ROUTING PROTOCOLS USED IN COMPUTER NETWORKS AND COMPARISON BETWEEN ALL PROTOCOLS

- **SAPNA BASSAN**

INTRODUCTION

A routing protocol is the language a router speaks with other routers in order to share information about the reach ability and status of network .It includes a procedure to select the best path based on the reach ability information it has and for recording this information in a route table. Regarding to select the best path, a routing metric will be applied and it is computed by a routing algorithm. A metric is a variable assigned to routers as a means of ranking them from the best to worst or from most preferred to least preferred. Different routing protocols have different metrics. When there is more than one route between two nodes, a router must determine a method of metrics by choose the routing protocol to calculate the best path.

ROUTING BASICS

To be able to route packets from source to the destination, a router should contain the following information's:

Destination Address

- Neighbour routers from which it learns about all remote networks
- Possible routes to all remote networks
- The best route to each remote network
- How to maintain and verify routing information

The router needs to prepare a routing table which is a map of the interconnectivity of the nodes in the internetwork which contains details of which path to follow and how

to reach the remote network. Such a map is built on the basis of the information shared among the nodes in the internetwork configured in the same routing protocol. The administrator can also manually build the routing table. Each and every node in the internetwork sends and receives updates to build up the topology. For the adjacent nodes, the node has the path to reach it i.e. the exit interface to reach the neighbour node. If a node is not directly connected or is connected by a sequence of nodes then the node must find its way to the destination node. Such a node can find the required path information either by Static Routing or by Dynamic Routing. Static routing requires manually creation and updating of the routing table by the administrator by inserting all network information into each node. Dynamic Routing is better than Static Routing. In the case of the Dynamic Routing, the nodes exchange details on the basis of the routing protocol configured in the node. This information is updated in the routing table. If any change occurs in the internetwork the sharing process starts and the information is exchanged until all the nodes are converged to the same routing table.

ADMINISTRATIVE DISTANCE

The administrative distance (AD) is used to rate the trustworthiness of routing information. The value depends on the information that a router receives from its neighbour routers. The Administrative Distance is a value which ranges from 0 to 255, where 0 means it is the most trusted and 255 means that it doesn't allows any traffic to pass through it. If in case, a router receives more than one update from the same network, and then the router which receives such updates checks for the AD value. The AD value for each update will differ and the router accepts only that AD value which is the lowest and this value are updated in the routing table of the router.

ROUTE SOURCE	DEFAULT AD
A connected interface	0

A Static Route	1
RIP	120
EIGRP	90
OSPF	100

If a network is directly connected to a router, then that router will use the interface connected to the network always. If any routing protocol is configured in the router, then also the router chooses the connected interface as default as its AD value is less. If in the router multiple routing protocols are configured then on receiving updates from the same network with similar routing protocols then it chooses the least AD value. For example, if the router has a static route, a RIP route and also an OSPF route to the same network, then the router will use the static route always by default.

ROUTING METRICS

The different routing metrics includes the following: -

1. Hop count: - The number of routers which a packet will pass before arriving at the destination router.

2. Cost: - It is generally an arbitrary value that is assigned by the administrator and is based on the bandwidth

3. Bandwidth: - It is the data capacity of the link.

4. Delay: - It measures the total time taken by a packet to move from the source router to the destination router.

5. Load: - It measures the amount of activity on a network source link a router or a link.

6. Reliability: - It refers to the network link's bit error rate.

7. MTU: - It stands for Maximum Transmission Unit. It resembles the maximum frame length in octets which is allowed to pass to the internetwork without fragmentation.

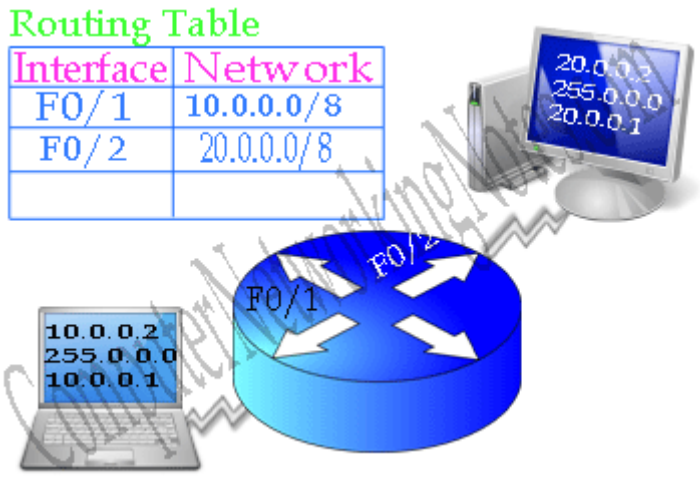
How Routing Protocols Work

Every network routing protocol performs three basic functions:

1. *discovery* - identify other routers on the network
2. *route management* - keep track of all the possible destinations (for network messages) along with some data describing the pathway of each
3. *path determination* - make dynamic decisions for where to send each network message

A few routing protocols(called *link state protocols*) enable a router to build and track a full map of all network links in a region while others (called *distance vector protocols)* allow routers to work with less information about the network area. IP routing is the process of moving data packets between different networks. By default two different IP networks cannot communicate with each other. They need a mediator device that can switch packet between them. Router takes this responsibility. Routers interfaces are associated with different networks. This association is kept in routing table. Routers use it to take switching decision.

Following figure illustrates a simple routing example.



Protocols can fall into two groups one is static routing and other is dynamic routing. Static routing is simply the process of manually entering routes into a device's routing table via a 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. When routers learn from an administrator, it is called static routing. In static routing we have to add all network locations manually. If any change occurs in network, administrator is responsible to update it by hand in all routers.

Advantage of static routing

- It is easy to implement.
- It is most secure way of routing, since no information is shared with other routers.
- It puts no overhead on resources such as CPU or memory.

Disadvantage of static routing

- It is suitable only for small network.
- If a link fails static route cannot reroute the traffic.

However, dynamic routing allows routers to select the best path when there is a real time logical network layout change. In our project, we will discuss the difference

between the EIGRP, RIP and OSPF. All of them are belong to dynamic routing protocols. When routers learn from neighbouring router through the routing protocols, it is called dynamic routing. In dynamic routing routers add network locations automatically form the routing information. If any change occurs in network, affected routers update others via routing information.

Advantage of dynamic routing

- It is suitable for all type of networks.
- Automatically build routing tables.
- Reroute the traffic from possible network, in link failure condition.

Disadvantage of dynamic routing

- It is hard to implement.
- It is less secure, since it shares routing updates with other routers.
- It puts additional overhead on resources such as CPU, memory and link bandwidth.

Depending on network requirement we can use either static routing or dynamic routing. Even more we can use a combination of both dynamic and static routing.

Routing updates

Routing update is a mechanism of sharing information with neighbouring routers. In a particular time duration router advertise its routing information through broadcast or multicast. Different protocols have different time intervals. Some protocols use broadcast for routing updates while some uses multicast. Routing updates contain all necessary information for routing protocol such as learned network, timers, AS, AD, matrix values, interface details etc.

Autonomous System

Autonomous System (AS) is a collection of routers that share same routing table information. AS is a boundary line for routing protocol. It could be your company, or group of companies. It is defined by a numeric value. To distinguish between different AS, Internet Assigned Numbers Authority (IANA) provides a range from 1 to 65535. There are two types of AS, private and public. Private AS numbers are used for internal network. Public AS numbers are used for internet backbone.

Administrative Distance

Administrative distance (AD) is the trustworthiness of routing update received from a neighbour router. If a router receives two routing updates for same path from two different routing protocols then router will check the AD value to choose the best path. AD is a numeric value from 0 to 255. If one update has lower AD value than other, then the route with the lowest AD will be placed in the routing table

Route source	Default AD value
Direct connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown	255

Lower AD value is more believable by router. 0 is considered as the most trustworthiness network while 255 is considered as invalid route and it will be never used.

Metric

If two routing updates for same network have same AD value then metric will use to choose the best path. Metric is a measurement to calculate best path. Route with the lowest metric will be chosen. Different routing protocols use different metrics. It may use single metric or multiple metrics. For example EIGRP uses bandwidth, delay, load, MTU and reliability while RIP only uses hop count as metric.

Routing Protocol	Metric	Description
EIGRP	Bandwidth	Capacity of link in Kbps
EIGRP	Delay	Time to reach in destination
EIGRP	Load	Path that is least utilize
EIGRP	MTU	Path that support largest frame size
EIGRP	Reliability	Path that have least down time
OSPF	Cost	Inverse of bandwidth links
RIP	Hop count	Hops (Routers) in the way of destination

Routing protocols can be classified into two classes:

- Distance vector and link state.

Distance vector routing protocol is based on Bellman – Ford algorithm and Ford – Fulkerson algorithm to calculate paths. A distance vector routing protocol uses a distance calculation and a vector direction of next hop router as reported by neighbouring routers to choose the best path. It requires that a router informs its neighbours of topology changes periodically.

Link state routing protocols build a complete topology of the entire network are and then calculating the best path from this topology of all the interconnected networks.

