Evaluation of EIGRP and OSPF Routing Protocols for Greener Internetworking

Vangala Rekha Andal
Assistant Professor, Department of ECE, Bharat Institute of Engineering and Technology.
rekhavangala@gmail.com

Abstract—Routing protocol is taking a vital role in the modern internet era. A routing protocol determines how the routers communicate with each other to forward the packets by taking the optimal path to travel from a source node to a destination node. In this paper we have explored two eminent protocols namely, Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) protocols. Evaluation of these routing protocols is performed based on the quantitative metrics such as Convergence Time, Jitter, End-to-End delay, Throughput and Packet Loss through The simulated network models. The evaluation results show that EIGRP routing protocol provides a better performance than OSPF routing protocol for real time applications. Through network simulations we have proved that EIGRP is more CPU intensive than OSPF and hence uses a lot of system power. Therefore EIGRP is a greener routing protocol and provides for greener internetworking.

Keywords – OSPF, EIGRP, CPU, Routing Protocol

1. INTRODUCTION

In Existing system, a routing protocol determines how the routers communicate with each other to forward the packets by taking the optimal path to travel from a source node to a destination node. In order to enable proper growth of the Internet it is of key importance to maximize both the energy-scalability index and cost-scalability index of the future Internet. The former is defined as the ratio between the relative network growth and the corresponding relative energy consumption increase; the latter is defined likewise where the divisor is the corresponding relative cost increase.

To addresses the problem in various complementary ways:

- Reduce per packet processing,
- Limit memory requirements in all network devices,
- Deploy larger switching units (thus reducing the switch reconfiguration frequency), enable full link utilization (thus enabling traffic to be concentrated on fewer optical channels, while the others can be put in a low-power idle mode),
- Enable realization of dynamic all-optical switching.

1.1. PROPOSED SYSTEM

In Proposed system, using EIGRP with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router. Routers that support EIGRP will automatically redistribute route information to IGRP neighbors by converting the 32 bit EIGRP metric to the 24 bit IGRP metric.

Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information.

1.1.2. ADVANTAGES

- A system where it sends only the updates needed at a given time; this is accomplished through neighbour discovery and maintenance
- A way of determining which paths a router has learned are loop-free
- A process to clear bad routes from the topology tables of all routers on the network
- A process for querying neighbours to find paths to lost destinations

- Enhanced Interior Gateway Routing Protocol – EIGRP
- Open Shortest Path First (OSPF)

2. Enhanced Interior Gateway Routing Protocol – EIGRP

The Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) is a routing protocol developed by Cisco Systems and introduced with Software Release 9.21 and Cisco Internetworking Operating System (Cisco IOS) Software Release 10.0. Enhanced IGRP combines the advantages of distance vector protocols, such as IGRP, with the advantages of link-state protocols, such as Open Shortest Path First (OSPF). Enhanced IGRP uses the Diffusing Update Algorithm (DUAL) to achieve convergence quickly.

Enhanced IGRP includes support for IP, Novell NetWare, and AppleTalk. The discussion on Enhanced IGRP covers the following topics:
Optimize routing in network with satellite links. Delay can be modified with the delay command.

- **Reliability**-Reliability is dynamically computed as a rolling weighted average over five seconds.

- **Load**-Load is dynamically computed as a rolling weighted average over five seconds. When Enhanced IGRP summarizes a group of routes, it uses the metric of the best route in the summary as the metric for the summary.

2.5. Enhanced IGRP Convergence

Enhanced IGRP implements a new convergence algorithm known as DUAL (Diffusing Update Algorithm). DUAL uses two techniques that allow Enhanced IGRP to converge very quickly. First, each Enhanced IGRP router stores its neighbors routing tables. This allows the router to use a new route to a destination instantly if another feasible route is known. If no feasible route is known based upon the routing information previously learned from its neighbors, a router running Enhanced IGRP becomes active for that destination and sends a query to each of its neighbors asking for an alternate route to the destination. These queries propagate until an alternate route is found. Routers that are not affected by a topology change remain passive and do not need to be involved in the query and response.

A router using Enhanced IGRP receives full routing tables from its neighbors when it first communicates with the neighbors. Thereafter, only changes to the routing tables are sent and only to routers that are affected by the change. A successor is a neighboring router that is currently being used for packet forwarding, provides the least cost route to the destination, and is not part of a routing loop. Information in the routing table is based on feasible successors. Feasible successor routes can be used in case the existing route fails. Feasible successors provide the next least-cost path without introducing routing loops.

