OSPF FOR WIRELESS MESH BACKBONE NETWORK

by

Ali Mohsen Alwan

B.Sc. in Computer Engineering
University of Technology, Iraq, 1991

A thesis
presented to Ryerson University to the
in partial fulfillment of the
requirements for the degree of
Master of Applied Science
in the Program of
Computer Networks

Toronto, Ontario, Canada, 2006

Author's Declaration

I hereby declare that I am the sole author of this thesis.

I authorize Ryerson University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Abstract

Ali Mohsen Alwan, OSPF for Wireless Mesh Backbone Network.
M.A.Sc., Computer Networks, Ryerson University, 2006.

Wireless mesh network (WMN) is popular for providing decentralized and relatively inexpensive Internet access, especially in Community network and geographically challenged areas of deployment. In this thesis, we proposed using OSPF as the underlying routing protocol in the Wireless Mesh Backbone (WMB) network. We investigated the convergence and configuration issues of OSPF in WMB network. We evaluated the performance of OSPF and compared with AODV (reactive ad hoc protocol) and OLSR (proactive ad hoc protocol). We proposed using multiple subinterfaces under a single physical wireless interface in configuring multiple subnets to deal with the hidden nodes problem in WMB networks. We also proposed using the BGP protocol to interconnect multiple OSPF areas for the sub-urban topology. The performance of this approach in terms of convergence time was studied.

Acknowledgements

I am grateful to my supervisor, Dr. Muhammad Jaseemuddin, for his guidance and assistance throughout this research. The suggestions and ideas Dr. Jaseemuddin raised during our meetings were highly beneficial and very much appreciated. Also I would like to thank Dr. Bobby Ma for his advice and support. Finally, I want to give my gratitude to my family my mother, father, sister, brother and to my friends, for their support and encouragement.

Content

List of Figures

List of Tables

List of Appendices

Chapter One - Introduction

Behind the exponential growth of the Internet technologies evolution is the desire to build a better environment for Internet access with the convenience and flexibility to reach out to communities in urban areas. This type of Internet access requires a decentralized infrastructure and must be relatively inexpensive, reliable and resilient.

We observe that wireless networking is the most attractive trend that has been discussed and developed for decades. Internet users are no longer sitting in front of desktops. Instead, they are carrying wireless mobile devices. Connecting to the Internet has become a new phase of network communication.

Two major wireless technologies are cellular networks and Wireless Local Area Networks (WLANs). Wireless Mesh Networks (WMNs) is mesh networking implemented over a Wireless LAN. This type of Internet infrastructure is decentralized, relatively inexpensive, very reliable and resilient [1] as each node needs only transmit as far as the next node, as shown in figure 1-1, which illustrates a community wireless mesh network. [13].

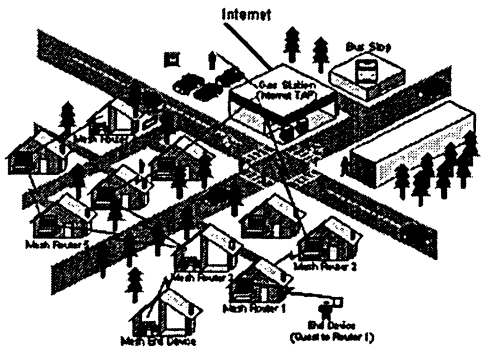

Figure 1-1: Community wireless mesh network

WMNs have been undergoing rapid commercialization in many application scenarios such as broadband home networking, community networking, building automation, high-speed metropolitan area networks and enterprise networking. WMN wireless networking solutions are less costly to deploy, wireless cell phone circuits have become popular and the public has already accepted wireless networks as an alternative to wired. Furthermore, WMS has found popularity due to its effectiveness in challenging geographical regions such as the development project in San Francisco [20].

Figure 1-2 illustrates a typical wireless mesh network with a number of Wireless Mesh Routers (WMRs) providing connectivity between the mobile nodes and wired Internet connections.

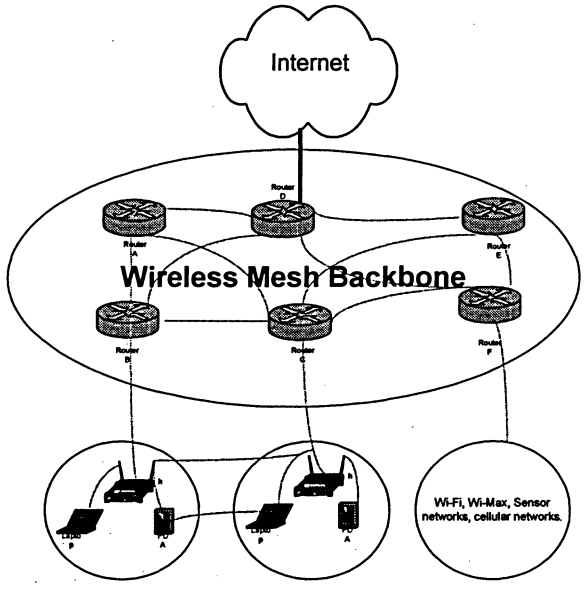

Figure 1-2: Backbone wireless mesh routers

Fixed wireless mesh routers form the backbone of WMN. Some of these WMRs are stationed at the edge of the wireless mesh backbone

connecting the wireless network with the wired network (e.g. Router D in Figure 1-2). Routers like B, C and F in Figure 1-2 are acting as access mesh routers (AMRs) which provide connectivity between wireless clients (mobile nodes) and the wireless mesh backbone network. This in turn provides access to the Internet via the wired network (in this case router D is a gateway to internet).

There are many factors affecting routing in WMN's including noise, number of hops, and interference with other radios. Routing proposals for WMN use some forms of ad-hoc routing with more innovative metrics to reflect wireless link conditions. (e.g. ETX [3] or WCETT [5]). For the purpose of this thesis we focus on routing within the WMN backbone network with fixed WMRs.

Four issues were studied:
Hidden nodes, which are out of range of other nodes or a collection of nodes. This issue is common in wireless network. We proposed a solution by creating multiple subnets using the subinterfacing configuration [1].
Different routing protocols were studied to select an appropriate one for the WMN backbone. We investigated three routing protocols: AODV, OLSR and OPSF. Our studies showed that OPSF is the most suitable protocol to use in WMN.
We examined factors affecting network convergence in two popular WMN settings (Campus and suburban WMNs).
We proposed to deploy the BGP protocol to interconnect OSPF areas for the sub-urban topology. The convergent time of the proposed solution was studied.

The remaining four chapters of this thesis are organized in the following order:

Chapter Two contains a review of related work done in various areas related to the thesis and presents the literature that was used to support the work.

In Chapter Three we present solutions for different scenarios in the Wireless Mesh Network.

In Chapter Four we present simulation and results for our proposed solutions for different scenarios in the Wireless Mesh Network.

Chapter Five summarizes the thesis and provides a conclusion with future work.

Chapter Two – Literature Review

Recently, Wireless Mesh Networks (WMNs) have become popular because of the fact that they can be deployed in area of difficult terrain. They are dynamically self-organized and self-configured. In a WMN a number of fixed wireless routers form the backbone network, which carries user traffic from the source to the destination. The fixed wireless routers are called Wireless Mesh Routers (WMRs). User terminals, called Mobile Nodes (MNs), are connected to WMRs through access links. A major benefit of wireless mesh networks is path diversity, which provides many routes to the destination. In the case that one of the routers fails or its transmission path is temporarily blocked, other routes can be used.

WMN has been the topic for research in the wireless research community in the past few years. Microsoft has made a major contribution to WMNs by developing a WMN architecture and implementing in the test environment, and making it available to the research community [13]. Researchers in Microsoft have created wireless technologies that allow neighbors to connect their home networks together through the community WMN. There are many advantages to enabling such connectivity and forming a community mesh network. For example, when enough neighbors cooperate and forward each others packets, they do not need to individually install an Internet "tap" (gateway), but instead can share faster, cost-effective Internet access via gateways that are distributed in their neighborhood. Packets dynamically find a route, hopping from one neighbor's node to another to reach the Internet through one of these gateways. Another advantage is that neighbors can cooperatively deploy backup technology and never have to worry about losing information due to a catastrophic disk failure. A third advantage is that this technology allows localization of communication by connecting

source and destinations within the community through the same community network without going through a service provider and the Internet. Neighborhood community networks allow faster and easier dissemination of cached information that is relevant to the local community. MIT RoofNet team [14] have deployed WMN in real life scenario in their RoofNet project where they have placed many Wireless Mesh Routers in different areas in the city of Cambridge. Roofnet is an experimental 802.11b/g mesh network in development at MIT CSAIL which provides broadband Internet access to users in Cambridge. There are currently around 20 active nodes in the network.

2.1 Mesh Access

A Wireless Access point (WAP) or an Access Point (AP) is a node that provides wireless access link to mobile nodes on one side and connecting to backbone network on the other side, where backbone could be Ethernet, wireless, ATM etc and acts as a central transmitter and receiver of WLAN radio signals. Figure 2-1 illustrates a number of mobile nodes communicating with an access point that provides connectivity to an Ethernet backbone network, which in turn provides access to Internet. In the Figure doted lines are wireless connectivity and solid line is wired connectivity.

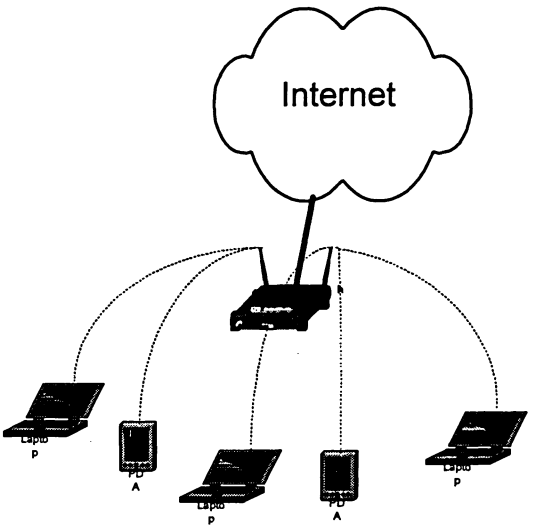

Figure 2-1: Access point providing communication to Mobile nodes to internet

A Collection of access points forms mesh network where they communicate among each other and with mobile nodes. Although mobile nodes in very small IEEE 802.11 WLANs can function without access points in so-called "ad hoc" or peer-to-peer mode, access points support "infrastructure" mode. The infrastructure mode bridges WLANs with a wired Ethernet LAN and also scales the network to support more clients (mobile notes). Figure 2-2 illustrates a number of mobile nodes communicate with two access points that provide connectivity either to the backbone network or to other mobile nodes by using one of AD-HOC routing protocols such as AODV (Ad-hoc On Demand Vector), DSR (Dynamic Source Routing) and OLSR (Optimized Link State Routing) . An example of the campus wireless networks is the one at University of Tennessee developing a large scale wireless network using access points were 1200 access points installed across 15 million square feet using 802.11b [7]

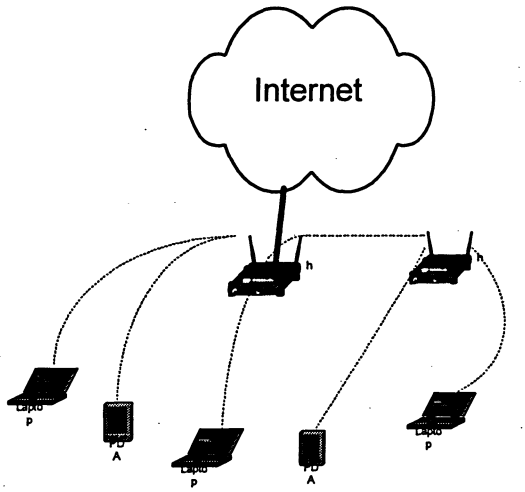

Figure 2-2: Multiple access point providing internet connectivity

2.2 WMN Types

A WMN comprises of two types of nodes: mesh routers and mesh clients (mobile nodes).

Mesh router contains additional routing functions to support mesh networking, where as conventional routers supports routing capability for gateway/bridges functions. Mesh router usually equipped with multiple wireless interfaces built on either same or different wireless access technologies. Mesh and conventional routers are usually built based on a similar hardware platform. Mesh routers are fixed and form mesh backbone for mesh clients [8].

WMN architectures are classified in three types: Infrastructure /backbone WMN, Client WMN and Hybrid WMNs.

2.2.1 Infrastructure/Mesh Backbone WMN

Mesh wireless backbone networks, expand WLAN access beyond traditional hotspot areas, enhancing coverage and offering true seamless mobility. However, as WLANs signal coverage and radio link speed improve, it is conceivable that WLAN deployment will inch toward some

enterprises core backbone, eventually turning the enterprise into a truly wireless computing environment. Mesh routers in this architecture form an infrastructure for clients, as shown in figure 2-3, where dashed lines are wireless links and solid lines are wired links. In this architecture various types of radios can be used beside IEEE 802.11 technologies. Mesh routers forms self-configuration and self-healing among themselves, and they connect to Internet by their gateway functionality. This approach also referred to as infrastructure meshing, provides a backbone for conventional clients and enables integration of WMNs with existing wireless network, through gateway/bridge functionalities in mesh routers. Conventional clients with Ethernet interface can connect to mesh routers via Ethernet links. Conventional clients with the same radio technology as mesh routers can directly communicate with mesh routers. Conventional clients with their radio technologies must communicate with their base stations that have Ethernet connections to mesh routers.

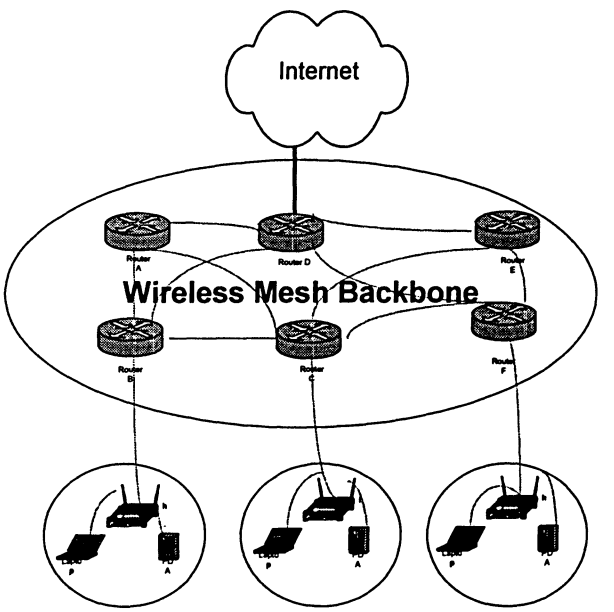

Figure 2-3: Infrastructure mesh router architecture

Wireless mesh backbone uses a set of wireless routers, which are in turn a network device that combines a wireless access point (base station), a wired LAN switch and a router with connections to a cable or DSL service. Wireless routers provide a convenient way to connect a small number of wired routers and any number of wireless computers to the Internet.

2.2.2 Client WMN

Client meshing is to form a peer-to-peer network among client devices. In this architecture, client nodes perform routing and end configuration functionalities as well as providing end-user applications to customers. Therefore, as shown in Figure 2-4, mesh routers are not needed in this architecture. Client WMNs are usually formed using one type of radio technology on devices. Thus, a Client WMN is actually the same as a conventional ad hoc network.

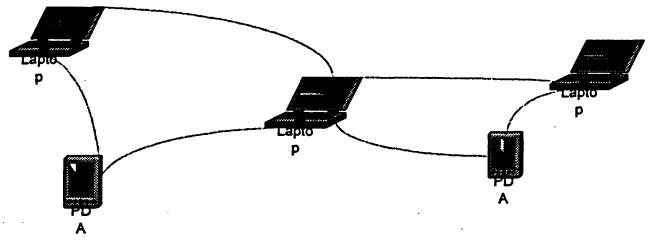

Figure 2-4: Peer-to-peer wireless network

2.2.3 Hybrid WMN

This architecture is a combination of infrastructure and client meshing, as shown in figure 2-5. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, Cellular, and senor networks. The routing

capabilities of clients provide improved connectivity and coverage inside WMNs.

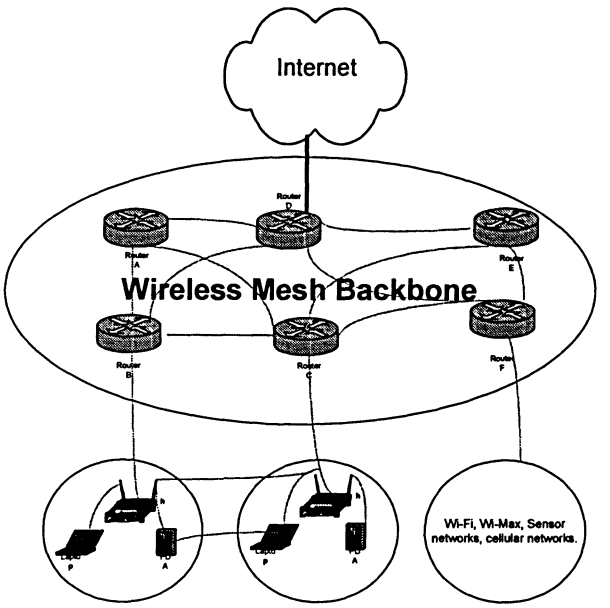

Figure 2-5: Infrastructure and peer-to-peer wireless connectivity

Hybrid architecture comprises all the advantages of WMN, as outlined below:

WMNs support ad hoc networking, and have capability of self-forming, self-healing, and self-organization.