It requires more processing power and memory because it has a complete picture of the network

The purpose of routing protocols is to learn of available routes that exist on the enterprise network, build routing tables and make routing decisions. IP routing protocols are divided into two classes: interior gateway protocols (IGPs) and exterior gateway protocols (EGPs) The Interior Gateway Protocols Interior protocols are used for routing networks that are under a common network administration. All IP interior gateway protocols must be specified with a list of associated networks before routing activities can begin. A routing process listens to updates from other routers on these networks and broadcasts its own routing information on those same networks. The interior routing protocols supported are as follows:

- IGRP (Internet Gateway Routing Protocol)
- EIGRP
- OSPF (Open Shortest Path First)
- RIP (Routing Information Protocol)
- IS-IS (Intermediate System-to-Intermediate System)and

Exterior protocols are used to exchange routing information between networks that do not share a common administration. IP exterior gateway protocols require three sets of information before routing can begin:

1. A list of neighbour (or peer) routers with which to exchange routing information
2. A list of networks to advertise as directly reachable
3. The autonomous system number of the local router

The supported exterior routing protocols are as follows:

- Border Gateway Protocol (BGP)
- Exterior Gateway Protocol (EGP)

Router Discovery Protocols

Our routers also support two router discovery protocols:

- Gateway Discovery Protocol (GDP)
- ICMP Router Discovery Protocol (IRDP)

Which allow hosts to locate routers? GDP was developed by Cisco and is not an industry standard.

Multiple Routing Protocols

You can configure multiple routing protocols in a single router to connect networks that use different routing protocols. You can, for example, run RIP on one subnetted network, IGRP on another subnetted network, and exchange routing information between them in a controlled fashion. The available routing protocols were not designed to interoperate with one another, so each protocol collects different types of information and reacts to topology changes in its own way. Our routers can handle simultaneous operation of up to 30 dynamic IP routing processes. The combination of routing processes on a router can consist of the following protocols:

- Up to 30 IGRP routing processes
- Up to 30 OSPF routing processes
- One RIP routing process
- One IS-IS process

- One BGP routing process

- Up to 30 EGP routing processes

Interior Gateway Routing Protocol (IGRP)

Interior Gateway Routing Protocol is a distance vector routing protocol developed by Cisco systems for routing multiple protocols across small and medium sized Cisco networks. It is proprietary which requires that you use Cisco routers. It is somewhat more scalable than RIP since it supports a hop count of 100, only advertises every 90 seconds and uses a composite of five different metrics to select a best path destination. It uses less bandwidth than RIP but converges much slower since it is 90 seconds before IGRP routers are aware of network topology changes.

Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol is a hybrid routing protocol developed by Cisco systems for routing many protocols across an enterprise Cisco network. It has characteristics of both distance vector routing protocols and link state routing protocols. EIGRP will route the same protocols that IGRP routes (IP, IPX, Decnet and Appletalk) and use the same composite metrics as IGRP to select a best path destination. As well there is the option to load balance traffic across equal or unequal metric cost paths. There is support for a hop count of 255 and variable length subnet masks. Convergence with EIGRP is faster since it uses an algorithm called dual update algorithm or DUAL, which is run when a router detects that a particular route is unavailable. EIGRP will update its routing table with the new route and the associated metric. Route changes are advertised only to affected routers when changes occur.

That utilizes bandwidth more efficiently than distance vector routing protocols. Key capabilities of EIGRP are:

- Fast Convergence
- Support for IPv4 and IPv6
- Support for summaries and discontagious work
- Uses DUAL algorithm
- Support for VLSM (variable Length Subnet Masking)
- Partial update support
- Multiple network layer protocol

The advantages using EIGRP are as follow:

1) Easy to configure.

2) Loop free routes.

3) Keeps backup path to the destination network.

4) Convergence time is low and bandwidth utilization.

5) Support Variable Length Subnet Mask (VLSM) and Classless Inter Domain Routing (CIDR).

6) Supports authentication.

The disadvantage of using EIGRP is as follow:

1) Considered as Cisco proprietary routing protocol.

2) Routers from other vendor are not able to utilize EIGRP.

Configuring EIGRP: To start an EIGRP session on a router, use the router eigrp command followed by the autonomous system number of the network. Remember as with IGRP, we use the classful network address, which is all subnet and host bits turned off.

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1 (config) #router eigrp?

<1-65535> Autonomous system number

R1(config)#router eigrp 10

R1(config-router)#network 20.0.0.0

R1(config-router)#

R1(config-router)#end

R1#

The AS number, as you see can be any number from 1 to 65535. A router can be a member of as many ASes as you want it to be. EIGRP works on the neighbour discovery mechanism. There are three conditions that must be met before there will any neighbour ship established.

