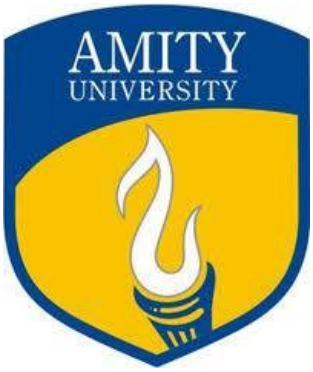
INDUSTRIAL TRAINING REPORT
ON
CONFIGURING D-LINK SWITCH FEATURES
(DHCP, LLDP & SWITCH CONFIGURATION BACKUP)

Submitted to

Amity University Uttar Pradesh



In partial fulfillment of the requirement for the award of the degree

of

Master of Technology

in

Computer Science & Engineering

By

Siddhant Tandon

(A2300913095)

Under the guidance of

Ms. Divya Upadhyay

Department of Computer Science & Engineering

Amity School of Engineering & Technology

Amity University Uttar Pradesh

Noida (U. P.)

ACKNOWLEDGEMENT

I express my sincere gratitude towards my faculty guide **Ms. Divya Upadhyay** and my industrial guide **Mr. Harsh Pandey** for their invaluable assistance, motivation, guidance and encouragement without which working on the industrial training was not possible. They provided me with spark required to set in motion this perticular internship. Inspite of their busy schedule, they were always present to iron out the difficulties, which kept on arising on regular intervals.

I also extend my thanks to entire faculty of the Amity School of Engineering & Technology (ASET) who have encouraged us to complete the internship. Last but not the least I am greatly indebted to all my friends who have encouraged directly or indirectly for successful completion of this Industrial training.

Siddhant Tandon
(A2300913095)

DECLAIRATION

I, Siddhant Tandon, student of M.Tech (CSE) hereby declare that the summer internship report on **"Configuring D-Link Switch Features"** which is submitted by me to Department of Computer Science & Engineering, Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida in partial fulfillment of requirement for the award of degree of Master of Technology in Computer Science & Engineering.

Noida.
Date : July 28, 2014.

Siddhant Tandon

CERTIFICATE

On the basis of term paper submitted by Siddhant Tandon, student of M. Tech. (CSE), I hereby certify that the summer internship report **"Configuring D-Link Switch Features"** which is submitted to Department of Computer Science & Engineering, Amity School of Engineering & Technology, Amity University Uttar Pradesh, Noida in partial fulfillment of requirement for the award of the degree of Master of Technology in Computer Science & Engineering.

Ms. Divya Upadhyay
(Asst. Professor)
Department of Computer Science & Engineering
Amity School of Engineering & Technology, Noida

Noida
Date : July 28, 2014

ABSTRACT

A Network is a collection of interconnected devices which can communicate with each other. These interconnected devices are known as the components of the network. The Components of a network can be :

- Hardware
    - Routers
    - Switches
    - Cables
    - Servers
    - Personal Computers (PCs)
- Software
    - TCP/IP Protocol Suite
    - Ethernet

Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by DHCP clients to obtain IP configuration information. DHCP allows the DHCP server to dynamically assign an IP address to a client from the IP pool of DHCP server.

Link Layer Discovery Protocol (LLDP) allows stations attached to a LAN to advertise itself to other stations attached to the same LAN segment. The information distributed via LLDP is stored by its recipients in a Management Information Base (MIB).

System maintenance and Backup is a very essential part of Network Management. System maintenance activities includes managing of firmwares and configuration files. Configuration files can be downloaded from a TFTP or RCP server so that new configurations can be performed on the switches. Similarly, Configuration files can be backed up on a TFTP or RCP server so that in case of any failure of the switch, normal working conditions can be restored using the configuration backup. Firmwares can also be updated of the switches so as to enhance the workings of the switch.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION.

D-Link managed switches (Layer 2 and Layer 3 switches) have capabilities to create smart networks. A Network can be termed as smart if it is capable of utilising its available resources to its full extent. Network resources can be available IP addresses and/or compute systems with certain capabilities. These switches maintains configuration files for their services and preferences which can be uploaded or downloaded from and to the switch thus providing backup facilities which is a very important operation on these switches.

“Dynamic Host Configuration Protocol or DHCP” is an IEEE standard network protocol used for dynamic assignment of network configuration parameters which inclused IP addresses, Subnet mask, etc. . With DHCP providing the network configuration automatically to the clients that are introduced into the network, involvement of a network administrator is reduced to a minimum. DHCP helps to efficiently utilise the IP address pool available for a local area network thus increasing the life time of IPv4 addressing space by dynamic allocation & reusability of same network address.

The “Link Layer Discovery Protocol or LLDP” is a data link layer protocol that can be utilised by stations over a specified LAN to publicise their identity and services and to recieve the same data from other data link layer peers. LLDP is a formal protcol defined as an IEEE 802.1AB standard. The standard was designed keeping in mind, open and extendable model of the protocol. The draft of this standard was created considering the basic concepts from various protocols like Cisco's CDP or Cisco Discovery Protocol, EDP or Extreme Discovery Protocol and others.

Switch Configuration Backup is a process in which the cofiguration files of the switch are saved on a remote location so as if something went wrong to the switch may it be a system crash or any other reason for failure, the switch can be restored to its previous working condition with its previous set of configurations. Every switch has some kind of software which maintains its workings and is responsible for every operation that has to be carried out by the switch, it is called a firmware. This software can be updated in the switch as the vendor, D-Link, keeps on releasing new firmware, a new copy of firmware can be downloaded from the vendor's website and then, using TFTP or RCP, installed on the switch. This updation procedure doesn't alter the configurations of the switch but it is advised that the administrator should take a backup of the switch's configurations as if

something goes wrong.

1.1 "Dynamic Host Control Protocol (DHCP)"

The "Dynamic Host Configuration Protocol (DHCP)" is used by compute systems over a network to request network configurations like IP address, subnet masks, etc from a DHCP server of the network on which the compute system is a part of. DHCP is a protocol that employs Client-Server model. A newly arriving host is termed as a Client which requires network configurations which includs an IP address & subnet mask for itself. The simplest scenario for a network with DHCP servers is that there is a DHCP server for every subnet existing on the network.

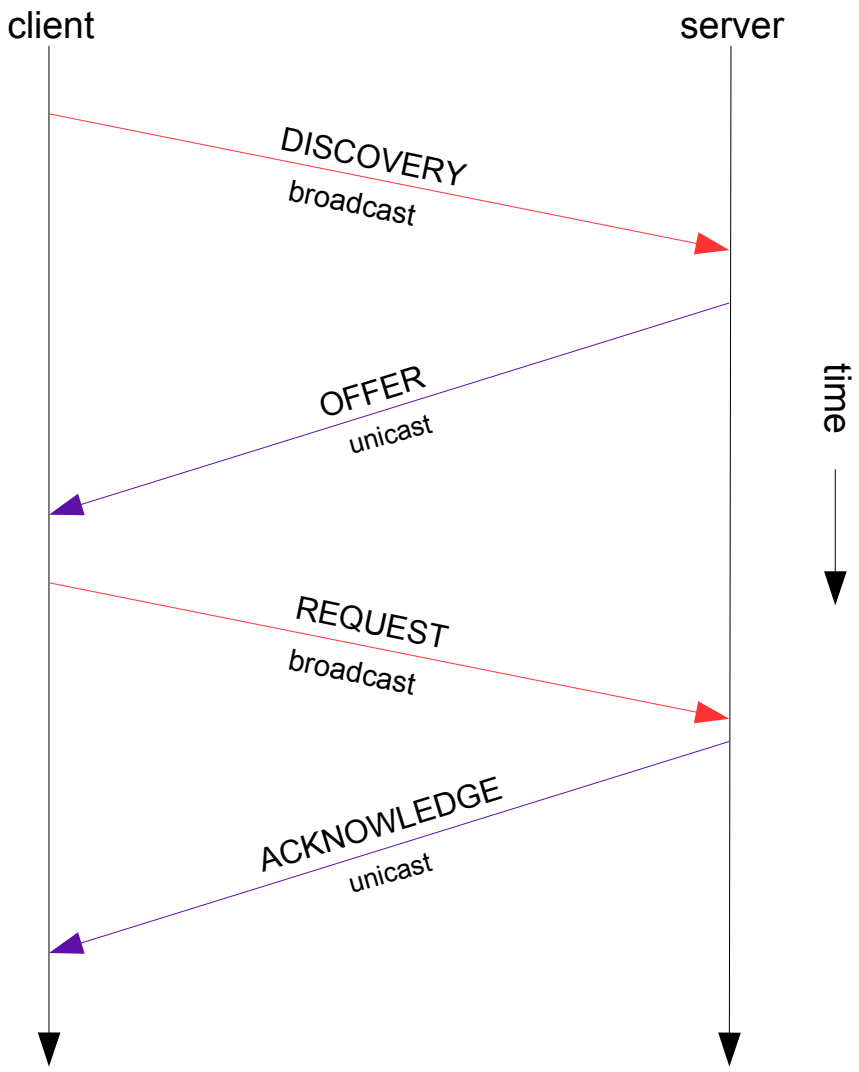


Fig. 1 : A typical DHCP session

DHCP uses a connectionless model utilising User Datagram Protocol (UDP). Two UDP

ports are used for the protocol to operate and since DHCP succeeds BOOTP, they share the same ports. DHCP servers utilises port 67 which is the destination port address for a request, DHCP clients utilises port 68 which is the destination port address of the response from the DHCP server.

Operation of DHCP starts with the broadcast of Request message from client. Clients could request a lease renewal for the existing address directly via UDP unicast as client is alreasy having an IP address associated to itself.

Before we begin the discussion about DHCP phases, First let us take a look at the basic protocol structure of DHCP. DHCP borrows its packet structure from BOOTP, the packet fields are similar but holds different meaning to them when used in DHCP. A DHCP packet has 14 fields in it, They are as follows :

1. *Operation Code* (Field Name : OP; Size : 1Byte) : This field tells the type of message the packet holds. Op = 1 represents Request message from client, whereas Op = 2 is Reply message from server.
2. *Hardware Type* (Field Name : HTYPE; Size : 1Byte) : This field tells what kind of hardware (network media) is used for local network. Op = 1 represents Ethernet, while a value of 6 represents an IEEE 802 network.
3. *Hardware Address Length* (Field Name : HLEN; Size : 1Byte) : Specifies the length of hardware address length. In other words, Its represents the number of octates in hardware address. For Ethernet or IEEE 802 MAC addresses, the value of this field is 6.
4. *Hops* (Field Name : HOPS; Size : 1Byte) : Client sets this field to 0 before transmission of packet so it can be utilised by the Relay agents to monitor & manage the relaying of DHCP packets.
5. *Transaction Identifier* (Field Name : XID; Size : 4Bytes) : This field is generated by the client when it initiates a DHCP request and it remains constant throughout the process. The server once recieving the DHCP server discovery packet from client uses this identifier for its response to the client.
6. *Seconds* (Field Name : Secs; Size : 2Bytes) : It represents the amount of time elapsed since the client started to make attempts for acquiring or renewing a lease. DHCP servers utilizes this field to prioritize client requests.
7. *Flags* (Field Name : Flags; Size : 2Bytes) : This field is a reserved field which, presently, contains just one flag subfield of 1Bit known as Broadcast flag represented

as B. The other 15bits are reserved and are set to zero.

8. *Client IP Address* (Field Name : CIADDR; Size : 4Bytes) : Client populates this field if and only if it has a valid IP address and the state is BOUND, RENEWING or REBINDING. Otherwise, it is set to 0 (0x00000000). The client utilises this field only when its address is actually valid and usable, not during acquisition process and perticulary not for requesting an IP.
9. *"Your" IP Address* (Field Name : YIADDR; Size : 4Bytes) : Assigned IP address that the server has allocated to the client.
10. *Server IP Address* (Field Name : SIADDR; Size : 4Bytes) : Network address of the DHCP server that the clients should be using for the next stage in 4-stage protocol. The server address in this field may or may not be same sending the Offer message.
11. *Gateway IP Address* (Field Name : GIADDR; Size : 4Bytes) : This address is used to route DHCP messages when DHCP relay agents are involued.
12. *Client Hardware Address* (Field Name : CHADDR; Size : 4Bytes) : This field holds the MAC address of the client utilised for recognition and communication.
13. *Magic Cookie* (Field Name : MAGICCOOKIE; Size : 4Bytes) : It is the token for the data passed between communicating programs, where the data is not meaningful to the recipient program.
14. *Options* (Field Name : OPTIONS; Size : Max. 4Bytes) : This field is populated with multiple parameters necessary for DHCP basic operations.

For a successful allocation of the network configurations, DHCP operations have 4 stages:

1. DHCP Server Discovery (Client broadcasts).
2. DHCP IP lease offer (Server responses).
3. DHCP IP request (Client broadcasts).
4. DHCP IP lease acknowledgement (Server responses).

1.1.1 DHCP Server Discovery

The Client broadcasts a request using the specific subnet broadcast address (generally 255.255.255.255). Clients keeps track of its assigned IP address and can request it from the DHCP server, It can grant or deny this request depending upon the availability of address and authority of server to grant the requested address. However if the server sends a rejection, Client could request a new IP address.

0	4	8	12	16	20	24	28	32
Source IP Address = 0. 0. 0. 0								
Destination IP Address = 255. 255. 255. 255								

Fig. 2(a) : Layer 2 header (IP header) – DHCP Server Discovery message.

Source Port = 68	Destination Port = 67

Fig. 2(b) : Layer 3 header (UDP header) – DHCP Server Discovery message.

0	8	16	24	32
Operation Code (OP) = 0x01	H/W Type (HTYPE) = 0x01 (Ethernet)	H/W Address Length (HLEN) = 0x06	Hops = 0x00	
Transaction ID (XID) = 0x11209b216				
Seconds (SECS) = 0x0000		Flags = 0x0000		
Client IP Address (CIADDR) = 0. 0. 0. 0				
Your IP Address (YIADDR) = 0. 0. 0. 0				
Server IP Address (SIADDR) = 0. 0. 0. 0				
Gateway IP Address (GIADDR) = 0. 0. 0. 0				
Client Hardware Address (CHADDR) = 00 : 25 : 64 : 5c : 24 : 6c				
Magic Cookie = 0x63825363 (DHCP)				
Options (DHCP message type = DHCP Discover; Host Name = “Lab-PC”)				

Fig. 2(c) : DHCP payload – DHCP Server Discovery message.

1.1.2 DHCP IP lease Offer

DHCP Offer message is the response message when the DHCP server recieves a DHCP server discovery message from a Client. Server Discovery message is interpreted by the server as lease request for IP configurations. The server now make an IP address reservation for that client and unicaste a lease offer message. Client's hardware address (CHADDR) in the DHCP server discovery message helps the server to determine what configuration to send in the DHCP offer message. The YIADDR field or your IP address field of offer

message is set to the reserved IP address of the client by the DHCP server.

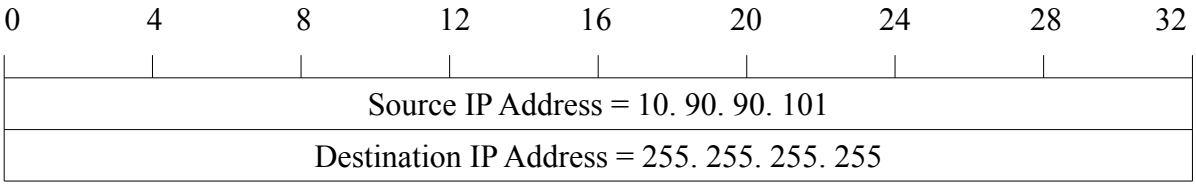


Fig. 3(a) : Layer 2 header (IP header) – DHCP Offer message.

Source Port = 67	Destination Port = 68

Fig. 3(b) : Layer 3 header (UDP header) – DHCP Offer message.

Operation Code (OP) = 0x02	H/W Type (HTYPE) = 0x01 (Ethernet)	H/W Address Length (HLEN) = 0x06	Hops = 0x00
Transaction ID (XID) = 0x11209b216			
Seconds (SECS) = 0x0000		Flags = 0x0000	
Client IP Address (CIADDR) = 0. 0. 0. 0			
Your IP Address (YIADDR) = 10. 90. 90. 10			
Server IP Address (SIADDR) = 10. 90. 90. 101			
Gateway IP Address (GIADDR) = 0. 0. 0. 0			
Client Hardware Address (CHADDR) = 00 : 25 : 64 : 5c : 24 : 6c			
Magic Cookie = 0x63825363 (DHCP)			
Options (DHCP message type = DHCP Offer; DHCP server identifier = 10. 90. 90. 101; IP address lease time = 1 day; Subnet mask = 255. 255. 255. 0; Router = 10. 90. 90. 101)			

Fig. 3(c) : DHCP payload – DHCP Offer message.

1.1.3 DHCP Request

Once a DHCP server makes an offer to the Client, Client creates a DHCP request requesting the offered IP address and broadcast it to the server. As the DHCP server discovery is

broadcasted over the channel, multiple responses to the discovery message could arrive at the client but it would only accept one of them. The Server Identification option in the offer message recieved and accepted by the client is used to create a request message for that server, any other servers are informed about which offer has been accepted.

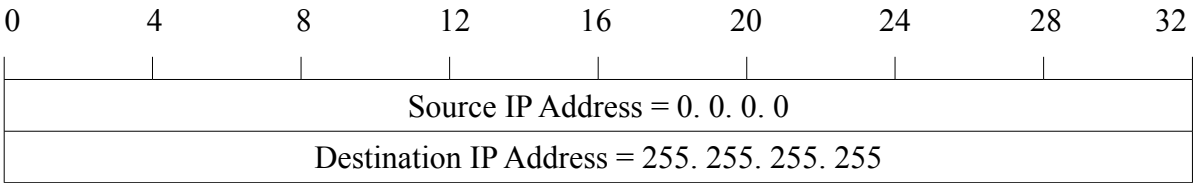


Fig. 4(a) : Layer 2 header (IP header) – DHCP Request message.

Source Port = 68	Destination Port = 67

Fig. 4(b) : Layer 3 header (UDP header) – DHCP Request message.

Operation Code (OP) = 0x01)	H/W Type (HTYPE) = 0x01 (Ethernet)	H/W Address Length (HLEN) = 0x06	Hops = 0x00
Transaction ID (XID) = 0x11209b216			
Seconds (SECS) = 0x0000		Flags = 0x0000	
Client IP Address (CIADDR) = 0. 0. 0. 0			
Your IP Address (YIADDR) = 0. 0. 0. 0			
Server IP Address (SIADDR) = 0. 0. 0. 0			
Gateway IP Address (GIADDR) = 0. 0. 0. 0			
Client Hardware Address (CHADDR) = 00 : 25 : 64 : 5c : 24 : 6c			
Magic Cookie = 0x63825363 (DHCP)			
Options (DHCP message type = DHCP Request; DHCP server identifier = 10. 90. 90. 101; Requested IP address = 10. 90. 90. 10; Host Name = “Lab-PC”)			

Fig. 4(c) : DHCP payload – DHCP Request message.

1.1.4 DHCP Acknowledgement

As soon as the DHCP request message from the client is recieved by the server, the configuration process is now finalising. The server response to this message with an acknowledgement message to the client, holding the IP lease time and other network configurations which might be needed by the Client for its operations. Now, wih the final acknowledgement message, the configuration process is at its finale.

DHCP protocol ensures that the client configure itself according to the negotiated network interface parameters. After the configuration, Client might use ARP or Address Resolution Protocol for preventing any address conflicts that might arise due to overlapping of DHCP address pools.

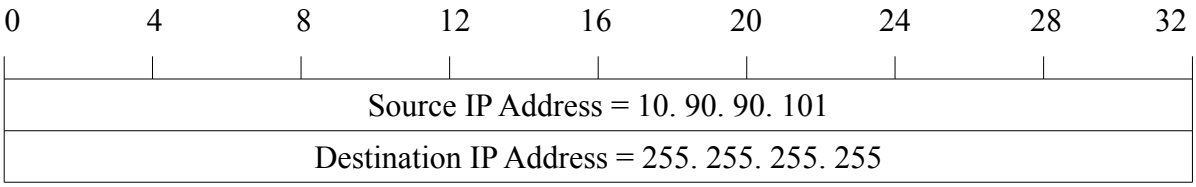
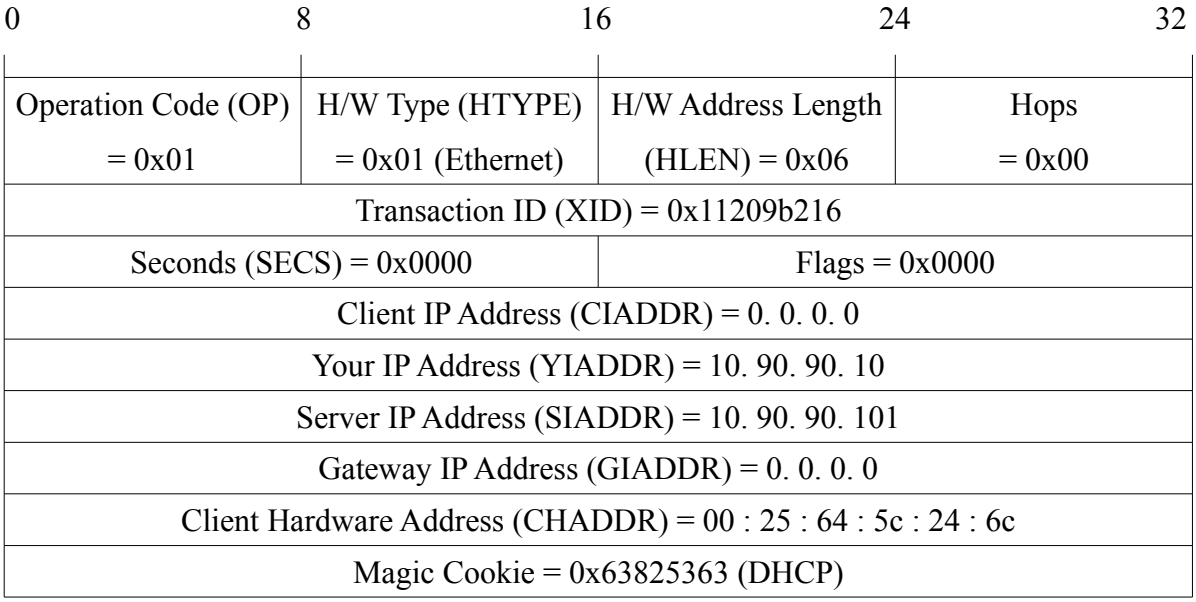


Fig. 5(a) : Layer 2 header (IP header) – DHCP Acknowledgement message.

Source Port = 67	Destination Port = 68

Fig. 5(b) : Layer 3 header (UDP header) – DHCP Acknowledgement message.



Options (DHCP message type = DHCP Ack; DHCP server identifier = 10. 90. 90. 101; IP address lease time = 1 day; Subnet mask = 255. 255. 255. 0; Router = 10. 90. 90. 101)

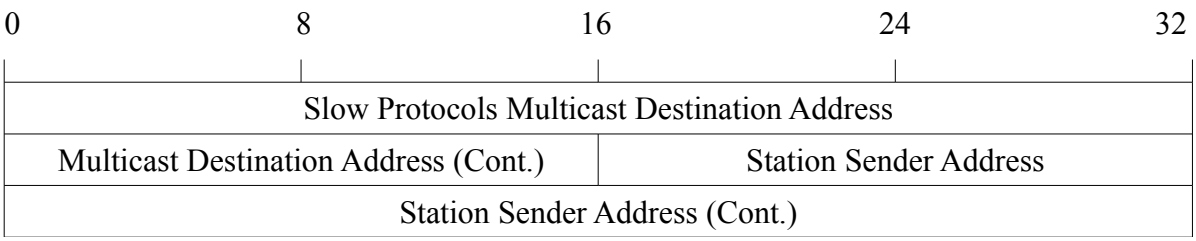
Fig. 5(c) : DHCP Payload – DHCP Acknowledgement message.

1.2 <u>"Link Layer Discovery protocol (LLDP)"</u>

The "Link Layer Discovery Protocol (LLDP)" is a protocol that provides media independance over every IEEE 802 complient devices which helped LLDP agents to discover higher level layer information from neighbouring devices.

LLDP supports all IEEE 802 compliant media. Moreover, Protocol works on the Data-Link layer only which made it possible for different compute systems working over seperate Layer 3 or Network layer protocols to discover each other. Each compute system which has a LLDP agent transmits a periodic transmission over all physical network interfaces configured for LLDP transmission. These agents have listeners as well on the same physical interfaces which listens for the LLDP messages. Each multicast transmission holds information of the source port which can be used as connection endpoint identifier.

The LLDP frame contrains minimum of one network address. This address could be utilised by a Network Management System (NMS) to get to a MA or Management Agent on the compute system using the specified source port. Each LLDP frame has an adjustable TTL or Time-To-Live value, which indicates to the recieving agent when to reject the known topology information. An LLDP Packet Data Unit (PDU) is encapsulated within an IEEE 802 frame, The format is shown in following :



Slow Protocols Type	Subtype	Reserved
LLDP PDU Message		

Fig. 6 : LLDP Frame encapsulation.

This frame consists of four basic type of fields, they are :

1. *Slow Protocols Multicast Destination Address* : This address is within the range reserved for protocols which have link-constrains and will not be subjected to forwarding by conformant MAC bridges.
2. *Station Sender Address* : Transmitting station's source MAC address.
3. *Slow Protocols Type* : Field encoding of the Length/Type field.
4. *Subtype* : TBD is set as the Slow Protocols Subtype.

Now, Let's discuss about the actual LLDP PDU. It is made up of a header which can be accompanied by a one or multiple Type-Length-Value attributes (TLVs). Single IEEE 802 media frame contains only one LLDP PDU for every transmission. The LLDP header is 4 Bytes or 32 Bits long, containing 3 fields as following :

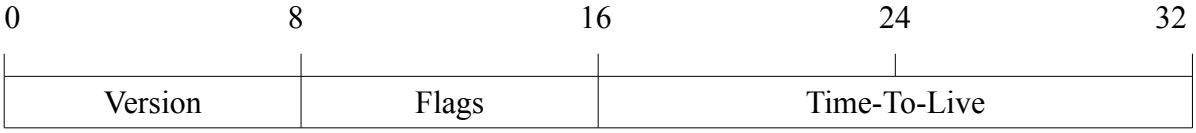


Fig. 7 : LLDP Header format.

The LLDP header consists of the following fields :

1. *Version* : Set to 0x01 for this version of the protocols.
2. *Flags* : This field is reserved for future developments in the protocol, it also helps the header word-aligned for easier processing.
3. *Time-To-Live* : The time for which the information in the message is treated as valid by the recipient.

LLDP header is followed by variable number of TLVs. The type of TLV depends upon the implementation and max. message size.

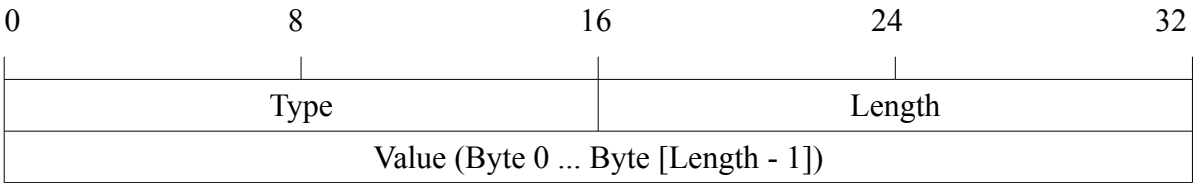


Fig. 8 : LLDP TLV format.

The TLV stands for :

1. *Type* : Information type contained in the value field.
2. *Length* : Length of the Value field in octets.
3. *Value* : Field containing instance specific information encoded in octet-string.

1.2.1 Protocol Operation

A correctly configured LLDP Agent must :

- Transmission of LLDP messages.
- Processing of LLDP messages recieved.
- Save a copy of the LLDP MIB.
- Save a copy of the PTOPO MIB.
- Maintain correct instances.
- Implement MIB objects.

1.3 Switch Configuration Backup

Any Switch requires a governing piece of software called a Firmware and a file (or set of files) holding all the configuration details about the switch called a Configuration file(s) for proper operation of the Switch.

In industrial working environment, Downtime of the devices should be to its minimum. Downtime is refered to the time period for which the concerned device is not working, since devices are not perfect they seem to develop some faults overtime. Businesses can't afford long downtimes within there networks as most of the businesses are online and all their trade is conducted over internet.

To reduce device downtime, Its essential to have proper backup of the firmware and configuration files which can be accomplished by using TFTP servers. TFTP uses client-server architecture and the client can be any machine running the TFTP client application. Because of the simplicity of the TFTP is prefered way to manage the firmware and configuration files. Most modern switches are now managed via Web interface or HTTP protocol for transferring firmware/ configuration files to/from the switch. TFTP server could be running locally within the network or on a remote location over the internet though it is quite unusual to have a local switch configuration over on a remote locaiton.

TFTP stands for Trivial File Transfer Protocol, it is a FTP notable for its simple design, normally used for automatic transfer of configuration between compute systems. It is prefered locally as it provides with no authentication and use a very small amount of memory and processing.

CHAPTER 2. MATERIALS & METHODS.

Every switch have certain capabilities or services within them, all it is needed to enable the services and configure them properly. We are working on Layer 2+ and Later 3 switches, namely, DGS-3420-28TC (Layer 2+ switches) and DGS-3620-26TC (Layer 3 switches). For all the experiments and practicals, we are going to adopt the following topology of switches.

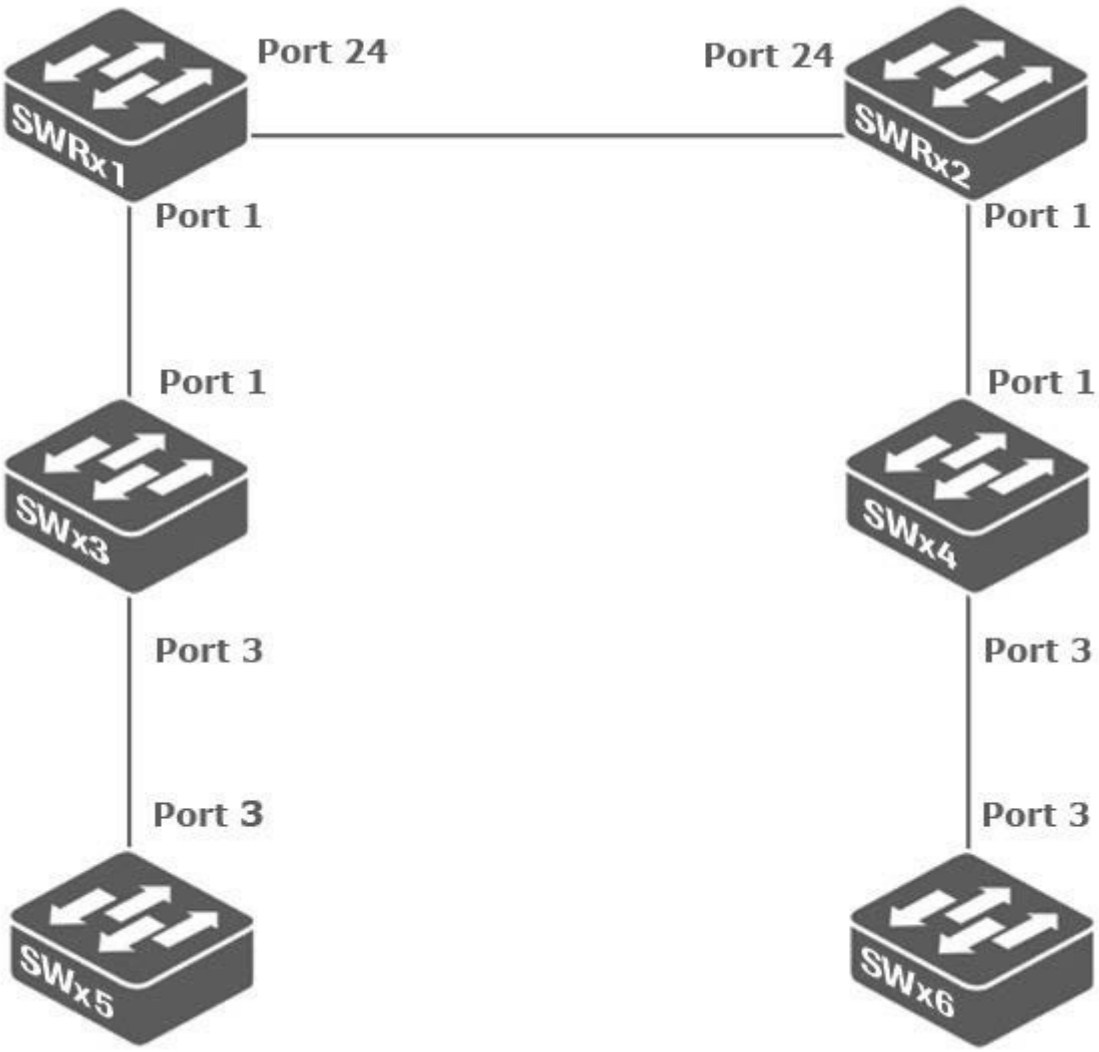


Fig. 9 : Topology to be used for the experiments.

SWRx1 & SWRx2 are Layer 3 switches connected to each other via Port 24. SWx3 & SWx4 are Layer 2+ switches connected to SWRx1 & SWRx2 respectively via Port 1. Finally, SWx5 & SWx5 are also Layer 2+ switches connected to SWx3 & SWx4 via Port 3.

Switch Name	Switch's IP Address	Enabled Ports	Connected PC (if any)	PC's IP Address
SWRx1	10. 90. 90. x1/24	1, 24	PCx1	10. 90. 90. x01/24
SWRx2	10. 90. 90. x2/24	1, 24	PCx2	10. 90. 90. x02/24
SWx3	10. 90. 90. x3/24	1, 3	PCx3	10. 90. 90. x03/24
SWx4	10. 90. 90. x4/24	1, 3	PCx4	10. 90. 90. x04/24
SWx5	10. 90. 90. x5/24	1	PCx5	10. 90. 90. x05/24
SWx6	10. 90. 90. x6/24	1	PCx6	10. 90. 90. x06/24

Table 1: Topology Details for Experiments conducted during Internship.

x in the table represents POD number or Point-Of-Delivery number in the network. It is a kind of repeatable pattern, its components helps the network managers to maximize the manageability, scalability and modularity of the networking systems. The components work in-sync to deliver networking services. To perform the experiments, All the switches are rebooted and reset to their original factory settings.

2.1 Enable / Disable Ports

When the Switches are set back to their original factory settings, by default, all the ports are enabled on the switches which might lead to looping of switches if they are connected.

To prevent looping as in case the STP is not enabled, We have to disable all other ports so that no loops are formed during the experiments.

1. To disable all the ports on the Switch, Enter ***config ports all state disable***.
2. To verify that all the ports are disabled, Enter ***show ports***.
3. Since all the ports are disabled, We have to enable the ports we will be using to create the topology. For enabling ports of the switch, enter ***config ports <portlist> state enable***, where <portlist> represents the port number.
    - For SWRx1 & SWRx2, We enable Ports 1 and 24. Enter ***config ports 1,24 state enable***.
    - For SWx3 & SWx4, We enable Ports 1 and 3. Enter ***config ports 1,3 state enable***.
    - For SWx5 & SWx6, We enable Port 1 only. Enter ***config ports 1 state enable***.

2.2 Dynamic Host Configuration Protocols (DHCP)

In this experiment, Only SWRx1 and SWRx2 will be used as DHCP servers; SWx3, SWx4, SWx5 and SWx6 will be used as DHCP clients. SWRx1, SWx3 and SWx5 will be in VLAN 10 and using addresses fromt he network of 10. 90. x1. 0/24. SWRx2, SWx4 and SWx6 will be in VLAN 20 and using addresses from the network of 10. 90. x2. 0/24.