The routing table keeps a list of the computed costs of reaching networks. The topology table keeps a list of all routes advertised by neighbors. For each network, the router keeps the real cost of getting to that network and also keeps the advertised cost from its neighbor. In the event of a failure, convergence is instant if a feasible successor can be found. A neighbor is a feasible successor if it meets the feasibility condition set by DUAL. DUAL finds feasible successors by the performing the following computations:

2.6. Enhanced IGRP Network Scalability

Network scalability is limited by two factors: operational issues and technical issues. Operationally, Enhanced IGRP provides easy configuration and growth.

- **Enhanced IGRP Network Topology**
- **Enhanced IGRP Addressing**
- **Enhanced IGRP Route Summarization**
- **Enhanced IGRP Route Selection**
- **Enhanced IGRP Convergence**
- **Enhanced IGRP Network Scalability**
- **Enhanced IGRP Security**
Technically, Enhanced IGRP uses resources at less than a linear rate with the growth of a network.

2.7. Memory
A router running Enhanced IGRP stores all routes advertised by neighbors so that it can adapt quickly to alternate routes. The more neighbors a router has, the more memory a router uses. Enhanced IGRP automatic route aggregation bounds the routing table growth naturally. Additional bounding is possible with manual route aggregation.

2.8. CPU
Enhanced IGRP uses the DUAL algorithm to provide fast convergence. DUAL re-computes only routes, which are affected by a topology change. DUAL is not computationally complex, so it does not require a lot of CPU.

2.9. Bandwidth
Enhanced IGRP uses partial updates. Partial updates are generated only when a change occurs; only the changed information is sent, and this changed information is sent only to the routers affected. Because of this, Enhanced IGRP is very efficient in its usage of bandwidth. Some additional bandwidth is used by Enhanced IGRP’s HELLO protocol to maintain adjacencies between neighboring routers.

2.10. Enhanced IGRP Security
Enhanced IGRP is available only on Cisco routers. This prevents accidental or malicious routing disruption caused by hosts in a network. In addition, route filters can be set up on any interface to prevent learning or propagating routing information inappropriately.

3. Open Shortest Path First (OSPF)
OSPF is an Interior Gateway Protocol (IGP) developed for use in Internet Protocol (IP)-based internetworks. As an IGP, OSPF distributes routing information between routers belonging to a single autonomous system (AS). An AS is a group of routers exchanging routing information via a common routing protocol. The OSPF protocol is based on shortest-path-first, or link-state, technology. Two design activities are critically important to a successful OSPF implementation:
- Definition of area boundaries
- Address assignment

Ensuring that these activities are properly planned and executed will make all the difference in an OSPF implementation. Each is addressed in more detail with the discussions that follow. These discussions are divided into six sections:
- OSPF Network Topology
- OSPF Addressing and Route Summarization
- OSPF Route Selection
- OSPF Convergence
- OSPF Network Scalability
- OSPF Security

3.1. OSPF Network Topology
OSPF works best in a hierarchical routing environment. The first and most important decision when designing an OSPF network is to determine which routers and links are to be included in the backbone and which are to be included in each area. There are several important guidelines to consider when designing an OSPF topology:
- The number of routers in an area—OSPF uses a CPU-intensive algorithm. The number of calculations that must be performed given n link-state packets is proportional to n log n. As a result, the larger and more unstable the area, the greater the likelihood for performance problems associated with routing protocol recalculation. Generally, an area should have no more than 50 routers. Areas with unstable links should be smaller.
- The number of neighbors for any one router—OSPF floods all link-state changes to all routers in an area. Routers with many neighbors have the most work to do when link-state changes occur. In general, any one router should have no more than 60 neighbors.
- The number of areas supported by any one router—A router must run the link-state algorithm for each link-state change that occurs for every area in which the router resides. Every area border router is in at least two areas (the backbone and one area). In general, to maximize stability, one router should not be in more than three areas.
- Designated router selection—In general, the designated router and backup designated router on a local-area network (LAN) have the most OSPF work to do. It is a good idea to select routers that are not already heavily loaded with CPU-intensive activities to be the designated router and backup designated router. In addition, it is generally not a good idea to select the same router to be designated router on many LANs simultaneously.

