ISSN:0975-9646

Comprehensive Analysis of Dynamic Routing Protocols in Computer Networks

Priya Asher

Department of Electronics and Telecommunication, K. J. Somaiya College of Engineering, University of Mumbai, India

Abstract— **In the field of computer networking, a routing protocol specifies how routers communicate to select the most effective route for information or data transfer between computer nodes. This paper discusses the routing process and looks at a generic classification of routing protocols. It also summarizes the features of some of the most significant protocols like RIP, OSPF, IS-IS, IGRP, EIGRP and BGP, while comparing their individual functioning.**

Keywords— **Routing Protocols, Autonomous Systems (AS), RIP, BGP, IGRP, EIGRP, OSPF, IS-IS, Dynamic Routing**

I. Introduction

Routing refers to the process of determining the best route for the transmission of data packets from source to destination and it is based upon routing protocols. Routing protocols are a set of rules which a communication network follows when computers try to communicate with each other across networks. A routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network [1]. Routing algorithms are responsible for selecting the best path for the communication. A routing protocol is therefore the language a router speaks with other routers in order to share information about the reachability and status of the network [2].

II. Classification

Routing is established by the configuration of routing tables in the routers. There are two different ways to configure routing tables in router- **static routing** and **dynamic routing**. Static routing is the process of manually entering routes into the routing table of a device using its configuration file that is loaded when the routing device starts up. In static routing, all the changes in the logical network layout need to be manually done by the system administrator. However, dynamic routing allows routers to select the best path when there is a real time logical network layout change. Static routing is easy to implement in small networks. [3] These networks are very safe and predictable as the route to the destination always remains the same and doesn't require any routing algorithm or update mechanisms. But dynamic routing protocols work well and are suitable in all topologies where multiple routers are required. They are scalable and automatically determine better routes if there is a change in the topology. Their ability to scale and recover from internetwork faults makes dynamic routing protocols a better choice for medium, large, and very large networks. Figure 1 depicts the classification of dynamic routing protocols.

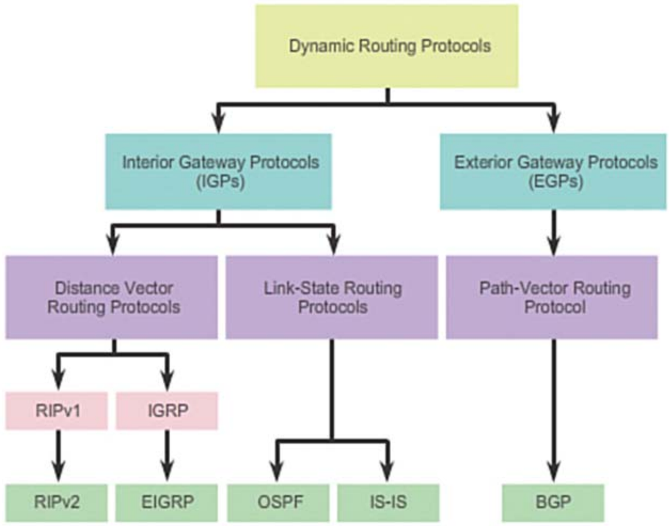

Fig. 1: Dynamic Routing Protocol Classification

Dynamic routing protocols are classified into EGP and IGP, which is further classified into distance vector routing protocol and link state routing protocol. Distance vector protocol uses simple algorithms to calculate cumulative distance value between routers based on hop count. Link state protocols use sophisticated algorithms that maintain complex database of internetwork topology.

A. IGP and EGP

An **Autonomous System (AS)** is a collection of routers under a common administration such as a company or an organization. An AS is also known as a routing domain. Typical examples of an AS are a company's internal network and an ISP's network. The Internet is based on the AS concept; therefore, two types of routing protocols are required:

- **Interior Gateway Protocols (IGP)**: Used for routing within an AS. It is also referred to as intra-AS routing. Companies, organizations, and even service providers use an IGP on their internal networks [4]. IGPs include RIP, EIGRP, OSPF, and IS-IS.
- **Exterior Gateway Protocols (EGP)**: Used for routing between autonomous systems. It is also referred to as inter-AS routing. Service providers and large companies may interconnect using an EGP. The Border Gateway Protocol (BGP) is the only currently viable EGP and is the official routing protocol used by the Internet.