VLAN	V10	V20
DHCP Server	SWRx1	SWRx2
DHCP Client	SWx3, SWx5	SWx4, SWx6
DHCP Pool	v10-pool	v20-pool
DHCP Network Address	10. 90. x1. 0/24	10. 90. x2. 0/24
DHCP Excluded Addresses	10. 90. x1. 1/24 to 10. 90. x1. 20/24	10. 90. x2. 1/24 to 10. 90. x2. 20/24

Table 2: DHCP configurations.

2.2.1 Configurations for SWRx1

For SWRx1 as a DHCP server, The configuration commands are as follows :

1. ***create vlan v10 tag 10***
2. ***config vlan v10 add tag 1,24***
3. ***create ipif v10-if 10.90.x1.11/24 v10***
4. ***create dhcp pool v10-pool***
5. ***config dhcp pool default_router v10-pool 10.90.x1.11***
6. ***config dhcp pool dns_server v10-pool 10.90.x1.11***
7. ***config dhcp pool network_addr v10-pool 10.90.x1.0/24***
8. ***create dhcp excluded_address begin_address 10.90.x1.1 end_address 10.90.x1.20***
9. ***enable dhcp_server***

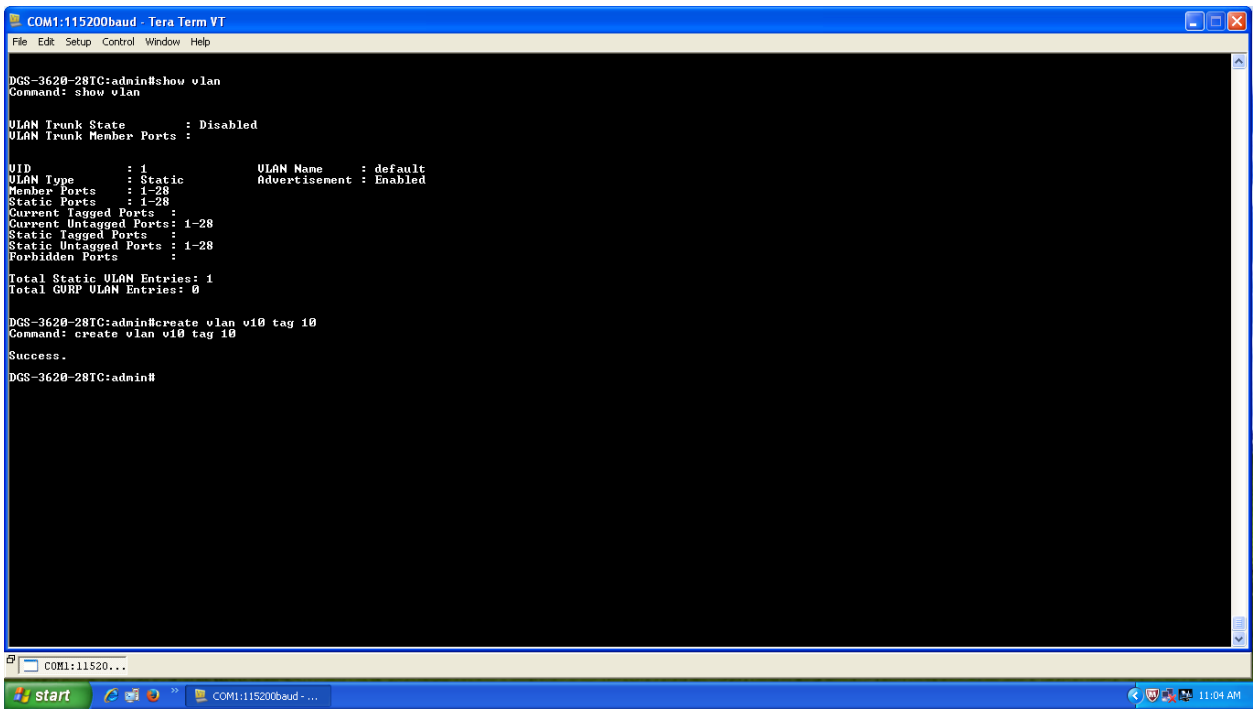


Fig. 10 : Creating vlan v10 on SWRx1.

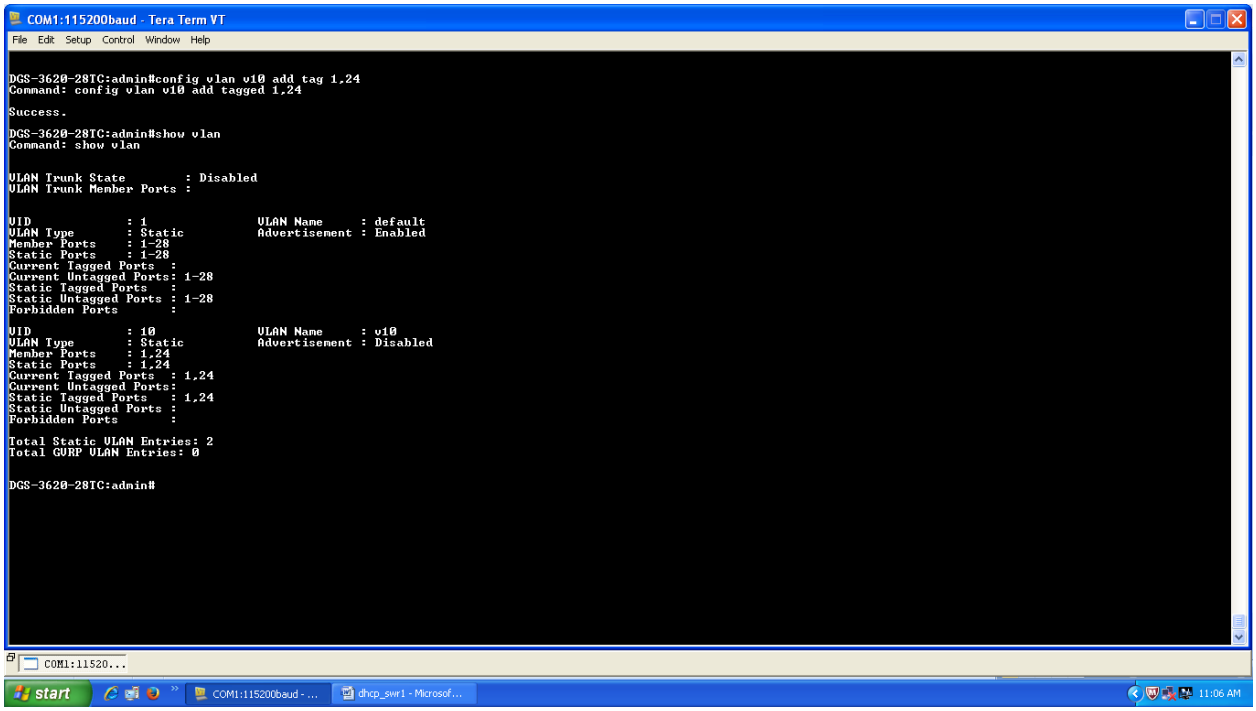


Fig. 11 : Configuring vlan v10 on SWRx1.

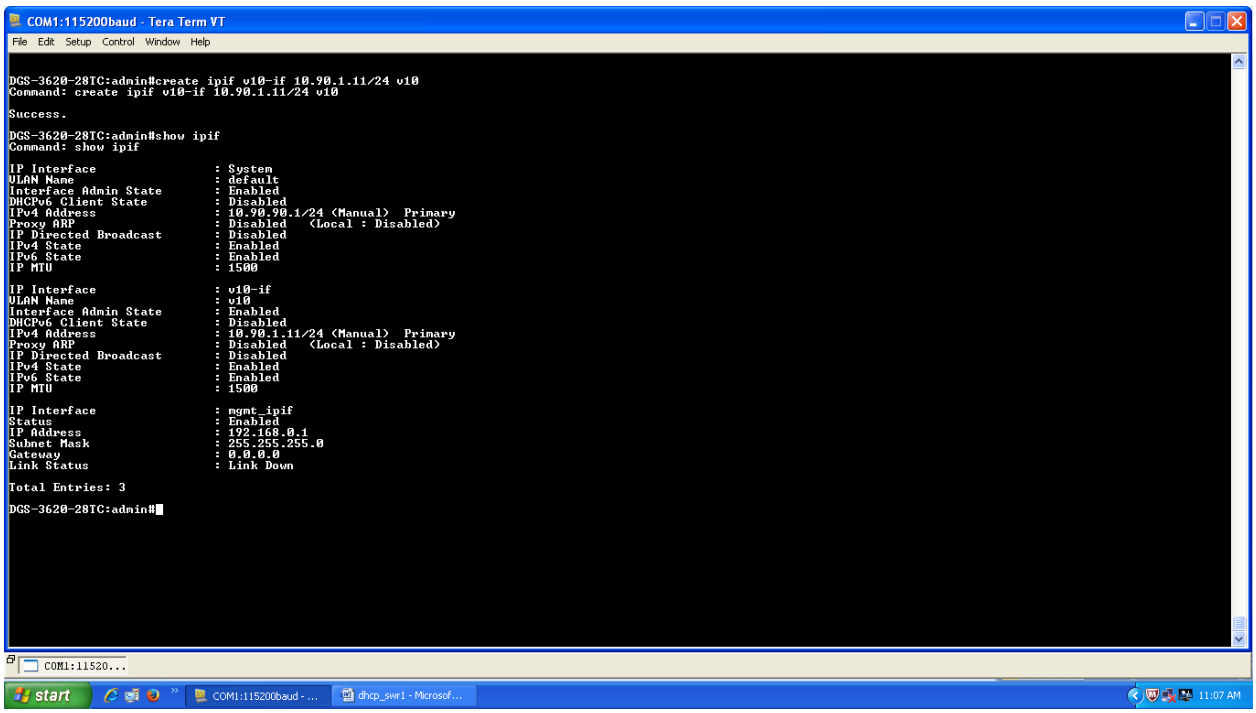


Fig. 12 : Create interface v10-if for vlan v10 on SWRx1.

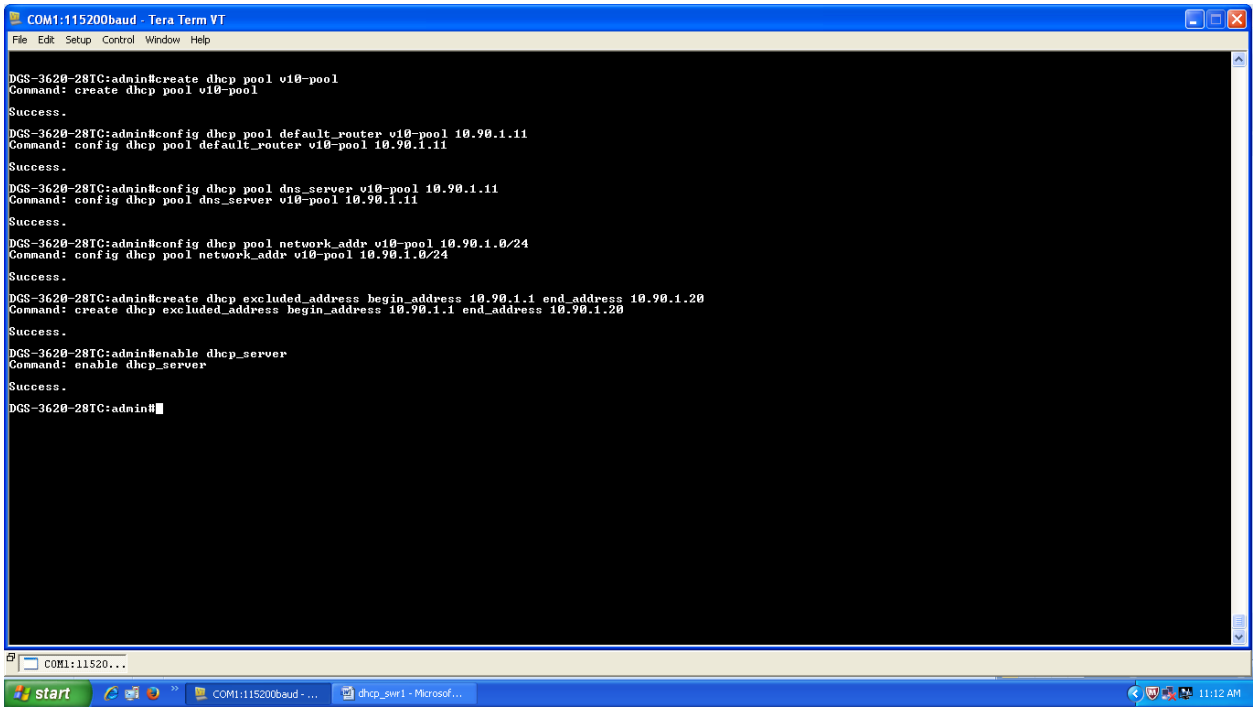


Fig. 13 : Create DHCP pool v10-pool and enable DHCP server on SWRx1.

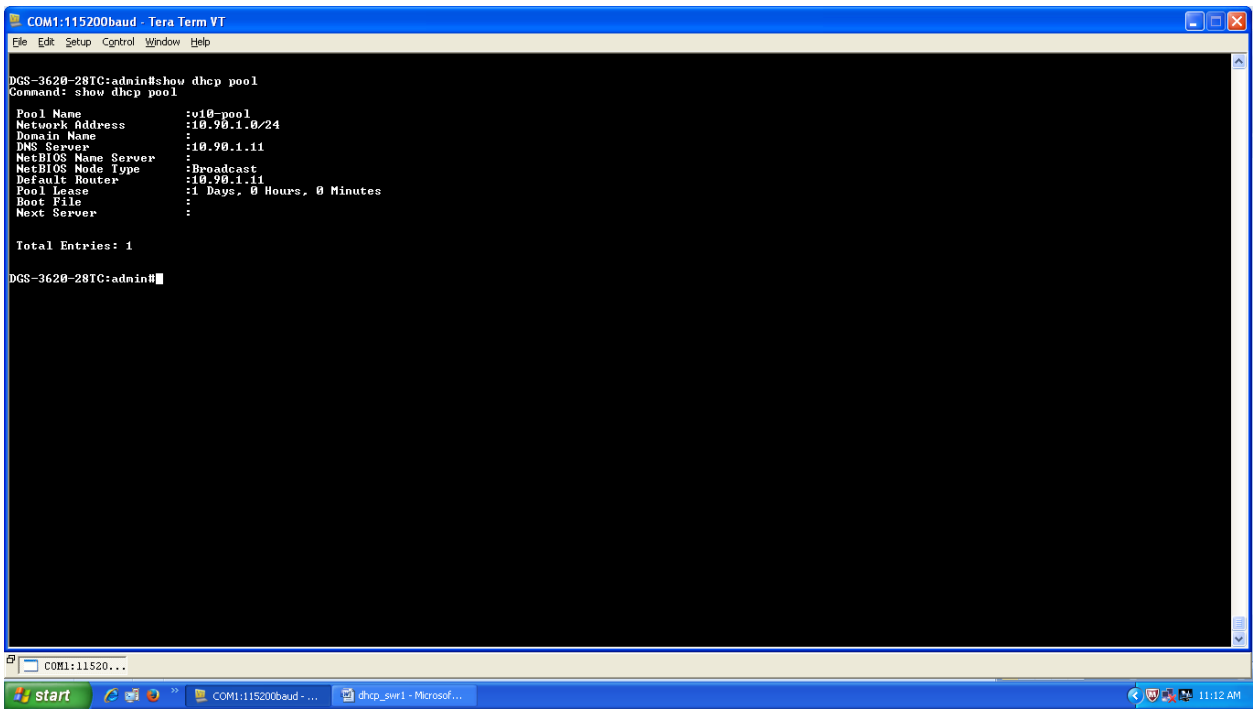


Fig. 14 : DHCP pool, v10-pool, on SWRx1.

2.2.2 Configurations for SWRx2

For SWRx2 as a DHCP server, The configuration commands are as follows :

1. ***create vlan v20 tag 20***
2. ***config vlan v20 add tag 1,24***
3. ***create ipif v20-if 10.90.x2.11/24 v20***
4. ***create dhcp pool v20-pool***
5. ***config dhcp pool default_router v20-pool 10.90.x2.11***
6. ***config dhcp pool dns_server v20-pool 10.90.x2.11***
7. ***config dhcp pool network_addr v20-pool 10.90.x2.0/24***
8. ***create dhcp excluded_address begin_address 10.90.x2.1 end_address 10.90.x2.20***
9. ***enable dhcp_server***

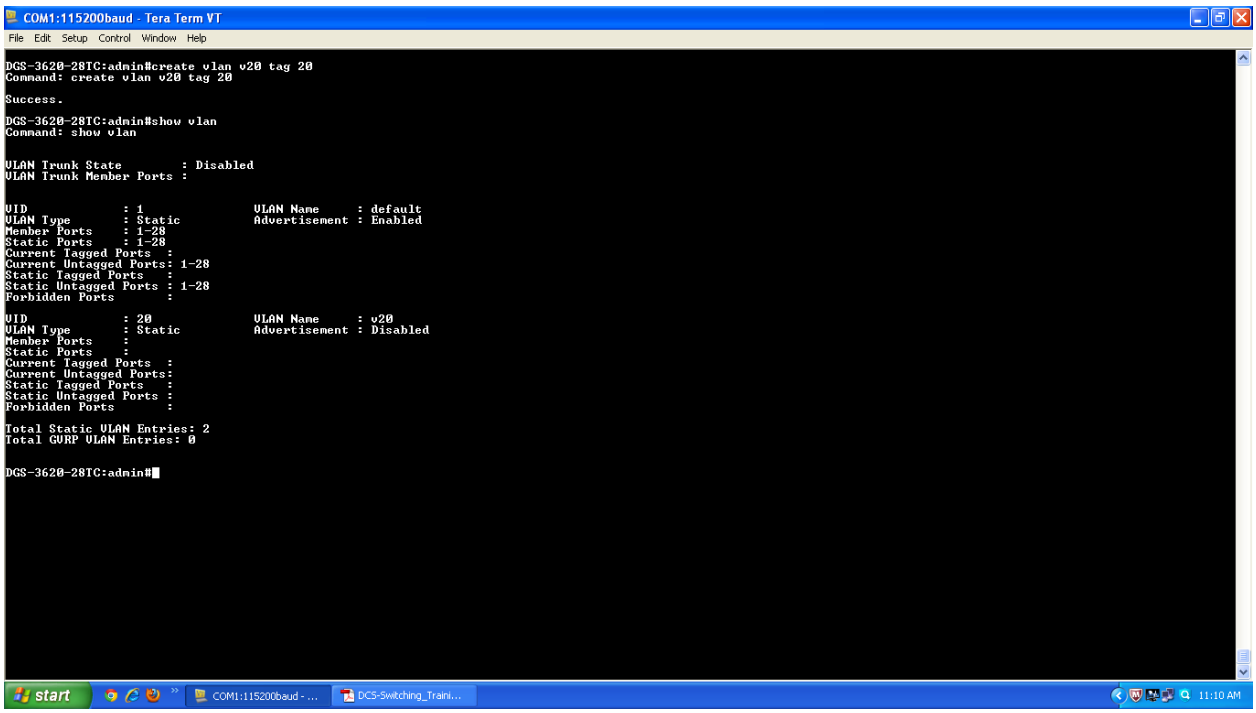


Fig. 15 : Creating vlan v20 on SWRx2.

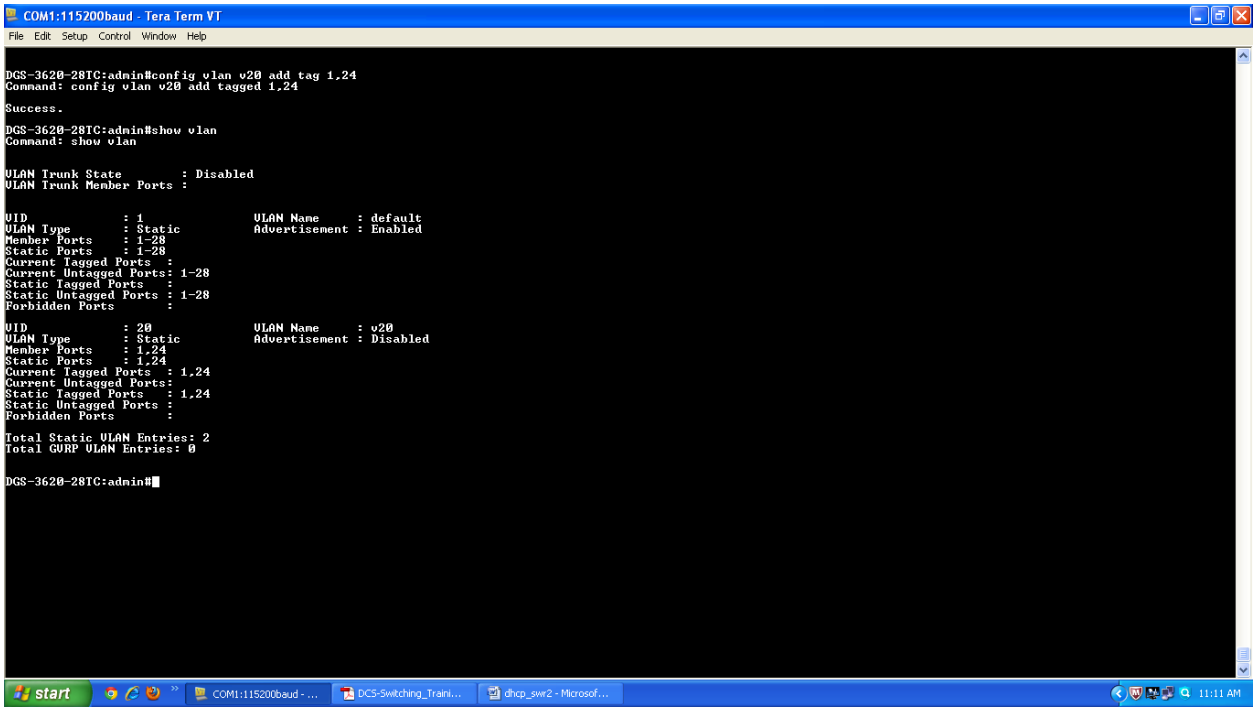


Fig. 16 : Configuring vlan v20 on SWRx2.

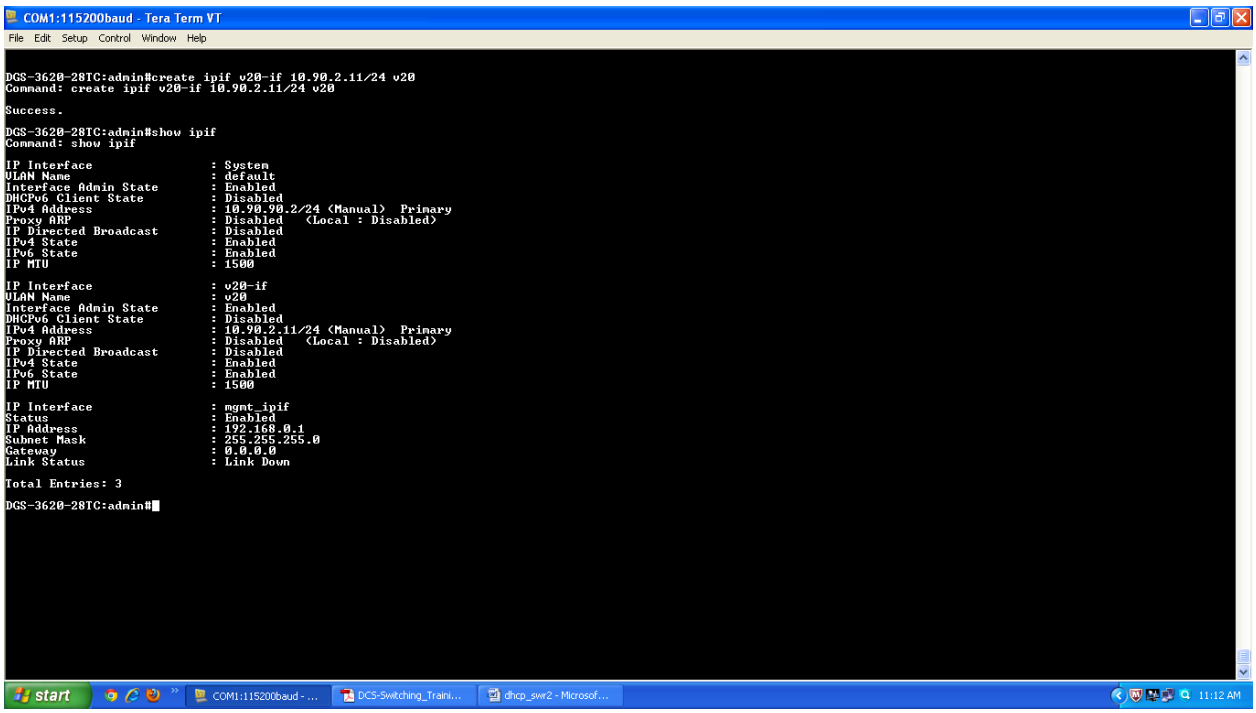


Fig. 17 : Create interface v20-if for vlan v20 on SWRx2.

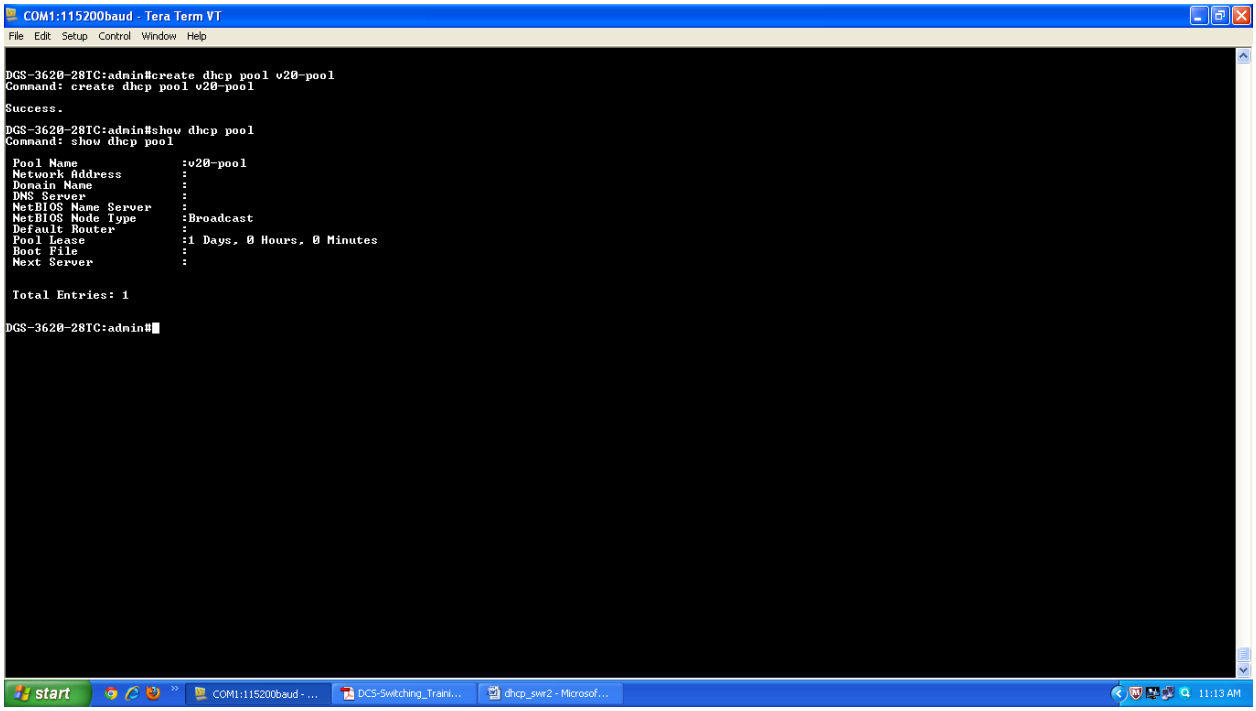


Fig. 18 (a) : Create DHCP pool v20-pool and enable DHCP server on SWRx2.

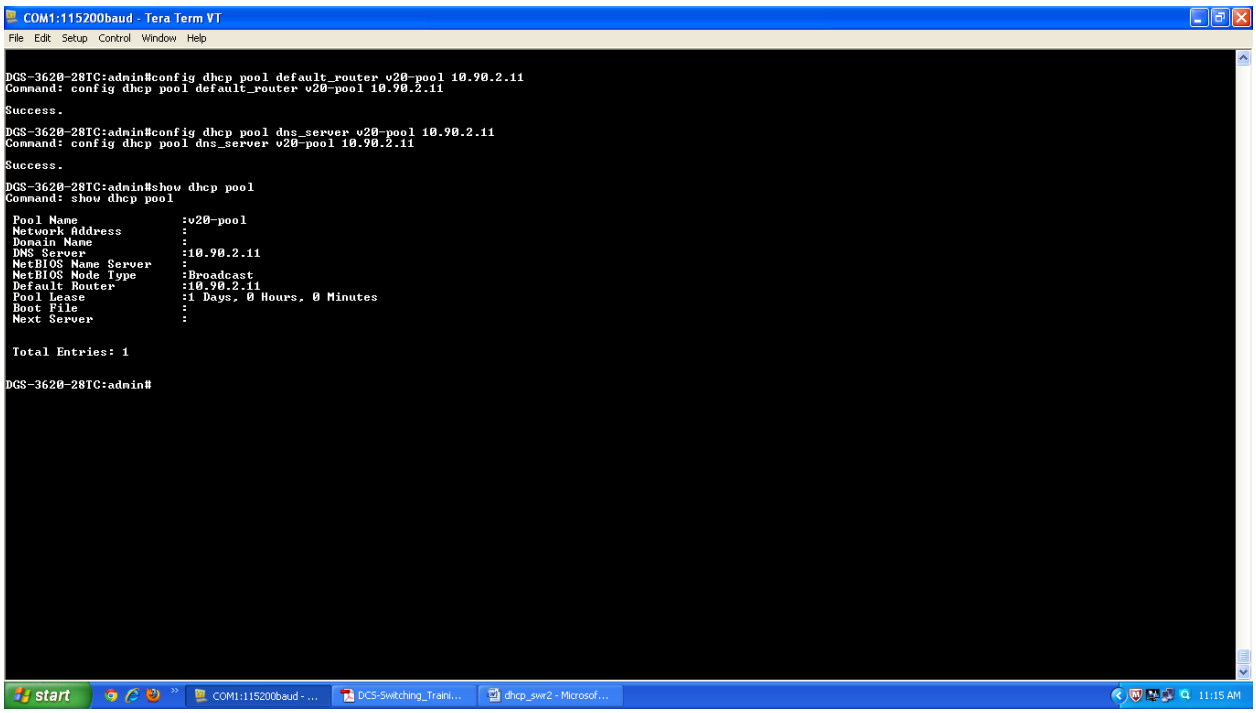


Fig. 18 (b) : Create DHCP pool v20-pool and enable DHCP server on SWRx2.

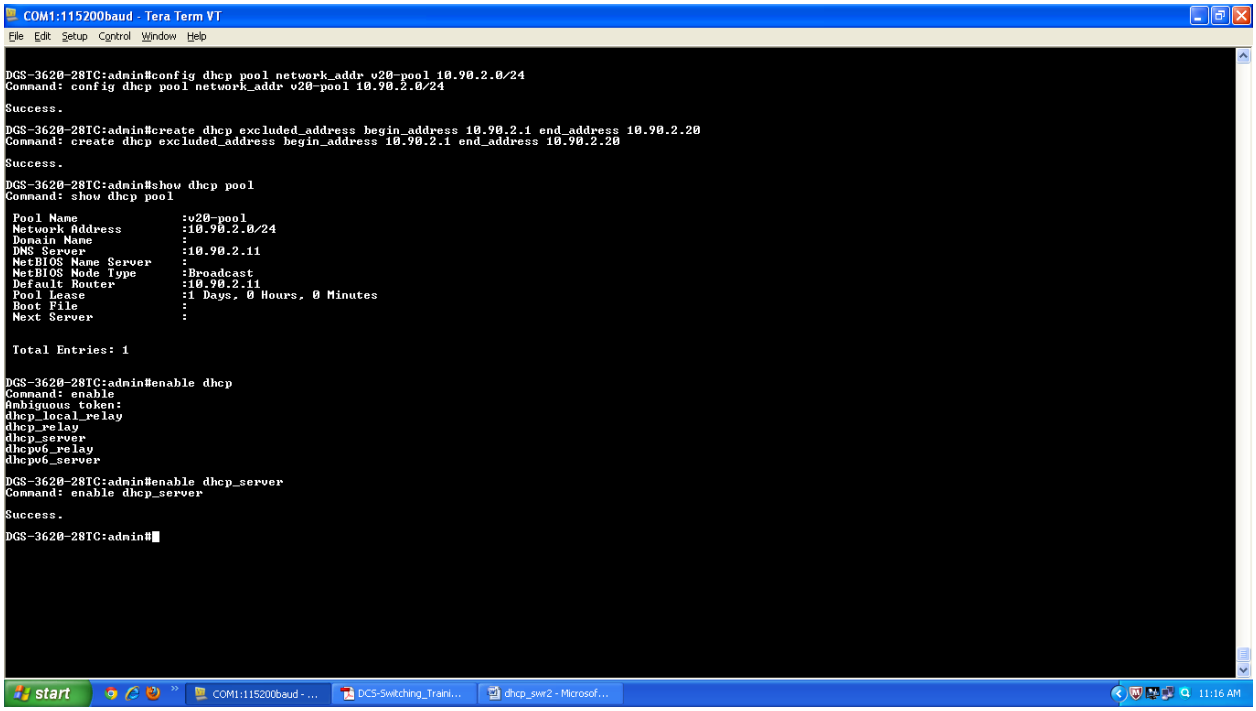


Fig. 18 (c) : Create DHCP pool v20-pool and enable DHCP server on SWRx2.

2.2.3 Configurations for SWx3

For SWx3 as a DHCP client, The configuration commands are as follows :

1. ***create vlan v10 tag 10***
2. ***config vlan v10 add tag 1***
3. ***config vlan v10 add untagged 3***
4. ***config ipif System vlan v10***
5. ***config ipif System dhcp***

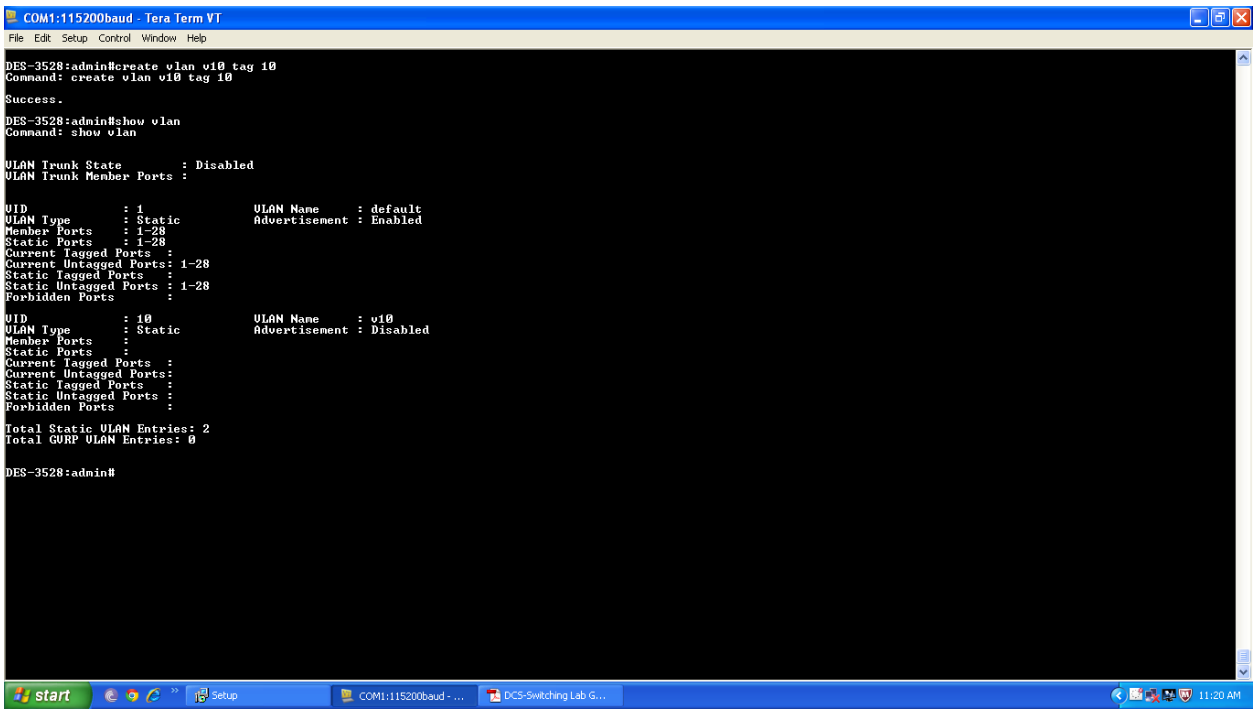


Fig. 19 : Creating vlan v10 on SWx3.