3.2. Backbone Considerations
Stability and redundancy are the most important criteria for the backbone. Keeping the size of the backbone reasonable increases stability. This is caused by the fact that every router in the backbone needs to re-compute its
Routes after every link-state change. Keeping the backbone small reduces the likelihood of a change and reduces the amount of CPU cycles required to re-compute routes. As a general rule, each area (including the backbone) should contain no more than 50 routers. If link quality is high and the number of routes is small, the number of routers can be increased.

Redundancy is important in the backbone to prevent partition when a link fails. Good backbones are designed so that no single link failure can cause a partition.

OSPF backbones must be contiguous. All routers in the backbone should be directly connected to other backbone routers. OSPF includes the concept of virtual links. A virtual link creates a path between two area border routers (an area border router is a router connects an area to the backbone) that are not directly connected. A virtual link can be used to heal a partitioned backbone. However, it is not a good idea to design an OSPF network to require the use of virtual links. The stability of a virtual link is determined by the stability of the underlying area. This dependency can make troubleshooting more difficult. In addition, virtual links cannot run across stub areas. See the section "Backbone-to-Area Route Advertisement," later in this chapter for a detailed discussion of stub areas.

Avoid placing hosts (such as workstations, file servers or other shared resources) in the backbone area. Keeping hosts out of the backbone area simplifies internetwork expansion and creates a more stable environment.

### 3.3. Area Considerations

Individual areas must be contiguous. In this context, a contiguous area is one in which a continuous path can be traced from any router in an area to any other router in the same area. This does not mean that all routers must share a common network media. It is not possible to use virtual links to connect a partitioned area. Ideally, areas should be richly connected internally to prevent partitioning.

The two most critical aspects of area design follow:

- Determining how the area is addressed
- Determining how the area is connected to the backbone

Areas should have a contiguous set of network and/or subnet addresses. **Without a contiguous address space, it is not possible to implement route summarization.** The routers that connect an area to the backbone are called area border routers. Areas can have a single area border router or they can have multiple area border routers. In general, it is desirable to have more than one area border router per area to minimize the chance of the area becoming disconnected from the backbone.

When creating large-scale OSPF internetworks, the definition of areas and assignment of resources within areas must be done with a pragmatic view of your internetwork. The following are general rules that will help ensure that your internetwork remains flexible and provides the kind of performance needed to deliver reliable resource access.

- Consider physical proximity when defining areas---If a particular location is densely connected, create an area specifically for nodes at that location.
- Reduce the maximum size of areas if links are unstable---If your internetwork includes unstable links, consider implementing smaller areas to reduce the effects of route flapping. Whenever a route is lost or comes online, each affected area must converge on a new topology. The Dykstra algorithm will run on all the affected routers. By segmenting your internetwork into smaller areas, you can isolate unstable links and deliver more reliable overall service.

### 3.4. OSPF Addressing and Route Summarization

Address assignment and route summarization are inextricably linked when designing OSPF internetworks. To create a scalable OSPF internetwork, you should implement route summarization. To create an environment capable of supporting route summarization, you must implement an effective hierarchical addressing scheme. The addressing structure that you implement can have a profound impact on the performance and scalability of your OSPF internetwork. The following sections discuss OSPF route summarization and three addressing options:

- Separate network numbers for each area
- Network Information Center (NIC)-authorized address areas created using bit-wise subnetting and VLSM
- Private addressing, with a "demilitarized zone" (DMZ) buffer to the official Internet world

### 3.5. OSPF ROUTE SELECTION

When designing an OSPF internetwork for efficient route selection, consider three important topics:

- Tuning OSPF Metrics
- Controlling Inter-area Traffic
- Load Balancing in OSPF Internetworks

### 3.6. OSPF Convergence

One of the most attractive features about OSPF is the ability to quickly adapt to topology changes. There are two components to routing convergence:
Detection of topology changes---OSPF uses two mechanisms to detect topology changes. Interface status changes (such as carrier failure on a serial link) is the first mechanism. The second mechanism is failure of OSPF to receive a hello packet from its neighbor within a timing window called a dead timer. Once this timer expires, the router assumes the neighbor is down. The dead timer is configured using the ip ospf dead-interval interface configuration command. The default value of the dead timer is four times the value of the Hello interval. That results in a dead timer default of 40 seconds for broadcast networks and 2 minutes for nonbroadcast networks.