Figure 2 shows the position of employment of the aforementioned protocols in a networking domain.

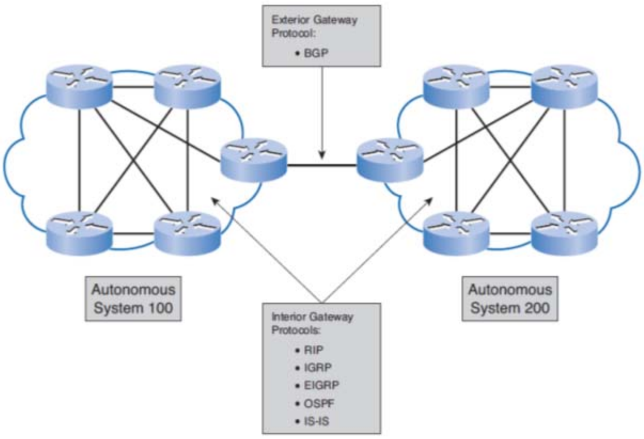

Fig. 2: Position of various protocols in a network infrastructure

III. Routing Information Protocol (RIP)

RIP stands for Routing Information Protocol in which distance vector routing is used for data/packet transmission [5]. RIP is a distance vector dynamic routing protocol that uses the hop count as its routing metrics.

When RIP is first configured on a router, it sends broadcast packets containing the request message and then listens for response messages. Routers receiving the request message respond to it by sending their routing tables in the response message. This process continues until the network is updated with the new router's position. Thus, a RIP router sends out its full routing table in its update once in 30 seconds. If any new entry is found in an update, the RIP router enters it into the routing table along with the sending router's address.

The metric used in RIP to find out the best path between two locations is Hop count. Hop count is the number of routers the packet must go through till it reaches the destination network [3].

RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15. This hop limit also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance. In other words, the route is considered unreachable. RIP implements the split horizon, route poisoning and hold down mechanisms to prevent incorrect routing information from being propagated [6].

A. RIP Versions

- **RIPv1:** RIPv1 supports Classfull routing; therefore variable length subnet masks (VLSM) cannot be used. There is also no authentication mechanism.

- **RIPv2:** RIPv2 supports Classless Inter-Domain Routing (CIDR). It uses MD5 mechanism for authentication.

B. Operation

RIP-based method is a passive method in IP layer. The precondition of this method is that the routers in the network use RIP protocol as the tool of the route information exchanges [7]. RIP-based method is quick and accurate in a small or medium sized network. However, it may cause serious problems in a large scale network. As RIP uses UDP to broadcast its route messages, the messages are not reliable and may be lost in the network. Also, it is unsafe to broadcast messages in a large scale network. When many broadcast messages are sent, it may cause broadcast storm, which can cause the network to breakdown. Besides, RIP protocol defines count of 16 as the state of unreachable. Hence, RIP-based protocol is available for small or medium networks.

In order to make sure the routing table entries are correct, RIP routing table is updated periodically, and sends the updated routing table to adjacent routers [8]. In addition, the routing table associated with each entry has a timer. When running RIP in the router where a route is not updated within the time prescribed, the route to measure the values is set to infinity and marked for deletion. Thus, when the router exchanges routing information with other routers, other routers know that the route has been ineffective.

C. Drawbacks

Although the RIP algorithm is relatively simple, there are some drawbacks.

1) RIP subnet address is not a concept. If a C class address in the last 8 bits of host number is 0, then the RIP cannot distinguish whether the non-zero parts are a subnet or a host address.
2) RIP router in the routing table provides the maximum hop count as 15. When the number of hops to the destination host is more than 15, that router is unreachable.
3) RIP route selection is only a measure of the number of hops; it cannot be combined with other network routing performance considerations.
4) When the network fails, it needs a long time to transfer this information to all routers. This process is relatively slow and slow convergence may cause problems. So it is not suitable for frequent changes in routing as in the case of a large-scale Internet environment.