WMNs are multi-hop wireless networks, but with wireless infrastructure /backbone provided by mesh routers.

Mesh routers perform dedicated routing and configuration, which significantly reduces the load of mesh clients and other end nodes.

Mobility of end nodes is supported easily through wireless infrastructure.

Mesh routers integrate heterogeneous networks, including both wired and wireless. Thus, multiple types of network access exist in WMNs.

2.3 Routing protocols

In multipath routing network traffic is split among two or more possibly disjoint paths in order to reduce latency, improve throughput, and balance traffic loads [6]. Once the control plane establishes multiple routes, a policy is needed for efficiently splitting traffic among the selected paths.

The IEEE 802.11 technology also provides ad hoc mode of operation in addition to the infrastructure mode. Mobile Ad Hoc Networks (MANETs) are characterized by infrastructure-less configuration and on-demand routing. A mobile node in MANET acts both as a router to forward the packets and as a host to generate the packets. Multi-hop communication in MANET further enhances the networking environment where users can access the Internet anywhere at anytime through their neighbors. MANET allows users to exchange information in a wireless environment without the need for a fixed infrastructure. Each user (or node), equipped with one or more radios, is free to roam about while communicating with others. The path between any pair of users can traverse multiple wireless links and the radios themselves can be heterogeneous, thus enabling an assortment of different types of links to be part of the same adhoc network.

Routing protocols are divided into two groups: reactive and proactive. Proactive protocols, or table driven protocols like DSDV [16] and OLSR [17] keep routes in routing tables, and periodically refresh them; therefore, in keeping an updated routing table in the routers, they run control traffic periodically. Reactive protocols, such as AODV [18] and DSR [19], on the other hand work on a need-driven basis, where a route discovery is only initiated based on-demand when a packet is available for transmission. Microsoft has developed Link Quality Source Routing

(LQSR) protocol for wireless mesh networks. LQSR, was developed to be used with Microsoft Mesh Connectivity Layer (MCL) technology, which facilitates the interconnection of computers into a mesh network using WiFi or WiMAX wireless service. The LQSR protocol is based on Dynamic Source Routing (DSR).

Wireless mesh networks using MCL technology hold promise for people in remote areas who have not previously had access to high-speed Internet services. Such a network can be connected to the Internet by a single leased, broadband T-1 or satellite connection, thereby providing Internet access over a significant geographical area without the need for an existing cable or wire infrastructure among the nodes.

In this thesis, we propose using OSPF (Open Shortest Path First)for the WMN backbone network. We also explore the role of BGP in connecting small OSPF domains in a large WMN.

The impact of performance metrics on routing protocols was studied in [5] where link quality source routing LQSR selects a routing path according to link quality metrics. Three performance metrics, i.e. expected transmission counts ETX, per-hop round trip time RTT, and per-hop packet pair, are implemented separately. The performance of the routing protocol with these performance metrics is compared with the method using minimum hop count. For stationary nodes WMNs, ETX achieves the best performance, while the minimum hop-count outperforms the three link quality metrics when MNs are mobile. This illustrates that the link quality metrics used in [5] are still not enough for WMNs when mobility is concerned.

For WMNs using multiple radios, A Multi-Radio LQSR is proposed in [9], where a new performance metric, called weight cumulated expected transmission time (WCETT), is incorporated. WCETT takes into account both link quality metric and the minimum hop count and achieves good trade off between delay and throughput. MR-LQSR assumes that all radios on each node are tuned to non-interferening channels with the assignment changing infrequently.

The main objectives of using multi path routing are to perform better load balancing and to provide high fault tolerance. Multiple paths are selected between source and destination to achieve the above objectives. When a link is broken on the path due to a bad channel quality or mobility, another path in the set of existing paths can be chosen, without requiring of setting up a new routing path and consequently the end-to-end delay, throughput, and fault tolerance can be improved. However, given a performance metric, the improvement depends on the availability of node-disjoint routes between source and destination [8].

In hierarchical routing a certain self-organization scheme is employed to group network nodes into clusters. Each cluster has one or more cluster heads. Nodes in a cluster can be one or more hops away from cluster head. Since connectivity between clusters is needed, some nodes can communicate with more than one cluster and work as a gateway. When node density is high, hierarchical routing protocol tend to achieve much better performance because of less overhead, shorter average routing path, and quicker set-up procedure of routing path. However, complexity of maintaining the hierarchy may compromise the performance of the routing protocol. Moreover, in WMN, a mesh client must avoid being a cluster head because it can become a bottleneck due to its limited capability.

In contrast to topology-base routing scheme, geographical routing schemes forward packets by only using position information of the nodes in the vicinity and the destination node [10]. Thus, a topology change has less impact on the geographic routing than the other routing protocols. Early geographic routing algorithms are type of single-path greedy routing scheme in which the packet forwarding decision is made based on the location information of the current forwarding node, its neighbors, and the destination node. However, all greedy routing algorithms have a common problem, i.e., delivery is not guaranteed even if a path exists between source and destination. In order to guarantee delivery, planar-graph-based geographic routing algorithms [10] have been proposed recently. However, these algorithms usually have much higher communication overhead than the single-path greedy algorithms.

Network convergence is the time taken by all the routers (running OSPF/AODV/BGP) in the network to go back to steady state operations after there is a change in the network state. For example, if introducing a new router to stable network new hello messages will be exchanged with other routers, which force each router to recalculate their routing tables. Thus all the routers in the steady state spent this time on recalculating shows new convergence time for the network. Similarly when one or more routers disappear from network due to link or their operational failures, they start new convergence. There are many factors that effect convergence calculation i.e. number of routers, distance between routers, bit error rate, network diameter.

Chapter Three – Proposed Solutions

In this thesis we propose using OSPF in the wireless mesh backbone network. Several existing WMNs use a variation of ad hoc routing protocol in their backbone, e.g. Microsoft [22] and MIT [14]. However, some commercial WMRs employ OSPF in the WMN backbone, e.g. Nortel [21]. In this chapter, we first compare the performance of OSPF with OLSR (proactive protocol), and with AODV (reactive protocol) in terms of their convergence time, routing overhead and average response time This analysis puts in perspective the use of OSPF in the backbone. The OSPF usage must address two issues: one, formation of multiple broadcast zones on a single interface due to hidden node problem in wireless links; and two, the constraint of single backbone OSPF area that is not suitable for long topology where OSPF areas form a chain, e.g. along a long street. In this thesis we propose a solution for each of those issues. We evaluate the performance of our proposed solutions in Chapter 4 through simulation.

3.1 Single physical wireless interface

In this thesis, we propose a scheme of configuring single physical wireless interface to handle multiple subnets and routing protocol. Due to hidden node problem, all the neighbors connected through a single interface do not form a single broadcast zone, which is they all are not visible to each other, shown in figure 3-1 [1].

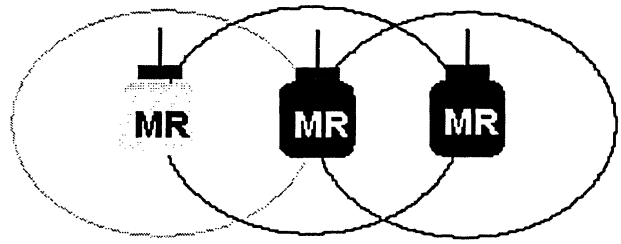

Figure 3-1: Transmission Range Diagram

Hence, we propose of creating as many subinterfaces as the broadcast zone attached to a single interface of a WMR. We treated each subinterface as a virtual standalone physical interface, i.e. it can be configured on a different subnet with different OSPF circuit. Should we configure a subinterface as point to multipoint or broadcast? Since, the current OSPF standard implementations do not support multiple broadcast networks to be configured on a single physical interface, we used a mesh of point-to-point to simulate a broadcast network. Figure 3-2 illustrates the proposed configuration of subinterfaces; where IF0 is the physical interface, IF01 is the first subinterface, and IF02 is the second subinterface of the physical interface IF0.

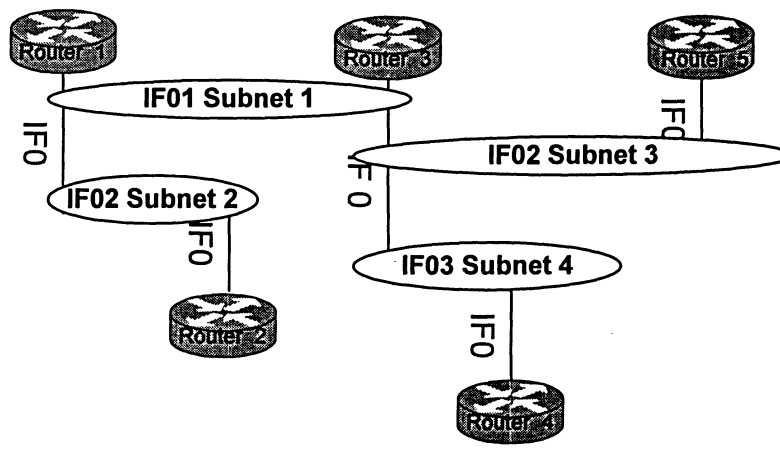

Figure 3-2: Subinterface configuration on single wireless interface

3.2 Comparison Between AODV, OLSR and OSPF for Backbone Routing

Since some research test-beds have used variations of ad hoc routing protocols, which are designed to deal with issues related to wireless links, it is important to compare the performance of OSPF with some representative ad hoc routing protocols. We chose OLSR and AODV to represent proactive and reactive class of ad hoc routing protocols. We compared the performance of AODV and OSPF on three measures: number of network convergence events, response time, and routing control overhead. We measured responses time, control traffic and number of replies received for comparing performance of OSPF with OLSR.

3.2.1 Network Convergence Time

As defined in chapter two, network convergence time is the time taken by all the routers (running OSPF/ BGP) in the network to reach steady "stable" state of operations after all routers started; whereas in AODV it is the length of time of route. Network convergence time includes any changes that might happen in the network state e.g. one link fails; a new router is introduced in the network, which would trigger route discovery and self-healing etc.

In case of using link state OSPF (Open Shortest Path First) protocol an action to build routes across network is done by exchanging hello packets between OSPF enabled interfaces. Hello packets are responsible for discovering new neighbors, carries number of parameters on which two routers must agree on to become neighbor, ensures a bi-directional

communication messages between routers and elects designated router (DR) and backup designated router (BDR) on broadcast networks. After adjacencies are established, each router sends link state advertisements (LSAs) over to all adjacencies. LSAs describes all of the router's links, each receiving router record LSA in link state database and send a copy of the LSA to all of its other neighbors, by flooding LSA throughout network (OSPF enabled interfaces) all routers will have identical link state database and each router will have full picture of which router is live (OSPF interface) in the network. Using database each router will start the shortest path first (SPF) algorithm to calculate best routes based on cost, then routing table will be built for each router based on SPF tree. When a network link state changes such as shutting down one of OSPF interfaces or enabling a new OSPF interface, unstable interface conditions and interference, all routers exchange new LSAs, then all they will run the SPF algorithm on the revised database and install any change in the forwarding table. At this point all routers will reach steady state. The time spent on recalculating and reaching steady state is the new convergence time for the network, there are many factors effect convergence calculation i.e. number of routers, distance between routers, bit error rate, network diameter. The lower convergence time is, more stable network is.

In contrast to OSPF in AODV, routes between nodes are established after on-demand traffic triggers request from source to destination, then AODV protocol will start to build routes using a route request/ route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across nodes in network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the routing tables. In addition to the source node's IP address, current sequence number, and broadcast ID,

the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ, which they have already processed, they discard the RREQ and do not forward it. AODV maintains routes it discovered as long as there are data packets following from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery

In this section we take a close look at WMN running OSPF protocol and AODV. For both protocols we measure network convergence time for the entire network after all routers performed routes discovery, built final routing table, and made route selection. This also includes the routes setup after network disturbance is introduced like adding new router(s) or link failure between two routers.

We used Bloor Street scenario used for this comparison, where a set of twelve routers with single wireless interface and 5mW of transmission power are configured in two rows with 650 meters distance between each router that covers a rectangular area of three kilometers length and 650 meters width are shown in figure 3-3. The duration of simulation is four minutes.

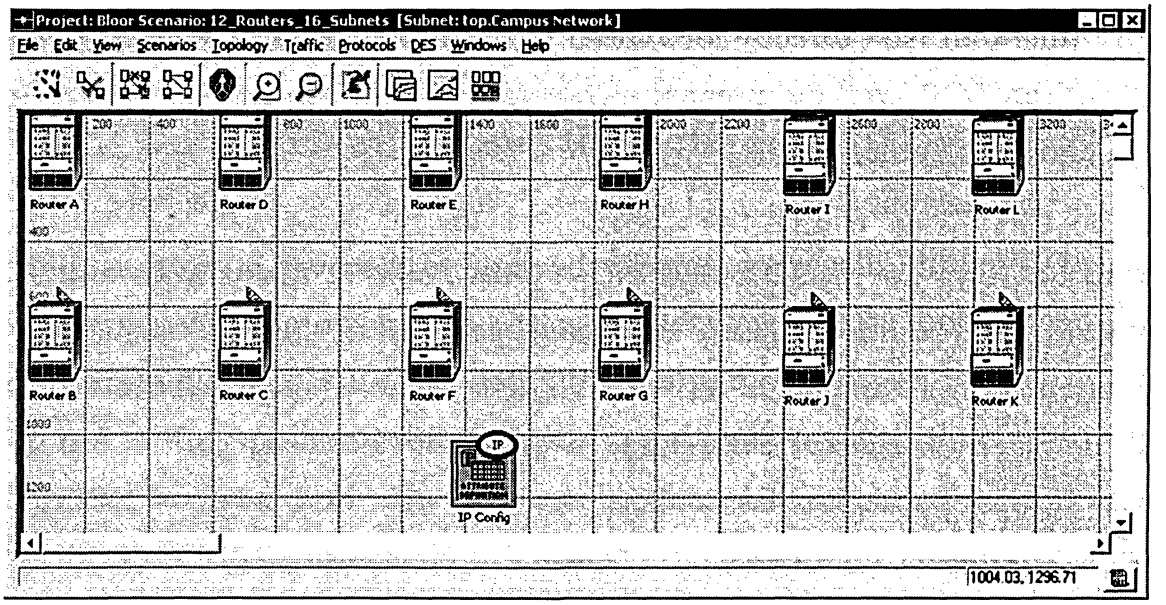

Figure 3-3: 12 routers Bloor Street scenario (suburban topology)

In this scenario, there are three types of Network convergence time: IP network convergence duration, OSPF network convergence duration, and AODV route discovery time.

IP Network Convergence Duration is the length of the time intervals during which convergence of the network's IP forwarding tables has been achieved.

OSPF Network Convergence Duration is the duration of convergence cycles for the OSPF routing tables across the whole network i.e. all routers with OSPF active interfaces have built their own OSPF database and no further changes occurs if change occurs then there would be another convergence time for that change.

The two statistics are looking at two different, although related, activities. The IP Convergence Duration is looking at the convergence activity of the IP Route Table while the OSPF Convergence Duration is looking at the

convergence of the OSPF Table. Therefore, if there is activity in the OSPF table that isn't directly forwarded to the IP Route Table, then the two will differ. OSPF will do internal calculations before the change is sent to the IP Route Table,

AODV route discovery time is the time to discover a route to a specific destination. More specifically, it is the time when a route request is sent out to discover a route to a destination until the time the corresponding route reply is received with a route to that destination.

OLSR operates as a table driven and proactive protocol, thus exchanges topology information with other nodes of the network periodically. The nodes that are selected as a multipoint relay (MPR) by some neighbor nodes announce this information periodically in their control messages. Thereby, a node announces to the network that it has reachability to the nodes, which have selected it as MPR. In route calculation, the MPRs are used to form the route from a given node to any destination in the network. The protocol uses the MPRs to facilitate efficient flooding of control messages in the network. OLSR inherits the concept of forwarding and relaying from HIPERLAN (a MAC layer protocol), which is standardized by ETSI. Each node periodically broadcasts Topology Control (TC) messages containing link state information. Since these TC messages are broadcast to the entire network, a serious flooding control mechanism needs to be implemented. Multipoint relays provide a localized and optimized way of flooding reduction in a mobile ad hoc network. Using 2-hops neighborhood information, each node determines a small set of forward neighbors for message relaying, which avoids multiple retransmissions. MPR has been designed to be part of OLSR to specifically reduce the flooding of TC messages sent by OLSR to create optimal routes. Depicted like this, one might think that both protocols are completely separated and could even be independently tested,

improved, or even changed. However, OLSR has a much different relationship with MPR.

