Routing protocol design

Dushan Aluth Patabendige
Bsc. (Hons) in Computing, Glyndwr University, UK.
hello@dushan.lk

Table of content

List of figures

Introduction to routing

Routing is moving data from source to destination in order to accomplish the communication in a computer network. Router is the hardware equipment which helps to achieve communications. Routing is the most important concept behind the communication of your home or office network and also the internet. Internet is a large network which is built by connecting many independent small networks together. An independent small network can refer as an Autonomous System (AS).

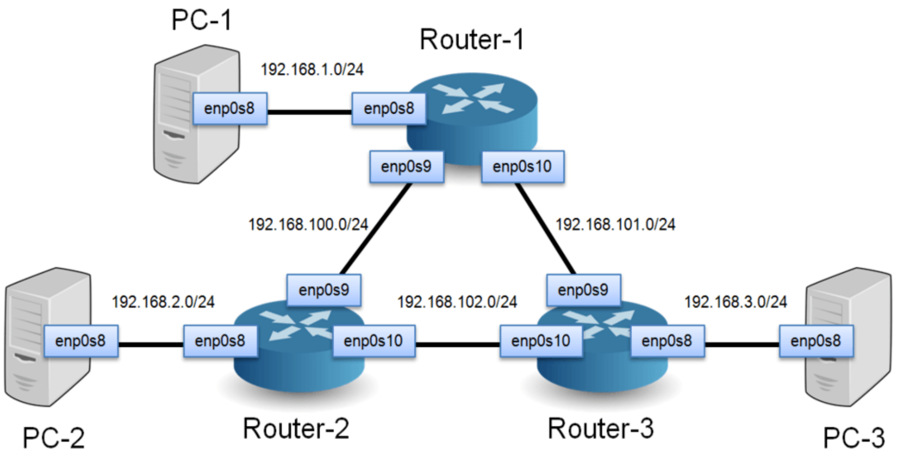


Figure 1: Source - https://www.brianlinkletter.com

Routing protocol

Routing protocol is a specification which defines how the communication should happen between routers of a computer network. And also, this defines how the network should handle failures, how to share updated network information and it calculates the best path to send data. Routing protocols can classify based on their purpose, operation and behavior.

- Purpose: Interior Gateway Protocol and Exterior Gateway Protocol
- Operation: Distance vector protocol, link-state protocol or vector path protocol
- Behavior: Classful or Classless

Routing table

Routing table is a dataset which stored inside the router and it has all reachable destinations for the particular router. Each row of the routing table represents a route and it contains important data like destination address, hop count and interface. We can configure the routing table manually or we can let it to learn and update automatically.

Static routing

If we enter or update routes on the routing table manually we call it static routing. In this case the router cannot learn about the network by itself. There are many advantages and disadvantages in static routing. Better security and less bandwidth usage are advantages of static routing and disadvantages are less maintainability and less scalability.

Dynamic routing

If routers learn about network changes by itself and update the routing table we call it dynamic routing. In dynamic routing always, routers are exchanging routing updates, so it uses an extra amount of bandwidth to maintain the network. But when we need to build a scalable large network, dynamic routing is the best option. Because it can handle network changes by itself, so it is easy to configure and maintain. The proposed routing protocol design also based on a dynamic routing protocol. So further discussion will be about dynamic routing protocols.

Dynamic routing protocol

Interior routing protocol

Interior routing protocol is the specific routing protocol, which is implemented within an autonomous system. Different autonomous systems may have different interior routing protocols. Interior Gateway Protocol (IGP) is another name to refer the interior routing protocol of an autonomous system. There are many IGPs available in use, for example RIP, IGRP and OSPF.

Distance vector routing protocol

In distance vector routing protocol, routes are advertised with two main properties. These are distance and vector.

- Distance: This is the distance from the source to the destination. The distance can calculate based on many matrices. For example: it can be based on the hop count, bandwidth or delay.
- Vector: Vector is the direction to the next hop.

