Journal

From the SelectedWorks of Kirat Pal Singh

Summer April 30, 2013

Review: Interior Gateway Protocols

Lateef Ahmad Bhat
Vishal Sudan
Kirat Pal Singh

This work is licensed under a Creative Commons CC_BY-NC International License.

Available at: https://works.bepress.com/kiratpalsingh/7/
Review: Interior Gateway Protocols

Lateef Ahmad Bhat, Vishal Sudan, Kirat pal singh
Dept. of ECE, Surya World, Punjab, India

Abstract
An Interior Gateway Protocol (IGP) is a routing protocol which is used to exchange routing information within routing domain or autonomous systems. This paper consists of different classification of Interior gateway routing protocols. This paper also includes the comparison between IGRP, EIGRP, OSPF, protocols.

Keywords
IGP, Routing protocol, OSPF, EIGRP, IGRP, RIP, IS-IS.

I. Introduction
IGPs are used for routing within a routing domain i.e. those networks within the control of a single organization. An autonomous system is commonly comprised of many individual networks belonging to companies, schools, and other organizations. An IGP is used to route within the autonomous system, and also used to route within the individual networks themselves. The IGP is mainly classified into two:

- Distance vector routing protocol
- Link state routing protocol

1. Distance Vector Routing Protocol
It uses distance vector algorithm or Bellman ford algorithm. In a distance vector algorithm, each router generates a map of its paths to all connected nodes in the network and sends this map to only its adjacent neighbors. A router using a distance vector protocol records the distance (a metric) from it to the destination and the next hop (which is the vector) to reach that destination and communicates this to its neighbors. Previously hop count is the only metric used by distance vector routing protocols, RIP protocol is an example of distance vector routing protocols which only uses hop count as metric. It also employs count-to-infinity rules and split-horizon techniques for loop avoidance. After this Distance vector interior gateway protocols were improved and make uses of more than just the hop-count as a metric and can take into account multiple link characteristics, such as bandwidth and delay. Interior Gateway Routing Protocol (IGRP) is an example and in this protocol additional loop avoidance techniques are built in and generally it send updates and not full tables.

2. Link State Routing Protocol
It uses Dijkstra Algorithm. It is also called shortest path first algorithm. Link state algorithm floods routing information to all nodes in the network however, each router sends only the portion of the routing table that describes the state of its own links. In link-state algorithms, each router builds a picture of the entire network in its routing tables. Open Shortest Path First (OSPF) protocol is an example of link state routing protocol.

II Overview

A. Open Shortest Path First (OSPF)
It is an interior gateway link state protocol which is used to allow routers to learn and advertise the routes dynamically. The advertisements containing routes are referred to link state advertisements. OSPF uses a hierarchical architecture. By having a hierarchical design, routing control packets in the domain are decreased and limited to a given area. OSPF allows a network to be segmented into multiple areas. An area is a collection of routers and networks.

A. Control Packets
Some control packets are used to guarantee neighbor discovery and maintenance and database synchronization, the following packet types are defined within the Type field of an OSPF control packet.

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hello</td>
</tr>
<tr>
<td>2</td>
<td>Data base description</td>
</tr>
<tr>
<td>3</td>
<td>Link state request</td>
</tr>
<tr>
<td>4</td>
<td>Link state update</td>
</tr>
<tr>
<td>5</td>
<td>Link state acknowledgement</td>
</tr>
</tbody>
</table>

Packet Type 1: Hello packets are used to establish connections and guarantee neighbor discovery and is also used for maintenance.
Packet Type 2: Database Description packets are used in the initial database synchronization.
Packet Type 3: During a database description exchange, the routers requests their missing LSA.
Packet Type 4: A router replies to the Link State Request packet by sending a Link State Update. Link State Update is also used when the routers are in Full state and there is a need to generate a new LSA due to any changes.
Packet type 5: The flooding operation should be reliable in order to guarantee that no information was lost while synchronizing the database. Link State Acknowledgment is sent in reply to a Link State Update packet.

