Improving Network Performance by Implementing the Path Control Tools

Derick Kolle Nduge, Augustine Chika, Mohammednur Ibrahim

Network Project 2013   7.5 hp

10 01 2014
Improving Network Performance by Implementing the Path Control Tools

Network Project DK2002

2013

Author: Derick Kolle Nduge
Augustine Chika
Mohammednur Ibrahim

Supervisor: Malin Bornhager
Examiner: Olga Torstensson

School of Information Science, Computer and Electrical Engineering
Halmstad University
PO Box 823, SE-301 18 HALMSTAD
Sweden
Improving Network Performance by Implementing the Path Control Tools
Derick Kolle Nduge
Mohammednur Ibrahim
Augustine Chika

© Copyright Derick Kolle, Mohammednur Ibrahim and Augustine Chika
2013. All rights reserved.

Network Project report IDE DK2002
School of Information Science, Computer and Electrical Engineering
Halmstad University
Preface

This project has increased our knowledge about ROUTE REDISTRIBUTION issues and most importantly a better understanding on how to use ROUTE MAPS for manipulating routing updates. We are so grateful for this wonderful experience given to us during our time at the university. We would like to express our special thanks of gratitude to our supervisors Malin Bornhager, Olga Torstensson, for all the help we got from them throughout the project.
Abstract

Designing an IP network requires a deep knowledge of both infrastructures, and the performance of the devices that are used. At the same time how packets are handled by the devices. In networking infrastructure where there are multiple branches with lots of redistribution points, performance is very important thing that a network designer should consider. A company can have different branches, where those branches use different routing protocols. Branches of the same company should communicate with each other. The existence of multiple routing protocols in different branches will require redistributing those protocols so that, routes from one routing protocol can be advertised in to another routing protocol.

The main issues, which can affect the performance of a network, are the results of improper redistribution. These issues, which affect the network performance, are excessive routing updates, suboptimal routing and routing loop, which can lead to network downtime.

This thesis discusses the issues of network performance. It explains how to overcome these issues using different path control tools. The authors of this thesis decided to present some of the network performance issues and also give a solution to the issues discussed earlier.
## Contents

Preface ......................................................................................................................... ii

Abstract ....................................................................................................................... iii

1 Introduction ............................................................................................................... 7

1.1 Goals .................................................................................................................... 8
1.2 Method ................................................................................................................. 8

2 Network performance issues and Tools ................................................................. 9

2.1 Excessive Routing Updates ................................................................................. 9
2.2 Route Redistribution .......................................................................................... 10
   2.2.1 Routing Feedbacks or Loops ......................................................................... 10
   2.2.2 Incompatible Routing Information .................................................................. 10
   2.2.3 Inconsistencies in Convergence Time ............................................................. 11
2.3 Redundant Paths ................................................................................................. 11
2.4 Load Sharing ....................................................................................................... 11
2.5 Path Control Tools ............................................................................................. 11
   2.5.1 Policy-based routing ...................................................................................... 12
   2.5.2 Administrative Distance .............................................................................. 13
   2.5.3 IOS IP SLA ................................................................................................. 13
   2.5.4 Offset-list .................................................................................................... 15

3 Experiments ............................................................................................................. 19

3.1 Design Network topology .................................................................................. 19
3.2 Suboptimal routing and routing loops ............................................................... 21
3.3 load sharing problem ......................................................................................... 23

4 Results and analysis ............................................................................................... 27

4.1 Suboptimal routing and routing loops solution .................................................. 28
4.2 Load Sharing solution ......................................................................................... 30

Conclusion .................................................................................................................. 37

Bibliography ............................................................................................................... 38
Chapter 1

1 Introduction

Network performance is an important aspect that every enterprise should put into consideration when designing a network. There are many reasons for a network to have performance issues. Most of the network performance issues in this project are routing related issues and they can be avoided by implementing the path control tools. These path control tools are very important tools, which help a network administrator to have full control of the network by controlling or directing traffic to take different paths in case problems do arise. Companies and business organizations are making big investments in their network to improve the performance.

So far, we have identified some possible issues that could reduce the network performance. They include;

- Excessive routing updates; Excessive routing update and size of the updates (depends on the routing protocol used), presence of any route maps or filters and number of routing protocols running in the same autonomous system can decrease network performance [1].
- Route redistribution; It is a powerful tool which adds complexity to the network which therefore increases the potentials for routing confusion [1].
- Availability of redundant paths
- Loadsharing.

These issues can exit in a real enterprise networks like an air plane ticket office, where branch offices should update how much and what tickets do they sell and might fail to do so. Also in companies, where customers look for some products in one branch of the company, and if that product is not available in this branch and might failed to search it in another branch. This can be solved by implementing the path control tools. The network performance issues will be explained later in this paper and also how they do come about.

The path control tools are used to help eliminate network performance issues mentioned above. There are many path control tools that can be implemented. But, we focused on the advanced path control tools. The tools identified include: the Policy-Based Routing PBR, AD, Passive Interface, Offset List and Cisco IOS IP Service Level Agreements SLA. Our project idea is based on these tools, which are used to solve network performance issues. In the following chapters, we will give a brief description of the tools and how they are used in a network to affect the path that traffic travel through the network. But we will begin by thoroughly explaining network performance issues.
1.1 Project goals

The main Goal of our study is to improve the network performance by controlling the path that traffic will travel using the path control tools. Our goals where achieved by:

(1) Improving network performance using the path controls tools to optimize the network.
(2) Comparing our results to show that we have truly improved network performance. We can achieve this by comparing the results before and after applying the path control tools.