3.2.2 Comparison scenarios between AODV, OSPF and OLSR

In this comparison between AODV, OSPF and OLSR, we evaluate their performance based on the response time between end-to-end wireless nodes separated by wireless routers and the overhead traffic generated by the routing protocols. Running on large-scale scenario consists of 12 wireless routers and two wireless nodes. All scenarios setups are identical in significant distance between wireless nodes is introduced so that both nodes can't communicate directly and their packets have to go through middle routers, see Appendix B for configuration details.

We have created nine AODV scenarios and nine OSPF scenarios and two wireless stations at ends of network. Figure 3-4 illustrates topology used for ADOV, OSPF and OLSR.

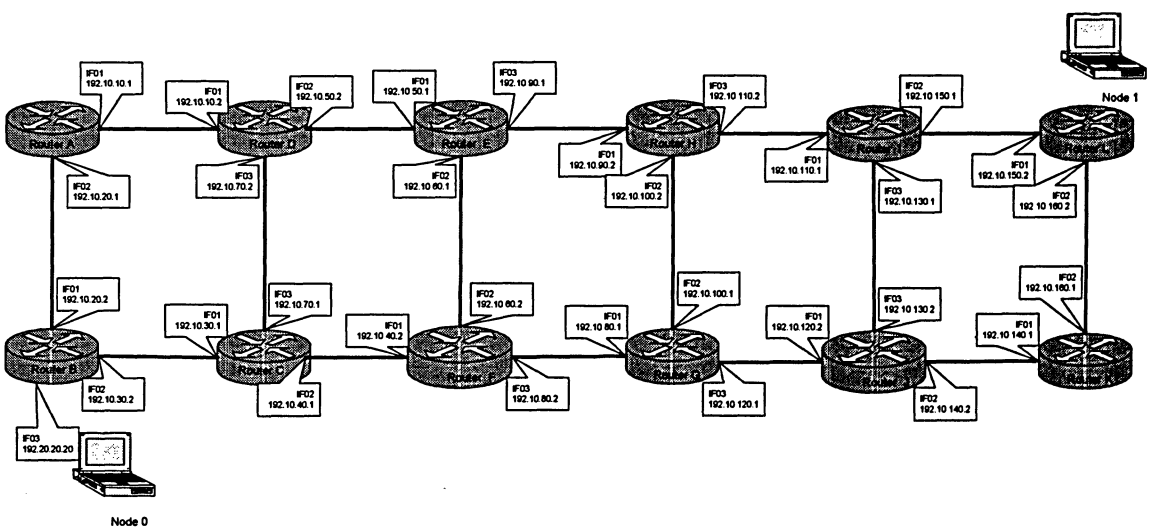

Figure 3-4: 12-router topology

Our proposed comparison is looking at interval times between ping traffic, which reflects users request to Internet, and Hello interval for routing protocol in place. Therefore, we set different times for Hello periods and ping traffic, and we monitored protocol overhead through (traffic control) and average response time received at end node_0, which reflects network delay, that compound of buffering and convergence time of routing protocol. We take average of best response time and control traffic and apply it to highly loaded network (that's in term of traffic).

3.2.3 AODV Response Time and Overhead

We ran different scenarios with three Hello time intervals and three ping intervals. Our testing based on ping between two end nodes (Node_0 and Node_1) as shown in figure 3-5.

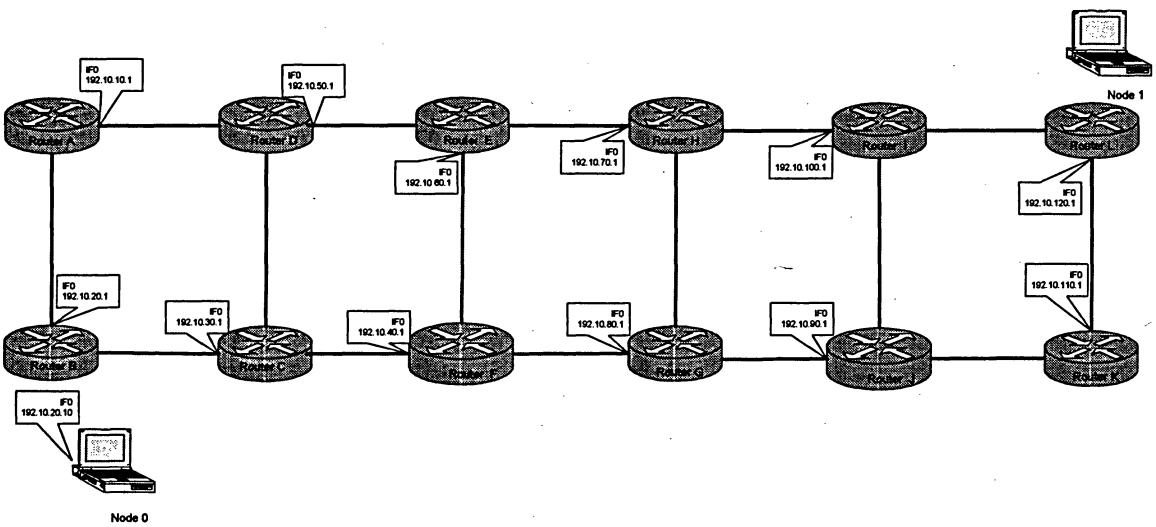

Figure 3-5: 12 routers AODV scenario

Figure 3-6 illustrates number of control traffic transmitted throughout all routers in topology, divided into three regions based on hello intervals: one second, five seconds and 10 seconds.

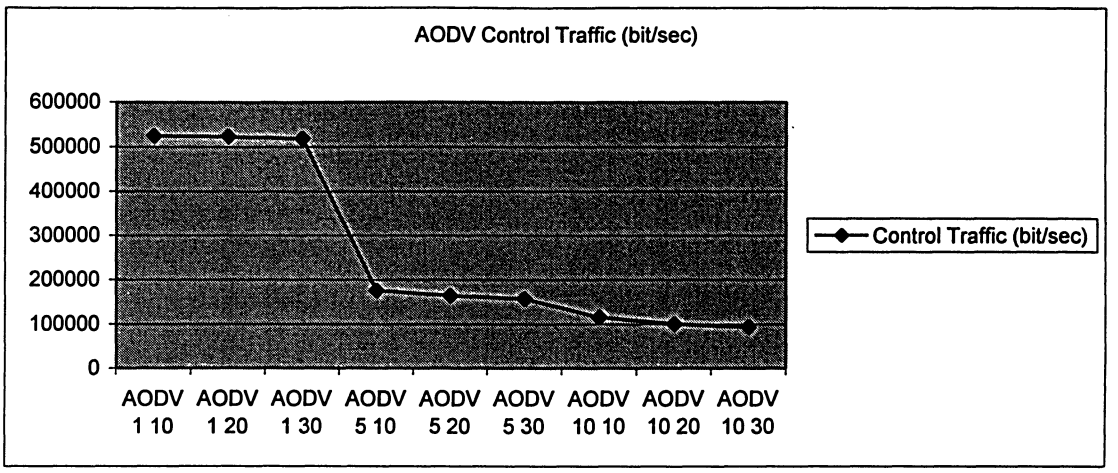

Figure 3-6: AODV control traffic in all scenarios

We used in this figure the notation AODV 1 10 that means protocol used is AODV, hello interval is 1 second and gap between ping (silence period between ping) is 10 seconds. As hello interval increases and ping gap increases the lower control traffic is.

As we can see that at hello interval 10 seconds and gap between ping 30 seconds achieves the lowest control traffic traveling (i.e. lower overhead bits traveling) were worst cases at AODV 1 10, AODV 1 20 and AODV 1 30, because of frequent hello messages traveling between routers.

Average ping response time, the average time delay for Node_0 to receive its ping replies from Node 1. Figure 3-7 illustrates average ping response time for AODV scenario.

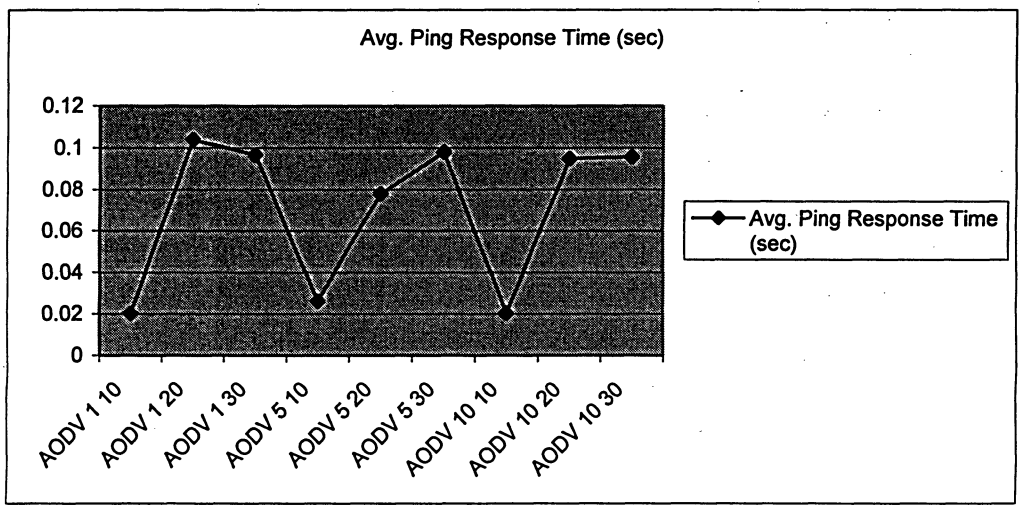

Figure 3-7: average ping response time for AODV scenario

Best average response time is recorded at ping gap of 10 seconds and hello interval didn't matter much as we can see best three at hello intervals 1 second, 5 seconds and 10 seconds.

3.2.4 OSPF Response Time and Overhead

We ran different scenarios with three Hello time intervals and three ping intervals. Our testing is based on ping between two end nodes (0 and 1) as shown in figure 3-4. Figure 3-8 illustrates number of control traffic transmitted throughout all routers in the topology.

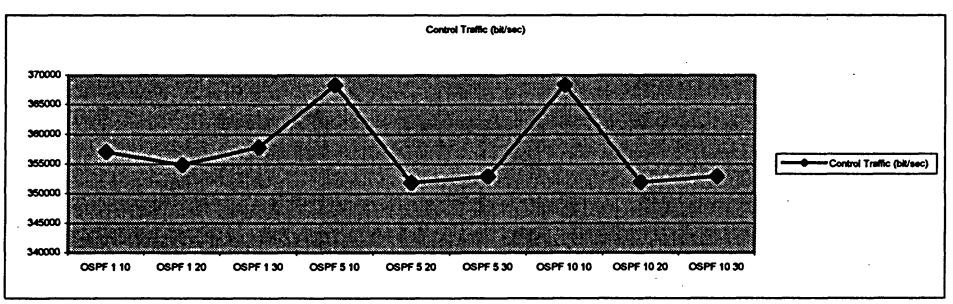

Figure 3-8: OSPF control traffic

At OSPF 5 20 (Topology with OSPF protocol, 5 seconds Hello interval time and 20 seconds Ping gap) has lowest control traffic (routing over head) traveling cross network followed by OSPF 10 30. In terms of how

many times OSPF had to converge for all 9 scenarios the overall network convergence event is 1.

Average ping response time is the average time delay for Node_0 to receive its ping replies from Node 1. Figure 3-9 illustrates average ping response time for OSPF scenarios.

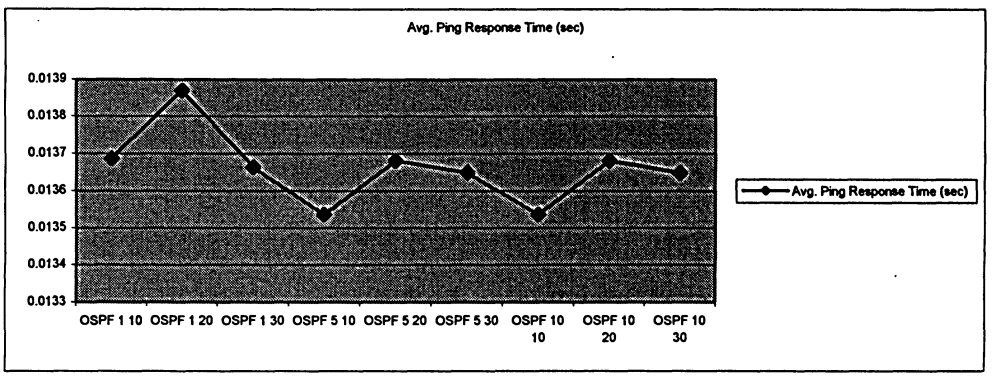

Figure 3-9: OSPF average response time

The lowest average response time is recorded at ping gap of 10 seconds and hello interval between 5 and 10.

3.2.5 OLSR Response Time and Overhead

We ran different scenarios with three Hello time intervals and three ping intervals. Our testing is based on ping between two end nodes (0 and 1) as shown in figure 3-4. Figure 3-10 illustrates number of control traffic transmitted throughout all routers in topology. Figure 3-10 is divided into three regions. In the first region where hello interval is one second, the control traffic tends to decrease as ping interval time increases.

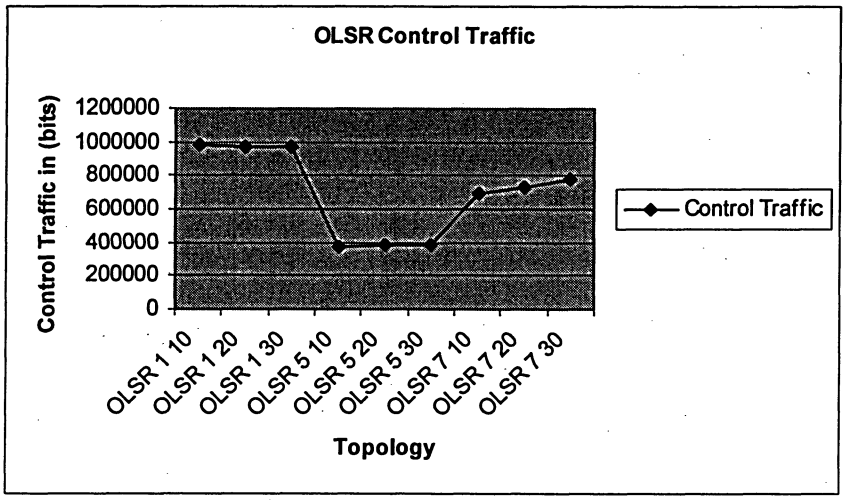

Figure 3-10: OLSR control traffic

Whereas in second and third regions of figure 3-10 hello interval has longer gap period than first region OLSR control traffic tend to increase as ping interval period increases. And if we stretch Hello period to more than 7 seconds there are more control traffic but no ping response at end station.

Average response time, as shown in figure 3-11, which illustrates average response time captured for OLSR in different scenarios at node_0.

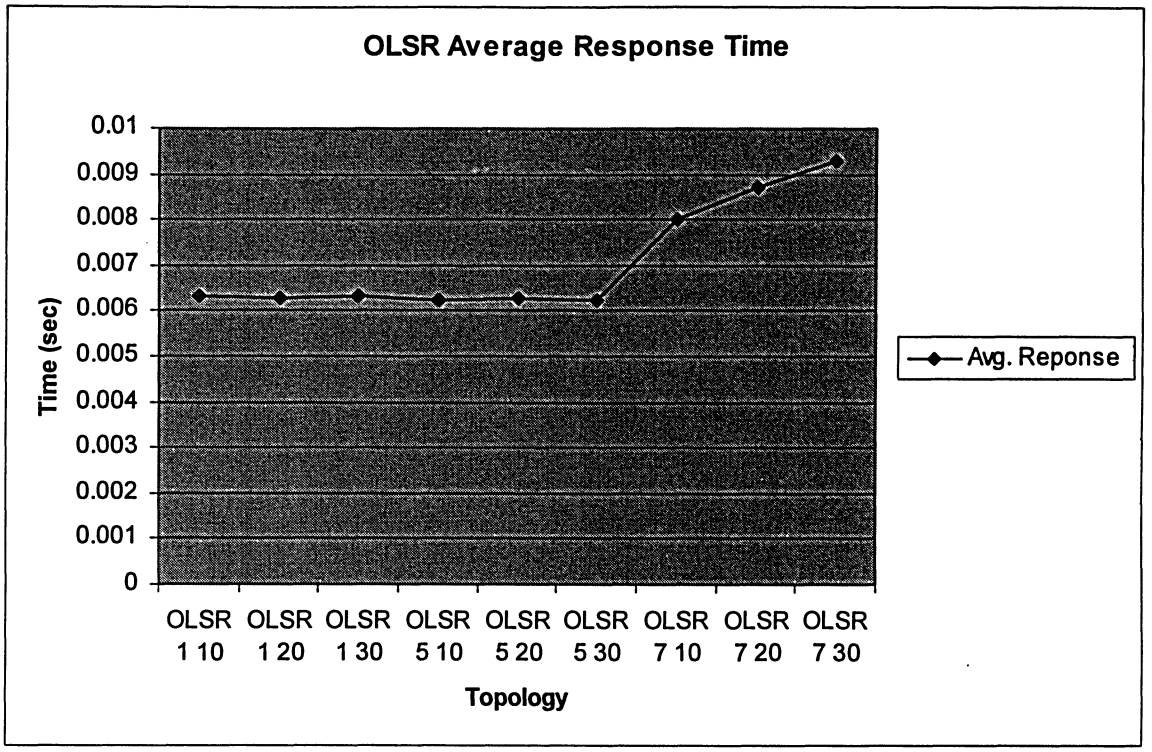

Figure 3-11: OSLR average response time

OLSR tend to have better response time at region two (OLSR 5 10 – OLSR 5 30) of the graph. As control traffic increases dramatically as shown in region three of the figure 3-11 leads to decrease response time at end station as hello interval time increases, then we noticed that increasing hello longer than 10 seconds increase control traffic, node_0 did not receive a response; which shows tradeoff between control traffic and response time.

