Anatomy of Routing and Routing Loops with the IP Backbone

Meshal Alnasheet
The Higher Institute of Telecommunication and Navigation
PAAET
Kuwait
send4meshal@hotmail.com

Abdulrahman Al-kandari
Department of Computer, Basic Education College
PAAET
Kuwait
aam.alkandari@paaet.edu.kw

***Abstract*-- This paper discussed what is routing, how it works, and how routing function protocols. What will be discussed are the types of protocols and their main characteristics. Then the conflicts of the routing state and how it occurs will be examined, given that such conflicts cause problems for routing loops. Some of protocols that solve this issue will also be elucidate. The discussion in this paper covers only routing, routing protocols, and routing loops within an IP backbone. Also, this paper discussed the causes routing loops in the IP backbone and how can be minimized.**

***Index Term*— Routing, Routing Protocol, Distance vector Protocols, Link state Protocols, Routing Loops.**

I. Introduction

A router is a Layer 3 device which operates on a network layer and connects two or more networks [1]. Each router has a routing table which represents the different routes the signal (data) may take between computers.

The conventions which manage the network devices when they communicate with each other are called 'network protocols'. Those protocols which work between routers are called 'routing protocols'. A routing protocol is a component of a network layer protocol; it gives information that lets routers select the best routes between two nodes on a network. There are three major types of routing protocols; we will discuss two of them with further details and will explain their main characteristics through some famous examples.

Even the best of these protocols have some points of weakness. This makes the most engineered network suffer from errors during the transmission of data. The errors which occur as a result of inconsistency in the routing state are called 'routing loops'. This may lead to data packet loss, which means the data will be resent again and takes more transmitting time. Some of the primary causes of routing loops will be discussed in this paper [1].

The data routes and network devices are combined to form what is called a 'network backbone', while the Internet Protocol works as an essential part of any large network, called the 'IP backbone'. Any internet service provider (ISP) may be considered as a separate IP backbone. ISPs are always trying to introduce high speed connections, more availability, and less connection errors to their customers. So the best engineering available for IP backbones guarantees [2].

II. Routing

Routing concerns selecting the best network paths and is applied to many kinds of networks, including data networks (the Internet) and the telephone network. In packet switching networks, the intermediate nodes are routers. Routers make use of routing tables which contains a record of the different network destinations. That makes constructing routing tables a very important for efficient routing.

There are two main types of routing algorithms:

- *Static Routing*: uses routing tables configured manually (this type may be used in small networks).
- *Adaptive or Dynamic Routing*: used in larger networks and constructs routing tables without human intervention, using information received from routing protocols, which allows the network to act nearly automatic in avoiding network problems and failures. Examples of this algorithm are RIP and OSPF protocols.

However, networks have not been developed yet to the point of being completely autonomous [2].

III. Routing Protocols

Protocols used by routers working on the IP backbone can be divided into major classes depending on their algorithms, as shown in Figure 1.

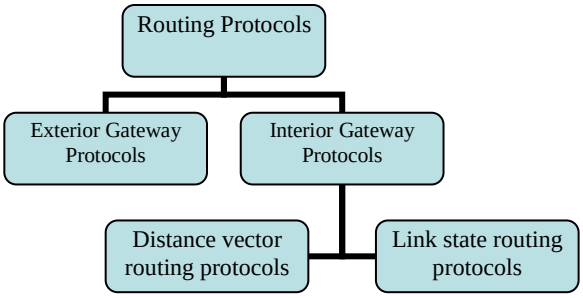

Fig. 1. Routing Protocols Classes

Exterior gateway protocols contain two protocols: Exterior Gateway (EGP) and Border Gateway (BGP). These protocols use a path vector routing algorithm, and are applied on the Internet for exchanging traffic between Autonomous Systems. [2]

We will discuss the main two classes of Interior Gateway Protocols (IGP), which are Distance Vector Protocols and Link State Protocols [3].