Recalculation of routes---Once a failure has been detected, the router that detected the failure sends a link-state packet with the change information to all routers in the area. All the routers recalculate all of their routes using the Dykstra (or SPF) algorithm. The time required to run the algorithm depends on a combination of the size of the area and the number of routes in the database.

3.7. OSPF Network Scalability
Your ability to scale an OSPF internetwork depends on your overall network structure and addressing scheme. As outlined in the preceding discussions concerning network topology and route summarization, adopting a hierarchical addressing environment and a structured address assignment will be the most important factors in determining the scalability of your internetwork.

Network scalability is affected by operational and technical considerations:

- Operationally, OSPF networks should be designed so that areas do not need to be split to accommodate growth. Address space should be reserved to permit the addition of new areas.
- Technically, scaling is determined by the utilization of three resources: memory, CPU, and bandwidth.

3.8. Memory
An OSPF router stores all of the link states for all of the areas that it is in. In addition, it can store summaries and externals. Careful use of summarization and stub areas can reduce memory use substantially.

3.9. CPU
An OSPF router uses CPU cycles whenever a link-state change occurs. Keeping areas small and using summarization dramatically reduces CPU use and creates a more stable environment for OSPF.

3.10. Bandwidth
OSPF sends partial updates when a link-state change occurs. The updates are flooded to all routers in the area. In a quiet network, OSPF is a quiet protocol. In a network with substantial topology changes, OSPF minimizes the amount of bandwidth used.

3.11. OSPF Security
Two kinds of security are applicable to routing protocols:

- Controlling the routers that participate in an OSPF network
OSPF contains an optional authentication field. All routers within an area must agree on the value of the authentication field. Because OSPF is a standard protocol available on many platforms, including some hosts, using the authentication field prevents the inadvertent startup of OSPF in an uncontrolled platform on your network and reduces the potential for instability.

- Controlling the routing information that routers exchange
All routers must have the same data within an OSPF area. As a result, it is not possible to use route filters in an OSPF network to provide security.

4. MODULES

4.1. EIGRP OPERATIONS
In this module, EIGRP is a distance vector protocol because it learns about other routing routes by rumours from the neighbouring routers.

a. Building neighbour relationship
In this module,
1. The first router generates a hello with its configuration information
2. If the configuration information (Autonomous system numbers and K values) matches then the second router responds with an update message with its local topology table information (not its routing table as done by the distance vector protocols)
3. The first router responds with an ACK message acknowledging the receipt of the second’s Update. The first router then sends its topology table to second router via an update message. The second router responds with an ACK message as for transferring of routing updates are concerned
There are 3 types of messages involved. They are
- **UPDATE**: Contains a routing update
- **QUERY**: Asks a neighbouring router to validate routing information
- **REPLY**: Responds to a query message.

**b. Choosing routes**

In this module, EIGRP has the following metrics bandwidth, reliability, delay, load and MTU. However only fixed metrics such as bandwidth and delay are activated. EIGRP maintains something such as successor route and a feasible successor route in the local topology table. Successor route is the route via which the packets are forwarded and has the best metric. Feasible successor route is the route with which the router will forward packets once the successor route goes down or has the second best metric. This is the advantage of EIGRP, once a route goes down it doesn’t have to send hello packets to find out another alternative route. It just brings on the feasible successor route.

4.2. **OSPF OPERATIONS**

**a. Finding neighbours**

In this module, a router finds its neighbours by sharing link state advertisements which exist in different types. OSPF generates hello messages every 10 seconds. When a neighbour is discovered and an adjacency is formed with the neighbour then the router expects to see hello messages every 10 from the neighbour.

If a neighbour’s message is not seen within 40 seconds (dead interval time). The hello packet contains information like the area number, hello and dead timer intervals, OSPF password if it is configured.

**b. Creating Adjacency**

In this module. In OSPF, adjacency is created if the information from the hello packets of one router match with the information present in the configuration file of the proposed router.

**c. Sharing routing information**

In this module, OSPF routers use link state advertisements to communicate with each other. One type of LSA is hello which is used to form neighbour relationships and as a keep alive function. Link state advertisements are sent to the disseminates this to everyone else at the multicast address.