- Hello Received
- AS number matching
- Same metric

Hello message is used to establish the initial phase of neighbourship establishment. EIGRP that belongs to different AS number do not share the routing automatically. **Reliable Transport Protocol (RTP)** EIGRP uses a proprietary protocol called Reliable Transport Protocol (RTP) to manage the communication of messages between EIGRP speaking routers. And as the name suggests, reliability is a key concern of this protocol. Cisco has designed a mechanism that leverages multi casts and uncast to deliver updates quickly and to track the receipt of the data. **VLSM Support in EIGRP** EIGRP supports the use of VLSM (Variable Length Subnet Masking). It allows the conservation of address space through the use of subnet masks that more closely fit the host requirement. **EIGRP Metrics** EIGRP uses a single factor to compare its routes and select the best possible path EIGRP can use a combination of four, called a composite metrics:

- Bandwidth
- Delay
- Reliability
- Load

EIGRP also supports the concept of load balancing.

Open Shortest Path First (OSPF)

Open Shortest Path First is a true link state protocol developed as an open standard for routing IP across large multi-vendor networks. A link state protocol will send link state advertisements to all connected neighbours of the same area to communicate route information. Each OSPF enabled router, when started, will send hello packets to all directly connected OSPF routers. The hello packets contain information such as router timers, router ID and subnet mask. If the routers agree on the information they become OSPF neighbours. Once routers become neighbours they establish adjacencies by exchanging link state databases. Routers with OSPF interfaces configured as broadcast (Ethernet) and NBMA (Frame Relay) will use a designated router that

establishes those adjacencies. OSPF uses a hierarchy with assigned areas that connect to a core backbone of routers. Each area is defined by one or more routers that have established adjacencies.

Fast convergence is accomplished with the SPF (Dijkstra) algorithm which determines a shortest path from source to destination. The routing table is built from running SPF which determines all routes from neighbour routers. Since each OSPF router has a copy of the topology database and routing table for its particular area, any route changes are detected faster than with distance vector protocols and alternate routes are determined.

Open Shortest Path First was created to overcome some of its limitations of RIP including

- the 15 hop count restriction
- the inability to organize networks into a routing hierarchy, important for manageability and performance on large internal networks
- The significant spikes of network traffic generated by repeatedly re-sending full router tables at scheduled intervals.

As the name suggests, OSPF is an open public standard with widespread adoption across many industry vendors. OSPF-enabled routers discover the network by sending identification messages to each other followed by messages that capture specific routing items rather than the entire routing table. It is the only link state routing protocol listed in this category.

OSPF also has three versions

- OSPFv1 was published in RFC 1131
- OSPFv2 was published in RFC 2328
- OPSFv3 was published for IPv6 was released in RFC 2740

OSPF is also quick in convergence but not as quick as EIGRP but it supports multiple, equal-cost routes to the same destination but OSPF doesn't support IPv6 and IPv4 both at the same time. OSPF had following features which makes it one of the best routing protocols in the field:-

- OSPF is a link state routing protocol
- OSPF consist of areas and autonomous system
- OSPF minimizes routing update traffic
- It also supports the VLSM/CIDR
- Support unlimited hop count

Characteristic	**OSPF**	**RIPv2**	**RIPv1**
Type of protocol	Link state	Distance vector	Distance vector
Classless support	Yes	Yes	No
VLSM support	Yes	Yes	No
Auto-summarization	No	Yes	Yes
Manual summarization	Yes	No	No
Discontiguous support	Yes	Yes	No
Route propagation	Multicast on change	Periodic multicast	Periodic broadcast
Path metric	Bandwidth	Hops	Hops
Hop count limit	None	15	15
Convergence	Fast	Slow	Slow
Peer authentication	Yes	Yes	No
Hierarchical network requirement	Yes (using areas)	No (flat only)	No (flat only)
Updates	Event triggered	Route table updates	Route table updates
Route computation	Dijkstra	Bellman-Ford	Bellman-Ford

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.

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 here:

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.

The Advantage of OSPF routing protocol are:

1) OSPF is not a CISCO proprietary protocol.

2) OSPF always determines the loop free routes.

3) If any changes occur in the network it updates fast.

4) Low bandwidth utilization.

5) Support multiple routes for a single destination network.

6) OSPF is based on cost of the interface

. 7) Support Variable Length Subnet Mask (VLSM)

The disadvantages of OSPF are:

1) Difficult to configure

2) More memory requirements.