Distance vector protocol does not have the knowledge about the entire map of the network topology and it uses periodic updates to share routing information with neighbors. So, it does not know the entire path to a destination. IGRP and EIGRP can mention as examples for the distance vector routing protocol.

Link-state routing protocol

Link state routing protocol has a view of entire map of the network. So, the source router always knows the exact entire path to reach the destination. Unlike the distance vector protocol, link state routing protocol sends network information updates when a network change occurs. Link state routing protocol is most suitable when having a large hierarchical network and when fast convergence requires.

Exterior routing protocol

Exterior routing protocol or Exterior Gateway Protocol (EGP) used to enable routing between autonomous systems. For example, companies, service providers and large organizations use EGP to establish interconnection. The only example for EGP is Border Gateway Protocol (BGP) which is the routing protocol of the internet.

Challenges in routing

With the massive increment of connected devices, networks are becoming larger and more complex. To manage routes of a complex network topology, routers need more processing power. And also, the network complexity makes it harder to maintain. Scaling the network is another challenge which occurs when networks become big.

Resource consumption

When network becomes big, there might be a lots of network changes within the network. Because of that routers need to process network updates in order to update their existing routes in routing table. This put a heavy load on the processor of the router. With the massive amount of network updates, this process might be slow or stuck somewhere after utilizing full processing power. This might cause to slow the network convergence or the network may not be convergence at all.

Complexity

Routing complexity makes network management more difficult. In corporate environment high availability of the network is so important. Complexity may cause to an unreliable network because troubleshooting and problem resolution is so hard. We can reduce the routing complexity by having consistent routing scheme and routing policy which can meet requirements.

Scaling

Routing protocols has been improved for years and years but still scaling is a major issue. Mainly scaling issues occur on routing calculations when network updates happen in autonomous systems. Because when the network becomes big, routers need more processing power to calculate new routes on network updates. We should avoid having too many routers within an autonomous system to overcome this issue.

Designing a routing protocol

Design goals

Designing a scalable routing protocol is so challenging and major design goals are,

- Accuracy
- Stability
- Redundancy
- Convergence

Design principles

When building a scalable network, design decisions are so important. Protocol design decisions, protocol implementation decisions and network design decisions are really important and can make a direct effect on scalability of the network. There are few main design principles as explained below.

Compartmentalization

To make a reliable and scalable network, fault isolation is so important. It means when some fault or problem occurs in some part of a big network it should not spread across the network and it should not consume resources of the entire network to overcome the fault. We can achieve compartmentalization by dividing a large network into small networks by having many IGPs and EGPs. So, the network will not be in a single flat routing system.

Define scalable routing policies

To make the network more scalable, we should define routing policies as simple as possible. Because when policies are complex it is so hard to configure, manage and debug.

Reduce route processing burdens

We already know large number of routes and routing information cause routing scalable issues. So, it is always best to reduce unnecessary routes and routing information without affecting on business requirements. And also, we better reduce alternative routes. Because this may cause to increase the memory consumption of router when processing too many alternatives. So always better to have a reasonable number of alternative routes which is enough to maintain the redundancy.

Proposed routing protocol

Introduction

The proposed protocol is an IGP and it is a link state routing protocol. There are many reasons to select link state routing over distance vector routing to design this protocol. For example, link state routing protocol has fast convergence, no persistence loops and less bandwidth consumption comparatively to the distance vector routing.

Convergence

Fast convergence of the network is really important when we expect to have a reliable network. For example, if we plan to stream a video or when we need to implement a voice over IP service, fast convergence is a must. In link state routing we can achieve convergence by having the hello protocol and database synchronization.

Hello protocol

Hello protocol is to establish and maintain relationships with router neighbors. This works by sending hello packets to neighbors periodically. In hello protocol there are two interval parameters as hello interval and dead interval. If two routers want to become neighbors the hello interval of both routers should be same and also the dead interval of both routers should be same. The hello interval is the time gap between two hello packets and the dead interval is the time period to wait before decide the particular router is dead, if it failed send a hello packet.

