Bachelor's Thesis(UAS)

Information Technology

Internet Technology

2013

Abayomi Awe

AN EVALUATION AND ANALYSIS OF THE OPTIMIZED LINK STATE ROUTING PROTOCOL IN AN AD HOC MOBILE WIRELESS MESH NETWORK

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES
Information Techology | Internet Technology
June 2013| 51
Instructor: Patric Granholm

Abayomi Awe

AN EVALUATION AND ANALYSIS OF THE OPTIMIZED LINK STATE ROUTING PROTOCOL IN AN AD HOC MOBILE WIRELESS MESH NETWORK

Abstract

Recent developments in computing and wireless technology have opened up new technologies for the future of mobile networking. The advent of mobile networking has lead to popularity of Mobile ad hoc network(MANET) over the decade, it have has drastically increased because of their network dynamic nature, sometimes rapidly-changing, multi-hop technologies which are likely composed of bandwidth consisting of wireless links.

A MANET is a network built on multi-hop where nodes can move freely in the topology. The network operate based on no infrastructure and can work as fast as possible in any environment. The optimized link state routing protocol (OLSR) is a the protocol for route management for such mobile ad hoc networks.

OLSR operates on the link state algorithm that maintain topology information of the network at each node by employing periodic exchange of messages because of the proactive or table-driven nature of the protocol. The process of optimization on OLSR in a pure link state protocol combines the size of information sent in the message which, is followed by flooding these message in the network into order to reduces the number of transmission.

The thesis is based on research of wireless mesh network using OLSR as the routing protocol through the network.

KEYWORDS: MANET, OLSR, hops, topology, nodes

FOREWORD

I would to like express my gratitude to God, who is the Alpha and Omega, the beginning and the end and all the sufficient One, who has granted me the grace and enablement throughout the course of my studies.

Also, I would like to appreciate my family, most especially my mum and all my brothers and sisters who have contributed immensely to my academic success. I really appreciate them for their support not only materially, mentally, physically, spiritually but also financially and to my lovely angel Omobolape for her tender loving care.

Finally,I would like thank my supervisor Patric Granholm for his patience and guidance during my thesis.

TABLE OF CONTENTS

FIGURES

TABLES

ACRONYMS ABBREVIATIONS AND SYMBOLS

NODE	Computing device actively participating in a network.
MANET	Mobile Ad Hoc Network
GSM	Global System for Mobile Communication
WLAN	Wireless Local Area Network
IBBS	Independent Basic Service Set
BSS	Basic Service Set
ESS	Extended Service Set
PRNET	Packet Radio Networks
SURAN	Survivable Adaptive Radion Networks
GloMo	Global Mobile Information System
CSMA	Carrier Sense Medium Access
AP	Access Point
NRDR	Near-Term Digital Radio
STA	Station
DAPRPA	Defence Advance Research Project Agent.
AODV	Ad-Hoc On Distance Vector Protocol
DSR	Dynamic Source Routing
ACOR	Admission Control Enabled On Demand Routing
ABR	Associatively Based Routing
MPR	Multipoint Relay
DD-WRT	Linux-based firmwares

1 INTRODUCTION

The trend of communication nowadays has moved from the traditional mobile network to mobile ad hoc network and this has changed our way of life to be more sophisticated. Most people use smartphones, iPad and tablet device as means of communication, these gadgets can serve as a stand-alone network on their own and it also a better alternative when the infrastructure networks are not safe.

In contrast, traditional mobile networks which are dependent on pre-existing infrastructure for connectivity while ad hoc network are formed without the use of any central administration but each host relies on each other to keep the network connected (Imrich et al 2003). The benefit of mobile ad-hoc networking is the ability to support robust and efficient operation in wireless a network, by intergrating routing functionality into mobile nodes. Thus, the moble ad-hoc network provide a solution to stay connected anywhere to a network which has made it an integral part of mobile technologies.

The first part of thesis will concentrate on the fundamentals of the mobile ad-hoc network, different types of mobile ad-hoc network, mode of operation of some ad-hoc network and the process on small and large network. In the second part, demonstrate how to deployed the Optimized Link State Routing Protocol behaviour in a small network topology will be established.

1.1 History of Mobile Ad hoc Routing Protocol

Ramramnatha et al, (2002) described briefly the history of mobile ad hoc as a new technology and it origin can traced back to the Defence Advance Research Project Agent (DAPRPA) funded by the U.S government for military research. Under the research concept, packet radio networks (PRNET) were achieved in 1972 which were later developed into the survivable adaptive radio networks (SURAN). In "*Computing Unplugged Magazine Humayun Bakh*t" explained the whole life cycle of an ad-hoc network which can be classifed into first, second, and third generation.

1.1.1 First Generation

The first generation came to limelight back in 1972, the packet radio network was the first technology invented, as the technological development grew, it combined the area location of hazardous atomsphere (ALOHA) and the carrier sense medium access (CSMA) to form the basis of medium access control and distance-vector routing. It was used as a trial for isolated or military environment. The network made used of a technology called radio frequency to transmit and receive data.

1.1.2 Second Generation

The second generation actually started in the 1980s with the SURAN (*surviable adaptive radio networks*) program as an improvement on the first generation. The technological improvements have made it portable, less expensive and more secure to electronic attacks. The aim of this program is to provide packet switched networking in an absent infrastructure mobile battle environment. The continuity for further research brought about the GloMo (*global mobile information system*) project and NRDR *(near-term digital radio)* that provide easy access to service and user friendly ethernet-type multimedia connectivity anywhere and anytime in handheld wireless mobile devices or gadgets.

1.1.3 Third Generation

Laptop computers, palmtop computer, personal digital assistance and other mobile communication equipment invention made the concept of commercial ad-hoc network to become a reality in the 1990s. Due to these innovations, the idea of a collection of most mobile gadget was proposed. The proposal led to its adoption by the IEEE 802.11 subcommittee which brought up the idea of deployment of ad-hoc networks and other applicable fields.

2 MOBILE AD HOC NETWORK

The MANET network is based on the autonomous transitory of mobile node and these nodes communicate with each other over a wireless link. When the nodes lie in close range within each other, communication is direct and they are responsible to discovering each other dynamically as shown in Figure 2.0. The mobile ad hoc network basically does not rely on a fixed infrastructure for its operation in contrast to infrastructure wireless networks where each user directly communicates with an access point or base station (Basagni 2003) Intermediate nodes act as routers to ensure consistent communication between nodes that are not directly within each other's send range, that relay packets generated by other nodes to their destination.

Some of the constraints and characteristic of MANET network as listed by Jeroen Hoebeke et al (2004) are as follows: autonomous and infrastructure-less, multi-hop routing, dynamic network topology, device heterogeneity, energy constrained operation, bandwidth-constrained variable capacity links, limited physical security, network scalability, self-creation, self-organization and self-administration. Andreas Tonnesan (2004) explained that the "ad-hoc mode is obviously the mode to use when setting up a MANET, but it lacks one basic requirement: multi-hop. Traffic is only transmitted to neighbors within radio range when using the ad-hoc mode, therefore, there is a need for MANET routing protocols to set up and maintain traffic paths".

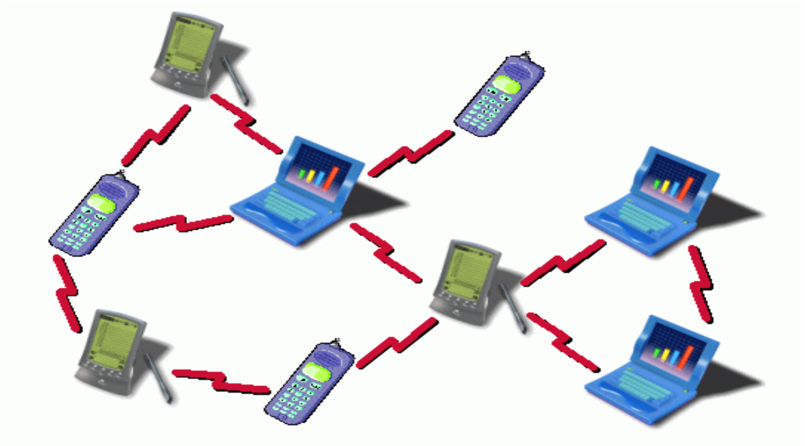


Figure 2.0. A Mobile Ad-hoc Network
(http://www.ece.iupui.edu/~dskim/manet/images/adhocnet.gif)

2.1.1 Wireless LAN

Wireless mobile ad-hoc network functions on any wireless network interface based on any IEEE specification 802.11a, 802.11b or 802.11g. Ad-hoc network nodes can also make use of any of these Wireless LAN interface without restriction to any hardware. The IEEE 802.11 has two modes for Wireless LAN devices and does not support multi-hop communication with itself as shown in Figure 2.1 The ad-hoc mode also knows as IEEE Ad-hoc mode is a configuration based on (IBSS) Independent Basic Service Set as shown in Figure 2.2.

The Independent Basic Service Set (IBSS) network topology that include nodes or wireless device that interact with each other based on peer-to-peer technology without any controlling access point or connection to the wired network and “it is useful for establishing a network where wireless infrastructure does not exist or where service are not received or required” (Sroka 2011).

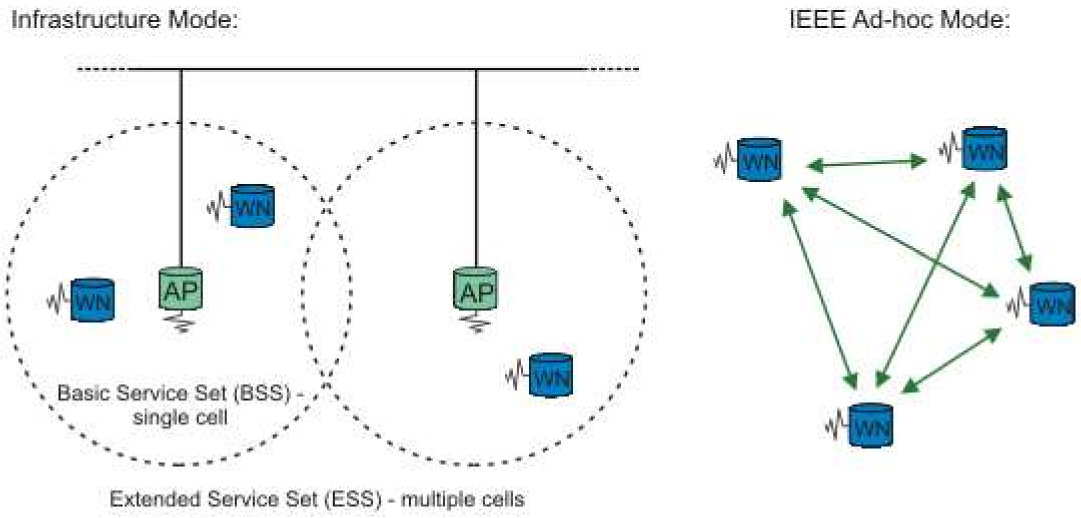

Infrastructure Mode:
IEEE Ad-hoc Mode:
WN
AP
AP
WN
WN
Basic Service Set (BSS) - single cell
Extended Service Set (ESS) - multiple cells
WN
WN
WN
WN

Figure 2.1. Conventional base station compared with ad-hoc multi-hop network (www.linuxdoc.org)

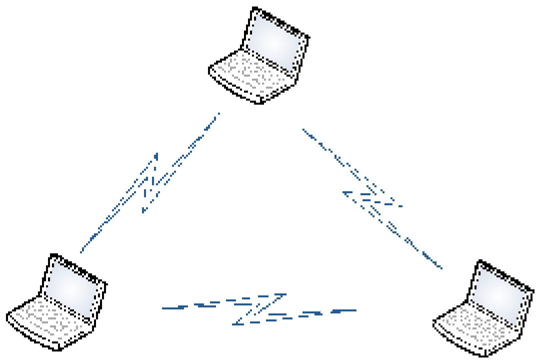


Fig 2.2: Independent Basic Service Set (IBSS) topology (Sroka 2011)

The infrastructure mode is a wireless network that consist of at least one access point connected to the wired network with a set of wireless nodes. This configuration is on Basic Service Set (BSS). The Extended Service Set (ESS) is a set of two or more BSSs (multiple cells). The infrastructure mode structure is based on an architecture of these following devices: (1) an access point and (2) a set of wireless nodes. The infrastructure mode wireless networking device (Access Point) that joins set of wireless nodes to a wired network is a configuration based on the basic building block of an 802.11 wireless LAN called the Basic Service Set (BSS) as depicted in Figure 2. However, if it involves a set of two or more BSSs (multiple cells) in a network it is referred to as Extended Service Set (ESS) as shown in Figure 2.4.

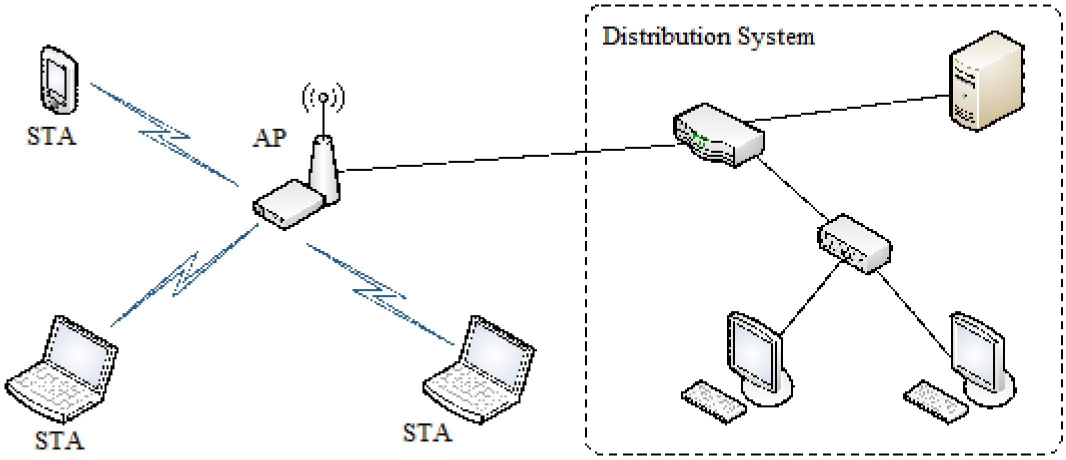


Fig 2.3. Basic Service Set (BSS) topology or network (Sroka 2011)