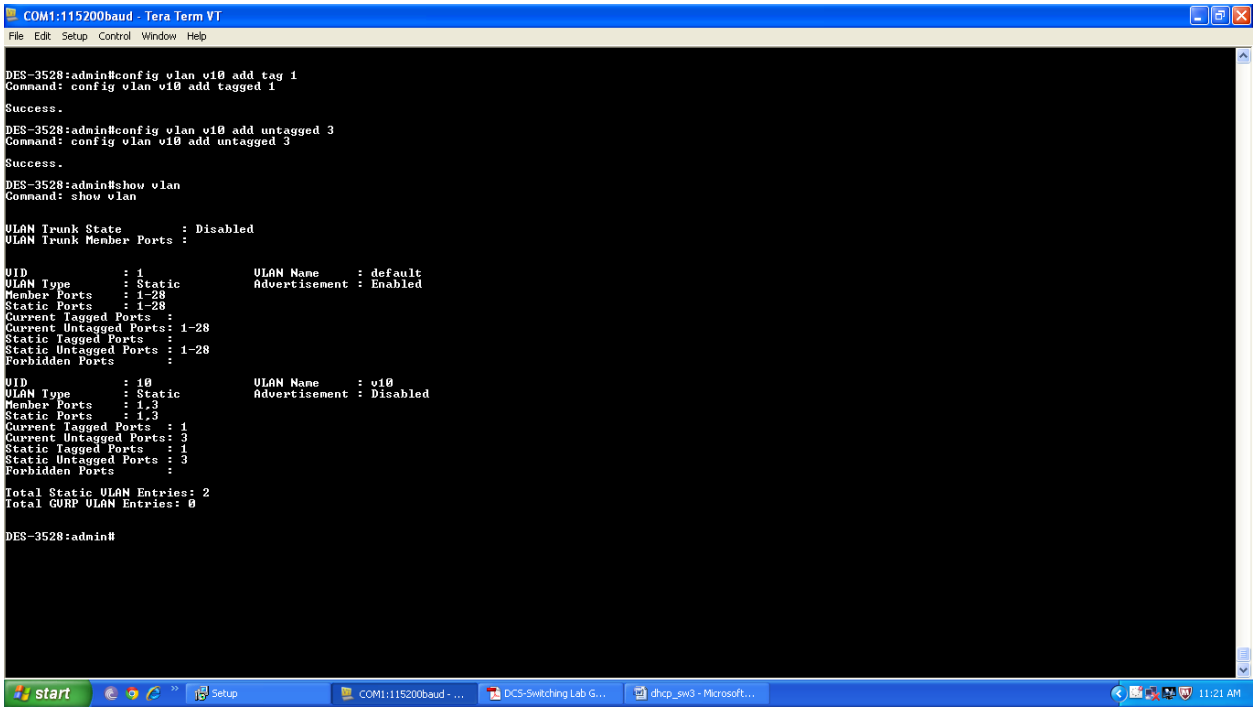


Fig. 20 : Configuring vlan v10 on SWx3.

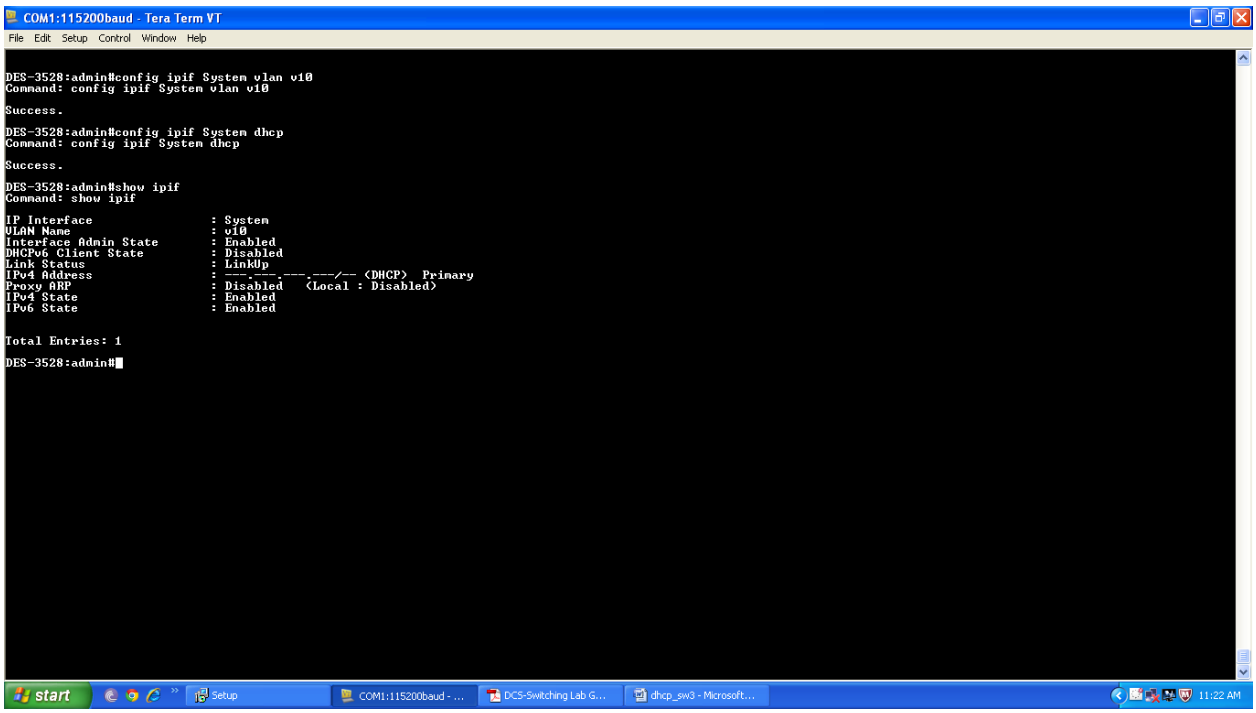


Fig. 21 : Configuring System interface for vlan v10 & DHCP on SWx3.

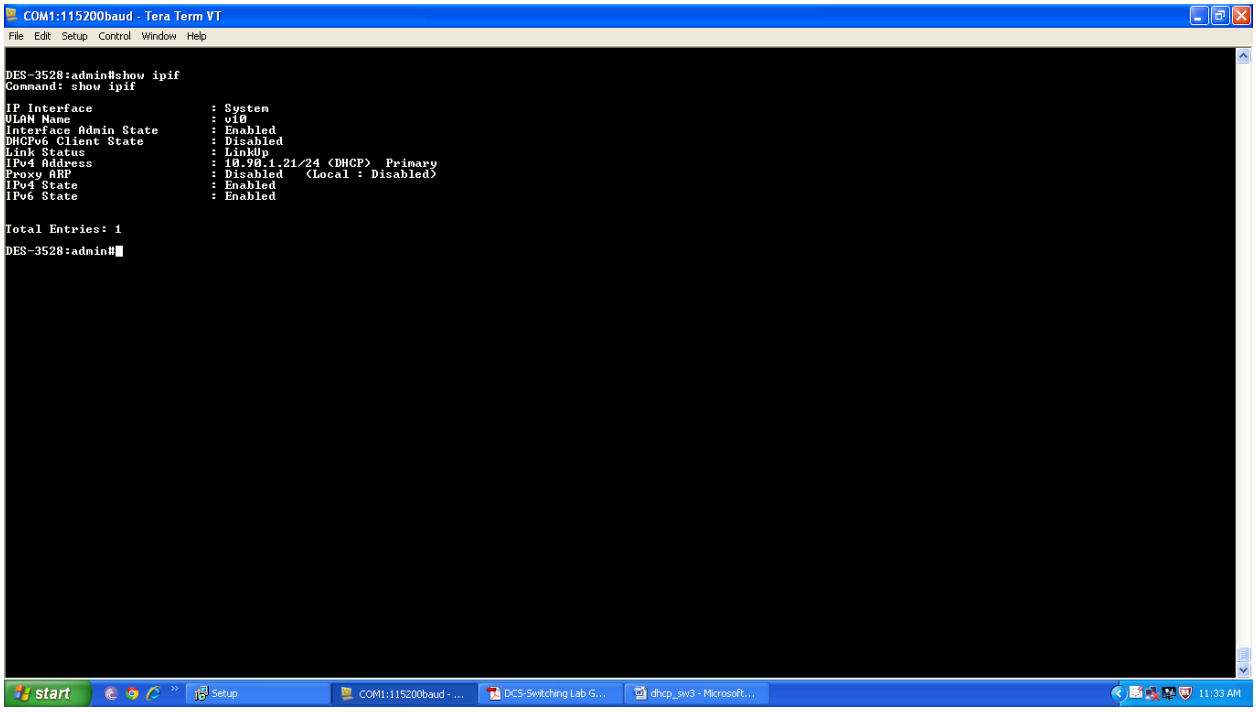


Fig. 22 : Network interfaces for on SWx3.

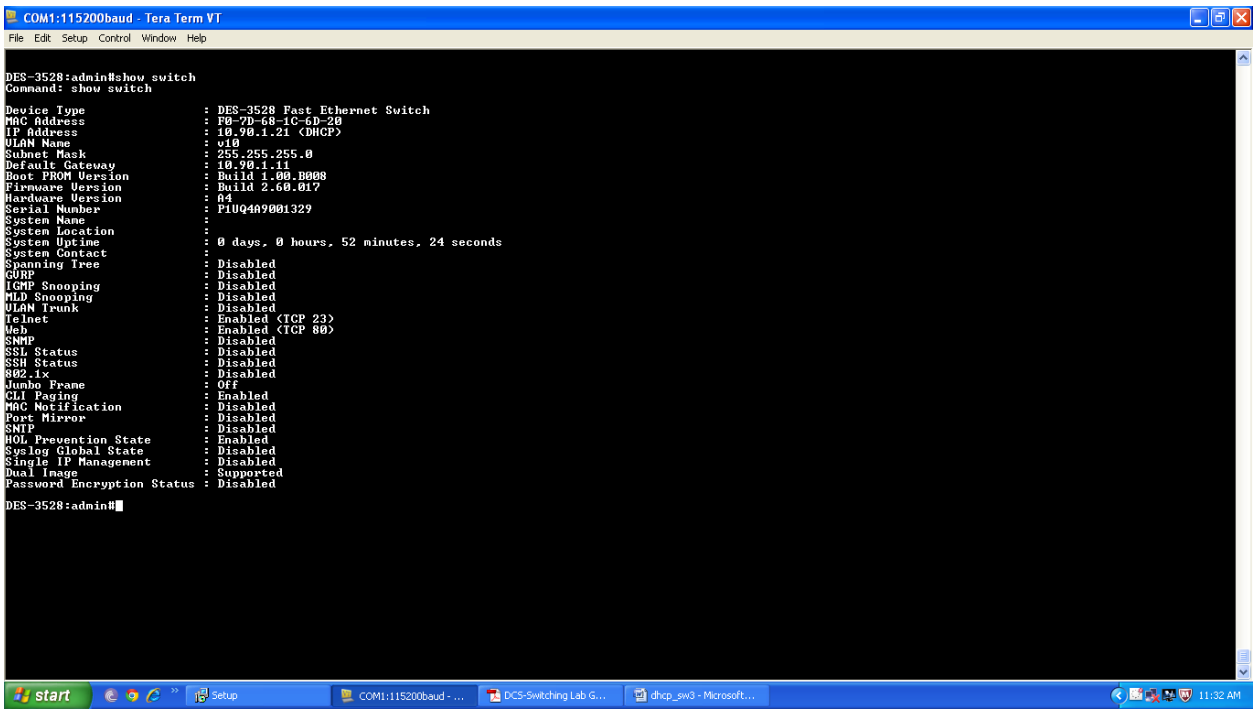


Fig. 23 : Basic Switch configurations on SWx3.

2.2.4 Configurations for SWx4

For SWx4 as a DHCP client, The configuration commands are as follows :

1. ***create vlan v20 tag 20***
2. ***config vlan v20 add tag 1***
3. ***config vlan v20 add untagged 3***
4. ***config ipif System vlan v20***
5. ***config ipif System dhcp***

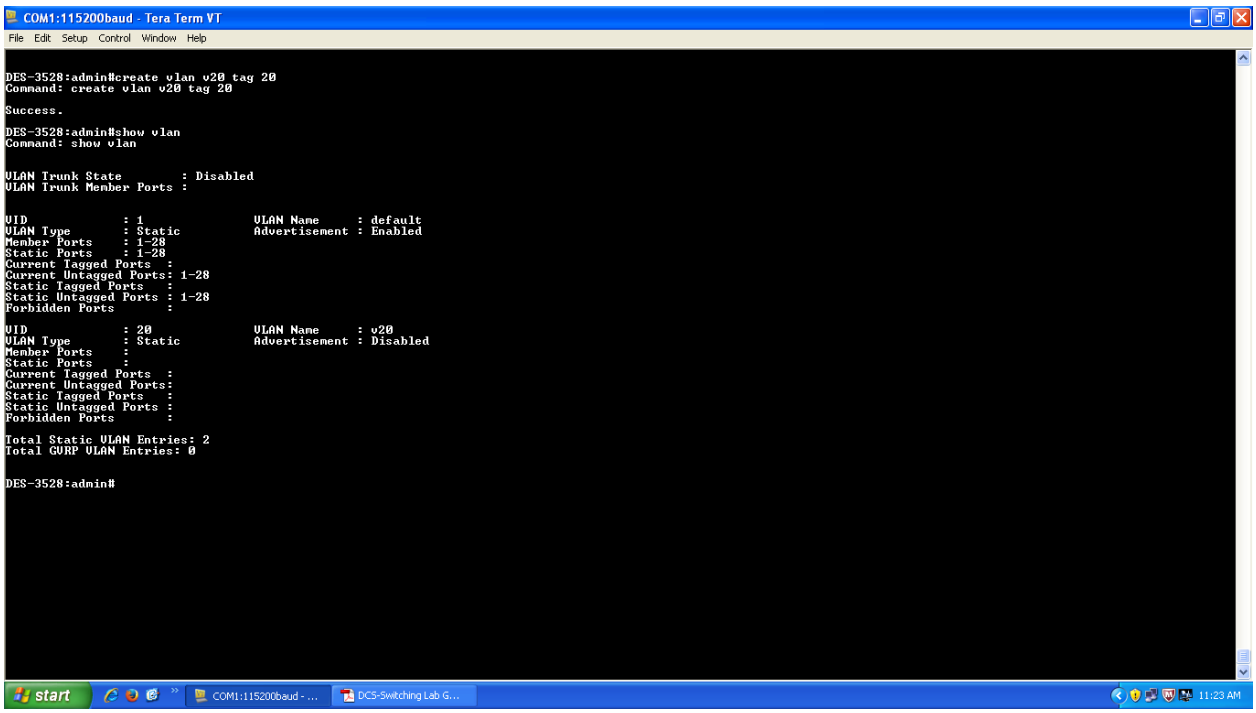


Fig. 24 : Creating vlan v20 on SWx4.

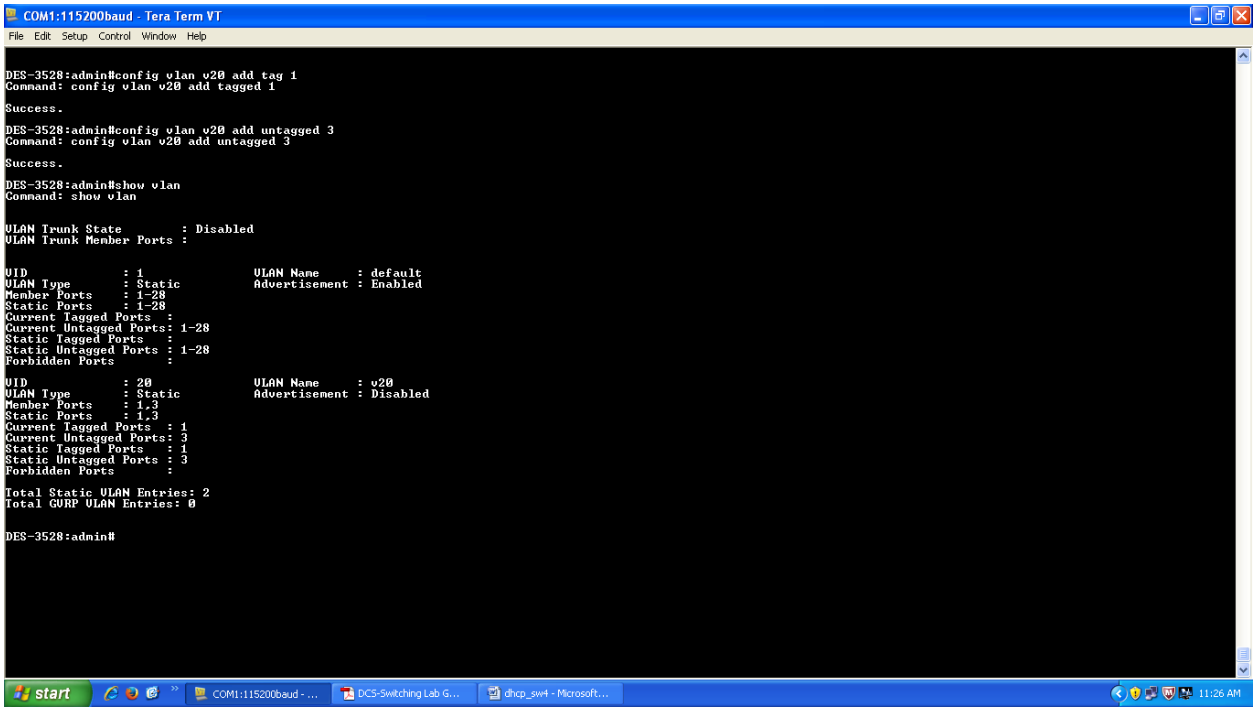


Fig. 25 : Configuring vlan v20 on SWx4.

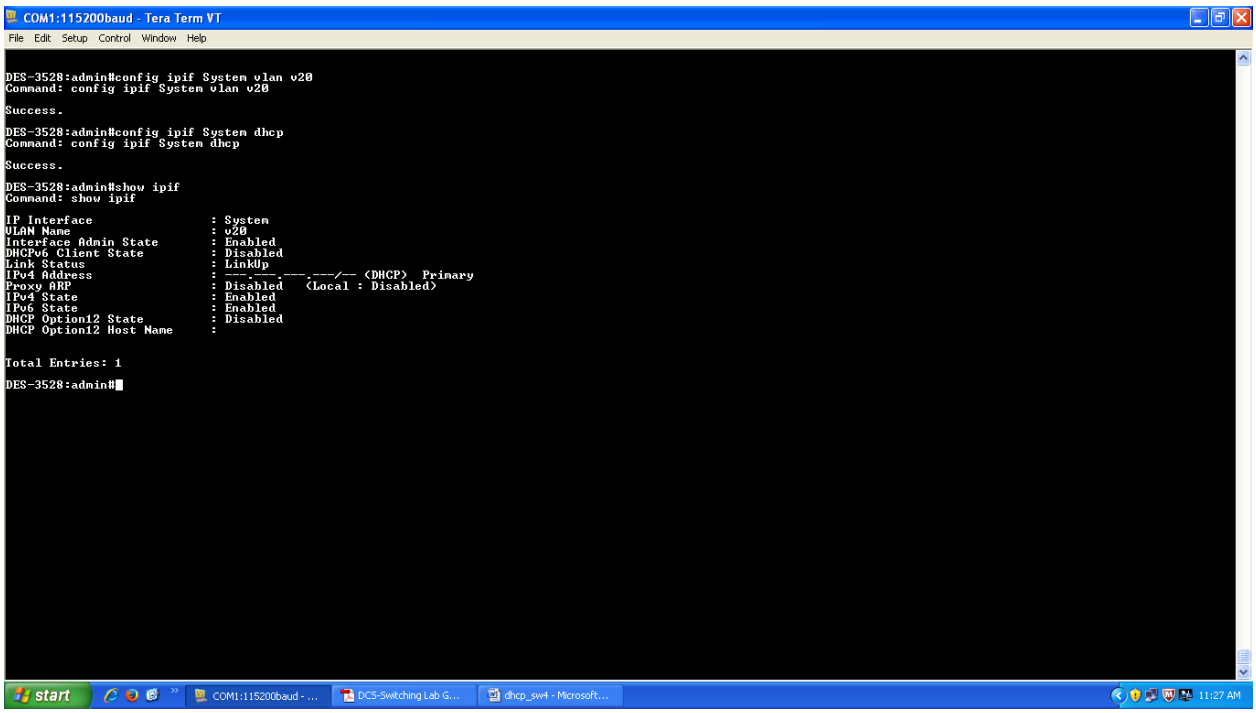


Fig. 26 : Configuring System interface for vlan v20 & DHCP on SWx4.

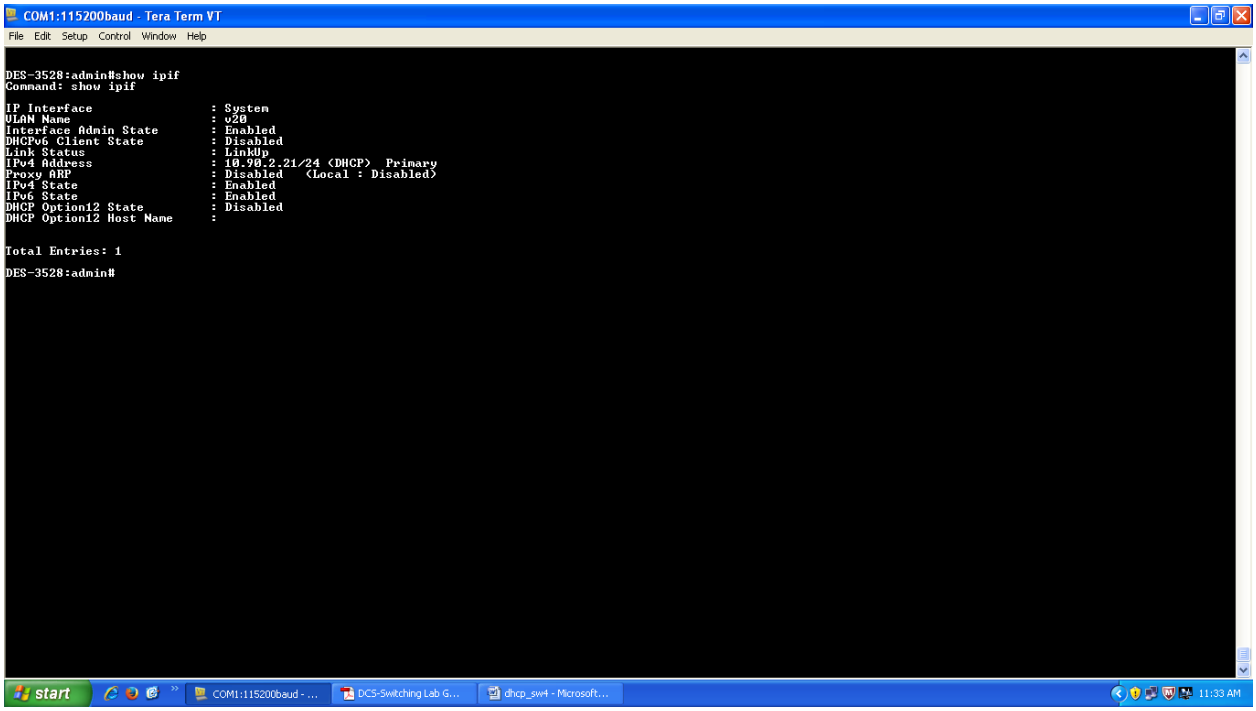


Fig. 27 : Network interfaces on SWx4.

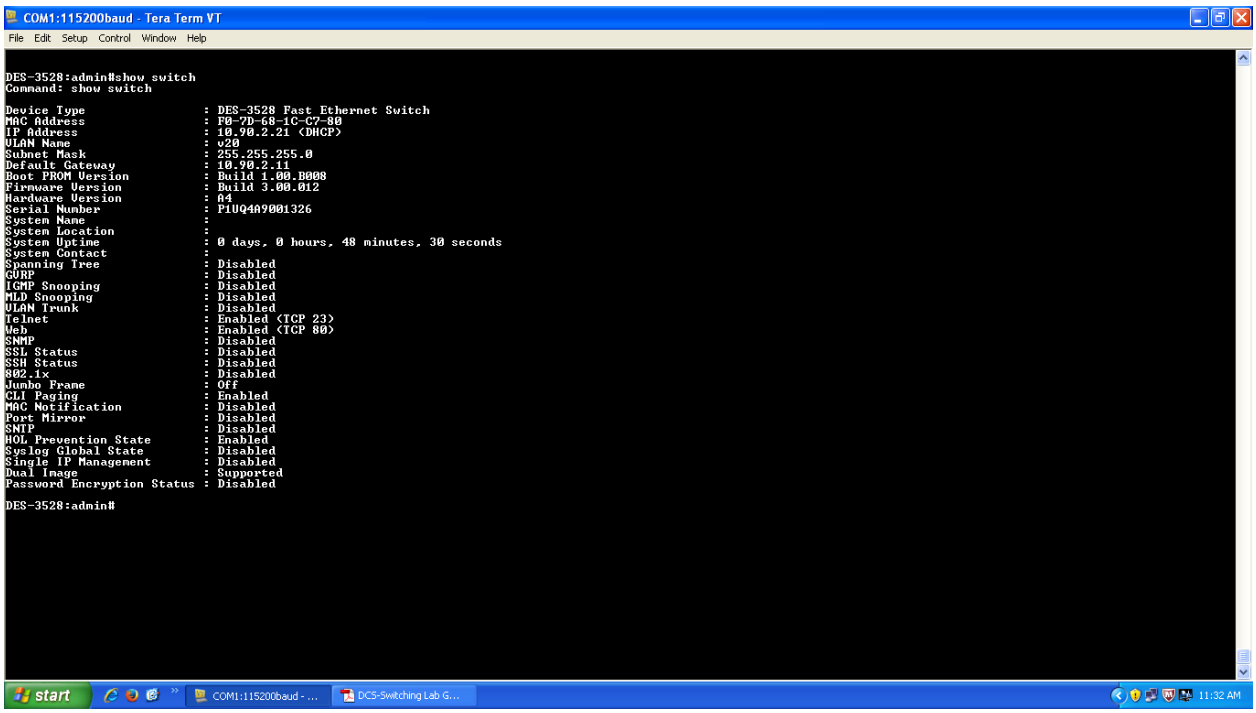


Fig. 28 : Basic Switch configurations on SWx4.

2.2.5 Configurations for SWx5

For SWx5 as a DHCP client, The configuration commands are as follows :

1. ***config ipif System dhcp***

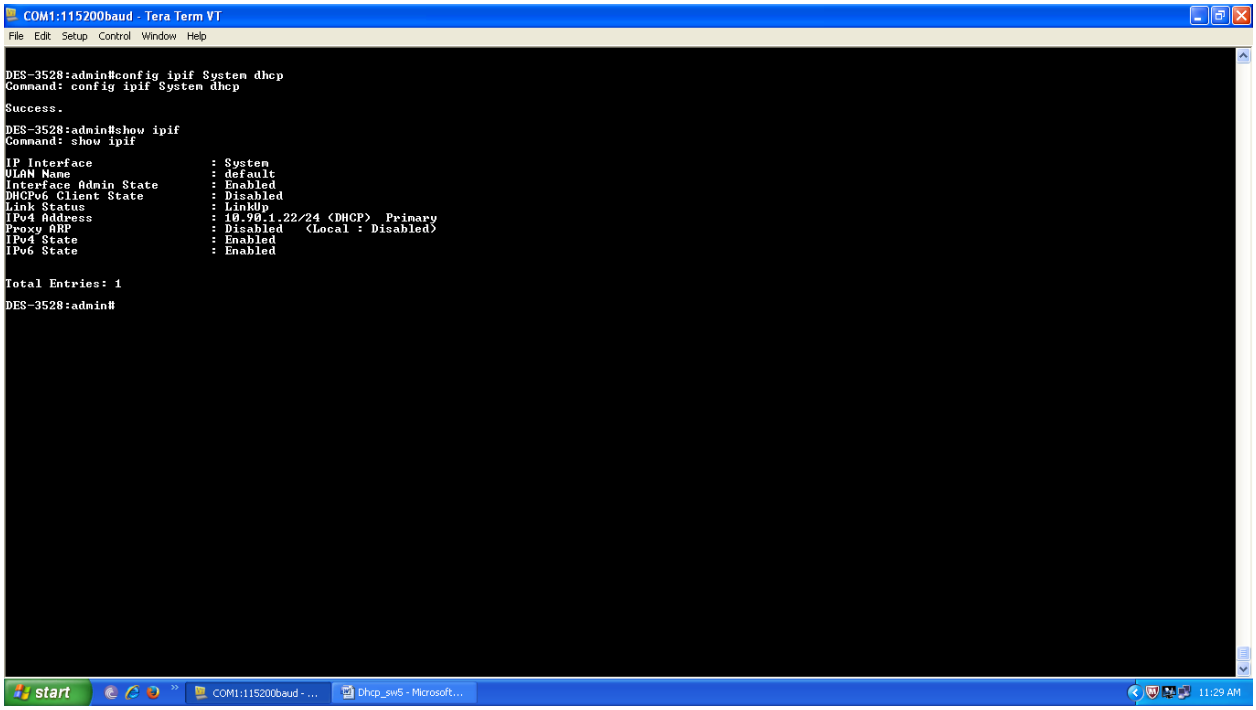


Fig. 29 : Configuring System interface for DHCP on SWx5.

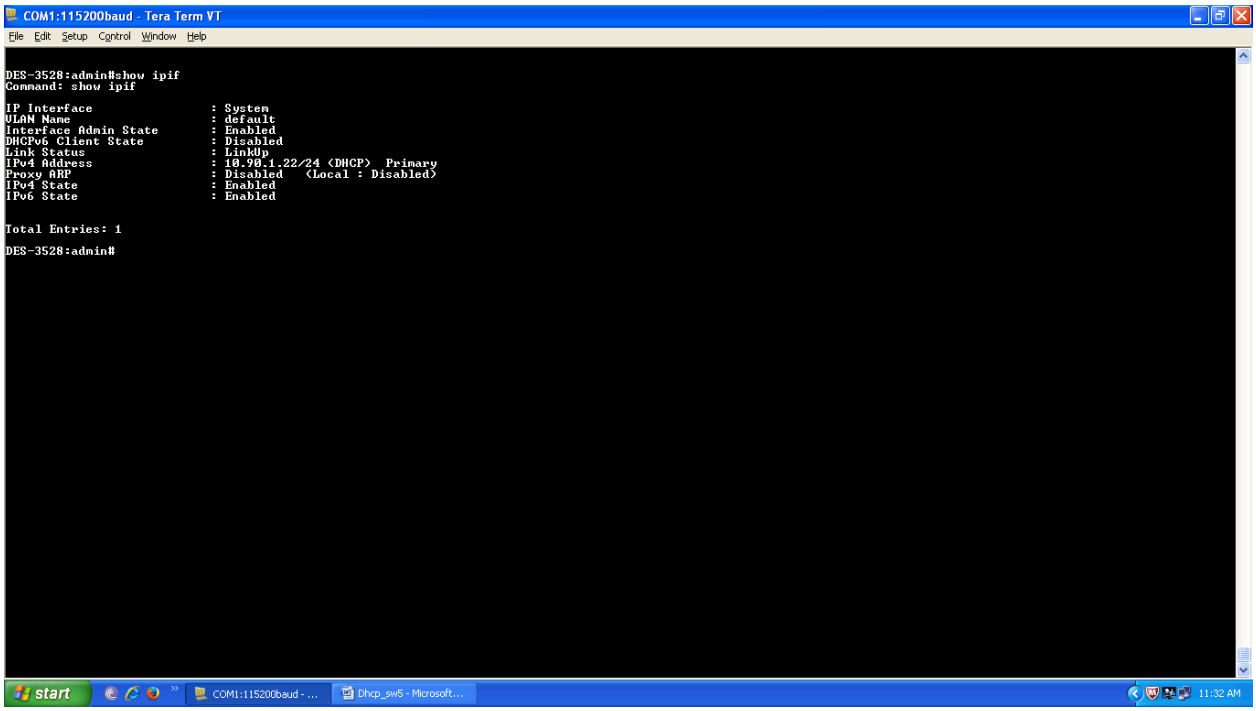


Fig. 30 : Network interfaces on SWx5.

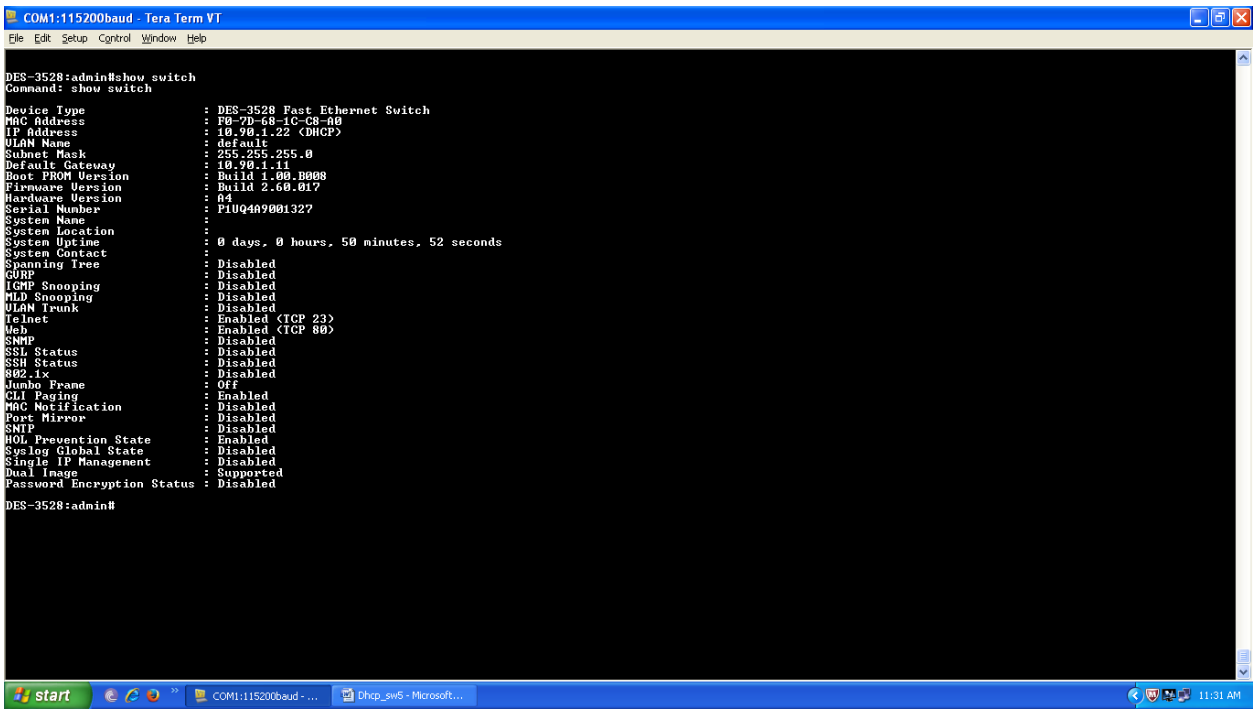


Fig. 31 : Basic Switch configurations on SWx5.