3.2.6 Performance under heavily loaded network

Here we had our test on two scenarios consisting of 12 routers with AODV, OSPF and OLSR protocol. We increased traffic load by adding 6 more stations and creating 4-ping traffic paths additional to pervious scenarios as shown in figure 3-12. All three protocols have there hello message interval of five seconds and ping interval time of 20 seconds.

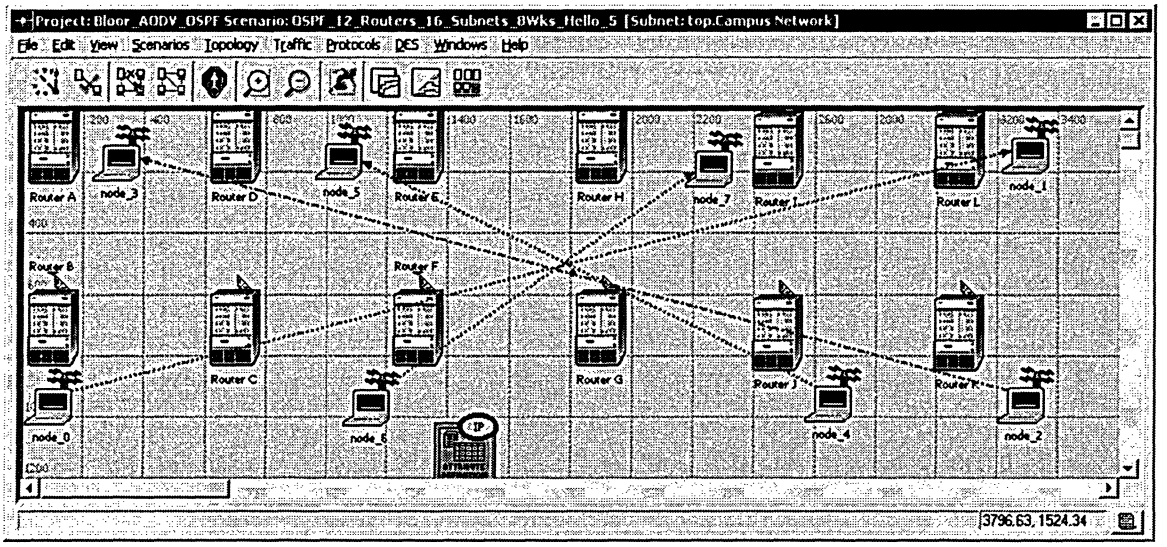

Figure 3-12: 12 wireless routers and 8 wireless nodes

In terms of control traffic (protocol overhead), OLSR tends to have more control traffic comparing with other two protocols as shown in figure 3-13.

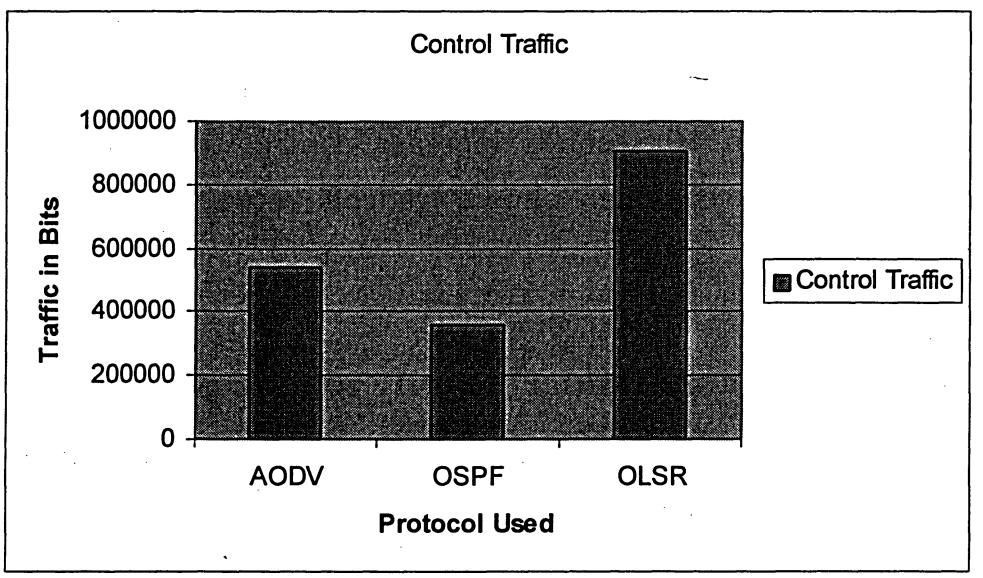

Figure 3-13: Traffic Overhead (control traffic) for AODV, OSPF and OLSR

Control traffic has effect on number response times node_0 received a reply. For instance with OSPF protocol node_0 received 33 replies while

with AVOD, node_0 received 20 replies. Figure 3-14 illustrates number of responses received at node_0

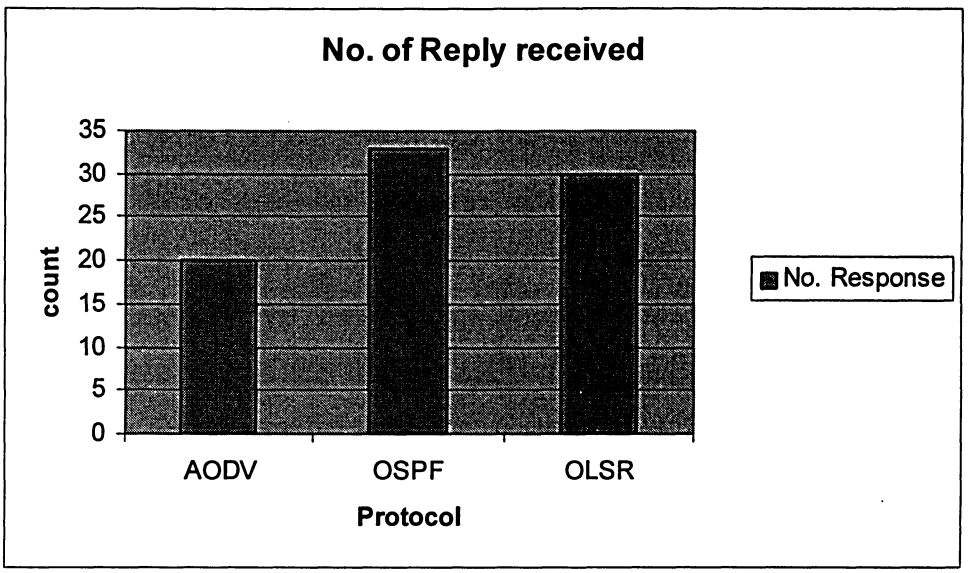

Figure 3-14: comparing number of replies received at node_0 for AODV, OSPF and OLSR

Finally, in terms of average response time AODV kept behind while OSPF and OLSR. Where with last two kept very close as shown in figure 3-15.

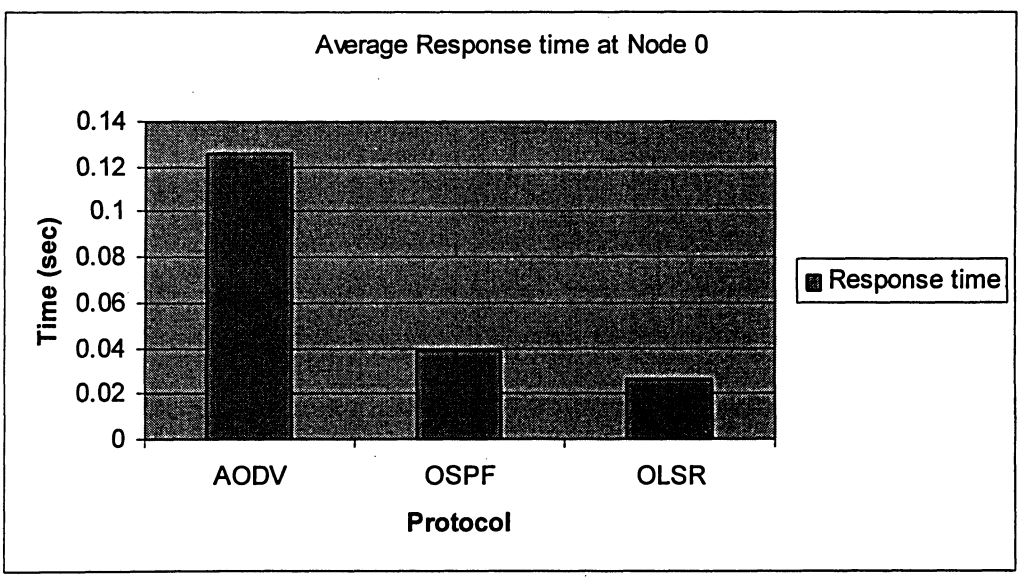

Figure 3-15: Comparing Average response time received at node_0 for AODV, OSPF and OLSR

3.3 Effect of Power on Network Convergence duration Of OSPF

Coverage applies to moderate-size or large WMR deployments and is a measurement or square meters per WMR. Rate-weighted coverage is the integral of the bit rate with respect to area covered (expressed as megabits/second times square meters). Range, coverage and rate-weighted coverage are strongly influenced by transmit power, receiver sensitivity, noise and interference, as well as the physical environment.
Bit Error Rate (BER) is major factor that effects OSPF convergence time, as BER increases number of packet drops increase and increase number of retransmitting LSAs packets. As Bit Error is function of Signal to noise ratio, which is in turn, is function of signal power as shown in formula 3-1.

$$(SNR)_{db} = 10 \log_{10} (\text{Signal Power}/\text{Noise Power}) \qquad (3\text{-}1)$$

Furthermore, signal power range is a function of transmission power (Appendix C – list formulas used in OPNet to represent BER) that has an effect on Bit Error Rate, the more transmission power, the less BER is and less packet drops. In our proposal, using certain range of transmission power to provide less packet losses. This study focuses on different transmission power ranges on two major scenarios: campus scenario and Bloor street scenario and as explained earlier, OSPF protocol is the chosen protocol to run cross these scenarios with its capability of supporting small to large network

3.4 Why choosing BGP over OSPF alone for multiple areas

In some WMN deployment mesh routers in a linear chain (e.g. long street like Bloor street), as shown in Figure 3-16 [1]. This deployment scenario is common for highway, countryside roads, and long urban and suburban streets.

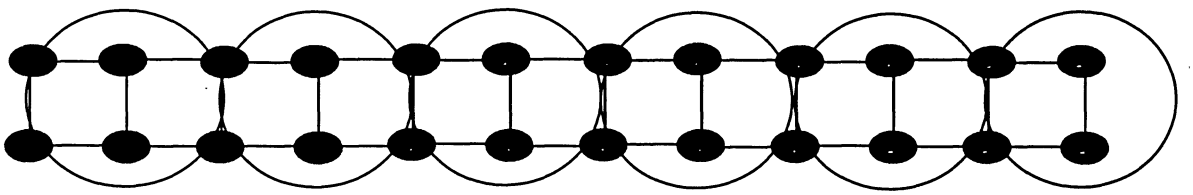

Figure 3-16: Long street topology

To configure OSPF routing protocol for this topology, either, choosing single area OSPF network will suffer long convergence time and propagation of route flapping and if, we setup multi area OSPF which one would be area Zero? And if Area Zero is selected some OSPF will more than two autonomous systems away from area Zero which virtual links can't handle it.

In this study we exam proposed solution [1] of deploying BGP between OSPF areas, as shown in figure 3-17.

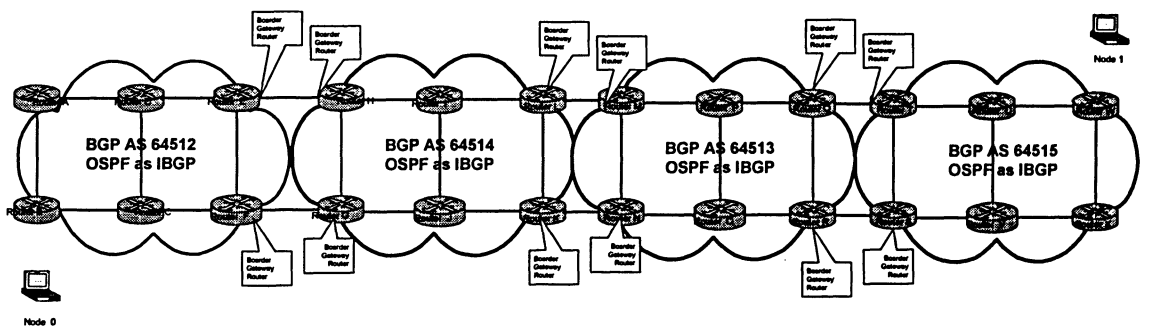

Figure 3-17: Integrating BGP with OSPF in Bloor topology

Using BGP protocol to connect OSPF autonomous systems (networks), most of the BGP configuration problems will not arise because all autonomous systems are under the same administrative control. In this study we configured OSPF in two scenarios: One, the whole network is configured for a single area OSPF. Two, interconnecting OSPF areas by

configuring BGP protocol on boarder gateway routers as shown in figure 3-17. Method we used to measure performance between One and Two scenarios is first response time received at node_0, because OPNet dose not provide convergence statistic for for BGP but it dose for OSPF. Therefore, to measure convergence of both OSPF and BGP for Figure 3-17 we starts ping at time t1(sec). Question is, at what time should we start two protocols? Two possible scenarios either both protocols to start at the same time or start one protocol first wait till finish convergence then start next protocol as shown in figure 3-19. When starting both protocol at the same time as shown in figure 3-18, BGP tends to be sensitive in convergence and when another protocol starts at the same as BGP, BGP will wait and take longer for node_0 to get its first response time (t5) as shown in figure 3-18.

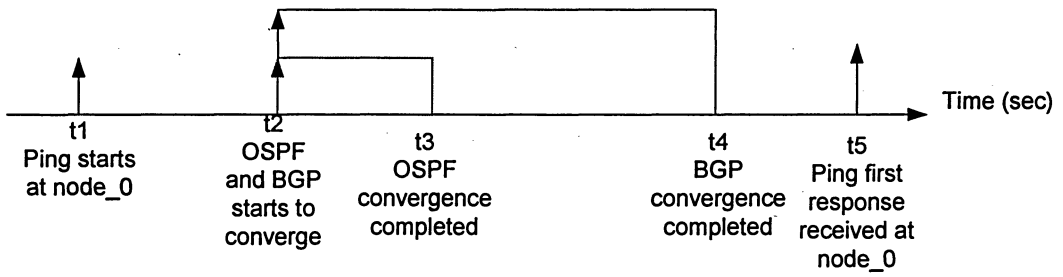

Figure 3-18: OSPF and BGP starting at the same time

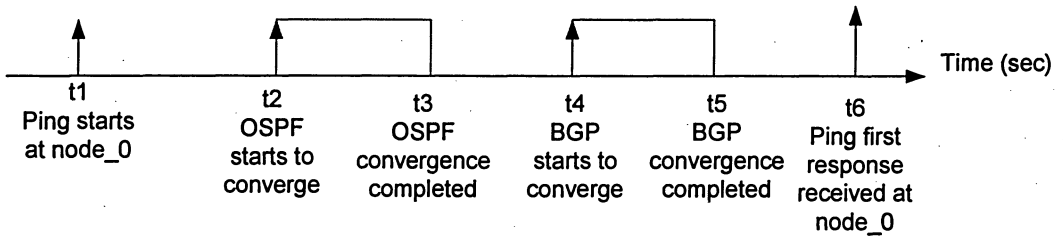

Figure 3-19: Starting OSPF and BGP at different times

By taking advantage of pervious scenario when having only OSPF configured, we were able to get OSPF convergence duration. Then we

estimates time taken by OSPF and apply it to OSPF-BGP scenario and finding best start up time for BGP. With different BGP startup time for 12 routers scenario with one domain and two domains, and measuring first response time at node_0. we were able to find out average of best time for BGP to startup and apply it on larger scenarios (18 routers and 14 routers) with two, four and six domains.

Chapter Four – Simulation and Results

OPNet software was used to simulate four different scenarios. This chapter is divided into two parts. Part One covers power effect on OSPF convergence time. Part two covers integrating BGP with OPSF of suburban area (Bloor topology).

4.1 The Effect of Power on OSPF Convergence Time

Scenarios are divided into two categories; Campus network and Bloor Street network. In the Campus scenario, two sub-scenarios were created. One scenario with single OSPF area and a second with central area 0 communicates with various OSPF areas around which act as a bridge between the different areas. In the Bloor topology, we worked on two scenarios. One scenario configuring entire network with same AS (area 0) and a second scenario having Boarder Gateway Protocol (BGP) link OSPF areas across a distance of approximately three kilometers.