1.2 Method

The method used includes the theoretical and practical experiment. Here, we will theoretically and practically implement the path control tools to help us improve network performance. The next step is associating and applying these tools to their respective issues we mention in the introduction to fully optimize the network performance.
Chapter 2

2 Network Performance Issues and Tools

Network performance is fundamental to every single enterprise and these enterprises would want their network to be stable in order to satisfy the needs of their customers. There are so many reasons as to why network performance can be reduced. The issues addressed are routing related problems, which include:

- Excessive routing updates
- Multiple routing protocols running on the network (Route redistribution)
- Redundant paths
- Loadsharing

2.1 Excessive routing updates

Excessive routing updates can greatly reduce network performance. The size of the routing updates is fully dependent on the routing protocol in use, the frequency of the updates and the design of the network such as IP addressing plan and the use of summarization can affect the network performance. [1] Excessive routing updates can be controlled by applying the passive interface command to an interface, which prevents a routing protocol’s routing updates from being sent out the specified interface.

Passive interface command with RIP and IGRP, routing updates are not sent out of the specified interface but, however, routers still receive routing updates on that interface. With EIGRP hello messages are not sent out of that specified interface and therefore no neighboring relationship is achieved with other routers because hello messages are used to communicate between routers. And lastly, with OSPF, passive interface command will prevent routers from establishing adjacencies with neighboring routers connected to that interface. [1]
2.2 Multiple routing Protocols running on the network (Route redistribution)

Multiple routing protocols can be configured on a single router to connect remote networks that use different routing protocols or routing domains. This can be achieved with the help of route redistribution. For example, we can exchange and advertise routing information between OSPF running in one domain, EIGRP in another domain and BGP routes if the single router is connected to an ISP. [1] During route redistribution, a lot of problems might arise if it is not properly controlled. [2] The problems that arise when redistributing includes the following:

- Routing feedbacks or loops
- Incompatible routing information
- Inconsistences in convergence time

2.2.1 Routing feedbacks or loops

A routing loop will occur when more than one boundary router is participating in route redistribution. Routers might send routing information received from one routing domain back into that same routing domain. Thus reducing the network performance.

Routing feedbacks or loops occurs when we redistribute between the same protocols in different domains or different protocols in different domains. For example, we can redistribute two OSPF processes in different domains and or redistributing between EIGRP and RIP in different domains. This will be explained in the implementation section on how they occur. [1]

2.2.2 Incompatible routing information

Each routing protocol uses different metrics to determine the best path to a destination. Because of this difference, routers will forward packets using a suboptimal path and this phenomenon is called suboptimal routing which reducing the network performance. When this occurs, routers will forward packets based on the administration distance of the routing protocol in use. For example, when we redistribute between OSPF in to EIGRP, routers will forward packets using the protocol with the lowest AD. In this case, the OSPF routes will be preferred over EIGRP routes because the AD in OSPF is lower than the AD in EIGRP. This will create routing feedbacks or loops in the network. This will be explained in details in the implementation section where we will use one of the path control tools to solve...
the problem. In this problem we will use the policy-based routing and or changing the AD to affect the path that traffic takes in the network.[1]

2.2.3 Inconsistencies in convergence time

Different routing protocol converges at different rates. For example RIP will converge slower than EIGRP.

2.3 Redundant paths

Redundancy provides multiple paths for packets to travel to a destination. If the administrator configures redundancy properly, users will hardly notice any problem or failure because packets travel through the right path. But what we do not see is that redundancy can become a problem if not configured properly. In a switch environment, redundancy can cause layer 2 loops which interns cause broadcast storms and duplicates unicast frames in the network. This can be fixed using Spanning Tree Protocol (STP). With routers running multi routing protocols and where there exist multiple paths, the network administrator should decide where to direct the traffic in order to avoid suboptimal routing and routing loops or feedback. [1]

2.4 Load sharing

Load sharing is the distribution of network updates or packet in different paths. A network manager can implement policies to distribute traffic among multiple paths based on the traffic characteristics.[1] We can implement load sharing when dual-homed into one ISP through multiple local routers. In this situation, we can have load sharing in multiple connections. The problem arises when a link from one ISP to the router fails. We will then use the path control tool to overcome this failure.

2.5 Path Control Tools

The tools presented below are used by an administrator to control the path that traffic takes through the network. These tools can be used to solve redistribution issues, controlling routing updates, redundant paths and so on.
2.5.1 Policy-Based Routing

Policy based routing PBR, is an advanced path control tool, which uses route maps to filter traffic. Router usually forwards packets to destination based on the information in their routing tables i.e. destination based routing. PBR, offers flexibility by giving the network administrator the ability to route traffic to take different paths based on source and destination addresses, protocol type, or application type i.e. source based destination. Thus overriding the router’s normal behavior. PBR provides an extremely powerful, simple, and flexible tool to implement solutions in case where legal, contractual or political constraints dictate that traffic be routed through specific paths. [4]

Policy-based routing offers significant benefits when trying to control traffic in a network. The benefits of using PBR will include: (1) source-based transit provider selection - where different users take different paths to forward packets, (2) QoS – differentiate traffic by setting the Type of Service (ToS) in the IP header and then use queuing to prioritize traffic in the network, (3) cost savings. Organizations can greatly reduced cost by routing non-interactive traffic across lower speed links and vice versa, (4) load sharing – distribute traffic between paths based on the traffic types.[4]

Configuring PBR using route-map

The first thing to do is to configure a route-map with is one the several methods of PBR ,by matching and setting commands and then applying the route map to the interface. The PBR is applied to incoming packets, for which the match commands are used to match the incoming packets and the set commands are used to change the default destination-based routing.