IV. Interior Gateway Routing Protocol (IGRP)

IGRP stands for Interior Gateway Routing protocol which uses distance vector protocol to exchange data within a system [9]. IGRP is a proprietary protocol that was created in part to overcome the limitations of RIP which had a maximum hop count of only 15, and a single routing metric when used within large networks. It supports multiple metrics for each node which includes delay, load and bandwidth, in order to compare the 2 routes which are combined into single metrics. The maximum configurable hop count of IGRP-routed packets is 255 (default 100), and routing updates are broadcast every 90 seconds by default. IGRP uses protocol number 9 for communication.

The IGRP protocol allows a number of gateways to coordinate their routing [10]. Its goals are the following:

- Stable routing even in very large or complex networks. No routing loops should occur, even as transients.
- Fast response to changes in network topology.
- Low overhead. That is, IGRP itself should not use more bandwidth than what is actually needed for its task.
- Splitting traffic among several parallel routes when they are of roughly equal desirability.
- Taking into account error rates and level of traffic on different paths.

A. *Operation*

The path for routing packets from source to destination is calculated in the network. Based on the metric information, a single composite metric is calculated for the path. The composite metric combines the effect of the various metric components into a single number representing the goodness of that path. It is the composite metric that is actually used to decide on the best path.

Periodically each gateway broadcasts its entire routing table to all adjacent gateways. When a gateway gets this broadcast from another gateway, it compares the table with its existing table. Any new destinations and paths are added to the gateway's routing table. Paths in the broadcast are compared with existing paths. If a new path is better, it may replace the existing one. Information in the broadcast is also used to update channel occupancy and other information about existing paths. This general procedure is similar to that used by all distance vector protocols. It is referred to in the mathematical literature as the Bellman-Ford algorithm. In IGRP, the general Bellman-Ford algorithm is modified in three critical aspects. First, instead of a simple metric, a vector of metrics is used to characterize paths. Second, instead of picking a single path with the smallest metric, traffic is split among several paths, whose metrics fall into a specified range. Third, several features are introduced to provide stability in situations where the topology is changing.

IGRP provides a system for interconnecting computer networks which can stably handle a general graph topology including loops. The system maintains full path metric information, i.e., it knows the path parameters to all other networks to which any gateway is connected. Traffic can be distributed over parallel paths and multiple path parameters can be simultaneously computed over the entire network.

V. Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced IGRP (EIGRP) is a classless, enhanced distance vector protocol. Like IGRP, EIGRP uses the concept of an autonomous system. EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link state protocols. For example, EIGRP doesn’t send link-state packets as OSPF does; instead, it sends traditional distance vector updates containing information about networks plus the cost of reaching them from the perspective of the advertising router [11]. EIGRP has link-state characteristics as well: it synchronizes routing tables between neighbours at start-up and then sends specific updates only when topology changes occur. This makes EIGRP suitable for very large networks. EIGRP has a maximum hop count of 255 (the default is set to 100).

Unlike many other protocols that use a single factor to compare routes and select the best possible path, EIGRP can use a combination of the following factors:

1) Bandwidth: Weakest link bandwidth in the total path
2) Delay: Sum of the delays for the entire path
3) Reliability
4) Load
5) MTU

Like IGRP, EIGRP uses only bandwidth and delay of the line to determine the best path to a remote network by default.

A. *Operation*

Before EIGRP routers exchange routes with each other, they must become neighbours. There are three conditions that must be met for adjacency establishment:

1. Hello or ACK received
2. AS numbers match
3. Identical metrics (K values)

Link-state protocols tend to use Hello messages to establish adjacency because they normally do not send out periodic route updates and there has to be some mechanism to help neighbours realize when a new peer has moved in or an old one has left or gone down. To maintain the neighbour- relationship, EIGRP routers must also continue receiving Hellos from their neighbours. As long as Hello packets are received, a router can determine that a neighbour is alive and functioning [12]. Once this is determined, the neighbouring routers can exchange routing information.

