EE 440 Data Communications and Networking

Project Report: Healthcare Network System

Project Spring: 2015

Team: DigiCom Networks

Team Members

Name	CIN
Babar Hassan Baig	304 XXXXXX
Nikhil A Kothari	304 XXXXXX

Table of Contents

Design Objective:

Today, healthcare centers generally conduct business with use of multiple integrated healthcare information systems. However, a network does not exist for each system, rather, it must be designed, and operated as a single, common infrastructure. Since a network system failure can lead directly to entire healthcare center routines and operations coming to a halt, a 'Non-stop Network' is one of the most important components within healthcare administration. Our team is taking a challenge to design a Local Area Network for the healthcare center. There are 6 main key requirements in designing a healthcare network.

- Security of personal and critical information. This includes internal and external threads.
- Redundancy and preventive measures against network / link failures.
- Effective use of Wireless LAN.
- Supports ease future expansions.
- Ease of operation.
- Cost effective.

Key statistics of the Healthcare Network system:

- Healthcare building consists of 3 floors.

- There are 18 main departments including administration, account dept, Human Resource dept, OBGYN, Pediatrics, medical records, nurse office, conference room, lab, material management, 12 physician offices.

- Healthcare center has 85 employees.

- 1 patients lobby at ground and first floor each.

Scope of the Project:

Here we would like to define some of the main features of our architecture.

- ***Redundancy and preventive measures against system failures***

If a hospital network stops suddenly, running applications shutdown. Therefore, a network system failure is a serious problem directly linked with system-wide hospital applications such as accounting or medical services. In order to construct a 'Non-stop Network,' it is necessary to ensure network device and path redundancy and enhance its reliability. By doing so, it becomes possible to keep network downtime at a minimum in the event of system failure. Sometimes a problem caused by human error may cause the entire network to shut down. It is also important to take measures to prevent unnecessary trouble, particularly network loops, when constructing a non-stop network.

- ***Secure and reliable network***

If personal or critical information is leaked or compromised, such as electronic medical charts, it can be very damaging to patients. Together with physical management (such as antitheft devices, limiting access to patients' rooms) using PCs and the server, the following measures must be taken on the network system:

Security measures are based on the proper control of various IT devices. For example, the possibility of computer virus infections must be minimized, since they can be caused by private PCs brought in from outside, unauthorized access via the Internet from outside the network, or even from within the hospital LAN. Therefore, firewall or virus protection is needed for the Internet, and network authentication must be in place to prevent the use of unauthorized PCs for LAN-related problems.

When constructing a regional alliance-based healthcare network via the Internet, it is necessary to build a VPN (Virtual Private Network). By doing so, even with access to public networks like the Internet, the virtual tunnel with encrypted communication safely connects all the LAN terminals. The security measures above are not automatic, but are established as post-installation steps. Following a strict protocol on a daily basis is crucial for their success.

- ***Effective use of Wireless LAN***

Today, in a hospital that includes patient rooms, the use of Wireless LAN (WLAN) technology is growing as people use laptops and other devices. While WLAN service is an effective way of providing Internet access to inpatients as a hospital amenity, adequate security measures must be taken when implementing an open LAN environment.

- ***Ease of operation***

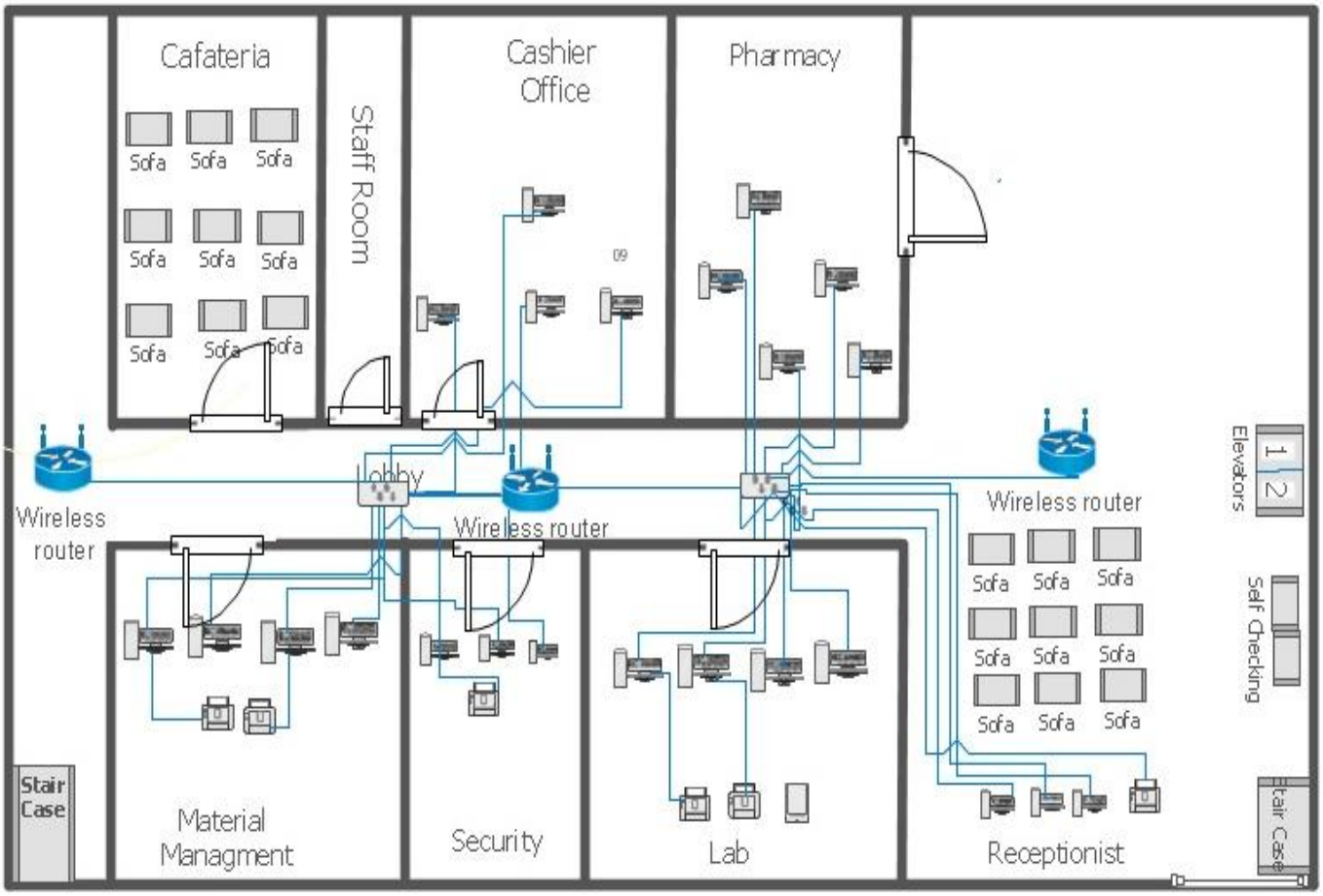
Early detection and restoration of system failures with the improvement in system functions of operation and control. By constantly monitoring network devices, early detection of a system failure can facilitate a quick recovery. For improvements in operation and control performance, it is highly important to use SNMP (Simple Network Management Protocol).

Healthcare floor plan:

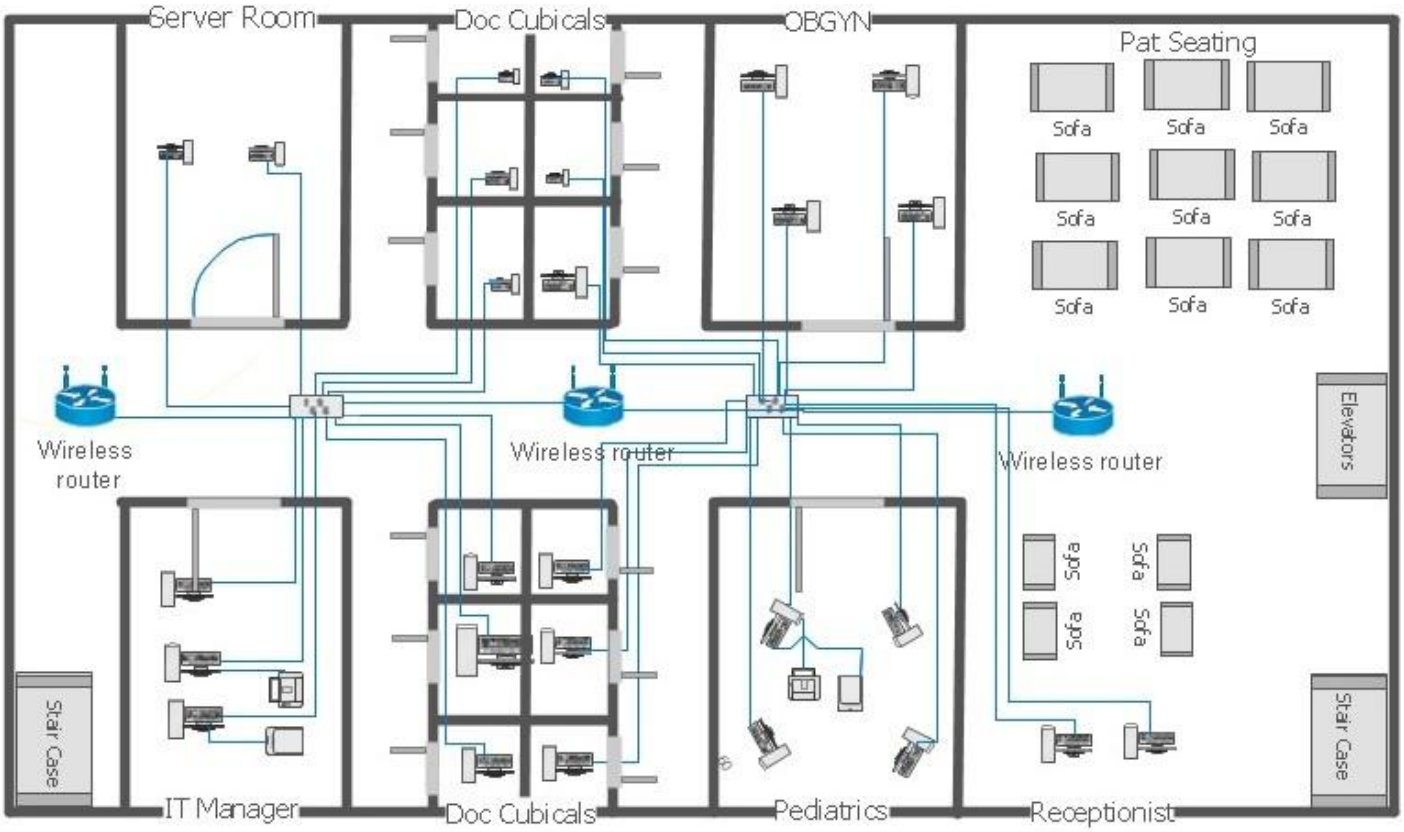
Floor plan plays a vital role in designing an architecture of the network and communication devices. This includes detail study of floor dimensions, department size, coverage areas.

Here we would like to draw and explain the need of network design.

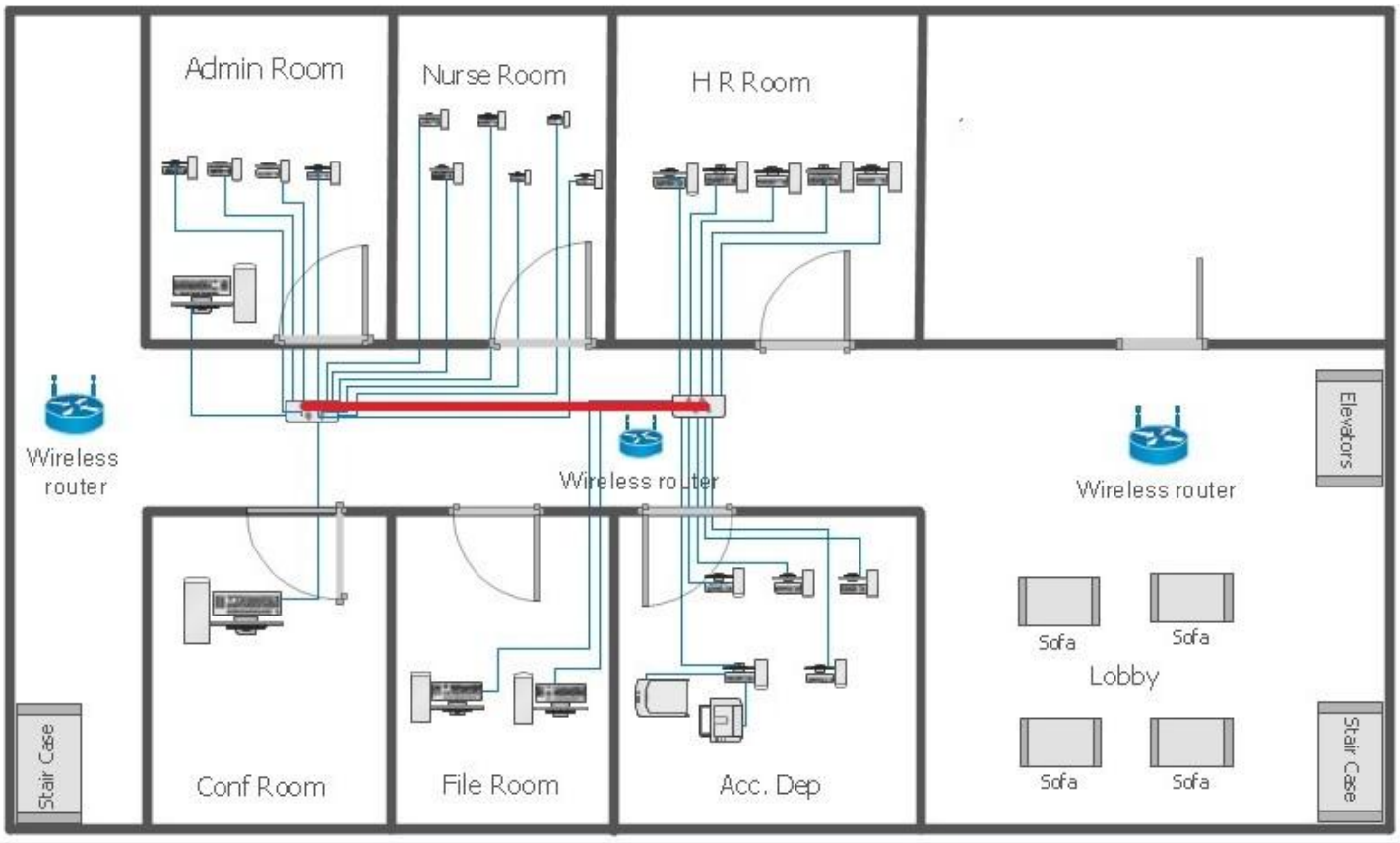
Ground floor:



First floor:



Second floor:



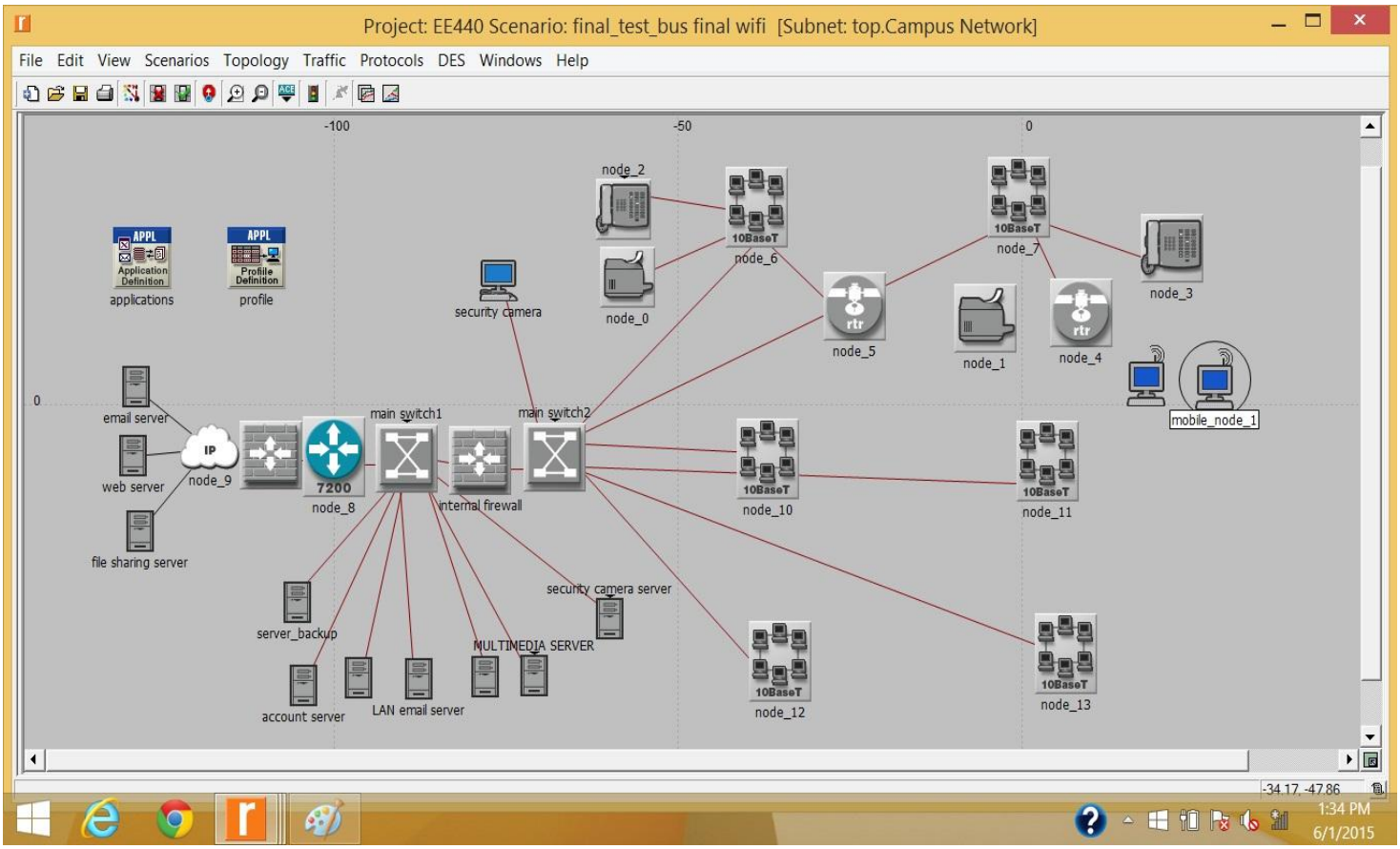
Our Approach and Research:

There are several ways to design a network architecture but being a professionals, its our responsibility to choose the best design which would have excellent implication over the performance of the network. As a part of our goal, we should also have to cover different aspects of this network architecture which highly desired to have a secure, redundant, non-stop network as we are dealing with patients life, our network should be error free. As our network directly deals with both internal and external nodes, it should be a safer network for its general users as well as high level confidential data transfer which include medical record number and social security numbers. For this we must protect the system from both internal and external threads.

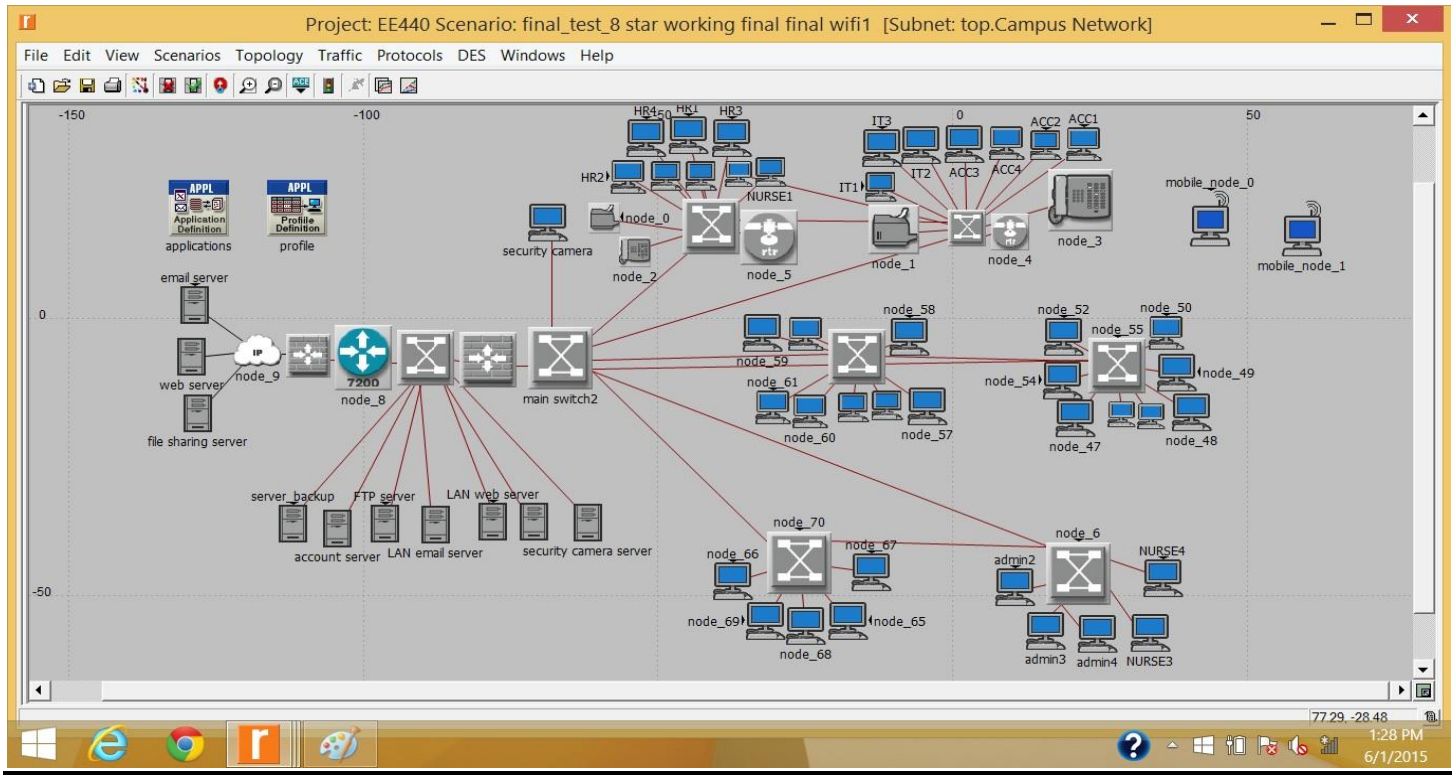
As we were asked to make our architecture flexible, so it should also support the future expansions with a least and minimal cost. It is not a professional way to run the cable to entire building if ever we need to add 6 more nodes of adjacent room or floor.

To support above requirements, our team comes up with two main and famous topologies in networking industry, Star and Bus topologies. Before we select and start testing the topologies, we should also study about their characteristics and performance. We should also consider the drawbacks of both topologies.

Bus Topology



Star Topology:



Why we are considering Star Topology:

Before we go any further, let us discuss some facts regarding both Bus and Star topologies.

Advantages of Star Topology:

- *As compared to Bus topology it gives far much better performance, signals don't necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of central hub.*
- *Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network. Similarly components can also be removed easily.*
- *Centralized management. It helps in monitoring the network.*
- *Failure of one node or link doesn't affect the rest of network. At the same time it is easy to detect the failure and troubleshoot it.*

Disadvantages of Star Topology:

- *Too much dependency on central device has its own drawbacks. If it fails whole network goes down.*
- *The use of hub, a router or a switch as central device increases the overall cost of the network*
- *Performance and as well number of nodes which can be added in such topology is depended on capacity of central device*.

Advantages of Bus Topology:

- *Easy to implement and extend*
- *Well suited for temporary networks (quick setup)*
- *Initially less expensive than other topologies*
- *Cheap*

Disadvantages of Bus Topology:

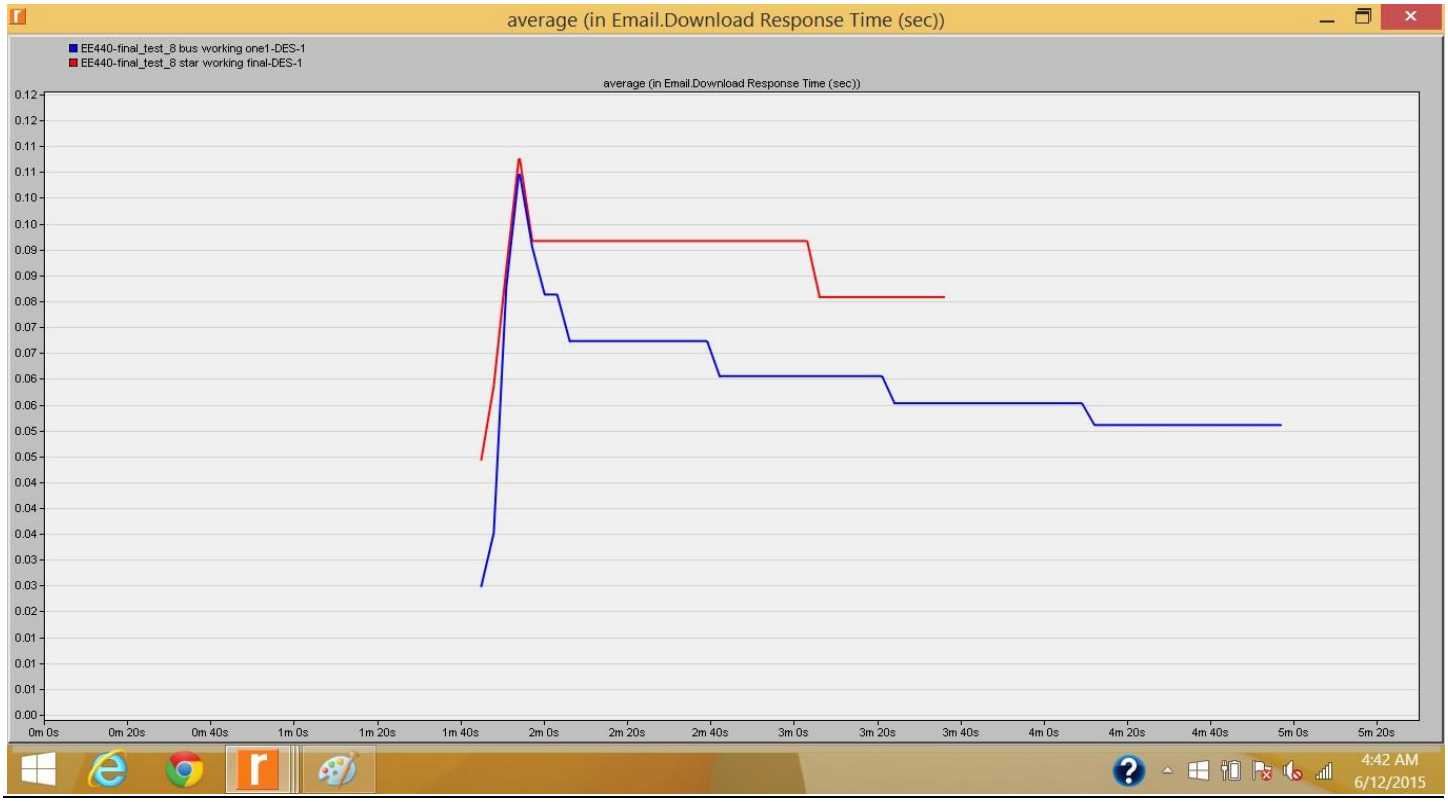
- *Difficult to administer/troubleshoot.*
- *Limited cable length and number of stations.*
- *If there is a problem with the cable, the entire network goes down.*
- *Maintenance costs may be higher in the long run.*
- *Performance degrades as additional computers are added or on heavy traffic.*
- *Low security (all computers on the bus can see all data transmissions).*
- *One virus in the network will affect all of them (but not as badly as a star or ring network).*
- *Proper termination is required.(loop must be in closed path).*
- *If one node fails, the whole network will shut down.*
- *If many computers are attached, the amount of data flowing causes the network to slow down.*

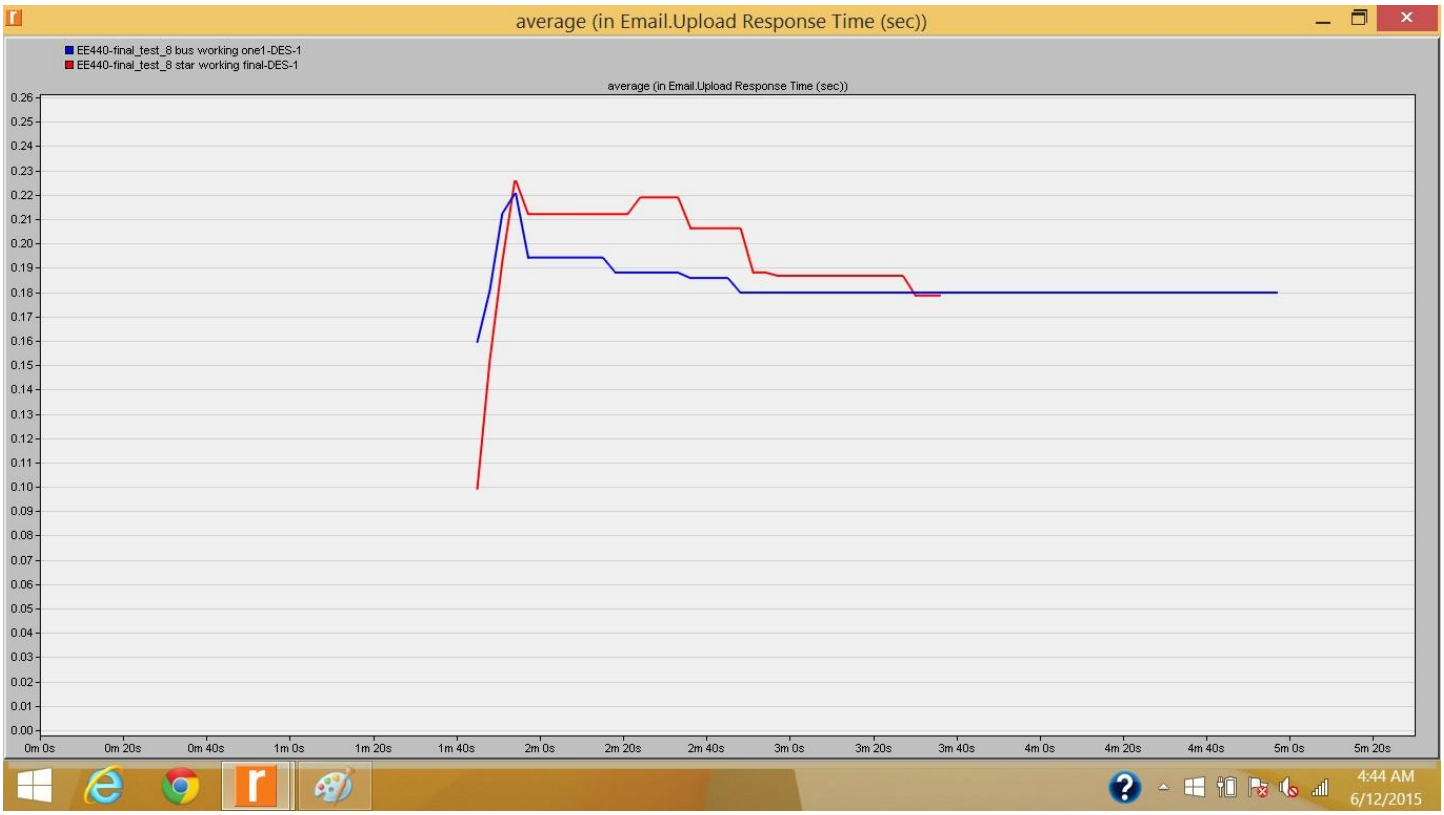
	Bus topology	Ring topology	Star topology
Structure	There is a single central cable(backbone)and all computers and al other devices connected to it.	All computers and other devices are connected in a circle.	There is a central host and all nodes connected to it.
Host existence	Depends on networks need.	Depends on network need.	Yes
Connection between nodes	it has no connection between nodes.	Yes.	No.
Host failure	Network can still run.	Network will fail.	Network will fail.

