Analyzing the network traffic in a local area network using the Cisco Packet tracer

Aadhaar Koul, Arjun Charak , Anil Kumar , Shobit Kitchloo and Sidharth Bhawani
Department of Computer science and Technology
Model institute of Engineering and Technology ,
Kot Bhalwal , Jammu , Jammu and Kashmir , India
{2020a1r040, 2020a1r057, 2020a1r055}@mietjammu.in

vishalika
Department of Computer Science and Technology
Model Institute of Engineering and Technology
Kot Bhalwal , Jammu , jammu ad kashmir
vishalika.cse@mietjammu.in

***Abstract*— [?][?]In our new era PCs become our part of life for every personal and professional requirement. Majority of organizations depend on the finest possible working of their systems for correspondences, organization, mechanization, online business solutions, and so on. LAN is the best fundamental and significant PC system claimed by discrete organizations and might be utilized for interconnection of wide region systems. A LAN provides effective cost sharing of fast processing information handling gear, for example, mass stockpiling media, centralized server PCs or tiny computers and various types of printers. Asset sharing is generally similar as significant where a Local Area Network (LAN) serves as the entrance path for an Internet. In view of this, framework supervisor's requirement professional tools to help them with the motivation of improvement of QoS and maintenance of LANs. So in our project, a LAN system is structured utilizing Cisco Packet Tracer. This project explains just how the apparatus can be used to build up a reenactment model of the Local Area Network (LAN) for College of Engineering which contains a department like Bio Technology (BT), Civil, Mechanical, ECE and EEE or any. The examination gives a knowledge into different ideas such as IP address setup, topology plan and how to send data as packets in a solitary network and for the usage of Virtual Local Area Networks to isolate the heavy traffic produced by various systems.**

***Index Terms*— N-Body, All-Pairs, Barnes-Hut, Parallelization, OpenMP, CUDA**

I. INTRODUCTION

[4]The requirement for PC systems administration was an effect of the requirement to use PCs for exchanging information in an association in form of messages or packets, exchanging documents and data bases, etc. Regardless of whether the organization is situated in one structure or spread over a huge grounds, the requirement for systems administration the computers cannot be over underscored. As the name assumes, a Local Area Network (LAN) connects PCs in a limited physical territory . It gives high-data transfer capacity correspondence over cheap transmission media .The corporate LAN has developed from an easy basis business segment to a profoundly vibrant, noticeable core asset that activities depend on to help everyday tasks to their market accomplishment. E-Governance is a system of open segment order and is a significant advance in the adjustment of metropolitan organization, with E-Governance joins the utilization of ICT's by government's association. The anticipated calculation utilizes insight of calculation for security of substance in e-governance executing a standard based methodology from computational Knowledge and client's present purpose of area data. On a work area PC, a recreation model had been actualized and assessment utilizing meandering client's continuous position-based data exhibits that proposed system can capably preserve wandering client position secrecy while giving better execution, ensured position privacy, and better nature of administration in e-Governance.

II. FRAMEWORK

A. Background

Cisco Packet Tracer is designed to be used as multitasking, that's been won't to organize and examine varied network exercises like application of dissimilar topologies, development of apt servers, subnetting and study of different network setups, configuration and different troubleshooting defined commands.

To initialize communication among two networking devices i.e., user networking devices and to organize a network, we intend to demand to pick applicable networking devices like switches , routers and interconnecting devices and build physical change of integrity by connecting cables, quick local area network seaports from the module list of packet tracer. Internet working devices square measure costly and thus it's well to perform 1st on the packet tracer to recognize the conception, performance of the designed network.

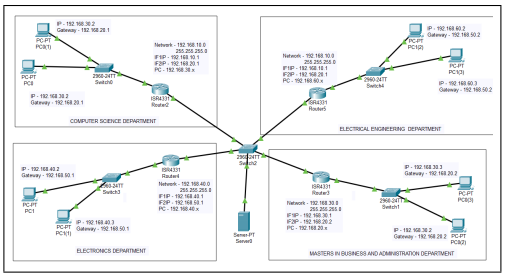

Fig. 1. Setting up the framework for the project

Fig. 2. Setting up the routers using the CLI

B. Framework Continued

Framework The graph of Fig. 1 is the finished graph of the LAN and at the center it connected to switch, switch and the servers framing the Network Operating Center and every one of the different departments in College are only a simple expansion of the system at the center. The allotted IP address picked to the inside system is 192.168.0.0 and it has been sub netted to acquire IP address obstructs that are allocated to various divisions and segments of this prescribed LAN.