2.2.6 Configurations for SWx6

For SWx6 as a DHCP client, The configuration commands are as follows :

1. ***config ipif System dhcp***

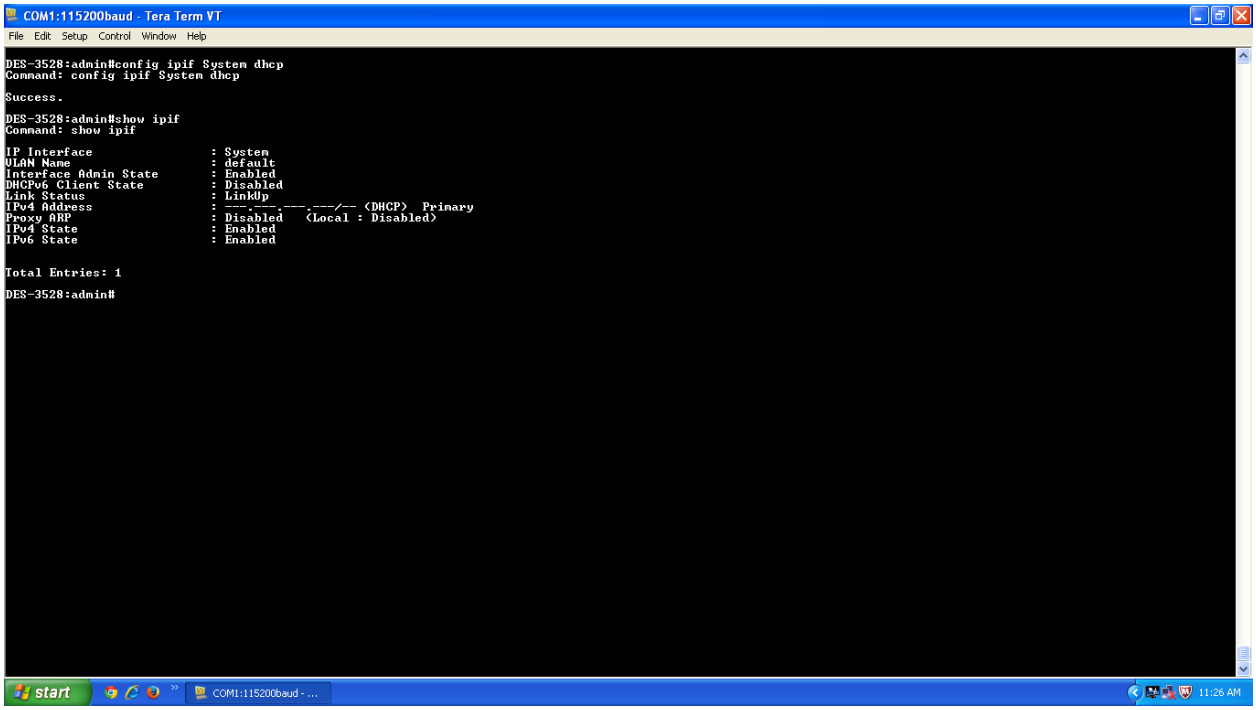


Fig. 32 : Configuring System interface for DHCP on SWx6.

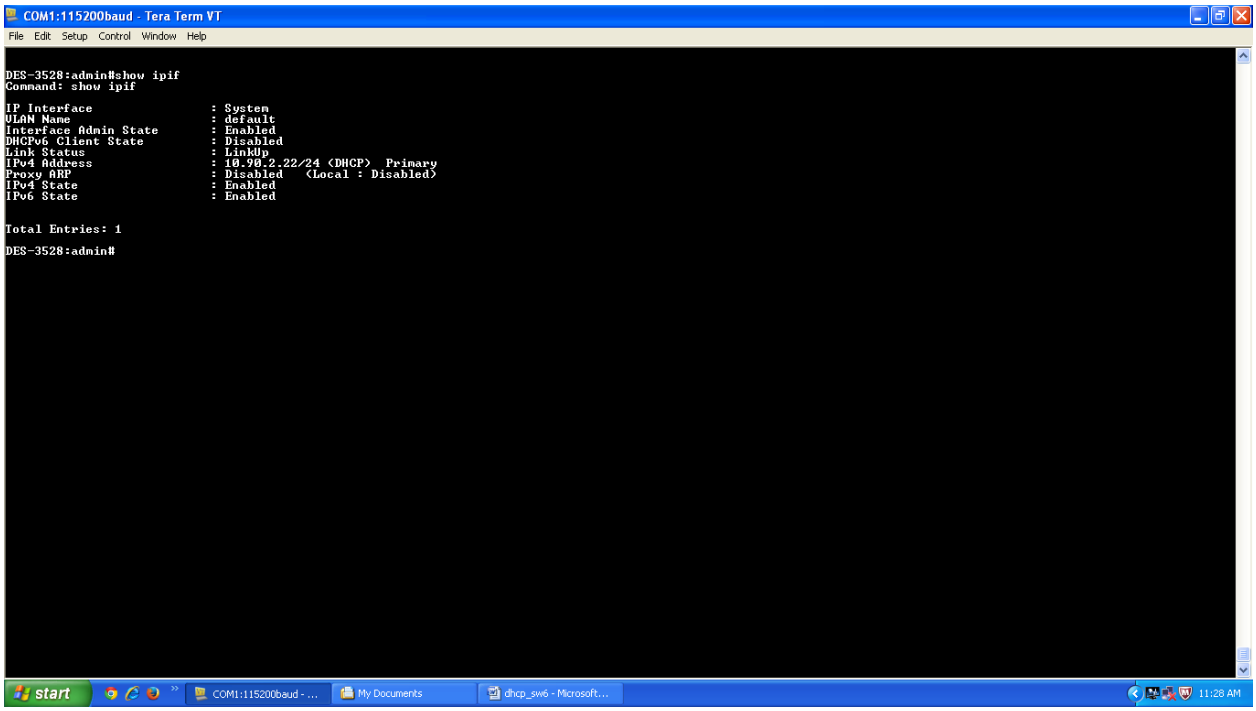


Fig. 33 : Network interfaces on SWx6.

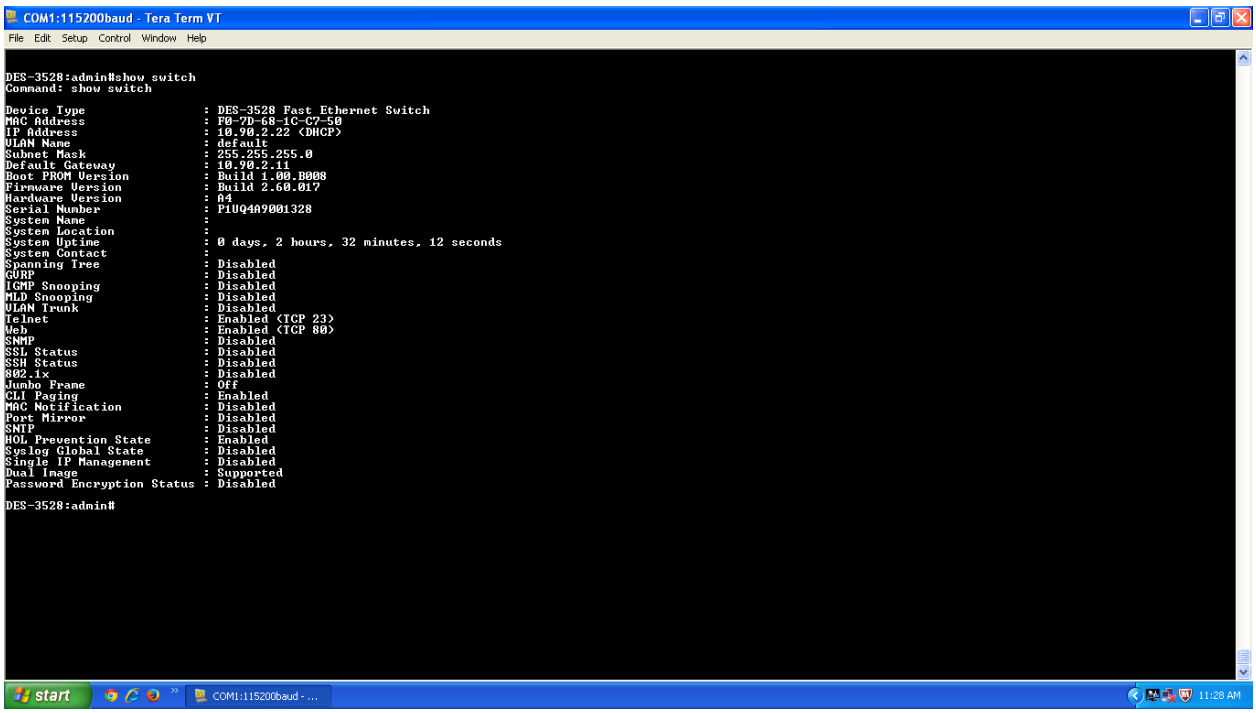


Fig. 34 : Basic Switch configurations on SWx6.

2.3 Link Layer Discovery Protocol (LLDP)

In this experiment, LLDP will be configured on all the six switches.

2.3.1 Configurations on SWRx1

For SWRx1, The configuration commands are as follows :

1. ***config lldp ports 1,24 basic_tlvs all enable***
2. ***config lldp ports 1,24 mgt_addr 1pv4 10. 90. 90. x1 enable***
3. ***config lldp ports 1,24 admin_status tx_and_rx***
4. ***config lldp ports 1,24 notification enable***
5. ***config snmp system_name SWRx1***
6. ***enable lldp***

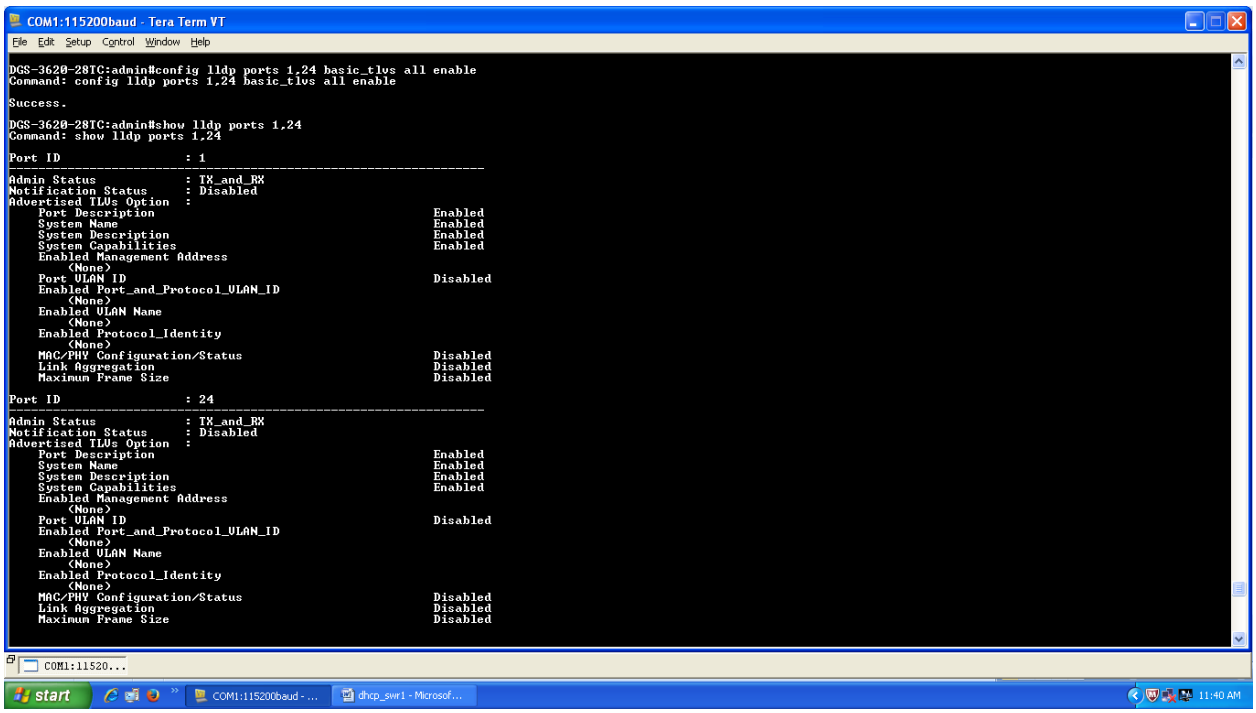


Fig. 35 : Configuring LLDP on SWRx1.

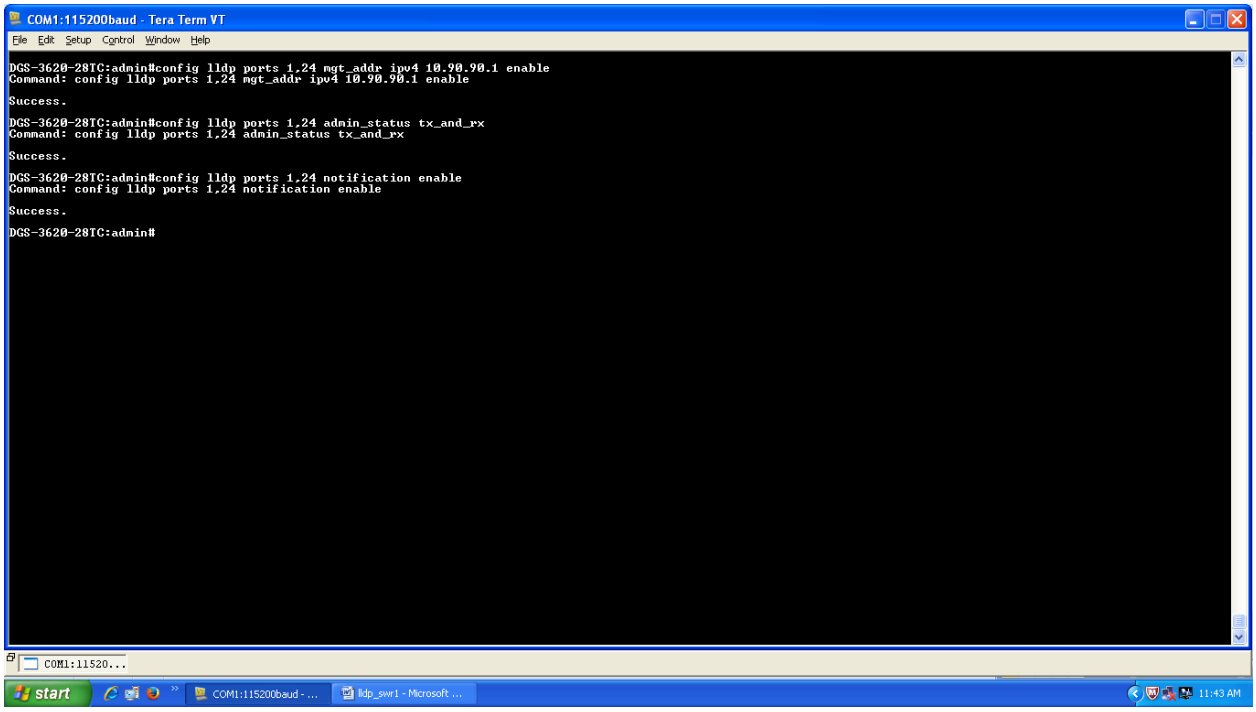


Fig. 36 : Configuring LLDP on SWRx1.

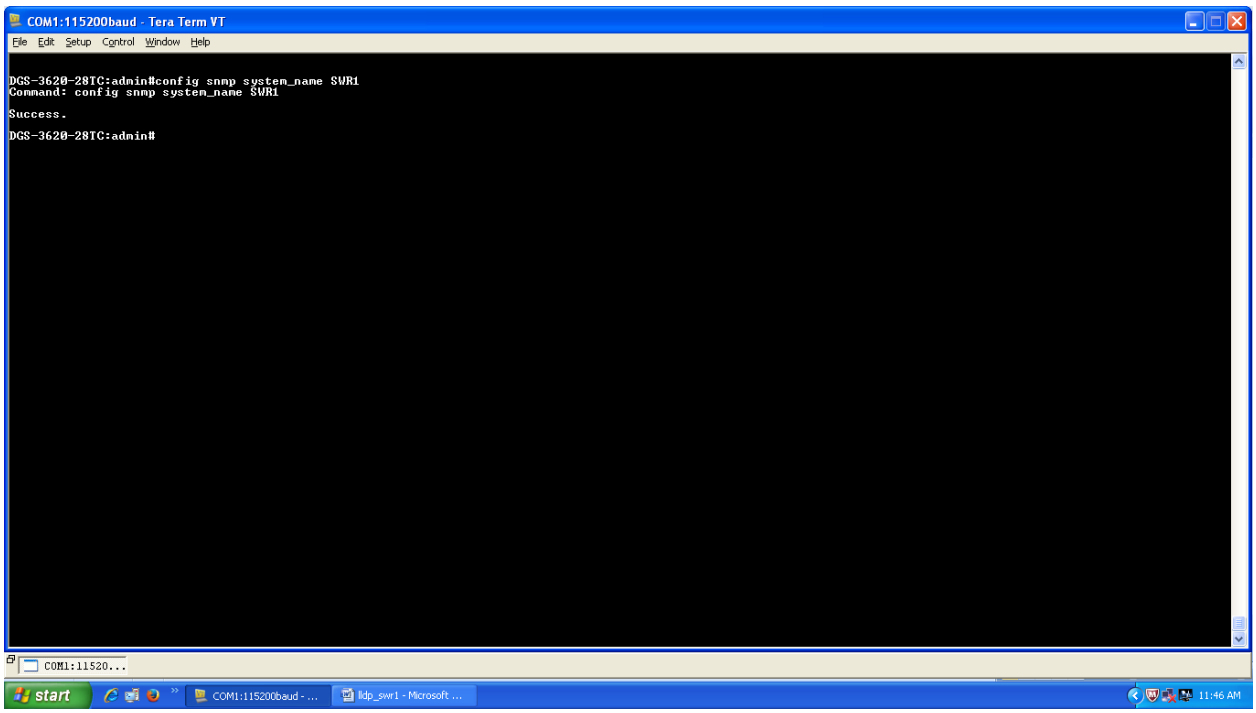


Fig. 37 : Configuring SNMP System name on SWRx1.

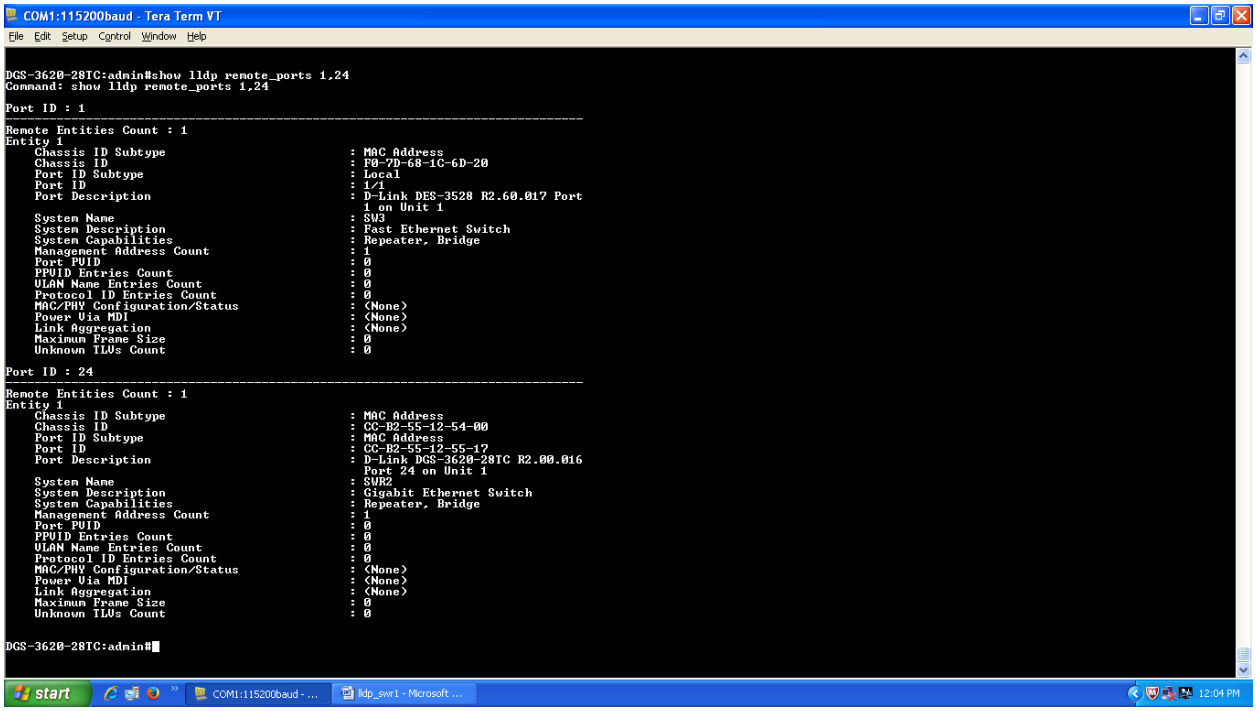


Fig. 38 : LLDP remote ports configurations on SWRx1.

2.3.2 Configurations on SWRx2

For SWRx2, The configuration commands are as follows :

1. ***config lldp ports 1,24 basic_tlvs all enable***
2. ***config lldp ports 1,24 mgt_addr ipv4 10. 90. 90. x2 enable***
3. ***config lldp ports 1,24 admin_status tx_and_rx***
4. ***config lldp ports 1,24 notifaction enable***
5. ***config snmp system_name SWRx2***
6. ***enable lldp***

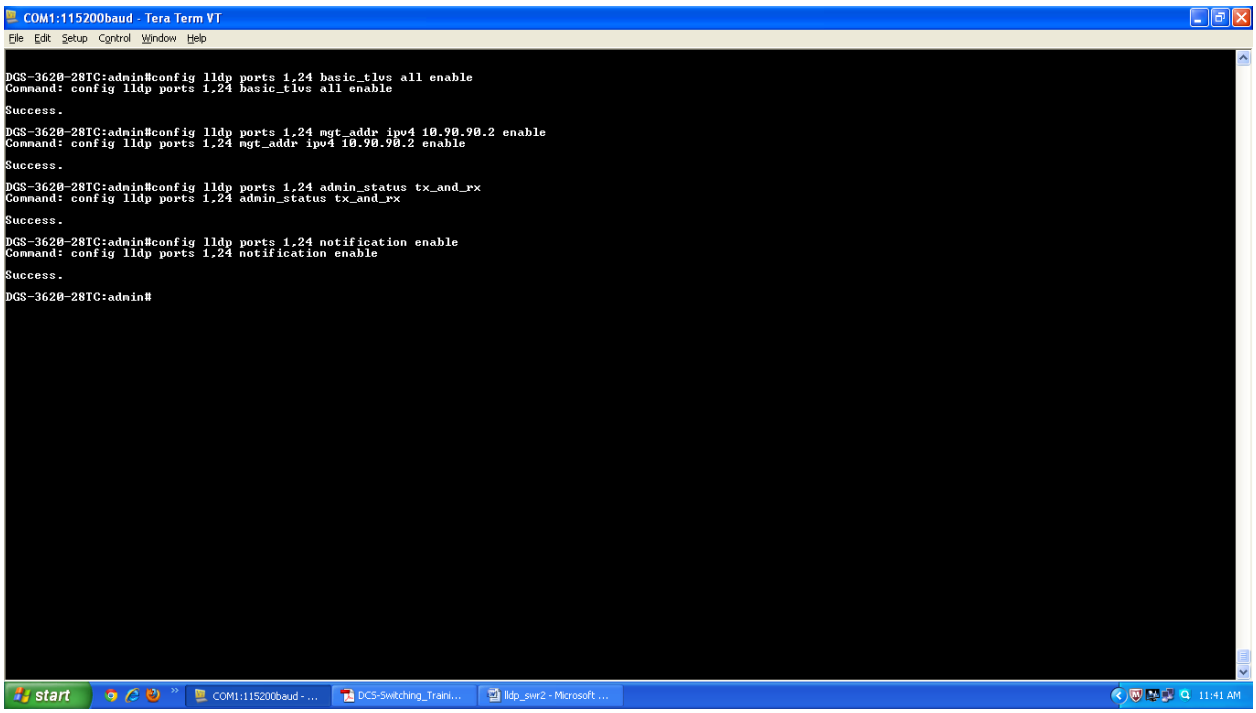


Fig. 39 : Configuring LLDP on SWRx2.

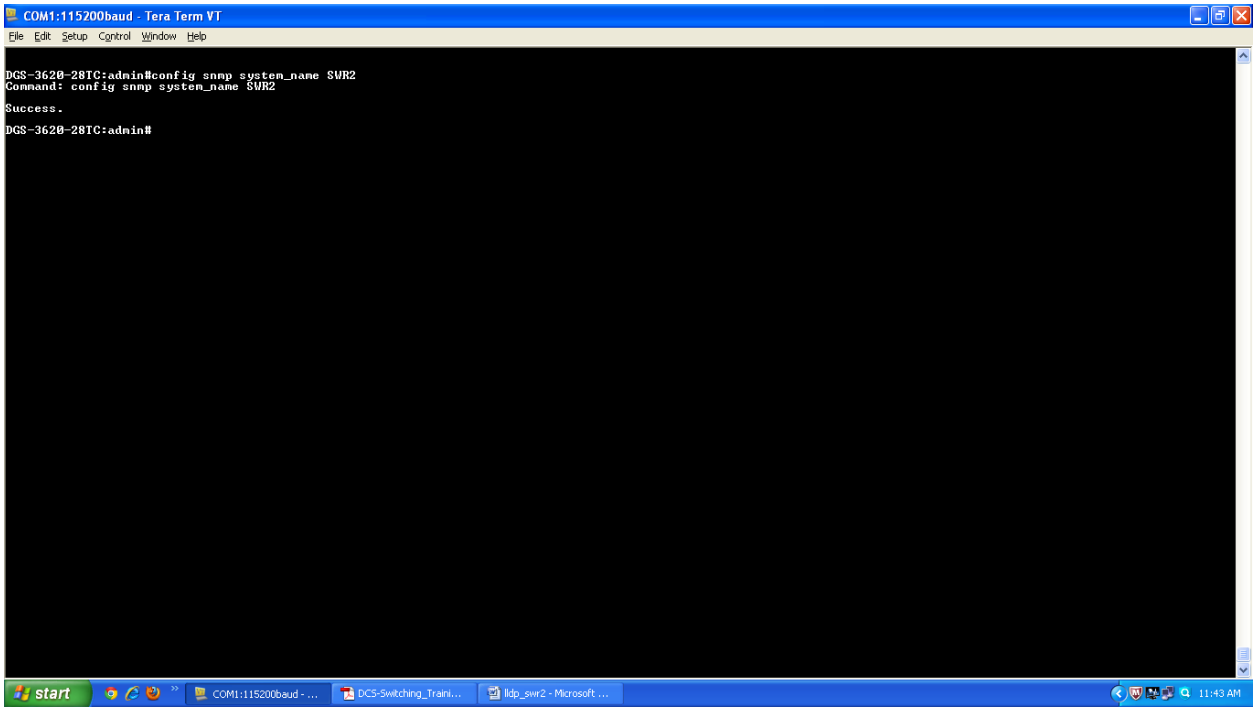


Fig. 40 : Configuring SNMP on SWRx2.

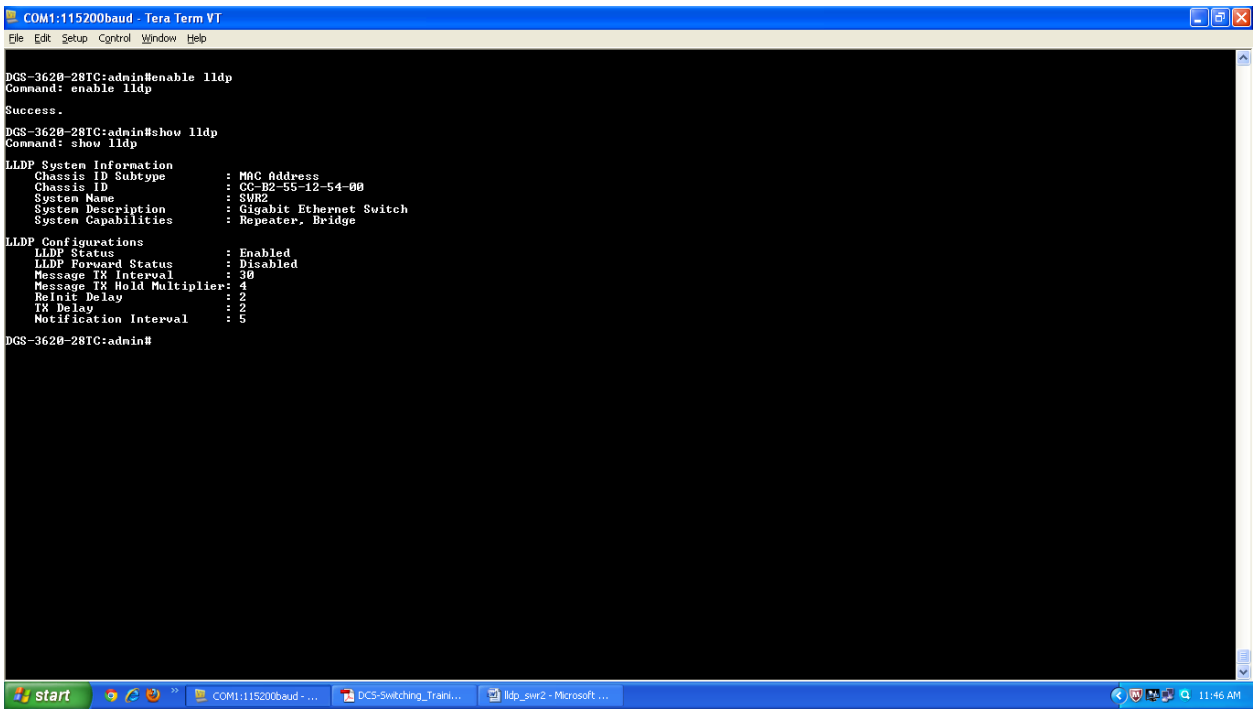


Fig. 41 : Basic LLDP configuration on SWRx2.

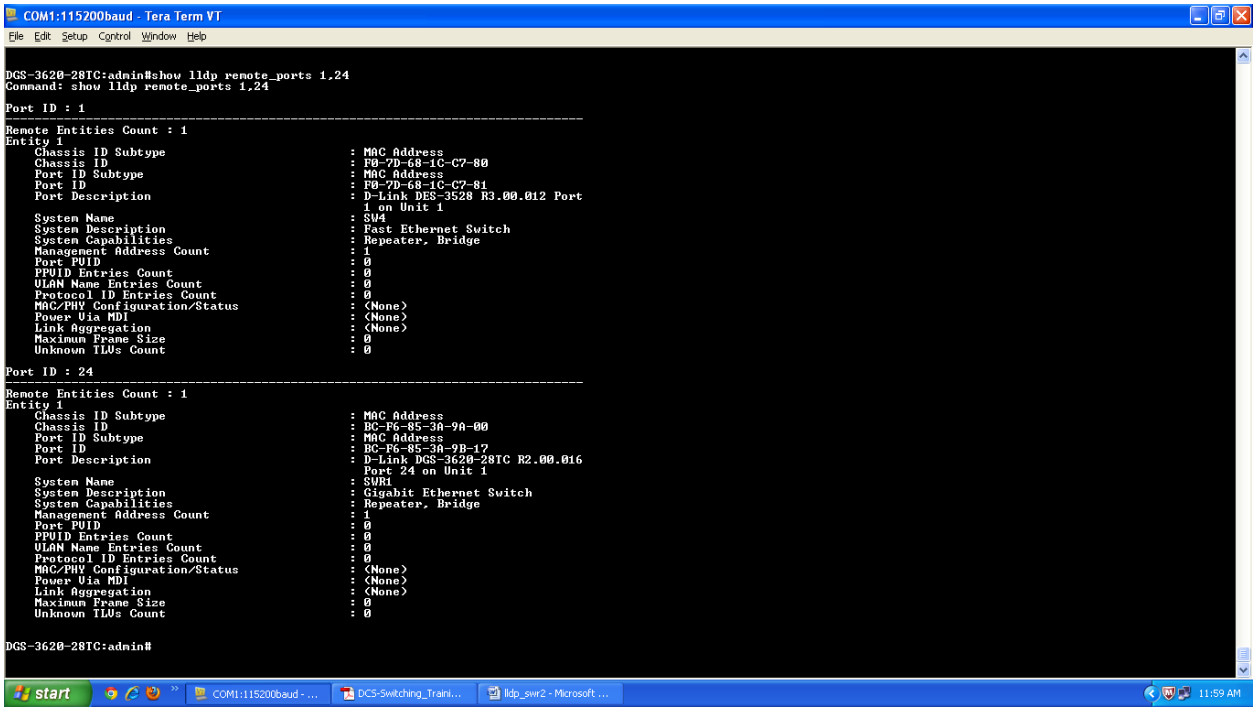


Fig. 42 : LLDP remote ports configurations on SWRx2.

2.3.3 Configurations on SWx3

For SWx3, The configuration commands are as follows :

1. ***config lldp ports 1,3 basic_tlvs all enable***
2. ***config lldp ports 1,3 mgt_addr ipv4 10. 90. 90. x3 enable***
3. ***config lldp ports 1,3 admin_status tx_and_rx***
4. ***config lldp ports 1,3 notification enable***
5. ***config snmp system_name SWx3***
6. ***enable lldp***

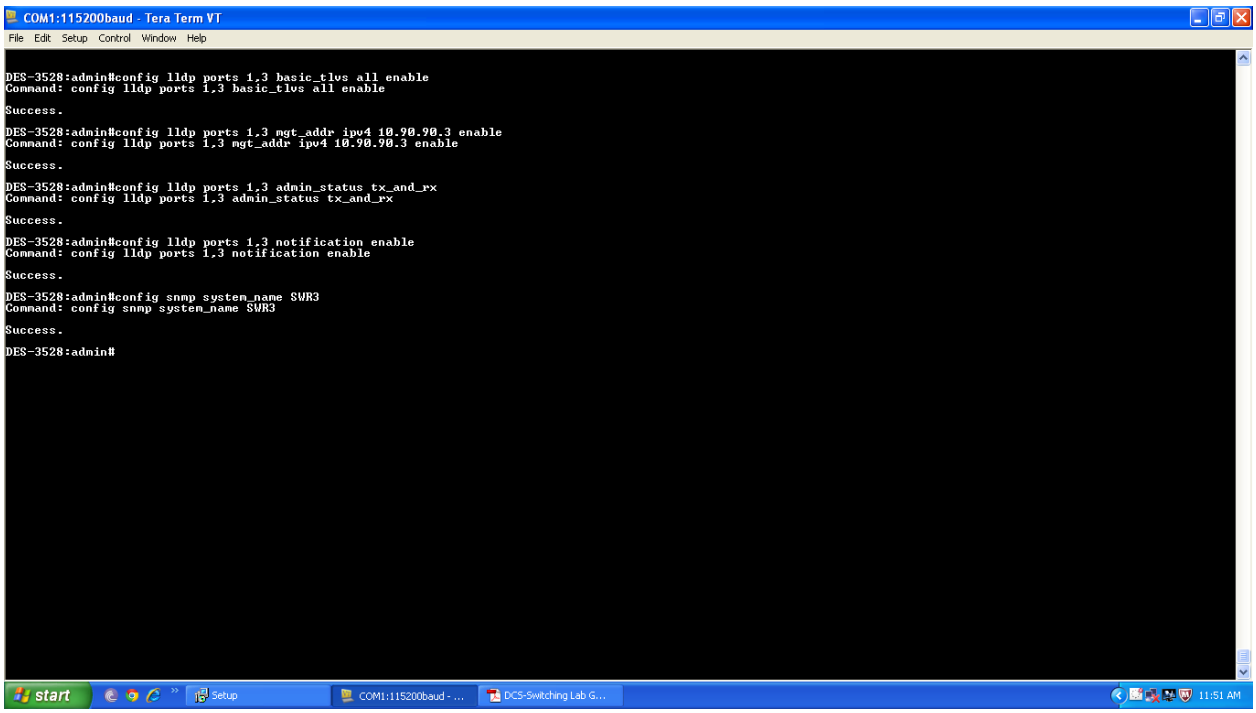


Fig. 43 : Configuring LLDP on SWx3.