Hello protocol ensures the communication between neighbors is bidirectional and also is the key feature of link state routing which reduces the bandwidth and processor consumption. Because sending and processing a tiny hello packet is lightweight than sending large tables.

Database synchronization

A reliable and accurate database synchronization is really important to maintain the network convergence. To forward packets over two adjacent routers, their databases should be identical. As soon as two neighbor routers decide to become adjacent, one of them becomes master and other becomes slave. After that master router sends database description packets to the slave router. Each of every database description packet contains a sequence number which can use to identify the relevant packet. After receiving the database description packet to the slave router, it acknowledges with the sequence number. Likewise, both routers exchange their databases and become synchronized.

Link state advertisement (LSA)

OSPF uses link state advertisements to exchange network topology information among routers. We can use the same mechanism in our theoretical routing protocol to exchange network topology information. Synchronization of network topology information is really important in order to achieve fast network convergence.

If two routers want to exchange and update network topology information, first each router should send link state advertisements from respective topology databases. Then each router checks their topology tables comparing with received LSAs, if any router found missing LSA or LSAs, then it will send a Link state request (LSR) to get missing LSAs from other router. Then the LSR receiver responds back with a Link state update (LSU) which contains requested LSAs by its neighbor. There are 05 LSA types. When sending a link state request, we have to mention the LSA type. These types are as follows,

- Type 1 - Router LSAs - Contains collected state information of router interfaces.
- Type 2 - Network LSAs - Contains information about connected routers to the network.
- Type 3 - Summary LSAs - Provide route information to network.
- Type 4 - Summary LSAs - Provide route information to autonomous system boundary routers.
- Type 5 - AS external LSAs - Provide route information about external routes.

Redundancy

Redundancy is really important when designing a high available network. We can use equal-cost paths for load balancing.

Scalability

Router memory consumption is the main challenge in scalability of routing. We can use route summarization and stub areas to reduce the memory usage and database size. Stub area is a network area with set of routers which we do not allow to advertise about external routers. Which mean this area have no idea about external routes and always need to route over an area border router to reach to an external destination.

Minimizing the network area, number of links and routing summarization helps our protocol to scale into a large network. We design our protocol to send small hello packets and link state updates when a network change happens. When considering the network bandwidth utilization this is a great chance to reduce the bandwidth usage, it is low comparatively to the distance vector routing protocols.

Security

Security is a really important characteristic in every system. Since network protocol defines the communication mechanism of the network, it is really important to have a security mechanism to avoid vulnerability. If no security implemented in the routing protocol, a middle man may modify packets and change destinations to his own router, so all the data will be routed to his router. Or he may modify packets and make the network malfunction, so the network owner may not be able proceed with his task. We selected two authentication types to enable security within our routing protocol.

Simple password authentication

This is a 64-bit value and need to configure for the network. Then this value must have in header of all routing packets. To detect data corruption the entire content of routing packet except the 64-bit authentication field will be checksummed. When having stub areas, routers need to configure for connected networks in order to start with routing. But this simple password authentication is not strong to deal with all aspects, this is vulnerable in some scenarios like when the attacker got physical access to the network.