4.1.1 Campus Network

4.1.1.1 Single OSPF Area

In this scenario transmission power range used is 1mW and 5mW. The distance between routers was set randomly at 400m-500m(+). All 8 routers have one physical wireless interface with two or three subinterfaces. Each subinterface was configured on a different subnet as shown in figure 4-1 and 4-2.

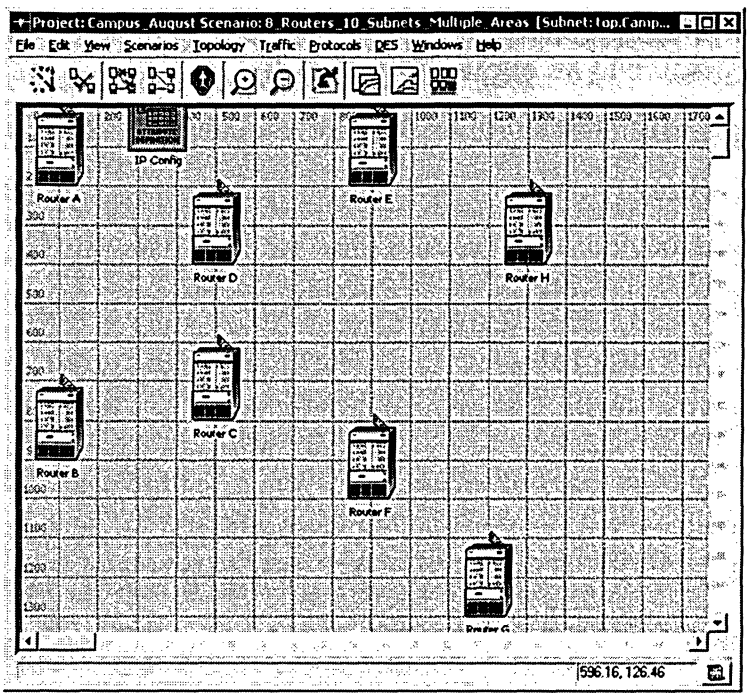

Figure 4-1: Wireless Router sets in OPNet simulation

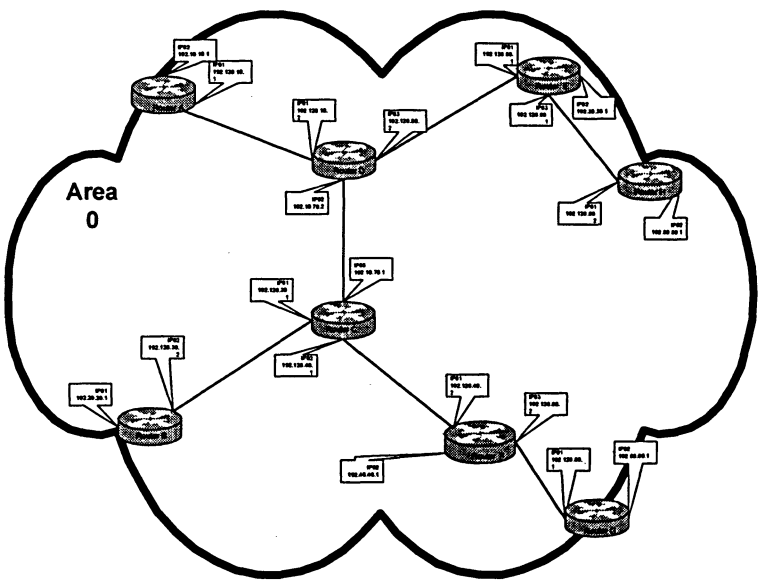

Figure 4-2: Campus Topology single area- Routers subinterface configuration

All OSPF wireless subinterfaces are configured in a single OSPF Area (area 0). Four routers are configured with two subinterfaces while the other four routers are configured with three subinterfaces.

We ran the scenario with power of 1 mW looking at OSPF convergence events for router D as shown Figure 4-3.

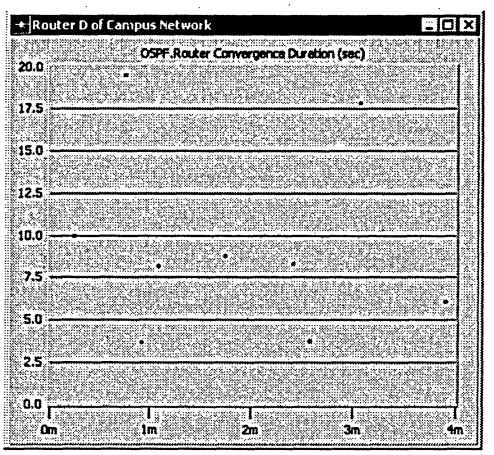

Figure 4-3: Convergence events – Campus topology 1mW Single Area

Figure 4-3 illustrates the number of OSPF convergence events taking place for simulation during of 240 seconds (four minutes). One possibility of causing frequent LAS exchange unstable link condition or adding, or removing link from network. Therefore, we investigated link instability by checking OSPF database of router D at different simulation stop times[1], then looking at the number of LSA received, we were able to plot these changes on chart as shown in Figure 4-4.

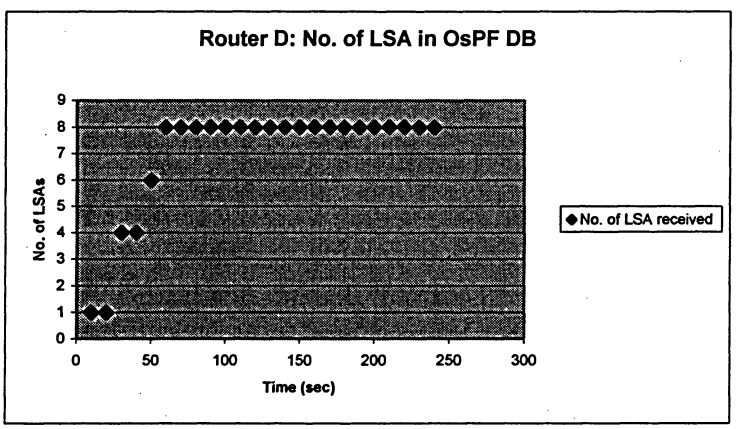

Figure 4-4: Campus Topology Single area – Router D: No. of LSAs received

[1] Simulation Stop Time: is the time when we stopped simulation and traced what happened till stop time for example we stop simulation at 170 seconds then we traced that at time167.140 seconds received LSA update and time 167.142 seconds router D received another LSA update.

During time period of (10-20) seconds, router D build OPSF database for its own subnets, then during period of (30 – 50) seconds, router D received LSAs from neighbor routers (D, A, C and B), then period (50-60) seconds router D received LSAs from (A, B, C, D, H and E) routers, and during time period of (50-70) seconds router D received LSAs from (A, B, C, D, E, H, G, and F) routers which make 8 LSAs as total in OSPF database and this number remained persistent for rest of simulation time. Up to this point we didn't find reason behind many convergence events on Figure 4-3, therefore, we examined each LSA content, we found that at time 96.204 seconds router D received from router C new LSA reporting a lost connection with router F, then at time 141.66 seconds router C sends new LSA which has a connection to router F, as shown in Figure 4-5.

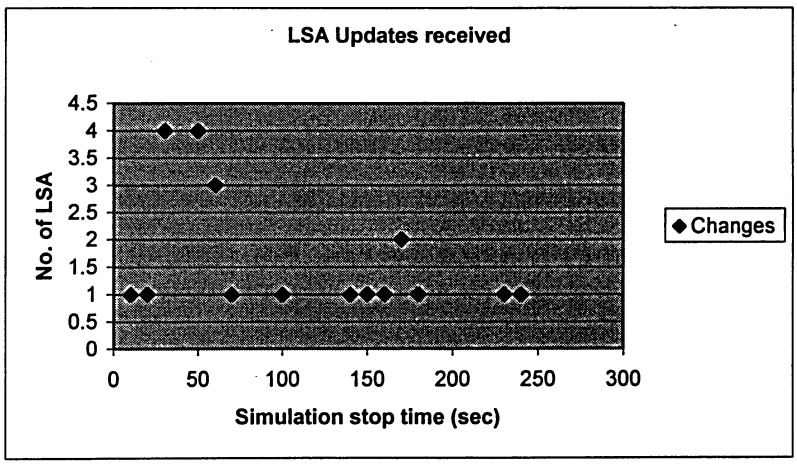

Figure 4-5: LSA updates in Router D OSPF Database - Single Area

Figure 4-6 illustrates path status (instability) between router C and router F during simulation time 240 seconds.

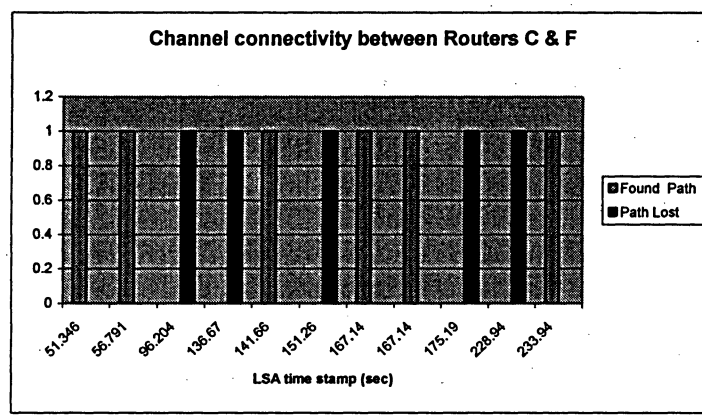

Figure 4-6: Campus Single area – path between router C & F

That made us to conclude there is channel unstable between two routers due to either noise or transmission single. For noise, since OPNet channel model is not affected with noise. And for transmission single, we applied two solutions: First solution is shortening the distance between routers C and F. Second solution is to increase the transmission power. When applied the first solution, router D experienced only two OSPF convergence events so as entire network convergence. When applying the second solution we had same results as in first solution in terms of number of OSPF convergence events, but time duration for these events were shorter and faster compared with the first solution. For example, with shortening distance between router C and F, the OPSF convergence event that started at 55.5 seconds required 30.14 seconds to complete while with the second solution OSPF convergence event started at 45.13 seconds and required 20 seconds.

4.1.1.2 Campus Network – Multiple OSPF Areas

In this scenario we set the transmission power for wireless interface et to 1mW and 5 mW and the distance between routers was 400m-500m (+). All 8 routers had only one physical wireless interface with two or three subinterfaces such that each subinterface was configured with different

subnets (some of them with different OSPF area). Figure 4-7 illustrates the OSPF configuration on the wireless subinterface with different OSPF areas assigned on each router. Four routers have two subinterfaces and the other four routers have three subinterfaces.

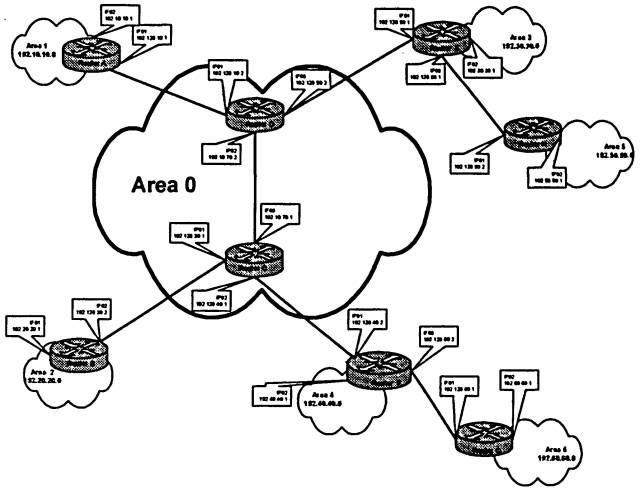

Figure 4-7: Campus Topology Multi area- Routers subinterface configuration

Under transmission power of 1 mW OSPF convergence at router D had many convergence events similar to the single area scenario as shown in Figure 4-8.

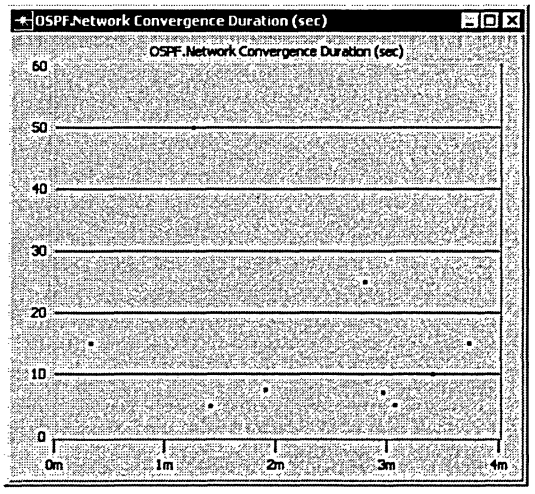

Figure 4-8: Convergence events – Campus topology 1mW Multi Area

The same procedure we did in Campus single scenario, we looked at first the OSPF database of router D for number of LSAs exchanged as shown in Figure 4-9.

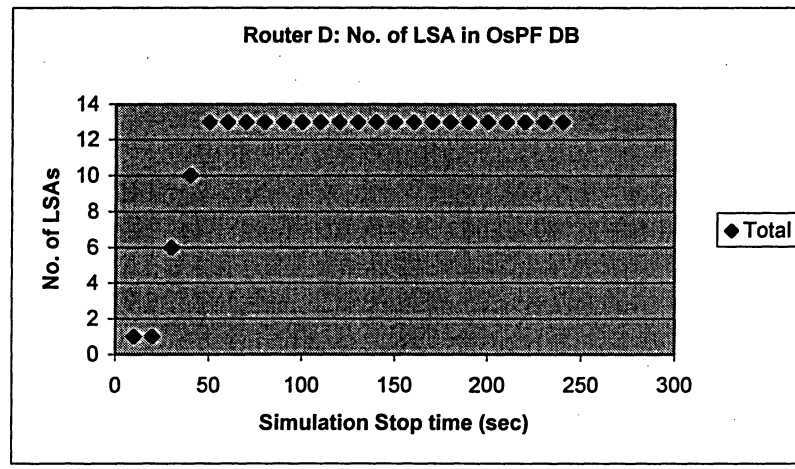

Figure 4-9: Campus Topology Multi area – Router D: No. of LSAs received

In this case there were more LSAs because of Area Border Routers (ABR) advertising network LSA (type 3). During time period of (10-30) seconds router D updated OSPF database with its own subnets, between (30-40) seconds router D received LSAs from routers (A, B, D and C) with two network LSAs (type 3), between (40-50) seconds router D received LSAs from routers (A, B, C, D, G and F) with four network LSAs, and between (50-60) seconds router D received LSAs from routers (A, B, C, D, E, F, G and H) with five network LSAs, which brings total of LSAs to 13 in OSPF database, this number remained persistent till end of simulation time 240 seconds. Then we looked at LSA exchanged in OPSF database, Figure 4-10 illustrates LSA changes during simulation time.

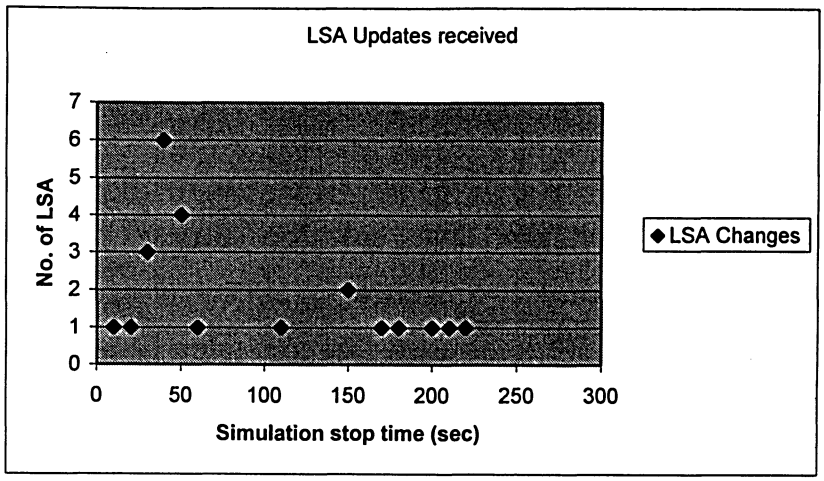

Figure 4-10: LSA updates in Router D OSPF Database - Multi Area

We noticed, that there was new LSA received from router C at time 107.461 seconds reporting lost connection with router F and 147.999 seconds router D received another LSA from router C reporting connection found with router F. Which made to conclude there is connection instability between router C and router F. Figure 4-11 illustrates connection (path status) between router C and F.