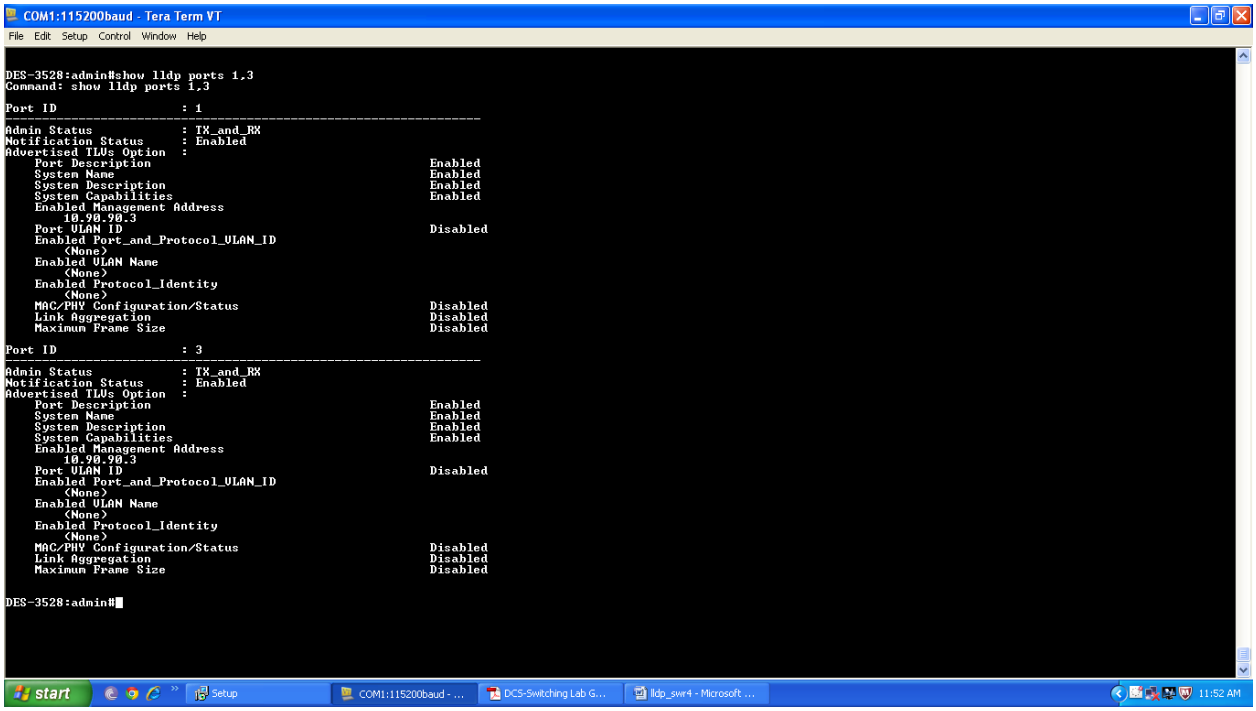


Fig. 44 : Configuring LLDP on SWx3.

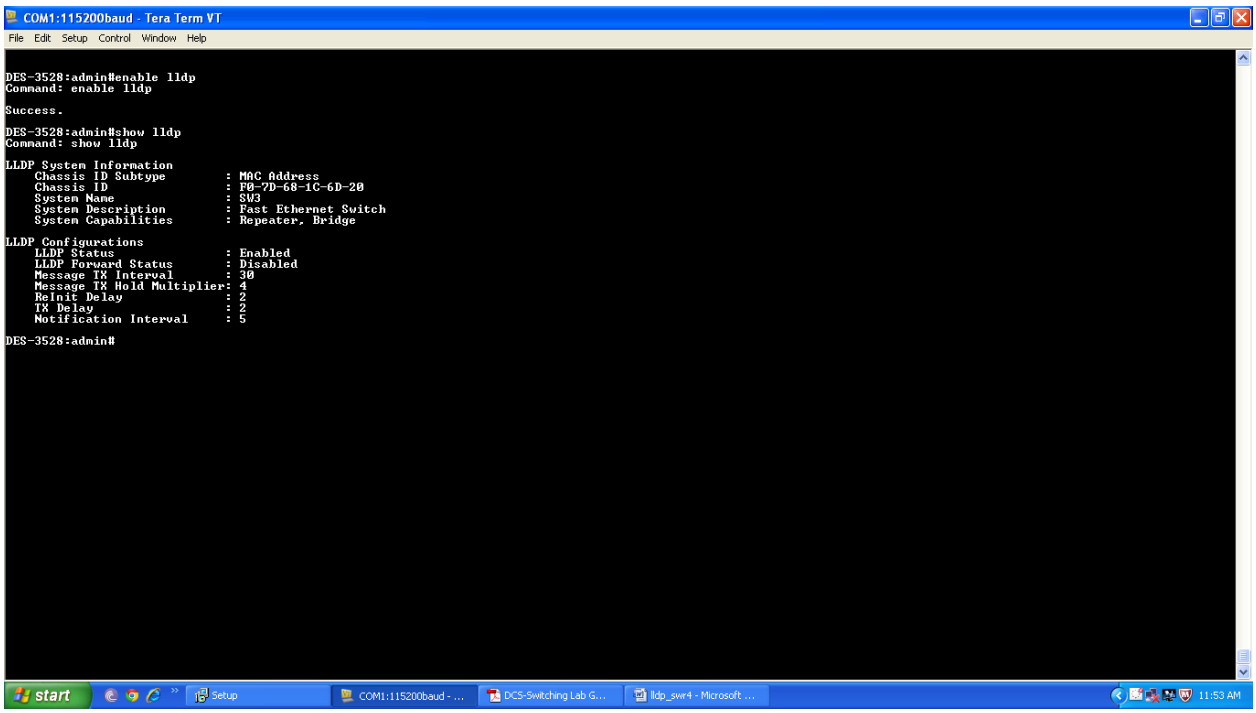


Fig. 45 : Basic LLDP configuration on SWx3.

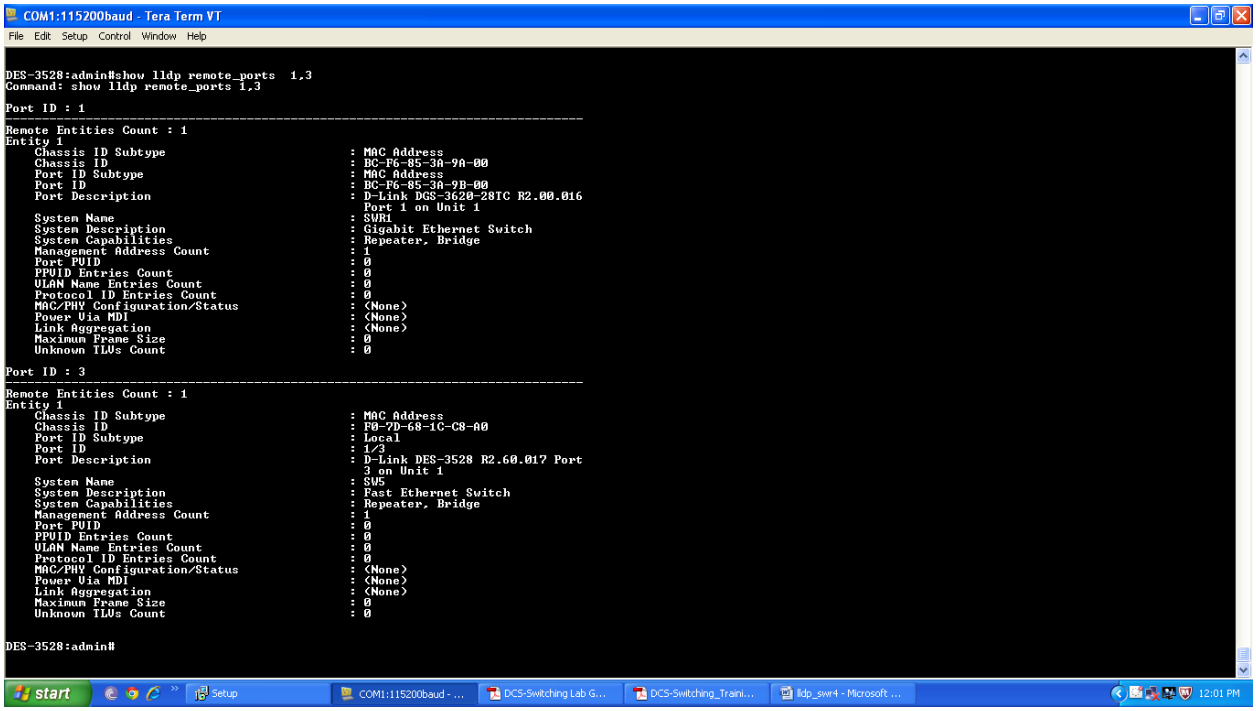


Fig. 46 : LLDP remote ports configurations on SWx3.

2.3.4 Configurations on SWx4

For SWx4, The configuration commands are as follows :

1. ***config lldp ports 1,3 basic_tlvs all enable***
2. ***config lldp ports 1,3 mgt_addr ipv4 10. 90. 90. x4 enable***
3. ***config lldp ports 1,3 admin_status tx_and_rx***
4. ***config lldp ports 1,3 notification enable***
5. ***config snmp system_name SWx4***
6. ***enable lldp***

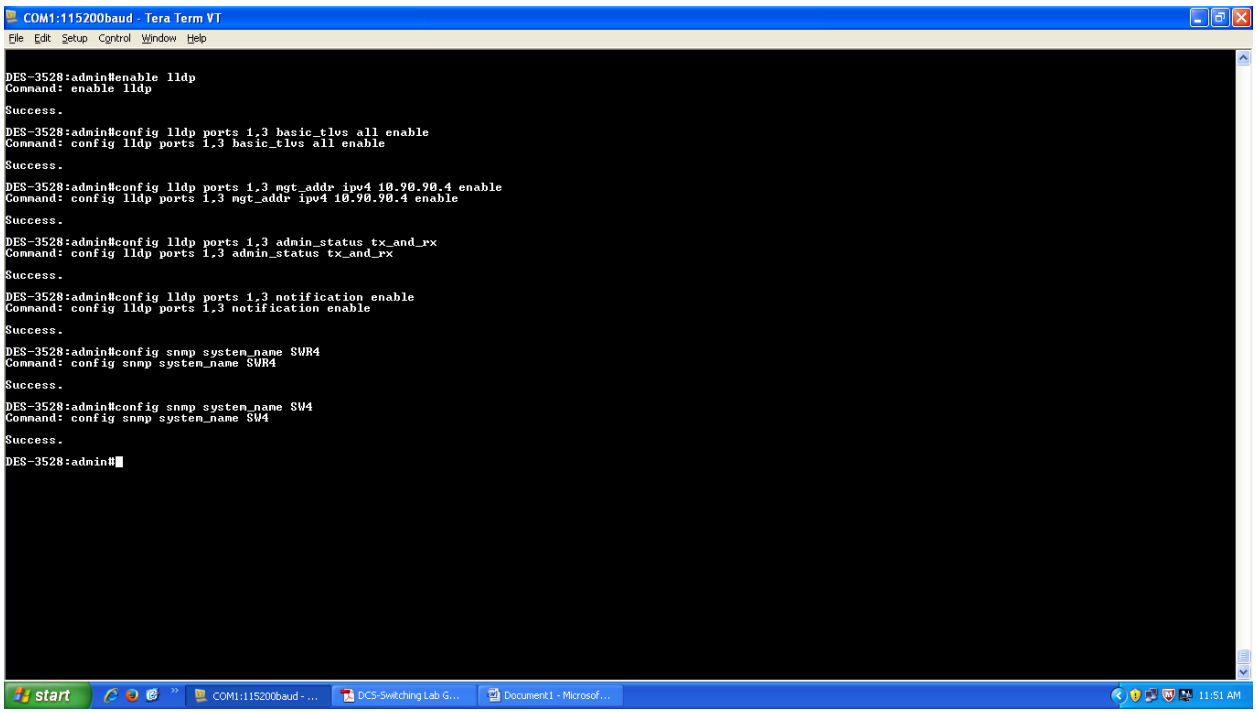


Fig. 47 : Configuring LLDP on SWx4.

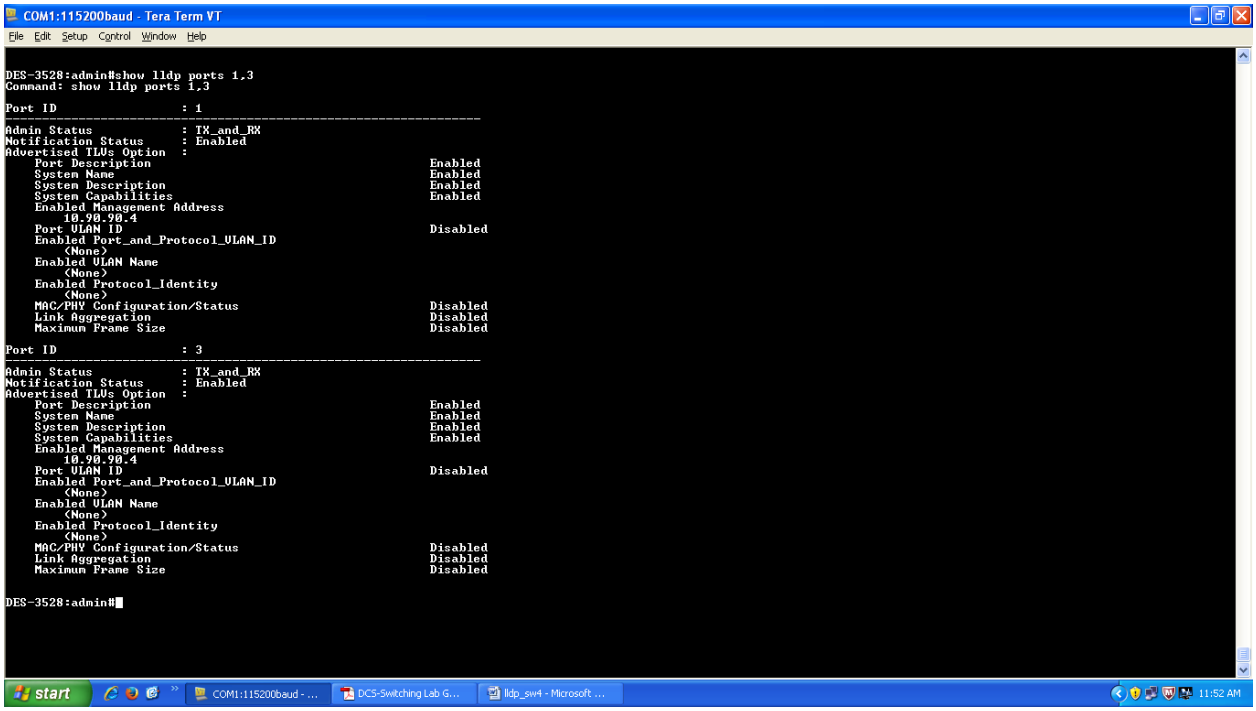


Fig. 48 : Configuring LLDP on SWx4.

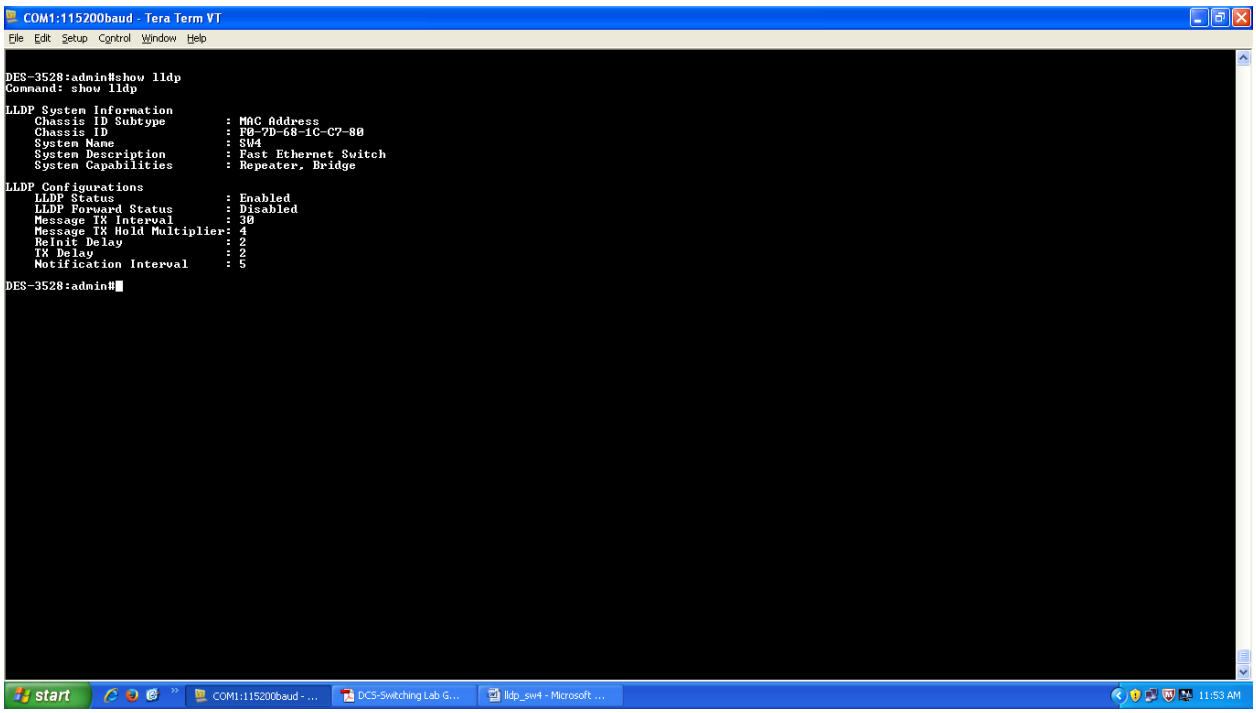


Fig. 49 : Basic LLDP configuration on SWx4.

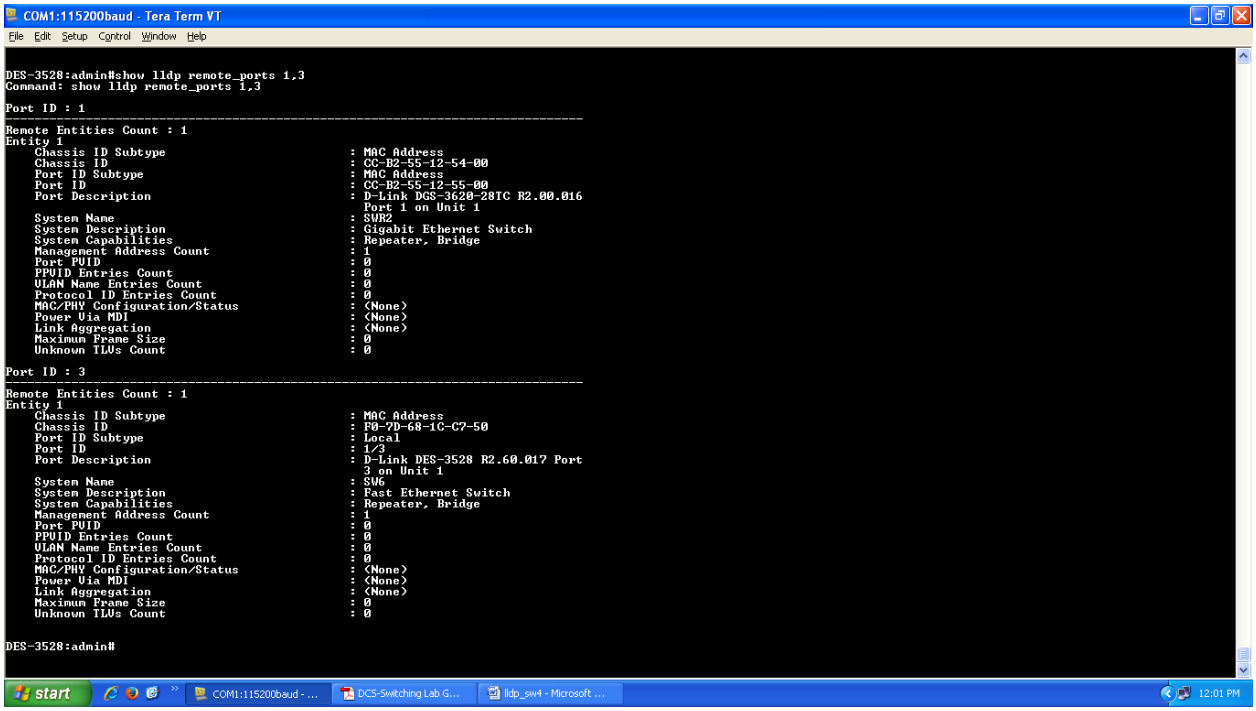


Fig. 50 : LLDP remote ports configurations on SWx4.

2.3.5 Configurations on SWx5

For SWx5, The configuration commands are as follows :

1. ***config lldp ports 3 basic_tlvs all enable***
2. ***config lldp ports 3 mgt_addr ipv4 10. 90. 90. x5 enable***
3. ***config lldp ports 3 admin_status tx_and_rx***
4. ***config lldp ports ports 3 notification enable***
5. ***config snmp system_name SWx5***
6. ***enable lldp***

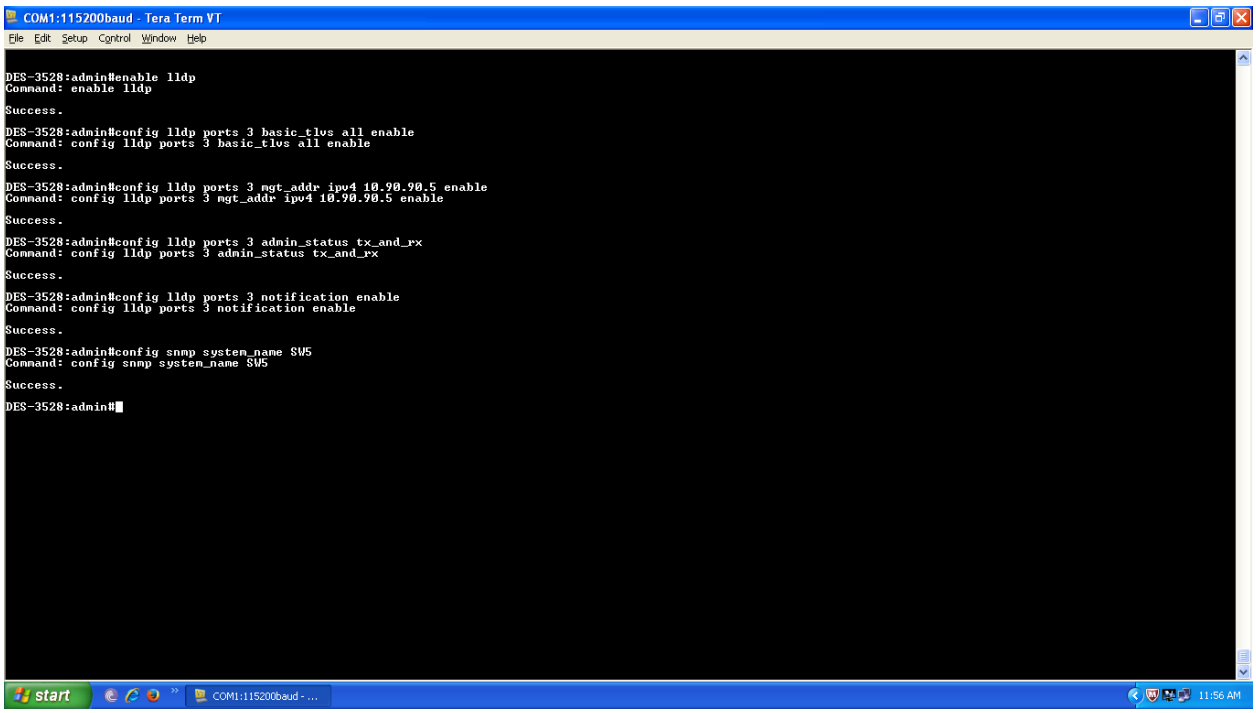


Fig. 51 : Configuring LLDP on SWx5.

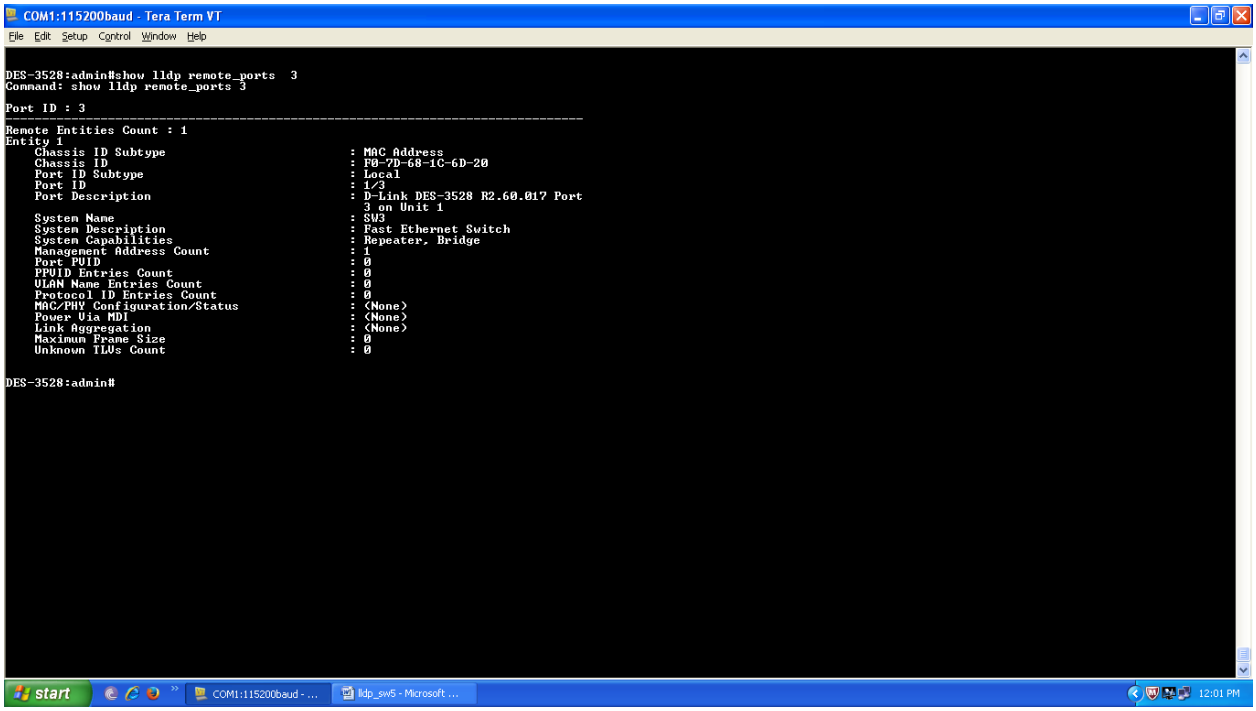


Fig. 52 : LLDP remote ports configurations on SWx5.

2.3.6 Configurations on SWx6

For SWx6, The configuration commands are as follows :

1. ***config lldp ports 3 basic_tlvs all enable***
2. ***config lldp ports 3 mgt_addr ipv4 10. 90. 90. x6 enable***
3. ***config lldp ports 3 admin_status tx_and_rx***
4. ***config lldp ports 3 notification enable***
5. ***config snmp system_name SWx6***
6. ***enable lldp***

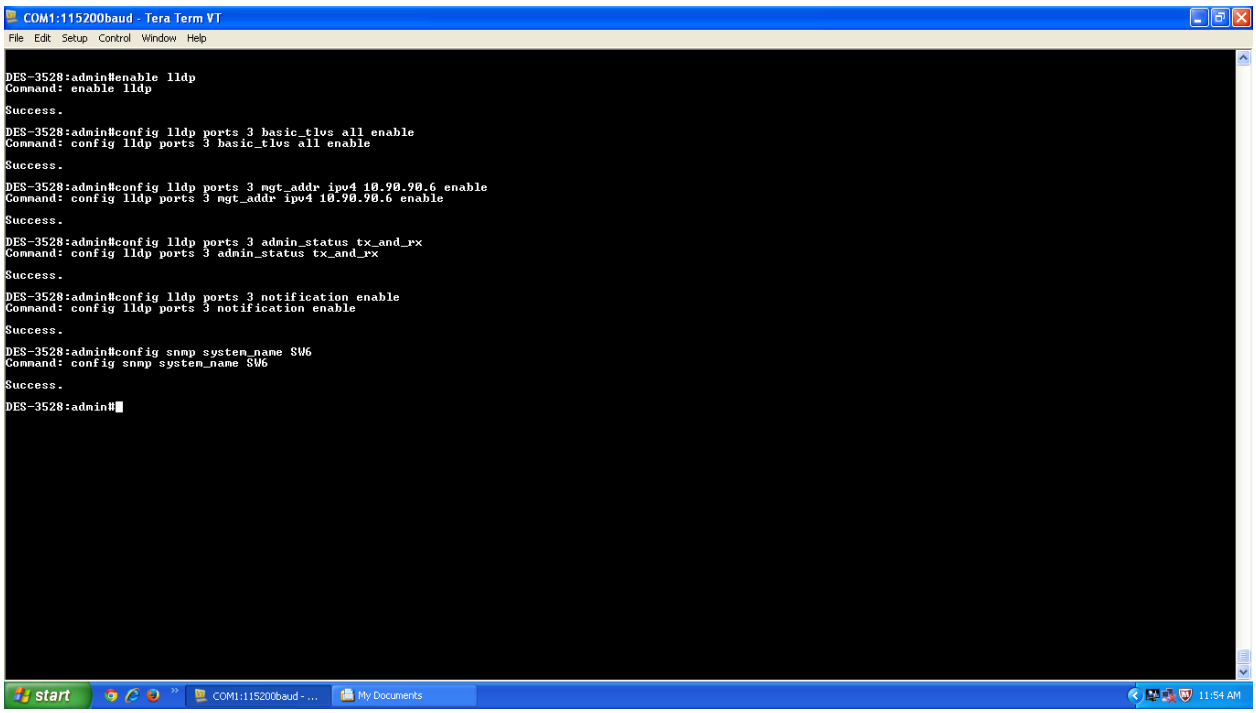


Fig. 53 : Configuring LLDP on SWx6.

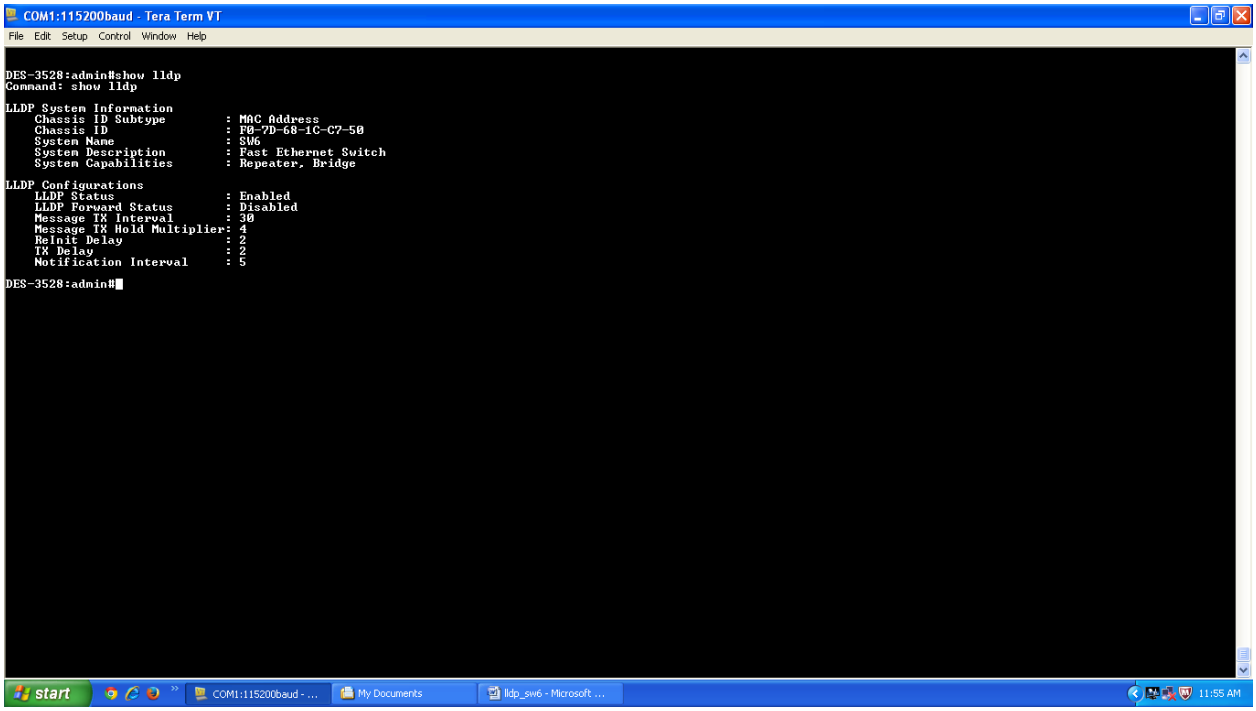


Fig. 54 : Basic LLDP configuration on SWx6.

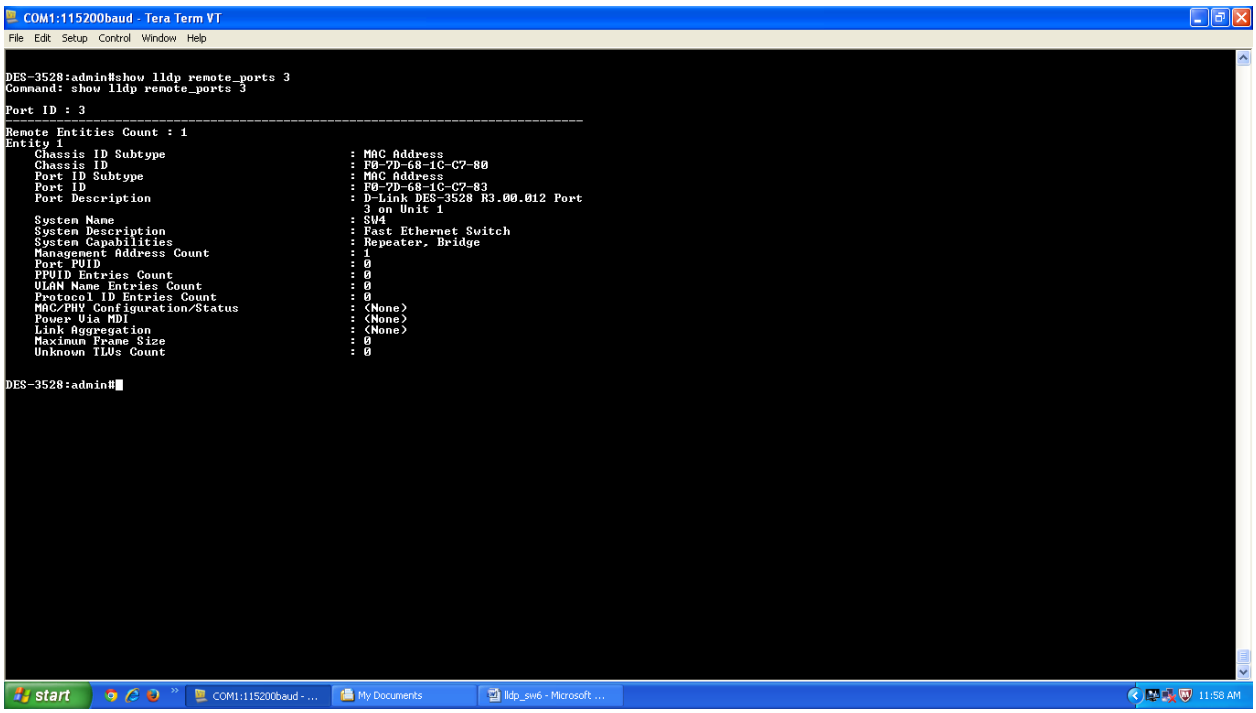


Fig. 55 : LLDP remote ports configurations on SWx6.