These steps below show how to configure and verify PBR for path control. The steps include:

- Define and name the route map with the route-map command.
  - Define the conditions for the match commands
  - Define the action for matched traffic using the set commands.
- Enable fast-switched PBR or Cisco Express Forwarding i.e. switched PBR (optional)
- Define the interface the route map will be attached to using the IP policy route-map interface configuration command.
  - Applying PBR to incoming traffic or to traffic generated by the router.
- Verify PBR configuration using show commands.

The route map statement can be configured either as permit or deny. If the statement is marked as deny, packets meeting the matched criteria is not policy-based routed meaning the packets is not dropped and thus is sent through the normal routing process. But if you decide that you want to drop the packets because they do not match the specified criteria, configure a set statement to route the packets to interface null 0 as a last entry in the route-map.

If the statement is marked as permit and the packets matches all the criteria, packets will be policy-based routed. [4]
2.5.2 Administrative Distance

The administrative distance is the trustworthiness of multiple sources of routing information running at the same time. That is each routing protocol is prioritized in the order of most believability to least believability. [5] When redistributing identical IP route between two different methods of resolving the best path, important information may be lost such as the relative metric of the route making route selection to be confusing at times. In some cases, routers will select a suboptimal path by believing a routing protocol that actually has a poorer route. This situation will create routing loops, which will cause the network to be unstable. This problem can be resolve by assigning a higher AD to routes from the undesired routing protocol since routes with lower AD is preferred over higher AD. This will be fully explained and implemented in our results in chapter. Also, depending on the routing protocol configured. For example, RIP uses hop count as its metric. That is RIP will choose a best path based on hop count. Lowest being preferred. With OSPF, the default metric is bandwidth and cost, which is, use to select the best path and with EIGRP, bandwidth and delay is use as a default metric in choosing the best path.[5]

2.5.3 IOS IP Service Level Agreement (SLA)

This section describes how IOS IP SLA uses the path control. Cisco IP IOS SLA is an embedded tool on the IOS, which uses active monitoring to generate traffic continuously to measure network performance. The IOS IP SLA send simulated packets to measure performance across multiple network locations or multiple path networks. The information collected is packet loss, jitter, response time, and availability on a network. We can use the IP SLA for performance monitoring application such as Internet Performance monitoring (IPM) because it is accessible by SNMP (simple network management protocol).

Advantages of IOS IP Service Level Agreement (SLA)

- IP SLA monitoring
  - Provides service level agreements monitoring, measurement and verification
- Network performance monitoring
  - Measure the jitter, latency, or packet loss in a network
  - Provides reliable, continuous and predictable measuring
Improving Network performance by implementing the path control tools

- Edge-to-edge network availability
- Troubleshooting of network operation. It helps the fault of the network and saves the troubleshooting time
- Voice over IP (VOIP) performance monitoring
- (MPLS) and (MPLS) performance monitoring and verification

**Network Performance Measuring Using Cisco IP SLA**

With the help of IP SLA, a network engineer can monitor the performance between any area in the network i.e. core, distribution, and edge. Monitoring can be done from anywhere without deploying a physical probe. The IP SLA probe is an application-ware by which we can measure the network response time. IP SLA generates traffic to measure the performance of network or between two networking devices. That is a device sends a generated packet to destination device. After the destination device receives the packet, and depending on the IP SLA operation the device will respond with time-stamp information for the source to make the calculation on metrics. The IP SLA uses special protocols such as UDP to measure the network from source to destination. And this is done via sources and responders.

**Cisco IP SLA Sources and Responders**

The IP SLA measurement probe is configured on the IP SLA source, via the command line interface (CLI) or by the SNMP tool that support the operation. The source sends probe packets to the receiver. The SLA responder is a component that is imbedded on the IOS, which allows the IP SLA responder to request packets. The IP SLA measurement accuracy is improved when the destination is an IP SLA responder.

**Cisco IP SLA Operation**

The IP SLA is specific to destination devices. There are two types of IP SLA operations. Devices that do not run the IP SLA responder component (web server IP Host) Mostly ICMP generated traffic. And devices running the IP SLAs (Cisco routers.) The measurement will be accurate whenever the destination is a responder where additional statics can be gathered.

An IP SLAs responder provides measurement accuracy without the need for external third party software or external probe and additional statistics that are not otherwise available via standard Internet Control Message Protocol (ICMP) based measurements. When a network manager configures an IP SLAs operation on the IP SLAs source, reaction conditions can also be defined, and the operation can be scheduled to run for a period of time to gather statistics. The source uses the IP SLAs control protocol to communicate with the responder before sending test packets. To increase security of IP SLAs control messages, message digest 5 (MD5)
authentications can be used to secure the control protocol exchange. We can use the following sequence for an IP SLA operation requires a responder on the target.

1. First, the source sends configured IP SLA control information (protocol, port number, and duration of the operation) to the UDP port of the detonation router (responder). If the MD5 authentication is enabled the checksum it will be sent with control message and responder should verify the MD5 checksum, if the authentication fails, the responder sends an authentication failure message.
2. If the responder can process the message it replays 'OK' message and listens to the ports for the specified duration, on the other hand if it cannot process the control message it will replay an error. If the IP SLA source does not get a replay it will resend the control information again until it gets a replay.
3. If an 'OK' message is replayed, the IP SLA on the source starts probing phase and sends one more test packet to compute the repose time. That message is sent on the control port 2020.
4. The responder responds with time stamp in and out to calculate delay.

2.5.4 Path Control Using Offset List

An offset list is a mechanism for increasing incoming and outgoing metric to routes learned via EIGRP or RIP. That is, it can only be use for distance vector routing protocols. Optionally, an offset list can be limited by specifying either an access list or an interface. [1]

Configuring Path Control using Offset list

To create an offset list, we use the offset list router configuration command where the offset value is added to the routing metric. Table 1.1 below defines and explains the offset-list Commands.