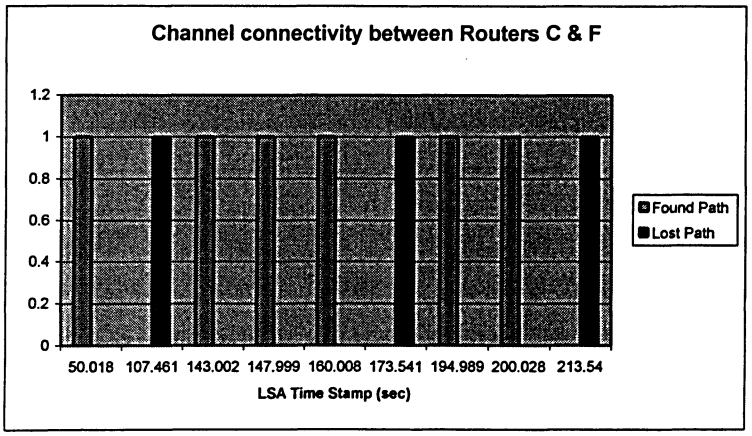

Figure 4-11: Campus Multi area – path between router C & F

As in single area OSPF in the last scenario, path instability between router was obvious, therefore, we locked at two possibilities either there was so much noise between these two routers or distance is stretch to

the limit of radio transmission. In term of noise, because we were using OPNet channel model is not affected with noise, we proposed same two solutions as in single area OSPF: First solution, shortening distance between routers C and F. Second solution, we increased transmission power to 5mW. For the first solution router D experienced three convergence events and two events for entire network convergence. For the second solution, we increased transmission power to 5 mW, network and router D experienced two convergence events only. Also, the convergence time was shorter and faster, for instance with first solution OPSF convergence event that started at 75 seconds required 49.63 seconds to complete convergence while with the second solution OSPF convergence event started at 65 seconds and required 39.87 seconds.

4.1.2 Bloor Street Network

In this topology, we work on two scenarios: one single OSPF area (area 0) and second scenario was configuring Border Gateway Protocol (BGP) interconnecting OSPF areas crossing a long distance of approximately of three kilometers. Transmission power used is 5 mW, with 1 mW can't reach to beyond eight hundred meters. The nature of Bloor topology is cover long distance with less amount of routers possible, therefore 1 mW transmission power is not feasible for this type of topology. However, higher transmission power is used 5mW, 20 mW and 100 mW. 12 routers, were used in this scenario, four routers configured with two subinterfaces and 8 routers configured with three subinterfaces.

4.1.2.1 Single Area

Figure 4-12, illustrates Bloor – street topology with OSPF enabled interfaces and there configuration.

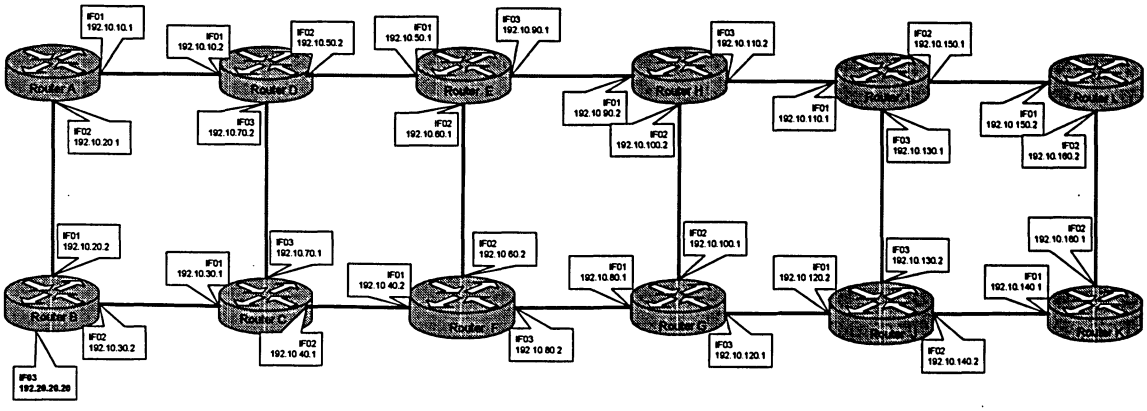

Figure 4-12: 12 routers Bloor Street Topology – One OSPF Area

4.1.2.2 OSPF and BGP protocol

In this scenario shows groups of four routers in the network with their own AS number, and Border Gateway Protocol on Area Border Routers (ABR) interconnecting different OSPF networks as shown in Figure 4-13 simulation duration set to four minutes.

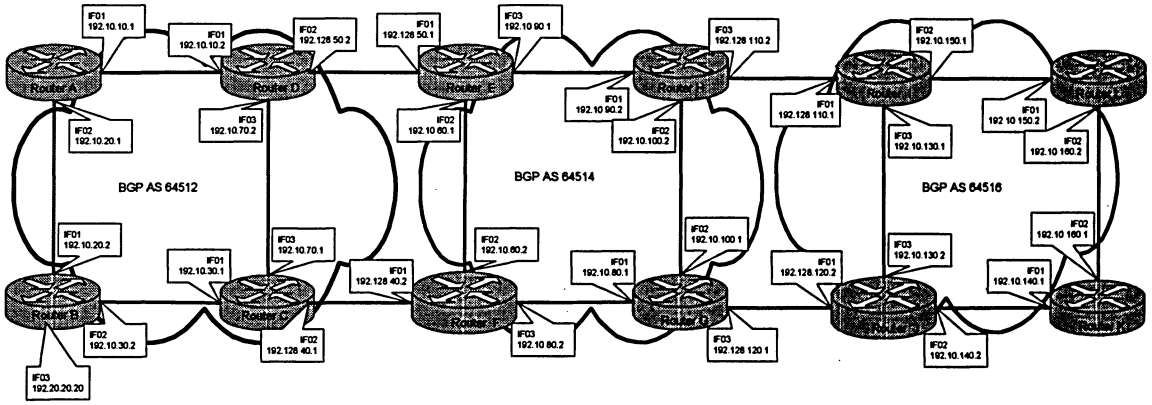

Figure 4-13: 12 routers Bloor Street Topology – Three OSPF Area with BGP

4.2.2.1 Transmission power of 5 mW

Network convergence was 50 seconds for OSPF to converge at time 55 seconds. Router D convergence time was at time 45 seconds events happened here on router D is boarder router, which handling both OSPF

and BGP routing, as shown in figure 4-13, the convergence event took place at time 45 second and lasted for 40 seconds. In looking OSPF database of router D we saw at time 40 seconds router D received four LSA then no other changes till end of simulation.

4.2.2.2 Transmission power of 50 mW

Increasing transmission power to 50 mW increases transmission range radio, and coverage. Router D, had one convergence event started at time 45 seconds and required 40 seconds to complete similar to pervious scenario.

4.2 Integrating BGP with OSPF in suburban topology

We created three scenarios 12, 18 and 24-routers with BGP interconnecting different OSPF AS systems. Both protocols started at the same time at 10th second of simulation time, then we measured the first response time received at Node_0, figure 4-14, illustrates 12-routers scenarios with two BGP domains configuration.

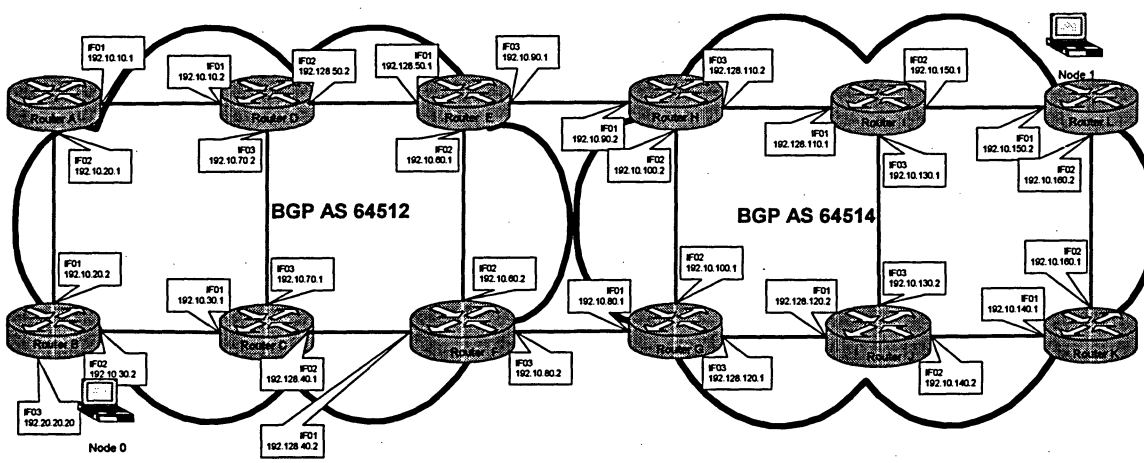

Figure 4-14: 12 routers Bloor Street Topology – Two OSPF Areas with BGP

The first response time takes 175.2 seconds after simulation started. A plausible reason for the longer response time, is BGP convergence started earlier than OSPF, and by that time OSPF started in for its own convergence, it has caused enough disturbance to affect detrimentally of BGP convergence time, which results in a longer time to for Node_0 to receive its first response time. We ran other scenarios with 18-routers and 24-routers as shown in figure 4-15 and 4-16 respectively.

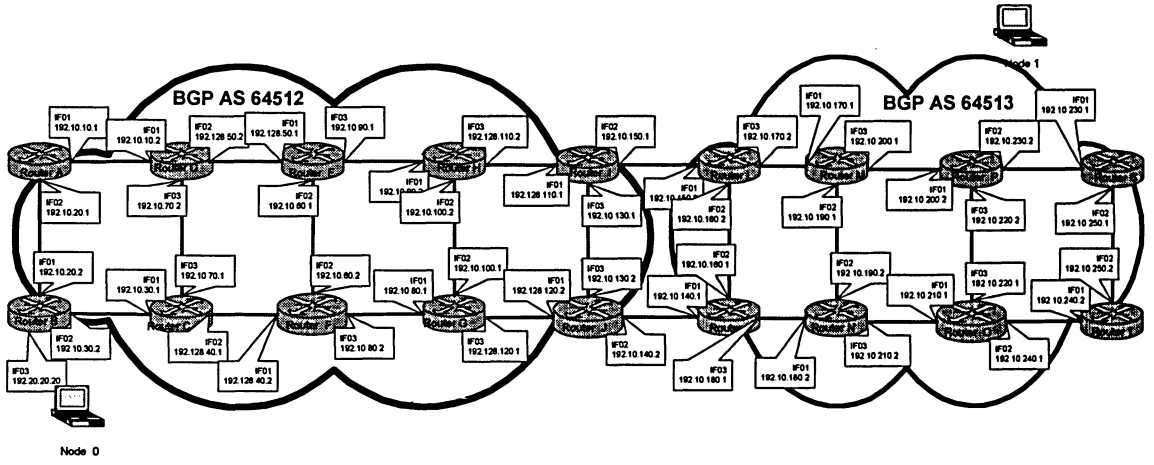

Figure 4-1518 routers Bloor Street Topology – Two OSPF Areas with BGP

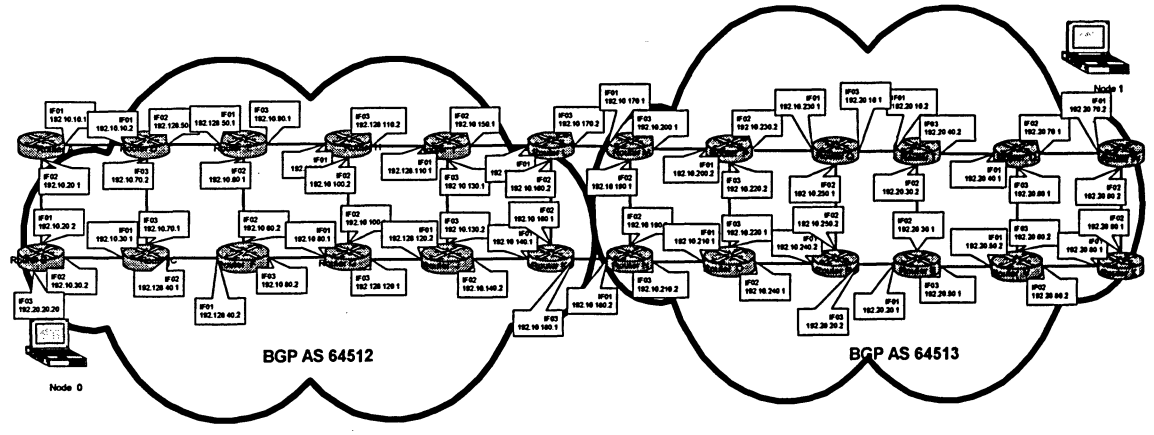

Figure 4-16: 24 routers Bloor Street Topology – Two OSPF Area with BGP

Table 4-1 shows first response time in seconds received by Node_0 in different scenarios including OSPF only , two and three domains.

Scenario No. of routers	OSPF only (sec)	2D BGP (sec)	3D BGP(sec)
12	48	175.2	52.8
18	48	48	175.2
24	69.6	252	180

Table 4-1: Bloor Street First response time received – 3 Scenarios

OPSF only scenario Node_0 received quicker response time compared with the other two scenarios. Also, in looking at BGP with two and three domains shows different response times with tendency of late response time received. Figure 4-17 illustrates first response time received at Node_0 when both protocols OSPF and BGP started at 10th second and ping traffic generation starts at 5th second.

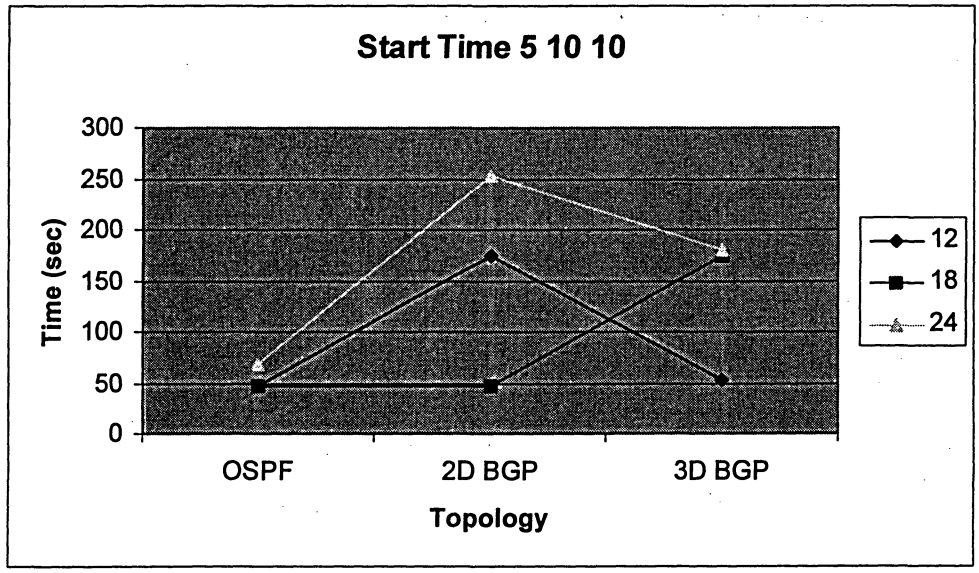

Figure 4-17: First response time when OSPF and BGP starting at same time

To increase first response time at Node_0 with two protocols running (BGP and OSPF), our solution is to have both BGP and OSPF protocols to start at different times. We worked on 12-routers scenario, ping traffic and OSPF protocol both starts at 5th second and BGP to starts at

different times ranging 10th – 70th second (with an increment of 10 seconds), then we measured first response time received at Node_0 for each BGP startup time. Figure 4-18 and 4-19 illustrates different BGP startup times and first response time received at Node_0 for two domains and three domains respectively for 12-router scenario.