2.4 Switch Configuration Backup & System Maintenance

In this experiment, A TFTP server is required. We set up a TFTP server connected to SWRx1 and configure its IP address to 10.90.90.100/24. To set up a TFTP server, configure the PC's IP address to 10.90.90.100 with a subnet mask of 255.255.255.0 .

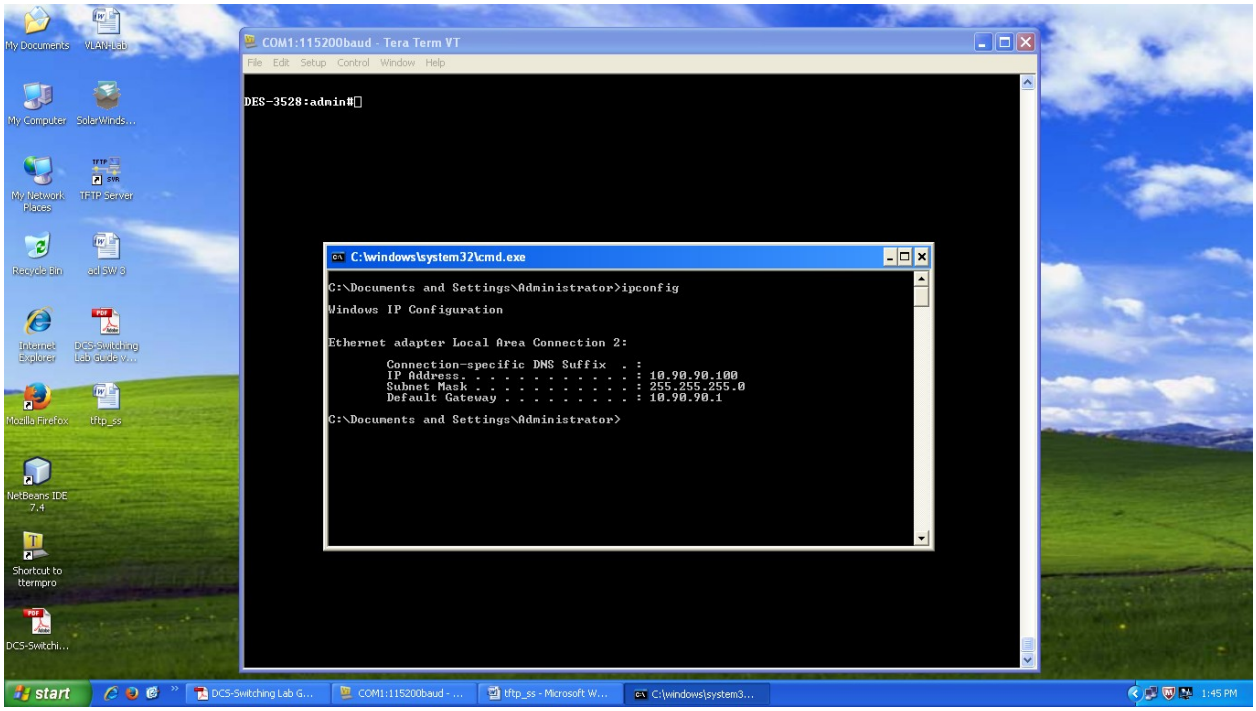


Fig. 56 : Setting up the IP address of the server to 10. 90. 90. 100/24.

Once the setup of the network configurations has been done on the PC. Its time to install the TFTP server program so that we can use it for backing up the configuration files for various switches.

There are various TFTP server programs which can be downloaded for free from the internet, SolarWinds TFTP server is one of the popular and free server. We downloaded a copy of the program and installed on to the system.

Once the server program is installed onto the system, We need to start the server and activate its working. The server listens for requests onto UDP Port 69, if any connection request arives on this port of the system, The server program would handle the request and serve the request accordingly.

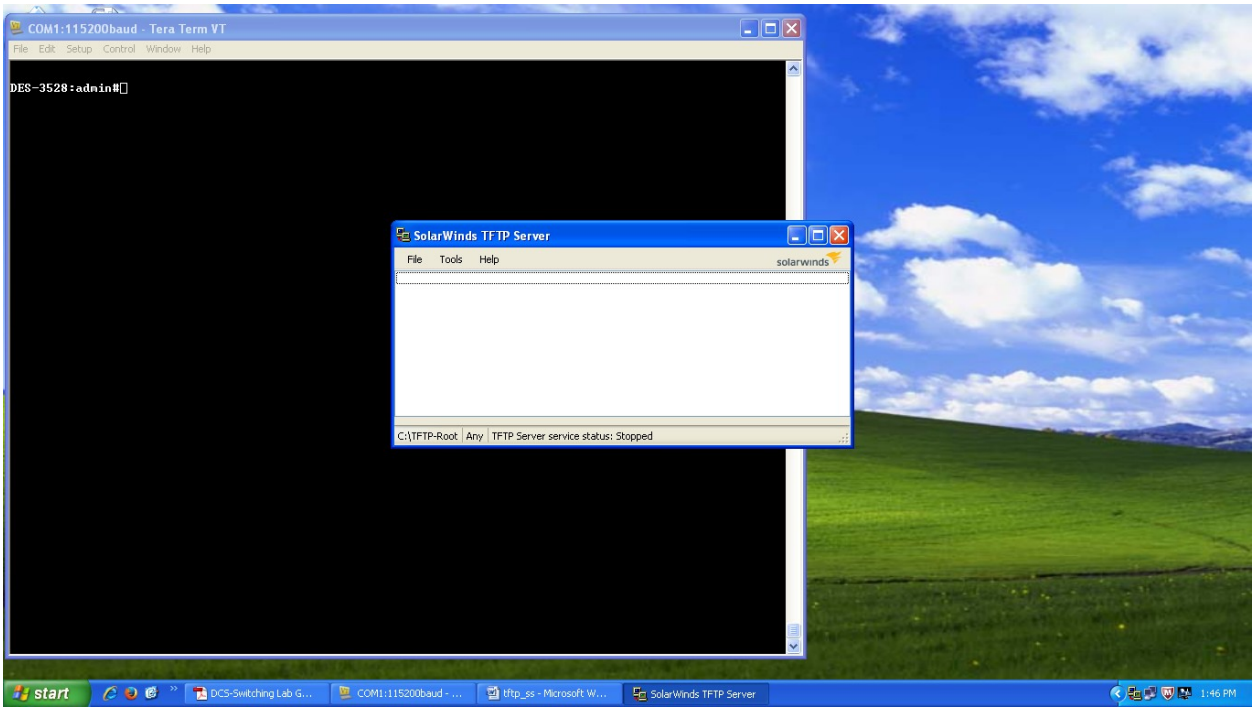


Fig. 57 : Setting up the TFTP server onto the PC.

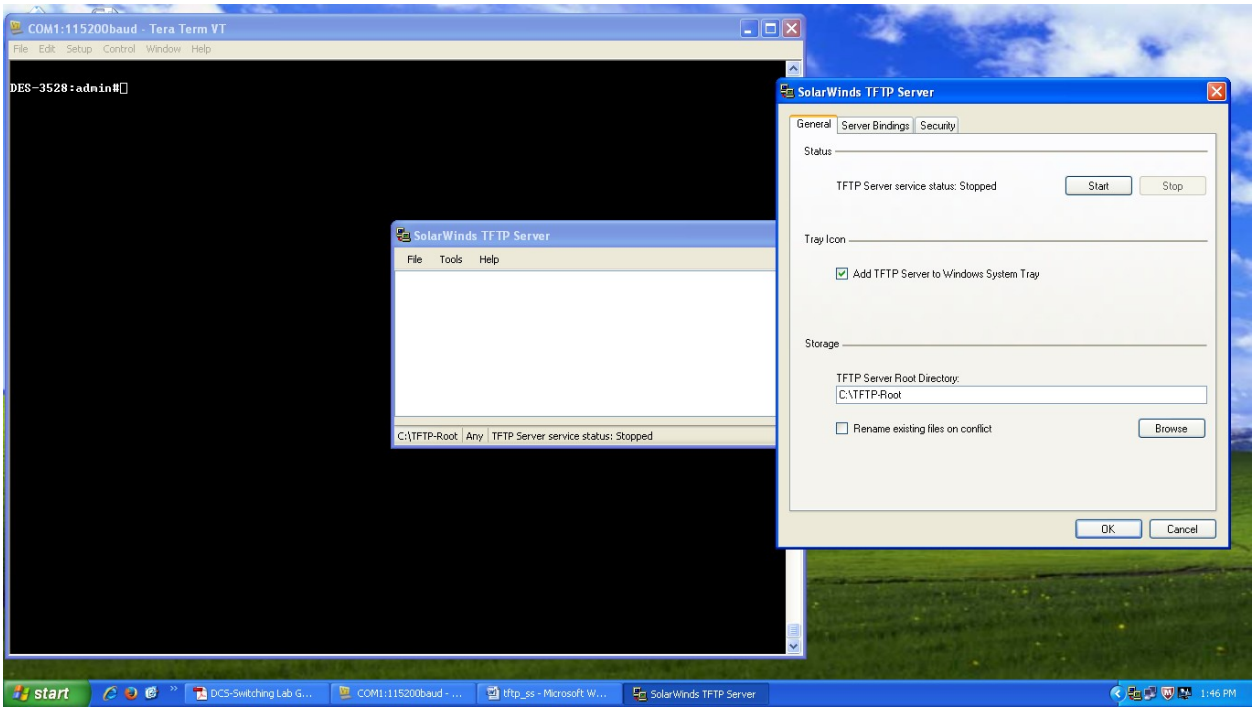


Fig. 58 : Starting up the TFTP server – Initially Stopped.

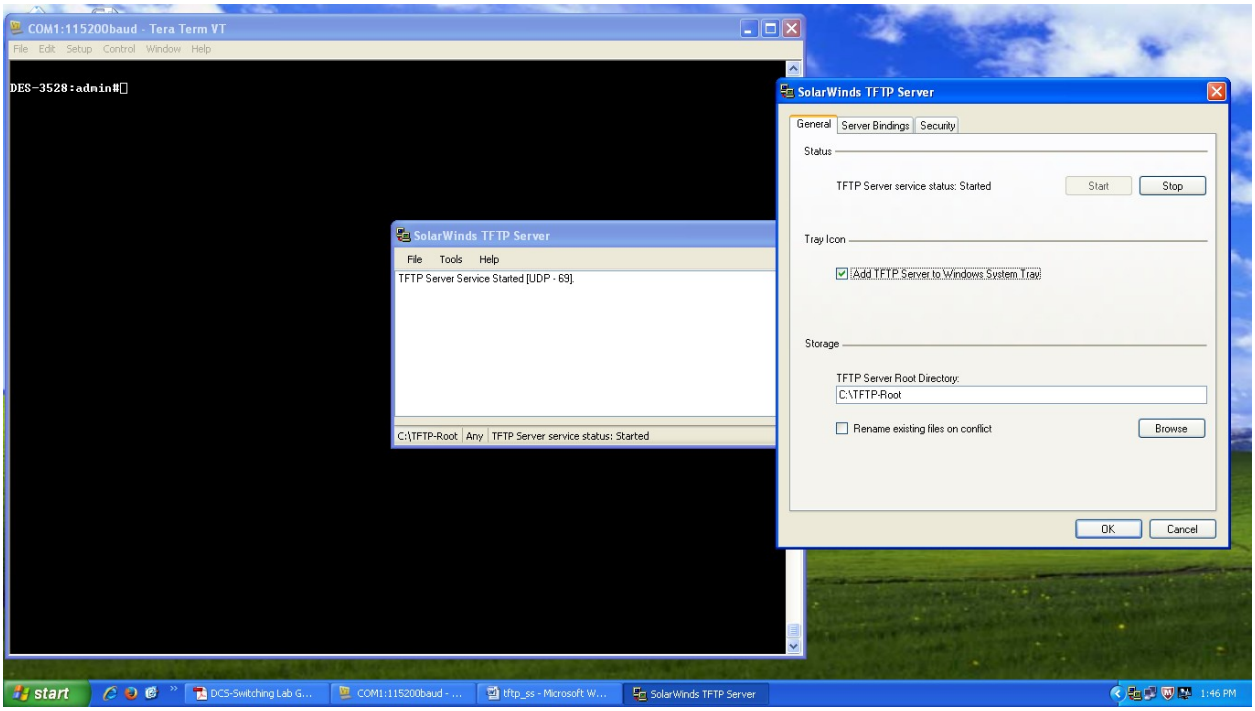


Fig. 59 : Starting up the TFTP server – Now Started.

Now, The TFTP server has been started and active on the PC with an IP address of 10.90.90.100 and a subnet mask of 255.255.255.0 . The server is now ready for all the uploads of configuration files from various switches.

All network managers should make it their practice to back up each switch's configuration file to the TFTP server. On all switches, Backup command should be run ***upload cfg_toTFTP 10.90.90.100 dest_file <switchname.cfg>***.

2.4.1 Configuration Backup for SWRx1

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SWR1.cfg

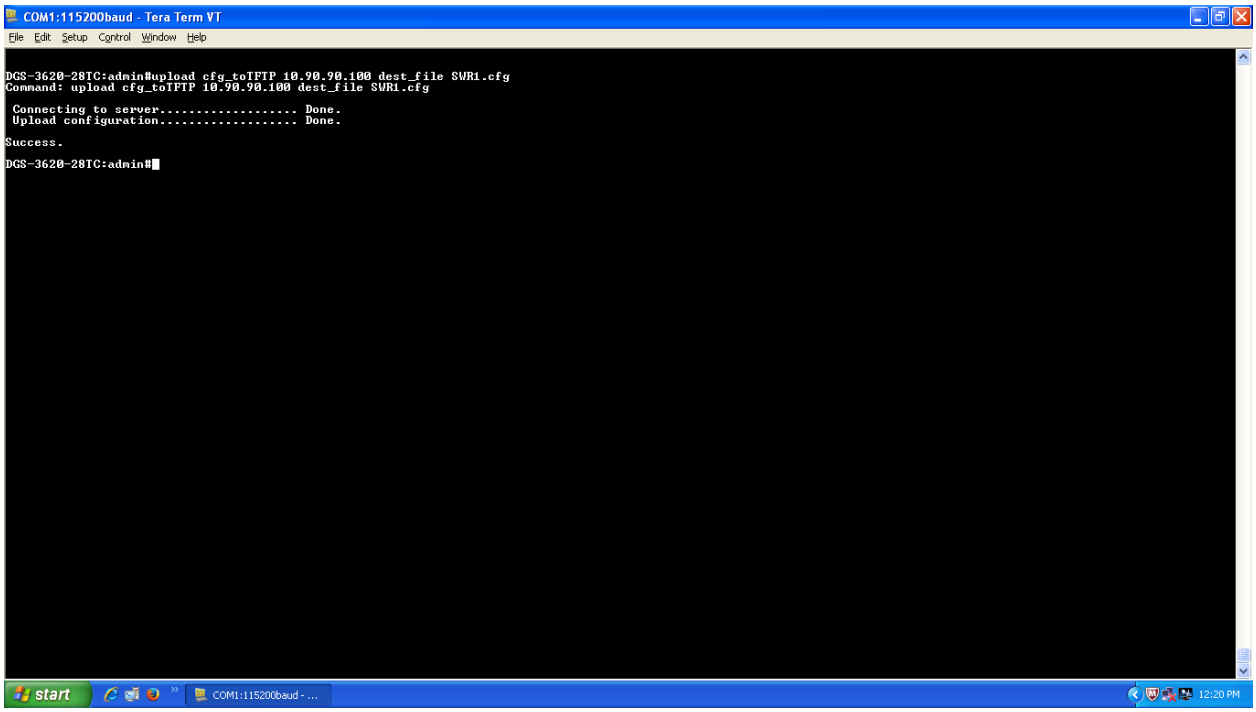


Fig. 60 : Uploading configuration for SWR1.

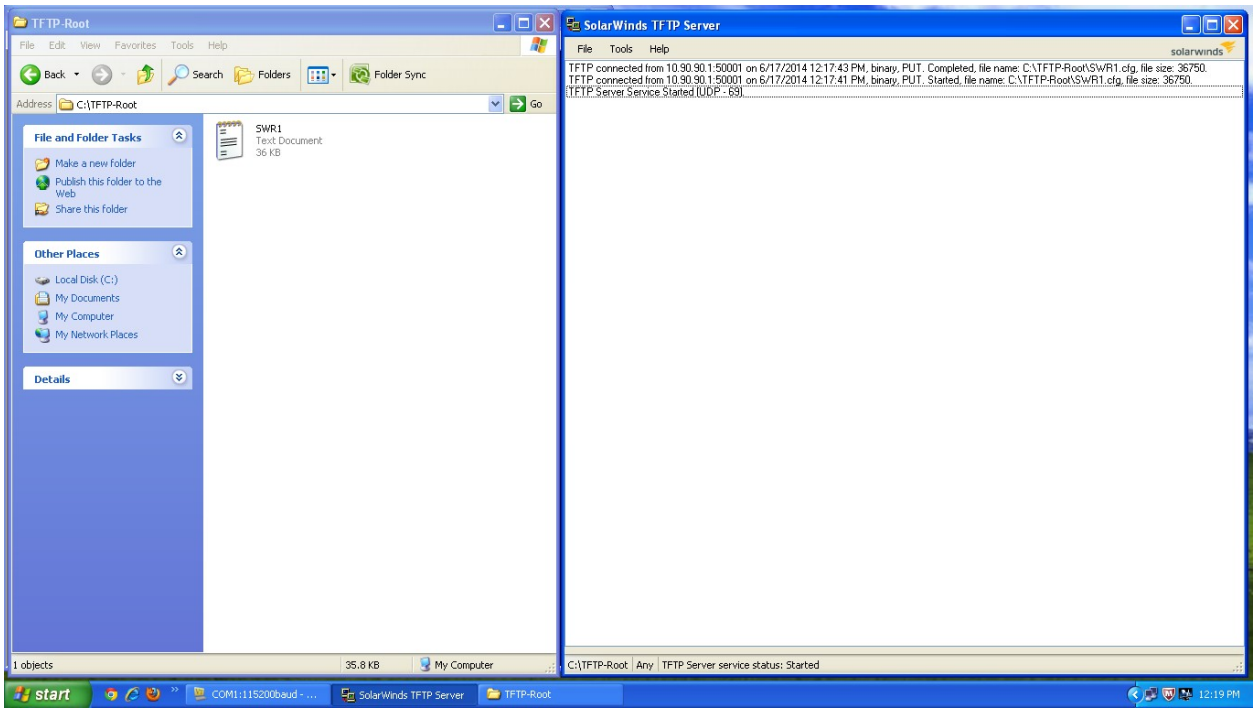


Fig. 61 : On TFTP server – SWR1.cfg holds configurations for SWR1.

2.4.2 Configuration Backup and Updating firmware for SWRx2

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SWR2.cfg

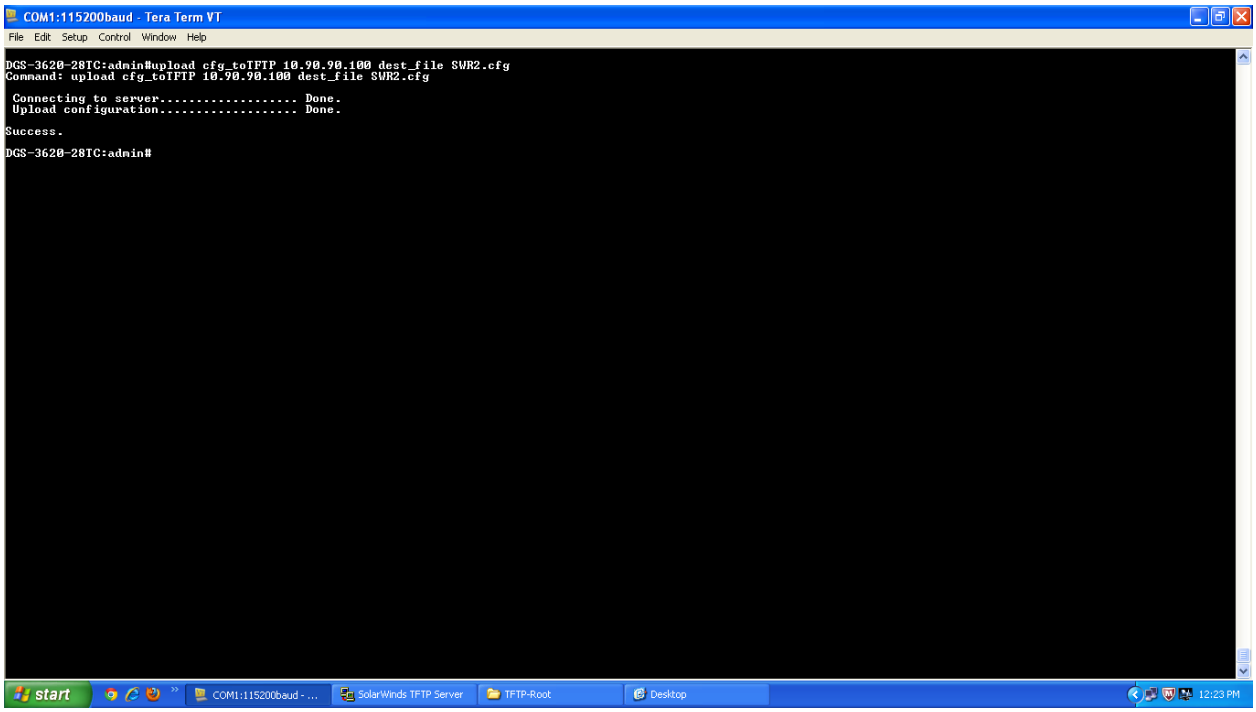


Fig. 62 : Uploading configuration for SWR2.

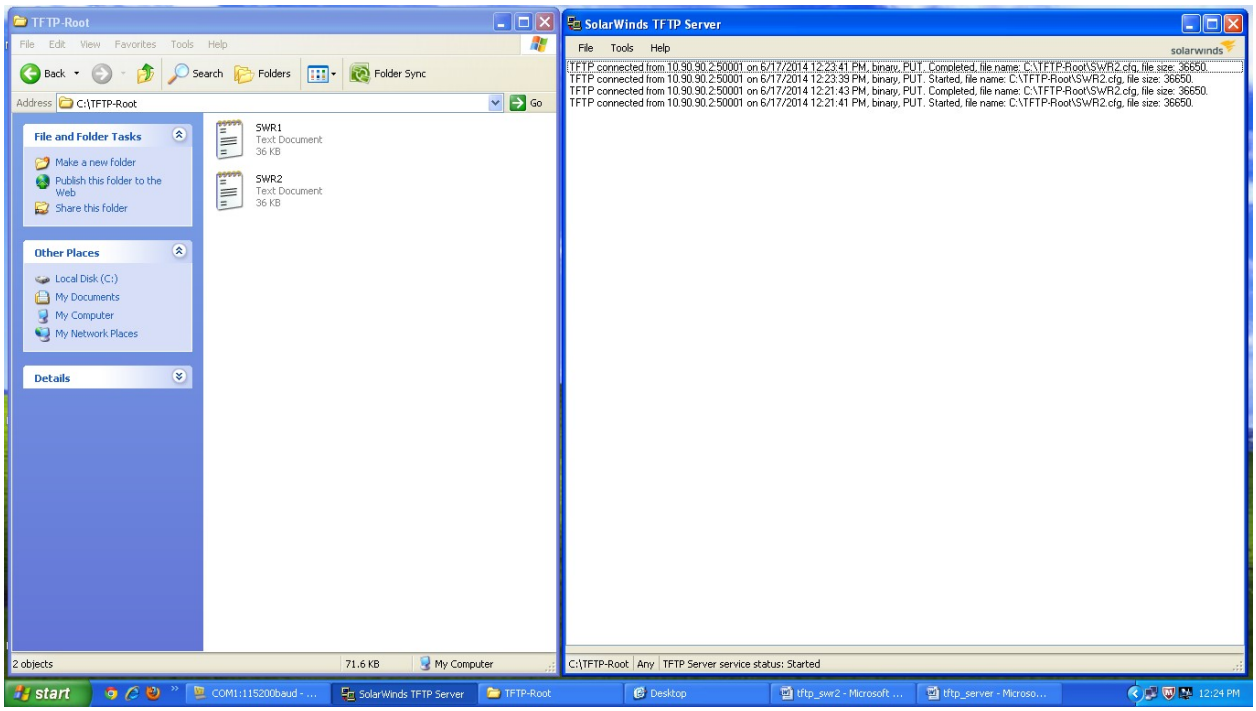


Fig. 63 : On TFTP server – SWR2.cfg holds configurations for SWR2.

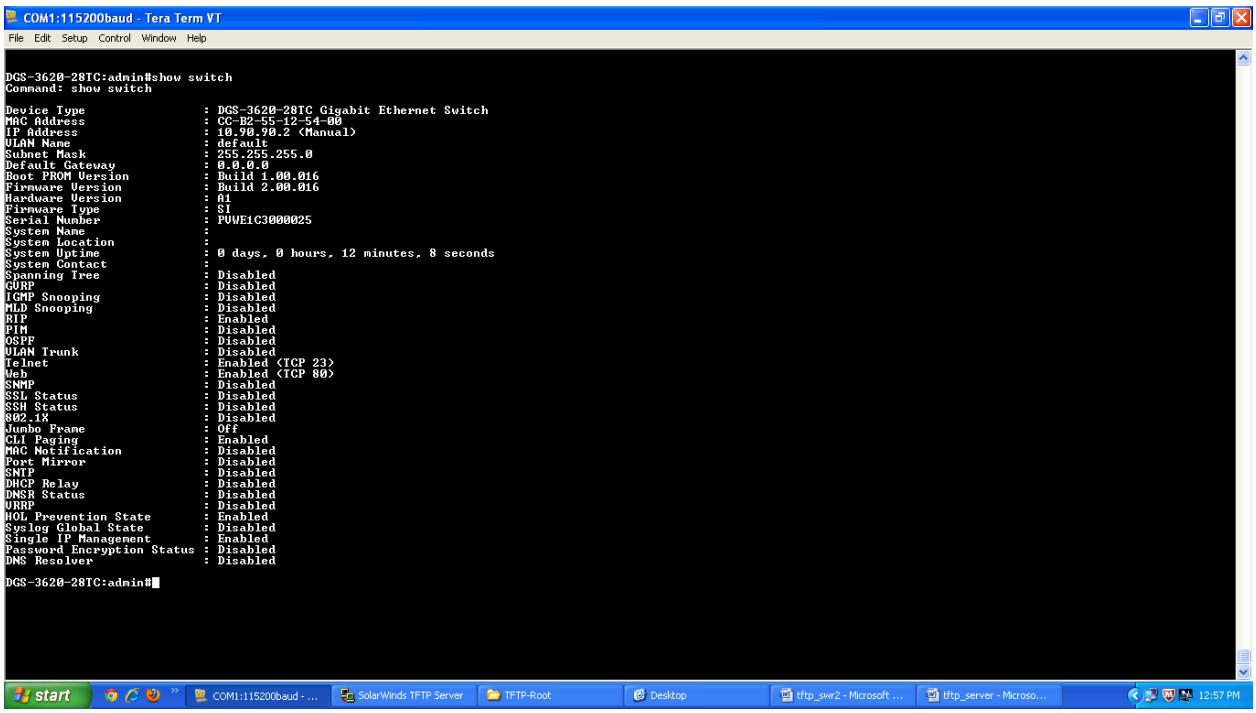


Fig. 64 : Switch firmware details before Updation.

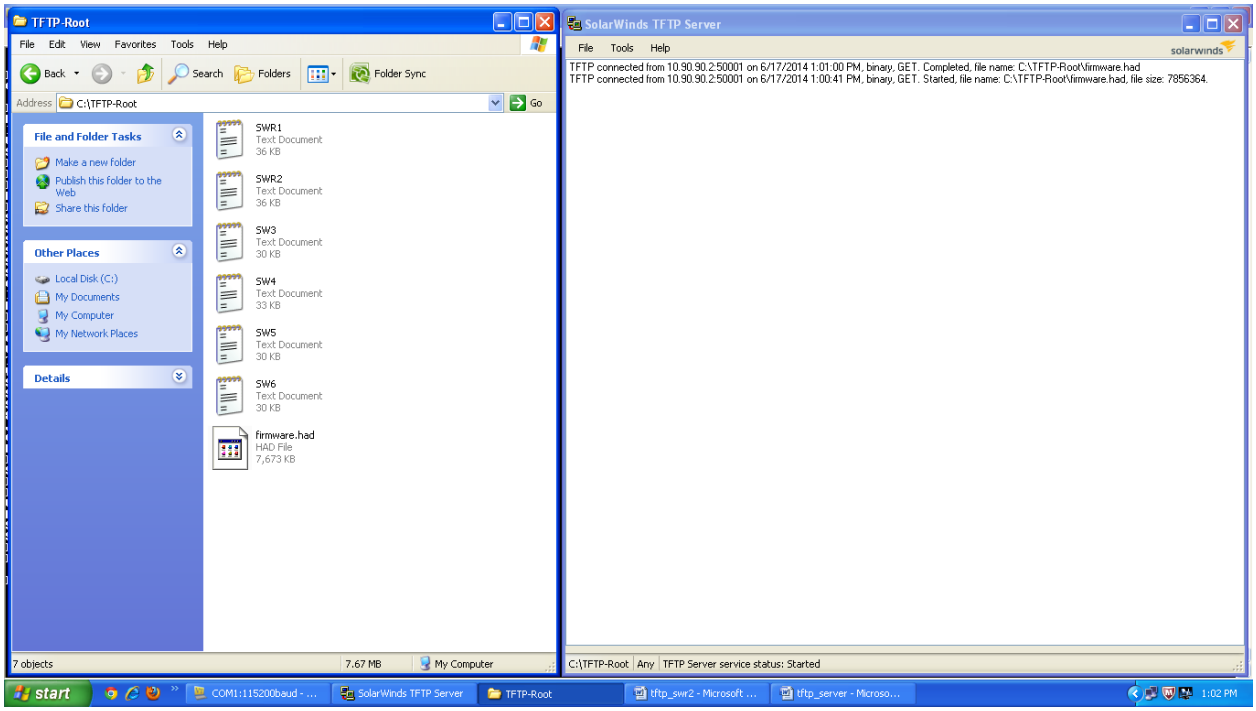


Fig. 65(a) : Updating firmware requires firmware file to be present on the server.

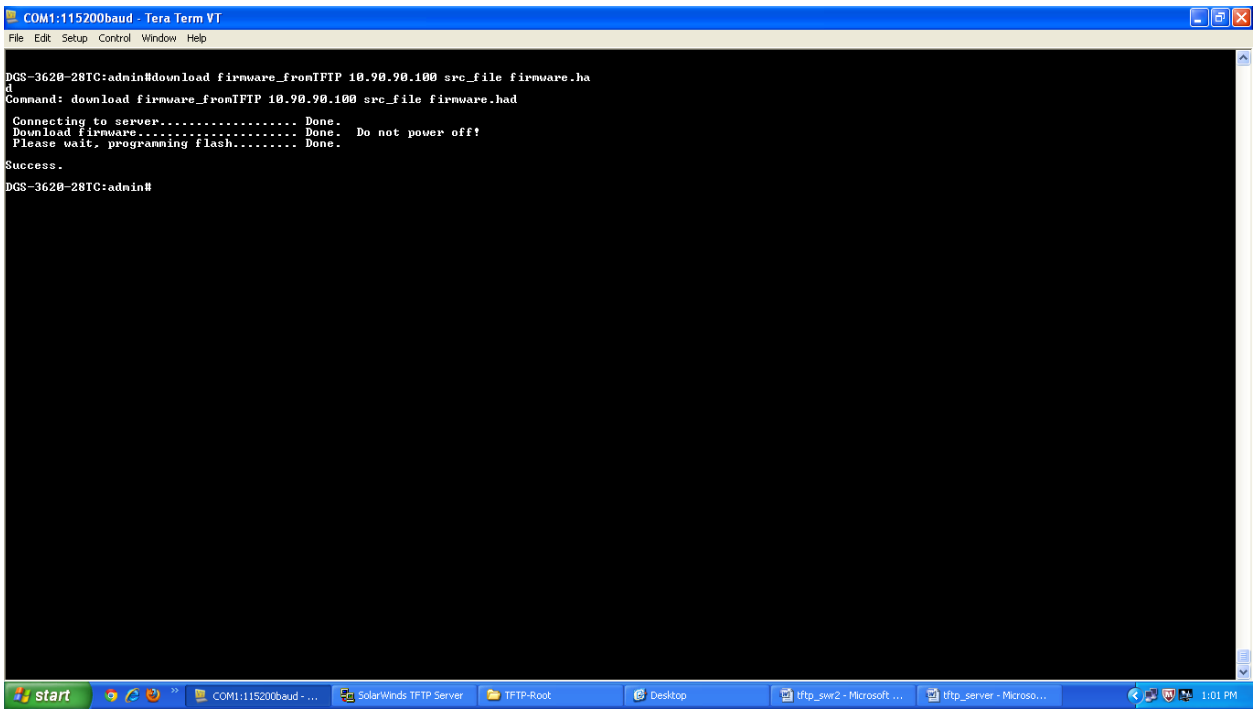


Fig. 65(b) : Updation Procedure on SWR2.

