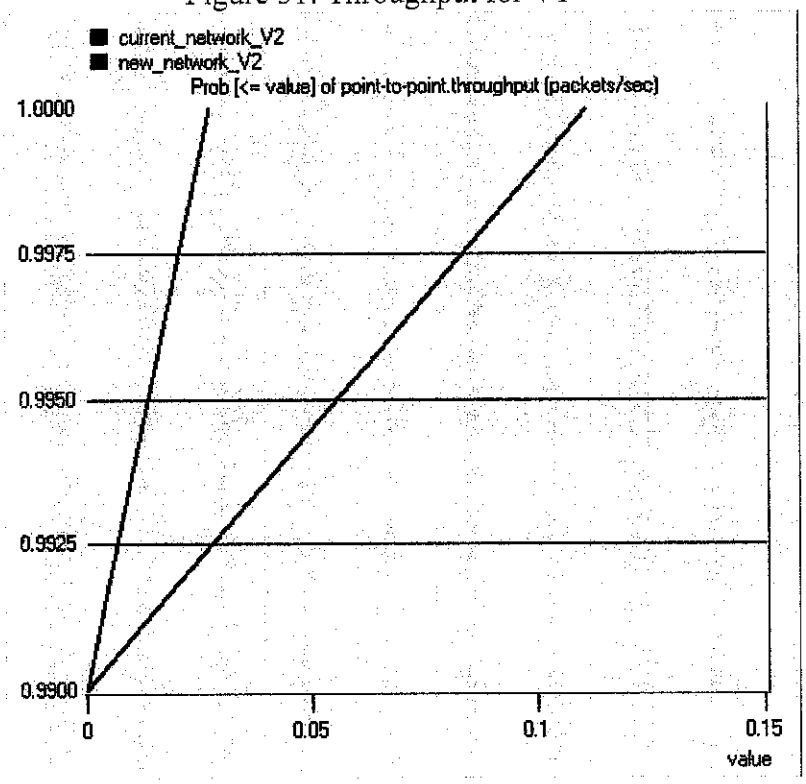


Figure 32: Throughput for V2

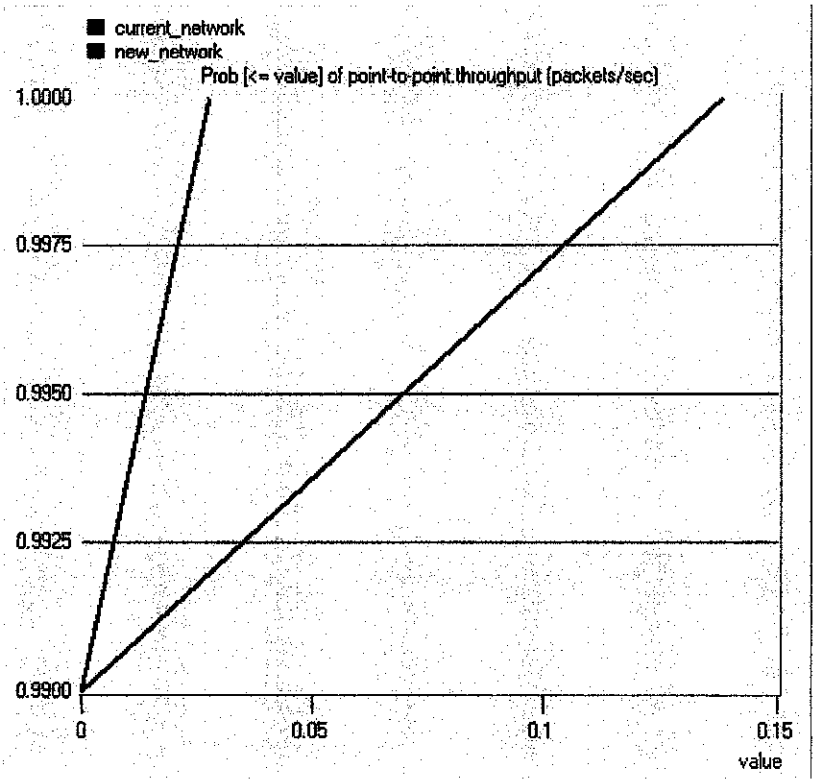


Figure 33: Throughput for academic complex

4.8.5 Utilization

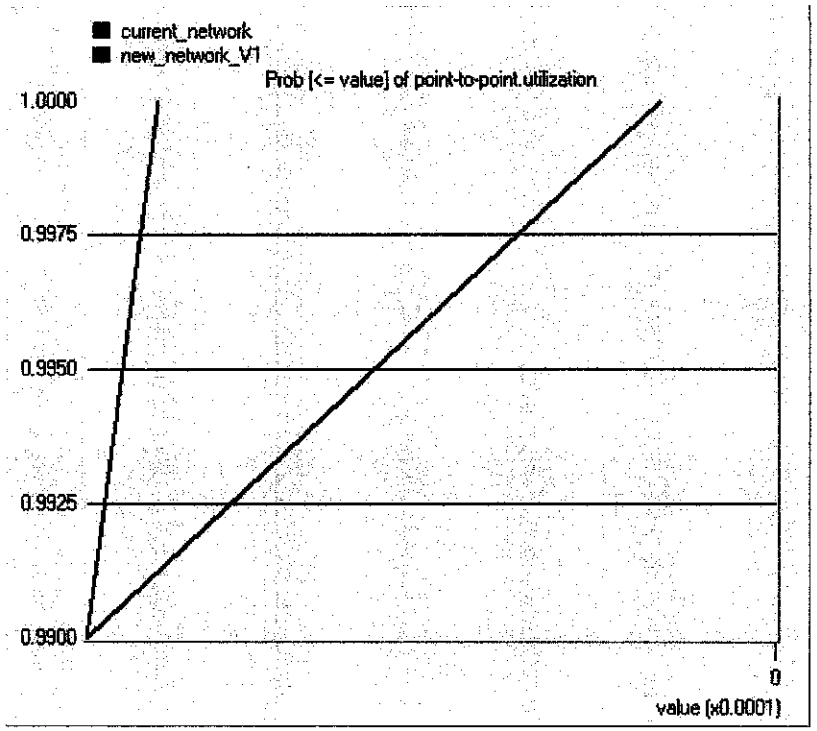


Figure 34: Network utilization for V1

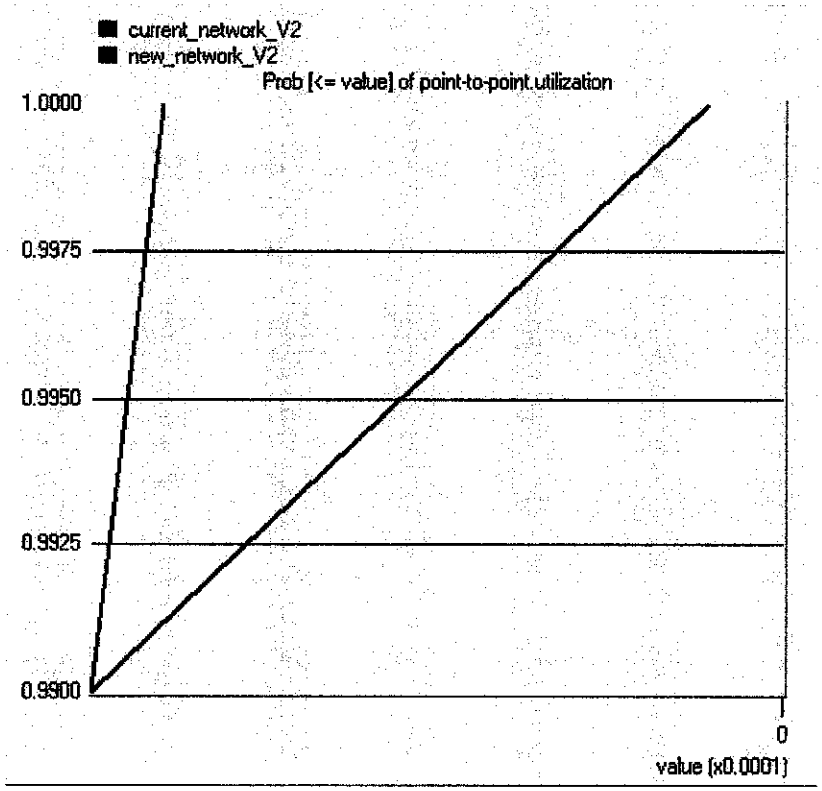


Figure 35: Network utilization for V2

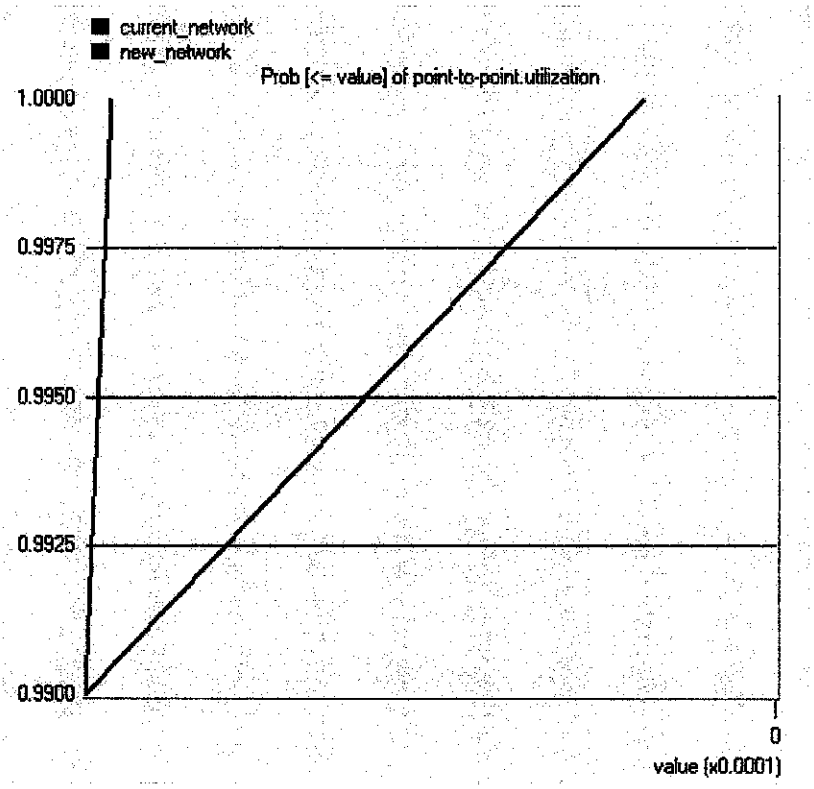


Figure 36: Network utilization for academic complex

4.9 Analyzing the Results

Based on the results of the simulation, the conclusion that can be made is that the new network performs better than the current network. There is hardly noticeable bit error rate in the new design. So, it can be assumed that there will be no loss of data in the network.

The Ethernet delay in the new network (with SMLT) is lesser than the current network. Even though the difference is not much but it can give great advantage to the network users. The processing delay of new network in each village and academic complex also differs from the current network used. The processing delay is shorter than the current network. The switches can send and receive packets faster.

The point-to-point throughput is different between current and new network. The new network has better throughput. There is more data moved successfully from one place to another for a given time in the new network compared to the current network. The new network is also being utilized more than the current network. There will be no unused ports.

SMLT provide huge increase in network availability. The level of availability is unique in the data world and truly moves data networking in the realms of carrier grade 99.999% uptime. In SMLT, there will be no single point of failure. Any single link or either aggregation switch can fail and the recovery will take place in less than three seconds. Moreover, SMLT is transparent to surrounding LAN devices. The deployment of SMLT will not modify other network component.

4.10 Failure Scenarios in SMLT

1. Loss of SMLT link

   The SMLT client switch detects link failure and sends traffic on the other SMLT link(s) just like what been done with standard MLT. Detection and fail-over takes less than one second.

2. Loss of aggregation switch

   The operational aggregation switch detects loss of partner (IST and keep alive packets lost) and changes all the SMLT trunks to regular MLT. If the partner returns, the operational aggregation switch detects this (IST becomes active) and moves the trunks back to regular SMLT operation once full connectivity is reestablished. Detection and fail-over takes less than five seconds.