Test results for Star and Bus topologies:

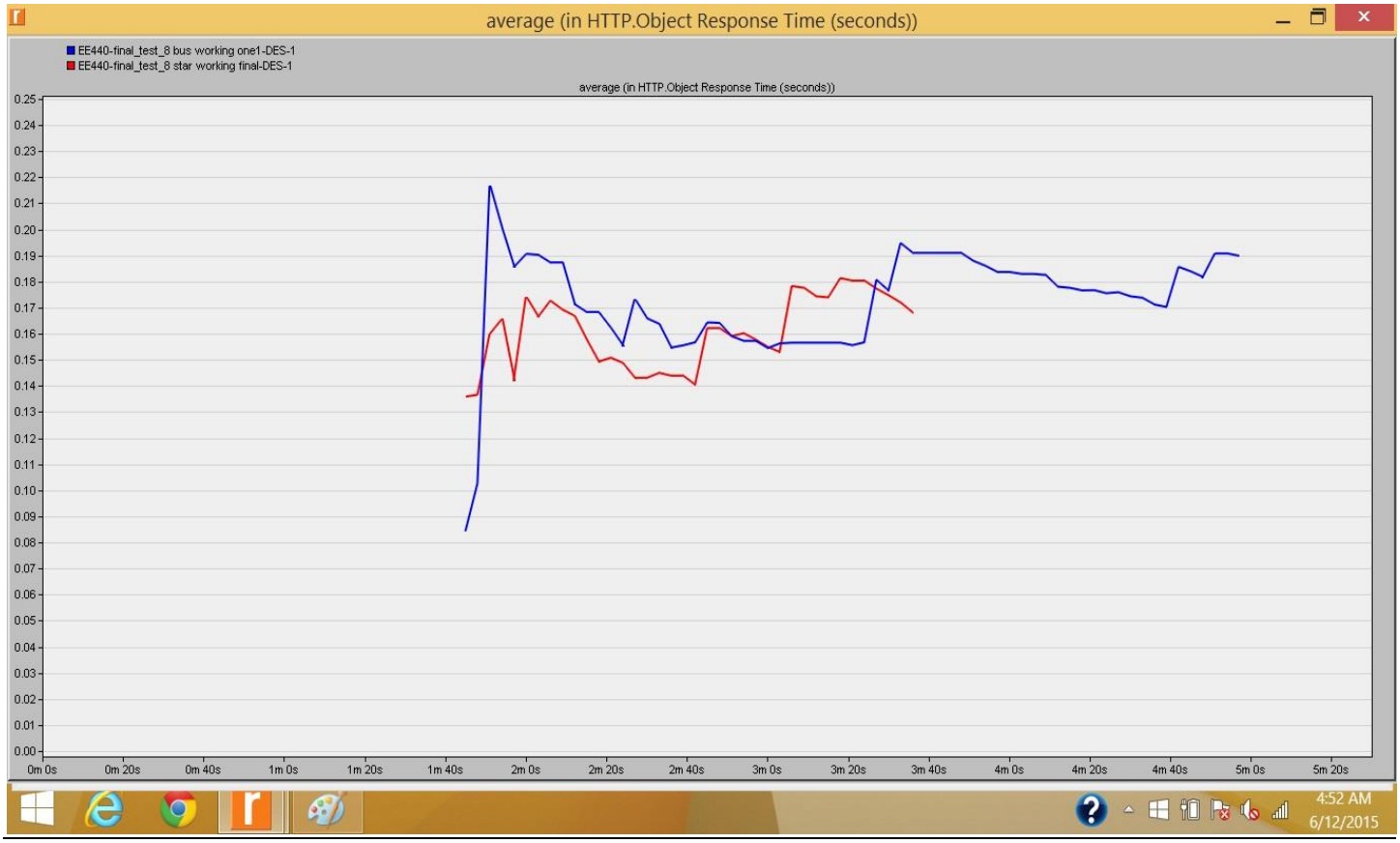
To justify and support our selection, we perform few tests between Star and Bus topologies.

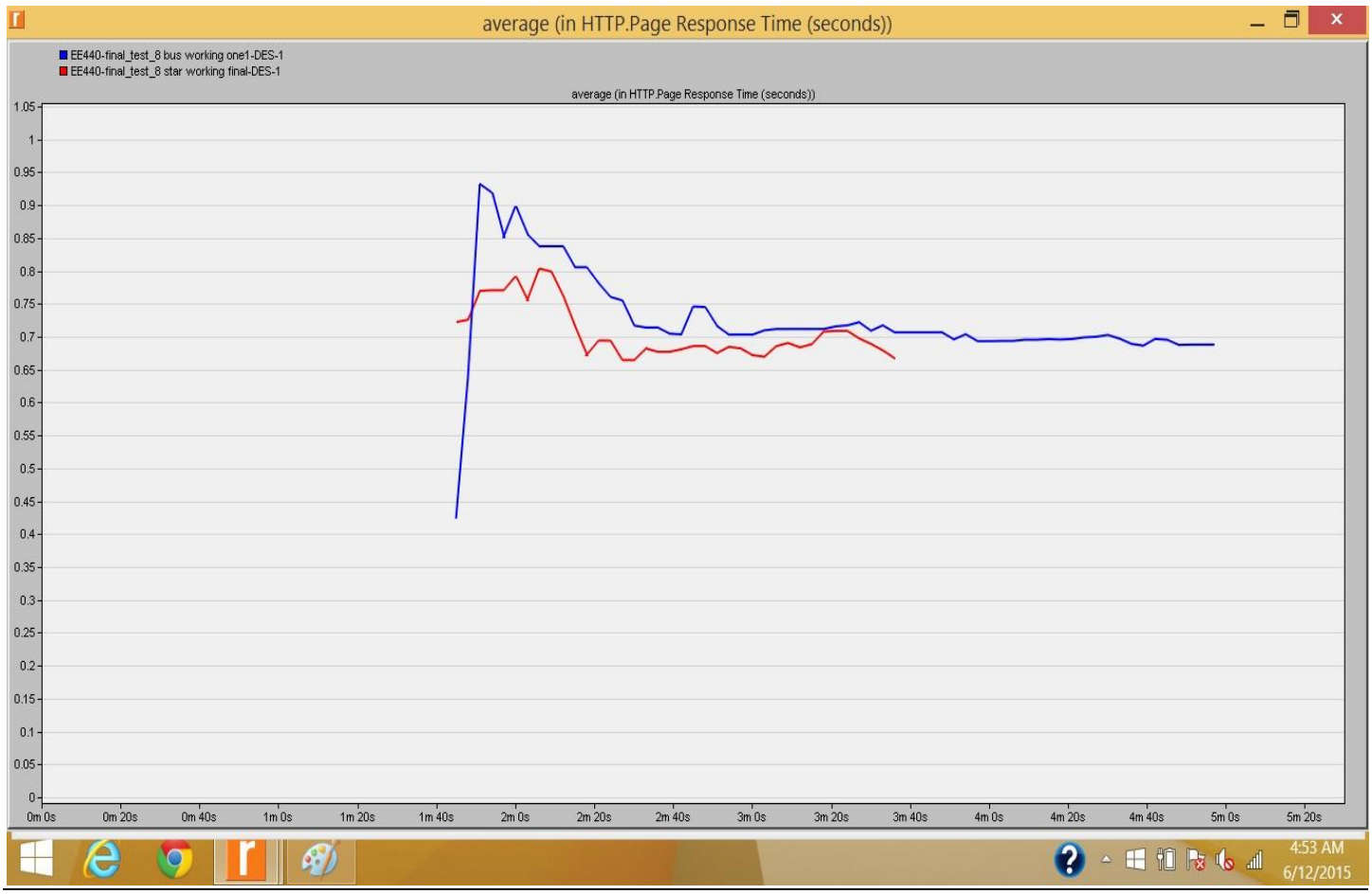
Email download and upload response time:



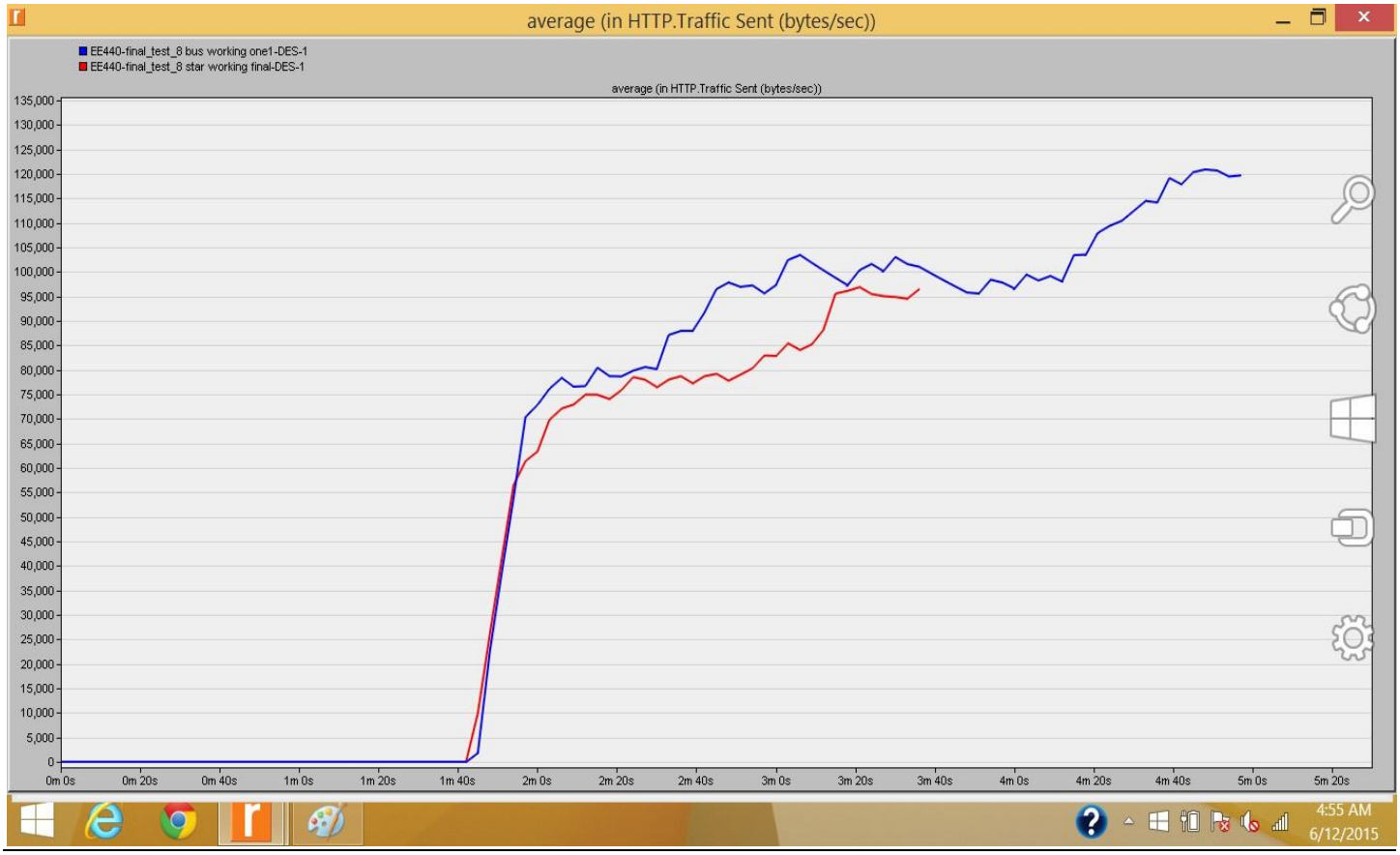


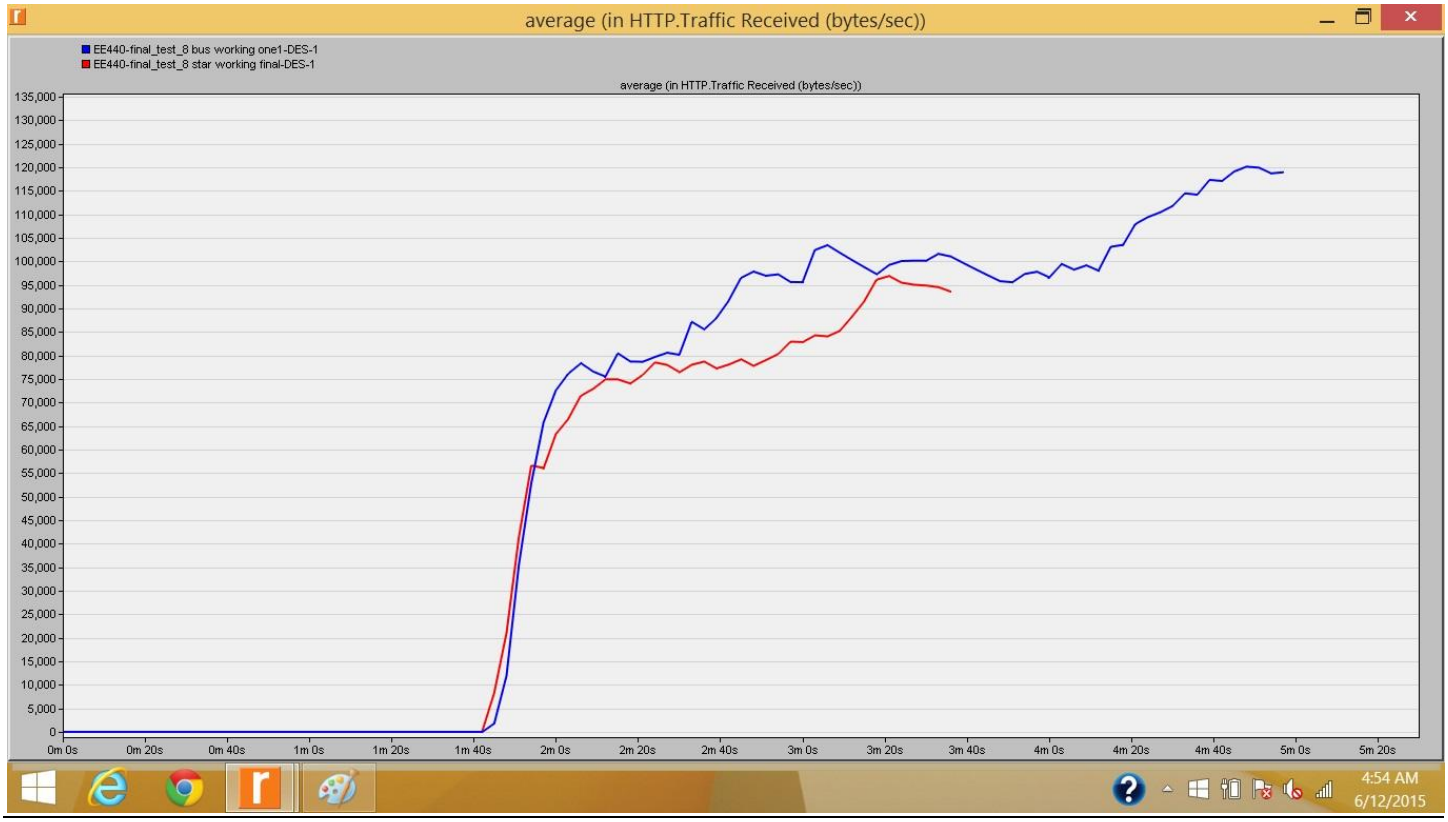
Http object & page response time:





Http traffic send & received:



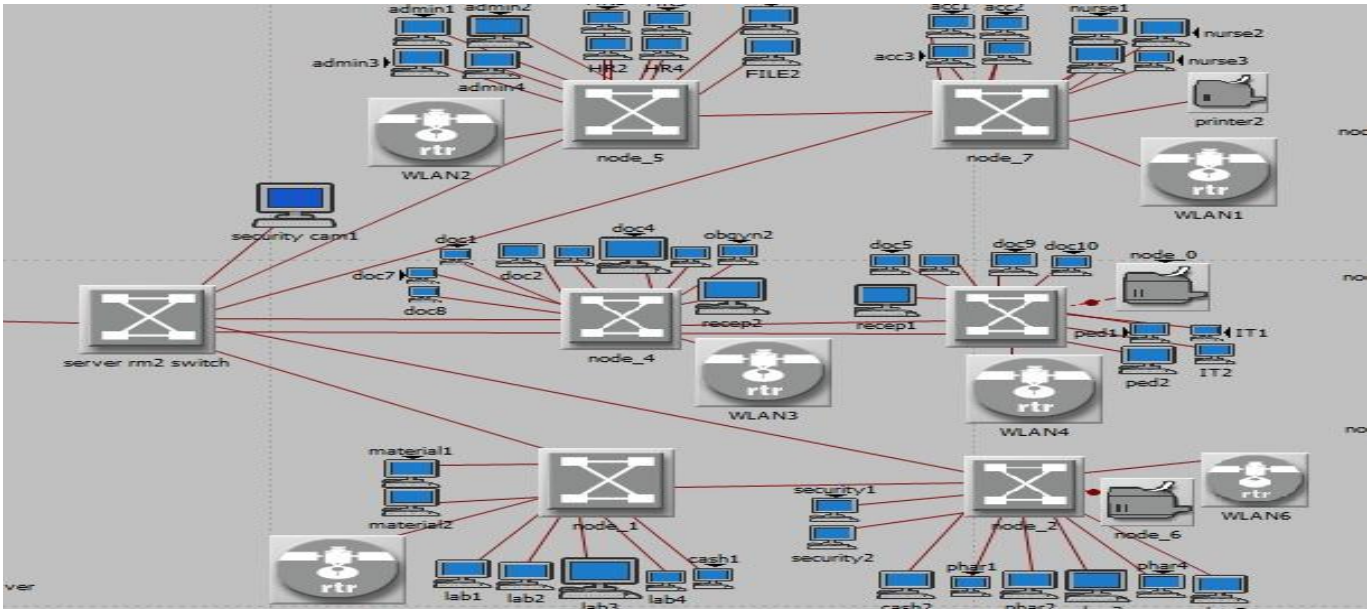


Final Statement:

Based on above test results, we decided to choose Star topology for our network architecture. As there is not much difference but Star topology is very beneficial for reliable, redundant and future expansion network.

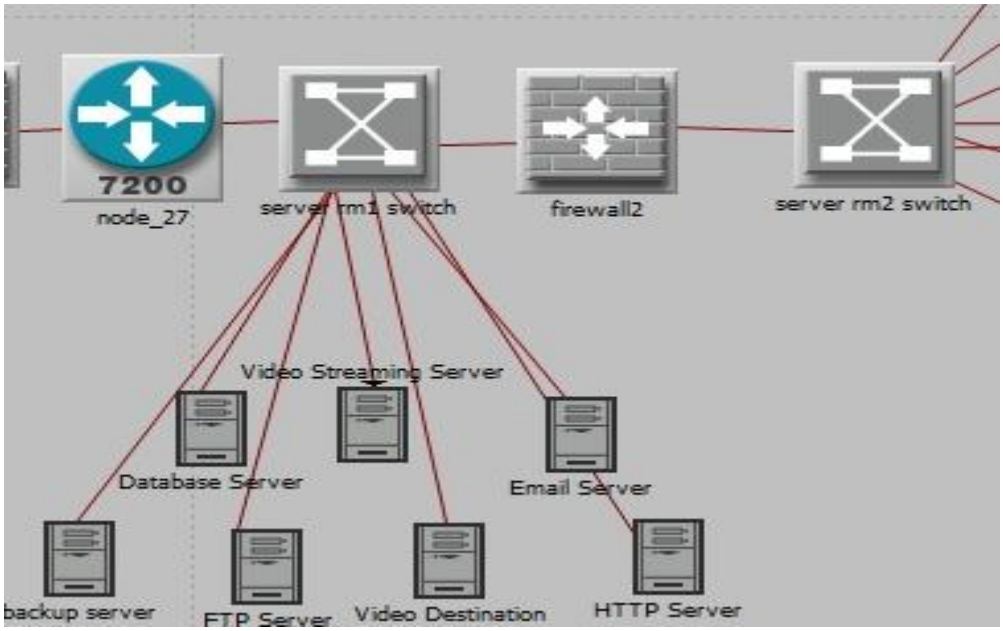
High-level Design plan:

After conduction a detail research and analysis, we choose the Star topology to build and architect our healthcare network. Our network will serve 80 work stations on every floor. We connect these work stations to the local floor switches, these local subnet switches than connect to main server room.

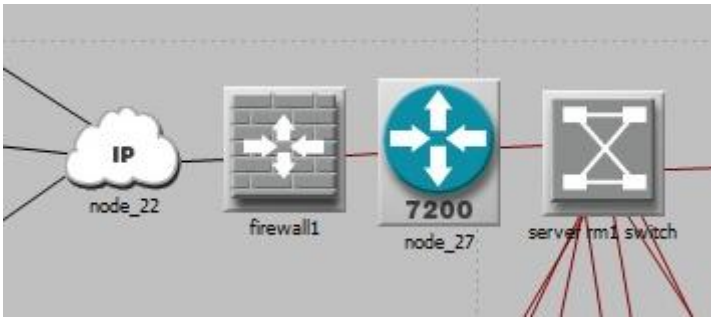


In our architecture, we decided to have server room at second floor. Having main server room in the middle of 2 floors has its own advantaged. First of all it will reduce the distance from any floor to the server room. For example, if we make a server room at ground floor, this will make it far from second floor's switch, this will effects the performance, reliability and increase the chances of errors as single long wire is never been a good design.

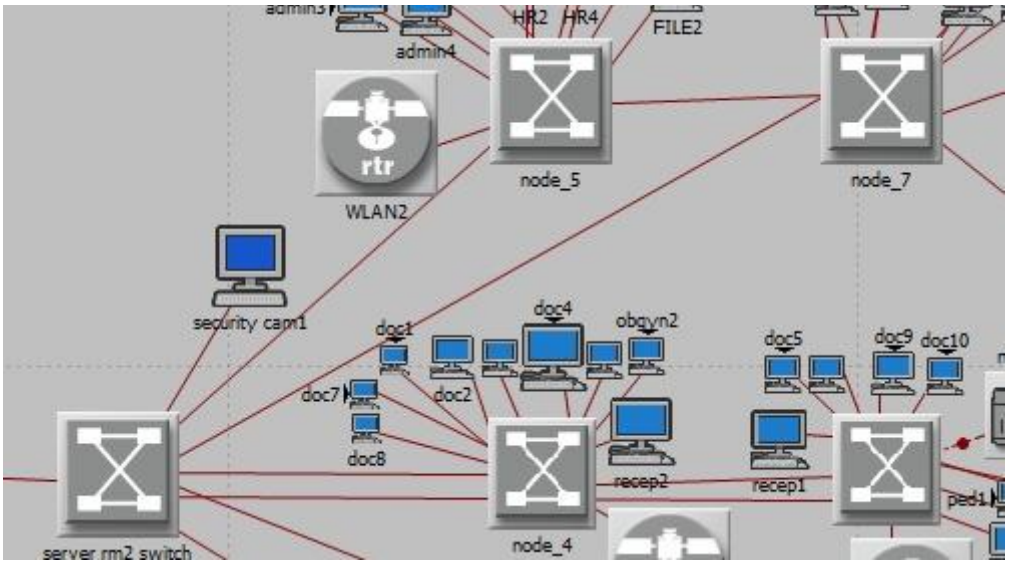
After receiving all subnet connection, we will connect them to the 1st server room switch. We plan to have 2 main switches in the server room. One is connected to all local subnets and the other is connected to local servers and the router. To make our network protected from internal threads, we put the firewall between two switches as it will blocks all the illegal traffic to get access from local subnets to LAN's servers.



To further secure our network from external threads, we also put a firewall between the router and the ip cloud. This will protect our whole local area network from outer illegal traffic and hackers.

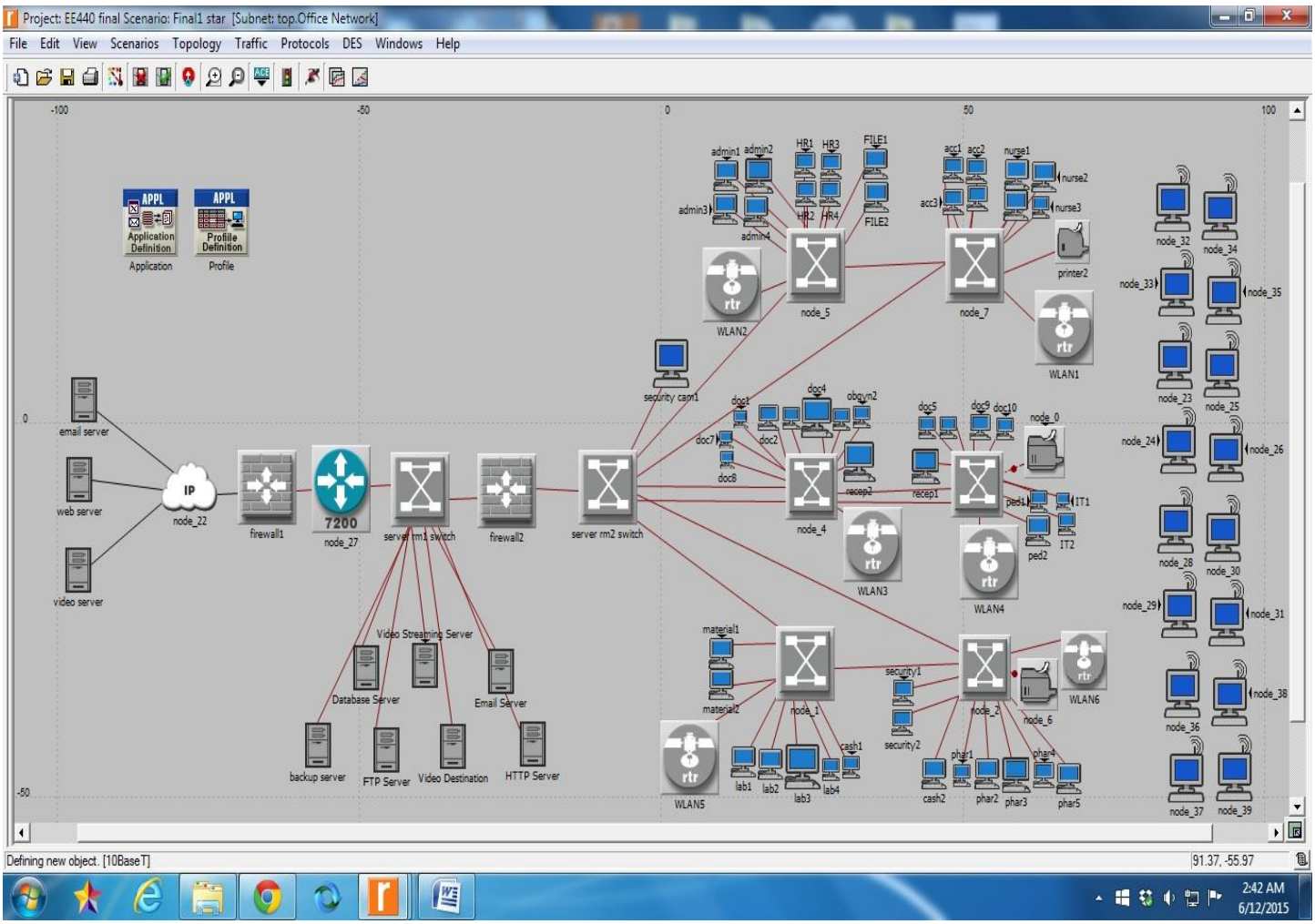


Redundancy is one of the major feature of our network design. To make sure that in case of any down link, our network will provide a non-stop service and keep the system running without any interruption. Our approach is to have multiple connections between two switches which will provide an alternative route for the traffic.



As you can see, the server switch is connected to 1st and 2nd floor's switches and having a multiple connections. So if one link is down, the data could be easily transmitted to the other switch from an alternative link.

Main Network model:



Components and Equipments:

To design our network, we need the following equipments and network devices. Here we will like to give a quick list and their functions.

- *Ethernet workstations* *75*
- *Ethernet 16 switches* *8*
- *Ethernet server* *7*
- *Cisco 7200 router* *1*
- *Firewall* *2*
- *Wireless LAN Ethernet router* *8*
- *10BaseT cable* *800 meters*

WorkStation: Ethernet Workstations.

General Node Functions:

The ethernet_wkstn node model represents a workstation with client-server applications running over TCP/IP and UDP/IP. The workstation supports one underlying Ethernet connection at 10 Mbps, 100 Mbps, or 1000 Mbps.

This workstation requires a fixed amount of time to route each packet, as determined by the "IP Forwarding Rate" attribute of the node. Packets are routed on a first-come-first-serve basis and may encounter queuing at the lower protocol layers, depending on the transmission rates of the corresponding output interfaces.

Protocols: *RIP, UDP, IP, TCP, IEEE 802.3 (Ethernet, Fast Ethernet, Gigabit Ethernet), OSPF.*

Interconnections:

Either of the following:

1) 1 Ethernet connection at 10 Mbps,
2) 1 Ethernet connection at 100 Mbps, or
3) 1 Ethernet connection at 1000 Mbps

Attributes:

Client Custom Application, Client Database Application, Client Email, Client Ftp, Client Remote Login, Client X Windows, Client Video Conferencing, and Client Start Time: These attributes allow for the specification of application traffic generation in the node.

Transport Address: *This attribute allows for the specification of the address of the node.*

General Function: workstation

Supported Protocols: UDP, IP, Ethernet, Fast Ethernet, Gigabit Ethernet, RIP, TCP, and OSPF.Port Interface Description: 1 Ethernet connection at 10 Mbps, 100 Mbps, or 1000 Mbps.

Switch: Ethernet16_switch.

General Node Functions:

The ethernet16_switch node model represents a switch supporting up to 16 Ethernet interfaces. The switch implements the Spanning Tree algorithm in order to ensure a loop free network topology. Switches communicate with each other by sending Bridge Protocol Data Units (BPDU's). Packets are received and processed by the switch based on the current configuration of the spanning tree.

Protocols: *Spanning Tree Bridge Protocol (IEEE 802.1D), Ethernet (IEEE 802.3).*

Interconnections:

1) 16 Ethernet connections at the specified data rate (10, 100, 1000 Mbps).

Restrictions: The switch can only connect LAN's of the same type (Ethernet to Ethernet, FDDI to FDDI, or Token Ring to Token Ring).

General Function: *switching*

Supported Protocols: Spanning Tree Bridge, Ethernet

Port Interface Description: Combination of up to 16 Ethernet ports (10 Mbps, 100 Mbps, or 1000 Mbps).