The three components in OSPF include:

- Neighbor discovery
- Database synchronization
- Shortest Path First (SPF) calculation

1. Neighbor Discovery
When OSPF is enabled on an interface; the router sends Hello packets periodically in order to discover the remote neighbor’s. When a router receives a Hello from its neighbor, it includes the Router ID of this neighbor in its next Hello. This ensures that there is two-way connectivity between routers. A Hello packet is also used to elect DR/BDR on a multi-access network (broadcast and NBMA) and make sure that the neighbors agree on the area type based on the option fields in the Hello packet.

2. Database Synchronization
It is important that the database of all routers within an area is synchronized in order so that they have the same view of the network. Synchronization is either the initial router synchronization or if there is any change to the network topology and the routers need to resynchronize. Synchronization is performed by the way of OSPF packet type 2, 3, 4, and 5. Once two routers achieve the 2-way state, they start synchronizing their database by establishing a master-slave relationship. After the 2-way state, the routers go to the Exstart state where they have to find out who is the master. This is done by Router ID. The master sends a Database Description packet.
packet by incrementing the LS sequence for every different packet, and the slave just echoes back the LS sequence number sent by the master. Only one Database Description packet is sent and echoed at a time. This guarantees a reliable exchange between the two routers.

### 3. Shortest Path First Calculation

After database synchronization, all routers in an area will have the exact same link state database. The database is just a collection of different LSAs that the router has received and should build up the routing table based on this information. There are two types of routes:

- **Network route**—a destination IP addresses.
- **Router route**—The path (outgoing interface and next hop) SPF needs to see the network as a collection of nodes and point-to-point links. A multi-access network is represented by a Pseudo node (DR). Every router announces a connection to the transit network (DR) and the DR announces a connection to all attached routers. A router first finds out the path (outgoing interface and next hop) to all the nodes in its area by running the Dijkstra algorithm. Once the path to all the nodes is found (outgoing interface and next hop), the path to all the IP addresses advertised by the node is calculated.

### B. Enhanced interior gateway routing protocol (EIGRP)

EIGRP is a distance-vector Interior Gateway Protocol, which evolved from IGRP. EIGRP transports the subnet mask Information, which makes it a Classless routing Protocol. EIGRP uses Bandwidth and Delay of the Line, by default, EIGRP applies an Administrative Distance of 170 for external routes, and 90 for internal routes originating within the local Autonomous System (AS).

#### EIGRP uses Diffusing Update Algorithm (DUAL)

EIGRP uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metrics. The bandwidth and delay metrics are determined from values configured on the interfaces of routers in the path to the destination network. Following formulae can calculate the metric of the EIGRP packet:

\[
\text{Metric} = \frac{\text{bandwidth} \times \text{delay}}{(256 - \text{load}) + \text{K3} \times \text{delay}} \times \left(\frac{\text{K4}}{\text{reliability}} + \frac{\text{K5}}{\text{load}}\right) \]

The default values for K are:

- K1 = 1
- K2 = 0
- K3 = 1
- K4 = 0
- K5 = 0

For default behavior metric can be calculated directly as follows:

\[
\text{Metric} = \text{bandwidth} + \text{delay}
\]

#### Characteristics of EIGRP

EIGRP adheres to the following characteristics:

- EIGRP uses Diffusing Update Algorithm (DUAL) to determine the best path among all “feasible” paths. DUAL also helps ensure a loop free routing environment.
- EIGRP will form neighbor relationships with adjacent routers in the same Autonomous System (AS).
- EIGRP traffic is either sent as unicast, or as multicasts on address 224.0.0.10, depending on the EIGRP packet type.
- Reliable Transport Protocol (RTP) is used to ensure delivery of most EIGRP packets.
- EIGRP routers do not send periodic, full-table routing updates. Updates are sent when a change occurs, and include only the change.
- EIGRP is a classless protocol, and thus supports VLSMs.
- EIGRP supports IP, IPX, and AppleTalk routing.
- EIGRP applies an Administrative Distance of 90 for routes originating within the local Autonomous System.
- EIGRP applies an Administrative Distance of 170 for external routes coming from outside the local Autonomous System.
- EIGRP uses Bandwidth and Delay of the Line, by default, to calculate its distance metric. It also supports three other...
parameters to calculate its metric: Reliability, Load, and MTU.