Cryptographic authentication

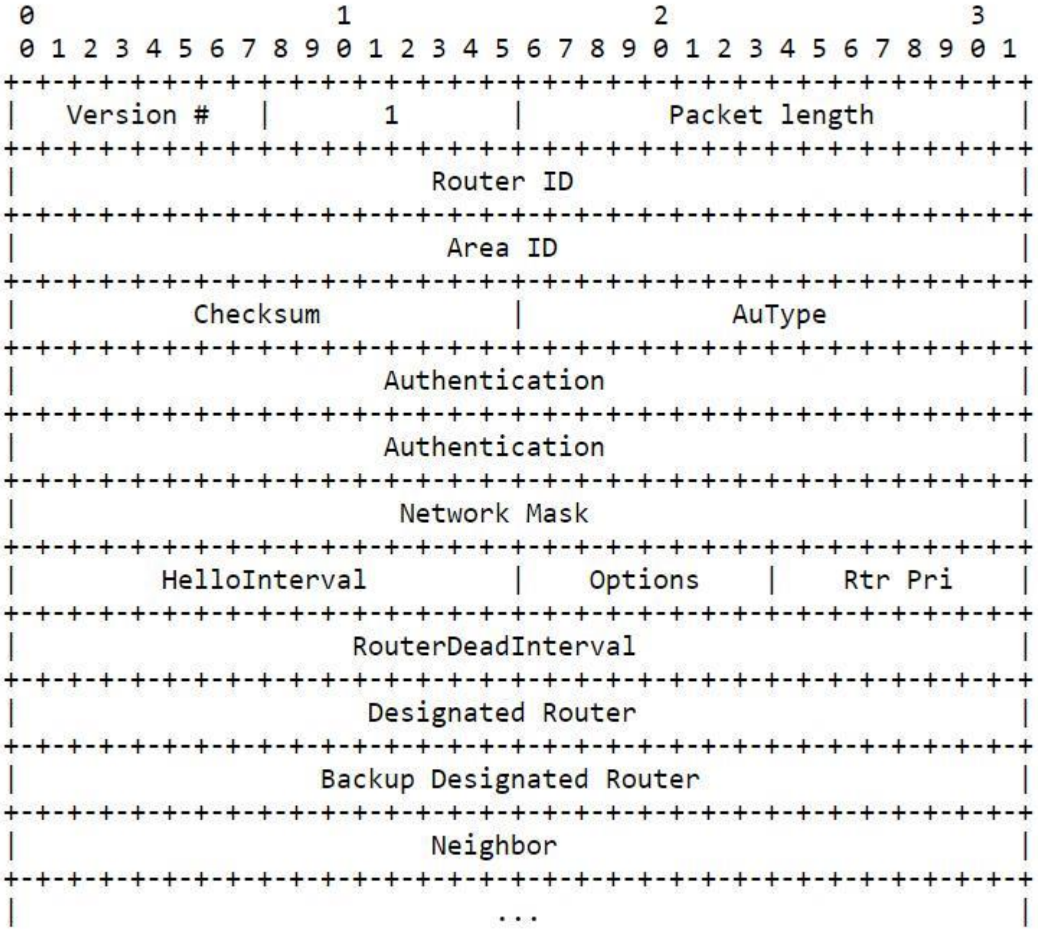
In this method we have to configure a shared secret key in all routers of the network. When sending routing packets, this key will use to generate the message digest and it will append at the end of the packet. And also, this shared key will use to verify the message digest. There is a protection against passive attacks because we do not send the secret key over the network.

Packets

Network packet is a structured data unit which is unique for the network protocol. It contains authentication data, request source, request destination and this may vary based on the protocol. The proposed protocol has 05 types of network packets as described below.

Hello packet

The main purpose of hello packet is to maintain relationships with neighbors. In order to become neighbors after exchanging hello packets, routers should agree on network mask, hello interval and router dead interval parameters. These parameters are available on hello packets and if any router send mismatched hello packets, it cannot join as a neighbor.



