Networking Lab Day 4

Kevin Neumann, Alain C. Mendy

May 25, 2014, Goettingen

Contents

1 Prelab

The prelab preperations can be found in the directory prelab in the known git repository (https://www.github.com/Phiology/networkingLab).

2 Part 1: Configuring RIP on Cisco Routers

The routers were set up according to the information given in the lab wiki using the RIP protocol. The connectivity was tested, and all routers and PCS could be reached.

3 Part 2: Configurating RIP on the PCs

3.1 Use the captured data of a single RIP packet and explain the fields in a RIP message.

There are 4 general fields in a RIP message:

The command field shows the kind of message sent.

The version field gives information about the version of RIP used.

The routing domain shows a network prefix and a set of routers exchanging routing information within an administrative domain

The ip addresses show the network addresss of the other networks on the other side of the router. Included are the address family, the route tag (to distinguish beweeen internal and external routes), the IP address, subnet mask for the network, next hop information and the metric (shows how many hops within the network were jumped on the way to the destination). 16 stands for an unreachable route.

3.2 Compare the output of show ip rip to the output of netstat -rn

show ip rip shows the cost metric for other destinations while netstat doesn't. Also, it has a time and from column and specifies the protocol of the connection.

Netstat -rn however shown the lo interface and has netmask and interface information.

3.3 What is the destination IP address of RIP packets?

224.0.0.9

3.4 Do routers forward RIP packets? In other words, does PC1 receive RIP packets sent by Router3?

Routers do not forward RIP packages. So, PC1 only receives RIP packages from its neighbors.

3.5 Which types of routing RIP messaegs do you observe? The type of a RIP message is indicated by the value of the field command. For each packet type that you observed, explain the role that this message type plays in the RIP protocol.

We only observed response messages. The routers try to update their routing entries by sending RIP messages to neighbor routers, and thus the replies were responses.

3.6 A RIP message may contain multiple routing entries. How many bytes are consumed in a RIP message for each routing table entry? Which information is transmitted for each message?

86 bytes are consumed and 2 routing entries were observed. The transmitted information are the network addresses on the other side of the routers.

4 Part 3: Updating the routing tables and convergence of RIP after a link failure

4.1 Count the number of lost packets and calculate the time it took RIP to update the routing tables. (The ping command issues an ICMP Echo Request message approximately once every second.)

There were 213 packets transmitted, 19 received, +126 errors, 91 % package loss, time 212830 ms.

Because one packet is tried to be send in 1 second, it took approximately 194 seconds (3 min 14 sec) to update the routing tables.

5 Part 4 : Adding PC3 to the network configuration, the count-to-infinity problem and avoiding the count-to-infinity problem

5.1 Use the saved RIP packets from Router3 and PC3 to describe the count-to-infinity problem in the preceding exercise. Include relevant fields from the saved RIP packets to illustrate your description.

Routing Information Protocol
Command: Response (2)
Version: RIPv2 (2)
Routing Domain: 0
IP Address: 10.0.1.0, Metric: 16

In the wireshark package, it can be seen that the metric to the network 10.0.1.0 is 16, measing infinity. This means that the nodes in the network are unreachable. Now, the distance vector routing algorithm adjusts the distance value slowly upwards. This takes a long time, that's why it is called "counting to infinity".

5.2 Use the output that you saved to show the difference between the outcomes of Exercise 4(B) and 4(C) with regard to the convergence of RIP.

In 4B, there were 198 packes transmited and 92 % lost. So it took about 3 minutes to converge. In 4C however, it only took about 2,5 minutes to converge, showing that triggered updates can decrease the downtime using RIP in case of a disabled route.

6 Part 5: Configuring OSPF on Linux PCs and routers and observing the convergence of OSPF

6.1 Count the number of lost packets and calculate the time it took OSPF to updatethe routing tables. (The ping command issues an ICMP Echo Request message approximately once every second.)

There were 78 packats transmitted and 52 lost. So the convergence took about 40 seconds to happen.

6.2 From your saved Wireshark output, include one packet from each of the different OSPF packet types that you have observed.

Three packets were observed: Hello packets, update packets, and acknowledgement packets.