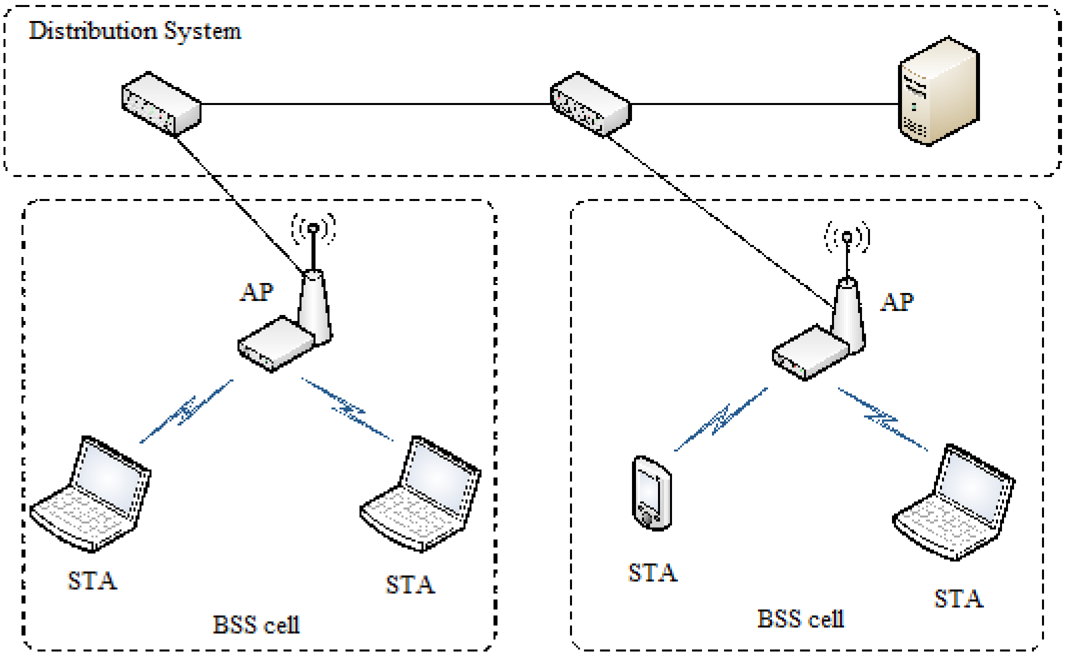


Figure 2.4. Extended Service Set (ESS) topology or network (Rafal Sroka, 2011)

2.1.3 Fundamentals for the Mobile Ad Hoc Networks

MANET characteristics can be divided into the four major and four minor as shown in Figure 2.5. The four major characteristics are referred to as **self-CHOP**. (Misra et al, 2009, 28-29). CHOP: stand for C - Configure, H - Heal, O - Optimized, P - Protect

Major Characteristics

a. Self-Configure is the ability to adjust or survive dynamically to changes in the environments or higher performance.
b. Self-Heal is the ability to discover, diagnose, react to disruption and automatically correct faults.
c. Self-Optimize is the ability to monitor its components and fine tune resoures automatically to optimized their performance.
d. Self-Protect is the ability to anticipate, detect, identify, and protect itself from threats in order to maintain overall integrity.

Minor characteristics

a. Self-aware is the ability to know its components, resources and relations
b. Self-adapt is the ability to adapt its behavior to a changing environment, generating methods on how to interact with neighouring systems and identify the environment automatically.
c. Self-evolve is the ability to implement open standards and generate new plans.
d. Self-anticipate is ability to anticipate the requests for resources from the users without involving them in the complexity of its functionality.

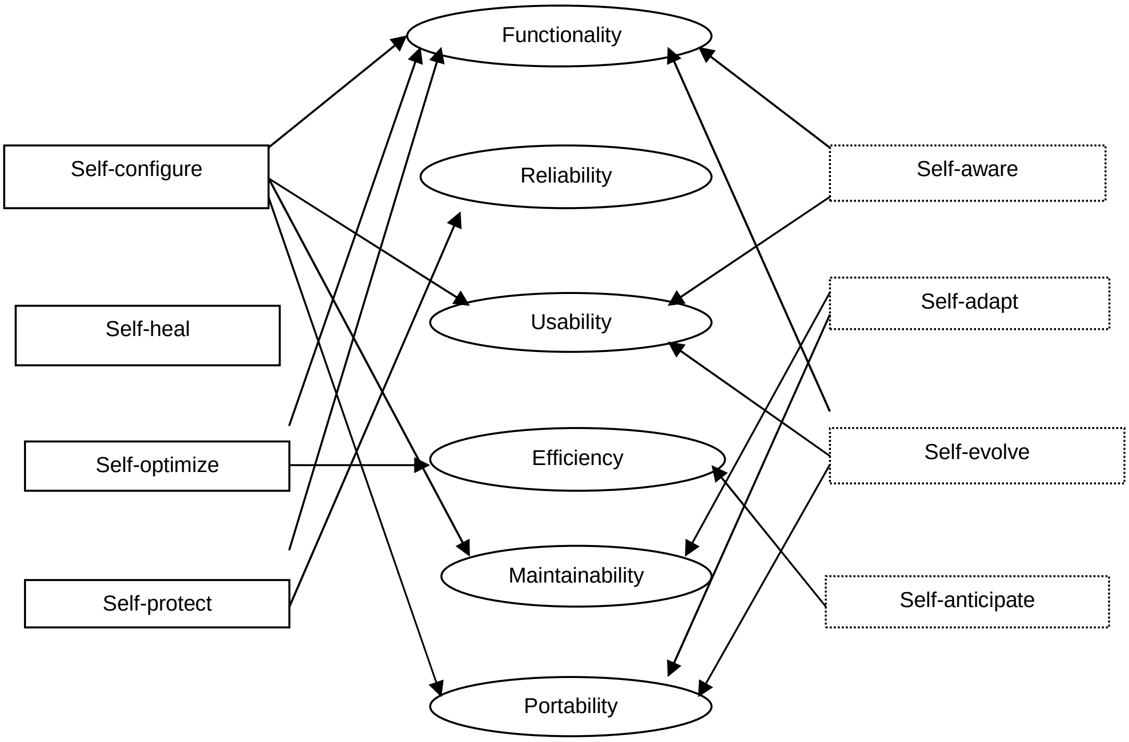


Figure 2.5. Characteritics of Mobile Ad-hoc Network (Misra et al 2009, 28-29)

3 MOBILE AD HOC NETWORK ROUTING PROTOCOL

Padmavathi et al (2010) explained that “the purpose of routing is the exchange of messages from one source to a destination for maintaining effective communication between distinct nodes”. Aishwarya et al (2010) stated further that *“Routing protocol not only discovers network topology but built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to the mobility of node*”. However, Wanning (2009) summarizes routing protocol as “the technique of finding, maintaining multi-hop paths. An ad-hoc network node requires a routing protocol that deals with the changes in topology that the node mobility may cause.”

3.1. Types of Mobile Ad hoc Network Protocol (MANETs)

MANET can be classified into three main categories according to their functionality. These are: On-Demand (Reactive) Protocols, Table-driven (Proactive) Protocols and Hybrid Protocols as shown in figure 3.1. (Qasim et al. 2008)

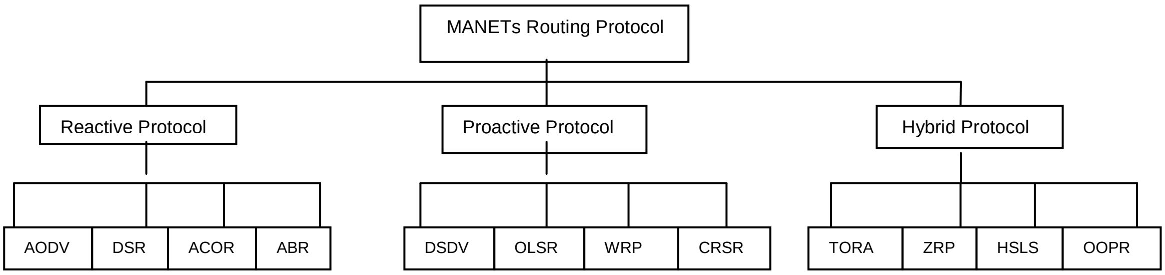


Figure 3.1. Classification of Routing Protocol (Qasim et al 2008)

3.1.1 Demand-driven (Reactive) Protocol

Reactive protocols are also called the on demand-driven protocol. In order words, the node do not keep the routing table unless it is part of the route. It is not unlike the wired network that the device on the network is connected to the either the access point or not and it always keeps the routing table. The reactive routing protocols create routes once a node wants to transmit data to a destination (Tokekar et al 2011). The reactive protocol avoids state route. This happens when a node keep the routing table but on a time scale in which it is going to be used when the node start moving and the number of the route becomes state route without any routes particularly realizing that the route has become useless. The state route is a kind of route that behaves as if it exists but it does not. Some examples of reactive protocols are the ad-hoc on demand distance vector protocol (AODV), dynamic source routing (DSR), admission control enabled on demand routing (ACOR) and associatively based routing ABR) protocols.

Reactive protocol functions in two phases: path discovery and data forwarding (Andel & Yasinsac 2007). Path discovery is initiated when the node requires a route, meanwhile the route has the information to send to the destination within the network. What it does is that it sends a route request message (RREQ) to its neighbors. If the intermediate neighbors node discover no route to the destination node, RREQ is rebroadcast until the neighbor node establishes a route to the destination node and it send a “Route Reply” (RREP) back to the destination node. The “Route Request” (RREQ) has these following information: source address, destination address, broadcast id (ensures that the route message can be uniquely identify), source sequence number, destination sequence number and hop counts. The “Route Request” (RREQ) is identified by source address and broadcast id. The broadcast is a unique number that the source assigned to every RREQ. After the phase has been completed, the data forwarding phase starts by sending the intended information to the destination using the path established in the route discovery phase. For a route to be established and data need to forwarded, the source node and destination node in a reactive protocol needs the source, so node-node routing comes to play.

The source routing does not depend on the intermediate neighbor routing table but allow the source to continually determine the route in which the node information will be sent through the network. This results in detecting simple errors, tracking unnecessary route and making nodes to determine the entire access path to the destination. This always occurs when frequent rapid responses to topology changes, keeping the resources and discarding congestion by channeling the message to move through a specified route or path.

When “Node A” wants to discover a path or route to “Node E”, the “Node A” initiates the route discovery by sending a “Route Request” message (RREQ) to intermediate neighbor “Node B” and “Node B” forward the RREQ to its immediate “Node C” and subsequently continues to forward RREQ until it reaches the final destination “Node E” as shown in Figure 3.2. The route request (RREQ) uses the same request identification (ID) to broadcast throughout the network. The packet transmission continues until “Node E”, which is the destination is reached.(Johnson et al 2001)

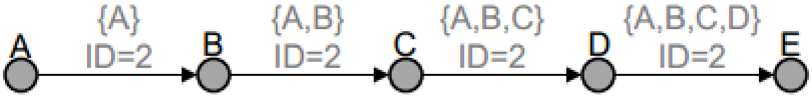
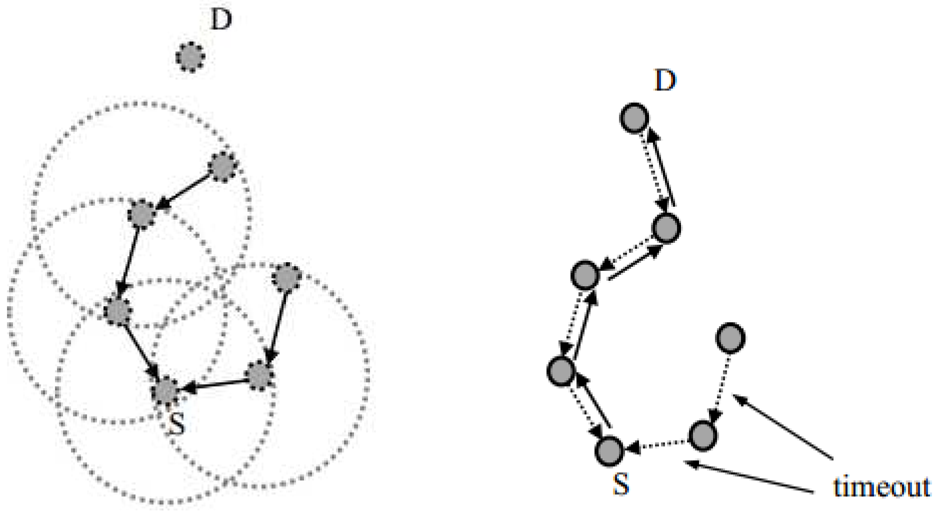


Figure 3.2. Source Routing (Andre Wolf, B.S, 2010)

Another process for establishing a path between a source node and a destination node through forwarding packet and maintaining the route information within the node is called “Node-by-Node” routing. When source “Node S” needs a network path or route to the destination node D as illustrated in Figure 3.3, the source node initiates or creates a route request RREQ and broadcasts it directly to the neighbor nodes. The intermediate node makes a “Reserve Route” entry for “Node S” if there are no routes to “Node D”, and then it rebroadcasts RREQ and updates the number of hop count between the source node and intermediate nodes. The RREQ is continuously rebroadcasted until it finally reaches destination “Node D” through “Reverse Route” to establish a link between the source and destination nodes (Perkin & Royer 1999).



a. Reserve Route b. Forward Route

Figure 3.3: Node by Node Routing (Perkin & Royer 1999)

Ad hoc On-Demand-Vector

Ad hoc On-Demand-Vector (AODV) is a “Node-by-node” routing reactive protocol and deals with table route management. The AODV makes use of a bi-directional route or path to send packets from the source to destination nodes. The route is actively maintained as long as in the packet there is a constant interaction from source to destination through the path. It occurs seldom that if the source node stops sending packets the route, the route is timed out and at the the same time deleted from the intermediate node routing table.

A “Route Error” (RERR) message are sent to the source node and informs the source about the unreachable destinations whenever there is a link failure while the route is still active. The “Route Error” (RREP) message is also sent to all range neighbors to notify them of the detection and error. After the source node has acknowledged the Route Error (RERR) and if it still needs the route, route discovery is reinitiate (Perkin and Royer 1999).

Dynamic Source Routing

Dynamic Source Routing (DSR) is a “Source routing” reactive protocol that works perfectly well on unidirectional and bidirectional links. The protocol stores the routing information on the each packet header and the information is used by the intermediate node in finding out the next hop. In addition, the source routing determines the source node valid route that the packet travels through or sends a “Route Error” (RRER) alert message for any failed link. DSR has the capability to rediscover all the active links by update source routing in the source node in order to renegotiate the path discovery operation as explained in AODV (Johnson et al 2001).

3.1.2 Proactive (Table-driven) Protocol

Proactive protocol is a table driven protocol where each node in the network regularly updates its routing table due to frequent change occurrences in network topology. The node can find the best route to the destination if it has a complete topology in the network. In the proactive protocol, route request (RREQ) and route reply (RREP) messages are not used because all the routes are already available to the destination. Therefore, the network detection and link sensing mechanism are used for path discovery in all proactive protocols. Proactive protocol continuously maintains information within the pathway (Perkins & Pravin 1994).

Each node has a table containing information on how to reach every other node and the algorithm tries to keep table up-to-table. Whenever there is a change in the topology, this table updates according to the changes (Irshad et al. 2010). The nodes exchange topology information with each other; they can have route information any time they are needed”. Examples of proactive protocols are Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR), Wireless Routing Protocol (WRP) and Cluster Head Gateway Switch Routing (CGSR) protocols.