- EIGRP has a maximum hop-count of 224, though the default maximum hop-count is set to 100. [4]

### C. Interior Gateway Routing Protocol (IGRP)

The Interior Gateway Routing Protocol (IGRP) is a routing protocol that was developed in the mid-1980s by Cisco Systems, Inc. Cisco's principal goal in creating IGRP was to provide a robust protocol for routing within an Autonomous System (AS). IGRP is designed to be more scalable than RIP.

IGRP adheres to the following characteristics:

- IGRP sends out periodic routing updates (every 90 seconds).
- IGRP sends out the full routing table every periodic update.
- IGRP uses a form of distance as its metric (in this case, a composite of bandwidth and delay).
- IGRP uses the Bellman-Ford Distance Vector algorithm to determine the best “path” to a particular destination.
- IGRP supports only IP routing.
- IGRP routes have an administrative distance of 100.
- IGRP, by default, supports a maximum of 100 hops. This value can be adjusted to a maximum of 255 hops.

- IGRP is a classful routing protocol. [4]

IGRP uses Bandwidth and Delay of the Line, by default, to calculate its distance metric. Reliability, Load, and MTU are optional attributes that can be used to calculate the distance metric. The general formulae which is used to calculate the Metric is given below:

\[
\text{Metric} = \left[ K_1 \times \text{bandwidth} + (K_2 \times \text{bandwidth}) / (256 - \text{load}) + K_3 \times \text{delay} \right] \times \left[ K_5 / (\text{reliability} + K_4) \right].
\]

The default values for \( K_4 \) and \( K_5 \) are:

\[
\begin{align*}
K_1 &= 1, \\
K_2 &= 0, \\
K_3 &= 1, \\
K_4 &= 0, \\
K_5 &= 0
\end{align*}
\]

### Stability Features-

IGRP provides a number of features that are designed to enhance its stability. These include Hold-downs, split horizons, and poison reverse updates.

### Hold-downs-

Hold-downs are used to prevent regular update messages from inaccurately reinstating a route that may have gone bad. When a router goes down, neighboring routers detect this via the lack of regularly scheduled update messages. These routers then calculate new routes and send routing update messages to inform their neighbors of the route change. Hold-downs tell routers to hold down any changes that might affect routes for some period of time.

### Split Horizons-

Split horizons derive from the fact that it is never useful to send information about a route back in the direction from which it came. The split-horizon rule helps prevent routing loops. Split horizons are implemented in IGRP because they provide extra algorithm stability.

### Poison Reverse Updates-

Whereas split horizons should prevent routing loops between adjacent routers, poison reverse updates are intended to defeat larger routing loops. Increases in routing metrics generally indicate routing loops. Poison reverse updates are then sent to remove the route and place it in hold-down. In Cisco’s implementation of IGRP, poison reverse updates are sent if a route metric has increased by a factor of 1.1 or greater.

### 1. IGRP Timers- IGRP has Four Basic Timers

- Update Timer (default 90 seconds) – indicates how often the router will send out a routing table update.
- Invalid Timer (default 270 seconds) – indicates how long a route will remain in a routing table before being marked as invalid, if no new updates are heard about this route. The invalid timer will be reset if an update is received for that particular route before the timer expires.

A route marked as invalid is not immediately removed from the routing table. Instead, the route is marked (and advertised) with a metric of 101 (remember, 100 maximum hops is default), indicating it is unreachable, and placed in a hold-down state. Hold-down Timer (default 280 seconds) – indicates how long IGRP will “suppress” a route that it has placed in a hold-down state. IGRP will not accept any new updates for routes in a hold-down state, until the hold-down timer expires.

Flush Timer (default 630 seconds) – indicates how long a route can remain in a routing table before being flushed, if no new updates are heard about this route. The flush timer runs concurrently with the invalid timer, and thus will flush out a route 360 seconds after it has been marked invalid.