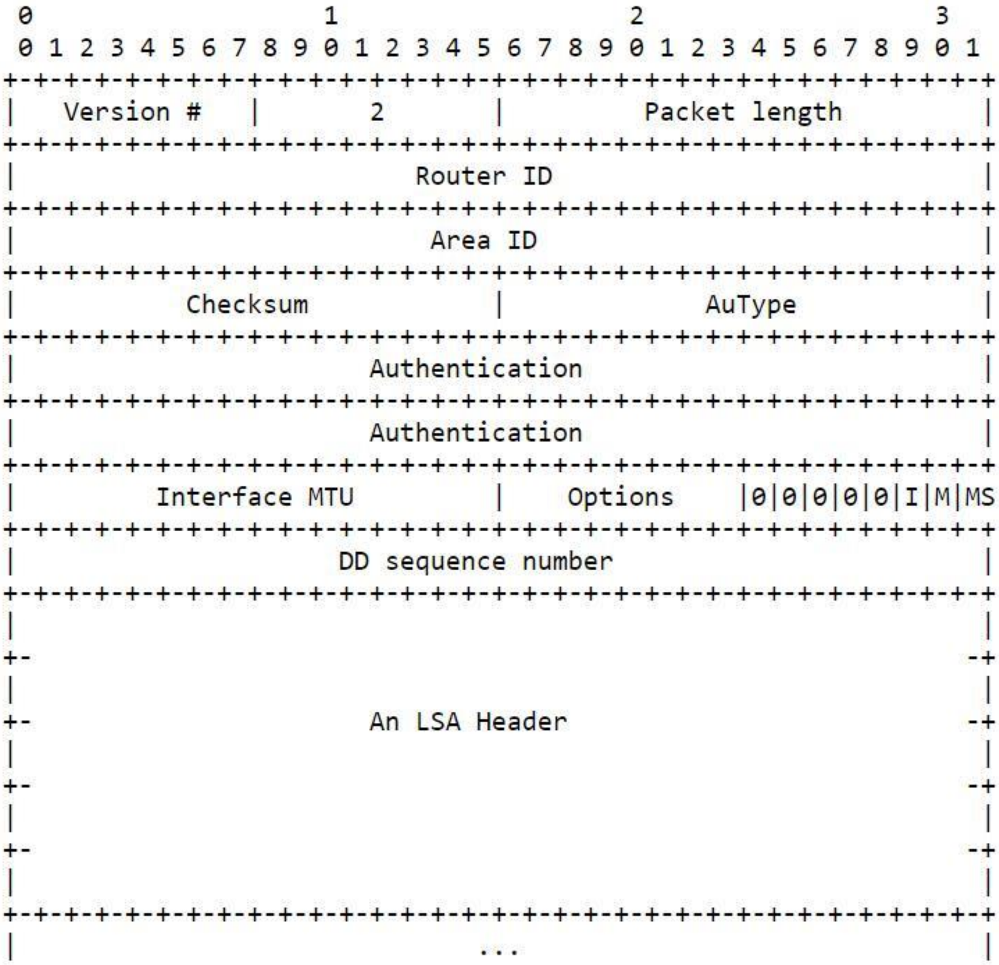
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Version #   |       1       |         Packet length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Router ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Area ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |             AuType            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Network Mask                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         HelloInterval         |    Options    |    Rtr Pri    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     RouterDeadInterval                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Designated Router                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Backup Designated Router                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Neighbor                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
```

Figure 2: Hello packet structure: Source - https://tools.ietf.org

- Network mask - The network mask of the interface.
- Hello interval - The delay between two hello packets of this router. The delay unit is seconds.
- Router dead interval - Timeout to decide on a dead router if no hello packet received. This interval is in seconds.
- Neighbor - Ids of alive neighbor routers of the network.

Database description packet