Optimized Link State Routing (OLSR)

Jacquet et al (2001) stated that “this protocol (OLSR) is designed purposely for large and dense mobile wireless networks, with special random behavior nodes. This behavior is based on the principle of multipoint relay”. This protocol is the main subject of this thesis, details of which will discussed later in the next chapter.

3.1.3 Hybrid Routing Protocol

Hybrid routing protocol is a new improved protocol that uses both proactive and reactive protocol together to achieve effective results (Shakywar et al. 2011). The protocol network is divided into zones which use different protocols in two different zones, meaning that, one of the protocols is used within a zone while the other protocol is used between them. Each zone can have different size and each node may be within multiple overlapping zones. Zone Routing Protocol (ZRP) is the example of Hybrid Routing Protocol (Shakywar et al. 2011). The hybrid routing protocol uses and combines features of proactive and reactive. In a case where proactive is used by node to establish routes to its closet neighbor and reactive is used by a node when communication is desired with another node that is outside of its closet neighbor radius (Amitabh 2008).

4 OPTIMIZED LINK STATE ROUTING PROTOCOL

The optimized link state routing protocol is stable in nature which it inherits from a link state algorithm and due to its natural proactivity, routes are available as soon as they are needed. (Clausen & Jacquet 2003) OLSR can be regarded as an optimization of pure link state routing protocol that behaves just like Open Shortest Path First (OSPF) (Tokekar et al 2011). Flathagen (2008) defines OLSR as a "protocol that makes its nodes to exchange their link state messages periodically in order to maintain the topology information. OLSR also has three types of control messages." They are Hello messages (neighborhood messages), topology messages Topology Control (TC messages), and Multiple Interface Interface Declaration (MID).

Two of the main functionalities that OLSR provides are: "Neighbor Discovery" and "Topology Dissemination". The purpose of these two main functionalities is to make each node be able to calculate the routes to all known destinations (Tokekar et al 2011). OLSR uses Topology Control (TC) messages in conjunction with MPR forwarding to broadcast neighbor information throughout the network (Wanning 2009). Multipoint relays also forward control messages, creating an advantage of reducing the number of retransmissions of broadcast control messages (Tokekar et al 2011).

Below, in Fgure 4.1(a) Joakim Flathagen, (2008) shows the normal flooding that occur in a conventional routing protocol and also demonstrates in Figure 4.1(b) that the originality of OLSR is to employ multipoint relays (MPRs) to reduce the number of control messages flooding in the network. OLSR (Wanning 2009) makes use of "Hello" messages to locate its one hop neighbors and through its one hop neighbors' responses, it will be able to locate its two hop neighbours. At this point, it is left to the sender to select its multipoint relays (MPR) based on the information gotten from the first hop node which offers the best routes to the second hop nodes. An MPR selector set is present in each node which lists the nodes that have selected it as an MPR node.

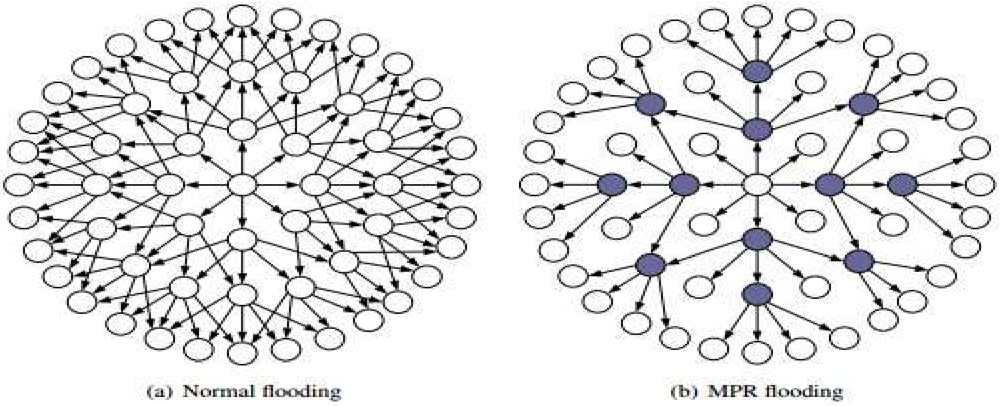


Figure 4.1. Flooding in a multihop network. Flooding through multipoint relays (MPRs) reduce the number of duplicate transmissions (Flathagen 2008).

The design of OLSR protocol works in a completely distributed manner and that makes it impossible to depend on any central source. It also does not also need a reliable transmission for its control messages: each node sends its control message periodically, and thereby making it possible to sustain any form of loss of packets from time to time which occurs constantly in radio networks due to collision or other transmission problems (Clausen & Jacquet 2003).

The OLSR protocol performs hop-by-hop routing and which in other words means that each of the nodes uses its recently updated information to route the packet. (Jacquet et al. 2001).

4.1 Basic layout of OLSR packet

OLSR is designed for use in mobile adhoc networks. It comprises of MAC header, IP header, UDP header, OSLR header and data as shown in table 1 as defined by RFC 3626. (Clausen & Jacquet 2003)

Table 1. OLSR Structure

MAC header	IP header	UDP header	OSLR header	Data…….

4.1.1 OLSR Header

Table 2. OLSR Header Structure

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Packet length																Packet sequence number															
OSLR messages																															

The OLSR Header, illustrated in Table 2 has three primary fields that are used by the application: packet length, packet sequence number and OSLR message as explained by RFC 3626. (Clausen & Jacquet 2003)

- ✓ Packet length-The length (in byte) in the packet.
- ✓ Packet Sequence Number- Packet sequence number must increase by one each time new OLSR packet is transmitted.

4.1.2 OLSR message

Table 3. OLSR message Structure

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MESSAGE TYPE								VTIME								MESSAGE SIZE															
ORIGINATOR ADDRESS																															
TTL								HOP COUNT								MESSAGE SEQUENCE NUMBER															
DATA																															

The OLSR message, illustrated in Table 3 has eigth primary field that is used by the application: message type, vtime, message size, originator address, TTL, hopcount, message sequence number and data (Clausen & Jacquet 2003)

- ✓ Message size -- This is message header length with data and it is 16 bits in size.

- ✓ Vtime - This is 8 bits and specifies the period of time after reception a node considers the information embedded in the message as valid, unless a more recent update to the information is received.
- ✓ Originator address - This is 32 bits in size and it contains the main address of the node which is originally generated this message. It should be noted that it (is not the same as the source address as that can be changed during retransmission but this will never be changed in retransmissions.
- ✓ TTL - This is 8 bits in size, 0 to 255 and contains the maximum number of hops a message will be transmitted. Whenever a message is retransmitted, the TTL decreases by 1 and when a node receives a message with a TTL equal to 0 or 1, the message will not be to process and pass the message across to the next hop and will eventually drop the message.
- ✓ Hop count - This is 8 bits in size and contains the number of hops a message has reached. The message originator sets the hop count to 0 and whenever a message is retransmitted, the hop count increases by 1.
- ✓ Message sequence number - While generating a message, the originating node assigns a unique identification number to each message and this number is inserted into the sequence number field of the message then the sequence number is increased by one for each message originating from the node. Message sequence numbers are basically used to ensure that a given message is not retransmitted more than once by any node.

The combination of OLSR header and OLSR messages form the OLSR packet format.

4.2 OLSR control messages

During transmission,several OLSR messages are defined and frequently changed when they are active in an network and this results in the formation of OLSR control traffic. OLSR uses UDP Port 698 to broadcast OLSR control messages, assigned by the Internet Assigned Number Authority (IANA). The three types of messages that OLSR supported are “Hello”, “Topology Control (TC)” and “Multiple Interface Declaration (MID)”.

4.2.1 Hello Messages

HELLO message are sent on periodic intervals due to the necessary information for link sensing and (one and two hop) neighborhood observed by a node. Every active node interface in the network generate and send these messages. (Popi & Festor 2010)

Table 4. OLSR Hello message Format

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="16">RESERVED</td><td colspan="8">HTIME</td><td colspan="8">WILLINGNESS</td></tr>
<tr><td colspan="8">LINK CODE</td><td colspan="8">RESERVED</td><td colspan="16">LINK MESSAGES SIZE</td></tr>
<tr><td colspan="32">NEIGHBOR INTERFACE ADDRESS</td></tr>
<tr><td colspan="32">NEIGHBOR INTERFACE ADDRESS</td></tr>
<tr><td colspan="32">---</td></tr>
<tr><td colspan="8">LINK CODE</td><td colspan="8">RESERVED</td><td colspan="16">LINK MESSAGES SIZE</td></tr>
<tr><td colspan="32">NEIGHBOR INTERFACE ADDRESS</td></tr>
<tr><td colspan="32">NEIGHBOR INTERFACE ADDRESS</td></tr>
<tr><td colspan="32">---</td></tr>
<tr><td colspan="32">---</td></tr>
</table>

4.2.2 Multiple Interface Declaration

Each node has multiple interface. In multiple interface declaration process, it announce these multiple interface frequently to other nodes by broadcasting MID messages as shown in Figure 4.5. Klein (2005) explained “that the nodes main address is already included in the originator address of the message header only the additional interface addresses have to be announced.” Based upon this information, the Multiple Interface Association Information Base is built in the receiving node.

Table 5. OLSR message MID format

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
OLSR INTERFACE ADDRESS																															
OLSR INTERFACE ADDRESS																															
--																															
OLSR INTERFACE ADDRESS																															

4.2.3 Topology Control

MPR optimization is used to flood “Topology Control (TC) messages”, which is usually done at a periodic interval. Moreover, “Topology Control (TC) messages” are generated immediately when changes are discovered in the MPR selector set. The Topology Control (TC) message has a sequence number which is updated regularly when the advertised neighbor set has changed. The list of advertised neighbors’ main addresses are shown in Table 6. (Klein 2005)

Table 6. Topology control Messages

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ANSN															RESERVED																
ADVERTISED NEIGHBOR MAIN ADDRESS																															
ADVERTISED NEIGHBOR MAIN ADDRESS																															
--																															

4.3 Network Detection or Sensing

Every node has to detect the neighbor nodes with which it is directly linked to. Each node broadcasts its “**hello messages”** from time to time, containing the information about its neighbors’ nodes and their link status. The link status can be “symmetric”, “asymmetric”, “multipoint relay” or “lost in nature” (Ermel & Muhlethaler 2006).

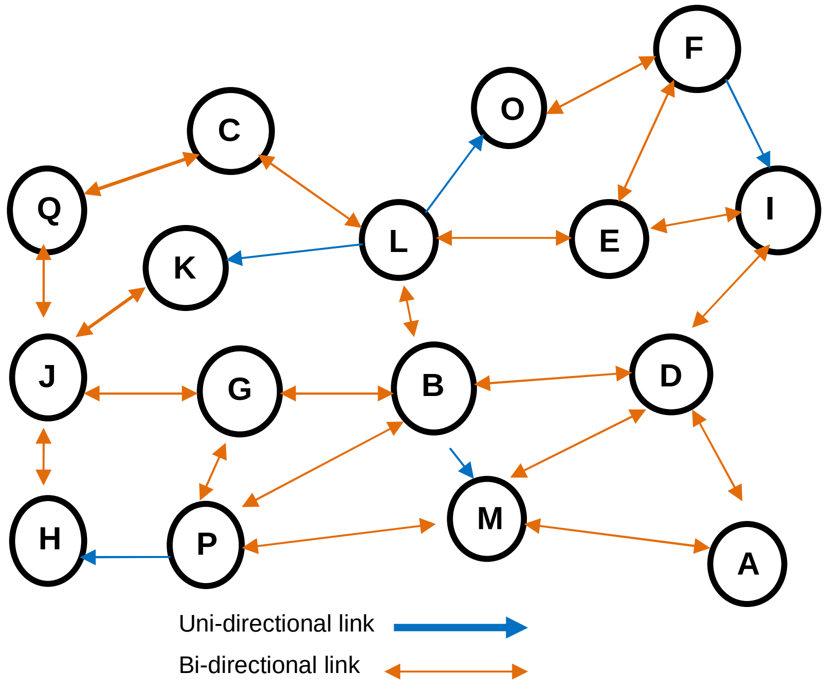


Figure 4.5 Sample of a small network with uni and bi directional links

- Symmetric (Bi-directional) means that the communication link is possible in both irections.
- Asymmetric (Uni-directional) means that the communication link is possible in one direction.
- Multipoint relay means that the communication link is symmetric and the sender of the hello message has selected this node as a multipoint relay (MPR).
- Lost means that the communication link is lost.

4.4 Multipoint Relay Selection Algorithm

OLSR describes that multipoint relays (MPRs) technique used to advertise link state information for their MPR selector at regular intervals ín their control messages. It is also used to form a route from a given node to any destination in route calculation. From Tonnesen’s 2004 perspective, OLSR uses flooding of packets to diffuse topology information throughout the network

Multipoint Relay Selection

Each node in the network selects individually its own set of MPRs. The MPRs technique restricts the set of nodes retransmitting a packet from all nodes to a subset of all nodes. However, the size of subset depends on the topology of the network. Thus, the concept of MPRs is an optimization of a pure flooding mechanism (Wang & Qian 2003).

MPR is performed by selecting of a neighbor as Multipoint (MRPs) and for every node by calculatiing own set of MRPs as a subset of its symmetric neighbor nodes chosen so that all 2 hop neighbors can be reached through a MPR. For further explanation, for every node in the network that can be reached from the local node by at least two symmetric hops, there must exist a MPR so that the node has a symmetric link to the MPR and the MPR is a symmetric neighbor of the local node.
Figure 4.8 illustrates how node F has selected the brown nodes as its MPRs (Tonnesen 2004).

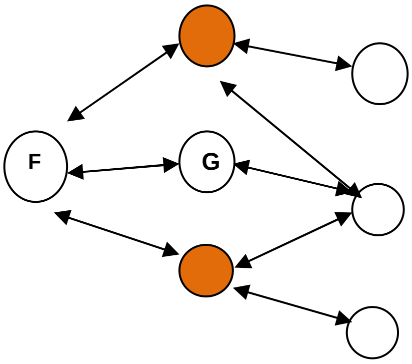


Figure 4.8. Node F has selected the brown nodes as its MPRs

5. STIMULATION AND PERFORMANCE ANALYSIS OF OLSR

In the project, it was decided to illustrate how OLSR works using DDWRT to establish a network topology using a downloaded firm software on two different routers that are compatible with the ad-hoc network topology.