3. Loss of IST link

   Normally, there will be more than one link in the IST. So, IST traffic resumes over the remaining links in the IST. Detection and fail-over takes less than one second.

4. Loss of multiple aggregation switches in different aggregation switch pairs
5. Loss of all IST links between an aggregation switch pair

   (In case 4 and 5, Nortel Networks claims that they have exceeded the goal of providing connectivity only after a single failure since this to occur, multiple failures must occur.)

4.11 Limitations of the Project

There are some limitations in this project. The limitations are:

1. OPNET IT Guru cannot simulate more than 20 trunk nodes in one design.

2. OPNET IT Guru does not have a detail specification on the link types.

3. SMLT features is only limited to 32 VLANs.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

In the proposed network structure, each access switch is connected to two Nortel Passport 8600 and both Nortel Passport 8600 is connected using an IST. This network structure has many advantages such as Layer 2 traffic load sharing, SMLT scaling and no single points of failure. Any single link or aggregation switch can fail and recovery will take place in less than three seconds. Compare to the current network structure, MLT is used to connect access switch (BPS) to Nortel Passport 8600. The disadvantage of this structure is that if the Nortel Passport 8600 encountered problem, the whole network connection for the network group will be separated from the overall network structure. SMLT should be implemented in UTP to improve the current network. SMLT does not require special hardware or complicated configurations. The hardware used currently will not be wasted because SMLT can be used with the available hardware. Besides providing the advanced resilient solutions, SMLT can increase the available bandwidth from the wiring closer to the network core by enabling a software feature. Connections that were unused because of the Spanning Tree's loop protection can now be used to the highest potential. Application like IP Telephony, multicast and e-learning is very valuable to an organization but without adequate bandwidth and network resiliency, these applications cannot perform their task. By using the simulation as a reference, the new network structure using SMLT can be implemented in UTP. With proper designed network solutions, the risk of network downtime can be minimized. Incorporating resiliency into the network core, the user access points can remain connected to the network even in the failure situation.