Figure 2.5.4 show a multi home network, using RIP and is connected to the two Internet service providers, ISPs. Our aim is to manipulate the RIP metric using the offset list tool and the metric in RIP is hop count. According to the diagram, the preferred RIP route will be between R2 and R5 because the metric is lower than the metric between R2 and R4, because it is only one hop. However, the preferred RIP route is the slowest and we want to use R2 and R4 as the preferred routed since it is the fastest link but however, more in hops. Using an offset list, this can be achieved by increasing the metric to the preferred route.
Improving Network performance by implementing the path control tools

Verification

The **traceroute** EXEC command verifies the normal path traffic takes. That is from R2 to R5 as shown in figure 2.5.4a.

```
R2#traceroute 10.10.50.5
Type escape sequence to abort.
Tracing the route to 10.10.50.5
                            1  10.10.50.5  40 msec 56 msec 16 msec
R2#traceroute 10.10.30.4
Type escape sequence to abort.
Tracing the route to 10.10.30.4
                        1  10.10.30.3  64 msec 20 msec 20 msec
                        2  10.10.30.4  44 msec 36 msec 40 msec
```

Figure 2.5.4 Offset list using RIP

Figure 2.5.4a traceroute from R2 - R5
Figure 2.5.4b Router 5 routing table

The `show IP route` in figure 2.5.4b shows the routing table before applying the offset list command, which identifies the metrics for learned routes. To improve network performance, an offset list and an ACL can be configured on R2 so that it prefers the RIP route to R4 for a specific set of destinations. The offset list configurations for R2 in figure 2.5.4c adds an offset of 3 to the default-metric (1) and applied to incoming routes via interface serial 0/2 that are permitted by access list 21. Thus, traffic will flow from R2 to R4, as that being least in hop.

Figure 2.5.4c configuring an offset list

Figure 2.5.4d `traceroute` after configuring offset list
Improving Network performance by implementing the path control tools

Verification

The **traceroute** EXEC command verifies that an offset list is affecting the route that traffic takes as shown in figure 2.5.4d. And the **show IP route** command will show the metrics for the learned routes as expected by the offset list configuration.

Figure 2.5.4e Routing table R5

Figure 2.5.4e shows the routing table after applying offset-list, which adds an offset of 3 to the default-metric (1), making this route less preferable to get to the ISP. That is more in hops. And finally we use the **debug IP rip** to view the real-time processing of incoming and outgoing RIP routing updates to ensure that the metric is processed correctly. In the above scenario, we have demonstrated how we can improve network performance by implementing an offset list and an ACL together to manipulate the RIP metric to direct traffic to a fastest path.
Chapter 3

3 Experiments

3.1 Design Network Topology

The enterprise network design above fig 3.1 is used as a case study to help improve network performance by implementing the path control tools. The enterprise network comprises of a main office and two other branch offices, branch 1 and 2 and they are all connected to a dual-homed single ISP through multiple local routers. The dual-homed to a single ISP provide load sharing between the three branch networks and redundancy is also added between R1 and R2 to provide connectivity and reachability between the different branches. For example, users in branch 1 use R3 to access the Internet. The main branch office and branch 2 users, use R4 to access the Internet respectively. But if, for some reason, the link to R4 is down, both users in the main office and branch 2 use the backup link R2-R1 then to R3 ISP to access the Internet. Similarly, users in the branch 1 use the same backup link R1-R2 then to R4 ISP to access the Internet if the link to R3 ISP fails.

The existence of multiple routing protocol such as OSPF running in the main office, BGP in the AS 100 and EIGRP running in the branch offices in the AS 100 and 300 respectively, will require to redistribute these protocols so that, routes from one routing protocol can be advertise into another routing protocol. There are 4 points of redistribution in this enterprise network. The first point is a two way redistribution of OSPF into EIGRP in both R2 and R5 in one direction, redistribution of EIGRP and BGP in R1 and R2 in both directions respectively and the redistribution of EIGRP in R6 between AS 200 and 300 in both directions respectively. During route redistribution, external routes are usually less preferred than locally learned routes. Because of these differences in Administrative distances (rates a routing protocol’s believability) the main issues encountered in this enterprise network are issues with suboptimal routing and routing loops and load is not being shared between the branch networks. These issues are explained in chapter 2 and the issues are also examined in this chapter.
Improving Network performance by implementing the path control tools

Fig 3.1 Network topology
3.2 Suboptimal routing and routing loops

One of the main issues is when redistributing OSPF running in the main office into EIGRP in AS 200 running between the main office and branch 2 offices. The OSPF learned routes in R2 and R5 are redistributed into EIGRP and these routes are seen as O E2 with an AD of 110 and a default metric of 20 is used. In order for users in branch 2 to communicate to the rest of the network, it is required to redistribute EIGRP in both ways in R6 between AS 200 and 300 because they have different AS. In R6, EIGRP routes redistributed into OSPF in the main office are seen as external routes with an AD of 170 (D EX). Similarly, routes redistribute from OSPF in EIGRP, will maintain their initial metric and are represented as O E2.

After redistribution, there were issues of suboptimal routing and routing loops because of differences in Administrative Distance as can be seen in the routing tables of R2, R5 and R6 below.