5.1 Building a Wireless Mesh Network

The architecture of wireless mesh network is based on these following hardware and software.The hardware used included: 2 Ethernet cable, 2 Laptops, 2 Linksys wireless router, 1 Desktop with wireless card. The software used included: dd-wrt.v24_mirco_olsrd_generic.bin, Wireshark, olsrd-0.5.6-r3-pre-cac1dfcd5-setup.exe, Any web browser (Internet Explorer or Firefox). Table.. below shows the system configurations and their properties used in building mesh wireless network

Table 7. System configuration and their properties

COMPUTER NAME	OPERATING SYSTEM	MEMEORY	CPU	HDD
Hewlett-Packard(Compaq Mini)	Window 7 Starter	1GB	Intel Atom 1.67GHz	210GB
Hewlett-Packard	Window Vista Basic	2GB	AMD Sempron 2.0GHz	140GB
Fujisu Seimens Computer(Desktop)	Window XP Professional	1GB	AMD Sempron 1.81GHz	100GB

Table 8. Types of Linksys Cisco Wireless Router

Model	Version
WRT54GL	1.0 or 1.1
WRT54G	6.0

Linksys Router Physical Architecture

1. Platform – It has Broadcom MIPS.

2. CPU – The CPU BCM5452 Broadcom operate at 200MHz. It supports DD-WRT because of overclocking feature of the CPU.

3. Flash – It has single 4 MB NAND chip.

4. System Memory – It has 16 bit 16 MB DDR SDRAM.

5. Wireless Radio – It has 802.11b/g Broadcom

6. Antenna – It has a removable, rotating and dual folding antenna.
7. Network Switch – It has a 4 LAN (10/100) and 1 WAN (10/100).

8. Serial pinout – It has a serial pinout on the router.

9. JTAP pinout – It has a JTAP pinout on the router.

Internal Architecture of Linksys Router WRT54GL v1.0, 1.1 or WRT54G v6.0

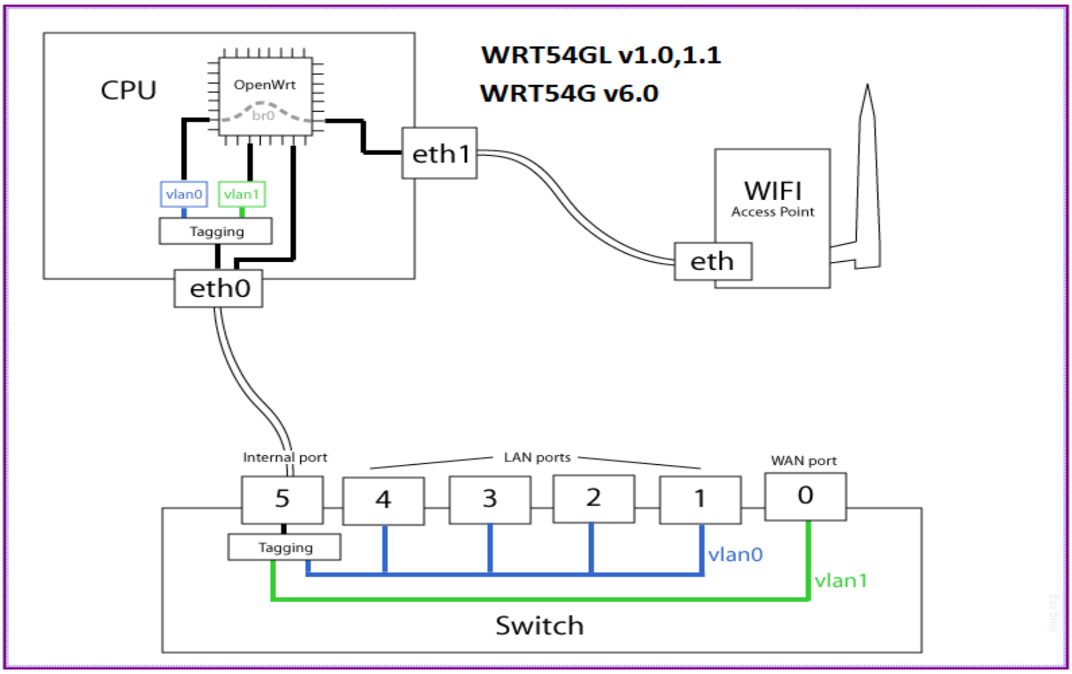
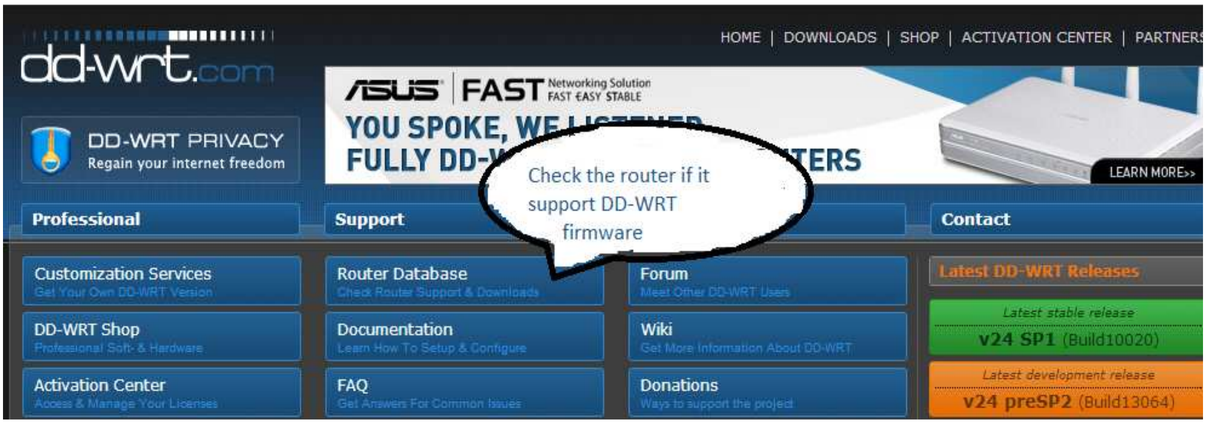


Figure 5.1. Internal architecture of Linksys router(www.openwrt.org)

Figure 5.1 shows the internal architecture of wrt54gl v1.0, 1.1 or wrt54g v6.0. The switch has port from 0 to 5. The port 0 is the internet (WAN) port, the port 1 to 4 is the LAN port and port 5 has an internal connection with the router's center processing unit (CPU).

5.2 Preparing a Wireless Mesh Network (Flashing Linksys WRT54GL and WRT54G with DD-WRT Firmware)

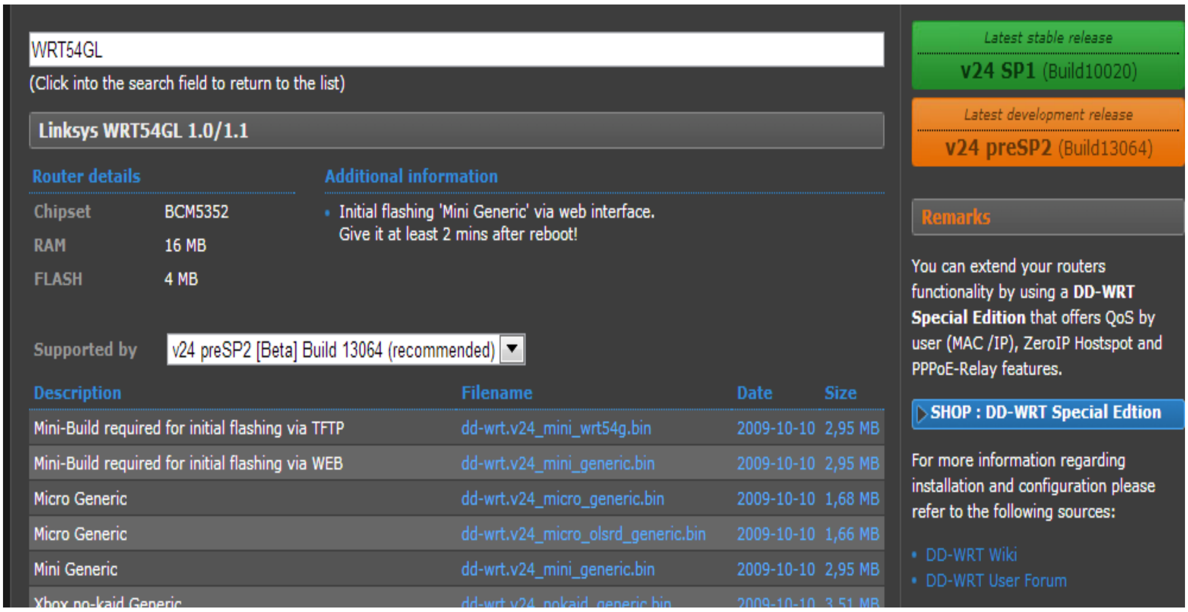
DD-WRT is an open source software under the licence of general public licence (GPL) used as a third-party firmware for broadcom or atheros wireless router with ieee 802.11a/b/g/n. DD-WRT firmware has a advance features that improves internet performance. There are three methods of flashing a Linksys router. They are flashing with web graphical user interface (GUI), flashing with TFTP and flashing with command line.


dd-wrt.com
HOME | DOWNLOADS | SHOP | ACTIVATION CENTER | PARTNERS
DD-WRT PRIVACY
Regain your internet freedom
ASUS FAST Networking Solution FAST EASY STABLE
YOU SPOKE, WE L
FULLY DD-W
TERS
LEARN MORE>>
Professional
Support
Contact
Customization Services
Get Your Own DD-WRT Version
DD-WRT Shop
Professional Soft- & Hardware
Activation Center
Access & Manage Your Licenses
Router Database
Check Router Support & Downloads
Documentation
Learn How To Setup & Configure
FAQ
Get Answers For Common Issues
Forum
Meet Other DD-WRT Users
Wiki
Get More Information About DD-WRT
Donations
Ways to support the project
Latest DD-WRT Releases
Latest stable release
v24 SP1 (Build10020)
Latest development release
v24 preSP2 (Build13064)

Check the router if it support DD-WRT firmware

Figure 5.2 DD-WRT website

From the dd-wrt website, it was checked if the routers planned to be used supports the dd-wrt firmware as shown Figure 5.1. The router database was checked on dd-wrt website and it gave “wrt54gl” of the dd-wrt software which has two versions, either for version 1.0 or 1.1. It is advisable to select the recommended micro generic firmware software specified on their website as shown in Figure 5.2.



WRT54GL

(Click into the search field to return to the list)

Linksys WRT54GL 1.0/1.1

Router details

Chipset	BCM5352
RAM	16 MB
FLASH	4 MB

Additional information

- Initial flashing 'Mini Generic' via web interface. Give it at least 2 mins after reboot!

Supported by: v24 preSP2 [Beta] Build 13064 (recommended)

Description	Filename	Date	Size
Mini-Build required for initial flashing via TFTP	dd-wrt.v24_mini_wrt54g.bin	2009-10-10	2,95 MB
Mini-Build required for initial flashing via WEB	dd-wrt.v24_mini_generic.bin	2009-10-10	2,95 MB
Micro Generic	dd-wrt.v24_micro_generic.bin	2009-10-10	1,68 MB
Micro Generic	dd-wrt.v24_micro_olsrd_generic.bin	2009-10-10	1,66 MB
Mini Generic	dd-wrt.v24_mini_generic.bin	2009-10-10	2,95 MB
Xbox no-kaid Generic	dd-wrt.v24_nokaid_generic.bin	2009-10-10	3,51 MB

Latest stable release
v24 SP1 (Build10020)

Latest development release
v24 preSP2 (Build13064)

Remarks

You can extend your routers functionality by using a **DD-WRT Special Edition** that offers QoS by user (MAC /IP), ZeroIP Hostspot and PPPoE-Relay features.

SHOP : DD-WRT Special Edtion

For more information regarding installation and configuration please refer to the following sources:

- DD-WRT Wiki
- DD-WRT User Forum

Figure 5.3. DD-WRT website to show the description of firmware to be used

Requirement for flashing

1. A computer with Window or Linux operating system
2. An internet connection
3. Cisco Linksys router (WRT54GL/WRT54G/SWRT54G) or other supporting router
4. Firmware image from DD-WRT website

5.3 Steps for Flashing

In order to begin the flashing procedure, it was necessary to check the router database first on the website “http://www.dd-wrt/site/support/router-database”. In the DD-WRT website, a wiki page which shows devices of all the routers that support DD-WRT. The Wiki also include page for incompatible devices for all router that do not support DD-WRT.

Flashing with DD-WRT firmware

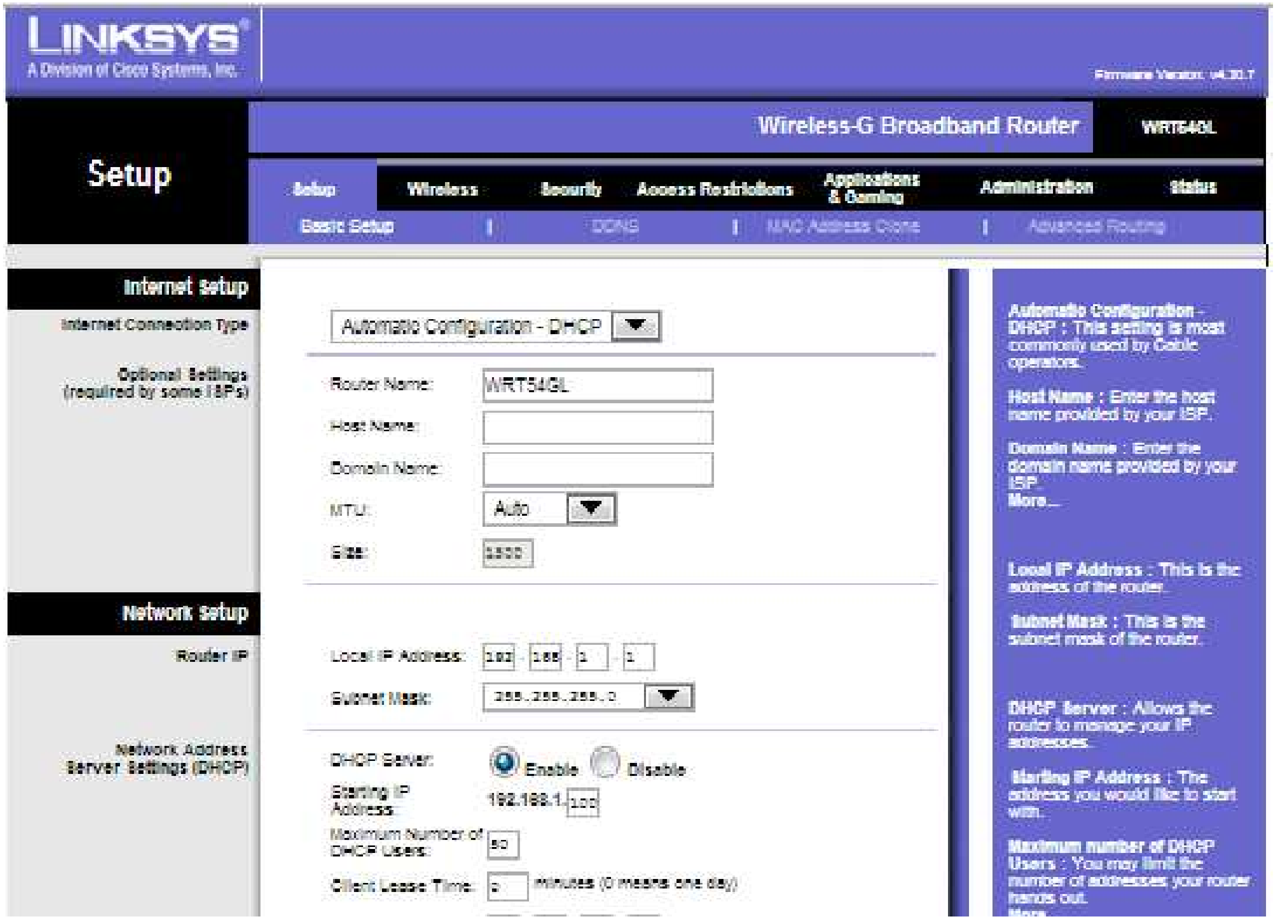
Hard reset or 30/30/30: The first operation carried on the router was 30/30/30 or hard reset. The procedure for the 30/30/30 started when the Linksys router was connected to a power supply, in the process continuously pressing and holding the reset button for 30 seconds. Secondly, with the reset button still on hold, the router was unplugged for another 30 seconds. Lastly, the router was re-plugged while still holding on the reset button for another 30 second in total, making 90 seconds to enable a hard reset.