III. LAN Simulation Model

[4]We require at least 252 hosts for every subnet the quantity of unmasked bits in the subnet mask is 8. Which infers that the amount of masked bits are 8.

A. Create and assign IP/subnet mask for VLANs:

In this VLAN, we are assigning the below gate ways to all the VLANs with ip address and subnet mask (255.255.255.0). Which is configured in the main switch of VLAN.

- ena .
- config t .
- VLAN 2 .
- VLAN 3 .
- VLAN 4.
- int VLAN 1 .
- ip address 192.168.20.1(Network ID) 255.255.255.0 (Host ID)
- int VLAN 2
- ip address 192.168.50.2(Network ID) 255.255.255.0 (Host ID)
- int VLAN 3
- ip address 192.168.20.2(Network ID) 255.255.255.0 (Host ID)
- int VLAN 4
- ip address 192.168.50.1(Network ID) 255.255.255.0 (Host ID)

B. Configuration mode access/trunk in VLANs:

1) The configuration is done between the main switch and the primary switchs of VLANs by using the cable interface we can trunk all the switchs. :

- int fa0/2.
- Switchport trunk encaptulation dot1q
- switchport mode trunk.

C. In the primary switch, the interface cable are connect to the laptop and access point. Swhich is used to trunk to the PC and access point.

- int fa1/1
- Switchport mode access
- switchport access VLAN 2

IV. Tell PC in VLANs where to get IP:

A. In this VLANs, the switch of different VLAN are getting there IP address from server.

- int VLAN 1 ip helper-address 192.168.10.1
- int VLAN 2 ip helper-address 192.168.50.2

V. Table : IP Address Allocation

Broadcast	First Valid Host	Last Valid Host	Network Address
192.168.1.255	192.168.1	192.168.1.25	192.168.1
192.168.2.255	192.168.2	192.168.1.25	192.168.1
192.168.3.255	192.168.3	192.168.1.25	192.168.1
192.168.4.255	192.168.4	192.168.1.25	192.168.1
192.168.5.255	192.168.5	192.168.1.25	192.168.1
192.168.6.255	192.168.6	192.168.1.25	192.168.1
192.168.7.255	192.168.7	192.168.1.25	192.168.1
192.168.8.255	192.168.8	192.168.1.25	192.168.1

Fig. 3. IP address table for the above mentioned framework

VI. CONFIGURING COMPONENTS

Fig. 4. Setting up a router using CLI

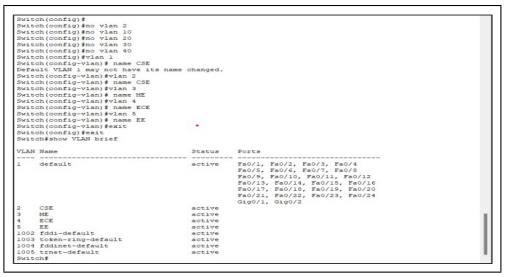

Fig. 5. Configuring / Setting up LANS using the CLi

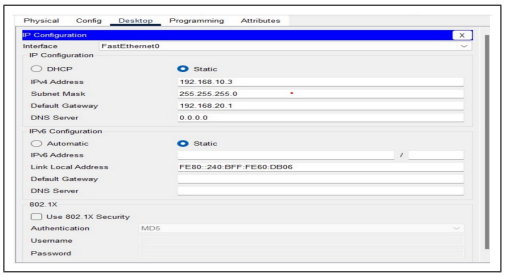

Fig. 6. Setting up the PCs for LAN 1,2,3 and 4

VII.

Fig. 6 displays the simulation results after the configuration of the DHCP server, viewing the address pools of every Virtual LAN created in the given Network. A dynamic IP address configuration was performed on the given network, i.e. when a client device trying to connect to the respective network; it is allotted an IP address that is fee and available in that network given address pool, to the pool that the client model is connected to. Fig. 5 displays client devices are successfully gaining an IP address that are proper to the Virtual LAN, to which the devices are associated to.