CONFIGURING OSPF:

Router(config)# router ospf 1

Router(config-router)# network 200.100.100.0 0.0.0.7 area 0

Routing Information Protocol (RIP)

RIP-enabled routers discover the network by first sending a message requesting router tables from neighboring devices. Neighbour routers running RIP respond by

sending the full routing tables back to the requestor, whereupon the requestor follows an algorithm to merge all of these updates into its own table. At scheduled intervals, RIP routers then periodically send out their router tables to their neighbours so that any changes can be propagated across the network.

Traditional RIP supported only IPv4 networks but the newer RIPng standard also supports IPv6. RIP utilizes either UDP ports 520 or 521 (RIPng) for its communication.

RIP is a standardized vector distance routing protocol and uses a form of distance as hop count metric. It is a distance vector. Through limiting the number of hop counts allowed in paths between sources and destinations, RIP prevents routing loops. Typically, the maximum number of hops allowed for RIP is 15. However, by achieving this routing loop prevention, the size of supporting networks is sacrificed. Since the maximum number of hop counts allowed for RIP is 15, as long as the number goes beyond 15, the route will be considered as unreachable. When first developed, RIP only transmitted full updates every 30 seconds. In the early distributions, traffic was not important because the routing tables were small enough. As networks become larger, massive traffic burst becomes more likely during the 30 seconds period, even if the routers had been initialized at different times. Because of this random initialization, it is commonly understood that the routing updates would spread out in time, but that is not the case in real practice.

RIP has four basic timers:

1. Update Timer (default 30 seconds): defines how often the router will send out a routing table update.
2. Invalid Timer (default 180 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 with a metric of 16, which means the route is unreachable, and will be placed in a hold down state.

3. Hold-down Timer (default 180 seconds): specifies how long RIP will keep a route from receiving updates when it is in a hold-down state. In a hold-down state, RIP will not receive any new updates for routes until the hold-down timer expires.

4. Flush Timer (default 240 seconds): When no new updates are received about this route, flush timer indicates how long a route can remain in a routing table before getting flushed out. The flush timers operates simultaneously with the invalid timer, so every 60 seconds, after it has been marked invalid, the route will get flushed out. When RIP timer is not in sync with all routers on the RIP network, system instability occurs. This timer must be set to a higher value than the invalid timer.

RIP Versions:

1. RIPv1: RIPv1supports Class full routing; therefore variable length subnet masks (VLSM) cannot be used. There is also no authentication mechanism.

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

Configuring RIP:

To configure RIP routing, just turn on the protocol with the router rip command and tell the RIP routing protocol which network to advertise.

```
Router1> enable
Router1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)# router rip version 2
Router1(config-router)# network 192.10.0.0
```

Disadvantages of RIP

1. It uses more bandwidth as updates are exchanged every 30 seconds where each update contains the complete routing table of the router.

2. It does not uses bandwidth as the metric for calculation of the shortest path. RIP has a very slow convergence.

3. RIP implementation can lead to routing loops in the network.

4. RIP is only applicable to small network and is inefficient for larger networks.

Integrated IS-IS

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 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. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both). Level 2 routers are interarea 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 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. Neighbour 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 and NBMA networks select a designated router that establishes adjacencies with all neighbour routers on that network. The designated router and each neighbour router will establish an adjacency with all neighbour routers by multicasting link state advertisements to the network itself.

Border Gateway Protocol (BGP)

Border Gateway Protocol is an exterior gateway protocol, which is different from the interior gateway protocols. The main difference is in the autonomous system used somewhat differently with protocols such as EIGRP than it is with BGP. Exterior gateway protocols such as BGP route between autonomous systems, which are assigned a particular AS number. AS numbers can be assigned to an office with one or several BGP routers. The BGP routing table is comprised of destination IP addresses, an associated AS-Path to reach that destination and a next hop router address. The AS-Path is a collection of AS numbers that represent each office involved with routing packets. An EIGRP network can configure many autonomous systems. They are all managed by the company for defining route summarization, redistribution and filtering. BGP is utilized a lot by Internet Service Providers (ISP) and large enterprise companies that have dual homed internet connections with single or dual routers homed to the same or different Internet Service Providers. BGP will route packets across an ISP network, which is a separate routing domain that is

managed by them. The ISP has its own assigned AS number, which is assigned by InterNIC. New customers can either request an AS assignment for their office from the ISP or InterNIC. A unique AS number assignment is required for customers when they connect using BGP. There are 10 defined attributes that have a particular order or sequence, which BGP utilizes as metrics to determine the best path to a destination.

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 reach ability 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 reach ability information from neighbouring autonomous systems.