Web GUI log on: The WAN port on the router was connected to the internet outlet via an Ethernet cable (RJ45). Another cable was connected from the LAN port of the router to the Internet port of the computer. A static IP address was configured on author's computer and the IP address on the computer was set as 192.168.1.2, subnet mask address as 255.255.255.0, and the default gateway address as 192.168.1.1.

When all the mentioned above have been completed, the following steps were followed to have a web access to the Linksys router. But it shoud be noted that, an enhanced javascript website interface without any security was used. Linksys firmware web graphical user interfaces are compatible with most web browser but in case the web browser gives an error, another compatible web browsers should be tried.

1. IP addresses of the Linksys router 192.168.1.1 was typed into the web browser address bar and entered on the keyboard.

2. Immediately, there was prompt option for the username and password in a dialog box. By default, the username was left blank and the password is *admin* in Linksys firmware. Likewise in the DD-WRT, the username is *root* and the password is *admin* by default. On the dialog box, the username was left blank and *admin* was written as the password and *ok* button was clicked. The Linksys graphical user interface prompts up the setup contol plane as shown in Figure 5.3.



Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name: WRT54GL

Host Name:

Domain Name:

MTU: Auto

Size: 1500

Network Setup

Router IP

Local IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

Network Address Server Settings (DHCP)

DHCP Server: ● Enable ○ Disable

Starting IP Address: 192.168.1.100

Maximum Number of DHCP Users: 50

Client Lease Time: 0 minutes (0 means one day)

Automatic Configuration - DHCP : This setting is most commonly used by Cable operators.

Host Name : Enter the host name provided by your ISP.

Domain Name : Enter the domain name provided by your ISP.
More...

Local IP Address : This is the address of the router.

Subnet Mask : This is the subnet mask of the router.

DHCP Server : Allows the router to manage your IP addresses.

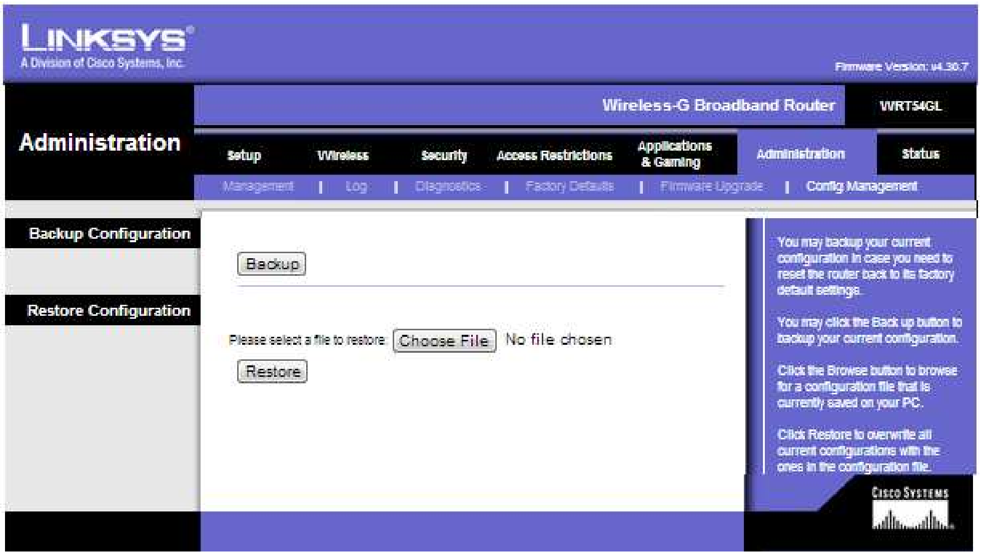
Starting IP Address : The address you would like to start with.

Maximum number of DHCP Users : You may limit the number of addresses your router hands out.
More...

Figure 5.4. Setup plane graphical user interface (GUI) of Linksys router

5.4 Firmware upload

On the setup plane graphical user interface (GUI), the administration option was navigated to, under the administration option, *config management* was clicked which has two options namely the backup configuration and restore configuration. The backup configuration option was used with backup button to backup the Linksys firmware. The restore configuration button will be used in case the upgrade firmware failed as shown in Figure 5.4



Please select a file to restore:

You may backup your current configuration in case you need to reset the router back to its factory default settings.

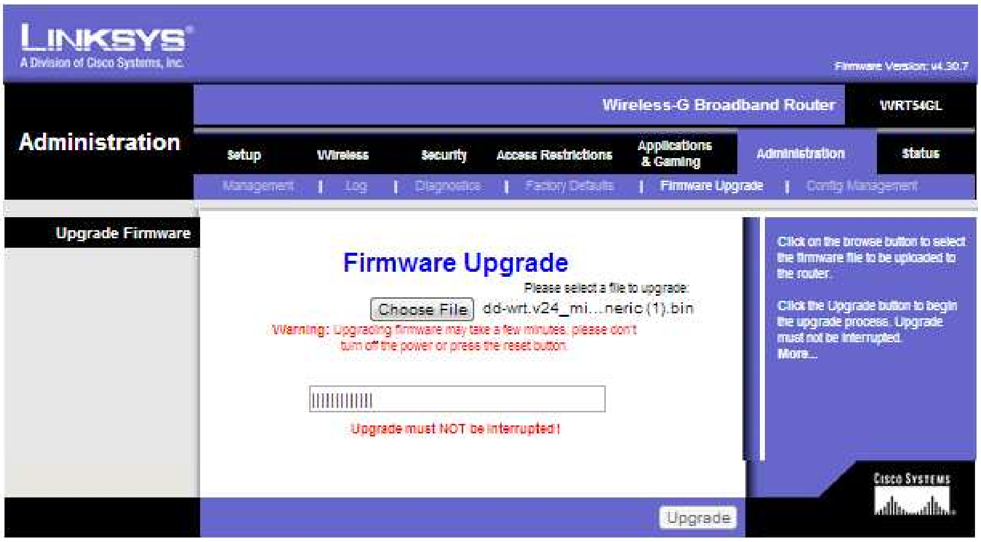
You may click the Back up button to backup your current configuration.

Click the Browse button to browse for a configuration file that is currently saved on your PC.

Click Restore to overwrite all current configurations with the ones in the configuration file.

Figure 5.5. How to backup and restore configuration in Linksys router.

The dd-wrt v24_micro_olsrd_generic.bin was downloaded from the DD-WRT website and saved on the computer. On the administration control plane, the file option was chosen after navigating to the firmware upgrade and then upload the dd-wrt v24_micro_olsrd_generic.bin was uploaded from where it was saved on the computer. After uploading the dd-wrt firmware, the upgrade button was clicked to install the dd-wrt firmware on the router. It takes some few minutes to install as shown in Figure 5.5. A dialog box with “upgrade is successful” appears with “Continue” button. The Continue button was clicked as shown in Figure 5.6, then the Linksys graphical user interface lost connection. After that, the reset button on the router (power cycle) was pressed which took awhile to restart the router. The IP address 192.168.1.1 was again typed in the web browser which shows the dd-wrt setup control as depicted in Figure 5.7.



LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v4.30.7
Wireless-G Broadband Router
WRT54GL
Administration
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade | Config Management
Upgrade Firmware
Choose File
Upgrade
Cisco Systems

Firmware Upgrade

Please select a file to upgrade:

dd-wrt.v24_mi…neric (1).bin

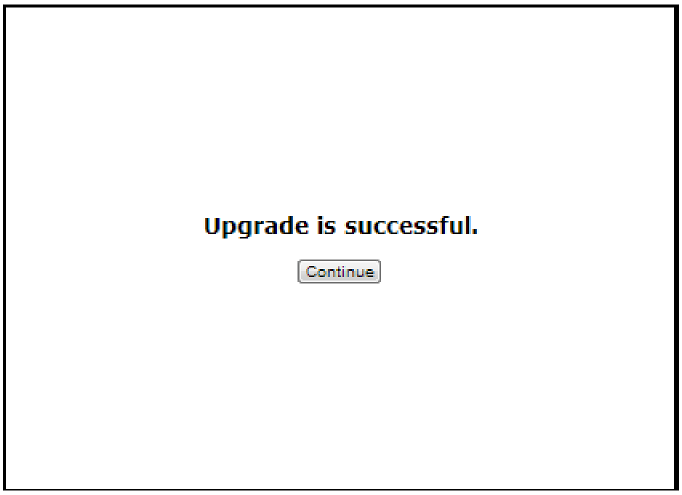
Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.

Upgrade must NOT be interrupted !

Click on the browse button to select the firmware file to be uploaded to the router.

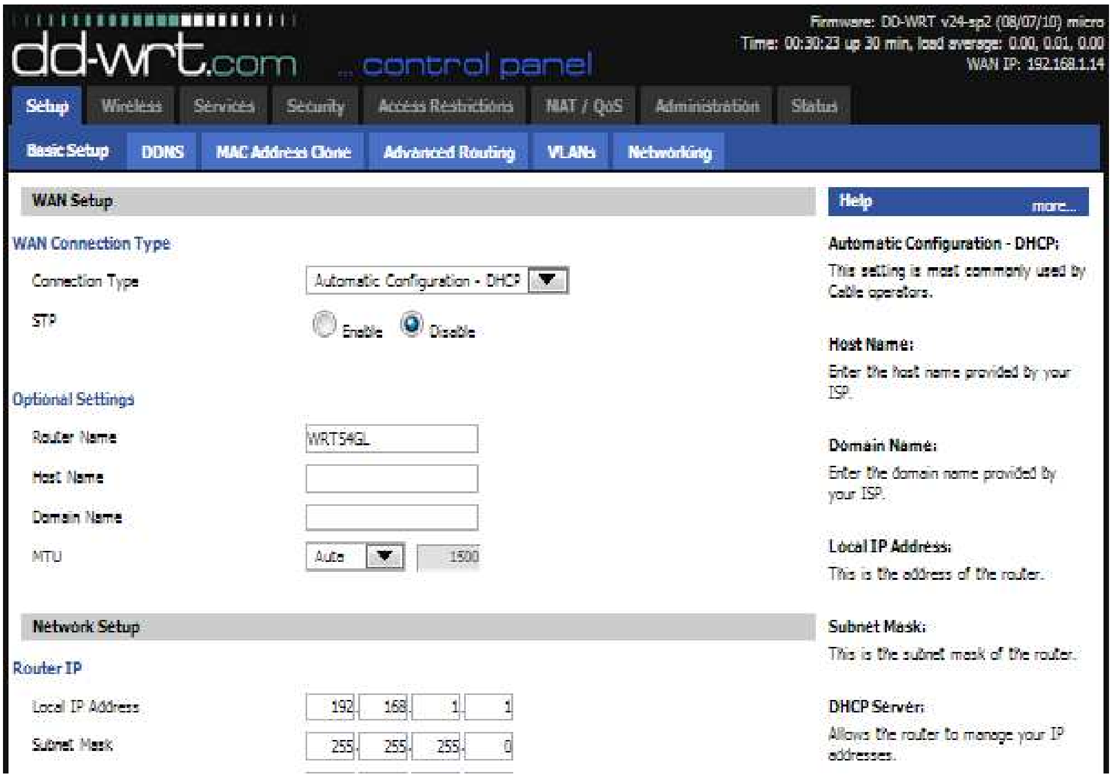
Click the Upgrade button to begin the upgrade process. Upgrade must not be interrupted.
More...

Figure 5.6. Installation of DD-WRT firmware on the Linksys router



Upgrade is successful.

Figure 5.7. DD-WRT firmware software was successful upgrade



Firmware: DD-WRT v24-sp2 (08/07/10) micro
Time: 00:30:23 up 30 min, load average: 0.00, 0.01, 0.00
WAN IP: 192.168.1.14

WAN Setup

WAN Connection Type

Connection Type: Automatic Configuration - DHCP

STP: ○ Enable ● Disable

Optional Settings

Router Name: WRT54GL

Host Name:

Domain Name:

MTU: Auto 1500

Network Setup

Router IP

Local IP Address: 192. 168. 1. 1

Subnet Mask: 255. 255. 255. 0

Automatic Configuration - DHCP:
This setting is most commonly used by Cable operators.

Host Name:
Enter the host name provided by your ISP.

Domain Name:
Enter the domain name provided by your ISP.

Local IP Address:
This is the address of the router.