5.2 Future Works

Suggestions for future works:

1. Get expert's feedback about the project.

2. Get approval from the expert about the project acceptance.

3. Analyze in detail the current UTP network.

4. Research on new technologies that can be used with SMLT and produce a new advance network for UTP.

5. Get proven data about the advantage of SMLT.
   Implement SMLT in the real UTP network. For example, implement SMLT in Village 1 and Village 2. Get the real data from the network itself to prove that SMLT really gives great benefit to UTP. Collect data that can be use as evidence rather than data from simulation.

REFERENCES

Article:

1. Eliminate Single Points of Failure by Nortel Networks (http://www.nortelnetworks.com/products/01/passport/8600_rss/collateral/nn108460-060304.pdf)

2. Designing Resilient Network by Nortel Networks (http://www.nortelnetworks.com/products/01/passport/collateral/nn107680-031804.pdf)

3. Passport 8600 Split Multi-Link Trunking Frequently Asked Questions by Nortel Network (http://www.nortel.com/products/library/collateral/p8600_smlt_faq.pdf)

4. Passport 8600 Split MLT Overview by Nortel Networks (http://www116.nortelnetworks.com/docs/bvdoc/ene_tech_pubs/pp8600_split_mlt_overview.pdf)

5. Understanding Spanning Tree Protocol by Cisco System Inc. (1997) (http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm)

Book:

1. Kevin Brown, Leann Christianson. 2005, OPNET *Lab Manual to Company*, New Jersey, Pearson Education, Inc.

APPENDICES

(This page is intended to be empty. Please refer to the next page)

Please mark [x] in the box given and answer all questions.

1. What is your profession?

   [ ] Academic Staff [ ] Management Staff [ ] Student

2. How do you rate the network connection in UTP?

   [ ] Excellent [ ] Good [ ] Ok [ ] Bad [ ] Very Bad

3. Is network connection important to you?

   [ ] Yes [ ] No

4. If yes, why do you need the network connection? *(can choose more than one answer)*

   [ ] Communication (e.g. email, Google Talk, Yahoo! Messenger, Skype, etc)

   [ ] Search for information (e.g. Google, Yahoo!, MSN, etc)

   [ ] On-line transaction (e.g. BCB, MAYBANK, etc)

   [ ] e-learning

   [ ] Others: _____

5. Do you have any difficulties in using the network connection?

   [ ] Yes [ ] No [ ] Sometimes

6. What is the problem that you usually faced in using the network? *(can choose more than one answer)*

   [ ] Slow connection speed [ ] Server down [ ] Unstable network

   [ ] Others: _____

7. Do you think network connection in UTP should be improved?

   [ ] Yes [ ] No

8. Briefly, please give your comment on question 7:

   _____

   _____

Thank you.

NORTEL NETWORKS
BUSINESS WITHOUT BOUNDARIES

eliminate

single points of failure

White Paper

Split Multi-Link cing/Routed Split ılti-Link Trunking

What is Split Multi-Link Trunking?

Typical resilient Ethernet networks consist of wiring closet (edge) switches dual homed to network center aggregation (core) switches in a building or campus.

More and more, network servers are being multi-homed to server switches—enabling higher bandwidth availability and improved resiliency. Similarly, in carrier and Internet Service Provider (ISP) environments, customer premises equipment (CPE) devices may also be dual homed to two aggregation switches at a point of presence (POP) to realize the same benefits. Such implementations, however, require the use of the Spanning Tree Protocol to protect the network against loops.

While the Spanning Tree Protocol in any form (IEEE 802.1D/w) suits this purpose, it is not without limitations. It will protect against loops, but cannot be optimized to build redundant networks and at the same time fully utilize all links (blocked ports) without micro-management of the protocol.

gregation technologies have become popular for improving link bandwidth and/or protecting against link failures. IEEE 802.3ad rt of IEEE 802.3-2002 clause 43) is the standardized link aggregation protocol, although various vendors have developed their prietary implementations. While IEEE 802.3ad has proven effective for point-to-point applications, it was not designed to recover nodal failure.

ulti-Link Trunking (SMLT), a Nortel Networks extension to IEEE 802.3ad, improves on the level of Layer 2 resiliency by ıg nodal protection in addition to link failure protection and flexible bandwidth scaling. It achieves this by allowing edge switches EE 802.3ad to dual home to two SMLT aggregation switches. It is important to note that SMLT is transparent to attached supporting IEEE 802.3ad.

SMLT inherently avoids loops due to its superior enhanced-link aggregation-control-protocol, when designing networks using it is not necessary to use the IEEE 802.1D/w Spanning Tree protocols. Instead, a method is used that allows two aggregation s to appear as a single device to edge switches that are dual homed to the aggregation switches. The aggregation switches are inter-ed using an InterSwitch Trunk (IST), over which they exchange addressing and state information, permitting rapid fault detection warding path modification. Although SMLT is primarily designed for Layer 2, it also provides benefits for Layer 3 networks.

ıre the enhancements for Layer 3?

· edge-switch aggregation applications, network operators choose to enable routing at the aggregation/distribution layer. The Router Redundant Protocol RFC 2338 (VRRP) provides router redundancy by defining a master VRRP routing instance as a gateway and a backup default gateway. This is a commonly used network topology that provides reasonably fast failover (approxi- hree seconds). However, it only allows one routing instance to be active at a time for a given IP address on a VLAN, thus limiting ing bandwidth to one router per VLAN.

Networks has extended VRRP in conjunction with SMLT to provide an active-active concept, which allows two or more active instances per VLAN/IP subnet—resulting in a significant boost to available routing performance while also providing redundancy.

RP active-active concept is achieved by a VRRP extension called VRRP Backup-Master. The VRRP Backup instance can also traffic as long as it is part of an SMLT VLAN. Thus, SMLT not only provides forwarding for all active links, but also provides on all participating routers. Since all VRRP instances for a given VLAN are forwarding traffic at the same time, network failures ause significant traffic interruption. The VRRP state machine delay of three seconds is not involved in the traffic recovery process, owing sub-second failover in case of a router failure.

outed Split Multi-Link Trunking (RSMLT), Nortel Networks has taken the router redundancy concept one step further to enable ndancy in core networks and to allow for rapid failover—eliminating routing protocol timer dependencies when network failures r.

is Routed Split Multi-Link Trunking?

y cases, core network convergence is dependent on the time that routing protocols require to converge. This can cause network otions ranging from seconds to several minutes, depending on the actual routing protocol.

outed Split Multi-Link Trunking (RSMLT), Nortel Networks introduces a feature that allows rapid failover for core topologies by ng an active-active router concept to core SMLT networks. Supported scenarios include SMLT triangles, squares, and SMLT full opologies with routing enabled on the core VLANs. Routing protocols can include any available routing protocol such as IP Static Routes, RIP1, RIP2, OSPF, BGP, and IPX RIP. In the case of core router failures, RSMLT takes care of the packet ling, thereby eliminating the possibility of packets being dropped during routing protocol convergence.