A. Distance Vector Protocols

The distance vector refers to the arrays (vectors) of distances to other nodes stored in the node. The algorithms of theses protocols assign a number to each link between nodes in the network. Nodes will send information from router A to router B based on the lowest total number path. When any node starts for the first time, only two pieces of information will be stored in its routing table; adjacent neighbors and the direct costs to reach them. Figure 2 shows adjacent nodes and links between them. Each link has a number beside it. The numbers refer to the cost needed to transmit data between two nodes.

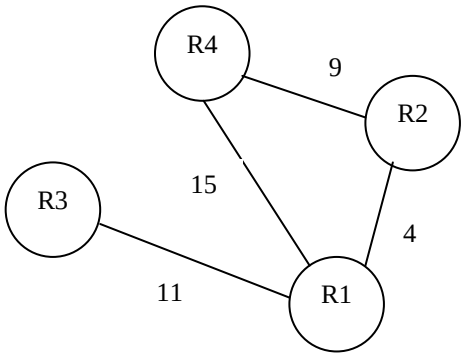

Fig. 2. Routing nodes

Normatively, the calculation of the total costs to all nodes is sent from each node to its neighbors. After receiving this information, the neighboring nodes compare it to what they already have; any improvements then will be inserted in their own routing tables. When one node goes down, other nodes discard the entry and build a new routing table. These nodes transfer the updated information to all their neighbors, which in turn repeat the process until all nodes in the network receive the updates and find new hops to all the destinations they can still reach. Over time, all the nodes will discover the best total costs and hops for all destinations.

Distance Vector Protocols have less computational complexity and message overhead than Link State Protocols, because the former requires each router to periodically tell its neighbors about any changes in the pathways. RIPv1, RIPv2 and IGRP are famous examples of Distance Vector Protocols.

Routers using a Distance Vector Protocol within the IP backbone do not know the entire path to a destination; it only calculates the distance and direction to any link in a network. The 'distance' is a measure of the cost to reach a certain node. The 'direction' means the next hop address and the exit interface. The best route between two nodes is one with a minimum distance. Each node has a table of the shortest distance to all nodes. Various route metrics are used to calculate the cost of reaching a destination. RIP uses the hop count of the destination [4].

A.1 Routing Information Protocol (RIP)

RIP is one of the oldest Distance Vector Protocols and uses the hop count as a routing metric. There are three versions of the RIP Protocol: RIPv1, RIPv2, and RIPng.

RIP defines the Request Message and Response Message. When an IP backbone router runs, the RIP protocol comes up and sends a broadcast Request Message (through all its enabled interfaces). The Response Message(s) containing routing tables then come back from all the adjacent routers which receive the Request Message. Figure 3 shows the rules for processing each entry of the table by the router.

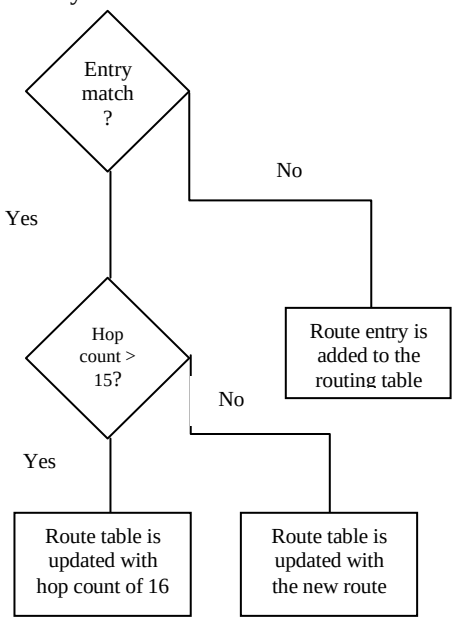

Fig. 3. router entry processing rules

There are some limitation in RIP such as the hop count can't exceed 15, also RIP networks does not have concept of areas and boundaries [4].