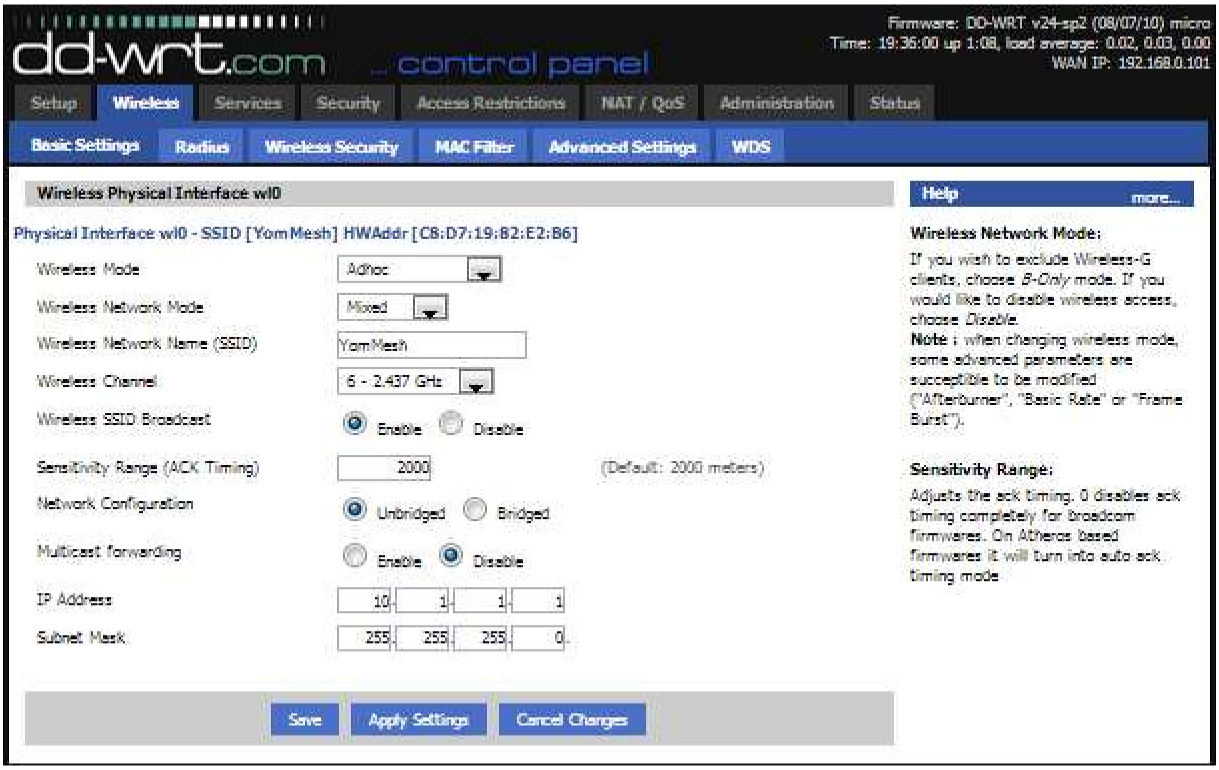
Subnet Mask:
This is the subnet mask of the router.

DHCP Server:
Allows the router to manage your IP addresses.

Figure 5.8. DD-WRT control plane

Configuration of routers on the DD-WRT graphical user interface (GUI)

On the DD-WRT router control plane under the “Wireless” option we have the “Wireless Physical Interface wl0” which states the following configurations: “Wireless mode” which must be configured as “Adhoc”, “Wireless Network Mode” which was configured as “Mixed”, “Wireless Network Name (SSID)” was named as “YomMesh” which will have the same name as the other router in order to communicate with each other. The “Network Configuration” was made “Unbridged” so as to have IP address for the routers. The IP addresses for the two routers are 10.1.1.1 and 10.1.1.2 with their subnet address as 255.255.255.0. The security mode was disabled and the “apply settings” option was selected.



Firmware: DD-WRT v24-sp2 (08/07/10) micro
Time: 19:36:00 up 1:08, load average: 0.02, 0.03, 0.00
WAN IP: 192.168.0.101

Wireless Physical Interface wl0

Physical Interface wl0 - SSID [YomMesh] HWAddr [C8:D7:19:82:E2:B6]

Wireless Mode	Adhoc
Wireless Network Mode	Mixed
Wireless Network Name (SSID)	YomMesh
Wireless Channel	6 - 2.437 GHz
Wireless SSID Broadcast	● Enable ○ Disable
Sensitivity Range (ACK Timing)	2000 (Default: 2000 meters)
Network Configuration	● Unbridged ○ Bridged
Multicast forwarding	○ Enable ● Disable
IP Address	10. 1. 1. 1
Subnet Mask	255. 255. 255. 0

Wireless Network Mode:
If you wish to exclude Wireless-G clients, choose *B-Only* mode. If you would like to disable wireless access, choose *Disable*.
Note : when changing wireless mode, some advanced parameters are susceptible to be modified ("Afterburner", "Basic Rate" or "Frame Burst").

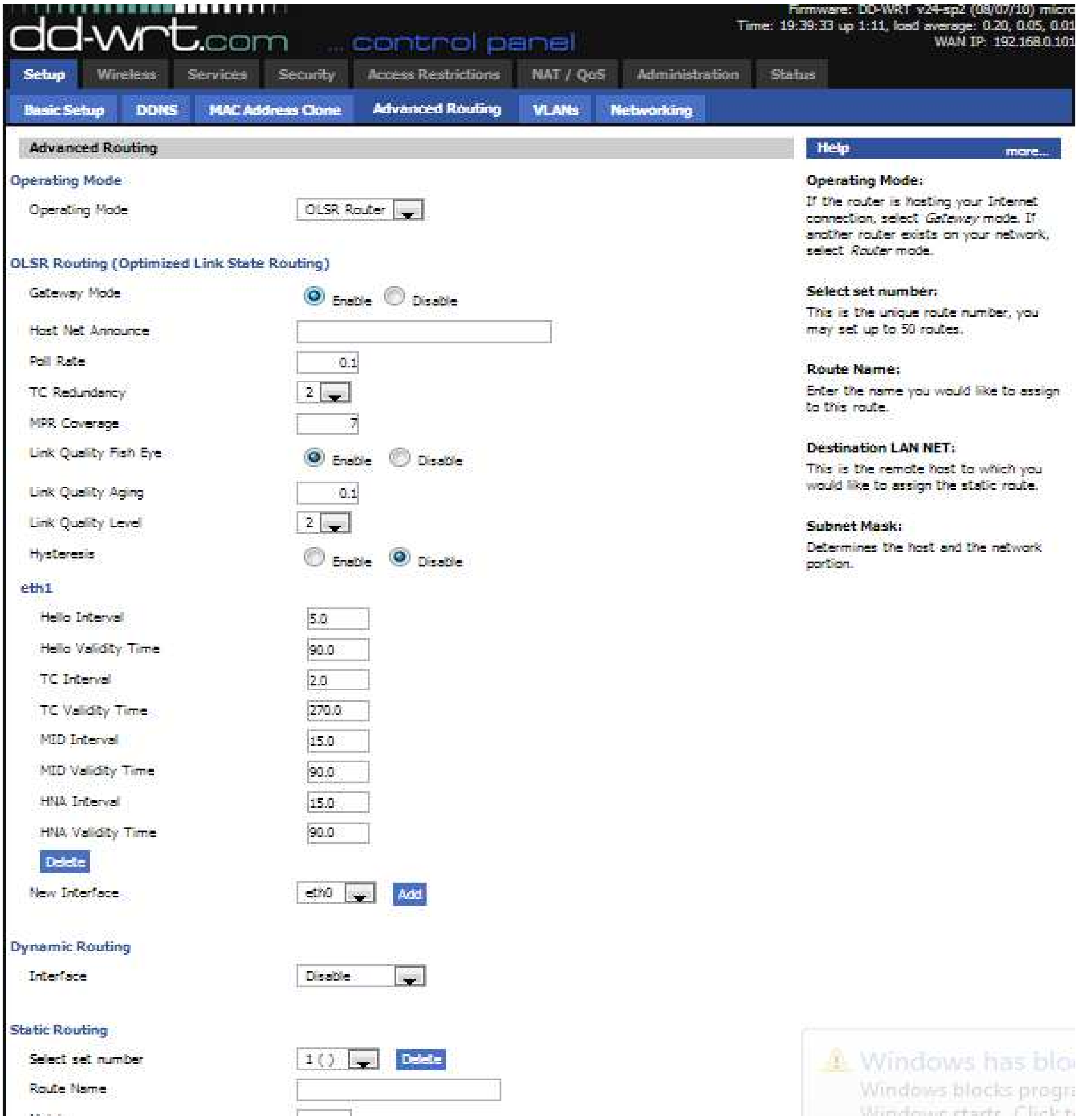
Sensitivity Range:
Adjusts the ack timing. 0 disables ack timing completely for broadcom firmwares. On Atheros based firmwares it will turn into auto ack timing mode

Figure 5.9: DD-WRT Set up the wireless interface.

On the DD-WRT router control plane security option, the SPI firewall was disabled because it will be easy to troubleshoot the setup. Firewall was disabled to mak the open ports work for OLSR. The network was later made more secure by enabling the firewall and configure the iptable on all routers in order to open the needed port (port 698 UDP is use for OLSR).

5.5 OLSR SETUP

In the DD-WRT graphical user interface (GUI), the setup tab was navigated to thereafter to the advance routing tab. In the advance routing tab, “OLSR Router” was chosen for operation mode and at lower part was the OLSR Routing (Optimized Link State Routing) which has new interface option. The “eth1” was selected from the drop down list and “eth1” has the same wireless interface as the Linksys wrt54gl router.



Firmware: DD-WRT v24-sp2 (08/07/10) micro
Time: 19:39:33 up 1:11, load average: 0.20, 0.05, 0.01
WAN IP: 192.168.0.101

Advanced Routing

Operating Mode

Operating Mode: OLSR Router

OLSR Routing (Optimized Link State Routing)

Gateway Mode: ● Enable ○ Disable
Host Net Announce:
Poll Rate: 0.1
TC Redundancy: 2
MPR Coverage: 7
Link Quality Fish Eye: ● Enable ○ Disable
Link Quality Aging: 0.1
Link Quality Level: 2
Hysteresis: ○ Enable ● Disable

eth1

Hello Interval: 5.0
Hello Validity Time: 90.0
TC Interval: 2.0
TC Validity Time: 270.0
MID Interval: 15.0
MID Validity Time: 90.0
HNA Interval: 15.0
HNA Validity Time: 90.0

New Interface: eth0

Dynamic Routing

Interface: Disable

Static Routing

Select set number: 1 ( )
Route Name:

Operating Mode:
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select *Router* mode.

Select set number:
This is the unique route number, you may set up to 50 routes.

Route Name:
Enter the name you would like to assign to this route.

Destination LAN NET:
This is the remote host to which you would like to assign the static route.

Subnet Mask:
Determines the host and the network portion.

Figure 5.10: Choosing OLSR Router operating mode and adding the eth1 interface to the OLSR configuration

5.6 Enabling NAT routing

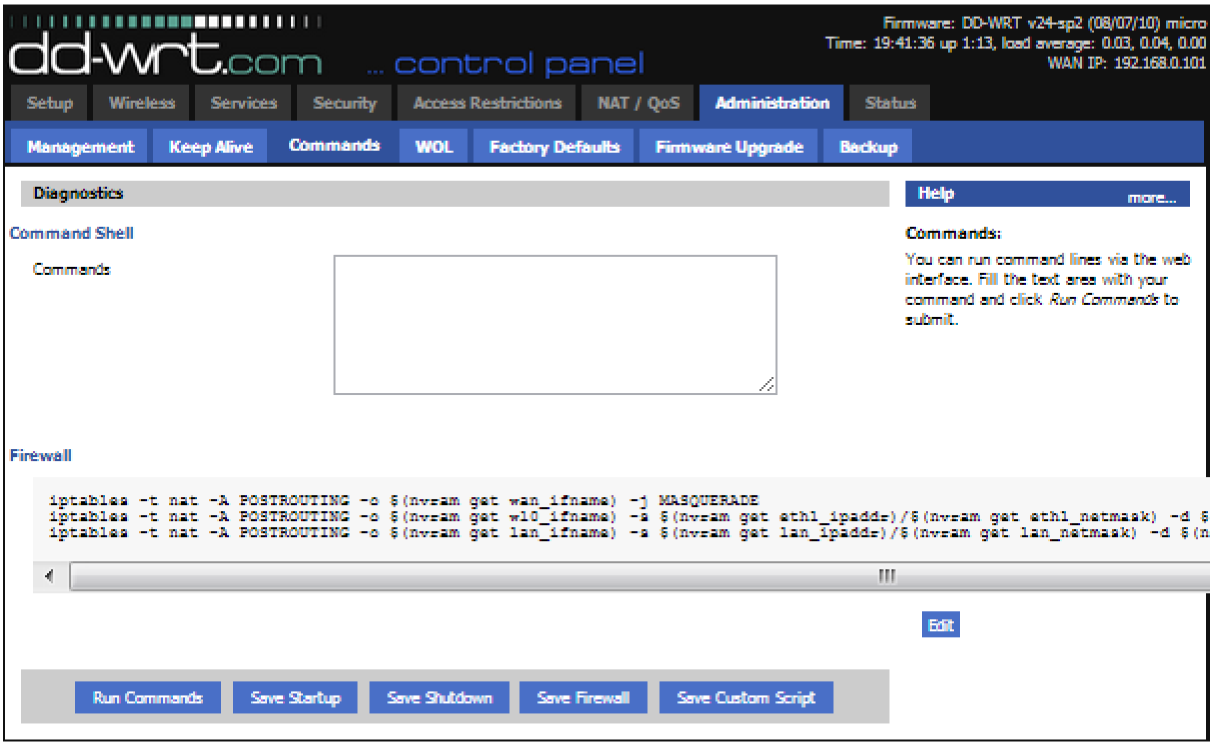
Each router in NAT routing is configured by default. Changing the advance routing operation mode to OLSR Router in order to perform optimized link state routing topology, it was set it to automatically turn off NAT routing in order to enable it. Turning the NAT back, these lines of script have to be input back to each router using an encryption.

iptables –t nat - A POSTROUTING - o $(nvram get wan_ifname) - j MASQUERADE

iptables –t nat – A POSTROUNTING - o $(nvram get wl0_ifname) - s $(nvram get eth1_ipaddr)/$(nvram get eth1_netmask) –d $(nvram get eth1_ipaddr)/$(nvram get eth1_netmask) - j MASQUERADE

iptable –t nat - A POSTROUTING - o $(nvram get lan_ifname) - s $(nvram get lan_ipaddr)/$(nvram get lan_netmasl) –d $(nvram get lan_ipaddr)/$(nvram get lan_netmask) – j MASQURADE

In the DD-WRT control plane, under administration click on commands appears an empty space, The above script were copied into the empty space and click on “Save Firewall”, which was performed on each router.



Firmware: DD-WRT v24-sp2 (08/07/10) micro
Time: 19:41:36 up 1:13, load average: 0.03, 0.04, 0.00
WAN IP: 192.168.0.101

Commands:

You can run command lines via the web interface. Fill the text area with your command and click *Run Commands* to submit.

```
iptables -t nat -A POSTROUTING -o $(nvram get wan_ifname) -j MASQUERADE
iptables -t nat -A POSTROUTING -o $(nvram get wl0_ifname) -s $(nvram get eth1_ipaddr)/$(nvram get eth1_netmask) -d $
iptables -t nat -A POSTROUTING -o $(nvram get lan_ifname) -s $(nvram get lan_ipaddr)/$(nvram get lan_netmask) -d $(n
```

Figure 5.11. Enabling the NAT routing in OLSR Router operation mode

5.5.1 Computer Configuration

For the computers to be successfully connected and communicate with the routers, the author had to setup the static IP addresses on the same subnet as the router. Figure 5.9 shows how static IP addresses are configured on each of the computers.