ons to deploy SMLT/RSMLT

vorks grow ever more critical, there is an increasing demand for multiple paths from all wiring closet switches into the core of the k to eliminate all single points of failure.

allenge of designing a resilient network involves not only eliminating single points of failure, but doing so without ending up with (and costly) capacity. The network must also be able to reroute around failures—with typical requirements in the sub-5-second

e and data convergence becomes more prevalent, today's network managers are seeking reliable and scalable solutions that focus on twork availability and optimal use of bandwidth. Solutions must be simple to implement, as transparent as possible, and have the to interoperate with the majority of existing server/wiring closet/CPE/edge devices. The SMLT solution succeeds in addressing all e requirements where previous efforts have failed.

izing down time during scheduled network maintenance, such as system upgrades or configuration changes, is also a key require- of today's networks. Providing network operators with tools that allow them to apply network changes during working hours, rather ter hours, can lead to significant cost savings over time. The SMLT/RSMLT solution provides a simple way of upgrading ation/core devices without impacting overall network availability.

tions

elving into a more detailed description on how SMLT works, it is important to define some of the terms that are used
aper.

aggregation switch—A switch that connects to multiple wiring closet switches, edge switches, or CPE devices, typically
a single building.

terSwitch Trunk)—One or more parallel point-to-point links that connect two aggregation switches together. The two
ation switches use this channel to share information so that they may operate as a single logical switch. There can be only
T per SMLT aggregation switch.

Multi-Link Trunk)—A method of link aggregation that allows multiple Ethernet trunks to be aggregated together in order
vide a single logical trunk. An MLT provides the combined bandwidth of the multiple links, as well as the physical layer
tion against the failure of any single link.

Split Multi-Link Trunk)—An MLT, in which one end is split between two aggregation switches.

Client—A switch that is located at the edge of the network (for example, in a wiring closet or CPE). An SMLT client switch must
e to perform link aggregation, such as with MLT or some other compatible method, but does not require any SMLT intelligence.

VLAN—A VLAN that has RSMLT enabled for router redundancy and is therefore protected by active-active SMLT aggregation
default gateways.

loes SMLT work in a Layer 2 network?

illustrates a configuration that includes two Passport* 8600 Routing Switches as link aggregation capable (MLT or IEEE
) switches E and F, and four separate wiring closet switches A, B, C, and D, which could represent any MLT-compatible
ncluding:

ort 8300 Ethernet Switch

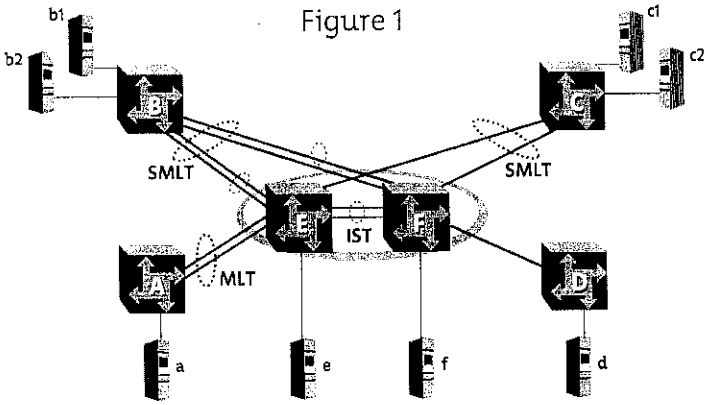
ack* 460 Switch

ack 470 Switch

ack 5510 Switch

closet switches B and C are connected to the
ion switches via multi-link trunks split
the two aggregation switches. For example,
client switch B may use two parallel links for
ection to E, and two additional parallel links
nection to F.

Figure 1



client switch C may have only a single link to both E and F. A is also configured for MLT, but the MLT terminates on only one
n the network core. Switch D has a single connection to the core. Although both switch A and switch D could also be configured
inate across both of the aggregation switches using SMLT, neither switch will benefit from the advantages of SMLT in the
ration shown.

example shows, implementation of SMLT only requires two SMLT-capable aggregation switches, which must be connected via
(InterSwitch Trunk). The aggregation switches use this communication channel for two processes.

is used to confirm that each switch is alive and to exchange MAC address information. This process requires that the link be
and not exhibit a single point of failure.

ly, the common channel is used for the forwarding of flooded packets or packets destined for non-SMLT-connected switches
ers physically connected to the other aggregation switch. The amount of traffic from a single SMLT wiring closet that requires
ling across the IST is likely to be small (often less than five percent); however, if the aggregation switches are terminating
tions to a large number of Gigabit-connected SMLT clients, the IST traffic may be significant. These requirements dictate

IST must be a multi-Gigabit MLT with connections across different line cards (Distributed-MLT) on both aggregation switches to ensure there is no single point of failure in the IST.

LT client switches are dual homed to the two aggregation switches but they require no knowledge of whether they are connected le switch or to two switches. SMLT intelligence is required only on the aggregation switches. Logically, they appear as a single) the edge switches.

also includes end stations connected to each of the switches. The end stations—**a**, **b1**, **b2**, **c1**, **c2**, and **d**—are typically hosts. ions **e** and **f** may be hosts, servers, or routers.

lient switches B and C may use any method for determining which link of their multi-link trunk connections to use for ng a packet, as long as the same link is used for a given Source/Destination (SA/DA) pair, regardless of whether or not the DA is)y B or C. This requirement ensures that there will be no out-of-sequence packets between any pair of communicating devices. ion switches will always send traffic directly to an SMLT client switch and only use the IST for traffic that cannot be forwarded 'e direct way. The examples below help explain the process.

om **a** to **b1** and/or **b2** (assuming **a** and **b1**/**b2** are communicating via Layer 2) goes from switch A to switch E and then is d through its direct link to switch B. Traffic coming down from **b1** or **b2** to **a** is sent by switch B on one of its MLT ports. Since ot know that the MLT is anything special, it sends traffic from **b1** to **a** on the link to switch E and the traffic from **b2** to **a** on to switch F. In the case of traffic from **b1**, switch E simply forwards the traffic directly to switch A, while traffic from **b2**, which it switch F, is forwarded across the IST to switch E and then to switch A.

om **b1**/**b2** to **c1**/**c2** will always be sent by switch B through its MLT to the core. Regardless of which switch (E or F) it arrives at, sent directly to switch C through the local link. This is why dual-homing all client switches to the SMLT aggregation pair will he amount of traffic on the IST link. A single IST failure (all SMLT links active) in this scenario will not cause traffic interrup- ereby minimizing the risk of network downtime even further.

om **a** to **d**, and vice versa, is forwarded across the IST because it is the shortest path, but this is treated purely as a standard link consideration given to SMLT and the fact that it is also an IST.

traffic from **f** to **c1**/**c2** will be sent directly from switch F. Return traffic from **c1**/**c2** will be passed across the IST if switch C sends gh the link to switch E.