### D. Routing Information Protocol (RIP)

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP is also one of the more easily confused protocols. Rip uses the same algorithm that use distance vector to mathematically compare routes to identify the best path to any given destination address. Routing Updates- RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

RIP stability feature- RIP prevents routing loops from continuing indefinitely by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops in a path is 15. If a router receives a routing update that contains a new or changed entry, and if increasing the metric value by 1 causes the metric to be infinity (that is, 16), the network destination is considered unreachable. The downside of this stability feature is that it limits the maximum diameter of a RIP network to less than 16 hops. RIP implements the split horizon and holddown mechanisms to prevent incorrect routing information from being propagated.

RIP timers- RIP uses numerous timers to regulate its performance. These include a routing-update timer, a route-timeout timer, and a route-flush timer. The routing update timer clocks the interval between periodic routing updates. Generally, it is set to 30 seconds, with a small random amount of time added whenever the timer is reset. This is done to help prevent congestion, which could result from all routers simultaneously attempting to update their neighbors. Each routing table entry has a route-timeout timer associated with it. When the route-timeout timer expires, the route is marked invalid but is retained in the table until the route-flush timer expires.
E. Intermediate system - intermediate system (IS-IS)-

Integrated Intermediate System - Intermediate System routing protocol is a link state protocol similar to OSPF that is used with large enterprise and ISP customers. An intermediate system is a router and IS-IS is the routing protocol that routes packets between intermediate systems. IS-IS utilizes a link state database and runs the SPF Dijkstra algorithm to select shortest paths routes. Neighbor routers on point to point and point to multipoint links establish adjacencies by sending hello packets and exchanging link state databases. IS-IS routers on broadcast networks select a designated router that establishes adjacencies with all neighbor routers on that network. The designated router and each neighbor router will establish an adjacency with all neighbor routers by multicasting link state advertisements to the network itself. That is different from OSPF, which establishes adjacencies between the DR and each neighbor router only.

IS-IS use a hierarchical area structure with level 1 and level 2 router types. Level 1 router is similar to OSPF intra-area routers, which have no direct connections outside of its area. Level 2 routers comprise the backbone area which connects different areas similar to OSPF area 0. With IS-IS a router can be an L1/L2 router which is like an OSPF area border router (ABR) which has connections with its area and the backbone area. The difference with IS-IS is that the links between routers comprise the area borders and not the router. Each IS-IS router must have an assigned address that is unique for that routing domain. An address format is used which is comprised of an area ID and a system ID. The area ID is the assigned area number and the system ID is a MAC address from one of the router interfaces. There is support for variable length subnet masks, which is standard with all link state protocols. Note that IS-IS assigns the routing process to an interface instead of a network.

Characteristics of IS-IS-
- It is Link state routing protocol
- It supports Variable length subnet masking
- Routing Advertisements are Partially sent When Routing Changes Occur.
- Load Balancing occurs Across 6 Equal Cost Paths.
- Hello timer interval is 10 seconds.
- Dead timer interval is 30 seconds.
- It uses areas as Hierarchical topology similar to OSPF.
- Designated router election is done but no BDR is elected.

III. Comparison Between RIP, IGRP, EIGRP, OSPF and IS-IS-

The comparison of different Interior gateway protocols is summarized below.

<table>
<thead>
<tr>
<th>Routing protocol</th>
<th>AD</th>
<th>Metric</th>
<th>Periodic updates</th>
<th>Triggering updates</th>
<th>Partial updates</th>
<th>Vlsm/cidr subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rip v1</td>
<td>120</td>
<td>Hop count</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Ripv2</td>
<td>120</td>
<td>Hop count</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>yes</td>
</tr>
<tr>
<td>ospf</td>
<td>110</td>
<td>Cost Bandwidth</td>
<td>No</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>igrp</td>
<td>100</td>
<td>Bandwidth</td>
<td>No</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>eigrp</td>
<td>90</td>
<td>Bandwidth, Load delay, Reliability</td>
<td>No</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

IV. Conclusion

This paper concludes the different Interior gateway protocols (IGP) and we explained every protocol briefly and quoted some important characteristics of the protocols which will help to decide the use of protocol in the network according to the network size and speed of the network.

References