VIII. CAPTURING RESULTS

A. To capture the packet routes and latecy we generate a message request or a ping request from the source PC to the destination PC and try to capture as much data as we can , on the basis of which our packet analysis will be drawn out. In our case we will try to capture the route hops , protocols , OSI layer usage , inbound / outbound PDU Details etc. We start with ping out a PC in VLAN 4 from the VLAN 1 by entering the command : "ping 192.168.30.2".

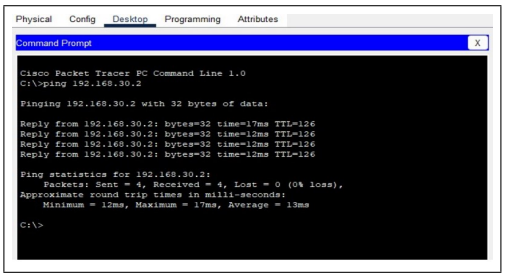

Fig. 7. Trying to ping to the destination target

B. Fig.7: IP addresses data (a-g) From Fig.4, it is clear that every client or device connected to network and is receiving IP address data lethargically, per the subnet the consumer is linked to. VLAN 4 Network Active checking Test (Ping) Network communications and network connectivity will be verified with the help of ping commands, tracked by the domain significant name of the device one wishes to check. Below is the list of routes and protocols that were traced by the packet tracer while the message was being passed across the differnet network devices that comprised the successful propogation of the message .

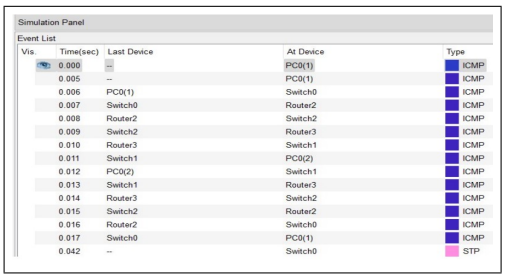

Fig. 8. ROuting table captured while the execution of the ping.

C. The above figure displays the message propogation routes in one cycle i.e. message ping from the source to the destiation and destination to the source . We can see that the message went through the router and the switches of the first LAN and entered the router and switch of the other LAN.This happened many a times to ensure the complete response of the receiver through the network .Other results fo the same are given as below.

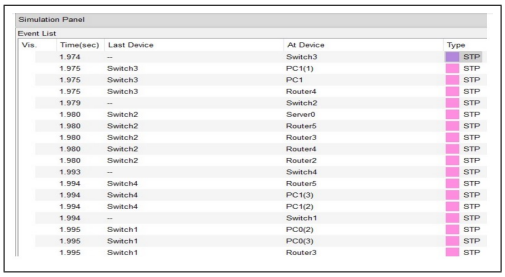

Fig. 9. Another set of routing table formed on the log.

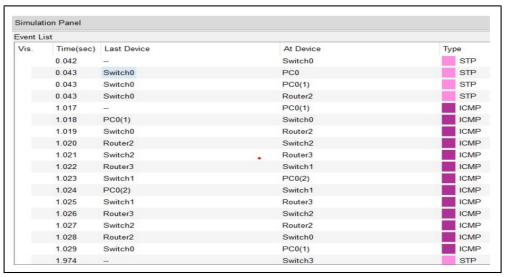

Fig. 10. 3rd set of cycle formed while the message propogation was happeneing.

D. Now we will try to analyze the each route hop by enumerating the captured hops by double clicking on then in the packet tracer . In the below examples we can see that each layer used / Protocol that was used in every step of the message propogation in the OSI Model can be seen below.

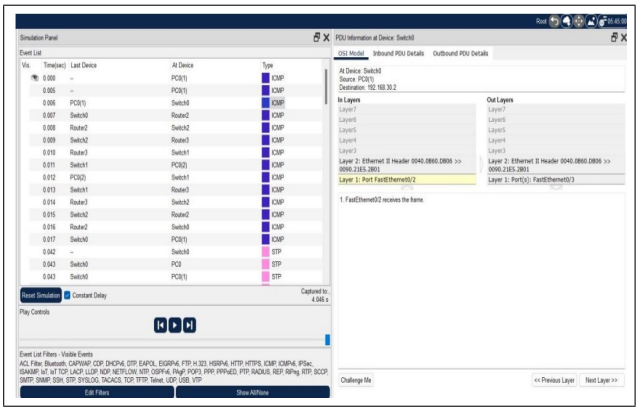

Fig. 11. OSI layer enumeration at the respective step.