Operation of BGP:

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. Keep alive: 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

BGP Characteristics

BGP is different from other routing protocols in several ways. Most important being that BGP is neither a pure distance vector protocol nor a pure link state protocol. Let's have a look at some of the characteristics that stands BGP apart from other protocols.

• Inter-Autonomous System Configuration: BGP's primary role is to provide communication between two autonomous systems.

• Next-Hop paradigm: Like RIP, BGP supplies next hop information for each destination.

• Coordination among multiple BGP speakers within the autonomous system: If an Autonomous system has multiple routers each communicating with a peer in other autonomous system, BGP can be used to coordinate among these routers, in order to ensure that they all propagate consistent information.

• Path information: BGP advertisements also include path information, along with the reachable destination and next destination pair, which allows a receiver to learn a series of autonomous system along the path to the destination.

• Policy support: Unlike most of the distance-vector based routing, BGP can implement policies that can be configured by the administrator. For Example, a router running BGP can be configured to distinguish between the routes that are known from within the Autonomous system and that which are known from outside the autonomous system.

• Runs over TCP: BGP uses TCP for all communication. So the reliability issues are taken care by TCP.

• Conserve network bandwidth: BGP doesn't pass full information in each update message. Instead full information is just passed on once and thereafter successive messages only carries the incremental changes called deltas. By doing so a lot of network Bandwidth is saved. BGP also conserves bandwidth by allowing sender to aggregate route information and send single entry to represent multiple, related destinations.

• Support for CIDR: BGP supports classless addressing (CIDR). That it supports a way to send the network mask along with the addresses.

• Security: BGP allows a receiver to authenticate messages, so that the identity of the sender can be verified.

BGP Functionality and Route Information Management

The job of the Border Gateway Protocol is to facilitate the exchange of route information between BGP devices, so that each router can determine efficient routes to each of the networks on an IP internetwork. This means that descriptions of routes are the key data that BGP devices work with. But in a broader aspect, BGP peers perform three basic functions.

The First function consists of initial peer acquisition and authentication. Both the peers establish a TCP connection and perform message exchange that guarantees both sides have agreed to communicate.

The second function primarily focus on sending of negative or positive reach ability information, this step is of major concern.

The Third function provides ongoing verification that the peers and the network connection between them are functioning correctly. Every BGP speaker is responsible for managing route descriptions according to specific guidelines established in the BGP standards.

BGP Route Information Management Functions Conceptually, the overall activity of route information management can be considered to encompass four main tasks:

• Route Storage: Each BGP stores information about how to reach networks in a set of special databases. It also uses databases to hold routing information received from other devices.

• Route Update: When a BGP device receives an Update from one of its peers, it must decide how to use this information. Special techniques are applied to determine when and how to use the information received from peers to properly update the device's knowledge of routes.

• Route Selection: Each BGP uses the information in its route databases to select good routes to each network on the internetwork.

• Route Advertisement: Each BGP speaker regularly tells its peers what it knows about various networks and methods to reach them. This is called route advertisement and is accomplished using BGP Update messages.

BGP Attributes

BGP Attributes are the properties associated with the routes that are learned from BGP and used to determine the best route to a destination, when multiple routes are available. An understanding of how BGP attributes influence route selection is required for the design of robust networks. This section describes the attributes that BGP uses in the route selection process:

- AS_path : When a route advertisement passes through an autonomous system, the AS number is added to an ordered list of AS numbers that the route advertisement has traversed.

- Next hop: The EBGP next-hop attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers. For IBGP, the EBGP next-hop address is carried into the local AS.

- Weight: Weight is a Cisco-defined attribute that is local to a router. The weight attribute is not advertised to neighbouring routers. If the router

learns about more than one route to the same destination, the route with the highest weight will be preferred.

- Local preference: The local preference attribute is used to prefer an exit point from the local autonomous system (AS). Unlike the weight attribute, the local preference attribute is propagated throughout the local AS. If there are multiple exit points from the AS, the local preference attribute is used to select the exit point for a specific route.

- Multi-exit discriminator: The multi-exit discriminator (MED) or metric attribute is used as a suggestion to an external AS regarding the preferred route into the AS that is advertising the metric. The term suggestion is used because the external AS that is receiving the MEDs may be using other BGP attributes for route selection.

- Origin: The origin attribute indicates how BGP learned about a particular route. The origin attribute can have one of three possible values:

    1. IGP—the route is interior to the originating AS. This value is set when the network router configuration command is used to inject the route into BGP.

    2. EGP—the route is learned via the Exterior Border Gateway Protocol (EBGP).

    3. Incomplete—the origin of the route is unknown or learned in some other way. An origin of incomplete occurs when a route is redistributed into BGP. The origin attribute is used for route selection.