B. *Salient Features*

The salient features of EIGRP are as follows:

- Support for IP and IPv6 (and some other routed protocols) via protocol dependent modules.
- Considered classless (same as RIPv2 and OSPF).
- Support for VLSM/CIDR.
- Support for summaries and noncontiguous networks.
- Efficient neighbor discovery.
- Communication via Reliable Transport Protocol (RTP).
- Best path selection via Diffusing Update Algorithm (DUAL).

C. *Diffusing Update Algorithm (DUAL)*

The basis of Enhanced Interior Gateway Routing Protocol’s operation is the Diffusing Update Algorithm (DUAL) [13], which is used to compute shortest paths without ever creating routing-table loops or incurring counting-to-infinity behaviour. DUAL has been shown to be free of routing-table loops at every instant, regardless of the type or number of changes in the network, and to converge to correct routing-table values within a finite time after the occurrence of an arbitrary sequence of link-cost or topological changes [14]. Because DUAL is loop-free at every instant, it does not have any hop-count limitation, which is a necessity in case of RIP.

The distance information, known as a metric, is used by DUAL to select minimum cost loop free paths. DUAL selects routes to be inserted into a routing table based on feasible successors. A successor is a neighbouring router used for packet forwarding that has a least cost path to a destination that is guaranteed not to be part of a routing loop. When there are no feasible successors but there are neighbours advertising the destination, a recomputation must occur. This is the process where a new successor is determined. The amount of time it takes to recompute the route affects the convergence time. Even though the recomputation is not processor intensive, it is advantageous to avoid recomputation if it is not necessary. When a topology change occurs, DUAL will test for feasible successors. If there are feasible successors, it will use any one that it finds in order to avoid any unnecessary recomputation.

Thus, EIGRP is the first internet routing protocol that provides loop-freedom at every instant and convergence times comparable to those obtained with standard link-state protocols. Furthermore, EIGRP provides multiple paths to every destination that may have different weights.

D. Advantages of EIGRP

- Easy to configure.
- Loop free routes.
- Keeps backup path to the destination network.
- Convergence time is low and bandwidth utilization.
- Support Variable Length Subnet Mask (VLSM) and Classless Inter Domain Routing (CIDR).
- Supports authentication.

E. Disadvantages of EIGRP

- Considered as Cisco proprietary routing protocol.
- Routers from other vendors are not able to utilize EIGRP.

VI. OPEN SHORTEST PATH FIRST (OSPF)

OSPF is a routing protocol developed by Interior Gateway Protocol (IGP) working group of the Internet Engineering Task Force (IETF) for Internet Protocol (IP) network. OSPF is a link state protocol which maintains the routing table for all connections in the network. OSPF runs on top of IP, i.e., an OSPF packet is transmitted with IP data packet header

The concept of OSPF routing is based on creating, maintaining and distributing a link state database, which describes a collection of routers and their operational interfaces, how they are interconnected and cost to use the interfaces. Cost is a metrics used to describe the relative efficiency of various routes to the destination [15]. Each router in a particular domain runs the algorithm using their link-state database.

Each router in the routing domain is responsible for the creation of its local piece of topology by link state advertisements (LSA). LSAs contain information describing routers, networks, reachable routes, route prefixes and metrics. The LSAs are then reliably distributed to all other routers in a process called flooding, which allows OSPF routers to synchronize their topology databases. Most of the OSPF operations are dedicated to keeping the link-state database synchronized among OSPF routers. As long as every OSPF router has an identical link state database, every router can calculate the shortest paths to the advertised destination using Dijkstra Shortest Path First algorithm [16]. Dijkstra algorithm uses the cost to each link available in the router network for computation.