Firewall :

General Node Functions:

The ethernet2_slip8_firewall node model represents an IP-based gateway with firewall features and server support. Hence, it can be also called as a multihomed-server firewall node. It supports two Ethernet and eight serial line interfaces at selectable data rates. IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address. The Routing Information Protocol (RIP), the Open Shortest Path First (OSPF), the Border Gateway Protocol (BGP) or the Interior Gateway Routing Protocol (IGRP) protocols may be used to automatically and dynamically create the gateway's routing tables and select routes in an adaptive manner. This gateway requires a fixed amount of time to route each packet, as determined by the "IP Forwarding Rate" attribute of the node. Packets are routed on a first-come-first-serve basis and may encounter queuing at the lower protocol layers, depending on the transmission rates of the corresponding output interfaces.

Protocols: *TCP, RIP, UDP, IP, Ethernet, Fast Ethernet, Gigabit Ethernet, OSPF, BGP, IGRP.*

Interconnections:

1) 1 Ethernet connection at a selectable data rate

2) 1 Serial Line IP connections at a selectable data rate

Attributes:

"IP Forwarding Rate": specifies the rate (in packets/second) at which the gateway can perform a routing decision for an arriving packet and transfer it to the appropriate output interface.

"IP Gateway Function": specifies whether the local IP node is acting as a gateway. Nodes with only one network interface should not act as network gateways.

"RIP Start Time": specifies the simulation time (in sec) at which the gateways start sending routing updates to build the IP routing tables.

"RIP Process Mode": specifies whether the RIP process is silent or active. Silent RIP processes do not send any routing updates but simply receive updates. All RIP processes in a gateway should be active RIP processes.

"Proxy Server Information": Table that can be used to configure the proxy servers on this firewall node. Existence of a proxy server for a certain application makes this application acceptable through the firewall. Each forwarded packet may also experience an additional proxy server delay again based on the configuration of proxy servers.

General Function: *gateway, firewall, multihomed-server.*

Supported Protocols: *TCP, UDP, IP, Ethernet, RIP, OSPF, BGP, and IGRP.*

Port Interface Description:

2 Ethernet connections at 10 Mbps, 100 Mbps, or 1000 Mbps

8 Serial Line IP connections at selectable data rates

Link: 10bastT_int.

General Description:

The 10BaseT_int duplex link represents an Ethernet connection operating at 10 Mbps. It can connect any combination of the following nodes (except Hub-to-Hub, which cannot be connected) :

1) Station

2) Hub

3) Bridge

4) Switch

5) LAN nodes

Packet Formats: *Ethernet*

Data Rate: *10 Mbps*

Model Attributes:

"Propagation Speed": specifies the propagation speed (in meters/sec) for the medium. If the "delay" attribute of the link is set to "Distance Based", this speed is used to calculate the propagation delay based on the distance between two nodes.

7201 Router:

Benefits of the Cisco 7201 include the following (refer to Table 1 for details):

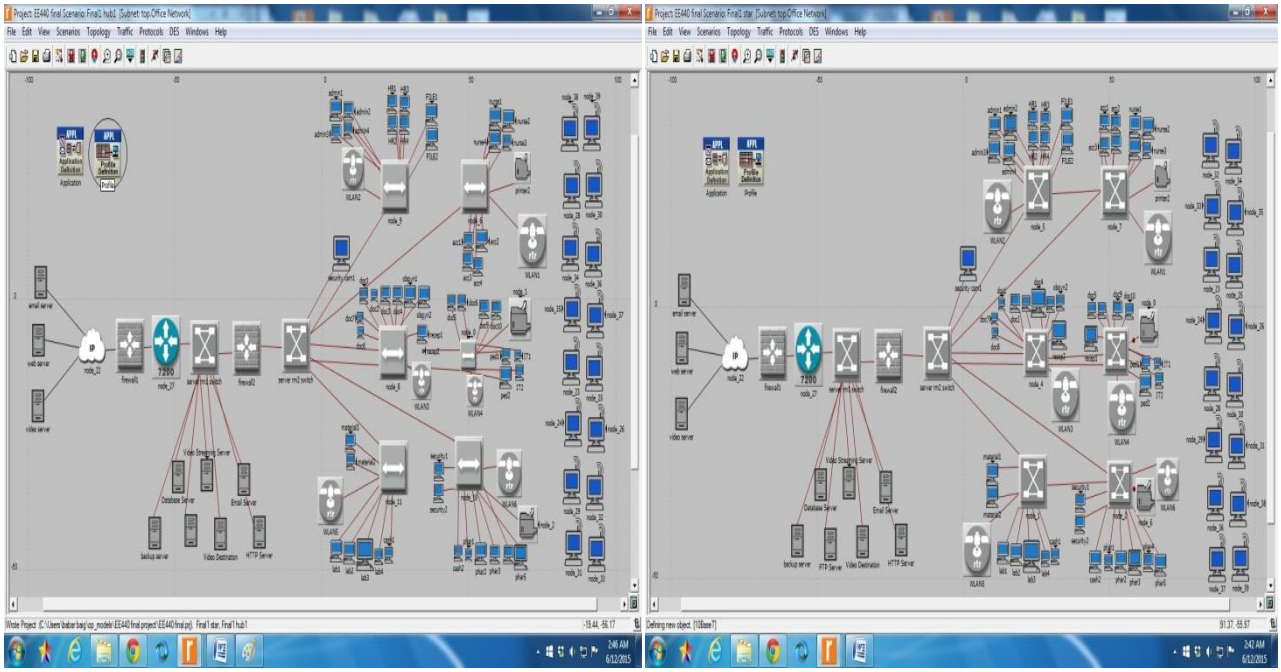
- Provides up to twice the performance compared to the Cisco 7301 – up to 2 million packets per second (2Mpps) in Cisco Express Forwarding
- Offers four built-in Gigabit Ethernet (GE) ports
- Provides one dedicated 10/100-Mbps copper Ethernet port for management
- Provides one USB port for general storage and security token storage
- Offers 1 GB of DRAM memory by default; upgradeable to 2 GB of available DRAM
- Offers greatly improved price/performance ratio
- Provides a single Cisco 7000 Series port adapter slot
- Supports complete Cisco IOS Software feature set
- Provides pluggable GE optics (Small Form-Factor Pluggable [SFP] optics)
- Has compact, power-efficient 1RU form factor
- Offers front-to-back airflow and single-sided management

Implementation and Simulation:

For our architecture we have choice to use different network equipments. Our primarily goal to choose cost effective but reliable and high performance equipments.

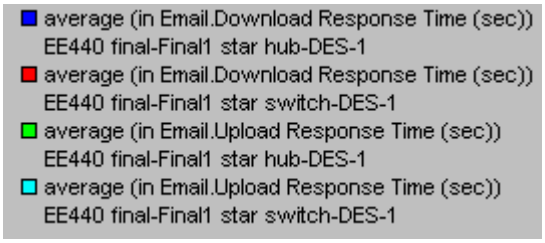
First we have to decide that what would we choose, switch or hub. As we studied earlier that both of them are pretty useful tools in networking industry but they have a difference in their price. Being a professional this is our job to test and justify our choice on the basis of facts. Here we have some technical details of switch and hub.

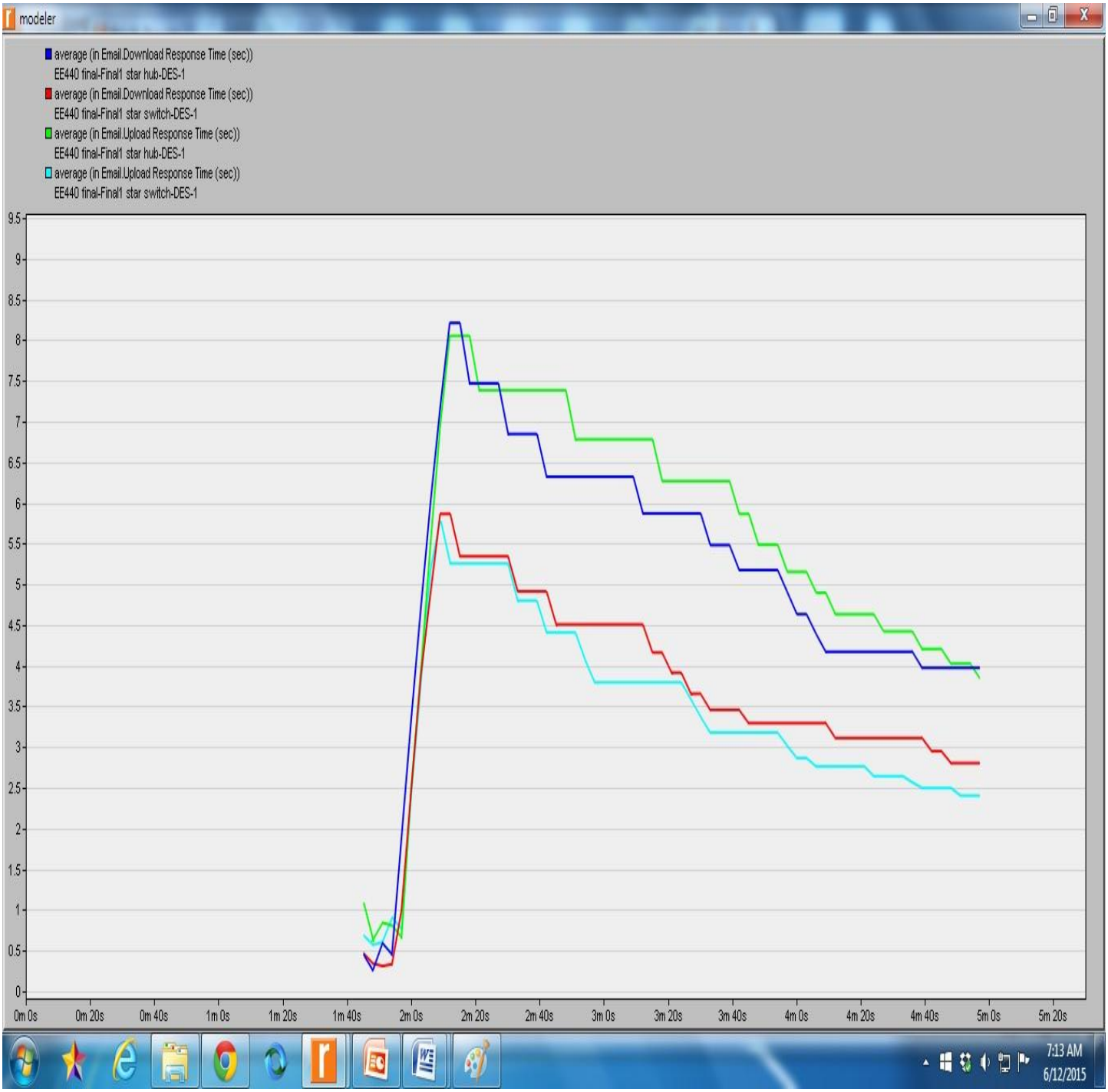
Switch	***Hub***
Data Link Layer	*Physical Layer*
Intelligent Device *Can recognize the MAC address*	*Not Intelligent Device* *Not recognize the MAC or IP address*
Switch Flood only First broad cast	*Hub forward the message without and reading from its all ports*
It is latest device and contains hundreds of ports depending upon the type of model	*IT is old device having less number of ports*
All the ports of a switch are connected with each other with a full mesh topology	*All the ports of hub are connected with each other with a single wire just like the bus topology*
The communication side it is full Duplex	*Communication inside it is half duplex*
Every computer connected to switch uses dedicated Bandwidth	*Every computer connected to the hub will use shared bandwidth as the number of computers increases bandwidth of each computer will decrease*
All ports have separate Collision Domains and Same Broadcast Domain	*All ports have same Collision Domain and Same Broadcast Domain*



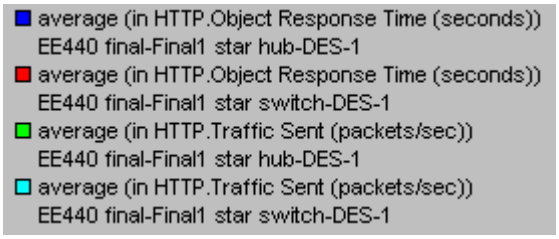
Test results of Switch vs Hub:

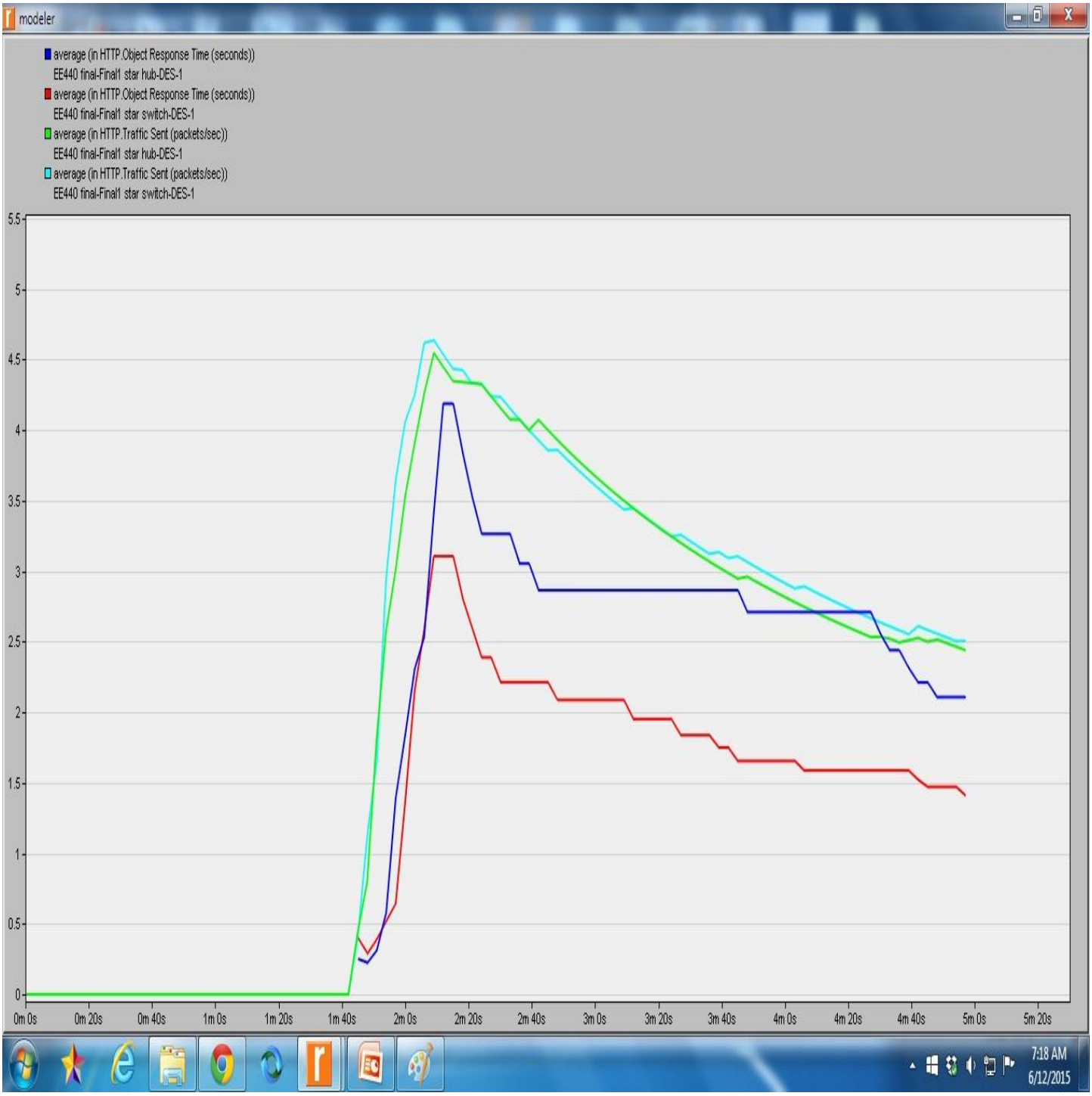
For email:





For Http:

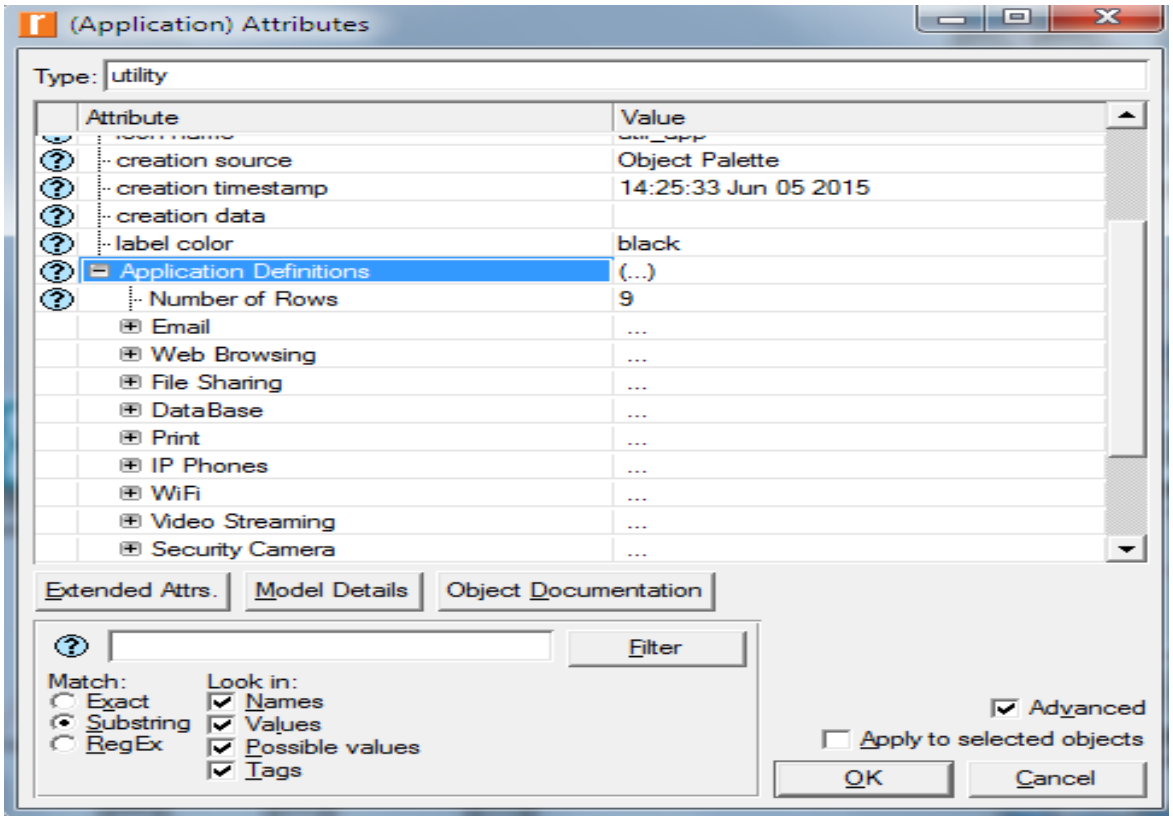




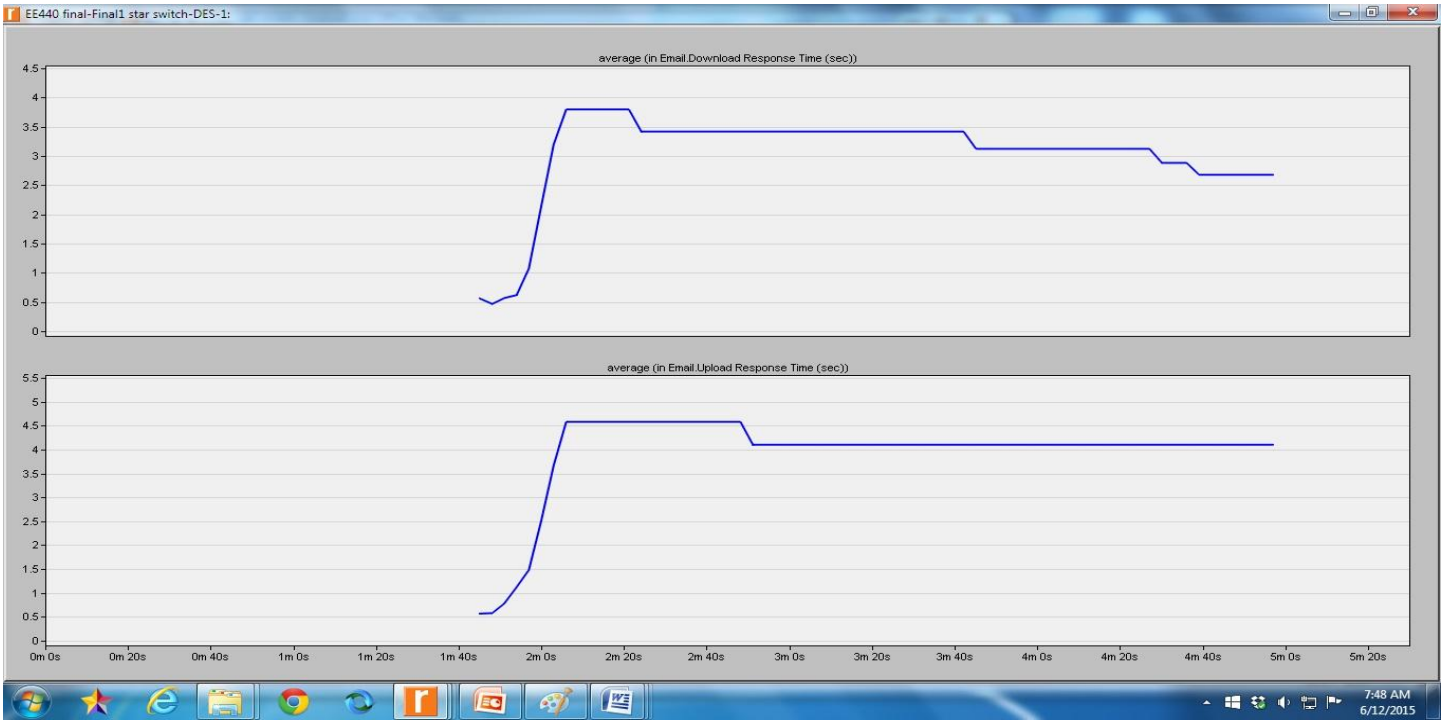
Based on above analysis, our conclusion is to choose switch as every computer connected to switch uses dedicated Bandwidth, all ports have separate Collision Domains and Same Broadcast Domain.

Applications:

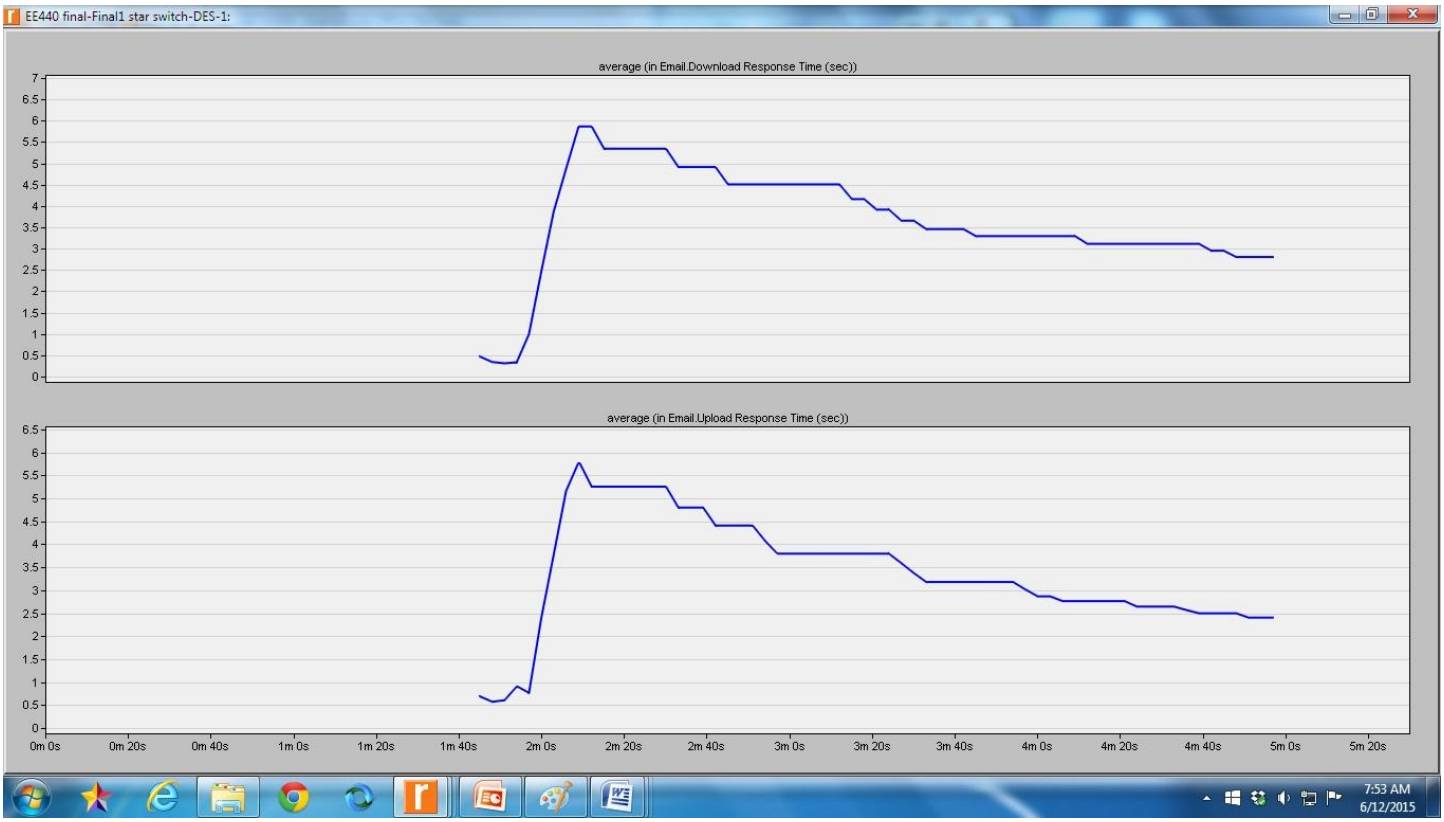
In our healthcare network, we are dealing with nine main applications. Here we will run applications on different traffic conditions.



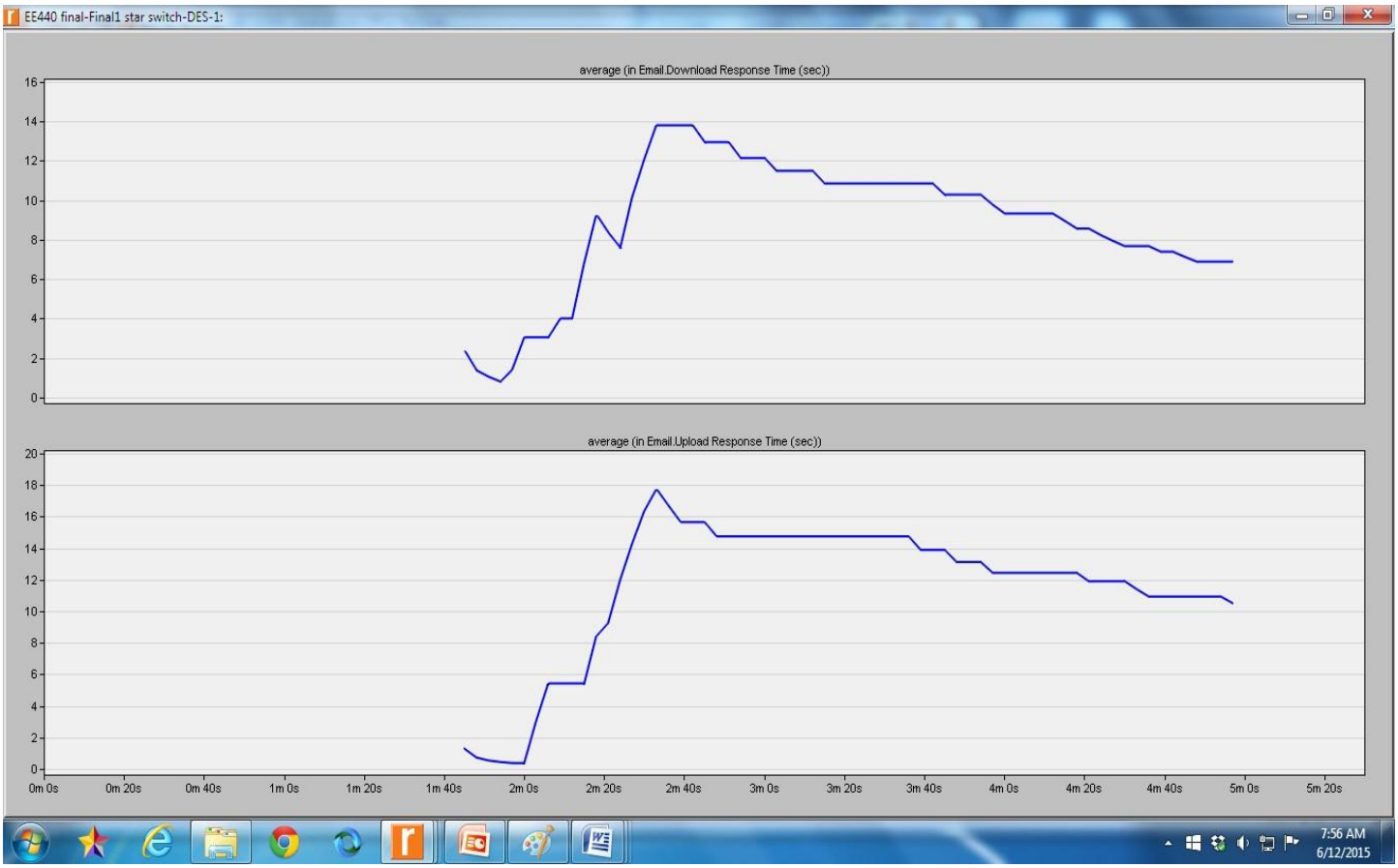
1.1 Email at Low load:



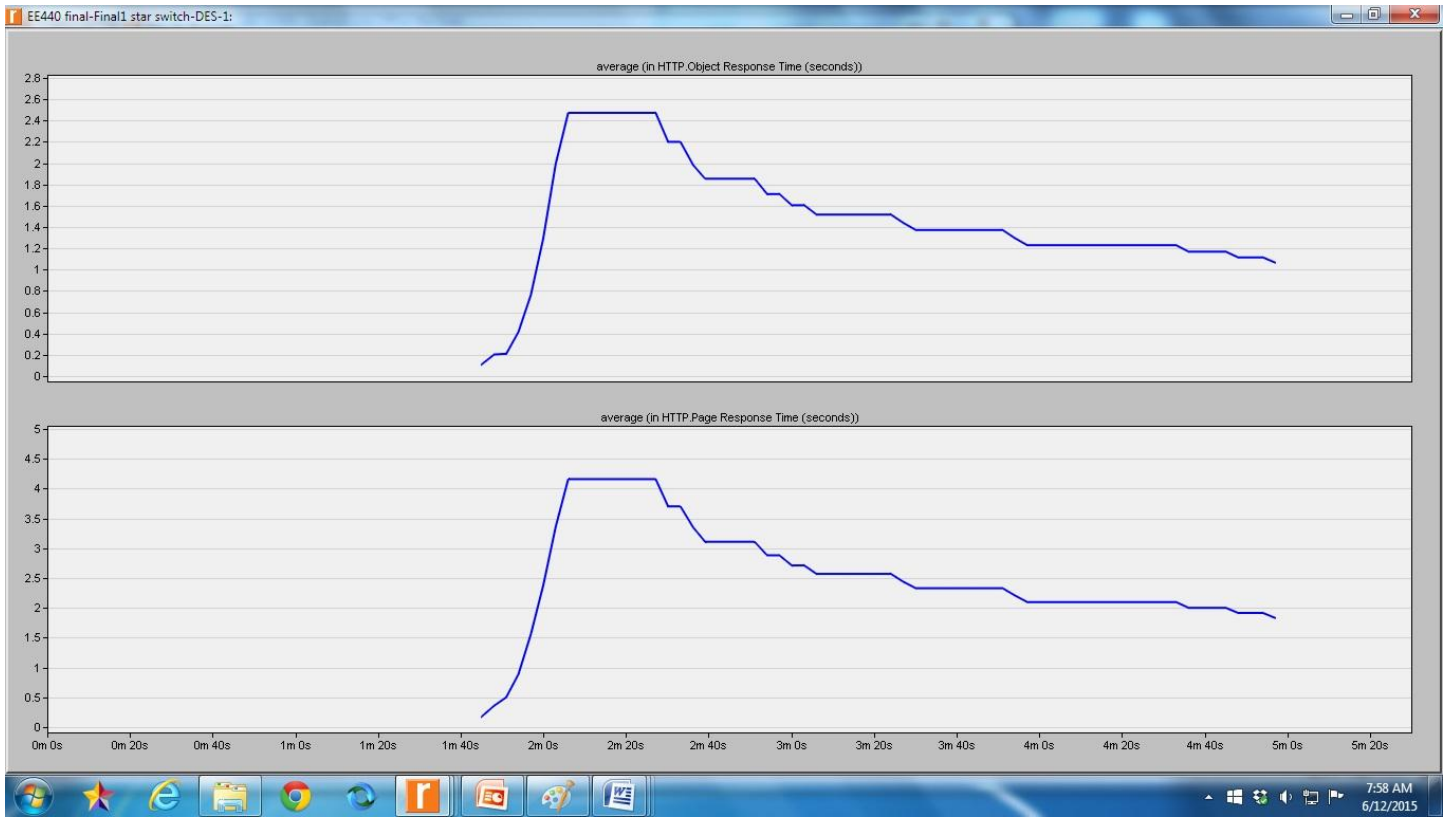
Email at medium load:



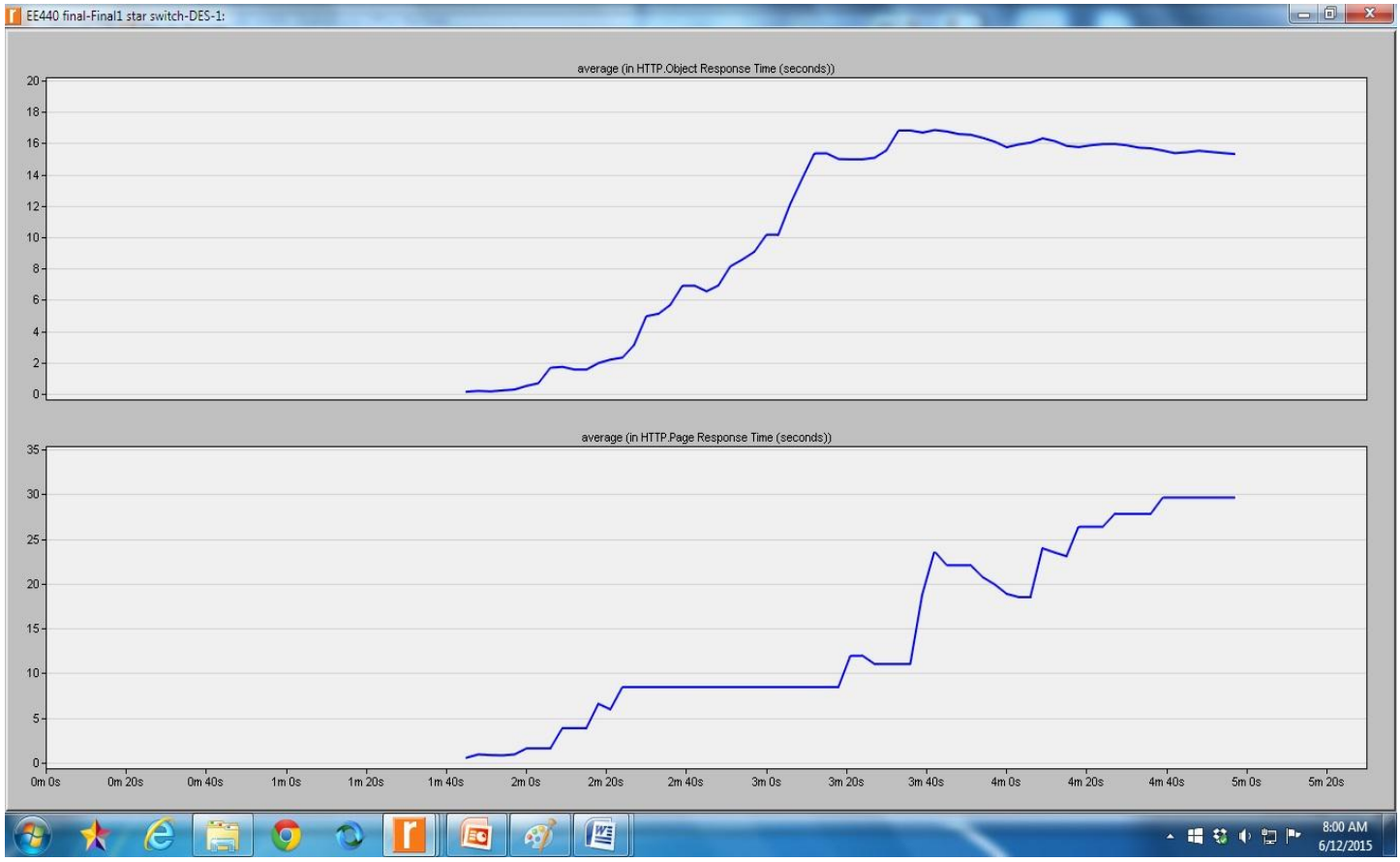
Email at high load:



Http light load:



Http heavy load:



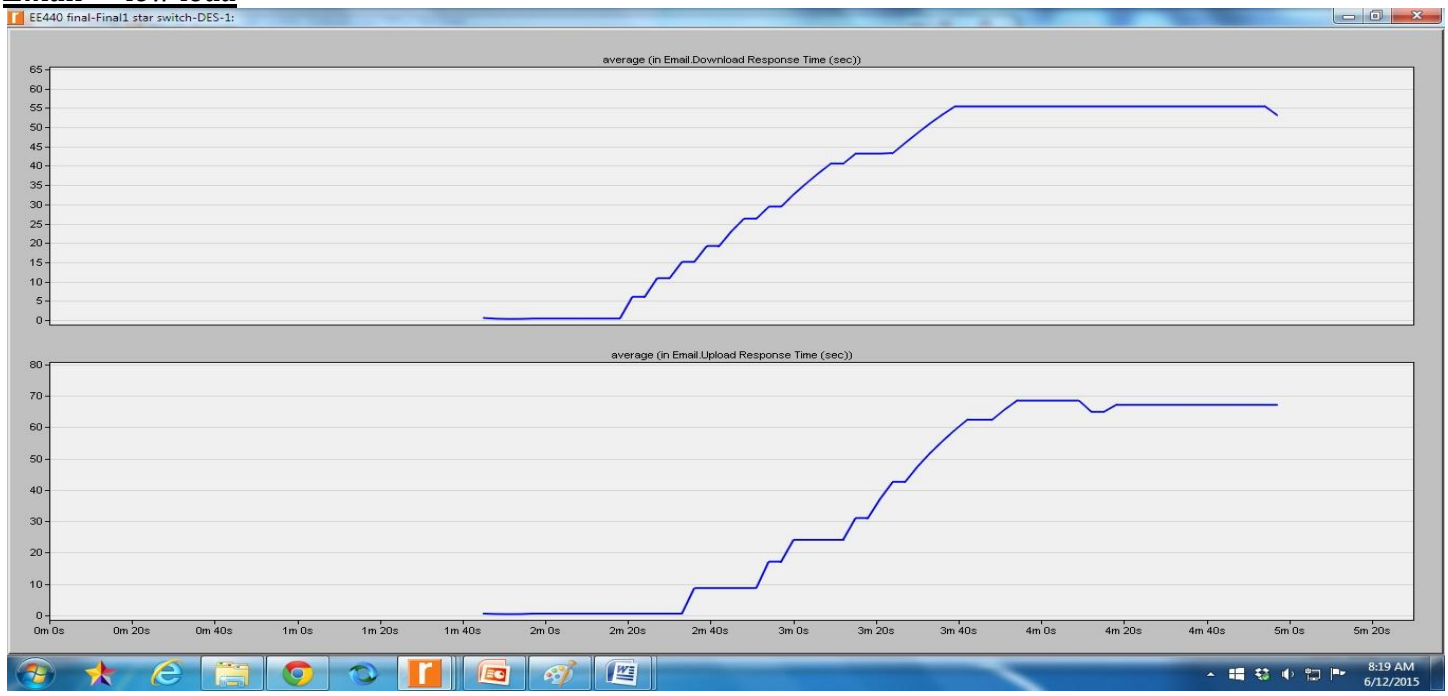
-

We created scenario to test the results:

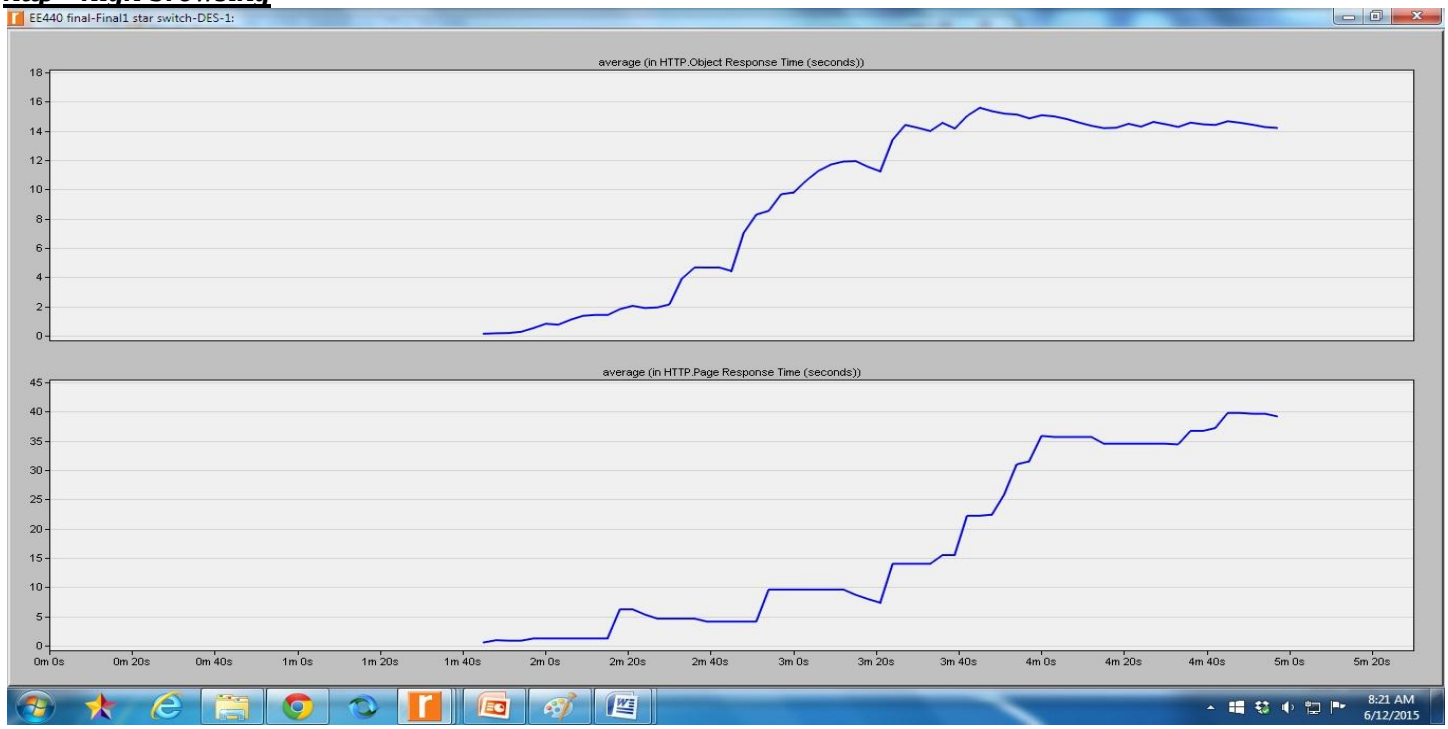
Scenario 1:

Email = low load
http =high browsing
FTP = low load
Wifi = light browsing

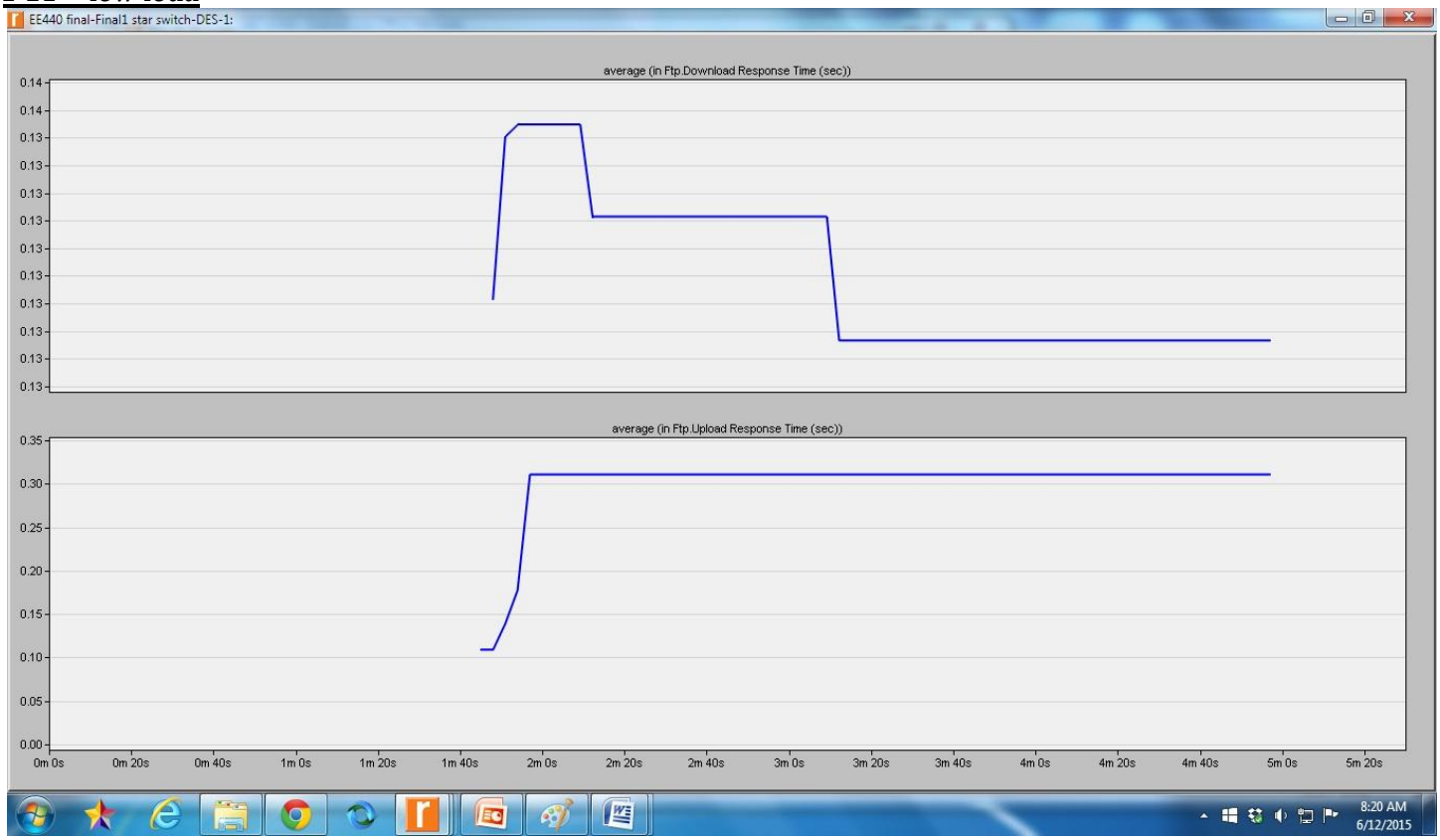
Email = low load



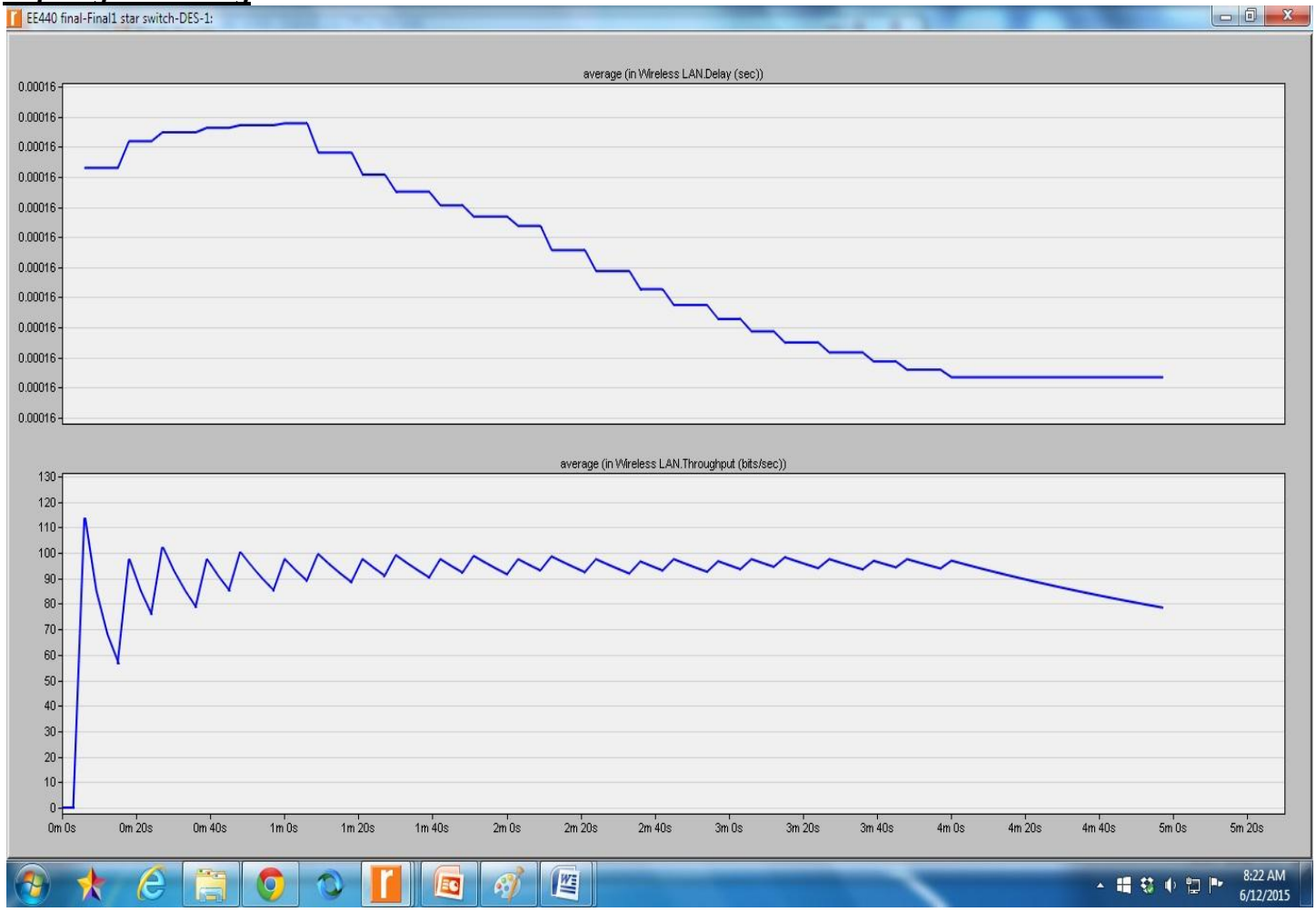
http =high browsing



FTP= low load



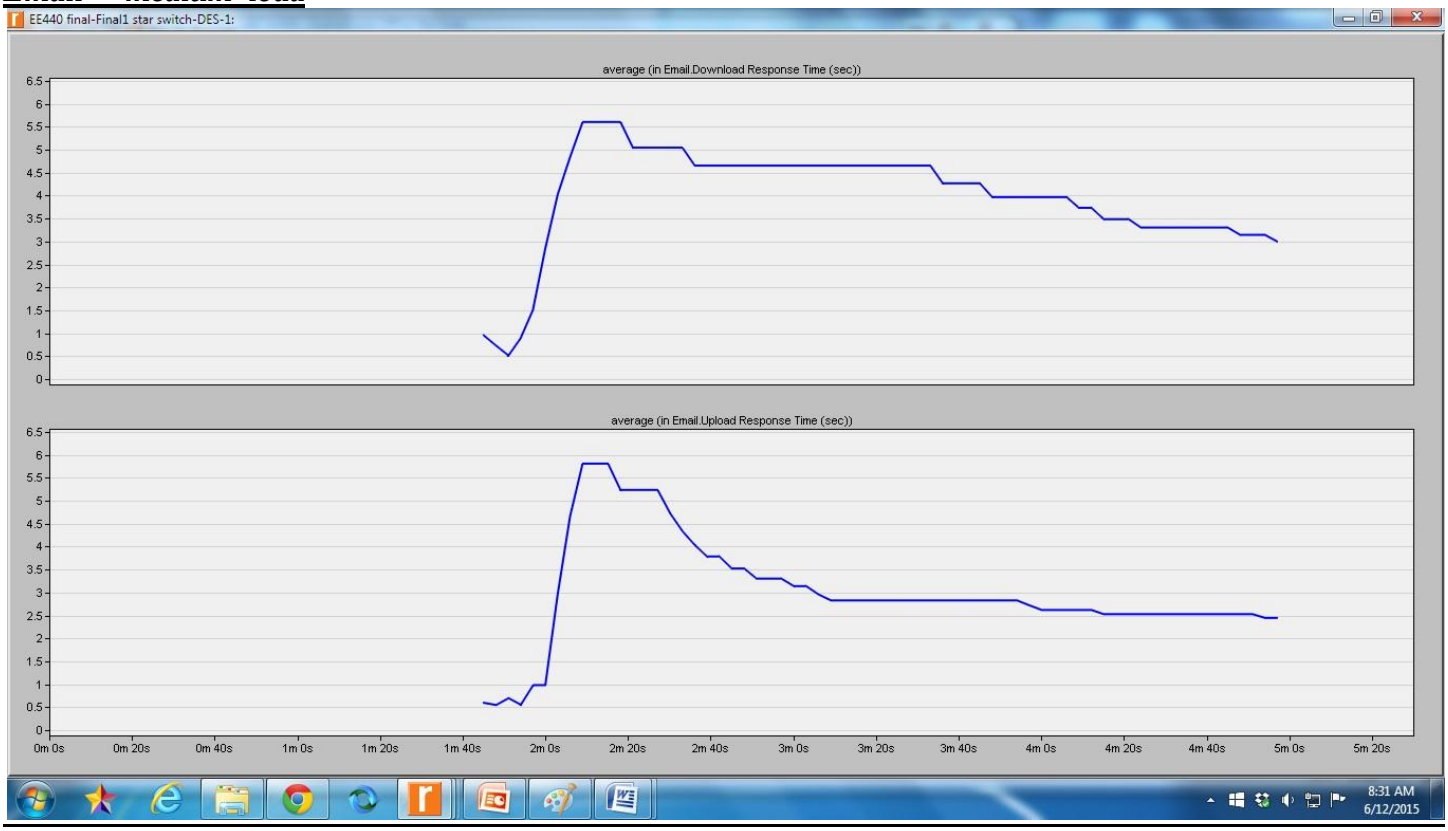
Wifi= light browsing



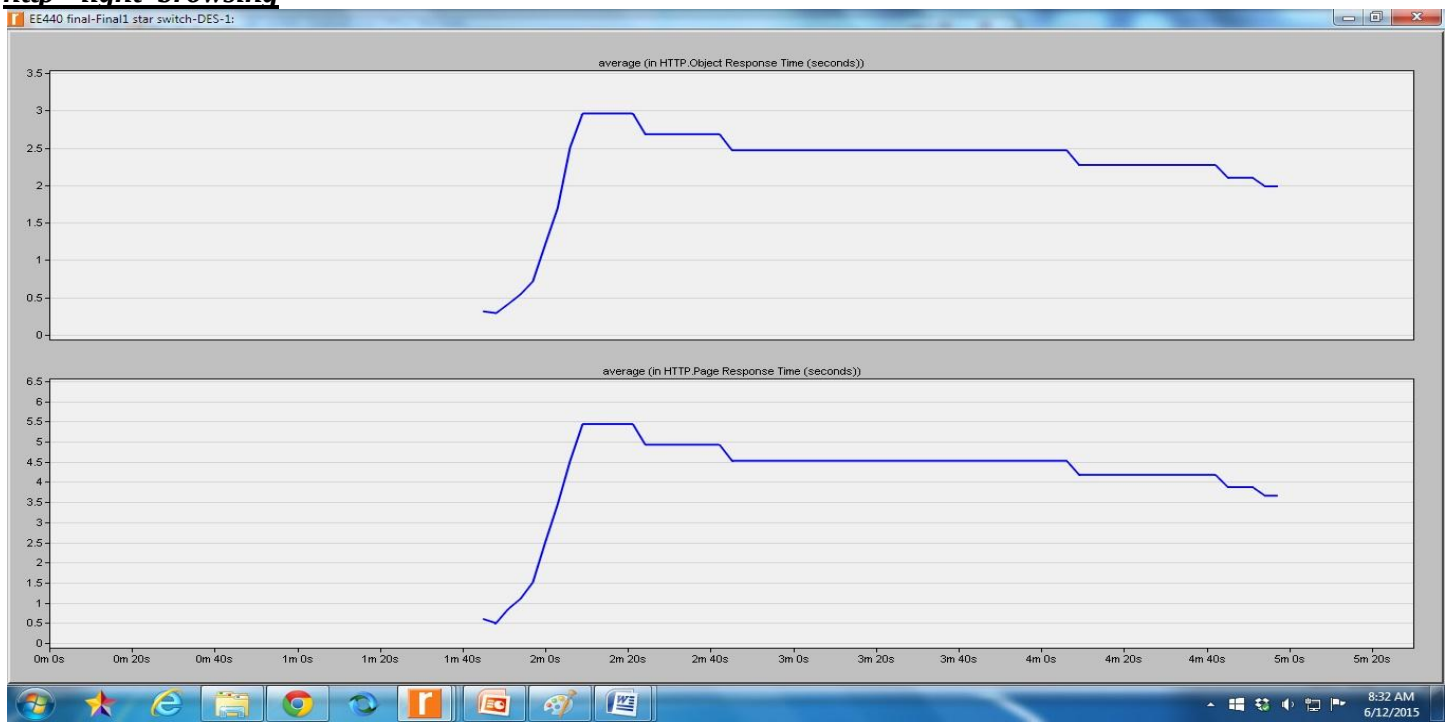
Scenario 2:

Email = medium load
http =light browsing
FTP = medium load
Wifi = light browsing

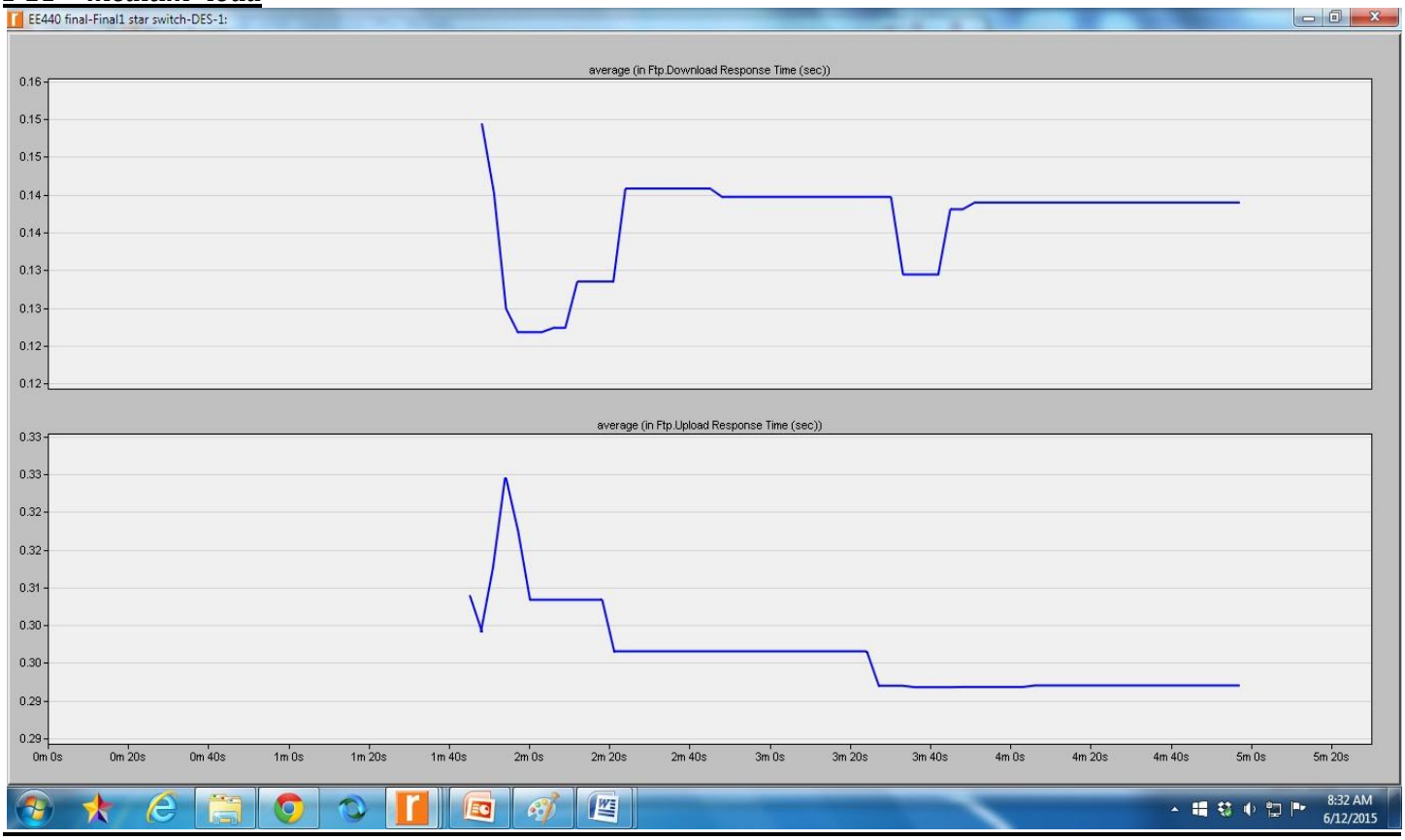
Email = medium load



http =light browsing



FTP= medium_load



Wifi= light browsing