To maintain the adjacency in the network, database synchronization is really important. This can achieve using the exchange database protocol. This protocol helps with database synchronization by sending database description packet. Database description packet contains content of the link state database and also sequence of packets may use during the synchronization. Below is the database description packet structure.

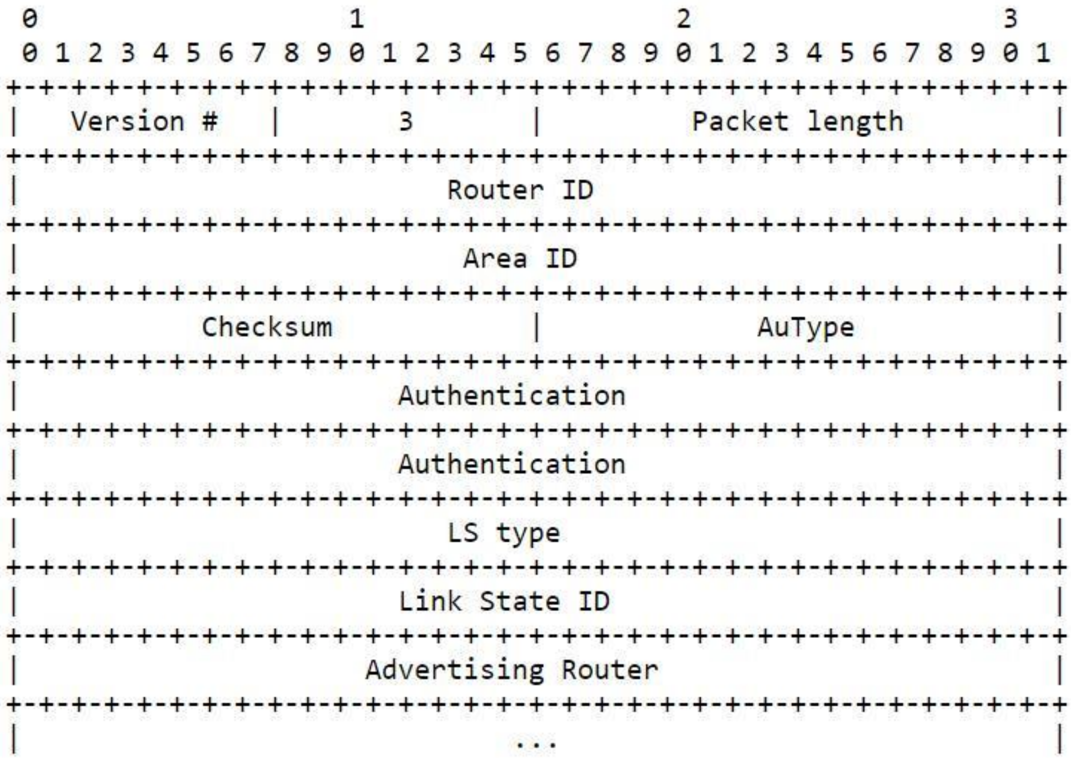


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Version #   |       2       |         Packet length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Router ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Area ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |             AuType            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Interface MTU         |    Options    |0|0|0|0|0|I|M|MS
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     DD sequence number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-                                                             -+
|                                                               |
+-                      An LSA Header                          -+
|                                                               |
+-                                                             -+
|                                                               |
+-                                                             -+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
```