OSPF has five different packet types, where each packet in the route has a specific purpose. The following types of packets are sent within these networks:

a. Hello packet
b. Database description
c. Link state request packet
d. Link state update
e. Link state acknowledgement packet

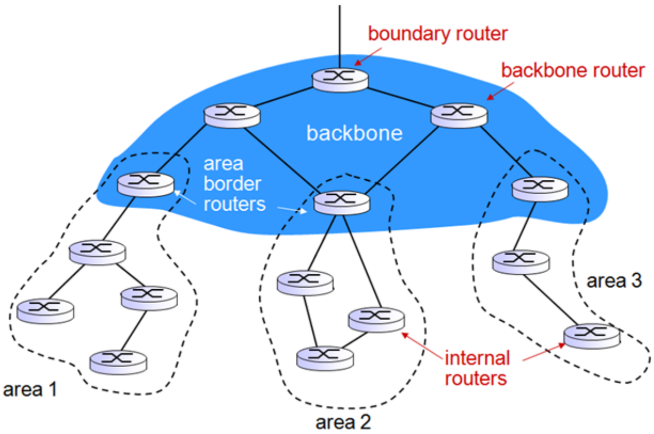

Fig. 3: Hierarchical OSPF Structure

Figure 3 shows the structure of an OSPF network. Based upon the information available in the topology table, each OSPF router runs SPF (Shortest Path First) algorithm and calculates the shortest path to every prefix within the same area. In case of any change in the state of a link, the OSPF router sends it in a partial update and is flooded throughout the entire network.

OSPF areas and address aggregation are crucial in enabling OSPF to scale for AS domains comprising hundreds or thousands of subnets; specifically, they play an important role in optimizing router and network resource consumption, as explained below.

1. **Router Memory:** For OSPF areas not directly connected to a router in the AS, the router's routing tables only need to contain entries corresponding to subnet aggregates rather than individual subnet addresses. In other words, a router stores individual subnet addresses in its routing table only for the OSPF areas that are directly linked to it. This observably leads to lesser routing table sizes and, thus, lowers memory requirements at routers.
2. **Router Processing Cycles:** The link-state database maintained at each router is much smaller, since it only needs to include summary information for subnets belonging to OSPF areas not directly connected to the

router. Consequently, the computational cost of the shortest-path calculation decreases substantially.

3. **Network Bandwidth:** For subnets within each OSPF area, only aggregate address information (rather than individual subnet addresses) is flooded into the rest of the AS network. As a result, the volume of OSPF flooding traffic necessary to synchronize the link-state databases of the AS routers is significantly reduced.

A. Advantages of OSPF

- OSPF is not a Cisco proprietary protocol
- OSPF always determines loop free routes
- If any changes occur in the network, it updates its database quickly
- Low bandwidth utilization
- Supports multiple routes for a single destination network
- OSPF is based on cost of the interface
- Supports Variable Length Subnet Mask (VLSM)

B. Disadvantages of OSPF

- Difficult to configure
- More memory requirements

VII. INTERMEDIATE-SYSTEM TO INTERMEDIATE-SYSTEM (IS-IS)

IS-IS stands for Intermediate - System to Intermediate - System which uses link-state routing algorithm for high speed data transmission. The protocol was defined in ISO/IEC 10589:2002 as an international standard within the Open Systems Interconnection (OSI) reference design [17].

Intermediate System-Intermediate System (IS-IS) is a Shortest Path First (SPF) protocol which is one of the most commonly used intra-domain internet routing protocols. It is similar to the OSPF protocol, which is also a link state protocol. The traffic is routed along shortest path to the destination. The weights of the links, and thereby the shortest path routes, can be changed by the network operator. A simple default weight setting suggested by Cisco is to make the weight of a link inversely proportional to its capacity. The general objective in setting weights is to route demands through an OSPF/IS-IS based network so as to avoid congestion in terms of link loads exceeding capacities with resulting packet loss and back-off in TCP [18].