A.2 Interior Gateway Routing Protocol (IGRP)

Another Distance Vector Protocol is IGRP. It is a more powerful protocol than RIP. It was eventually replaced by a new design protocol called the Enhanced Interior Gateway Routing Protocol (EIGRP). Both protocols use the same routing metrics [4].

B. Link state Protocols

The other main class of routing protocols used in packet switching networks is the Link State Protocol, where routing tables are built up from the best paths. Every node in a Link State Protocol builds a special map called a 'network connectivity map'. After that, each node mathmatically finds the next best logical path to every destination in the network, which are the paths that make the tables.

The Link State Protocol gives a network's map to every node. When a node receives the link state advertisement, it looks up the sequence number it has stored for the source of that message. If a newer sequence number is detected it will be saved and each node sends a copy of the latest version of its advertisement to other nodes in the network.

In a Link State Protocol, the data passed between routers relates only to its connectivity, while in Distance Vector Protocols, each node shares its routing table with adjacent nodes.

Another advantage of Link State Protocols is the division the hierarchies which limit the scope of route changes. All these features make Link State Protocols better to larger networks.

To considere a correctly reported node, two nodes must agree; if one of the nodes doesn't report that it is connected to the other, then the link is not included on the map and a problem will arise.

Each node runs an algorithm to decide the shortest path from itself to other nodes in the IP backbone. After that, the shortest paths are filled in the routing table. To create the routing table, all one must do is walk the tree, keeping in mind the identity of the next node and putting in an entry for each node that comes across the routing table.

There are two famous Link State Protocols: Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) [5].

B.1 Open Shortest Path First (OSPF)

OSPF was designed for IP and avoids large control packets. The packet in this protocol is called 'LSP'. OSPF avoid large LSPs. Since OSPF needs more storing bits, it should have more bits of bandwidth to send data. It really requires 3 times as much bandwidth to transmit the complete LSP database as IS-IS in the level 2 network. OSPF needs techniques in order for neighbor routers to compare their LSP databases.

In OSPF, the data needed to summarize the LSP database can be huge. OSPF depends on fixed format packets which align the fields. Explicit area repair mechanisms are not supported in OSPF. It uses manually configured virtual link. OSPF has increased bandwidth usage and needs more memory and CPU requirements. It can configure a stub area. Nonstub areas needs more storage than stub areas. OSPF doesn't try to make the best route selection from a stub area to a target outside the AS, but it attempts to find that best route from a stub area to targets within the AS.

OSPF has the capability of using authentication, which is in the form of a simple password. It uses only one password per link. As such, the routers would all have to be brought down to change the password.

OSPF collects clear and precise acknowledgments from all receiving routers. However, this protocol doesn't state any techniques to deal with the overloading of a database. Its implementations prefer either to break down or carry ong work on a part of the information. Sometimes the database becomes larger than what a router was configured [5].

B.2 Intermediate System to Intermediate System (IS-IS)

IS-IS was in the beginning not designed for IP, however, it supports the IP network layer and hierarchical routing. The IS-IS packet is sent out directly on top of the data link layer.

IS-IS avoids large control packets. It uses a packet called a 'Complete Sequence Numbers Packet' (CSNP). In IS-IS, LSPs list all the adjacent nodes around any node. It equires techniques to let neighbors know how to measure up their databases with each other. This is done upon linking and also not so often by the main router on a LAN. The CSNP database is expected to be smaller than the DD in OSPF. Although it is still likely that a CSNP will not fit into a single packet, IS-IS reacts to this problem by taking the beginning and end LSP source addresses and appending them in the CSNP. The variable length is the major characteristic of most fields in IS-IS, which sometimes makes processing slower.

IS-IS has mechanisms to automatically detect and repair the nework partition stricken with a problem such as diconnection or going down temporarily. IS-IS needs a path from all level 2 routers to each other. IS-IS doesn't try to optimize the route from a stub area to a target outside the AS. Some routes to other ASs here will be less favourable than those used in OSPF.