2.4.3 Configuration Backup for SWx3

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SW3.cfg

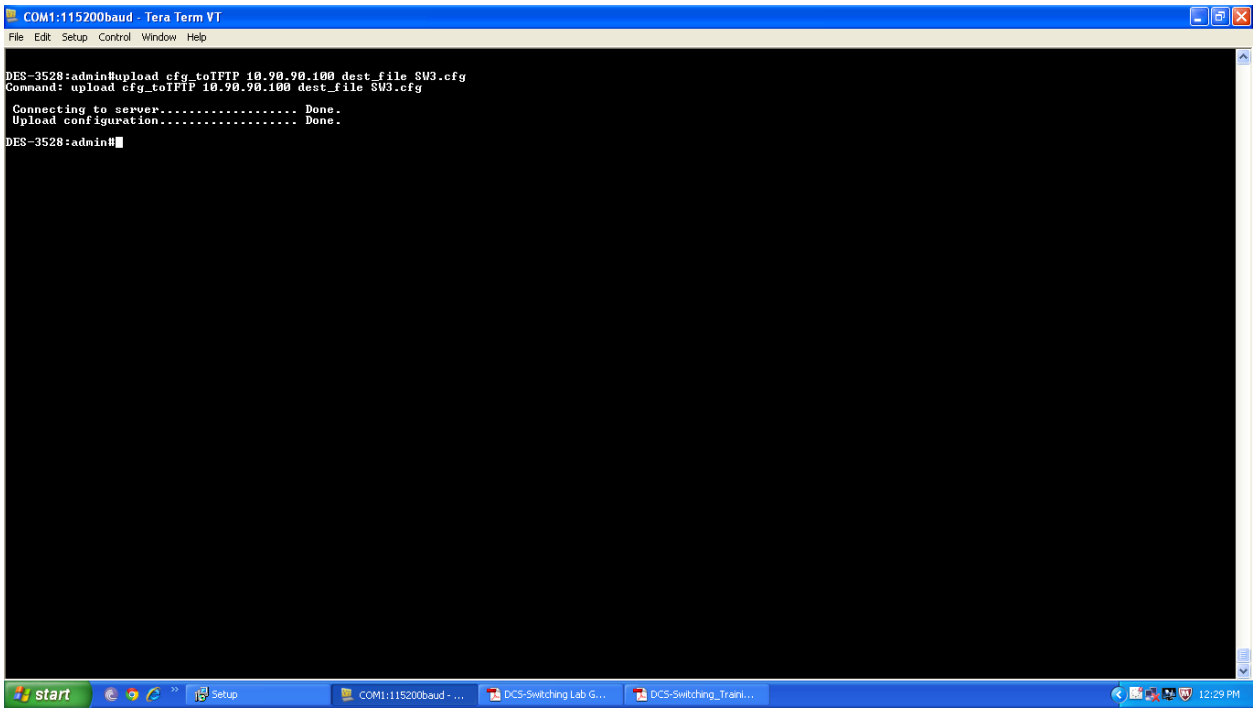


Fig. 66 : Uploading configuration for SW3.

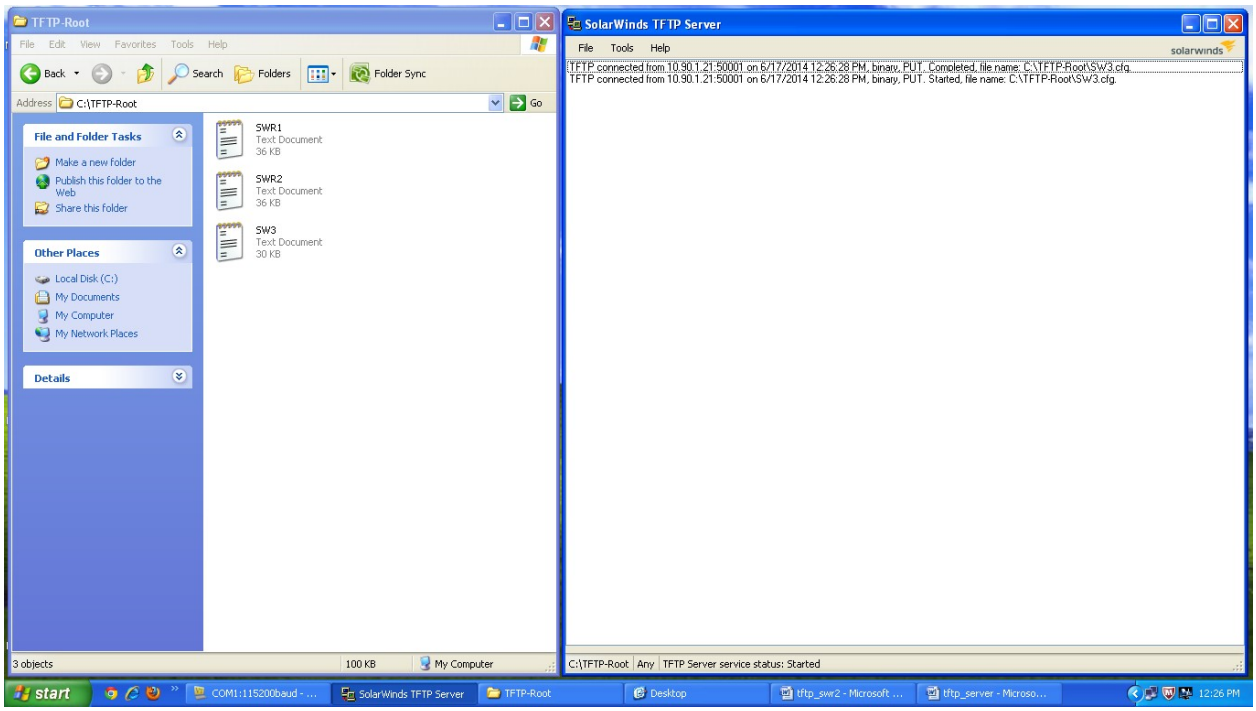


Fig. 67 : On TFTP server – SW3.cfg holds configurations for SW3.

2.4.4 Configuration Backup for SWx4

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SW4.cfg

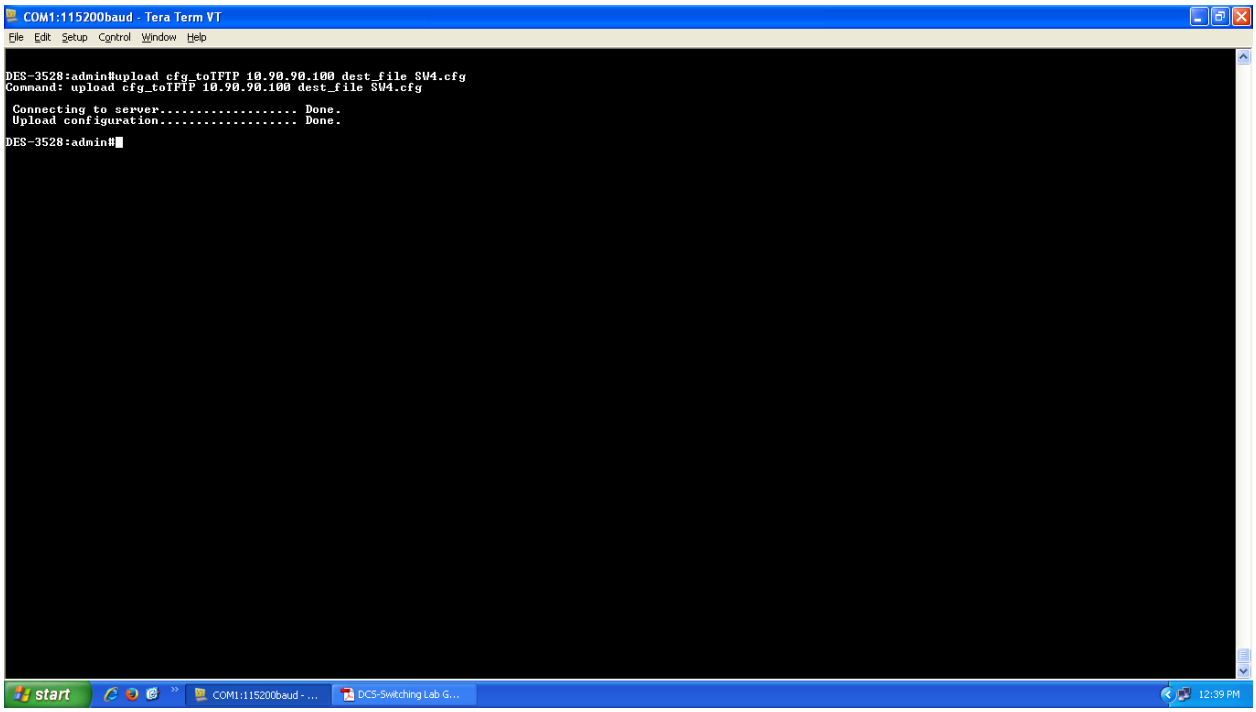


Fig. 68 : Uploading configuration for SW4.

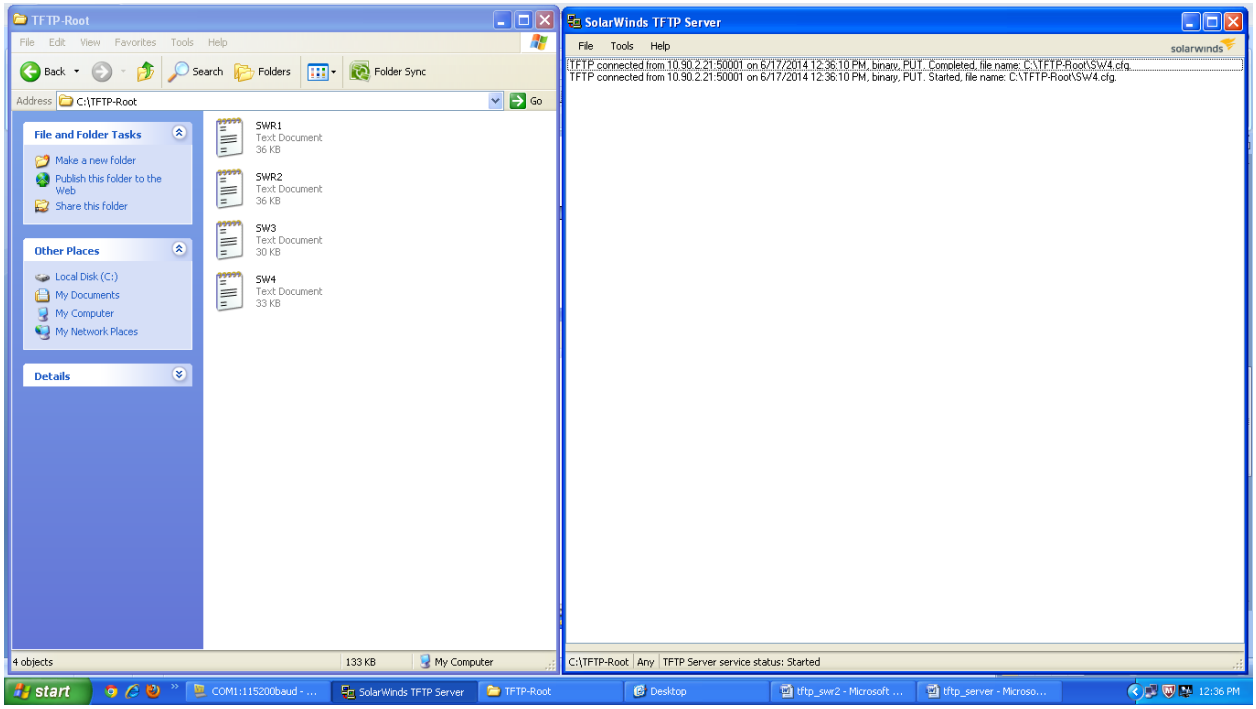


Fig. 69 : On TFTP server – SW4.cfg holds configurations for SW4.

2.4.5 Configuration Backup for SWx5

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SW5.cfg

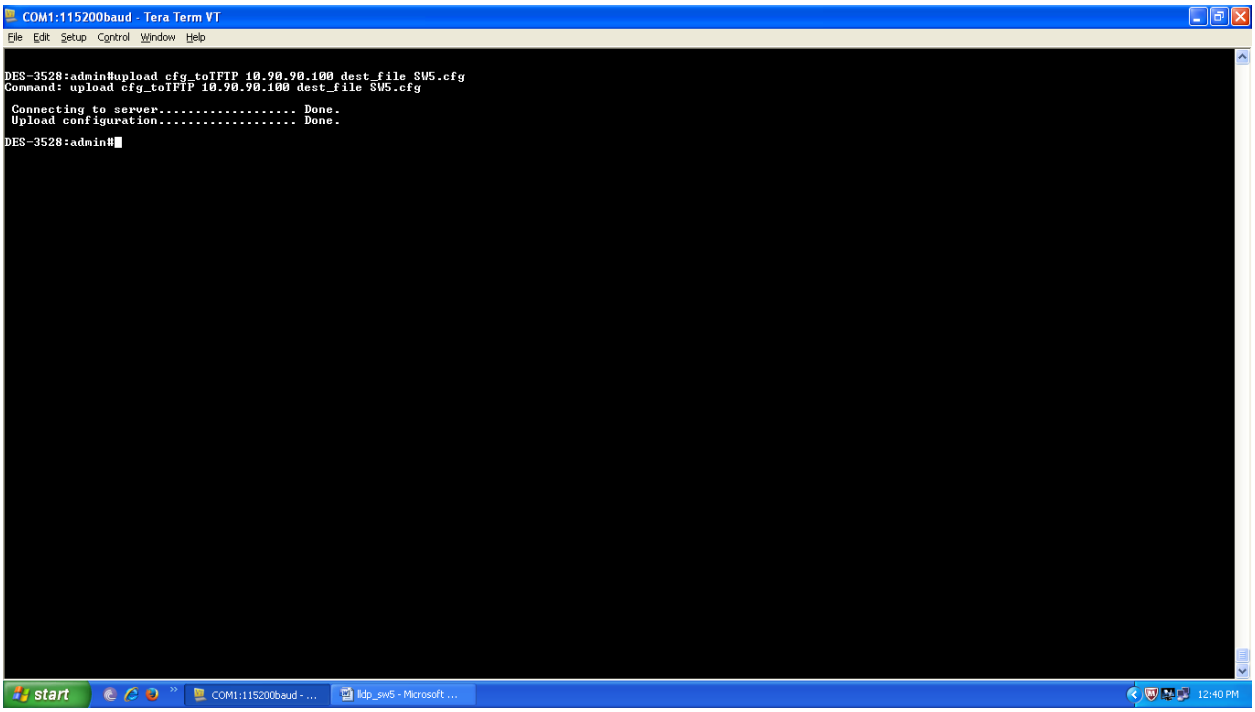


Fig. 70 : Uploading configuration for SW5.

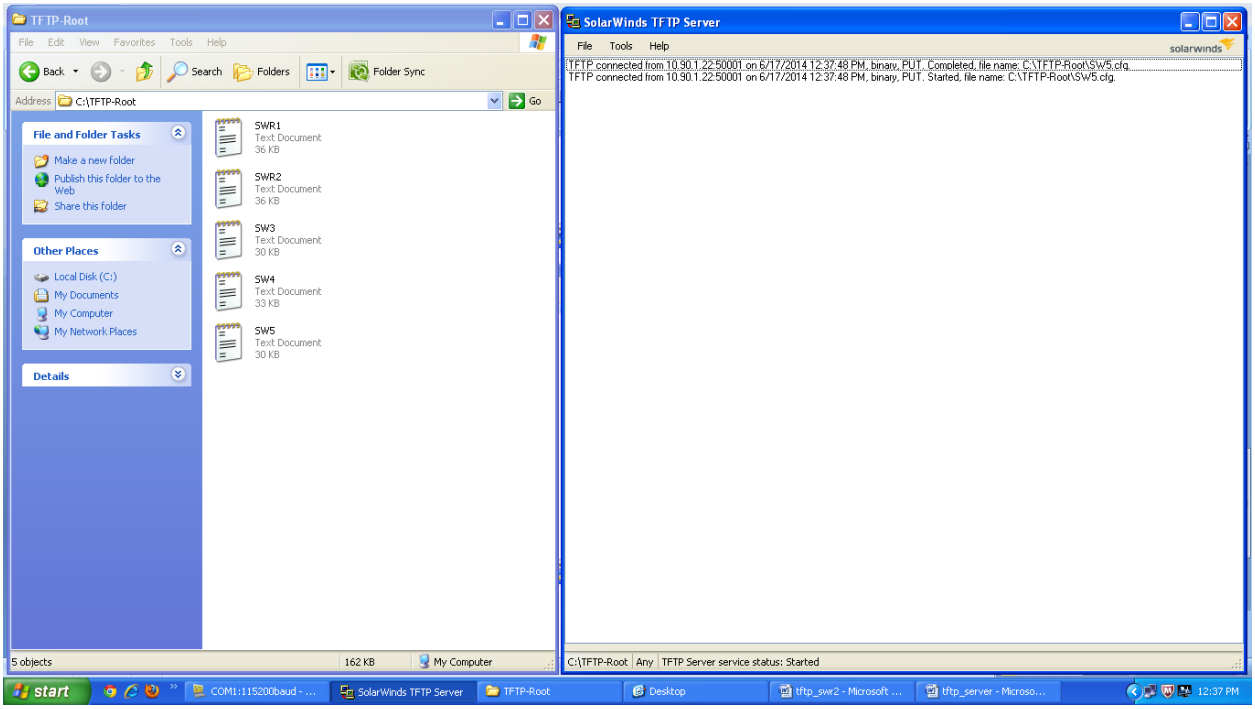


Fig. 71 : On TFTP server – SW5.cfg holds configurations for SW5.

2.4.6 Configuration Backup for SWx6

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SW6.cfg

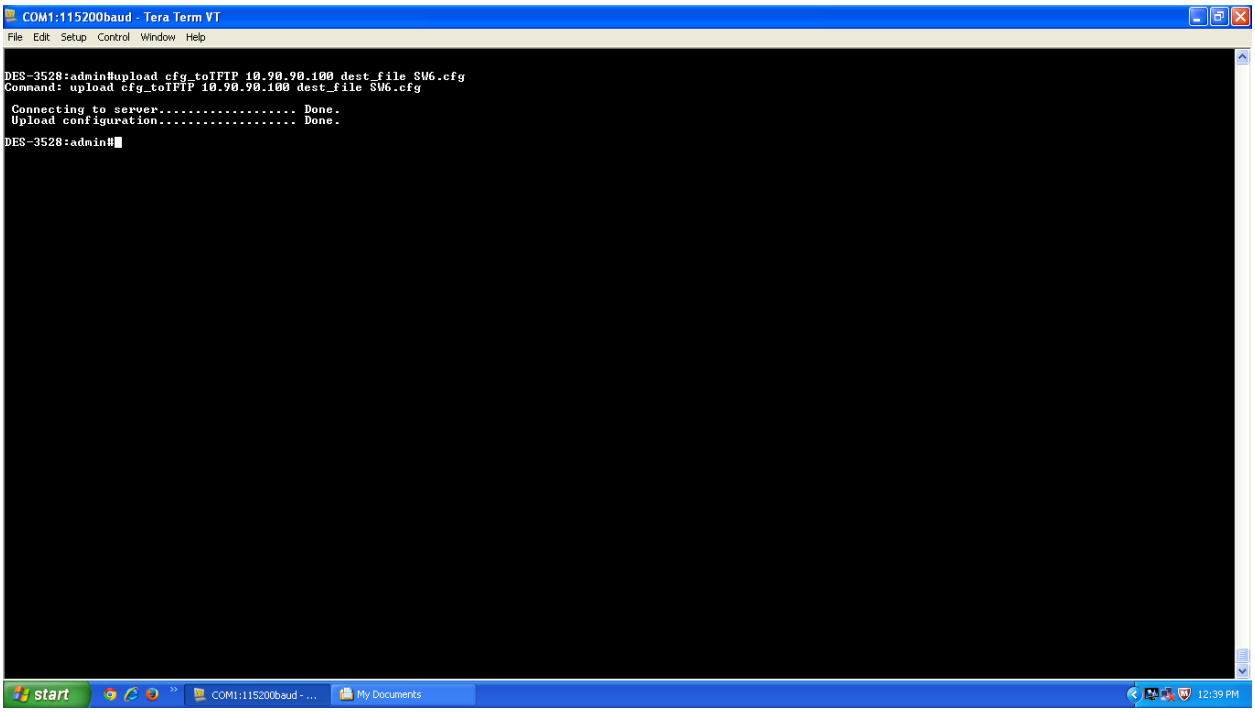


Fig. 72 : Uploading configuration for SW6.

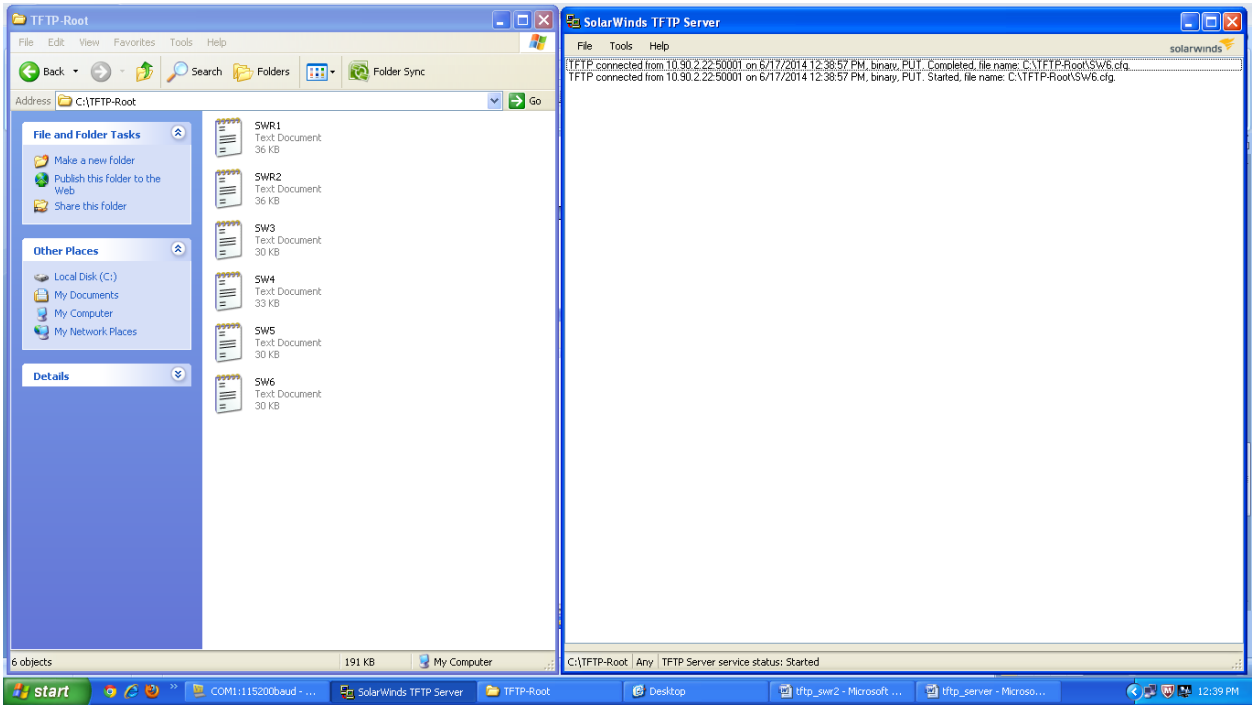


Fig. 73 : On TFTP server – SW6.cfg holds configurations for SW6.

CHAPTER 3. RESULTS & DISCUSSION.

We have conducted various experiments on the “Dynamic Host Configuration Protocol (DHCP) & Link Layer Discovery Protocol (LLDP)” during the course of this internship. In the course of our internship, We discussed how DHCP & LLDP work under-the-hood.

For display of our results, We have used a packet sniffer program called Wireshark. The program captures packets from a perticular network interface and displays them in a user friendly, color coded manner.

3.1 Results of DHCP experiments

From our experiments conducted with DHCP, We came to the understanding of the workings of the protocol. It is a protocol utilising client-server model, the DHCP client broadcasts a Discovery message onto the media which generates response in form of a DHCP Offer from the DHCP server. Once the Client recieves the Offer message, It generates a DHCP Request message and broadcasts it onto the media. The DHCP server recieves the Request message from the client and sends an Acknowledgement message. Thus, Concluding the DHCP assignment procedure.

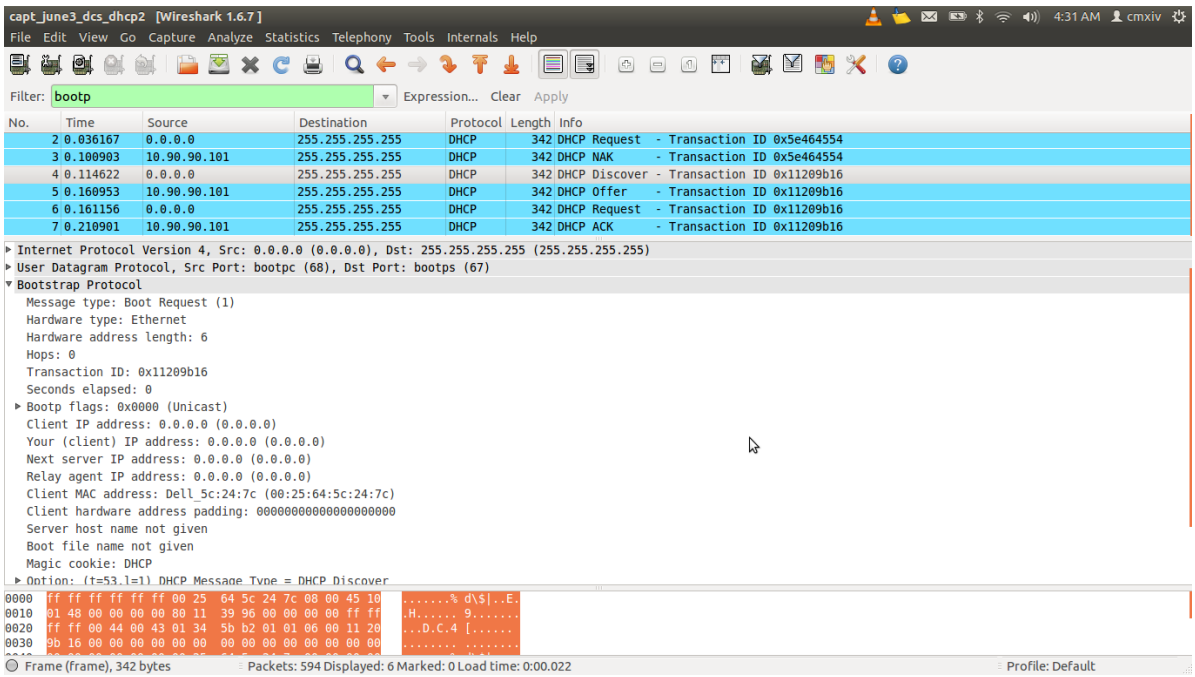


Fig. 74 (a) : DHCP Discover message.

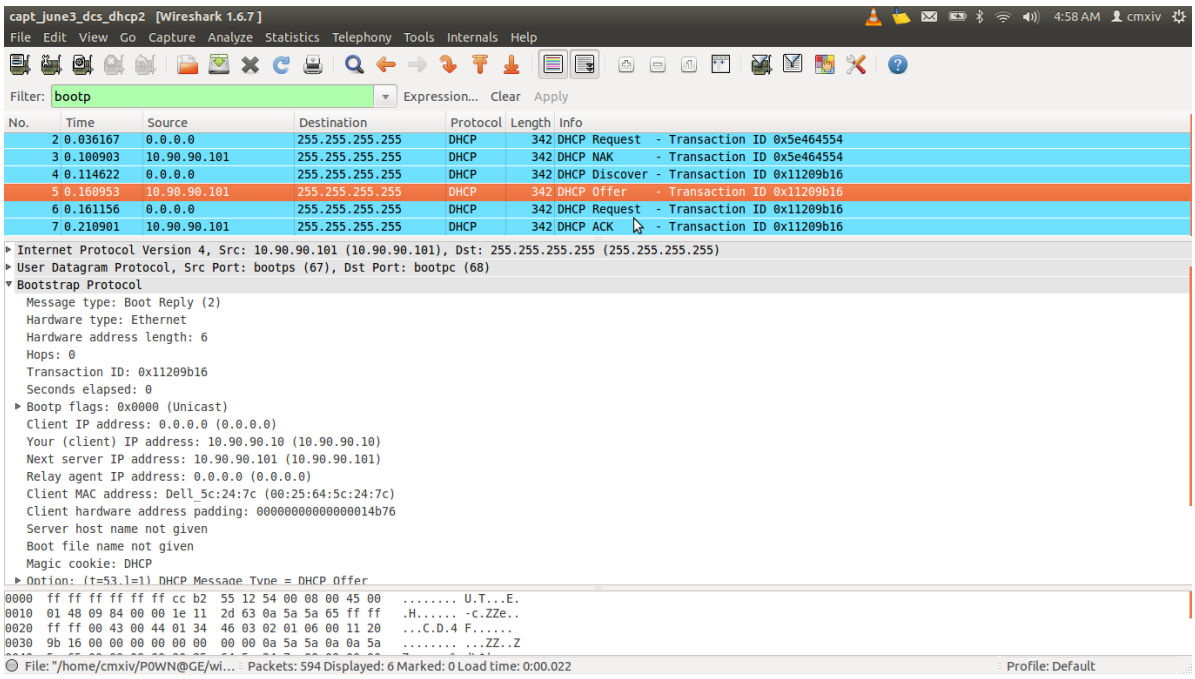


Fig. 74 (b) : DHCP Offer message.

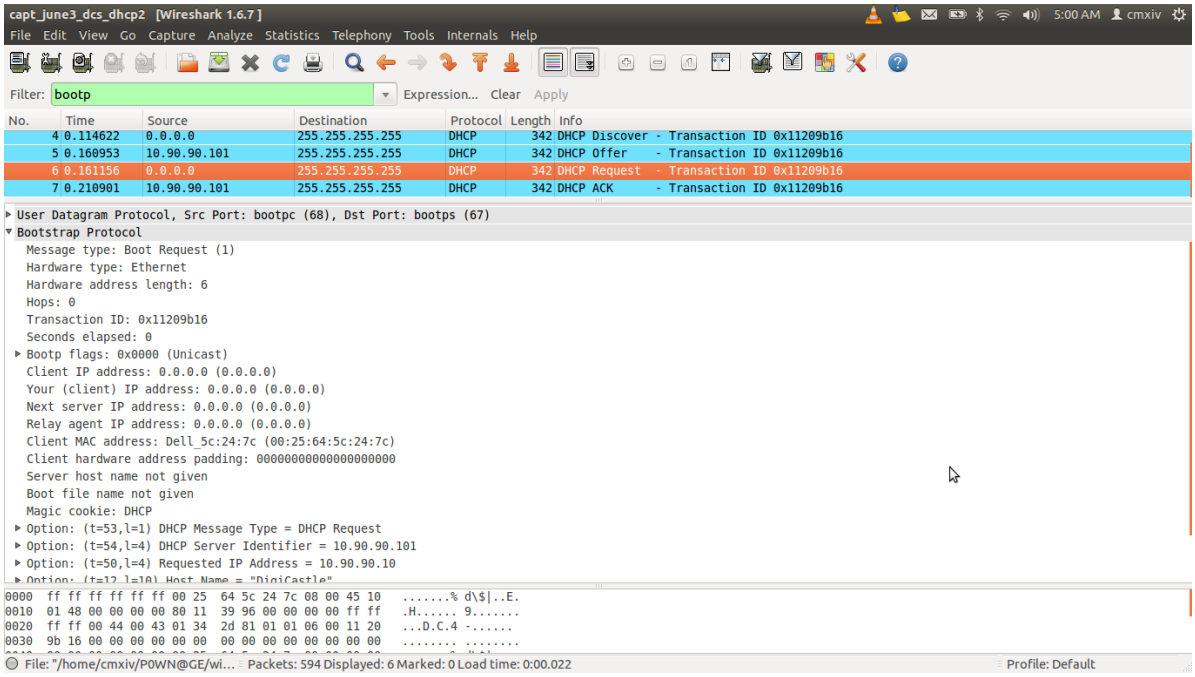


Fig. 74 (c) : DHCP Request message.

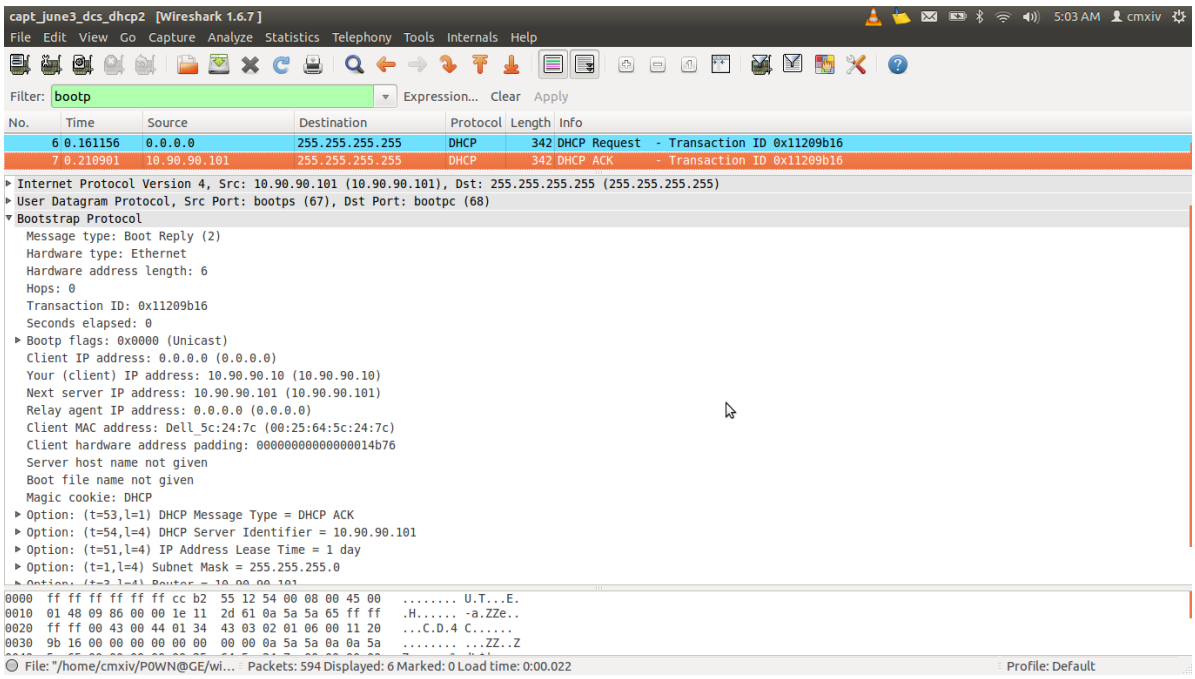


Fig. 74 (d) : DHCP Request message.

3.2 Results of LLDP experiments

From our experiments conducted with LLDP, We came to the understanding of the workings of the protocol. The "Link Layer Discovery Protocol (LLDP)" is a medium independent protocol for IEEE 802 devices. It allows discovery of capabilities of its peers.

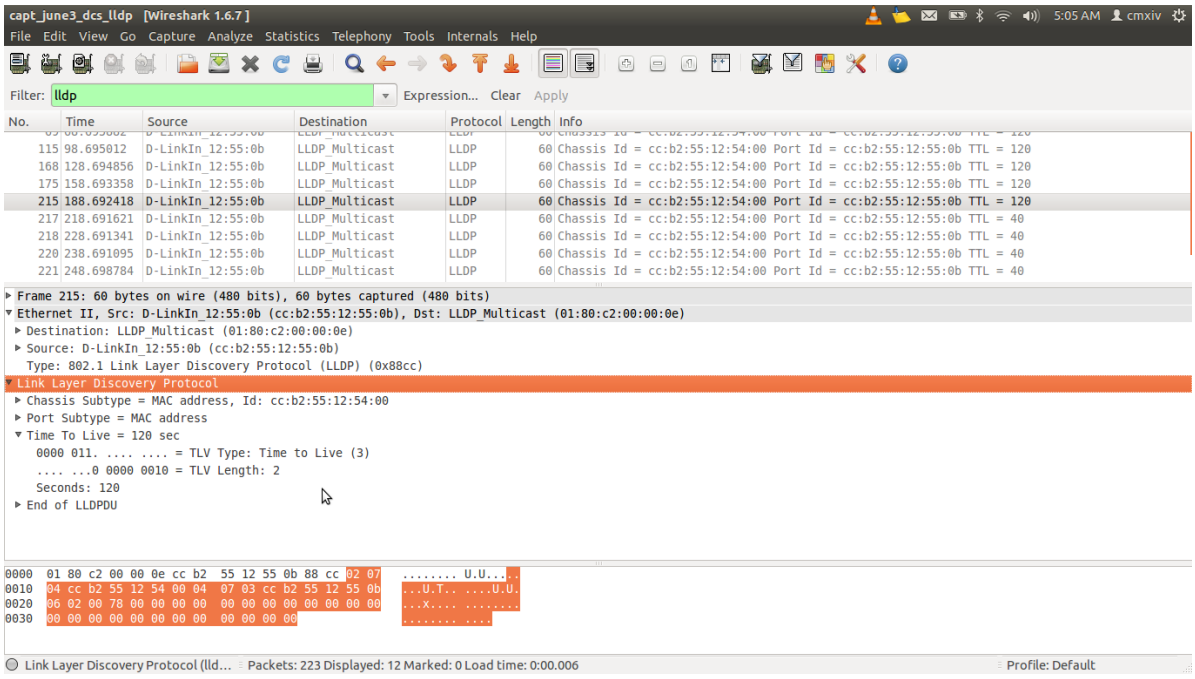


Fig. 75 : LLDP packet with TLV – Time to live = 120.