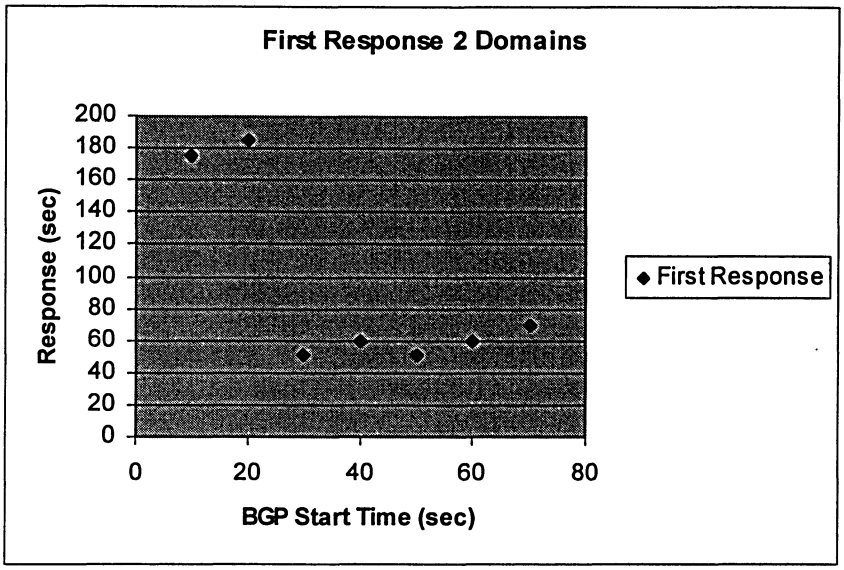

Figure 4-18: First response time – 12 router and two OSPF areas with BGP

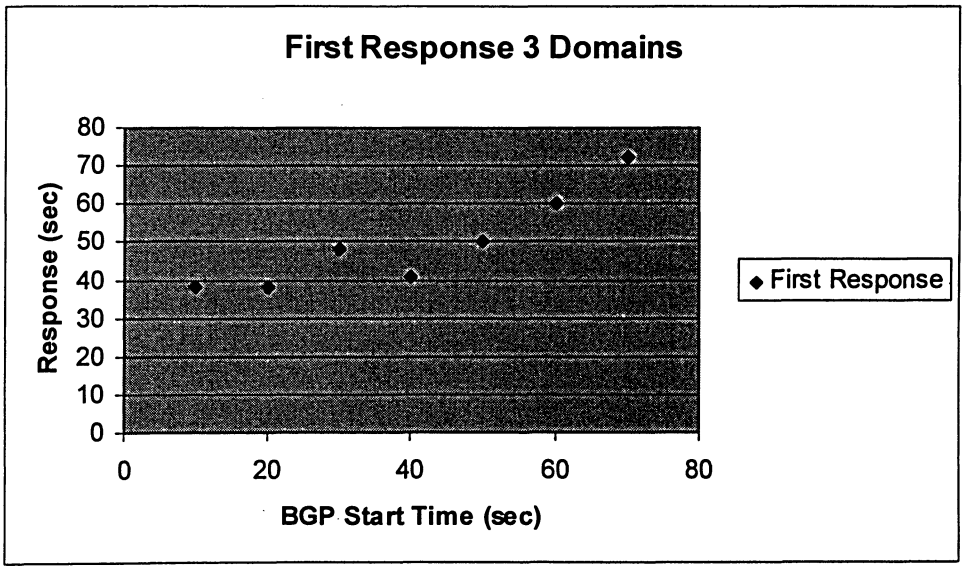

Figure 4-19: First response time – 12 router and three OSPF areas with BGP

4.2.1 Finding best BGP startup time

From Figures 4-18 and 4-19, we concluded that, for the two domains scenario there were the two best times for BGP to start, they were at 30 seconds and 50 seconds, the first response time received at Node_0 for both BGP startup times was at 50.4 seconds. For three domains scenario, best BGP startup times were at 30, 40 and 50 seconds, the first response times at Node_0 were 48, 40.8 and 50.4 seconds respectively. By taking average of best BGP startup time for both scenarios (two and three domains), which are 35 seconds and 45 seconds are the best time for BGP to start. Applying these two BGP startup times on two domains and three domains (12-routers scenario). For two domain scenario, the first response times recorded at Node_0 were 55.2 seconds and 45.6 seconds for BGP startup times at 35 seconds and 45 seconds respectively. For three domains scenario the first response times at Node_0 were is 43.2 and 45.6 seconds for BGP startup 35 seconds and 45 seconds. Figure 4-13 illustrates 12-routers with three domains scenario.

Applying the best BGP startup time 35 and 45 seconds on 18-routers s and 24-routers scenarios as explained in the next section.

4.2.2 Applying best BGP startup time

4.2.2.1 18-routers scenario

Applying the best BGP startup time (35 and 45 seconds) on 18-routers scenario with two AS domains and three AS domain. Figure 4-36 illustrates first response time with BGP startup time at 35 seconds and 45 seconds; when BGP started at 35th second, Node_0 received the first response at 52.2 seconds for two domains and at 55.2 seconds for three

domains. When BGP started at 45th seconds, Node_0 received the first response at 48 seconds for two domains and at 45.6 seconds for three domains

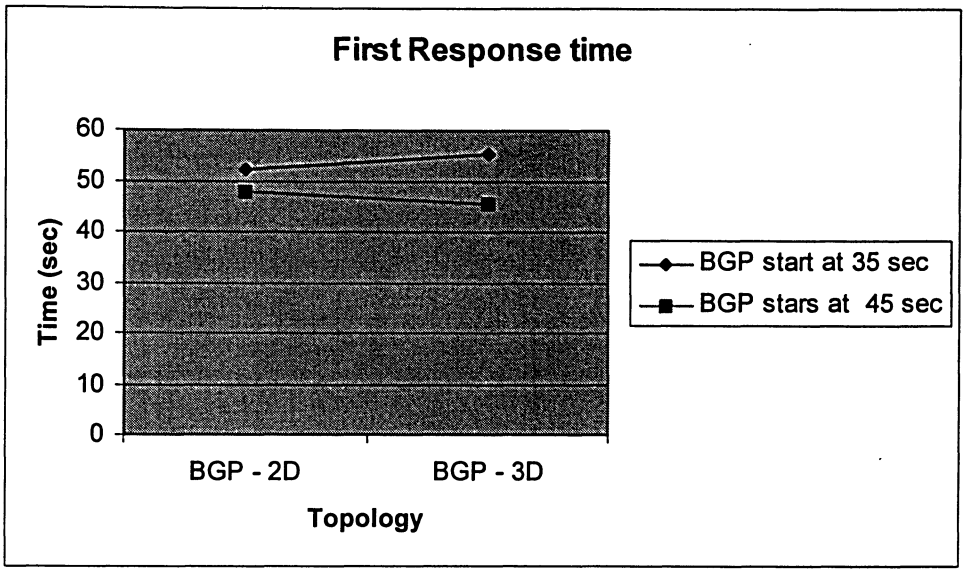

Figure 4-20: First response time – 18 routers with Best BGP startup time

4.2.2.2 24-routers scenario

With two and three domains configuration, BGP has to start at time 45 seconds (not at 35 seconds) to allow enough time for OSPF convergence to complete because the number routers per OSPF domain has increased compared with 12 and 18-routers scenarios. However, BGP startup time chosen (35 and 45 seconds) still can by applied in this scenario with four and six domains configuration, figures 4-21 and 4-22 illustrates four and six domains respectively with BGP startup time 35 and 45 seconds. Startup times for 24-routers scenarios were 5 seconds for ping and OSPF to start then 35 seconds and 45 seconds for BGP to start.

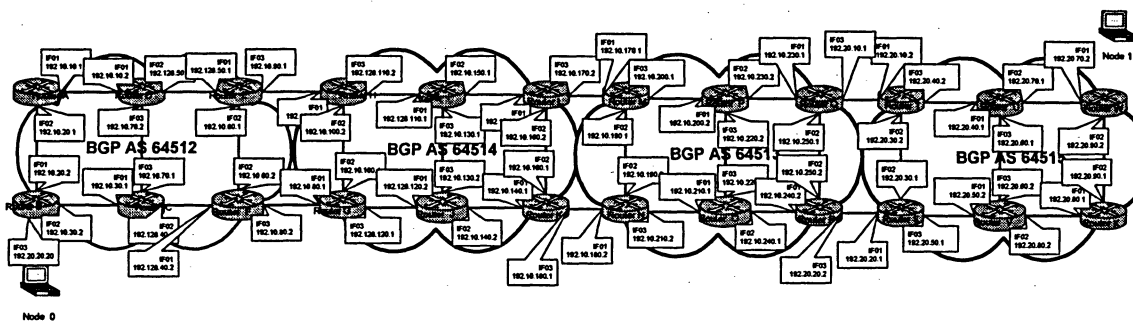

Figure 4-21: 24 routers Bloor Street Topology – Four OSPF Area with BGP

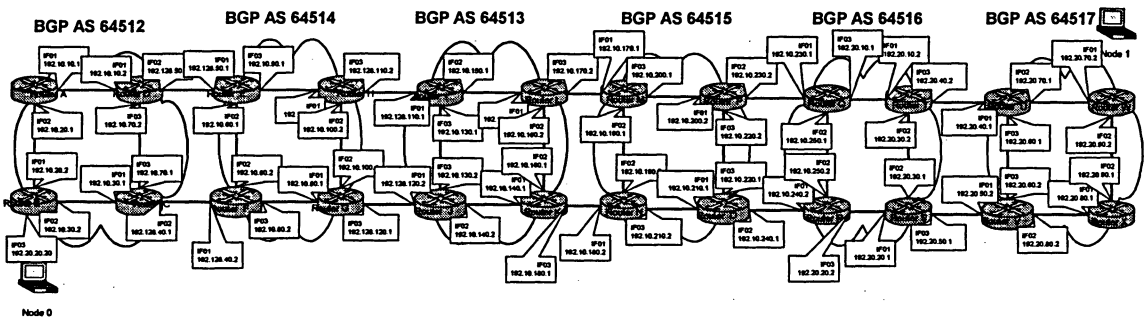

Figure 4-22: 24 routers Bloor Street Topology – Six OSPF Area with BGP

Figure 4-23, illustrates 35 and 45 seconds BGP startup time for four scenarios (two, three, four and six domains): the two domains as shown in figure 4-24, three domains as shown in figure 4-25, four domains and six domains.

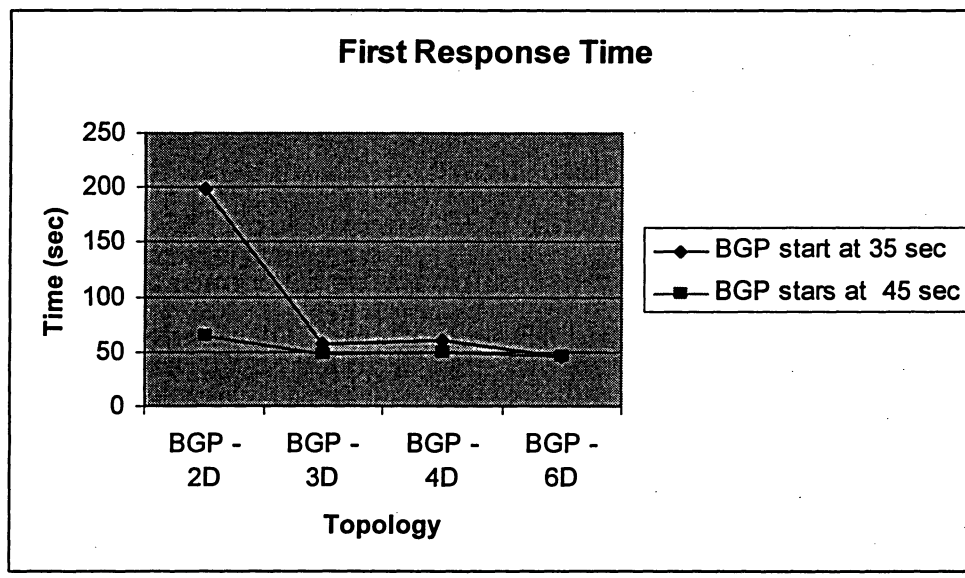

Figure 4-23: First response time comparison - 24 routers 2D, 3D, 4D and 6D

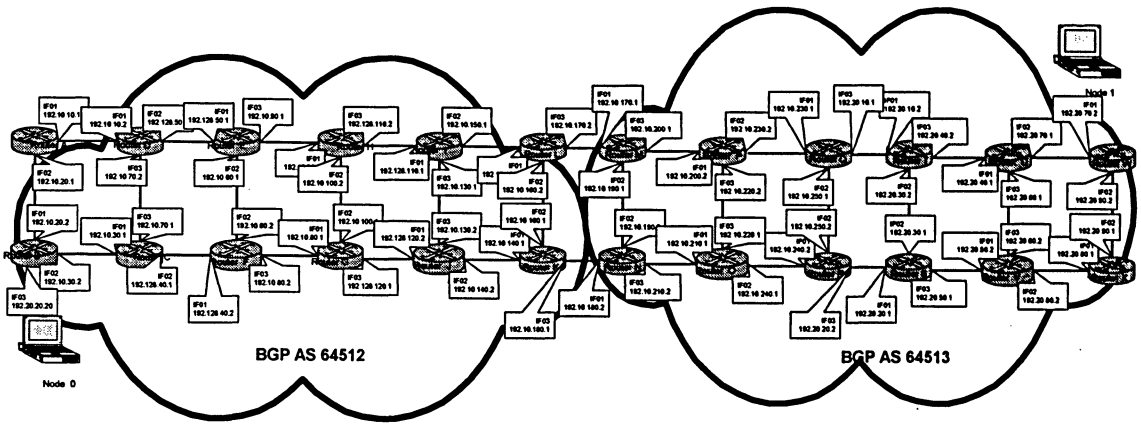

Figure 4-24: 24 routers Bloor Street Topology – Two OSPF Area with BGP

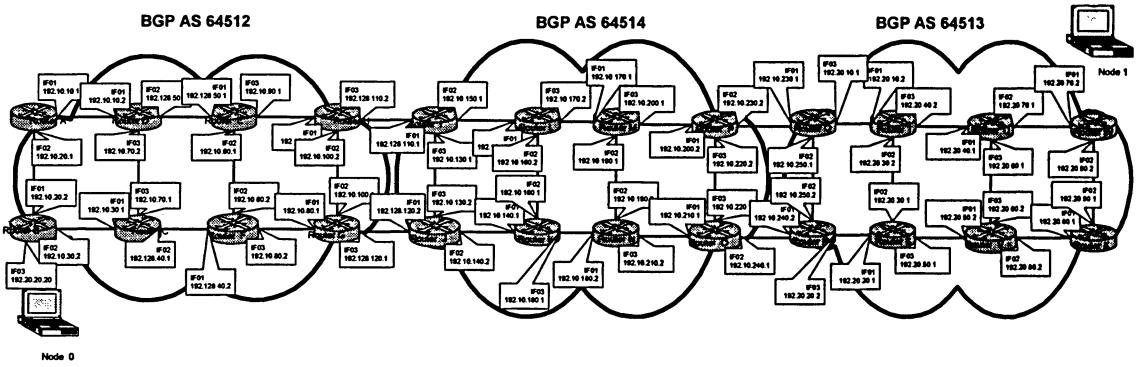

Figure 4-25: 24 routers Bloor Street Topology – Three OSPF Area with BGP

4.2.3 Conclusion

Comparing results in figure 4-20 and in figure 4-23, we have noticed that when BGP started at 45 seconds, Node_0 received a quicker first response time compared with BGP starting at 35 seconds, that was for both 18 and 24 routers scenarios. And when BGP started at 35 seconds, Node_0 recorded a quicker response time compared with OSPF only (no BGP configuration).

Figure 4-26 shows the first response time recorded at Node_0 for 24-router scenario with OSPF only configuration and with BGP (start up time at 45 seconds) interconnecting OSPF areas configuration.

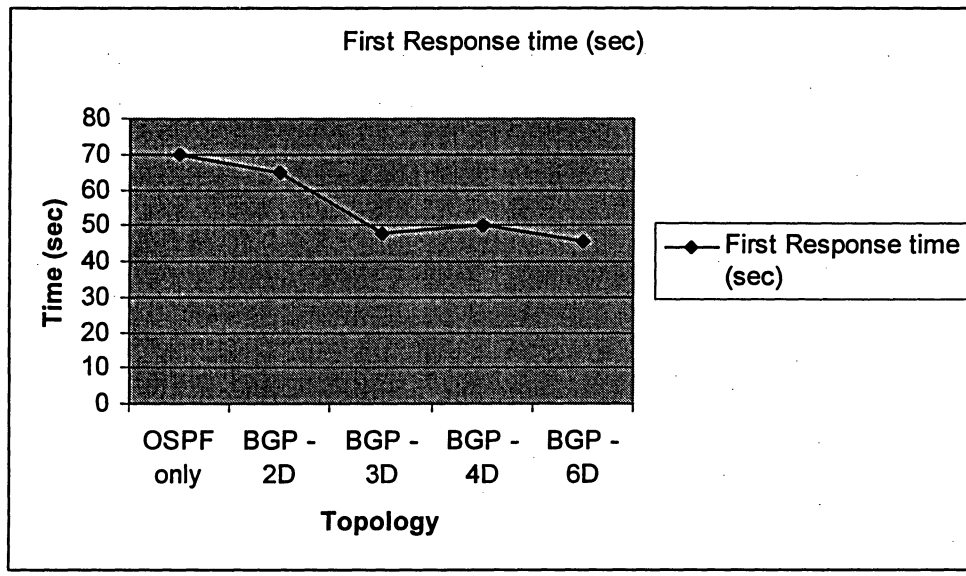

Table 4-26: First response time comparison - 24 routers 1D, 2D, 3D, 4D and 6D

Similarly, with 12-routers scenarios, when BGP to started at 45th second, Node_0 received first response time was at 45.6 seconds, which is faster than 48 seconds with OSPF only configuration, as shown in figure 4-27. And with 18-routers scenario, the first response time recorded at Node_0 with OSPF only configuration was at time 69.6 seconds, compared with 48 seconds for two domains and with 45.6 seconds for three domains (BGP started at 45 seconds).