IS-IS has the capability of using authentication. It has only one type of authentication, which is a simple password. The length of authentication data varies. In IS-IS, there is a transmit password as well as a set of received passwords with each router per link. The IS-IS configures new passwords without disrupting the network.

The router that initially created an LSP places the password field into the LSP. In IS-IS the DR on a LAN is the router with the highest configured priority. IS-IS can propagate LSPs throughout the network. With no packets lost, IS-IS needs only one single packet transmission per LSP. IS-IS will always have a constant periodic overhead. The IS-IS protocol will be more efficient with larger numbers of routers on a LAN.

IS-IS always has a way to configure routers while the network is running. There is no need for adjacent nodes to have the same timers' value. In IS-IS, the CSNP exchange is used as an optimization to prevent the need for transmitting all LSPs on the link, thereby reducing traffic in the network [5].

IV. ROUTING LOOPS

Routing loops are a common problem which result in packets stuck in the loop that relocates the link multiple times in the same network. There are three types of loops:

- *Forwarding Loop*: The router forwards a packet and then it comes back again to the same router.
- *Information Loop*: The router acts on connectivity data taken from data gathered earlier.
- *Trace Route Loop*: The measurement reports the same chain of routers many times.

Routing loops happens because of temporary inconsistency or permanent inconsistency. The temporary inconsistency comes up during the process of convergence , and the permanent inconsistency occurs as a result of a wrong configuration or route oscillation.

Routing protocols spread data through the network so that all the network's routers finally have nearly the same view of the network. The main idea of routing loops requires the availability of two routers and a single node or more that separate them. The main reasong for having a routing loop is that the routing data in each router are not synchronized.

Routing loops are of two types: transient and persistent routing loops. It is very hard to study persistent loops because they are so rare. It arises mainly due to bad router configuration, so it requires human intervention. In our discussion here, we will focus on transient loops, which occur due to the variation of delays while transporting data to different parts of the network. Transient loops should be resolved without intervention, as the routers converge.

Let's take a simple example of how a loop can occur. In Figure 4, node X is transforming data to Z via node Y, If the connection between Y and Z is disrupted for any reason and node Y does not inform node X about the disconnected link, then node X will send data to Y assuming that the link (X-Y-Z) is still available. Node Y recognizes there is a broken link between itself and node Z, so it tries to reach Z via node X; in this way the original data is coming back to node X, which then consults its routing table which says that it can reach Z via node Y. Then it will send the data back to node Y, which will continue on forever [6].

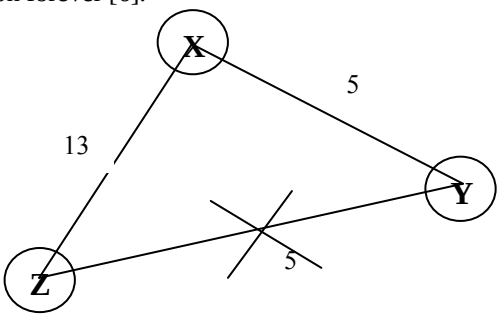

Fig. 4. a simple routing loop

If there are any changes on the topology of the IP network caused by a failure or a modification in link metric, it is needed for the routing table to be updated. Transient loops can happen from those updates. The main problem that most ISPs must solve is fast convergence after failures have occured. Solving this problem is so complicated because it needs to detect the error first, then create a Link State Packet (LSP) which describes the error, declares the LSP to let other routers know about it, and then lastly updates the routing tables in all the routers connected with the error.

In the meantime, detours around the disconnected link are needed to have a very fast convergence in an IP network. In MPLS (Multi-Protocol Label Switching) networks, several solutions have been proposed recently to create those tunnels. In a pure IP network, using protection tunnels is not a complete solution because of micro loops that can happen during updating of the routing tables; the packets that go to the protection tunnels may take the shortest path to its destination so that's why the routers need to update their Forwarding Information Base by taking into account the change in topology of their Standard Penetration Test.