We can Even see then Inbound and the Outbound captured results so as to get a proper detailed view of the captured packet.[3]The Outbound PDU Details tab shows similar information for outgoing packets. This tab only applies if the device has a PDU to send. Most of the time, a device will receive a PDU and then, as a result, send out a PDU. In this case, both the Inbound PDU Details and the Outbound PDU Details tabs apply.

E. In the Cisco packet tracer we can find the below information related to our packet / Message :

- Number of IP Bits
- IP ID
- Flags
- Offsets
- Checksum
- Source IP
- Destination IP
- Data Variable Length
- Type of protocol
- Protocol Sequence Number
- PDU Variable size length

Following is the example of the Outbound PDU Details of the message hop / propogation when the packet leaves the source IP to move further.We can see that Our packet comprises of total 32bits for the IP , 32bits for the protocol type , 32bits for the PDU size.The source IP is 192.168.10.3 from the VLAN1 and the Destination IP is : 192.168.30.2 from the VLAN4.

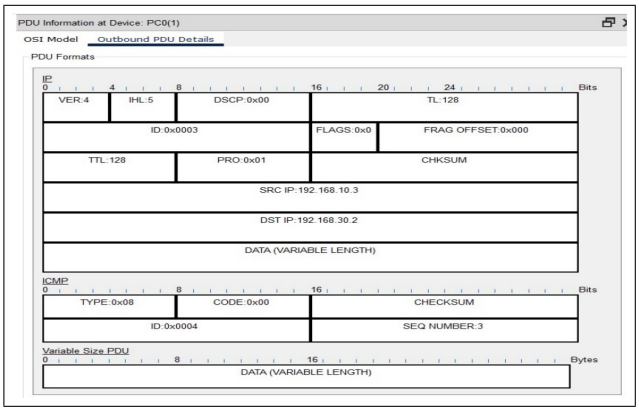

Fig. 12. Outbound PDU result.

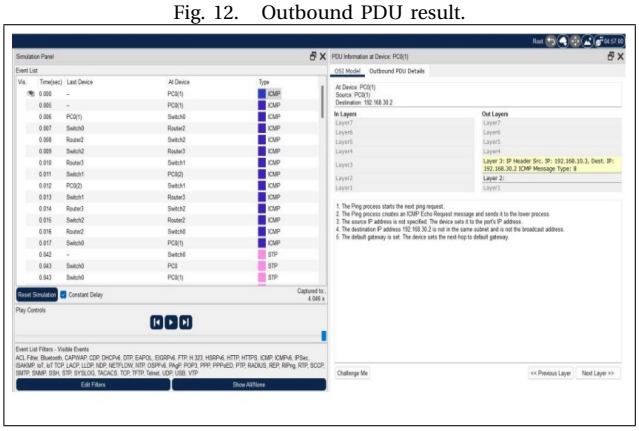

Fig. 13. Inbound PDU Details

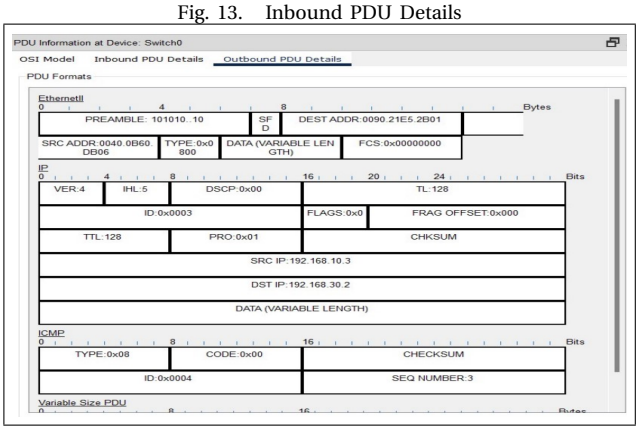

Fig. 14. Outbound PDU result.