![R2#su ip route
Codes: C - connected, S - static, R - RIP, M - mobile, E - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
* - candidate default, u - per-user static route
o - ODR, p - periodic downloaded static route
Gateway of last resort is 10.2.4.4 to network 0.0.0.0
C  192.168.30.0/24 is directly connected. Serial0/2
D EX 192.168.60.0/24 [170/2707456] via 192.168.30.6, 02:24:14, Serial0/2
C  192.168.10.0/24 is directly connected, Serial0/1
D  192.168.40.0/24 [90/2681856] via 192.168.30.6, 02:38:02, Serial0/2
B  192.168.50.0/24 [200/100] via 192.168.2.1, 00:52:16
O  102.168.20.0/24 [110/74] via 102.168.10.5, 01:45:16, Serial0/1
10.0.0.0/24 is subnetted, 2 subnets
C  10.2.4.0 is directly connected, Serial0/0
D EX 10.3.4.0 [170/3193556] via 192.168.30.6, 00:38:15, Serial0/2
D EX 192.168.50.0/24 [170/2681856] via 192.168.30.6, 02:24:14, Serial0/2
C  192.168.1.0/24 is directly connected, FastEthernet0/1
C  192.168.2.0/24 is directly connected, FastEthernet0/0
B  192.168.70.0/24 [200/0] via 192.168.2.1, 00:52:20
B*  0.0.0.0/0 [20/0] via 10.2.4.4, 00:35:00

Figure 3.2a R2 routing table

The routing table in figure 3.2b of R5 shows a situation of suboptimal routing and routing loops. Packets take different path via 192.168.10.2 (R2) in order to communicate with users in 192.168.50 and 192.168.60 network (branch office 2) respectively. Packets travel via the longest route instead of travelling directly via R6. This is called suboptimal routing. Because R2 is sending packets back to R5 and R6 is sending packets back simultaneously a loop is created. This occurs because the AD of OSPF (110) is lower than the AD of external EIGRP (170). The network 19.168.60.0 is also wrongly represented. This network should be represented as D EX route.
Improving Network performance by implementing the path control tools

Figure 3.2.b Routing table R5

The routing table in figure 3.2d shows the issues of suboptimal routing and routing loops when redistributing EIGRP (AS200) into EIGRP (AS 300). The issue is, R6 prefers the OSPF route, which is a suboptimal path via 192.168.40.5 (R5) to 10.3.4.0 R4 ISP. Similarly, packets travel via 192.168.40.4 to reach the 192.168.1.0 and 192.168.2.0 network respectively. Packets should instead travel via 192.168.30.2 (R2). Packets keep on travelling forth and back between R2, R5 and R6 causing suboptimal routing and routing loops.

---

```
R5#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, SI - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - IS-IS inter area, * - candidate default, U - per-user static route
        P - periodic downloaded static route

Gateway of last resort is 192.168.10.2 to network 0.0.0.0

D  192.168.30.0/24 [90/2681856] via 192.168.40.6, 02:33:22, Serial0/0
O  E2  192.168.40.0/24 [110/20] via 192.168.30.2, 00:42:36, Serial0/1
O  C  192.168.10.0/24 is directly connected, Serial0/1
C  192.168.40.0/24 is directly connected, Serial0/0
C  192.168.20.0/24 is directly connected, FastEthernet0/1
O  E2  10.3.4.0/24 [110/20] via 192.168.10.2, 00:33:32, Serial0/1
O  E2  192.168.50.0/24 [110/20] via 192.168.10.2, 00:42:36, Serial0/1
O  E2  192.168.1.0/24 [110/1] via 192.168.10.2, 00:48:55, Serial0/1
O  E2  192.168.2.0/24 [110/1] via 192.168.10.2, 00:47:44, Serial0/1
O  E2  192.168.30.0/24 [110/1] via 192.168.10.2, 01:21:28, Serial0/1
O  E2  0.0.0.0/0 [110/1] via 192.168.10.2, 00:00:00, Serial0/1
```

Fig 3.2c. R6 routing table R6
Figure 3.2d below verifies suboptimal routing and routing loops from the branch 2 networks by using the traceroute and the ping command. The ping is successful but using the traceroute command, packets travel via the longest path via the OSPF network because the AD of external EIGRP (170) is greater than that of the AD of OSPF. Packets travel via 192.168.50.6 into OSPF (R5) then to R2. Packet should not travel into the OSPF network; it should travel via R2 and then to its final destination instead.

```
R7#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/72/156 ms
```

```
R7#traceroute 192.168.1.2
Type escape sequence to abort.
Tracing the route to 192.168.1.2

1 192.168.50.6 96 msec 46 msec 60 msec
2 192.168.40.5 212 msec 116 msec 236 msec
3 192.168.10.2 100 msec * 88 msec
```

Figure 3.2d the ping and traceroute from R7

### 3.3 Load sharing Problems

Verifying Load sharing in R1 and R2, it is required to redistribution in order to reach the ISP (R3 and R4). Redundancy is added between R1 and R2 to provide connectivity and reachability between the different branch networks. If one link fails, the other link is used to reach other parts in the network. The first issue of load sharing is that it is unreachable from R7. Users in branch 2 should normally use R4 to connect to the Internet but instead packets travel through the longest path creating loops in the network and load is not being shared. That is users in the branch 2 cannot reach R4, ISP. Figure 3.3a is a traceroute to the ISP (R4), which shows issues of suboptimal routing and routing loops and load sharing.
Improving Network performance by implementing the path control tools

Figure 3.3a. Traceroute R7 to ISP

In the branch 1 network, it was easy to reach the ISP after redistributing EIGRP into BGP in both directions. Figure 3.3b below shows a ping to the ISP, R3 was successful and the traceroute command also shows the path it’s supposed to take.

Figure 3.3b. Ping and Traceroute from R8 to ISP

The idea of using a multi-homed to one ISP is to apply load sharing. If for some reasons, the link to R1 to ISP R3 fails, packets should follow the link between R1 and R2 to R4, ISP. Unfortunately, this did not work as can be seen in figure 3.3c below.
Figure 3.3c. Ping and Traceroute to R4 ISP

R8#ping 10.3.4.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.4.3, timeout is 2 seconds:

Success rate is 0 percent (0/5)
R8#trace
R8#traceroute 10.3.4.3

Type escape sequence to abort.
Tracing the route to 10.3.4.3.