ems solved

2 *traffic load sharing*

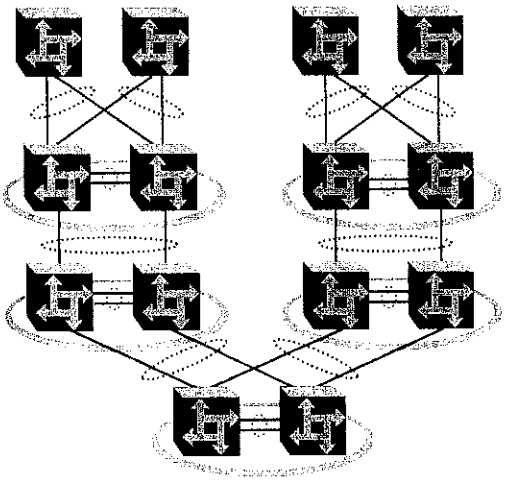
e SMLT client perspective, load sharing is achieved by the MLT path n algorithm used on the edge switch. Usually this is done on an ST MAC address basis, or SCR/DST IP basis.

aring from the aggregation switch perspective is achieved by sending all estined to the SMLT client switch directly, and not over the IST trunk. trunk is never used for cross traffic to and from an SMLT dual- wiring closet. Traffic received on the IST by an aggregation switch is rwarded on SMLT links because the other aggregation switch will have ed that job, thus eliminating the possibility of a loop in the network.

caling

re 2 shows, it is also possible to configure SMLT groups within the the network; however, in this case both sides of the link are configured LT.

Figure 2



ology allows to build multi-tiered bridged networks without intro-
etwork loops and at the same time have all links forwarding traffic.

LT building block depicted in Figure 3 is referred to as the SMLT
Configuration. The SMLT configuration in Figure 4 shows an
ull-Mesh Configuration. Note that in both configurations all SMLT
the same SMLT ID (shown through the MLT ring).

Figure 3

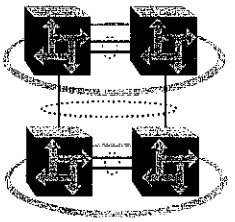
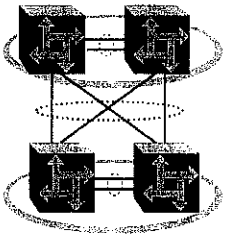


Figure 4



ile point of failure

le link or aggregation switch can fail and recovery will take place in
three seconds. Note that this number is conservative. The inten-
at some traffic will suffer no packet loss and the remaining traffic
rience loss for less than one second. See the analysis that follows
er details.

e scenarios

o 1: Loss of SMLT link

LT client switch detects link failure and sends traffic on the other SMLT link(s) in the same manner as a standard MLT.
n and failover takes less than one second.

ık is not the only one between the SMLT client and aggregation switches in question, then the aggregation switch also simply
dard MLT detection and rerouting to move traffic to the remaining links. If the link is the only one to the aggregation switch,
failure detection, the switch informs the other aggregation switch of SMLT trunk loss. The other aggregation switch then treats
T trunk as a regular MLT trunk. If the link is re-established, the aggregation switches detect this and move the trunk back to
MLT operation. Detection and failover/recovery takes less than one second.

o 2: Loss of aggregation switch

LT client switch detects link failure and sends traffic on the other SMLT link(s) in the same manner as a standard MLT.
n and failover takes less than one second.

rational aggregation switch detects loss of partner (IST and keep alive packets lost) and changes all the SMLT trunks to regular
nks. If the partner returns, the operational aggregation switch detects this (IST becomes active) and moves the trunks back to
MLT operation as soon as full connectivity is re-established.

n and recovery takes less than five seconds.

o 3: Loss of IST link

LT client switches do not detect a failure and communicate as usual. In normal use, there will be more than one link in the IST
self a distributed MLT). Thus IST traffic resumes over the remaining links in the IST. Detection and failover takes less than one

o 4: Loss of multiple aggregation switches in different aggregation switch pairs

this case we have exceeded the goal of providing connectivity only after a single failure, since for this to happen, multiple failures
ur.

LT client switches do not detect a failure and communicate as usual.

h aggregation switch pair is a separate entity, they are not affected by failures elsewhere. Connectivity is also unaffected; however,
ilable bandwidth is drastically reduced, packet loss and increased latency may occur.

o 5: Loss of all IST links between an aggregation switch pair

this case we have exceeded the goal of providing connectivity only after a single failure, since for this to happen, multiple failures ur.

y unlikely event that all links in the IST fail (up to eight links can be part of an IST and they can reside on up to eight different ules), the aggregation switches do not see each other anymore (keep alive lost) and both assume that their partner switch is dead. for the most part there are no ill effects in the network if all SMLT clients (server/switches) are dual homed to the SMLT aggre- itches, because no data traffic is flowing through the IST for those devices. All single-homed devices will likely see a traffic ecause some traffic has to flow through the IST to reach its destination. In this case, the recommendation is to dual-home all evices to both SMLT aggregation switches.

varding, while functional, may not be optimal since the aggregation switches may never learn some of the MAC addresses, in flooded traffic that would normally not be flooded.

ompared to Spanning Tree/Rapid Spanning Tree

designed as an extension to the IEEE 802.3ad link aggregation specification and also covers some IEEE 802.1D/w network , especially at network edges where loops are introduced due to dual homing of network edge devices.

owing characteristics distinguish SMLT from the Spanning Tree/Rapid Spanning Tree protocol.

es not have any blocking links. Therefore all configured bandwidth is available for traffic forwarding. In a Spanning Tree network ngle trunk is forwarding and all other links are blocking. To overcome this in a Spanning Tree scenario, multiple Spanning Tree ave to be configured on switch-to-switch links. The multiple Spanning Tree groups then have to be engineered in a way to link bandwidth. This can be very cumbersome. A given VLAN however can never be optimized to use all available links in ng Tree environment. SMLT overcomes this disadvantage by allowing all links to be active and forwarding for all VLANs.

iT protocol is used only on a set of two switches—the SMLT aggregation pair. The protocol, therefore, does not have any delays because the two neighbors are directly connected. The Spanning Tree protocol, in contrast, uses a network protocol that ng multiple switches. This introduces latency and slows the network convergence down significantly and increases the network ity.

nvergence targets are sub-second in every failure scenario. Rapid Spanning Tree can be as fast in certain network failure , but it can also take much longer if the root bridge fails or multi-hop convergence is required. Up to 10 seconds of network ie have been measured.

g Tree has a maximum of seven hops, limiting scalability significantly. SMLT, however, does not have a hop limit. SMLT mitations are dictated by the amount of MAC addresses that a Layer 2 network can support.

nning Tree network, any network link status change causes a TCN (Topology Change Notification) and all members of the g Tree flood all of the learned MAC address forwarding tables. Significant flooding occurs until all MAC addresses are re-learned. MLT network, however, only the two SMLT aggregation switches, which are directly/indirectly connected to the failing link, will purge their forwarding databases. The flooding is not propagated throughout the whole network, thus reducing network traffic ntly.

work convergence scenario of a Rapid Spanning Tree network, the IEEE standard notes that some amount of duplicate traffic is during failover. In SMLT, however, the state-machines have been designed to avoid packet duplication.

g Tree is a great technology to avoid network loops; however, SMLT is far superior in providing the tools for:
ning resilient networks
ging all installed bandwidth
ng the VLAN/IP subnet complexity low
ing for network maintenance during working hours

nhancements

introduction in 2001, SMLT has seen several enhancements. Initially introduced as a dual-homing architecture of switches ng static link aggregation, it has been extended to support large amounts of dual-homed network servers leveraging link aggrega- th the support of Link Aggregation Control Protocol (LACP), the dynamic link aggregation protocol of IEEE 802.3ad, and an extension for link-aggregation tunneling through a service provider core, an even wider range of applications can be covered.