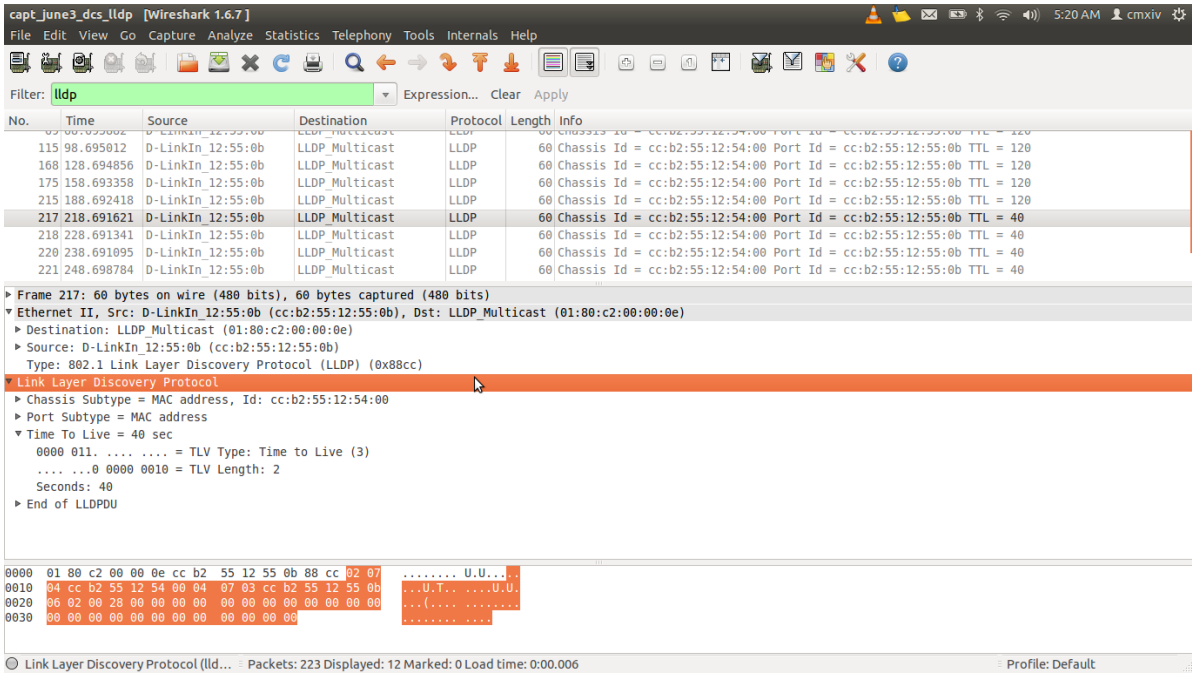


Fig. 76 : LLDP packet with TLV – Time to live = 40.

CHAPTER 4. CONCLUSIONS.

With these experiments that we have conducted in the course of our internship, We came to certain conclusions.

1. DHCP is a client-server model based protocol. It has successfully replaced ARP or BOOTP for distribution of network configuration.
2. Each DHCP server can be configured to work on certain set of IP addresses.
3. Generally, Each subnet has its own DHCP server but if they are not present on every subnet, DHCP Relay agents can be used to relay the DHCP messages between the Clients and the servers.
4. In the experiments, SWRx1 & SWRx2 serves as DHCP servers. SWx3 & SWx4 served as DHCP Relay agents for SWx5 & SWx6.
5. We were able to assign all the clients attached to the switches IP addresses from the two IP address pools on SWRx1 & SWRx2.
6. LLDP is a medium independent protocol which allows capability discovery of other devices in the network.
7. LLDP TLVs can be programmed onto the switches and can be used to share the capabilities of other devices.
8. In the experiment with LLDP, We have successfully changed the time to live (TTL) from 120 seconds to 40 seconds.

CHAPTER 5. IMPLICATIONS FOR FUTURE RESEARCH.

DHCP has been the standard for IPv4 network configuration however with the introduction of IPv6, DHCP has to be updated to DHCPv6 and implemented on the devices yet to come in the future.

DHCPv6 is further being developed to make available configurations to clients that have been using “Stateless Address AutoConfiguration (SLAAC)”. As specified in RFC 4862, The SLAAC is performed as a component of the Neighbour Discovery Protocol (NDP).

“Link Layer Discovery Protocol (LLDP)” can simplify the operation of troubleshooting of networks and increase the capability of network management tools to manage, monitor and maintain accurate network topologies in a network setup which have devices from various manufacturers. It would be used in the future generations of the network devices to effectively manage and monitor the devices.

REFERENCES

[1] D-Link Academy Publication - DCS Switching guide & manual.

[2] D-Link Academy Publication - DCS Switching Lab manual.

[3] Wikipedia Article – Dynamic Host Configuration Protocol (DHCP).
(http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)

[4] Wikipedia Article – Link Layer Discovery Protocol (LLDP).
(http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol)

[5] Wikipedia Article – Dynamic Host Configuration Protocol version 6 (DHCPv6).
(http://en.wikipedia.org/wiki/DHCPv6)

[6] Wikipedia Article – Link-Local Address (StateLess Address AutoConfiguration)
(http://en.wikipedia.org/wiki/Stateless_address_autoconfiguration)

[7] Cisco Press Article – Mastering IPv6 SLAAC Concepts and Configuration.
(http://www.ciscopress.com/articles/article.asp?p=2154680)

APPENDIX

Siddhant_Tandon_Section_3

by

FILE	SIDDHANT_TANDON_SECTION_3.DOCX (32.83K)		
TIME SUBMITTED	08-JUL-2014 11:27AM	WORD COUNT	5193
SUBMISSION ID	438458897	CHARACTER COUNT	25886

CHAPTER 1. INTRODUCTION.

D-Link managed switches (Layer 2 and Layer 3 switches) have capabilities to create smart networks. A Network can be termed as smart if it is capable of utilising its available resources to its full extent. Network resources can be available IP addresses and/or compute systems with certain capabilities. These switches maintains configuration files for their services and preferences which can be uploaded or downloaded from and to the switch thus providing backup facilities which is a very important operation on these switches.

"Dynamic Host Configuration Protocol or DHCP" is an IEEE standard network protocol used for dynamic assignment of network configuration parameters which inclused IP addresses, Subnet mask, etc. . With DHCP providing the network configuration automatically to the clients that are introduced into the network, involvement of a network administrator is reduced to a minimum. DHCP helps to efficiently utilise the IP address pool available for a local area network thus increasing the life time of IPv4 addressing space by dynamic allocation & reusability of same network address.

The "Link Layer Discovery Protocol or LLDP" is a data link layer protocol that can be utilised by stations over a specified LAN to publicise their identity and services and to recieve the same data from other data link layer peers. LLDP is a formal protcol defined as an IEEE 802.1AB standard. The standard was designed keeping in mind, open and extendable model of the protocol. The draft of this standard was created considering the basic concepts from various protocols like Cisco's CDP or Cisco Discovery Protocol, EDP or Extreme Discovery Protocol and others.

Switch Configuration Backup is a process in which the cofiguration files of the switch are saved on a remote location so as if something went wrong to the switch may it be a system crash or any other reason for failure, the switch can be restored to its previous working condition with its previous set of configurations. Every switch has some kind of software which maintains its workings and is responsible for every operation that has to be carried out by the switch, it is called a firmware. This software can be updated in the switch as the

vendor, D-Link, keeps on releasing new firmware, a new copy of firmware can be downloaded from the vendor's website and then, using TFTP or RCP, installed on the switch. This updation procedure doesn't alter the configurations of the switch but it is advised that the administrator should take a backup of the switch's configurations as if something goes wrong.

1.1 "Dynamic Host Control Protocol (DHCP)"

The "Dynamic Host Configuration Protocol (DHCP)" is used by compute systems over a network to request network configurations like IP address, subnet masks, etc from a DHCP server of the network on which the compute system is a part of. DHCP is a protocol that employs Client-Server model. A newly arriving host is termed as a Client which requires network configurations which includs an IP address & subnet mask for itself. The simplest scenario for a network with DHCP servers is that there is a DHCP server for every subnet existing on the network.

Fig. : A typical DHCP session

DHCP uses a connectionless model utilising User Datagram Protocol (UDP). Two UDP ports are used for the protocol to operate and since DHCP succeeds BOOTP, they share the same ports. DHCP servers utilises port 67 which is the destination port address for a request, DHCP clients utilises port 68 which is the destination port address of the response from the DHCP server.

Operation of DHCP starts with the broadcast of Request message from client. Clients could request a lease renewal for the existing address directly via UDP unicast as client is alreasy having an IP address associated to itself.

Before we begin the discussion about DHCP phases, First let us take a look at the basic protocol structure of DHCP. DHCP borrows its packet structure from BOOTP, the packet fields are similar but holds different meaning to them when used in DHCP. A DHCP packet has 14 fields in it, They are as follows :

1. *Operation Code* (Field Name : OP; Size : 1Byte) : This field tells the type of message the packet holds. Op = 1 represents Request message from client, whereas

Op = 2 is Reply message from server.

2. *Hardware Type* (Field Name : HTYPE; Size : 1Byte) : This field tells what kind of hardware (network media) is used for local network. Op = 1 represents Ethernet, while a value of 6 represents an IEEE 802 network.

3. *Hardware Address Length* (Field Name : HLEN; Size : 1Byte) : Specifies the length of hardware address length. In other words, Its represents the number of octates in hardware address. For Ethernet or IEEE 802 MAC addresses, the value of this field is 6.

4. *Hops* (Field Name : HOPS; Size : 1Byte) : Client sets this field to 0 before transmission of packet so it can be utilised by the Relay agents to monitor & manage the relaying of DHCP packets.

5. *Transaction Identifier* (Field Name : XID; Size : 4Bytes) : This field is generated by the client when it initiates a DHCP request and it remains constant throughout the process. The server once recieving the DHCP server discovery packet from client uses this identifier for its response to the client.

6. *Seconds* (Field Name : Secs; Size : 2Bytes) : It represents the amount of time elapsed since the client started to make attempts for acquiring or renewing a lease. DHCP servers utilizes this field to prioritize client requests.

7. *Flags* (Field Name : Flags; Size : 2Bytes) : This field is a reserved field which, presently, contains just one flag subfield of 1Bit known as Broadcast flag represented as B. The other 15bits are reserved and are set to zero.

8. *Client IP Address* (Field Name : CIADDR; Size : 4Bytes) : Client populates this field if and only if it has a valid IP address and the state is BOUND, RENEWING or REBINDING. Otherwise, it is set to 0 (0x00000000). The client utilises this field only when its address is actually valid and usable, not during acquisition process and perticulary not for requesting an IP.

9. *"Your" IP Address* (Field Name : YIADDR; Size : 4Bytes) : Assigned IP address that the server has allocated to the client.

10. *Server IP Address* (Field Name : SIADDR; Size : 4Bytes) : Network address of the

DHCP server that the clients should be using for the next stage in 4-stage protocol. The server address in this field may or may not be same sending the Offer message.

11. *Gateway IP Address* (Field Name : GIADDR; Size : 4Bytes) : This address is used to route DHCP messages when DHCP relay agents are involued.
12. *Client Hardware Address* (Field Name : CHADDR; Size : 4Bytes) : This field holds the MAC address of the client utilised for recognition and communication.
13. *Magic Cookie* (Field Name : MAGICCOOKIE; Size : 4Bytes) : It is the token for the data passed between communicating programs, where the data is not meaningful to the recipient program.
14. *Options* (Field Name : OPTIONS; Size : Max. 4Bytes) : This field is populated with multiple parameters necessary for DHCP basic operations.

For a successful allocation of the network configurations, DHCP operations have 4 stages:

1. DHCP Server Discovery (Client broadcasts).
2. DHCP IP lease offer (Server responses).
3. DHCP IP request (Client broadcasts).
4. DHCP IP lease acknowledgement (Server responses).

1.1.1 DHCP Server Discovery

The Client broadcasts a request using the specific subnet broadcast address (generally 255.255.255.255). Clients keeps track of its assigned IP address and can request it from the DHCP server, It can grant or deny this request depending upon the availability of address and authority of server to grant the requested address. However if the server sends a rejection, Client could request a new IP address.

Fig. 2(a) : Layer 2 header (IP header) – DHCP Server Discovery message.

Fig. 2(b) : Layer 3 header (UDP header) – DHCP Server Discovery message.

Fig. 2(c) : DHCP payload – DHCP Server Discovery message.

1.1.2 DHCP IP lease Offer

DHCP Offer message is the response message when the DHCP server recieves a DHCP server discovery message from a Client. Server Discovery message is interpreted by the server as lease request for IP configurations. The server now make an IP address reservation for that client and unicaste a lease offer message. Client's hardware address (CHADDR) in the DHCP server discovery message helps the server to determine what configuration to send in the DHCP offer message. The YIADDR field or your IP address field of offer message is set to the reserved IP address of the client by the DHCP server.

Fig. 3(a) : Layer 2 header (IP header) – DHCP Offer message.

Fig. 3(b) : Layer 3 header (UDP header) – DHCP Offer message.

Fig. 3(c) : DHCP payload – DHCP Offer message.

1.1.3 DHCP Request

Once a DHCP server makes an offer to the Client, Client creates a DHCP request requesting the offered IP address and broadcast it to the server. As the DHCP server discovery is broadcasted over the channel, multiple responses to the discovery message could arrive at the client but it would only accept one of them. The Server Identification option in the offer message recieved and accepted by the client is used to create a request message for that server, any other servers are informed about which offer has been accepted.

Fig. 4(a) : Layer 2 header (IP header) – DHCP Request message.

Fig. 4(b) : Layer 3 header (UDP header) – DHCP Request message.

Fig. 4(c) : DHCP payload – DHCP Request message.

1.1.4 DHCP Acknowledgement

As soon as the DHCP request message from the client is recieved by the server, the configuration process is now finalising. The server response to this message with an

acknowledgement message to the client, holding the IP lease time and other network configurations which might be needed by the Client for its operations. Now, wih the final acknowledgement message, the configuration process is at its finale.

DHCP protocol ensures that the client configure itself according to the negotiated network interface parameters. After the configuration, Client might use ARP or Address Resolution Protocol for preventing any address conflicts that might arise due to overlapping of DHCP address pools.

Fig. 5(a) : Layer 2 header (IP header) – DHCP Acknowledgement message.

Fig. 5(b) : Layer 3 header (UDP header) – DHCP Acknowledgement message.

Fig. 5(c) : DHCP Payload – DHCP Acknowledgement message.

1.2 "Link Layer Discovery protocol (LLDP)"

The "Link Layer Discovery Protocol (LLDP)" is a protocol that provides media independance over every IEEE 802 complient devices which helped LLDP agents to discover higher level layer information from neighbouring devices.

LLDP supports all IEEE 802 compliant media. Moreover, Protocol works on the Data-Link layer only which made it possible for different compute systems working over seperate Layer 3 or Network layer protocols to discover each other. Each compute system which has a LLDP agent transmits a periodic transmission over all physical network interfaces configured for LLDP transmission. These agents have listeners as well on the same physical interfaces which listens for the LLDP messages. Each multicast transmission holds information of the source port which can be used as connection endpoint identifier.

The LLDP frame contrains minimum of one network address. This address could be utilised

by a Network Management System (NMS) to get to a MA or Management Agent on the compute system using the specified source port. Each LLDP frame has an adjustable TTL or Time-To-Live value, which indicates to the recieving agent when to reject the known topology information. An LLDP Packet Data Unit (PDU) is encapsulated within an IEEE 802 frame, The format is shown in following :

Fig. 6 : LLDP Frame encapsulation.

This frame consists of four basic type of fields, they are :

1. *Slow Protocols Multicast Destination Address* : This address is within the range reserved for protocols which have link-constrains and will not be subjected to forwarding by conformant MAC bridges.
2. *Station Sender Address* : Transmitting station's source MAC address.
3. *Slow Protocols Type* : Field encoding of the Length/Type field.
4. *Subtype* : TBD is set as the Slow Protocols Subtype.

Now, Let's discuss about the actual LLDP PDU. It is made up of a header which can be accompanied by a one or multiple Type-Length-Value attributes (TLVs). Single IEEE 802 media frame contains only one LLDP PDU for every transmission. The LLDP header is 4 Bytes or 32 Bits long, containing 3 fields as following :

Fig. 7 : LLDP Header format.

The LLDP header consists of the following fields :

1. *Version* : Set to 0x01 for this version of the protocols.
2. *Flags* : This field is reserved for future developments in the protocol, it also helps the header word-aligned for easier processing.
3. *Time-To-Live* : The time for which the information in the message is treated as valid by the recipient.

LLDP header is followed by variable number of TLVs. The type of TLV depends upon the implementation and max. message size.

Fig. 8 : LLDP TLV format.

The TLV stands for :

1. *Type* : Information type contained in the value field.
2. *Length* : Length of the Value field in octets.
3. *Value* : Field containing instance specific information encoded in octet-string.

1.2.1 Protocol Operation

A correctly configured LLDP Agent must :

- Transmission of LLDP messages.
- Processing of LLDP messages recieved.
- Save a copy of the LLDP MIB.
- Save a copy of the PTOPO MIB.
- Maintain correct instances.
- Implement MIB objects.

1.3 Switch Configuration Backup

Any Switch requires a governing piece of software called a Firmware and a file (or set of files) holding all the configuration details about the switch called a Configuration file(s) for proper operation of the Switch.

In industrial working environment, Downtime of the devices should be to its minimum. Downtime is refered to the time period for which the concerned device is not working, since devices are not perfect they seem to develop some faults overtime. Businesses can't afford long downtimes within there networks as most of the businesses are online and all their trade is conducted over internet.

To reduce device downtime, Its essential to have proper backup of the firmware and configuration files which can be accomplished by using TFTP servers. TFTP uses client-server architecture and the client can be any machine running the TFTP client application. Because of the simplicity of the TFTP is prefered way to manage the firmware and configuration files. Most modern switches are now managed via Web interface or HTTP protocol for transferring firmware/ configuration files to/from the switch. TFTP server could be running locally within the network or on a remote location over the internet though it is quite unusual to have a local switch configuration over on a remote locaiton.

TFTP stands for Trivial File Transfer Protocol, it is a FTP notable for its simple design, normally used for automatic transfer of configuration between compute systems. It is prefered locally as it provides with no authentication and use a very small amount of memory and processing.

CHAPTER 2. MATERIALS & METHODS.

Every switch have certain capabilities or services within them, all it is needed to enable the services and configure them properly. We are working on Layer 2+ and Later 3 switches, namely, DGS-3420-28TC (Layer 2+ switches) and DGS-3620-26TC (Layer 3 switches). For all the experiments and practicals, we are going to adopt the following topology of switches.

Fig. 9 : Topology to be used for the experiments.

SWRx1 & SWRx2 are Layer 3 switches connected to each other via Port 24. SWx3 & SWx4 are Layer 2+ switches connected to SWRx1 & SWRx2 respectively via Port 1. Finally, SWx5 & SWx5 are also Layer 2+ switches connected to SWx3 & SWx4 via Port 3.

Table : Topology Details for Experiments conducted during Internship.

x in the table represents POD number or Point-Of-Delivery number in the network. It is a kind of repeatable pattern, its components helps the network managers to maximize the manageability, scalability and modularity of the networking systems. The components work in-sync to deliver networking services. To perform the experiments, All the switches are rebooted and reset to their original factory settings.

2.1 Enable / Disable Ports

When the Switches are set back to their original factory settings, by default, all the ports are enabled on the switches which might lead to looping of switches if they are connected.

To prevent looping as in case the STP is not enabled, We have to disable all other ports so that no loops are formed during the experiments.

1. To disable all the ports on the Switch, Enter ***config ports all state disable***.
2. To verify that all the ports are disabled, Enter ***show ports***.
3. Since all the ports are disabled, We have to enable the ports we will be using to create the topology. For enabling ports of the switch, enter ***config ports <portlist> state enable***, where <portlist> represents the port number.

- For SWRx1 & SWRx2, We enable Ports 1 and 24. Enter ***config ports 1,24 state enable***.
- For SWx3 & SWx4, We enable Ports 1 and 3. Enter ***config ports 1,3 state enable***.
- For SWx5 & SWx6, We enable Port 1 only. Enter ***config ports 1 state enable***.

2.2 Dynamic Host Configuration Protocols (DHCP)

In this experiment, Only SWRx1 and SWRx2 will be used as DHCP servers; SWx3, SWx4, SWx5 and SWx6 will be used as DHCP clients. SWRx1, SWx3 and SWx5 will be in VLAN 10 and using addresses fromt he network of 10. 90. x1. 0/24. SWRx2, SWx4 and SWx6 will be in VLAN 20 and using addresses from the network of 10. 90. x2. 0/24.

Table : DHCP configurations.

2.2.1 Configurations for SWRx1

For SWRx1 as a DHCP server, The configuration commands are as follows :

1. ***create vlan v10 tag 10***
2. ***config vlan v10 add tag 1,24***
3. ***create ipif v10-if 10.90.x1.11/24 v10***
4. ***create dhcp pool v10-pool***
5. ***config dhcp pool default_router v10-pool 10.90.x1.11***
6. ***config dhcp pool dns_server v10-pool 10.90.x1.11***
7. ***config dhcp pool network_addr v10-pool 10.90.x1.0/24***
8. ***create dhcp excluded_address begin_address 10.90.x1.1 end_address 10.90.x1.20***
9. ***enable dhcp_server***

Fig. 10 : Creating vlan v10 on SWRx1.

Fig. 11 : Configuring vlan v10 on SWRx1.

Fig. 12 : Create interface v10-if for vlan v10 on SWRx1.

Fig. 13 : Create DHCP pool v10-pool and enable DHCP server on SWRx1.

Fig. 14 : DHCP pool, v10-pool, on SWRx1.

2.2.2 Configurations for SWRx2

For SWRx2 as a DHCP server, The configuration commands are as follows :

1. ***create vlan v20 tag 20***
2. ***config vlan v20 add tag 1,24***
3. ***create ipif v20-if 10.90.x2.11/24 v20***
4. ***create dhcp pool v20-pool***
5. ***config dhcp pool default_router v20-pool 10.90.x2.11***
6. ***config dhcp pool dns_server v20-pool 10.90.x2.11***

7. ***config dhcp pool network_addr v20-pool 10.90.x2.0/24***
8. ***create dhcp excluded_address begin_address 10.90.x2.1 end_address 10.90.x2.20***
9. ***enable dhcp_server***

Fig. 15 : Creating vlan v20 on SWRx2.

Fig. 16 : Configuring vlan v20 on SWRx2.

Fig. 17 : Create interface v20-if for vlan v20 on SWRx2.

Fig. 18 (a) : Create DHCP pool v20-pool and enable DHCP server on SWRx2.

Fig. 18 (b) : Create DHCP pool v20-pool and enable DHCP server on SWRx2.

Fig. 18 (c) : Create DHCP pool v20-pool and enable DHCP server on SWRx2.

2.2.3 Configurations for SWx3

For SWx3 as a DHCP client, The configuration commands are as follows :

1. ***create vlan v10 tag 10***
2. ***config vlan v10 add tag 1***
3. ***config vlan v10 add untagged 3***
4. ***config ipif System vlan v10***
5. ***config ipif System dhcp***

Fig. 19 : Creating vlan v10 on SWx3.

Fig. 20 : Configuring vlan v10 on SWx3.

Fig. 21 : Configuring System interface for vlan v10 & DHCP on SWx3.

Fig. 22 : Network interfaces for on SWx3.

Fig. 23 : Basic Switch configurations on SWx3.

2.2.4 Configurations for SWx4

For SWx4 as a DHCP client, The configuration commands are as follows :

1. ***create vlan v20 tag 20***
2. ***config vlan v20 add tag 1***
3. ***config vlan v20 add untagged 3***
4. ***config ipif System vlan v20***
5. ***config ipif System dhcp***

Fig. 24 : Creating vlan v20 on SWx4.

Fig. 25 : Configuring vlan v20 on SWx4.

Fig. 26 : Configuring System interface for vlan v20 & DHCP on SWx4.

Fig. 27 : Network interfaces on SWx4.

Fig. 28 : Basic Switch configurations on SWx4.

2.2.5 Configurations for SWx5

For SWx5 as a DHCP client, The configuration commands are as follows :

1. ***config ipif System dhcp***

Fig. 29 : Configuring System interface for DHCP on SWx5.

Fig. 30 : Network interfaces on SWx5.

Fig. 31 : Basic Switch configurations on SWx5.

2.2.6 Configurations for SWx6

For SWx6 as a DHCP client, The configuration commands are as follows :

1. ***config ipif System dhcp***

Fig. 32 : Configuring System interface for DHCP on SWx6.

Fig. 33 : Network interfaces on SWx6.

Fig. 34 : Basic Switch configurations on SWx6.

2.3 Link Layer Discovery Protocol (LLDP)

In this experiment, LLDP will be configured on all the six switches.

2.3.1 Configurations on SWRx1

For SWRx1, The configuration commands are as follows :

1. ***config lldp ports 1,24 basic_tlvs all enable***
2. ***config lldp ports 1,24 mgt_addr 1pv4 10. 90. 90. x1 enable***
3. ***config lldp ports 1,24 admin_status tx_and_rx***
4. ***config lldp ports 1,24 notification enable***
5. ***config snmp system_name SWRx1***
6. ***enable lldp***

Fig. 35 : Configuring LLDP on SWRx1.

Fig. 36 : Configuring LLDP on SWRx1.

Fig. 37 : Configuring SNMP System name on SWRx1.

Fig. 38 : LLDP remote ports configurations on SWRx1.

2.3.2 Configurations on SWRx2

For SWRx2, The configuration commands are as follows :

1. ***config lldp ports 1,24 basic_tlvs all enable***

2. ***config lldp ports 1,24 mgt_addr ipv4 10. 90. 90. x2 enable***
3. ***config lldp ports 1,24 admin_status tx_and_rx***
4. ***config lldp ports 1,24 notifaction enable***
5. ***config snmp system_name SWRx2***
6. ***enable lldp***

Fig. 39 : Configuring LLDP on SWRx2.

Fig. 40 : Configuring SNMP on SWRx2.

Fig. 41 : Basic LLDP configuration on SWRx2.

Fig. 42 : LLDP remote ports configurations on SWRx2.

2.3.3 Configurations on SWx3

For SWx3, The configuration commands are as follows :

1. ***config lldp ports 1,3 basic_tlvs all enable***
2. ***config lldp ports 1,3 mgt_addr ipv4 10. 90. 90. x3 enable***
3. ***config lldp ports 1,3 admin_status tx_and_rx***
4. ***config lldp ports 1,3 notification enable***
5. ***config snmp system_name SWx3***
6. ***enable lldp***

Fig. 43 : Configuring LLDP on SWx3.

Fig. 44 : Configuring LLDP on SWx3.

Fig. 45 : Basic LLDP configuration on SWx3.

Fig. 46 : LLDP remote ports configurations on SWx3.

2.3.4 Configurations on SWx4

For SWx4, The configuration commands are as follows :

1. ***config lldp ports 1,3 basic_tlvs all enable***
2. ***config lldp ports 1,3 mgt_addr ipv4 10. 90. 90. x4 enable***
3. ***config lldp ports 1,3 admin_status tx_and_rx***
4. ***config lldp ports 1,3 notification enable***
5. ***config snmp system_name SWx4***
6. ***enable lldp***

Fig. 47 : Configuring LLDP on SWx4.

Fig. 48 : Configuring LLDP on SWx4.

Fig. 49 : Basic LLDP configuration on SWx4.

Fig. 50 : LLDP remote ports configurations on SWx4.

2.3.5 Configurations on SWx5

For SWx5, The configuration commands are as follows :

1. ***config lldp ports 3 basic_tlvs all enable***
2. ***config lldp ports 3 mgt_addr ipv4 10. 90. 90. x5 enable***
3. ***config lldp ports 3 admin_status tx_and_rx***
4. ***config lldp ports ports 3 notification enable***
5. ***config snmp system_name SWx5***
6. ***enable lldp***

Fig. 51 : Configuring LLDP on SWx5.

Fig. 52 : LLDP remote ports configurations on SWx5.

2.3.6 Configurations on SWx6

For SWx6, The configuration commands are as follows :

1. ***config lldp ports 3 basic_tlvs all enable***
2. ***config lldp ports 3 mgt_addr ipv4 10. 90. 90. x6 enable***
3. ***config lldp ports 3 admin_status tx_and_rx***
4. ***config lldp ports 3 notification enable***
5. ***config snmp system_name SWx6***
6. ***enable lldp***

Fig. 53 : Configuring LLDP on SWx6.

Fig. 54 : Basic LLDP configuration on SWx6.

Fig. 55 : LLDP remote ports configurations on SWx6.

2.4 Switch Configuration Backup & System Maintenance

In this experiment, A TFTP server is required. We set up a TFTP server connected to SWRx1 and configure its IP address to 10.90.90.100/24. To set up a TFTP server, configure the PC's IP address to 10.90.90.100 with a subnet mask of 255.255.255.0 .

Fig. 56 : Setting up the IP address of the server to 10. 90. 90. 100/24.

Once the setup of the network configurations has been done on the PC. Its time to install the TFTP server program so that we can use it for backing up the configuration files for various switches.

There are various TFTP server programs which can be downloaded for free from the internet, SolarWinds TFTP server is one of the popular and free server. We downloaded a copy of the program and installed on to the system.

Once the server program is installed onto the system, We need to start the server and activate its working. The server listens for requests onto UDP Port 69, if any connection request arives on this port of the system, The server program would handle the request and serve the request accordingly.

Fig. 57 : Setting up the TFTP server onto the PC.

Fig. 58 : Starting up the TFTP server – Initially Stopped.

Fig. 59 : Starting up the TFTP server – Now Started.

Now, The TFTP server has been started and active on the PC with an IP address of 10.90.90.100 and a subnet mask of 255.255.255.0 . The server is now ready for all the uploads of configuration files from various switches.

All network managers should make it their practice to back up each switch's configuration file to the TFTP server. On all switches, Backup command should be run ***upload cfg_toTFTP 10.90.90.100 dest_file <switchname.cfg>***.

2.4.1 Configuration Backup for SWRx1

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SWR1.cfg

Fig. 60 : Uploading configuration for SWR1.

Fig. 61 : On TFTP server – SWR1.cfg holds configurations for SWR1.

2.4.2 Configuration Backup and Updating firmware for SWRx2

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SWR2.cfg

Fig. 62 : Uploading configuration for SWR2.

Fig. 63 : On TFTP server – SWR2.cfg holds configurations for SWR2.

Fig. 64 : Switch firmware details before Updation.

Fig. 65(a) : Updating firmware requires firmware file to be present on the server.

Fig. 65(b) : Updation Procedure on SWR2.

2.4.3 Configuration Backup for SWx3

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SW3.cfg

Fig. 66 : Uploading configuration for SW3.

Fig. 67 : On TFTP server – SW3.cfg holds configurations for SW3.

2.4.4 Configuration Backup for SWx4

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SW4.cfg

Fig. 68 : Uploading configuration for SW4.

Fig. 69 : On TFTP server – SW4.cfg holds configurations for SW4.

2.4.5 Configuration Backup for SWx5

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SW5.cfg

Fig. 70 : Uploading configuration for SW5.

Fig. 71 : On TFTP server – SW5.cfg holds configurations for SW5.

2.4.6 Configuration Backup for SWx6

Network administrator should backup the switch configurations via the following command :

upload cfg_toTFTP 10.90.90.100 dest_file SW6.cfg

Fig. 72 : Uploading configuration for SW6.

Fig. 73 : On TFTP server – SW6.cfg holds configurations for SW6.

CHAPTER 3. RESULTS & DISCUSSION.

We have conducted various experiments on the "Dynamic Host Configuration Protocol (DHCP) & Link Layer Discovery Protocol (LLDP)" during the course of this internship. In the course of our internship, We discussed how DHCP & LLDP work under-the-hood.

For display of our results, We have used a packet sniffer program called Wireshark. The program captures packets from a perticular network interface and displays them in a user friendly, color coded manner.

3.1 Results of DHCP experiments

From our experiments conducted with DHCP, We came to the understanding of the workings of the protocol. It is a protocol utilising client-server model, the DHCP client broadcasts a Discovery message onto the media which generates response in form of a DHCP Offer from the DHCP server. Once the Client recieves the Offer message, It generates a DHCP Request message and broadcasts it onto the media. The DHCP server recieves the Request message from the client and sends an Acknowledgement message. Thus, Concluding the DHCP assignment procedure.

Fig. 74 (a) : DHCP Discover message.

Fig. 74 (b) : DHCP Offer message.

Fig. 74 (c) : DHCP Request message.

Fig. 74 (d) : DHCP Request message.

3.2 Results of LLDP experiments

From our experiments conducted with LLDP, We came to the understanding of the

workings of the protocol. The "Link Layer Discovery Protocol (LLDP)" is a medium independent protocol for IEEE 802 devices. It allows discovery of capabilities of its peers.

Fig. 75 : LLDP packet with TLV – Time to live = 120.

Fig. 76 : LLDP packet with TLV – Time to live = 40.

CHAPTER 4. CONCLUSIONS.

With these experiments that we have conducted in the course of our internship, We came to certain conclusions.

1. DHCP is a client-server model based protocol. It has successfully replaced ARP or BOOTP for distribution of network configuration.
2. Each DHCP server can be configured to work on certain set of IP addresses.
3. Generally, Each subnet has its own DHCP server but if they are not present on every subnet, DHCP Relay agents can be used to relay the DHCP messages between the Clients and the servers.
4. In the experiments, SWRx1 & SWRx2 serves as DHCP servers. SWx3 & SWx4 served as DHCP Relay agents for SWx5 & SWx6.
5. We were able to assign all the clients attached to the switches IP addresses from the two IP address pools on SWRx1 & SWRx2.
6. LLDP is a medium independent protocol which allows capability discovery of other devices in the network.
7. LLDP TLVs can be programmed onto the switches and can be used to share the capabilities of other devices.
8. In the experiment with LLDP, We have successfully changed the time to live (TTL) from 120 seconds to 40 seconds.

CHAPTER 5. IMPLICATIONS FOR FUTURE RESEARCH.

DHCP has been the standard for IPv4 network configuration however with the introduction of IPv6, DHCP has to be updated to DHCPv6 and implemented on the devices yet to come in the future.

DHCPv6 is further being developed to make available configurations to clients that have been using "Stateless Address AutoConfiguration (SLAAC)". As specified in RFC 4862, The SLAAC is performed as a component of the Neighbour Discovery Protocol (NDP).

"Link Layer Discovery Protocol (LLDP)" can simplify the operation of troubleshooting of networks and increase the capability of network management tools to manage, monitor and maintain accurate network topologies in a network setup which have devices from various manufacturers. It would be used in the future generations of the network devices to effectively manage and monitor the devices.

Siddhant_Tandon_Section_3

ORIGINALITY REPORT

2%	2%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ieee802.org Internet Source	2%
2	computerlinks.fr Internet Source	<1%
3	Toy, . "PB (Provider Bridges), PBB (Provider Backbone Bridges), and PBT (Provider Backbone Transport)", Networks and Services Carrier Ethernet PBT MPLS-TP and VPLS, 2012. Publication	<1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	ON		