1   *   *

Figure 3.3c. Ping and Traceroute to R4 ISP
Improving Network performance by implementing the path control tools
Chapter 4

4 Results and Analysis

Designing an IP network requires a deep knowledge of both infrastructures, and the performance of the devices that are used. At the same time how packets are handled by the devices. In networking infrastructure where there are multiple branches with lots of redistribution points, performance is very important thing that a network designer should consider. A company can have different branches, where those branches use different routing protocols. Branches of the same company should communicate with each other. The existence of multiple routing protocols in different branches will require redistributing those protocols so that, routes from one routing protocol can be advertised in to another routing protocol. The main issues, which can affect the performance of a network, are the results of improper redistribution. These issues, which affect the network performance, are excessive routing updates, suboptimal routing and routing loop, which can lead to network downtime.

The approach used to prevent suboptimal routing and routing loops and load sharing which are the main issues in the network topology is to use the path control tools. The path control tools used are Route Maps and default route.

The route-maps function is a generic mechanism of Cisco IOS software configuration. You can apply it to many different tasks, for example, policy-based routing (PBR) and Border Gateway Protocol (BGP) neighbor update modification. One of the most common uses of route-maps is to apply them to routes that are redistributed between dynamic routing protocols.[13]

The route map is configured or applied in the redistribution points of R1, R2 and R6. There are two maps applied in R1 and R2, a route map for load sharing which allow packets to travel in and out of the BGP area and allows users in the branch offices to reach the Internet, R3 and R4 and a route map to permit the networks that are to distributed. To reduce the size of the routing table, a route map is also applied in router R6 to filter the networks in the OSPF main area. After applying the route map, the routing tables of R2, R5 and R6, ping and traceroute commands is analyze to verify the absence of the issues of suboptimal routing and routing loops and load sharing is also verified and examine in the network topology. From any of the branch networks, load sharing can be verified when one of the links for example, the link to R4, ISP is shut down and packets travel via the backup link R2 to R1 then to the R3 ISP. Finally, in R7, a default static route is used to provide connectivity and reachability to the rest of the network.
The first redistribution Point R1, which is a two-way redistribution between EIGRP AS 200 and BGP AS 100 and the second redistribution Point R2, is a two-way redistribution between BGP and OSPF and a one-way redistribution BGP into EIGRP AS 200 are analyzed for load sharing. Users in branch 1 should use R3 ISP and users in the main office and branch 2 by default should use the R4 ISP. The first issue encountered is that when the link to R3 is down traffic could not travel from the branch 1 via the backup link R1 via R2 to R4 ISP and the second issue of load sharing is that traffic coming from the main office and branch 2 could not use the backup link R2 via R1 to R3 ISP when the link to R4 ISP fail.

4.1 Suboptimal routing and routing loop Solution

As it was discussed earlier packet from R7 where taking the longer path to reach the destination or the Internet. The longest path is via R7 through 192.168.10.0 /24 networks. And packets come to R7 comes through the same path. This is called suboptimal routing. To overcome this, a route map is applied in R6 and using access list we denied the network that the router prefers as a main path (192.168.10.0/24). On R2 we redistributed EIGRP in to OSPF, after configuring redistributions, OSFP to BGP, and vice versa, at the same time EIGRP to BGP.

In R6, which is a two-way redistribution between EIGRP of different AS 200 and 300 respectively? When redistributing EIGRP 200 to 300 we used a route-map. This helps to filter which networks that should be redistributed. All the networks where permitted using the route map but blocked the network R5 -R2 (192.168.10.0 network) using access list. This is because packets from R7 where taking that path to reach the Internet causing suboptimal routing and routing loops. There is no redistribution between OSPF into EIGRP because the network is not permitted by route map statement, so no need to redistribute the network. Rather than having the entire routing table exchange, which could possibly cause suboptimal routing and routing loops, static default route is applied in R7 to reach main office and to the rest of the network.
In R2, there are two route maps applied like in R1. One is for load sharing and the other to permit learned routes from EIGRP AS 200 and AS 300 and OSPF to pass through to access R4 ISP. Figure 4.1 shows the configuration of how to apply a route map. The route-map R2-R4 out allows the learned routes to be redirected or access R4 ISP and the next hop self statement works where if the serial link to R4 ISP fails or is shutdown traffic is directed to the next hop address via the backup link R2 – R1 to R3 then back to R4 ISP. Similarly, the route map statement in R1, route map R1-R3 out permits all users in the branch 1 to access R3 internet and the next hop self address 192.168.1.2 is used if the link to R3 ISP fails. Traffic flow via the backup link R1-R2 to R4 then back to R3 ISP.

```
R7#ping 10.3.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.4.4, timeout is 2 seconds:
!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 58/209/258 ms
R7#traceroute 10.3.4.4
Type escape sequence to abort.
Tracing the route to 10.3.4.4
1 192.168.50.6 32 msec 4 msec 60 msec
2 192.168.30.2 24 msec 8 msec 24 msec
3 10.2.4.4 148 msec 60 msec 108 msec
```

Fig 4.1 ping from R7 to the ISP

To verify the issues of suboptimal routing, the routing table of R2, R5 and R6 are analyzed. The routing table in figure 4.1a is that of R2. Before, traffic passing through R2 was being sent back into the EIGRP AS 200 causing suboptimal routing and loops. Now, with the use of a route map, traffic is allowed to pass through via 10.2.4.4 to 10.3.4.0 network. Moreover, the network is truly represented as a BGP network. Before it was seen as D EX network.
Improving Network Performance by Implementing the Path Control Tools

Figure 4.1a R2 routing table

Figure 4.1b below is the routing table of R5. Before, traffic where using a suboptimal path via the OSPF (192.168.10.0) network. But now, traffic is travelling via the EIGRP network (192.168.40.6) network to reach the branch networks 192.168.60 and 192.168.60.0 respectively. The network 192.168.60.0 is also rightly represented. Before, it was seen as O E2 network.