- Community: The community attribute provides a way of grouping destinations, called communities, to which routing decisions (such as acceptance, preference, and redistribution) can be applied. Route maps are used to set the community attribute. Predefined community attributes are listed here:

    i. No-export—Do not advertise this route to EBGP peers.

    ii. No-advertise—do not advertise this route to any peer.

    iii. Internet—Advertise this route to the Internet community; all routers in the network belong to it.

Salient Features

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

1. BGP is an incremental protocol, where after a complete routing table is exchanged between neighbours, only changes to that information are exchanged. These changes may be new route advertisements, route withdrawals, or changes to route attributes.

2. BGP is a path-vector protocol where advertisements contain a list of autonomous systems used to reach the destination.

3. Routes are advertised at the prefix level, so an AS would send a separate update for each of its reachable prefixes.

4. 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.

BGP Path Selection

BGP could possibly receive multiple advertisements for the same route from multiple sources. BGP selects only one path as the best path. When the path is selected, BGP puts the selected path in the IP routing table and propagates the path to its neighbors. BGP uses the following criteria, in the order presented, to select a path for a destination:

- If the path specifies a next hop that is inaccessible, drop the update.
- Prefer the path with the largest weight.
- If the weights are the same, prefer the path with the largest local preference.
- If the local preferences are the same, prefer the path that was originated by BGP running on this router.
- If no route was originated, prefer the route that has the shortest AS_path.
- If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than incomplete).
- If the origin codes are the same, prefer the path with the lowest MED attribute.
- If the paths have the same MED, prefer the external path to the internal path.
- If the paths are still the same, prefer the path through the closest IGP neighbor.
- Prefer the path with the lowest IP address, as specified by the BGP router ID.

Comparison of different Routing Protocols:

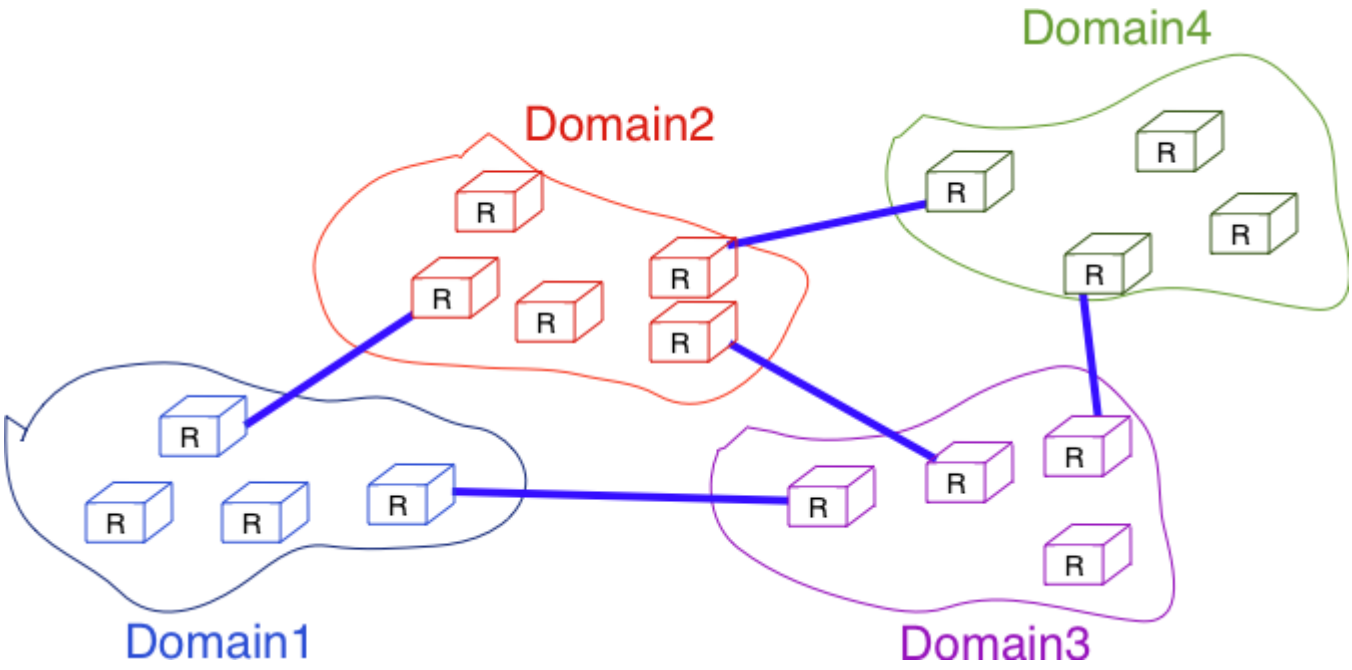
	Type	**Convergence**	**Class**	**AD**	**Metric**	**Classless**	**Transport Type**