5. **PERFORMANCE COMPARISON OF OSPF AND EIGRP**

When OSPF and EIGRP routers are compared, it is the OSPF routing protocol which demands a lot of resources from the router, since OSPF has to undergo a lot of background processes such as electing a DR and a BDR. Also the router ID has to be computed on each router. This induces a lot of delay when compared to EIGRP routing protocol. Therefore total delay will be equal to average delay × no of routers. OSPF causes massive CPU utilization therefore more heat is produced; more amount of cooling is required. EIGRP being a hybrid protocol uses fewer amounts of CPU resources. Since OSPF uses server-client relationship the DR router should be a powerful router to process a lot of incoming traffic otherwise it will crash bringing the entire router area down.

The use of a server client model jams the bandwidth since the routing updates from all the routers have to go to the path connected to the DR after which the DR will forward them to the other routers. In case of EIGRP there will be no election of DR or BDR and hence there is less time delay and less consumption of router resources. Since EIGRP doesn’t use the client-server model, therefore there will be no jamming of bandwidth.

Supposing in a network, a path goes down then OSPF will have to use LSA hello packets again causing the finding Neighbour process to start all over again. Therefore OSPF will fail to act fast in high speed networks and also a lot of energy is consumed due to high overhead of router. In case of EIGRP the router carries an alternative route known as the feasible successor router which will be used once the successor router goes down. Therefore EIGRP doesn’t have to send hello packets once again or find its neighbours again.

OSPF uses a backbone router to route between different areas, which increases equipment cost. EIGRP uses BGP protocol to route between different autonomous systems, and this saves the cost of the extra router required in OSPF.

6. **EXPERIMENTAL RESULTS**

We have tried to use 3 different networks having same topologies. One is configured with EIGRP, the second one with OSPF and the third with OSPF and EIGRP. The common network topology is shown in Fig 1.
From the experiment we have observe the following

- From Fig 2 and Fig 5 we can see that in the process 174 have 369 threads when EIGRP is running and when OSPF is running the number of free threads is 193.
- From Fig 3 and Fig 6 we can see that the memory used in NVRAM when EIGRP is running is 191 Kbytes and when OSPF is running 291 Kbytes.
- Fig 4 shows the CPU process history of the router during the last 60 seconds when EIGRP is running.
- Table 1 shows the summary of the time taken for the various network parameters.

A. Screenshots of EIGRP
All 3 routers are configured with EIGRP protocol. The processes that occur and the overheads of the 2 routers are as shown in fig2, fig 3, fig 4.

B. Screenshots of OSPF analysis
In this case all 3 routers are configured with OSPF.

Fig 2 Shows the processes running on the first EIGRP router

Fig 3 Shows the memory consumption of the first router running on EIGRP

Fig 4- CPU graph for the last 60 seconds of router 1 when it is running on EIGRP

Fig 5 showing the processes running on the first OSPF router

Fig 6- Showing the memory consumption of the first router running on OSPF
<table>
<thead>
<tr>
<th>Scenarios</th>
<th>OSPF</th>
<th>EIGRP</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Startup</td>
<td>1 min 22 seconds</td>
<td>47 seconds</td>
</tr>
<tr>
<td>When one of the network</td>
<td>180 seconds</td>
<td>16*5 seconds</td>
</tr>
<tr>
<td>goes down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When a change occurs in</td>
<td>Convergence</td>
<td>Convergence</td>
</tr>
<tr>
<td>the network</td>
<td>time of 3</td>
<td>time almost</td>
</tr>
<tr>
<td></td>
<td>seconds</td>
<td>instantaneous</td>
</tr>
</tbody>
</table>

7. CONCLUSION

From the results obtained from our experiments we can
Thoroughly conclude that EIGRP uses less system
resources when compared to OSPF. However EIGRP is a
Cisco proprietary protocol, but since Cisco routers make
85% of the internet backbone, it is necessary for us to
implement a greener solution on Cisco routers itself.

By using lesser system resources, EIGRP is used
as a routing protocol produces lesser heat and therefore
the cooling cost is also saved.EIGRP also uses its own
external routing protocol and therefore unlike OSPF
doesn’t need a separate router to do routing between areas.
Therefore resources are also saved.

8. REFERENCES