.o SMLT/RSMLT work in a Layer 3 environment?

depicts a typical redundant network with user aggregation, core, and server access layers. In order to keep the amount of IP .ow, one VLAN/IP subnet A is spanning all wiring closets. SMLT provides the loop-free topology and enables all links to be ng for VLAN 1/subnet A. The aggregation layer switches have routing enabled and provide an active-active default gateway ality through either VRRP with Backup-Master (as described earlier) or through RSMLT. In either case, routers R1 and R2 ırding traffic for IP subnet A.

ıre IP subnet B with OSPF as the routing protocol is being used. Routers R1 and R2 are providing router backup for each ıt only for the edge IP subnet A, but also for the core subnet B. Similarly, routers R3 and R4 are providing router redundancy .bnet C and also for core subnet B.

ɔ you design and configure an RSMLT network?

is based on SMLT, which means all SMLT configuration rules apply. In addition to this, RSMLT is enabled on the SMLT ion switches on a per VLAN basis. The VLAN has to be a member of SMLT links and the IST trunk, and also be routable ess configured). All four routers in Figure 5 must have an Interior Routing Protocol (IGP), such as OSPF, configured on them, ·ugh it is independent from RSMLT. There are no changes to any IGP state machines and any routing protocol, including static an be used with RSMLT.

pair switches provide backup for each other. As long as one of the two routers of an IST pair is active, traffic forwarding is for both next hops R1 and R2, and R3 and R4, respectively.

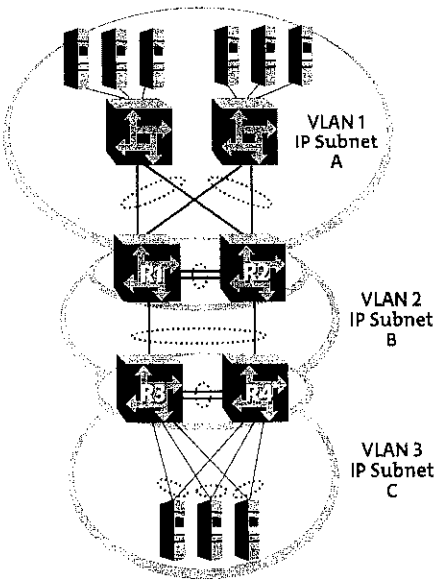
ɔ scenarios

ɪ1 failure:

ıple, R3 and R4 are using both R1 as their next hop to reach IP subnet A. Even R4 sends the packets to R2, they will be routed directly at R2 into subnet A. R3 packets towards R1 and they are also sent directly into subnet A. When R1 fails, ɔts will be directed to R2, with the help of SMLT. R2 still routes for R2 and R1. SPF convergences, the routing tables in R3 and R4 change their next hop to R2 to reach IP subnet A. The network administrator can choose to set the hold-up e., for the amount of time R2 will route for R1 in a failure case) for a time period han the routing protocol convergence, or set it as indefinite (i.e., the pair always ɔr each other).

ɔplication where RSMLT is used at the edge instead of VRRP, the hold-up timer indefinite is recommended.

Figure 5.
Router R1 recovery



ɪ1 recovery

ɔ1 reboots after a failure, it becomes active as a VLAN bridge first. Packets to R1 are switched, using the bridging forwarding table, to R2 for as long as the wn timer is configured. Those packets are routed at R2 for R1. Similar to VRRP, l down timer value needs to be greater than what the routing protocol requires to ɔ its tables.

e hold down time expires and the routing tables have converged, R1 starts routing packets for itself and also
herefore, it does not matter which one of the two routers is used as the next hop from R3 and R4 to reach
t A.

homed IP subnets are configured on R1 or R2, it is recommended to add another routed VLAN to the ISTs
er routing protocol metrics as a traversal VLAN/subnet in order to avoid unnecessary ICMP redirect genera-
sages. This recommendation is also applicable to VRRP implementations.

sion

ilure analysis shows, SMLT/RSMLT provide a huge increase in network availability. In all cases, except
5, there is no permanent loss of connectivity and the recovery from any failure is in the sub-second area.
es, including scenario 5, only a small percentage of traffic will be affected by the failure, while the remaining
completely unaffected. This level of availability is unprecedented in the data world and truly moves data
ng in the realms of carrier-grade 99.999 percent uptime.

LT/RSMLT is transparent to surrounding LAN devices, the solution is scalable throughout the LAN and
eployed without the need to modify other network components.

ed States:
orks
ive, Research Triangle Park, NC 27709

:
orks
Road,Suite 100, Brampton, Ontario L6T 5P6

an and Latin America:
orks
de Terrace, Sunrise, FL 33323 USA

orks
Office Park, Westacott Way, Maidenhead Berkshire SL6 3QH UK

orks
Victoria Avenue, Chatswood, NSW, 2067, Australia

tworks is an industry leader and innovator focused on transforming how the world
icates and exchanges information. The company is supplying its service provider and
e customers with communications technology and infrastructure to enable value-added
oice and multimedia services spanning Wireless Networks, Wireline Networks, Enterprise
, and Optical Networks. As a global company, Nortel Networks does business in more
countries. More information about Nortel Networks can be found on the web at:

.nortelnetworks.com

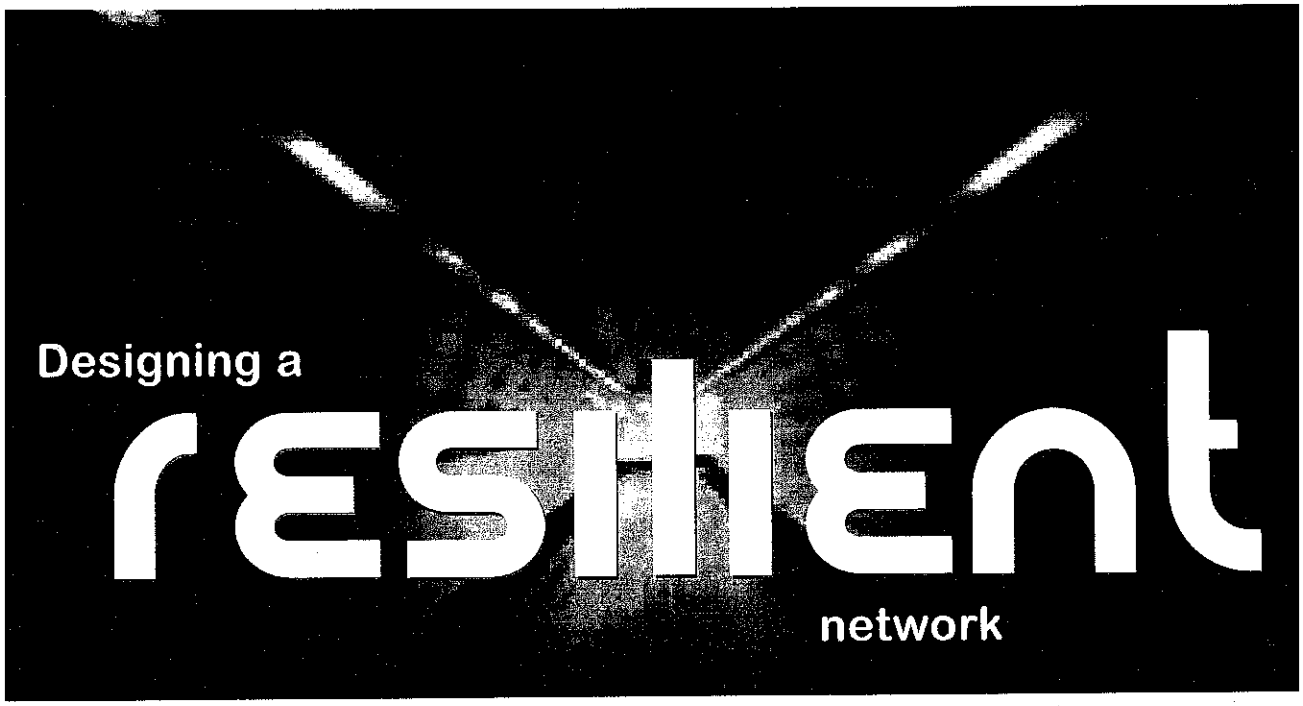
nformation, contact your Nortel Networks representative, or
4 NORTEL or 1-800-466-7835 from anywhere in North America.

works, the Nortel Networks logo, the globemark design, BayStack, and Passport are trademarks of Nortel
ll other trademarks are the property of their owners.

2004 Nortel Networks. All rights reserved. Information in this document is subject to change without notice.

60-060304

RTEL
NETWORKS
SS WITHOUT BOUNDARIES



Technical Brief

lit Multi-Link Trunking
Passport 8600

Market requirements for a resilient network

Unplanned network outages can affect all aspects of a business. Lost sales, increased overtime, loss of employee productivity, and even declining customer loyalty can be attributed to issues surrounding network outages. The current business environment is more competitive than ever. Any company that possesses even a slight advantage whether with collaborative applications or customer relationship management tools can dominate a market. Now more than ever, companies are looking for a competitive edge.

Business-critical applications are greatly affected by network outages. An unreliable network does not allow applications like IP Telephony to provide the benefits they were designed to provide. When applications on the network don't perform as expected, service issues can quickly become overwhelming. Converged applications can, and usually do, require predictable response times. Call servers, IP phones, and gateways all possess requirements for network uptime and network quality of service. Properly designed network solutions can minimize the risk of network downtime and alleviate convergence application apprehension.

Integrating network resiliency into core networking devices can provide a manageable solution to a growing problem. By incorporating resiliency into the network core, user access points can remain connected to the network even in the event of a failure. By ensuring the availability of the network, core converged applications can provide the services and benefits they were designed to without impediments.

Technology solutions

Routing protocols inherently provide a basic level of resiliency. The ability to "route" around problem areas defines the efficiency of a routing protocol. However, the time to re-converge the network can vary greatly depending on the protocol being used; for example, routing protocols including RIP and OSPF can take anywhere from seconds to minutes to establish a new route after a failure.

NORTEL NETWORKS
NESS WITHOUT BOUNDARIES

Equal Cost Multi-Path Routing (ECMP) provides multiple routed paths to an end destination; however, designing a network with truly equal cost paths greatly increases the complexity of the network design and often times is not possible.

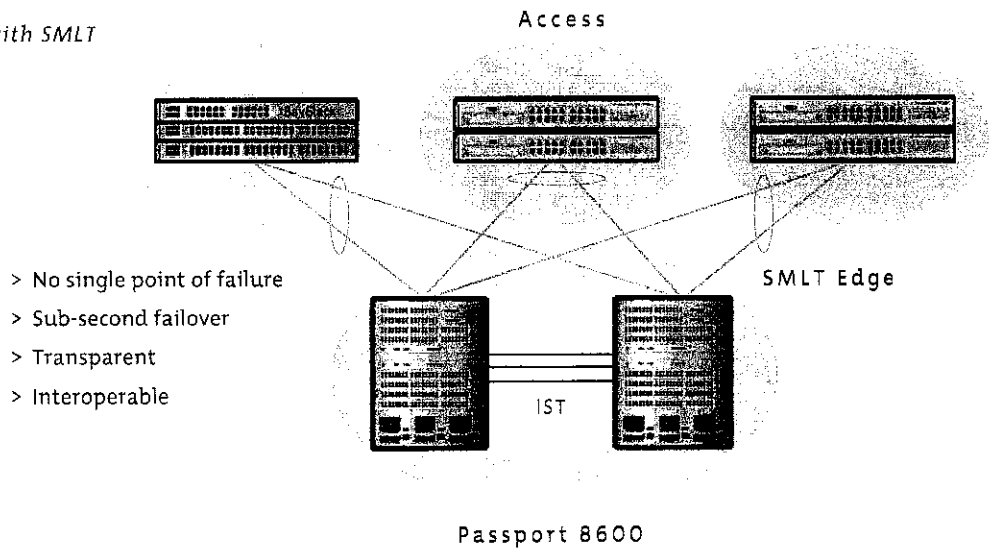
Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the single point of failure that can occur when the single static default gateway router for an end station is lost. VRRP introduces the concept of a virtual IP address, which provides a dynamic default gateway redundancy in the event of failover. However, VRRP can take up to 3 seconds to reconverge after an outage, and up to 90 seconds when used with other routing protocols. Converged applications can begin to fall apart as network delays increase.

Split Multi-Link Trunking (SMLT) is a Nortel Networks architecture that helps eliminate single points of failure and creates multiple paths from user access switches to the core of the network. Compatible with 802.3ad, SMLT does more than prevent network loops. SMLT provides an architecture to design resiliency directly into the network. It also works to reroute failures as quickly as possible. In most cases, network reconvergence is sub-second.

Nortel Networks SMLT is an extension to the IEEE 802.3ad link aggregation specification. SMLT avoids loops due to its superior enhanced link aggregation-control protocol. If 802.1d is used, multiple Spanning Tree groups are required and VLANs must be manually assigned to those groups—all of which makes ongoing administration and troubleshooting extremely complex.

With SMLT it is no longer necessary to use the Spanning Tree protocols to design resilient networks. SMLT provides much faster convergence times than Spanning Tree (typically one second versus 30 to 60 seconds). SMLT also eliminates the blocking of ports by Spanning Tree protocols, thus increasing network bandwidth since all links in a trunk can be utilized for forwarding traffic.