Figure 4.1b R5 routing table

In figure 4.1c in R6, before, traffic went via the OSPF route then back into the EIGRP AS 200 network which is a suboptimal path via 192.168.40.5 (R5) to 10.3.4.0 R4 ISP. Similarly, packets travelled via 192.168.40.4.5 to reach the 192.168.1.0 and 192.168.2.0 network respectively. Now packets travel via 192.168.30.2 (R2) to reach 10.3.4.0, 192.168.1.0 and 192.168.2.0 networks. Suboptimal routing and loops no longer exist in the network and the load sharing work perfectly well.
Chapter 4. Results and Analysis

4.2 Load sharing Solution

Figure 4.2a in R8 shows that users in the branch 1 network could reach the Internet via R1 to R3 ISP using the ping command targeting the network to R3 ISP and the traceroute command also shows the supposed path that packet will travel.
Figure 4.2b. Link to R3 shutdown

**R3(config)#int s0/0**
**R3(config-if)#sh**
**R3(config-if)#**

*Mar 1 11:44:41.188: &BGP-5-ADJCCHANGE: neighbor 10.1.3.1 Down Interface Flap*
*Mar 1 11:44:41.181: &LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down*
*Mar 1 11:44:41.181: &LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,*

Figure 4.2c. Traceroute to R4

```
R3#traceroute 10.3.4.4
Type escape sequence to abort.  
Tracing the route to 10.3.4.4:

1 192.168.70.1 128 msec 40 msec 44 msec
2 192.168.2.2 184 msec 180 msec 192 msec
3 192.168.4.4 276 msec 232 msec 244 msec
```

**R3#ping 10.3.4.4**

Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echoes to 10.3.4.4, timeout is 2 seconds:

```
+++++
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/158/204 msec
```

Figure 4.3 shows the new path when the link to R3 ISP is shutdown. Packets travel from R8, branch 1 office via the backup links R1-R2 to R4 ISP and finally to R3 ISP. After applying a route map in R1, users can now access the backup links R1-R2, via R4 ISP to R3 ISP from the branch 1 network as can be seen above.

Figure 4.2d is a ping from R8, which verifies that packets could reach the main office.

```
R8#ping 192.168.20.5
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echoes to 192.168.20.5, timeout is 2 seconds:

+++++
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/180/184 msec
```

Figure 4.2d Ping to the main office

In figure 5.5 in R2, there are two route maps applied like in R1. One is for load sharing and the other to permit learned routes from EIGRP AS 200 and AS 300 and OSPF to pass through to access R4 ISP. Figure 4.4 shows the configuration of how to apply a route map. The route-map R2-R4 out allows the learned routes to be redirected or access R4 ISP and the next hop self statement works where if the serial link to R4 ISP fails or is shutdown traffic is directed to the next hop address via the backup link R2 – R1 to R3 then back to R4 ISP. Similarly, the route map statement in
Chapter 4. Results and Analysis

R1, route map R1-R3 out permits all users in the branch 1 to access R3 internet and the next hop self address 192.168.1.2 is used if the link to R3 ISP fails. Traffic flow via the backup link R1-R2 to R4 then back to R3 ISP.

```
routerr eigrp 200
    redistribute bgp 110 metric 100 1 255 1 1500
    network 192.168.30.0
    auto-summary

router ospf 1
    log-adjacency-changes
    redistribute bgp 110 subnets
    network 192.168.10.0 0.0.0.255 area 0
default-information originate always

router bgp 110
    no synchronization
    bgp log-neighbor-changes
    network 192.168.1.0
    network 192.168.2.0
    redistribute static
    redistribute ospf 1 match internal external 1 external 2
    redistribute eigrp 200 metric 90 route-map T0-BGP
    neighbor 10.2.4.4 remote-as 100
    neighbor 10.2.4.4 route-map R2-R4 out
    neighbor 192.168.2.1 remote-as 110
    neighbor 192.168.2.1 next-hop-self
    maximum-paths 2
default-information originate
    no auto-summary
```

Figure 4.2e. Route map configuration in R2

Figure 4.2f verifies load sharing. Users in R5 main office can now use the R4 ISP. The ping is successful and the traceroute also shows the supposed path traffic travel. But, if the link to R4 ISP is shutdown traffic flow via the backup link R2-R1 then R3 ISP using the next hop self-address to direct traffic to R3 ISP.

```
R5#ping 10.3.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.4.4, timeout is 2 seconds:
!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/59/244 ms

R5#traceroute 10.3.4.4

Type escape sequence to abort.
Tracing the route to 10.3.4.4

  1 192.168.10.2 4 msec 60 msec 4 msec
  2 10.2.4.4 116 msec 100 msec 52 msec
```

Figure 4.2f Ping and Traceroute to R4 ISP

Figure 4.2g verifies load sharing when the link to R4 ISP is down. Users in R5 main office can now use the backup link R2-R1 then R3 ISP. The ping is successful and the
traceroute also shows the supposed path traffic travel using the next hop self-address to direct traffic to R3 ISP.

```
R5#ping 10.3.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.4.4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/120/188 ms
R5#trac
R5#traceroute 10.3.4.4
Type escape sequence to abort.
Tracing the route to 10.3.4.4
1 192.168.10.2 76 msec 60 msec 4 msec
2 192.168.2.1 168 msec 152 msec 80 msec
3 10.1.3.3 204 msec 184 msec 148 msec
4 10.3.4.4 244 msec 316 msec 226 msec
```