The maximum number of routers that a packet can cross in RIP is 15. The packet is discarded when the value reaches 16 (which is considered infinity). In a Distance Vector Protocol, such as RIP, the error will continue until the metrics for Z becomes infinite.

To prevent routing loops, RIP limits the maximum number of hops permitted between source and destination to 15, which also limits the networks' size that RIP can bear. The value 16 is considered an unreachable route.

In order to stop incorrect routing information from being transmitted, RIP implements 3 mechanisms: 'hold down', 'route poisoning', and 'split horizon'.

To handle the "count to infinity" problem, we can also use the RIP with a Metric-Based Topology (RMTI) algorithm [7].

We can discuss the "count to infinity" problem like this: if node L tells node M that it has a path, M can't know if the path has M as part of it or not. To clarify this issue, imagine a sub-network contains 3 nodes connected in this order (L–M–N), and let us take the "number of jumps" metric, which is the nodes between the routers. Now let us suppose that L went offline. When the process to update the vector (array) occurs, M notices that the route to L is disconnected. M does not receive any new information from L. The problem is, M also receives new information from N, which also is not aware of the fact that L is disconnected, so it tells M that L is only two jumps away, which is not true. This continues slowly through the sub-network until it exceeds the value of 15.

With RMTI, to detect every possible loop, all RIP needs is a small calculation. Initially, the RIP router transmits new data about its state every 30 seconds. In the early days, routing tables were small but the traffic was light. As networks got bigger and bigger, there could be a huge traffic rupture every 30 seconds, even if the routers had been given initial values randomly. Due to random initialization, the new data would be broadcasted on time, but practically this was not the case.

In current IP backbones, RIP is not the best choice for routing because of poor convergence time and scalability compared to EIGRP. However, RIP does not require any parameters unlike other protocols, which makes it's configuration process very easy.

While RIP is seen as a helpful solution for small indistinguishable networks, the transmission of the entire routing table every 30 seconds may put a serious amount of extra traffic in larger, more complicated networks.

To decrease the possibility of forming loops and using a max number of hops to reverse the 'count-to-infinity' problem, RIP uses the split horizon with poison reverse techniques. These measures may sometimes avoid loops from happening. However, this causes a considerable raise in convergence times.

Recently, engineers have developed a number of Distance Vector Protocols that prevent routing loops from happening in all cases, and the most famous examples of these protocols are EIGRP, DSDV and Babel. However, the main disadvantage of these protocols is the bigger complexity, and their use has been held up by the huge success of Link State Protocols such as OSPF [7].

The detection link failure time, the flood new topology data time, and the shortest path recalculation time, are three factors that have direct effects on convergence times of Link State Protocols (OSPF and IS-IS). Several factors affect these times: damping algorithms used to avoid false updates, the diameter of the network, and the way that the shortest path algorithm is implemented. See Figure 5.

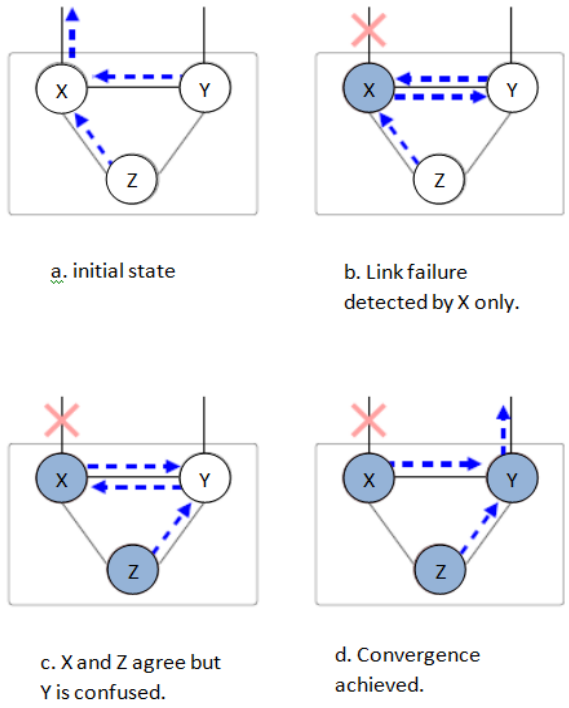

Fig. 5. A transient routing loop scenario.