Figure 3: Database description packet structure: Source - https://tools.ietf.org

Link state request packet

This packet type is to request information from neighbor router database which are more up to date comparatively to the sender's database.

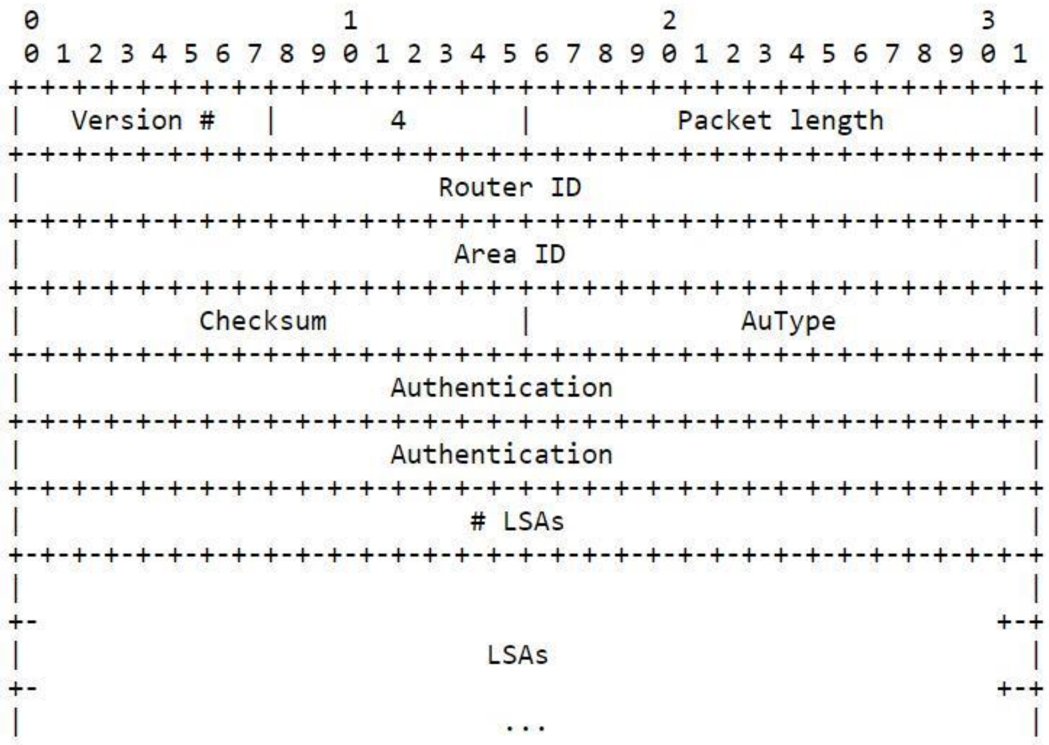


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Version #   |       3       |         Packet length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Router ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Area ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |             AuType            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          LS type                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Link State ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Advertising Router                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
```

Figure 4: Link state request packet structure: Source - https://tools.ietf.org

Link state update packet

This packet type is to implement the LSA flooding. Link state update packet may contain a list of LSAs and it brings LSAs one hop beyond from their origin.

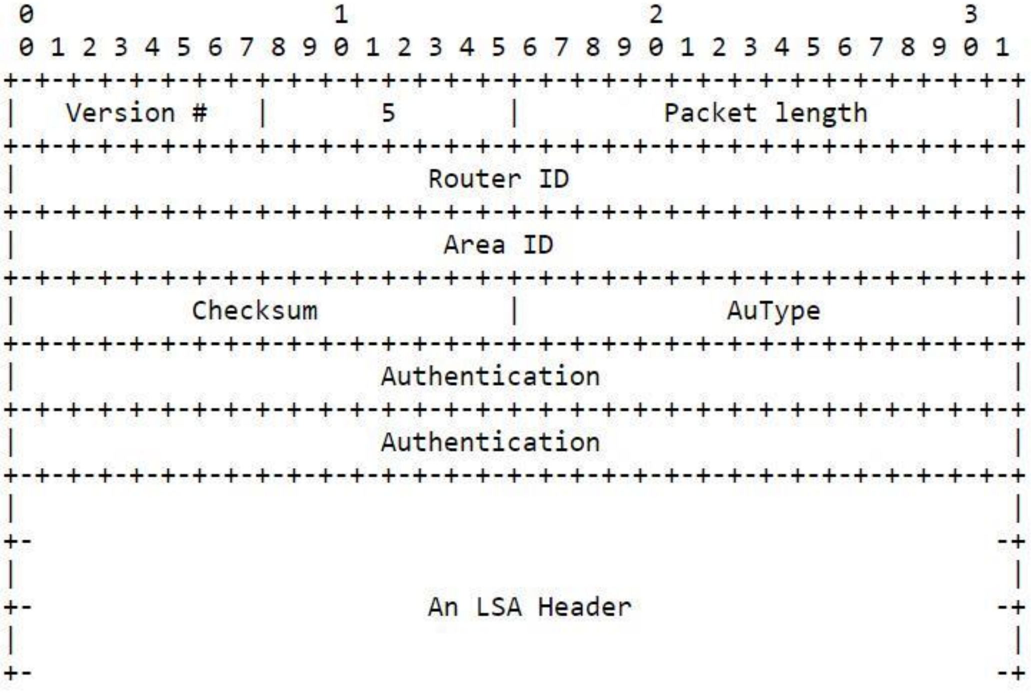


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Version #   |       4       |         Packet length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Router ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Area ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |             AuType            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            # LSAs                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-                                                            +-+
|                             LSAs                              |
+-                                                            +-+
|                              ...                              |
```