IS-IS does not use IP to carry routing information messages. IS-IS is neutral regarding the type of network addresses for which it can route. OSPF version 2 on the other hand, was designed for IPv4. This allowed IS-IS to be easily used to support IPv6. To operate with IPv6 networks, the OSPF protocol was rewritten in OSPF v3 [17]. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both). Level 2 routers are inter-area routers that can only form relationships with other Level 2 routers. Routing information is exchanged between Level 1 routers and other Level 1 routers, and Level 2 routers only exchange information with other Level 2 routers. Level 1-2 routers exchange information with both levels and are used to connect the inter area routers with the intra area routers.

IS-IS uses Dijkstra's algorithm in which independent database is built by each IS-IS router for computing the best path for transmission in a network [5].

VIII. BORDER GATEWAY PROTOCOL (BGP)

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also classed as a distance-vector routing protocol [19]. The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.

BGP is the routing protocol used to exchange reachability information across Autonomous Systems [20]. The Border Gateway Protocol (BGP) was born out of the need for Internet Service Providers (ISPs) to control route selection (where to forward packets) and propagation (who to export routes to). When BGP was first introduced, it was a fairly simple path vector protocol. Over time, many incremental modifications to allow ISPs to control routing were proposed and added to BGP. A modified version of BGP is version 4 (BGP4).

A. Types of BGP

- **Internal BGP (iBGP):** When BGP runs between two peers in the same autonomous system, it is referred to as Internal BGP (iBGP). This BGP provides each AS a means to propagate reachability information to all AS-internal routers.
- **External BGP (eBGP):** When BGP runs between different autonomous systems, it is called External BGP (eBGP). This BGP provides each AS a means to obtain subnet reachability information from neighboring autonomous systems.

Figure 4 depicts the area of operation of eBGP and iBGP.

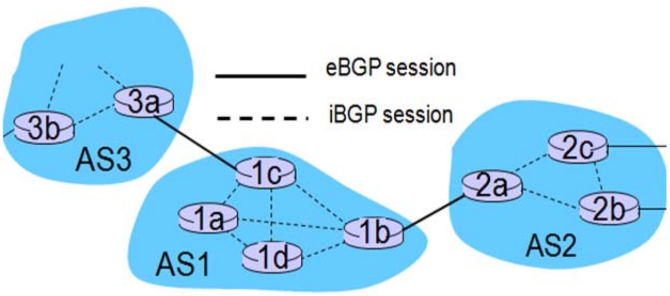

Fig. 4: Border Gateway Protocol

B. Operation

A router may learn about more than one route to the destination AS. In such a case, it selects the route based on:

- Local preference value attribute: policy decision
- Shortest AS-Path
- Closest Next-Hop router: hot potato routing
- Additional criteria

The BGP messages exchanged between peers over TCP connection could be any of the following:

a. **Open:** Opens TCP connection to peer and authenticates sender
b. **Update:** Advertises new path (or withdraws old)
c. **Keepalive:** Keeps connection alive in absence of Updates; also acknowledges Open request
d. **Notification:** Reports errors in previous message; also used to close connection

BGP sessions are established between border routers that reside at the edges of an AS and border routers in neighbouring autonomous systems. These sessions are used to exchange routes between neighbouring autonomous systems. Border routers then distribute routes learned on these sessions to non border (internal) routers as well as other border routers in the same AS using internal-BGP (iBGP). In addition, the routers in an AS usually run an Interior Gateway Protocol (IGP) to learn the internal network topology and compute paths from one router to another. Each router combines the BGP and IGP information to construct a forwarding table that maps each destination prefix to one or more outgoing links along shortest paths through the network to the chosen border router.

C. *Salient Features*

Thus, BGP is a relatively simple protocol with the following salient features.

- BGP is an incremental protocol, where after a complete routing table is exchanged between neighbors, only changes to that information are exchanged. These changes may be new route advertisements, route withdrawals, or changes to route attributes.
- BGP is a path-vector protocol where advertisements contain a list of autonomous systems used to reach the destination.
- Routes are advertised at the prefix level, so an AS would send a separate update for each of its reachable prefixes.
- BGP update messages may contain several fields, including a list of prefixes being advertised, a list of prefixes being withdrawn, and a list of route attributes that describe various characteristics of each advertised route.