Figure 5 shows that node X links all three nodes with the outer world. When a disconnection happens in that link, node X is the first node that will recognize it. Traffic must now pass via Y to the outer world, but until Y knows about the disconnection of X, other nodes (Y and Z) will continue to pass traffic to X. But because X knows about its own problem and also knows that there is an alternative route via Y, it will return this traffic back to Y, which results in looping the traffic as Figure 5 (b) shows.

Figure 5 (c) shows that the corrected data has reached Z before Y, which results in making Z send traffic to other networks via Y instead of X. Lastly, Y receives the information about the disconnection of X, so it stops sending traffic to other networks via X and uses its own connection. Figure 5 (d) shows how the loop has stopped.

In a study to detect and analyze routing loops in Packet traces [3], routing loops make a duplicate of the packet, the purpose of which is to cross a specific point in the loop. A set of duplicates are called a 'duplicate stream' and it is used to detect routing loops by three algorithm steps: Detect duplicates, Validate duplicate streams, and Merge them into routing loops.

This study found that performance can be severely affected by routing loops and could be responsible for up to 90% of packet loops. Routing loops increase delay time for packet transmitting as well. Those delayed packets may also be delivered with problems in their original order.

V. Conclusion

In this paper, we discussed router, their primary main objective, and how do they work. There are two types of routing: static and dynamic routing. Then we discussed the routing protocols within routers. There are many types of these protocols. The main two classes are IGP and EGP. IGP Protocols have two main algorithms: Link State (such as OSPF and IS-IS protocols) algorithms and Distant Vector algorithms (such as RIP). Both algorithms have many protocols designated to perform routing within the IP backbone. Each one of these protocols has points of strengths and points of weakness.

We showed also the main characteristics for each of the RIP, OSPF and IS-IS routing Protocols. Then we talked about routing loops, which happened due to an inconsistency in the routing state among a set of routers. This problem may lead to a loss of data packets, which increases the transmitting time to send those lost packets again. Each protocol type has its own algorithms to deal with routing loops. We talked briefly about a study on routing loops and some of its findings.

Finally, we concluded that the Link State Routing Protocols (OSPF and IS-IS) have better algorithms, techniques, and design than Vector Distance Protocols (especially RIP) to deal with routing loops and eliminate them from the IP backbone, even preventing them from happening. Newer versions of RIP solve its predecessor's weakness points.

References

[1] Christensson, P. (2006). *Router Definition*. Retrieved 2015, Sept 15, from

[2] P. Francois and O. Bonaventure, "Avoiding transient loops during IGP convergence in IP networks," *IEEE INFOCOM 2005: The Conference on Computer Communications, Vols 1-4, Proceedings*, pp. 237-247, 2005.

[3] M. Enachescu, Y. Ganjali, A. Goel, N. McKeown, and T. Roughgarden, "Part III: Routers with very small buffers," Computer Communication Review, vol. 35, pp. 83-89, Jul 2005.

[4] V. Paxson, "End-to-end routing behavior in the Internet," IEEE/ACM Transactions on Networking, vol. 5, pp. 601-615, 1997.

[5] R. Perlman, "A Comparison Between Two Routing Protocols: OSPF and IS-IS", *IEEE Magazine*, Sep 1991.

[6] Medhi, Deepankar and Ramasamy, Karthikeyan (2007). *Network Routing: Algorithms, Protocols, and Architectures*..Pierre Francois, Olivier Bonaventure," Avoiding transient loops during IGP convergence in IP networks".

[7] G. Appenzeller, I. Keslassy, and N. McKeown, "Sizing router buffers," Computer Communication Review, vol. 34, pp. 281-292, Oct 2004.