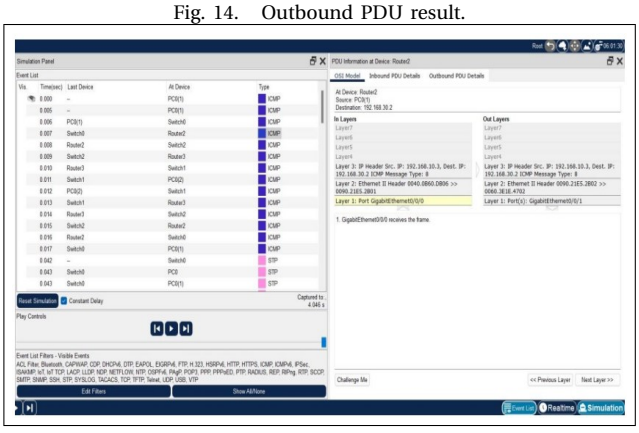

Fig. 15. Inbound PDU Details

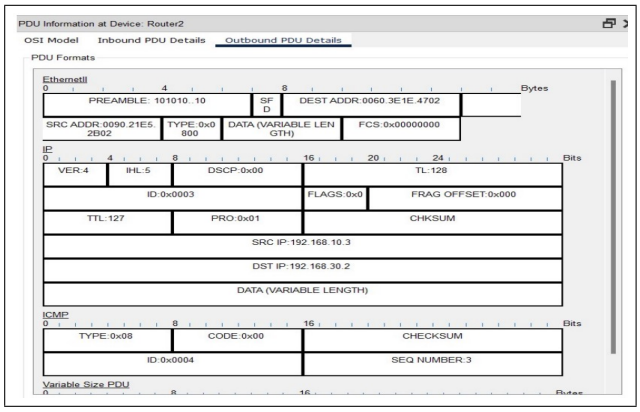

Fig. 16. Outbound PDU result.

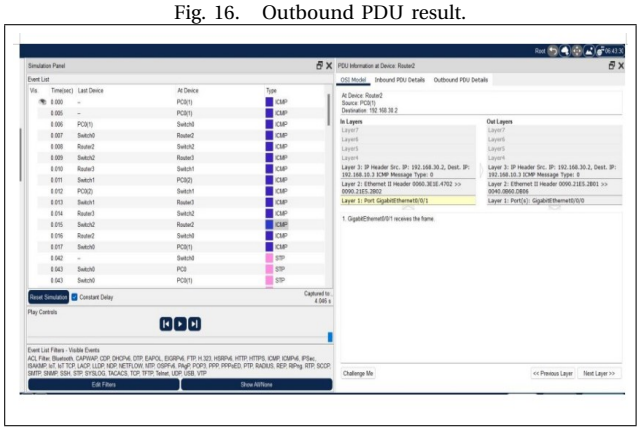

Fig. 17. Inbound PDU Details

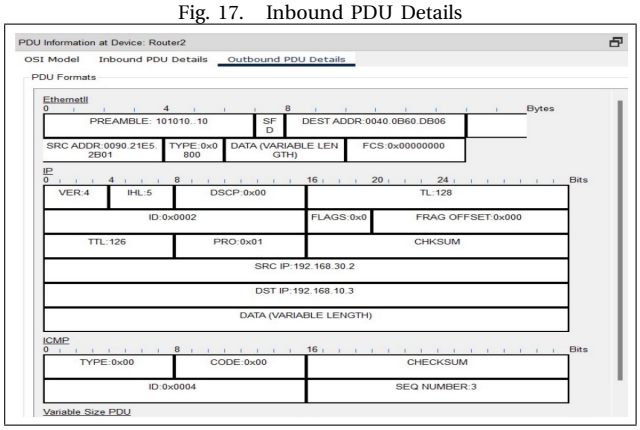

Fig. 18. Outbound PDU result.