Figure 1. Reliability with SMLT



llows two aggregation switches to appear as a single device to dual homed switches. regation switches make use of an InterSwitch Trunk (IST) over which they : information, permitting rapid fault detection and forwarding path modification. ve network element protection, SMLT extends link aggregation to allow dual of IEEE 802.3ad attached devices. Both of the dual homed connected devices e and pass traffic. This architecture provides twice the available bandwidth of sing the Spanning Tree Protocol.

nproves the reliability of a Layer 2 network operating between the user access in a building and the network center aggregation switch, as well as with the ons to multi-homed servers. It does so by providing load sharing among all links and fast failover in the case of a link or core switch failure.

Split Multi-Link Trunking

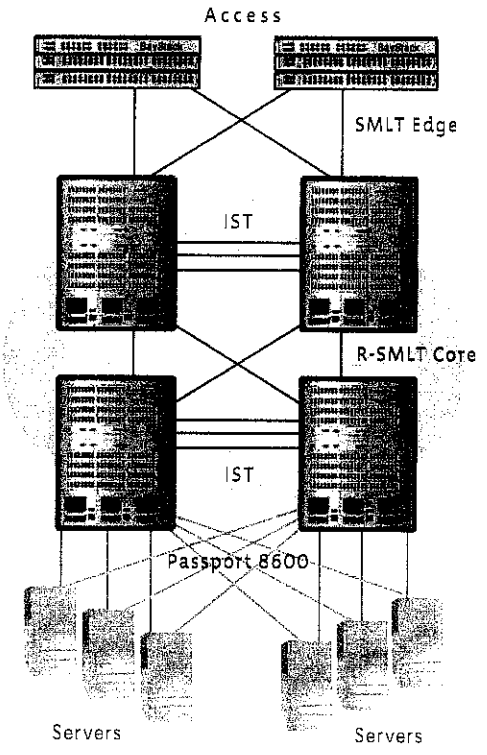
SMLT (R-SMLT) is an extension of the Split Multi-Link Trunking architecture, g sub-second failover for routed core networks using Layer 3 routing protocols IP, OSPF, and BGP. R-SMLT brings resiliency to the network core similar to SMLT brings resiliency to the network edge. Two Passport 8600s operate as one nit within the network core, allowing all connections to the network core to d. In addition, each unit provides backup for the other. R-SMLT and SMLT ond merely eliminating network loops and provide an architecture to design ork resilience.

extends the reliability of SMLT to routed core networks. By providing sub- ilover for Layer 3 information, R-SMLT ensures converged applications are d maintainable throughout the network. This sub-second IP data recovery provides the first resiliency solution for IPX traffic in the SMLT network. with SMLT provides a complete Layer 2 and Layer 3 resiliency solution is the network end-to-end.

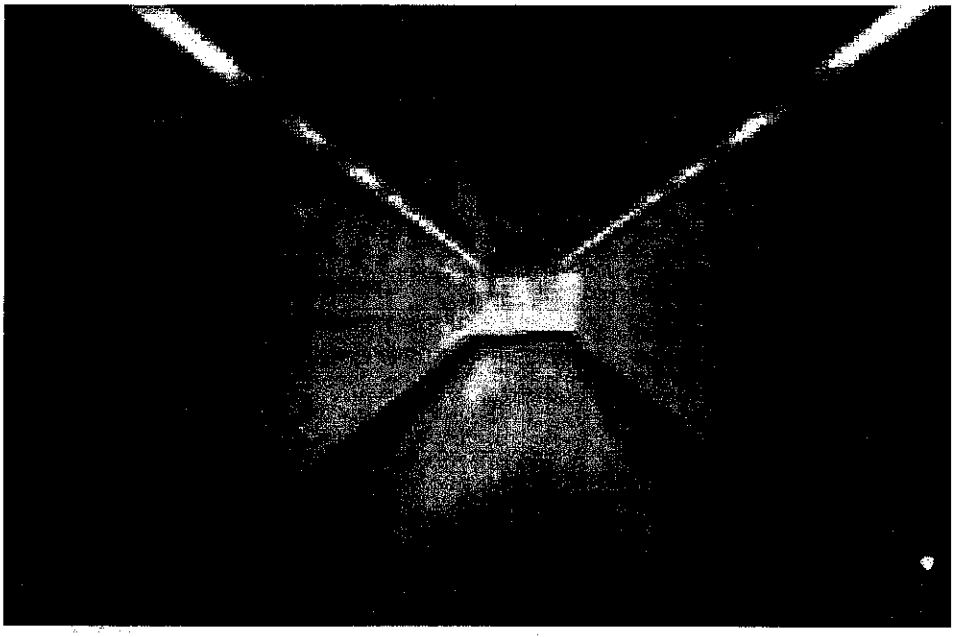
ıg the right technology solution

ndors implement resiliency protocols into their switches. Some use a pure : approach with VRRP and ECMP providing the bulk of the resiliency services. ıately, these protocols rarely meet the resilient bandwidth requirements for d applications like IP Telephony. VRRP can have recovery times measured in as opposed to seconds and can be difficult to implement. Some vendors are ıg their own proprietary solutions that work solely with their own products. lutions can only work in a single vendor environment and become very ted as remote sites and users are added.

Figure 2. Reliability with R-SMLT



- *Sub-second failover*
- *Transparent*
- *Fully automatic*
- *Routed resiliency*



etworks SMLT architecture provides a fully resilient 802.3ad compatible network
. the ability to support multiple vendors in the wiring closets or access points.
oes not require special hardware or complicated configurations. In addition to
; the most advanced resilient solution, SMLT can increase the available band-
m the wiring closet to the network core by merely enabling a software feature.
ons that were once unused due to Spanning Tree's loop protection can now be
neir highest potential.

blossoming of converged applications throughout the network, resiliency has
n more critical. Applications like IP Telephony, multicast, and e-learning
aluable business benefits; however, without adequate bandwidth and network
these applications can't perform their tasks. With SMLT, the ability to provide
on investment from a resiliency feature has never been more pronounced.

*tworks is an industry leader and innovator focused on transforming how the world com-
s and exchanges information. The company is supplying its service provider and enterprise
s with communications technology and infrastructure to enable value-added IP data, voice
imedia services spanning Wireless Networks, Wireline Networks, Enterprise Networks, and
etworks. As a global company, Nortel Networks does business in more than 150 countries.
ormation about Nortel Networks can be found on the Web at:*

.nortelnetworks.com

nformation, contact your Nortel Networks representative, or
4 NORTEL or 1-800-466-7835 from anywhere in North America.

vorks, the Nortel Networks logo, the globemark design are trademarks of Nortel Networks.
demarks are the property of their owners.

2004 Nortel Networks. All rights reserved. Information in this document is subject to change
ice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

30-031804

In the United States:
Nortel Networks
35 Davis Drive
Research Triangle Park, NC
27709
USA

In Canada:
Nortel Networks
8200 Dixie Road, Suite 100
Brampton, Ontario L6T 5P6
Canada

In Caribbean and Latin America:
Nortel Networks
2500 Concorde Terrace
Sunrise, FL 33323
USA

In Europe:
Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead Berkshire SL6
3QH
UK

In Asia:
Nortel Networks
6/F Cityplaza 4
Taikooshing
12 Taikoo Wan Road
Hong Kong

RTEL
NETWORKS
ESS WITHOUT BOUNDARIES