RIP	IGP	Slow	Distance Vector	120	Hop count	No	UDP
OSPF	IGP	Fast	Link State	110	Cost	Yes	IP Protocol 89
IS-IS	IGP	Fast	Link State	115	Cost	Yes	Layer2
EIGRP	IGP	Very Fast	Hybrid	5 summary 90 internal 170 external	Hop count 100	Yes	IP Protocol 88
BGP	EGP	Very Fast	Path Vector	20 external 200 internal	Path Attribute	Yes	TCP/179

Routing in IP Network

In a large IP network such as the global Internet, routers need to exchange routing information. The Internet is an interconnection of networks, often called domains that are under different responsibilities. The Internet is composed on more than 40,000 different domains and this number is still growing. A domain can be a small enterprise that manages a few routers in a single building, a larger enterprise with a hundred

routers at multiple locations, or a large Internet Service Provider managing thousands of routers. Two classes of routing protocols are used to allow these domains to efficiently exchange routing information.



Organisation of a small Internet

The first class of routing protocols are the *intradomain routing protocols* (sometimes also called the interior gateway protocols or ***IGP***). An intradomain routing protocol is used by all routers inside a domain to exchange routing information about the destinations that are reachable inside the domain. There are several intradomain routing protocols. Some domains use ***RIP***, which is a distance vector protocol. Other domains use link-state routing protocols such as ***OSPF*** or ***IS-IS***. Finally, some domains use static routing or proprietary protocols such as ***IGRP*** or ***EIGRP***.

These intradomain routing protocols usually have two objectives. First, they distribute routing information that corresponds to the shortest path between two routers in the domain. Second, they should allow the routers to quickly recover from link and router failures.

The second class of routing protocols are the *interdomain routing protocols* (sometimes also called the exterior gateway protocols or ***EGP***). The objective of an interdomain routing protocol is to distribute routing information between domains. For scalability reasons, an interdomain routing protocol must distribute aggregated routing information and considers each domain as a black box.

A very important difference between intradomain and interdomain routing are the *routing policies* that are used by each domain. Inside a single domain, all routers are considered equal, and when several routes are available to reach a given destination prefix, the best route is selected based on technical criteria such as the route with the shortest delay, the route with the minimum number of hops or the route with the highest bandwidth.

When we consider the interconnection of domains that are managed by different organisations, this is no longer true. Each domain implements its own routing policy. A routing policy is composed of three elements: an *import filter* that specifies which routes can be accepted by a domain, an *export filter* that specifies which routes can be advertised by a domain and a ranking algorithm that selects the best route when a domain knows several routes towards the same destination prefix. As we will see later, another important difference is that the objective of the interdomain routing protocol is to find the *cheapest* route towards each destination. There is only one interdomain routing protocol: ***BGP***.

How Network Protocols Are Implemented

Modern operating systems contain built-in software services that implement support for some network protocols. Applications like Web browsers contain software libraries that support the high level protocols necessary for that application to

function. For some lower level TCP/IP and routing protocols, support is implemented in directly hardware (silicon chipsets) for improved performance.

Each packet transmitted and received over a network contains binary data (ones and zeros that encode the contents of each message). Most protocols add a small *header* at the beginning of each packet to store information about the message's sender and its intended destination. Some protocols also add footer at the end. Each network protocol has the ability to identify messages of its own kind and process the headers and footers as part of moving data among devices.

A *protocol family*. Students of networking traditionally learn about the OSI model that group of network protocols that work together at higher and lower levels are often called a conceptually organizes network protocol families into specific layers for teaching purposes.

REREFERENCES

[1] Comprehensive Analysis of Dynamic Routing Protocols in Computer Networks Priya Asher, International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4450-4455

[2] Enhanced Comparative Study of Networking Routing Protocols BY Vishal Nigam, Md. Samil Farouqui , Gunjan Gandhi , Volume 4, Issue 2, February 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[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, RejiThomas, "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] 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

[7] Routing Protocol Convergence Comparison using Simulation and Real Equipment D. Sankar and D. Lancaster Centre for Security, Communications and Network Research Plymouth University, United Kingdom

[8] Book of Routing and Congestion Control Version 2

[9] International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 011, 1962-1964 A Comparative Study of Routing Protocols by Rajender Kumar, Jitender Vats, Arvind Kumar