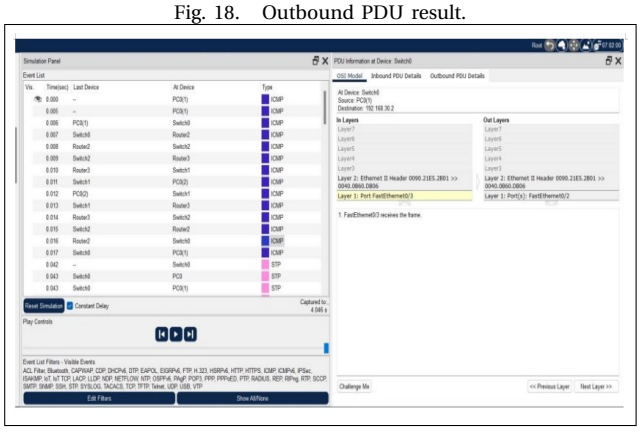

Fig. 19. Inbound PDU Details

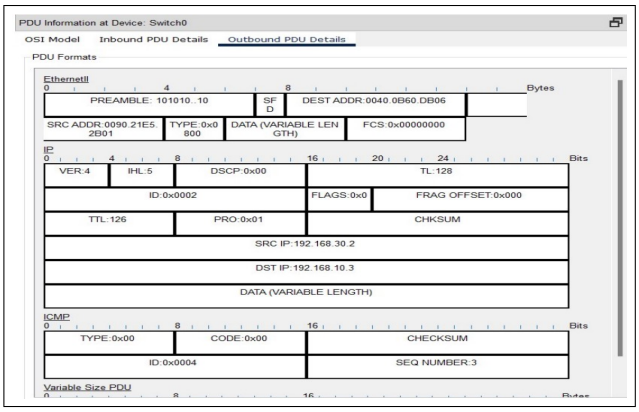

Fig. 20. Outbound PDU result.

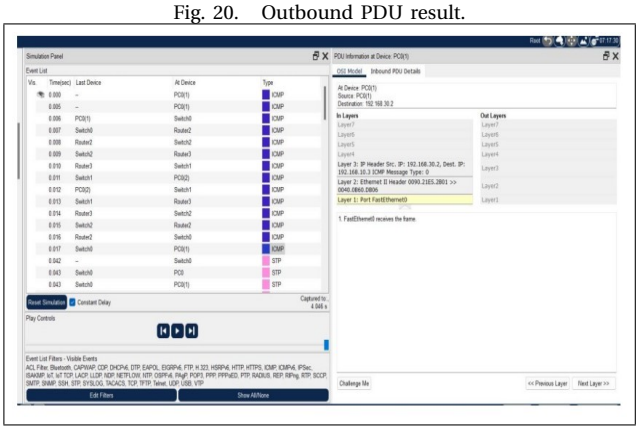

Fig. 21. Inbound PDU Details

IX. Figure 12,13,14,15,16,17,18,19,20,21 Demonstrate the Successful propogation of the message throughout the Network Devices with their status throughout their life cycle.That was captured by the packet tracer. Until now we had all the packets captured and just needed to see whether the message passing was successful or not .For this we used the Bottom right status bar where we can determine whether the message was passed successfully or not . We can determine this by observing the last status of the packet , if we get a failed message it means there is some problem with the device configuration that needs to be looked at , otherwise we'll get a 'SUCCESSFUL'message that means all the processes involved in passing the message were executed successfully and we have performed the experiment successfully.

In the below figure we can see that the last status of the packet is 'SUCCESSFUL'which means we were able to perform the activity with perfection and there was no error in the configurations or in the message itself that could debacle the entire activity.

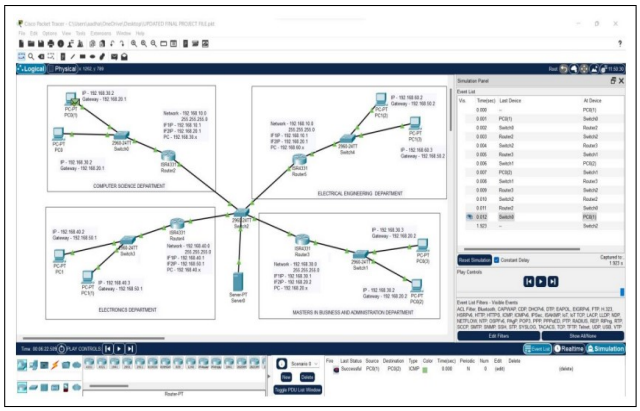

Fig. 22. Final Framework of the Project.

X. CONCLUSIONS

A. In our analysis, a Local Area Network that utilizes wired topology has been executed with some significant ideas like Dynamic Host Configuration Protocol, Domain Name System and Virtual LANs in a solitary system in Cisco Packet Tracer. Virtual Local Area Networks have been utilized to intelligently amass customers on the system, and with the guide of a switch and switch setups, information bundles directed starting with one gadget then onto the next. It is likewise important that, the design and particulars are for the underlying model and can further be created and extra usefulness can be added to expand backing and inclusion.

XI. REFERENCES

,