Computer 1: IP address 10.1.1.25

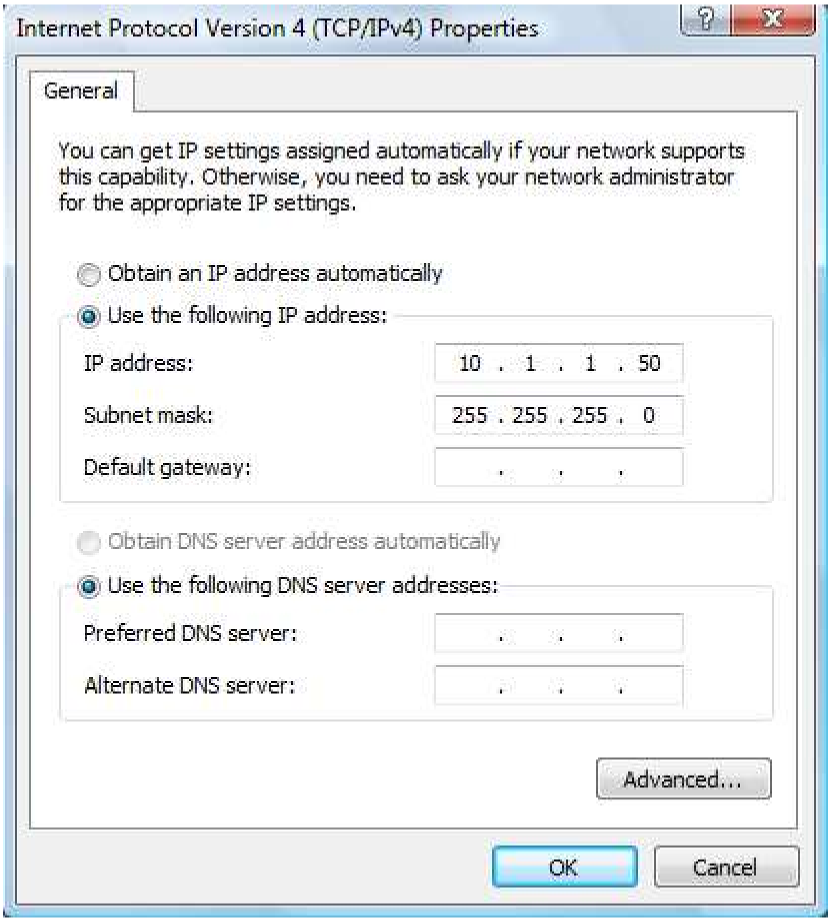
Subnet mask: 255.255.255.0

Computer 2: IP address 10.1.1.65

Subnet mask: 255.255.255.0

Computer 3: IP address 10.1.1.50

Subnet mask 255.255.255.0



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 1 . 1 . 50

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

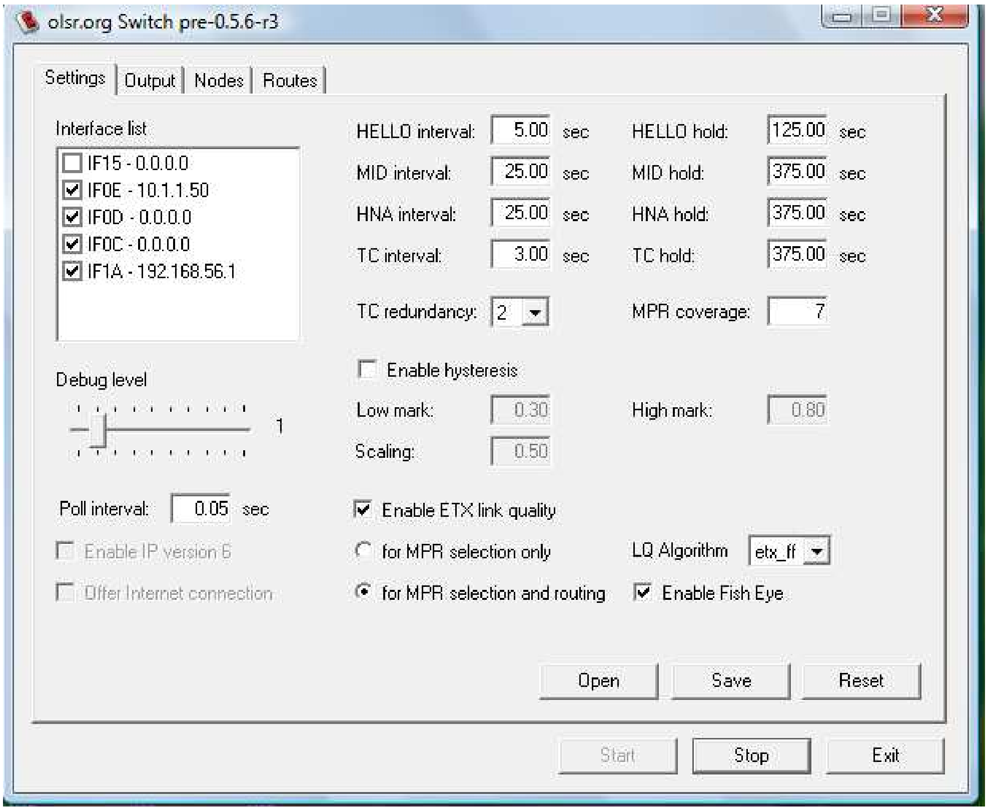
Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 5.12. Setting up a static IP

5.7 OLSR IMPLEMENTATION

Monitoring the mesh routing on each computer, the free window version of the "olsrd-5.6 software" was downloaded and installed. This software is used for implementation of the OLSR protocol and it also allows mesh routing for different network equipment. After installation, each computer was re-booted which started the olsrd program. The interface that has the IP address was selected and the button "start" was clicked on. Figure 5.10 shows the setting up olsrd on the computer, Figure 5.11 display "logs for olsrd, Figure 5.12 display "nodes" discovery by OLSR protocol, and Figure 5.13 shows "routes" created by OLSR repectively.



Interface list
□ IF15 - 0.0.0.0
☑ IF0E - 10.1.1.50
☑ IF0D - 0.0.0.0
☑ IF0C - 0.0.0.0
☑ IF1A - 192.168.56.1

Debug level 1

Poll interval: 0.05 sec
□ Enable IP version 6
□ Offer Internet connection

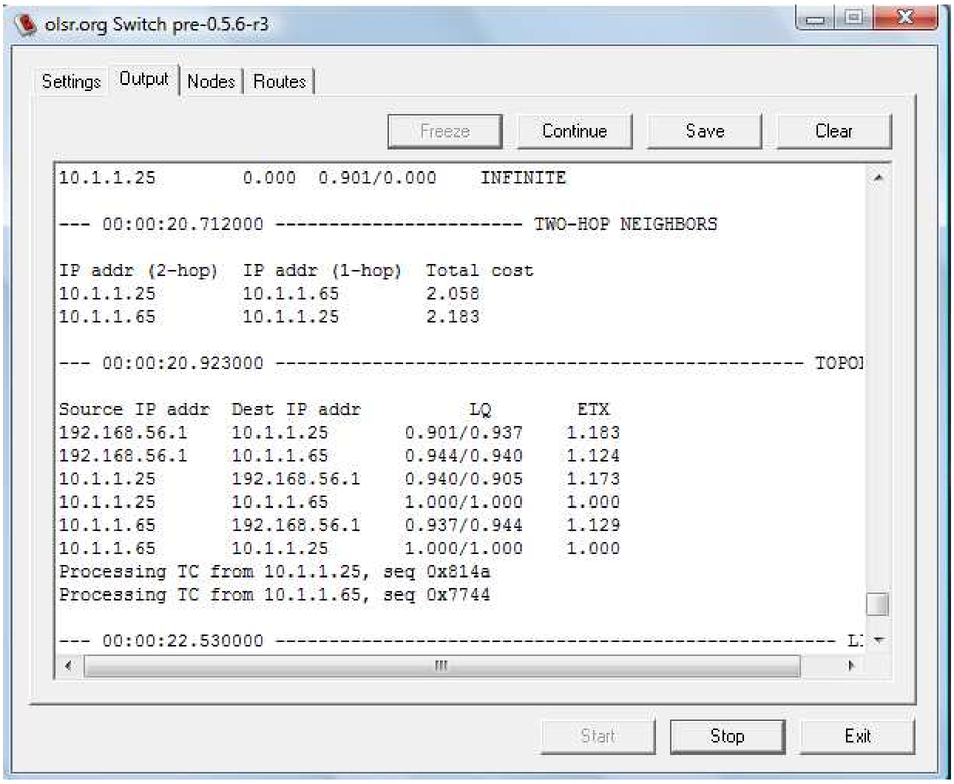
HELLO interval: 5.00 sec HELLO hold: 125.00 sec
MID interval: 25.00 sec MID hold: 375.00 sec
HNA interval: 25.00 sec HNA hold: 375.00 sec
TC interval: 3.00 sec TC hold: 375.00 sec

TC redundancy: 2 MPR coverage: 7

□ Enable hysteresis
Low mark: 0.30 High mark: 0.80
Scaling: 0.50

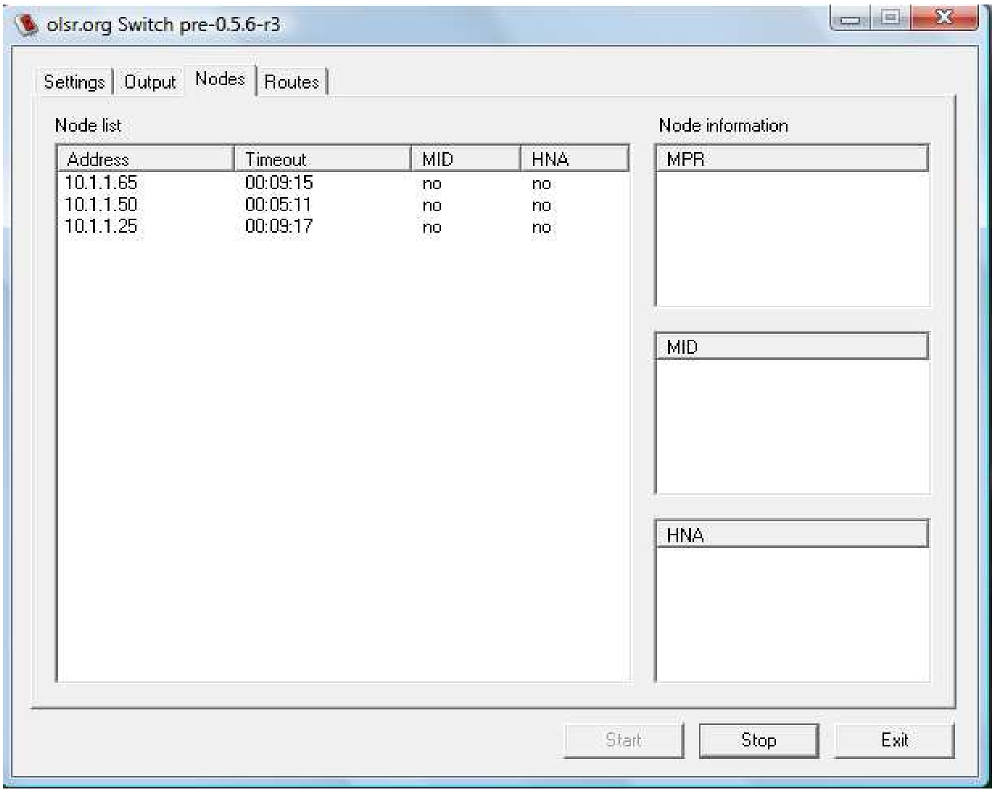
☑ Enable ETX link quality
○ for MPR selection only LQ Algorithm etx_ff
● for MPR selection and routing ☑ Enable Fish Eye

Figure 5.13. Setting up olsrd on the computer



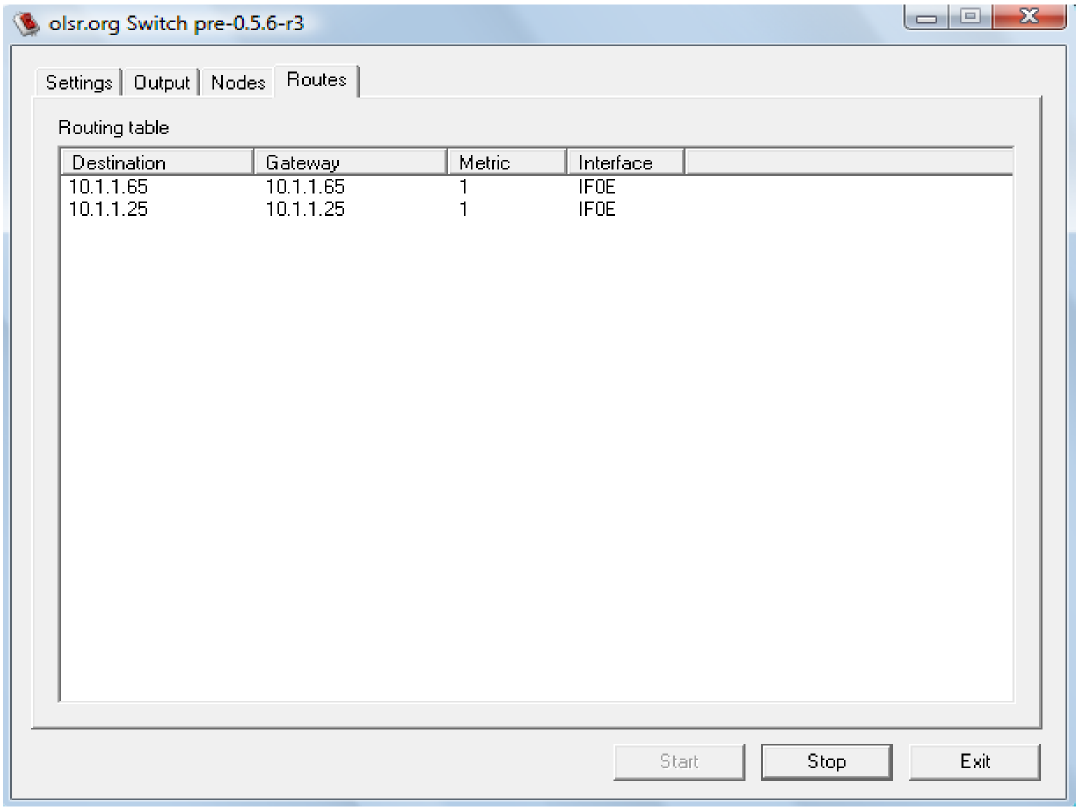
```
10.1.1.25        0.000  0.901/0.000    INFINITE

--- 00:00:20.712000 ----------------------- TWO-HOP NEIGHBORS

IP addr (2-hop)  IP addr (1-hop)  Total cost
10.1.1.25        10.1.1.65        2.058
10.1.1.65        10.1.1.25        2.183

--- 00:00:20.923000 ------------------------------------------------- TOPOI

Source IP addr  Dest IP addr          LQ        ETX
192.168.56.1    10.1.1.25       0.901/0.937    1.183
192.168.56.1    10.1.1.65       0.944/0.940    1.124
10.1.1.25       192.168.56.1    0.940/0.905    1.173
10.1.1.25       10.1.1.65       1.000/1.000    1.000
10.1.1.65       192.168.56.1    0.937/0.944    1.129
10.1.1.65       10.1.1.25       1.000/1.000    1.000
Processing TC from 10.1.1.25, seq 0x814a
Processing TC from 10.1.1.65, seq 0x7744

--- 00:00:22.530000 ---------------------------------------------------- LI
```