Figure 4.2g Ping and Traceroute to R3 ISP after R4 link down

The third redistribution point is in R6, which is a two-way redistribution between EIGRP of different AS 200 and 300 respectively. When redistributing EIGRP 200 to 300 we used a route-map. This helps to filter which networks that should be redistributed. All the networks where permitted using the route map but blocked the network R5-R2 (192.168.10.0 network) using access list. This is because packets from R7 where taking that path to reach the Internet causing suboptimal routing and routing loops. There is no redistribution between OSPF into EIGRP because the network is not permitted by route map statement, so no need to redistribute the network. Rather than having the entire routing table exchange, which could possibly cause suboptimal routing and routing loops, static default route is applied in R7 to reach main office and to the rest of the network.

Figure 4.2h is a ping and a traceroute from R7 to R4 ISP before the link is shutdown. The ping is successful meaning users in the branch 2 can connect to the internet using R4 ISP and the traceroute also shows the path it is supposed to travel and also verifies that packets are travelling using the shortest path to reach R4 ISP. Before traffic was travelling via the suboptimal path i.e. longest path via the OSPF network (192.168.40.0 network) thereby creating routing loops in the network.

```
R7#ping 10.3.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.4.4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/209/258 ms
R7#trac
R7#traceroute 10.3.4.4
Type escape sequence to abort.
Tracing the route to 10.3.4.4
1 192.168.50.6 32 msec 4 msec 60 msec
2 192.168.30.2 24 msec 8 msec 24 msec
3 10.2.4.4 148 msec 60 msec 100 msec
```
Figure 4.2h Ping and Traceroute to R4 ISP

```
R2(config-if)#sh
R2(config-if)#
*Mar 1 10:58:14.365: *BGP-5-ADJCHANGE: neighbor 10.2.4.4 Down Interface flap
*Mar 1 10:58:16.329: *LINK-5-CHANGED: Interface Serial0/0, changed state to admin
*Mar 1 10:58:17.329: *LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0
```

Figure 4.2i Link to R4 ISP shutdown

Figure 4.2i is a ping and a traceroute from R7 to R3 ISP after the link to R4 is shutdown as it can be seen in figure 4.2i. The ping is successful meaning users in the branch 2 can connect to the internet using R4 ISP and the traceroute also shows the path it is supposed to travel and also verifies that packets are travelling using the shortest path to reach R4 ISP via the backup link R2-R1 and then R3-R4 ISP. Before traffic was travelling via the suboptimal path i.e. longest path via the OSPF network (192.168.40.0 network) and back into EIGRP network. Thereby, creating routing loops in the network.

```
R7#ping 10.3.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.4.4, timeout is 2 seconds:
!! ! ! ! ! ! ! !
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/193/252 ms
R7#tra
R7#traceroute 10.3.4.4
Type escape sequence to abort.
Tracing the route to 10.3.4.4
   1 192.168.30.6 44 msec 106 msec 24 msec
   2 192.168.30.2 60 msec 44 msec 40 msec
   3 192.168.2.1 140 msec 104 msec 104 msec
   4 10.1.3.3 228 msec 296 msec 184 msec
   5 10.3.4.4 240 msec 232 msec 324 msec
```

Figure 4.2j Ping and Traceroute after link to R4 ISP shutdown

Figure 4.2j is a ping from R7, which verifies that packets could reach the main office.
Improving Network Performance by Implementing the Path Control Tools

Figure 4.2k Ping to the main office

```
R7#ping 192.168.20.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.5, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/118/172 ms

R7#ping 192.168.70.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.8, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/172/232 ms
```
Conclusion

The purpose of this paper is to improve network performance using the path control tools to manipulate routing updates. To improve network performance, an enterprise network topology was designed to present network performance issues. The network performance issues like excessive routing updates, suboptimal routing and loops, redundant paths and load sharing where explained to give readers an idea of the possible causes of network issues. The path control tools where also examined briefly. The tools include: policy-based routing, administrative distance, Cisco IOS IP SLAs and offset list. For better understanding, the offset list tool was practically examined separately because it could not be setup in the network topology since it is use for distance vector protocols RIP and EIGRP.

The enterprise network topology consists of a main office and two other branch networks branch 1 and 2 all connected to a dual-homed to a single ISP via multiple local routers to provide redundancy and load sharing between the different branches. The main issues in the enterprise network are issues of suboptimal routing and loops and load is not being shared between the different branch networks. The issues occur when redistributing one routing protocol into another routing protocol in the redistribution points R1, R2, R5, and R6 causing suboptimal routing and routing loops. When redistribution occurs between different routing protocols, routers forward packets using a suboptimal path because of the differences in AD and metric. With these issues, users in the different branch networks could not communicate with each other and could not access the Internet.

To address the issues, the path control tool route map, which is one of the tools in Policy-Based Routing, is used to fix the issues of suboptimal routing and routing loops and load sharing as well. After apply the route map on the redistribution points of R1, R2 and R3, users in the different branches can communicate with each other using R3 and R4 ISP. Load is also shared and works perfectly. For example, load sharing works and is verified when if the link to the R4 ISP fails, users from the main and branch 2 offices use the backup links via R2-R1 to R3-R4 ISP.

To verify that suboptimal routing and routing loops are not existing in the network, the routing tables of the redistribution points R2, R5 and R6 causing suboptimal routing and loops are examined and compared. Comparison is done after redistributing and after applying he route map on the redistribution points. This proves to be also successful as no suboptimal routing and routing loops exist.

In conclusion, we can say that we have improved the network performance of the enterprise network by using the path control tools.
Bibliography