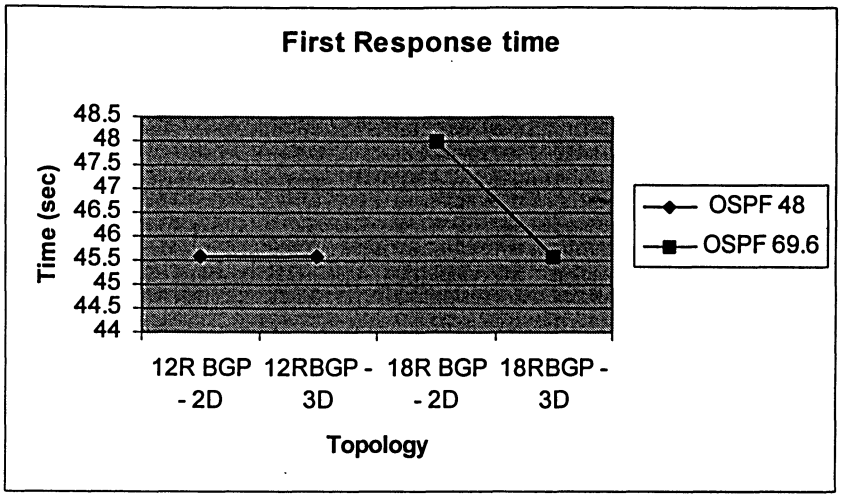

Figure 4-27: First response time comparison – 12 and 18 routers (2D and 3D)

Chapter Five

Conclusion

We have proposed four solutions for different wireless mesh network scenarios.

The first proposal is a sub-interfacing physical wireless interface to multiple subinterfaces to allow the configuration of multiple subnets, which reduces hidden node problem in the wireless networking environment. We then applied this solution on a number of scenarios as we move along with other proposal we kept using the sub-interfacing physical wireless interface to accommodate a number of subnets (both single and multiple OSPF areas).

For the second proposal we used OSPF as the protocol for our Wireless mesh backbone network after looking at proactive Ad hoc protocols like OLSR and reactive protocols like AODV. Our measurements were based on the overhead traffic of the protocols and the average response time at the end station. OSPF had less overhead and more replies to end stations.

For the third proposal, the transmission power had a direct effect on OSPF convergence and responses time. We ran scenarios (Campus and Bloor topologies) and measured OSPF convergence events and length of time for these events. Stretching the distance between wireless routers to the transmission limit caused LSAs to regenerate frequently due to channel instability in convergence and response time. Reducing distance resolved channel instability but, nevertheless, a convergence event still

took more time to convergence whereas using higher transmission power resolved channel instability and reduced time for OSPF convergence.

Our forth proposal integrated BGP protocol for large, long stretching networks (suburban, highway, Bloor street topology...etc.). For this type of topology OSPF protocol has limitations in covering many autonomous systems with virtual links to backbone area (area 0). Integrating with BGP protocol resolved this issue, but our challenge was response time at the end stations due to BGP convergence sensitivity. When OSPF starts at the same time as BGP, BGP takes longer to converge. Therefore, looking at different BGP startup time becomes essential. We reviewed the average of best start up times and applied them on different scenarios to determine which returned the better response time at the end station.

Five areas have been identified for future work:

1) We have found that the channel became unstable when the radio signal was stretched to it's limit, causing the loss of channel connection between routers.
2) Throughput drops significantly as the number of nodes or hops in WMNs increase.
3) When the protocol control traffic increases it had a direct effect on the response time at the end station.
4) Simulating a protocol convergence under different channel noise condition.
5) Auto configuring router's subinterface.
6) I-BGP performance sensitivity to the number of BGP gateways in wireless mesh network.

Bibliography

[1] Muhammad Jaseemuddin, Amir Esmailpour, Ali Alwan and Osama Bazan. "Integrated Routing System for Wireless mesh networks", CN3-3 CCECE 2006 IEEE.
[2] Daniel Aguayo, John Bicket, Sanjit Biswas, Glenn Judd and Robert Morris. Link-level Measurements from an 802.11b Mesh Network., SIGCOMM 2004, Aug 2004
[3] Daniel Aguayo, John Bicket, Sanjit Biswas, Glenn Judd and Robert Morris. A high-throughput path metric for multi-hop wireless routing. In proceedings of ACM Mobicom conference, September 2003 pp. 134-146.
[4] Violeta Gambiroza, Bahareh Sadeghi, Edward W. Knightly. End-to-End Performance and Fairness in Multihop Wireless Backhaul Networks, in Proceedings of ACM MobiCom 2004, Philadelphia, PA, September 2004.
[5] Richard Draves, Jitendra Padhye and Brian Zill. Comparison of Routing Metrics for Static Multi-Hop Wireless Networks, SIGCOMM'04, Aug 2004,Portland, USA.
[6] Coskun Cetinkaya, Edward Knightly. Opportunistic Traffic Scheduling Over Multiple Network Paths, in Proceedings of IEEE INFOCOM 2004, Hong Kong, China, March 2004.
[7] Philippe Hanset. Large Scale Wireless Netwroks, UTs case University of Tennessee -NANOG 27, February 2003.
[8] Ian F. Akyildiz and Xudong Wang. A Survey on Wireless Mesh Networks. IEEE Communications September 2005, Vol. 43, No. 9 page S23
[9] Richard Draves, Jitendra Padhye and Brian Zill. Routing in multi radio, Multihop Wireless Mesh Network. ACM Annual International conference Mobile comp. And Net.(MOBICOM),2004, pp 114-28
[10] H. Frey, "Scalable Geographic Routing Algorthms for Wireless Ad Hoc Networks,"IEEE Network Mag., July/Aug. 2004, pp.18-22
[11] RFC 3561 Ad hoc On-Demand Distance Vector (AODV) Routing, http://www.ietf.org/rfc/rfc3561.txt, last time accessed was on September 16, 2006 at 16:00 pm EST.
[12] RFC 2328 - OSPF Version 2, http://www.ietf.org/rfc/rfc2328.txt, last time accessed was accessed on September 16, 2006 at 16:00 pm EST.
[13] Microsoft Networking Research Group, http://research.microsoft.com/mesh/, last time accessed was on September 16, 2006 at 16:00 pm EST.
[14] MIT Computer Science and Artificial Intelligence Laboratory Mesh network development,http://pdos.csail.mit.edu/roofnet/doku.php, last time accessed was accessed on September 16, 2006 at 16:00 pm EST.
[15] Mobile Ad Hoc Network (MANET) Charter. http://www.ietf.org/html.charters/manet-charter.html, last time accessed was on September 16, 2006 at 16:00 pm EST.
[16] DSDV (Highly Dynamic Destination-Sequenced Distance Vector routing protocol) - C. E. PERKINS, P. BHAGWAT Highly Dynamic Destination-Sequenced Distance Vector (DTDV) for Mobile Computers Proc. of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp 234-244.
[17] OLSR (Optimized Link State Routing Protocol) - PHILIPPE JACQUET, PAUL MUHLETHALER, AMIR QAYYUM, ANIS LAOUITI, LAURENT VIENNOT, THOMAS CLAUSEN Optimized Link State Routing Protocol (OLSR), RFC 3626.
[18] Ad-hoc On-demand Distance Vector - C. PERKINS, E.ROYER AND S. DAS Ad hoc On-demand Distance Vector (AODV) Routing, RFC 3561

[19] Dynamic Source Routing - DAVID JOHNSON, DAVID MALTZ, YIH-CHUN HU: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks, Internet Draft, draft-ietf-manet-dsr-10.txt, work in progress, July 2004 / DAVID B. JOHNSON, DAVID A. MALTZ: Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Thomas Imielinski and Hank Korth (Editors), Vol. 353, Chapter 5, pp. 153-181, Kluwer Academic Publishers, 1996
[20] The North American Network Operators' Group, www.nanog.org, last time accessed was on September 16, 2006 at 16:00 pm EST.
[21] Nortel's Wireless Mesh Network solution, www.nortel.com/corporate/news/collateral/ntj2_wireless_mesh.pdf, last time accessed was on September 16, 2006 at 16:00 pm EST.
[22] Micrsoft product documentation Configuring wireless network clients http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wlan_client_configuring_concept.mspx?mfr=true, last time accessed was on September 16, 2006 at 16:00 pm EST.
[23] OPNET Technologies, Inc. http://www.opnet.com, last time accessed was on September 16, 2006 at 16:00 pm EST.

Appendix A – Acronyms used in this thesis

ABR	Area Boarder Router
AMR	Access Mesh Router
AODV	Ad hoc On-Demand Distance Vector
AS	Autonomous System
BDR	Backup Designated Route
BER	Bit Error Rate
BGP	Boarder Gateway Protocol
DR	Designated Route
DSDV	Destination Sequence Distance Vector
DSL	Digital Subscriber Line
DSR	Dynamic Source Routing
ETX	Expected Transmission count
LQSR	Link Quality Source Routing
LSA	Link State Advertisements
MANET	Mobile Ad-hoc NETwork
MCL	Mesh Connectivity Layer
MR-LQSR	Multi-Radio Link Quality Source Routing
OLSR	Optimized Link State Routing
OSPF	Open Shortest Path First
QoS	Quality of Service
RREP	Route REPly
RREQ	Route REQuest
RTT	Round-Trip Time
SPF	Shortest Path First
TC	Topology Control
WCETT	Weighted Cumulative Expected Transmission Time
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WMN	Wireless Mesh Network
WMR	Wireless Mesh Router

Appendix B – Scenarios configuration

Scenarios configuration for protocol comparison based on overhead traffic and average response time at node_0. All scenarios have 12 wireless fixed routers, and two wireless nodes. Distance between router is set to 600 meters with transmission power of 5 mW. Ping, parameters are set with startup time at 10 seconds, maximum repetition time was unlimited, counts was set to 10, and inter repetition time was set to three different sets (10, 20, 30 seconds). Finally, protocol hello times were set to (1, 5, 10 seconds). Measured Control traffic out of routers interfaces and first ping response time at Node_0.

B.1 AODV scenario Configuration

All IP addresses are set up on physical interfaces as shown in Figure B-1.

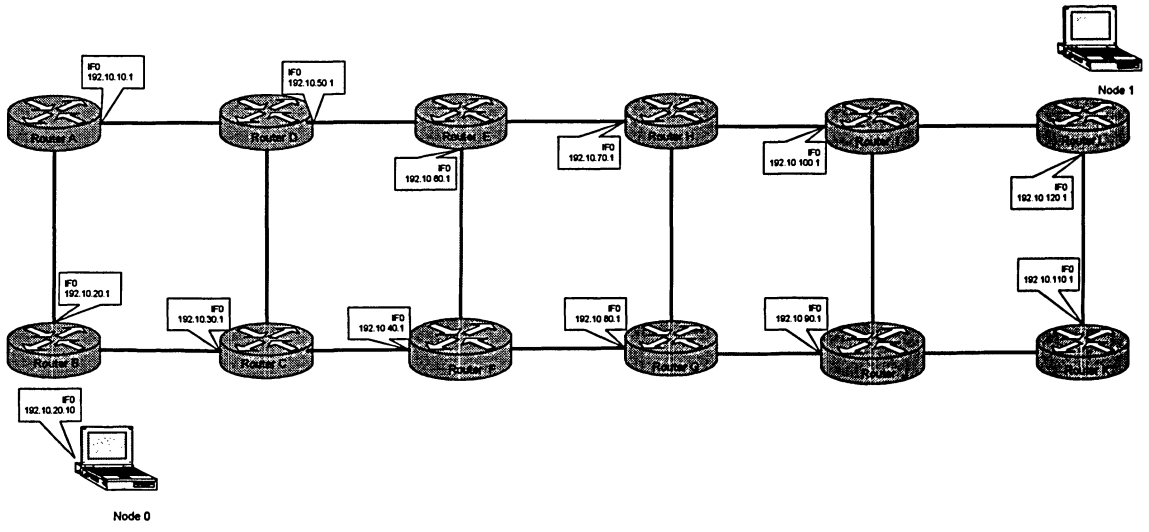

Figure B-1: AODV scenario routers IP configurations

B.2 OSPF scenario configuration

All IP addresses are set up subinterfaces of one physical wireless interface as shown in Figure B-2.

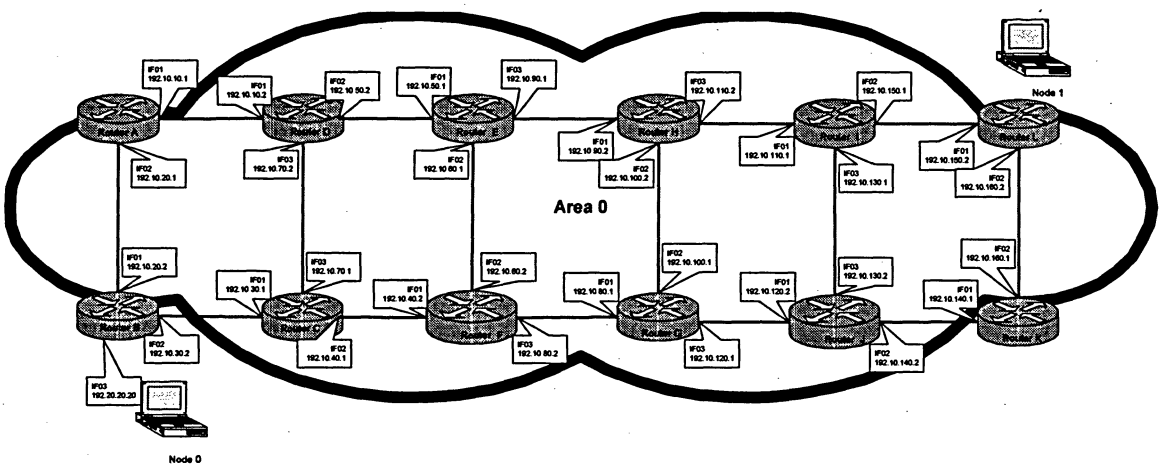

Figure B-2: OSPF scenario routers IP configurations

B.3 OLSR scenario configuration

All IP addresses are set up on physical interfaces as shown in Figure B-3, turned on the second physical wireless interface.

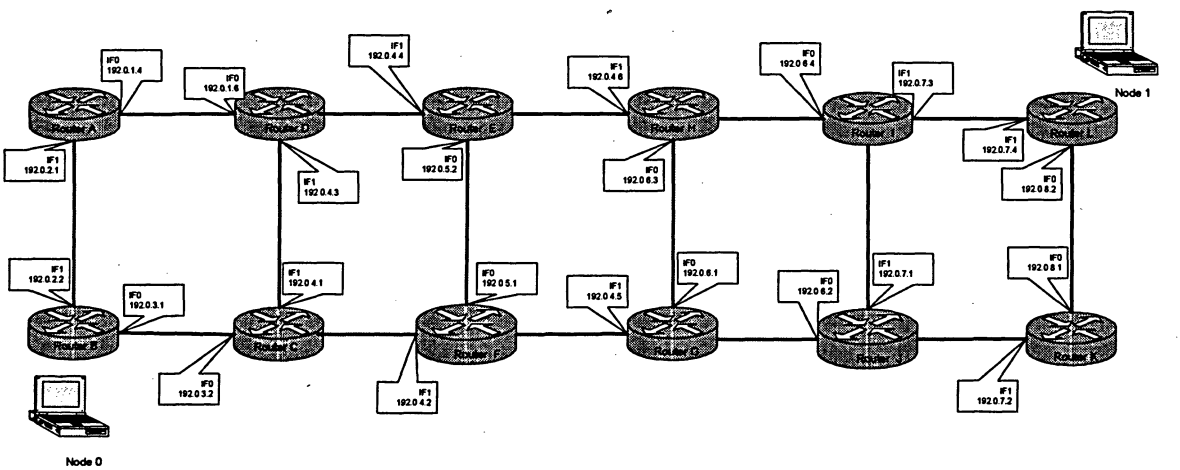

Figure B-3: OSLR scenario routers IP configurations

Appendix C - Bit Error rate in OpNet simulator

The following formulas are copy from OPNet code, and factors affecting Bit Error Rate. Where BER is bit error rate and SNR signal to noise ratio and proc_grain is process gain.

$$BER = SNR + proc\_gain \quad \text{(B-1)}$$

Where SNR is factor of received power and noise as shown in equation B-2

$$SNR = 10 \log \{rcvd\_pwr/(accum\_noise + noise)\} \quad \text{(B-2)}$$

Where rcvd is received power, accum_noise is accumulated noise and bkg_noise is background noise. Received power and noise are the main factors where received power is function of in bound transmit power and transmission bandwidth as shown in equation B-3 and B-4.

$$rcvd\_pwr = in\_bound\_tx\_pwr \times path\_loss \times (tx\&rx\ gain) \quad \text{(B-3)}$$

$$in\_bound\_tx\_pwr = \{tx\_pwr \times (bandmax - bandmin)/tx\_bw\} \quad \text{(B-4)}$$

Where tx_pwr is transmission power, tx&rx transmission and receiving gain, tx_bw transmission bandwidth.
The second major factor in SNR equation is background noise, equations B-5, B-6, B-7 and B-8 explains other factors effecting noise.

$$noise = amb\_noise + bkg\_noise \quad \text{(B-5)}$$

$$amb\_noise = rx\_bw \times amb\_noise\_level \quad \text{(B-6)}$$

bkg_noise = (rx_temp + bkg_temp)x rx_bw x boltzman (B-7)

rx_temp = (rx_noiseFigure – 1) x 290 (B-8)

Where amb_noise is ambient noise, rx_bw is received bandwidth, bkg_temp is background temperature. By changing noise factors and checking results on signal to noise ratio, there wasn't noticeable change on SNR because of noise value is very small and many factors can be neglected like noise Figure and background temperature. Therefore, the other factor that can make an effect on SNR equation is by changing tx_pwr in equation B-4 had an effect on SNR and subsequently on BER and that led to number of different convergence event.