Figure 5: Link state update packet structure: Source - https://tools.ietf.org

Link state acknowledgement packet

The link state acknowledgment packet type is to enable the acknowledgement mechanism for flooded LSAs. This makes the flooding procedure more reliable and flooded LSAs may explicitly acknowledged. A single acknowledgment packet can acknowledge multiple flooded LSAs.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Version #   |       5       |         Packet length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Router ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Area ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |             AuType            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-                                                             -+
|                                                               |
+-                         An LSA Header                       -+
|                                                               |
+-                                                             -+
```

Figure 6: Link state acknowledgment packet structure: Source - https://tools.ietf.org

Neighbor table

This table contains all information of adjacent neighbor routers.

Topology table

This table stores topology structure of the network.

Routing table

The routing table stores information which requires to send a data packet to the destination. Each routing table entry contains best paths to the relevant destination.

Find the best path

In link state routing we use the shortest path as the best path. There are many algorithms to find the shortest path. In the OSPF protocol uses Dijkstra’s algorithm. For the proposed routing protocol will use the Floyd–Warshall algorithm. The main reason to select that over the Dijkstra’s algorithm is, Floyd-Warshall algorithm can implement in distributed systems.

In current routing protocols, routers should calculate the shortest path by them self. In this case some routers may get a heavy load while others get a low load based on the usage and the traffic distribution. If we implement the shortest path calculation in distributed way, we may use routers with low usage to calculate the best path on behalf of high usage routers. This may help to increase the scalability and performance in large complex networks.

While the Dijkstra’s algorithm finds the shortest path from a single-source to all nodes, the Floyd-Warshall algorithm is capable of finding the shortest path between any node-pair. Following is the formula of Floyd-Warshall algorithm.

$$D_{ij}^{n} = \min(D_{ij}^{n-1}, D_{ik}^{n-1} + D_{kj}^{n-1})$$

To find the cost between adjacent routers of Link state routing protocol uses following formula.

$$Cost\ =\ Reference\ bandwidth\ /\ Interface\ bandwidth$$

The cost between adjacent routers may use as distance values for the Floyd-Warshall algorithm.

References

[1] John Moy. (1998, April). *OSPF Version 2* [Online]. Available: https://tools.ietf.org/html/rfc2328

[2] *Networking, Routers and Routing* [Online]. Available: http://units.folder101.com/cisco/sem2/Notes/ch6-routing/routing.htm

[3] *Cisco Networking Academy's Introduction to Routing Dynamically* [Online]. Available: http://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7

[4] Jieyun (Jessica) Yu. (2000, July). *Scalable Routing Design Principles* [Online]. Available: https://tools.ietf.org/html/rfc2791

[5] *Cisco Router Handbook* [Online]. Available: http://ods.com.ua/win/eng/net-tech/CiscoRouterHandbook/chap04.phtml

[6] Donnie V. Savage, James Ng, Steven Moore, Donald Slice, Peter Paluch, Russ White. (2016, May). *Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)* [Online]. Available: https://tools.ietf.org/html/rfc7868

[7] *Floyd-Warshall algorithm*. [Online]. Available: http://www.programming-algorithms.net/article/45708/Floyd-Warshall-algorithm

[8] *Comparison of Dijkstra's and Floyd–Warshall algorithms* [Online]. Available: https://www.geeksforgeeks.org/comparison-dijkstras-floyd-warshall-algorithms/