Figure 5.14. Logs for the olsrd



Address	Timeout	MID	HNA
10.1.1.65	00:09:15	no	no
10.1.1.50	00:05:11	no	no
10.1.1.25	00:09:17	no	no

Figure 5.15. Nodes discovered by the OLSR protocol



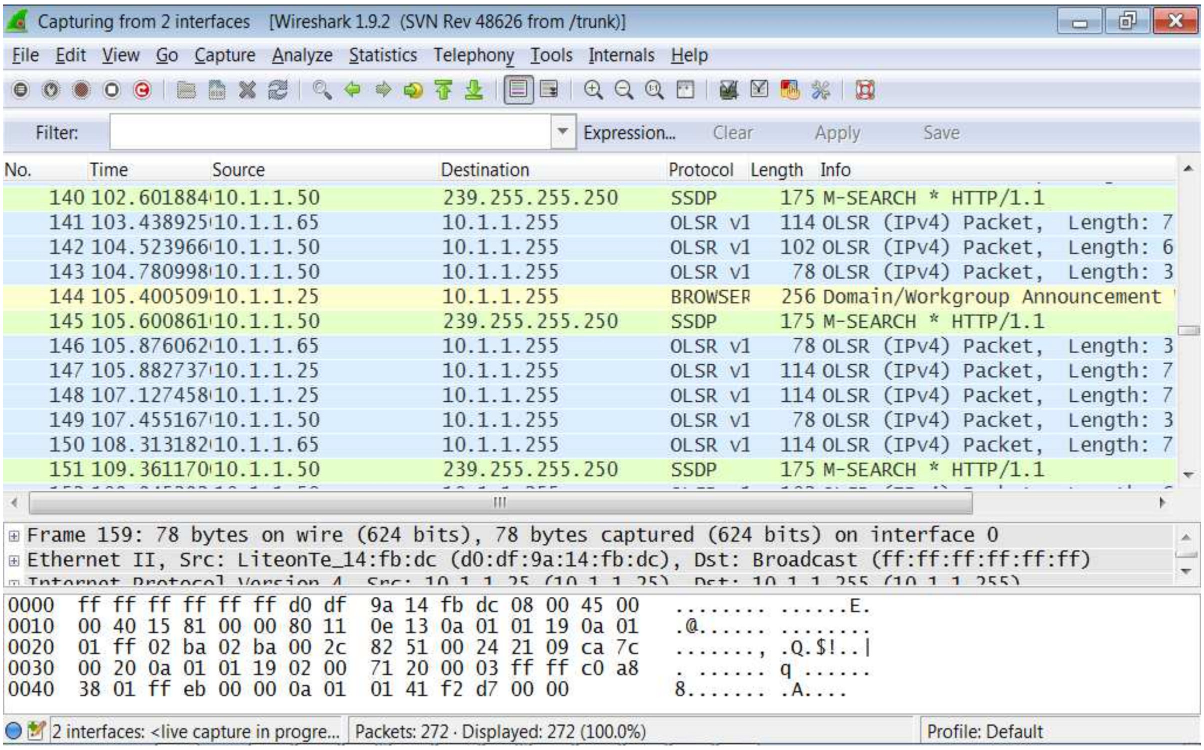
Routing table

Destination	Gateway	Metric	Interface
10.1.1.65	10.1.1.65	1	IF0E
10.1.1.25	10.1.1.25	1	IF0E

Figure 5.16: Routes created by OLSR

5.6.1 Performance Tests

The performance test was carried out after all the setup has been completed. Wireshark was used to test the network analysis to see how the OLSR packets are sent out to the broadcast address (10.1.1.255) as shown in Figure 5.14.


Capturing from 2 interfaces [Wireshark 1.9.2 (SVN Rev 48626 from /trunk)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
No.    Time          Source       Destination       Protocol   Length Info
   140 102.601884 10.1.1.50     239.255.255.250   SSDP          175 M-SEARCH * HTTP/1.1
   141 103.438925 10.1.1.65     10.1.1.255        OLSR v1       114 OLSR (IPv4) Packet,  Length: 7
   142 104.523966 10.1.1.50     10.1.1.255        OLSR v1       102 OLSR (IPv4) Packet,  Length: 6
   143 104.780998 10.1.1.50     10.1.1.255        OLSR v1        78 OLSR (IPv4) Packet,  Length: 3
   144 105.400509 10.1.1.25     10.1.1.255        BROWSER       256 Domain/Workgroup Announcement
   145 105.600861 10.1.1.50     239.255.255.250   SSDP          175 M-SEARCH * HTTP/1.1
   146 105.876062 10.1.1.65     10.1.1.255        OLSR v1        78 OLSR (IPv4) Packet,  Length: 3
   147 105.882737 10.1.1.25     10.1.1.255        OLSR v1       114 OLSR (IPv4) Packet,  Length: 7
   148 107.127458 10.1.1.25     10.1.1.255        OLSR v1       114 OLSR (IPv4) Packet,  Length: 7
   149 107.455167 10.1.1.50     10.1.1.255        OLSR v1        78 OLSR (IPv4) Packet,  Length: 3
   150 108.313182 10.1.1.65     10.1.1.255        OLSR v1       114 OLSR (IPv4) Packet,  Length: 7
   151 109.361170 10.1.1.50     239.255.255.250   SSDP          175 M-SEARCH * HTTP/1.1
```

```
⊞ Frame 159: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
⊞ Ethernet II, Src: LiteonTe_14:fb:dc (d0:df:9a:14:fb:dc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 10.1.1.25 (10.1.1.25), Dst: 10.1.1.255 (10.1.1.255)
```

```
0000  ff ff ff ff ff ff d0 df  9a 14 fb dc 08 00 45 00   ........ ......E.
0010  00 40 15 81 00 00 80 11  0e 13 0a 01 01 19 0a 01   .@...... ........
0020  01 ff 02 ba 02 ba 00 2c  82 51 00 24 21 09 ca 7c   ......., .Q.$!..|
0030  00 20 0a 01 01 19 02 00  71 20 00 03 ff ff c0 a8   . ...... q ......
0040  38 01 ff eb 00 00 0a 01  01 41 f2 d7 00 00         8....... .A....
```

```
2 interfaces: <live capture in progre...   Packets: 272 · Displayed: 272 (100.0%)   Profile: Default
```

Figure 5.17. Wireshark analyzing packets sent to the network.

6. LIMITATIONS AND CONCLUSION

In most wireless network, the performance of the protocols can be affected coupled with various factors such as the physical technology, the link-state layer behaviours, the choice of codes and errors which makes it hard to explain specifically the performance of a routing protocol.

This project illustrated the usefulness of various protocol used in mobile ad-hoc network. The optimized link state protocol was analysed to show how the protocol is actually behaves. However,many problems was encountered during the process of building a wireless mesh network used in testing the performance of OLSR protocol. In the Windows, olsrd switch was installed on each of the computer used as node. The operation olsrd switch shows how the routers and computers made used of multipoint relay (MPR) and multiple Interface declaration (MID) message in optimized link state routing (OLSR). With the Wireshark, it shown how the OLSR packet was sent out of port 698 (UDP) on the all computers but not on the routers.

It was discovered that on the olsrd switch “Node” tab shows no multipoint relay (MPR) for any of the IP interfaces (either computers or routers). With these result no computer can be calculated as next possible MPR through which the shortest route to another computer on the network, if one of the computer is down. After,much troubleshooting in the network the result still remains the same. Creating this mesh network on Linux environment should be the best option but due to difficulties faced, the author later switched to Windows environment for the analysis.

As explained by Phillippe Jacquet et. al (2000), “OLSR protocol which is proactive in nature, obviously favours a networking context in which all time-kept information is used more and more and where route requests for a new destinations are very frequent”. It can be assumed that the OLRS protocol is meant to be adapted to a network that is dense and communication is assumed to occur frequently between a large number of nodes to establish a continue network topology.

Furthermore, the protocol favours of an application which does not permit the delay for transmitting data packets. In other words, if the transmission is prone to error, there is high a probability that a correct packet received by the the intended destination will not be guaranteed which is a common problem to all ureliable communication network.

REFERENCES

Aishwarya, S., Ukey, A., & Chawla, M., 2010. “Detection Of Packet Dropping Attack Using Improved Acknowledgement Based Scheme In MANET”, IJCSI International Journal Of Computer Science Issue. Vol. 7, Issue 4, No 1,

Amitabh, M., 2000. “Security and quality of service in ad hoc wireless networks” Cambridge, UK: Cambridge University Press. pp 2-112

Andel, T.R. & Yasinsac, A., 2007 ”Surveying security analysis techniques in manet routing protocols” Communications Surveys & Tutorials, IEEE, 9(4)’ pp. 70-84 http://mars.cs.kent.edu/~peyravi/Bibs/Security/andel07.pdf,

Chlamtac,I., Conti, M., & Liu J., 2003, “Mobile ad hoc networking: imperatives and challenges”, Ad-hoc Networks, Elsevie. pp 13-64

Clausen, T. & Jacquet, P., 2003. “Optimized Link State Routing Protocol (OLSR)”. RFC 3626 (Experimental), October 2003

Cristian, P. & Festor, O., “WiMFlow: a distributed, self-adaptive Architecture for Flow Monitoring in Wireless Mesh Networks” http://hal.inria.fr/docs/00/52/60/06/PDF/62539_1.pdf., Accessed 19th February, 2013.

Erwan, E. & Muhlethaler, P. “Using OLSR Multipoint Relays (MPRs) to estimate node positions in a Wireless Mesh Network” http://hal.inria.fr/docs/00/12/15/42/PDF/RR-6072.pdf,. Accessed Feburary 2013

Flathagen, J., 2008. “Service Discovery in Mobile Ad-hoc Networks” Master thesis, University of Oslo, Sweden”, http://folk.uio.no/joakif/Flathagen_Thesis.pdf., Accessed December 2012.

Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A.,& Viennot, L., 2001, “Optimized link state routing protocol for adhoc networks” pp 62-68. www.cs.jhu.edu/~dholmer/600.647/papers/OLSR.pdf., Accessed March 2013.

Klein, J., 2005. “Implementation of an ad-hoc routing module for an experimental network” http://www.read.cs.ucla.edu/click/_media/klein05implementation.pdf., Accessed March 2013

Johnson, D.B., Maltz D. A., & Broch J., 2001. “The dynamic source routing protocol for multihop wireless ad hoc networks”. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.131.5263&rep=rep1&type=pdf, Accessed February 2013.

Linux Optimized Link State Routing Protocol (OLSR) IPv6 HOWTO http://www.linuxdoc.org/HOWTO/OLSR-IPv6-HOWTO/intro.html, Accessed December 2012

Misra, S., Woungang, I., & Misra S. C., 2009.Springer-verlag London limited, , pp 28-29 “Guide to Wireless Ad Hoc Networks”
OpenWrt Wireless Freedom https://openwrt.org/

OLSR, Optimized Link State Protocol, http://www.networksorcery.com/enp/protocol/olsr.htm# Accessed January 2013

Padmavathi, G., Subashini, P. & , A. D., 2010. “Hybrid Routing Protocols To Secure Network Layer For Mobile Ad Hoc Networks”. IEEE

Perkins, C. E. & Bhagwat, P.1994. “Highly Dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers Communications architectures, protocols and applications” (SIGCOMM '94). ACM, New York, NY, USA. DOI=10.1145/190314.190336. pp. 234-244, http://doi.acm.org/10.1145/190314.190336 Accessed February, 2013.

Perkins, C.E. & Royer, E.M.,1999. Ad-hoc on-demand distance vector routing. Mobile Computing Systems and Applications". Proceedings. WMCSA '99. Second IEEE Workshop. pp.90-100. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=749281, Accessed February 2013.

Pucha. H., Das, S. M. & Hu Y.C., 2007. "The Performance Impact of Traffic Pattern on Routing Protocols in Mobile Ad Hoc Network", (COMNET). Vol. 51(12), pp 3595-3616

Qasim, N., Fatin, S., & Hamid, A., 2008. " Mobile Ad Hoc Networks Simulations Using Routing Protocols for Performance Comparisons" http://www.iaeng.org/publication/WCE2008/WCE2008_pp787-792.pdf, Accessed 24 March, 2013

Qayyum, A., 2000. , "Analysis and Evalution of Channel Access Schemes and Routing Protocols in Wireless LANs". PhD thesis, Universite de Paris-sud, France

Shuhui, Y., Wu, J., & Jiannong, C., "Connected k-Hop Clustering in Ad Hoc Networks" http://repository.lib.polyu.edu.hk/jspui/bitstream/10397/845/1/connected-hop_05.pdf. Accessed November 2012

Sunil, K., Vineet, R.S. & Jing, D. "Medium Access Control protocols for ad hoc wireless networks: a survey" http://www.ece.gatech.edu/research/labs/bwn/ee6610/supplements/adhocmac.pdf. Accessed March 2013

The history of mobile ad-hoc networks http://zatz.com/computingunplugged. Accessed November 2012

Tokekar, M. & Radhika, J. D., 2011. “Enhancement of Optimized Linked State Routing Protocol for Energy Conservation” CS & IT-CSCP 2011. http://airccj.org/CSCP/vol1/csit1228.pdf. Accessed November 2012

Tonnesen, A. 2004. “Implementing and extending the Optimized Link State Protocol”,. www.olrs.org/docs/report.pdf, Accessed 3rd November 2012.

Ullah, I., & Ur Rehman, S., 2010. "Analysis Of Black Hole Attack On Manets Using Different MANET Routing Protocols” Program Electrical Engineering With Emphasis On Telecommunication, Type Of Thesis-Master Thesis, Electrical Engineering, Thesis No : MEE-2010-2698.

Wang, M., & Qian, C. “More Efficient Routing Algorithm for Ad Hoc Routing Algorithm” http://www2.ensc.sfu.ca/~ljilja/ENsSC835/Fall03/Projects/qian_wang/Report.pdf. Accessed March 2013

Wolf, A., 2012. “A performance analysis of the optimized link state protocol using voice traffic over mobile ad hoc network” http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA556301&Location=U2&doc=GetTRDoc.pdf., Accessed February 2013

Zhu,W., 2009. “Multipoint Relay Flooding: Network Coding Improvements” Masters’ Thesis, http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/090421-Wanning_Zhu-with-cover.pdf, Accessed November 2012