IX. CONCLUSION

This paper thus presented a detailed analysis of various routing protocols. Routing protocols aim at finding the best path in the network to ensure proper connectivity. Each routing protocol has its own set of standards to judge a route quality by using metrics like next hop count, bandwidth and delay. The specific characteristics of routing protocols also include the manner in which they avoid routing loops, the manner in which they select preferred routes, using information about hop costs, the time they require to reach routing convergence, their scalability, and other factors. The requirements of a networking application would therefore determine the choice of a particular protocol for computer communication.

REFERENCES

[1] R.Devi, B.Sumathi, T.Gandhimathi, G.Alaiyarasi, “Performance Metrics of MANET in Multi-Hop Wireless Ad-Hoc Network Routing Protocols”, International Journal of Computational Engineering Research (IJCER).
[2] Behrouz A. Forouzan, “TCP/IP Protocol Suite”, McGraw-Hill Education Press. P. 269. ISBN 0-073-37604-3. Retrieved on March 25, 2009.
[3] Archana C, “Analysis of RIPv2, OSPF, EIGRP Configuration on router Using CISCO Packet tracer”, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 4, Issue 2, March 2015
[4] www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7
[5] P. Kalamani, M. Venkatesh Kumar , M. Chithambarathanu, Reji Thomas, “Comparison of RIP, EIGRP, OSPF, IGRP Routing Protocols in Wireless Local Area Network (WLAN) by using OPNET Simulator tool - A Practical Approach”, IOSR Journal of Computer Engineering (IOSR-JCE), Jul-Aug 2014
[6] www.cisco.com/c/en/ US/ td/docs/ios/
[7] V. Vetriselvan, Pravin R. Patil, M. Mahendran, “Survey on the RIP, OSPF, EIGRP Routing Protocols”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1058-1065
[8] Song Yang, Zhang Zhi Yong, “RIP Internet Protocol Failure Analysis and Research”, 2012 International Conference on Industrial Control and Electronics Engineering
[9] S. Barakovićand J. Baraković, “Comparative Performance Evaluation of Mobile Ad Hoc Routing Protocols,”Proceedings of the 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2010), Opatija, Croatia, May 2010
[10] www.cisco.com/c/en/us/support/docs/ip/interior-gateway-routing-protocol-igrp/26825-5.html
[11] Er. Ankit Sharma, Er.Sheilly Padda, “Configuring an EIGRP based Routing Model”, International Journal of Scientific and Research Publications, Volume 2, Issue 2, February 2012
[12] Bob Albrightson, J.J. Garcia-Luna-Aceves, Joanne Boyle , “EIGRP- A Fast Routing Protocol Based on Distance Vectors”
[13] J.J. Garcia-Luna-Aceves, “Method and Apparatus for Distributed Loop-Free Routing in Computer Networks," U.S. Patent application, SRI International, Menlo Park, California, 1993.
[14] J.J. Garcia-Luna-Aceves, “Loop-Free Routing Using Diffusing Computations," IEEE/ACM Trans. Networking, Vol. 1, No. 1, February 1993
[15] Rajneesh Narula, Pallavi Aggarwal, “Performance Evaluation of RIP and OSPF in IPv6 using OPNET 14.5 Simulator”, International Journal of Technical Research and Applications, Volume 2, Issue 6, Nov-Dec 2014
[16] www.ixiacom.com/pdfs/library/white_papers/ospf.pdf
[17] en.wikipedia.org/wiki/IS-IS
[18] Bernard Fortz , “On the evaluation of the reliability of OSPF routing in IP networks”, Universit´e Catholique de Louvain, Louvain-la-Neuve, Belgium
[19] en.wikipedia.org/wiki/Border_Gateway_Protocol
[20] Matthew Caesar, Jennifer Rexford, “BGP routing policies in ISP networks”