Internet Protocol, Src Addr: 10.0.1.1 (10.0.1.1), Dst Addr: 224.0.0.5 (224.0.0.5) Version: 4 Header length: 20 bytes Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00) .... ..0. = ECN-Capable Transport (ECT): 0 ....0 = ECN-CE: 0 Total Length: 68 Identification: 0x3555 (13653) Flags: 0x00 .0.. = Don't fragment: Not set ..0. = More fragments: Not set Fragment offset: 0 Time to live: 1 Protocol: OSPF (0x59) Header checksum: 0x9906 (correct) Source: 10.0.1.1 (10.0.1.1) Destination: 224.0.0.5 (224.0.0.5) Open Shortest Path First OSPF Header OSPF Version: 2 Message Type: Hello Packet (1) Packet Length: 48 Source OSPF Router: 10.0.1.1 (10.0.1.1) Area ID: 0.0.0.1 Packet Checksum: 0xd093 (correct) Auth Type: Null Auth Data (none) OSPF Hello Packet Network Mask: 255.255.255.0 Hello Interval: 10 seconds Options: 0x2 (E) Router Priority: 1 Router Dead Interval: 40 seconds Designated Router: 10.0.1.2 Backup Designated Router: 10.0.1.1 Active Neighbor: 10.0.1.2

Internet Protocol, Src Addr: 10.0.1.2 (10.0.1.2), Dst Addr: 224.0.0.5 (224.0.0.5) Version: 4 Header length: 20 bytes Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00) .... ..0. = ECN-Capable Transport (ECT): 0 ....0 = ECN-CE: 0 Total Length: 84 Identification: 0x3706 (14086) Flags: 0x00 .0.. = Don't fragment: Not set ..0. = More fragments: Not set Fragment offset: 0 Time to live: 1 Protocol: OSPF (0x59) Header checksum: 0x9744 (correct) Source: 10.0.1.2 (10.0.1.2) Destination: 224.0.0.5 (224.0.0.5) Open Shortest Path First OSPF Header OSPF Version: 2 Message Type: LS Update (4) Packet Length: 64 Source OSPF Router: 10.0.1.2 (10.0.1.2) Area ID: 0.0.0.1 Packet Checksum: 0x4563 (correct) Auth Type: Null Auth Data (none) LS Update Packet Number of LSAs: 1 LS Type: Router-LSA LS Age: 2 seconds Options: 0x22 (E/DC) Link-State Advertisement Type: Router-LSA (1) Link State ID: 10.0.4.4 Advertising Router: 10.0.4.4 (10.0.4.4) LS Sequence Number: 0x80000016 LS Checksum: cef5 Length: 36 Flags: 0x00 Number of Links: 1 Type: Transit ID: 10.0.5.6 Data: 10.0.5.8 Metric: 10 IP address of Designated Router: 10.0.5.6 Link Data: 10.0.5.8 Link Type: 2 - Connection to a transit network Number of TOS metrics: 0 TOS 0 metric: 10

Internet Protocol, Src Addr: 10.0.1.1 (10.0.1.1), Dst Addr: 224.0.0.5 (224.0.0.5) Version: 4 Header length: 20 bytes Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00) .... ..0. = ECN-Capable Transport (ECT):

0 ....0 = ECN-CE: 0 Total Length: 64 Identification: 0x355c (13660) Flags: 0x00 .0.. = Don't fragment: Not set ..0. = More fragments: Not set Fragment offset: 0 Time to live: 1 Protocol: OSPF (0x59) Header checksum: 0x9903 (correct) Source: 10.0.1.1 (10.0.1.1) Destination: 224.0.0.5 (224.0.0.5) Open Shortest Path First OSPF Header OSPF Version: 2 Message Type: LS Acknowledge (5) Packet Length: 44 Source OSPF Router: 10.0.1.1 (10.0.1.1) Area ID: 0.0.0.1 Packet Checksum: 0x6591 (correct) Auth Type: Null Auth Data (none) LSA Header LS Age: 2 seconds Options: 0x22 (E/DC) Link-State Advertisement Type: Router-LSA (1) Link State ID: 10.0.4.4 Advertising Router: 10.0.4.4 (10.0.4.4) LS Sequence Number: 0x80000016 LS Checksum: cef5 Length: 36

6.3 Include the output of the link state database of PC2

Instead, the outpu of the database of router 3 is submitted.

$OSPFRouterwithID$(10.0.3.4)

Router Link States (Area 0.0.0.1)

Link ID ADV Router Age Seq CkSum Link count 10.0.1.1 10.0.1.1 518 0x8000000a 0x2cae 2 10.0.1.2 10.0.1.2 402 0x8000000b 0x3b8f 2 10.0.2.1 10.0.2.1 547 0x80000002 0x2ab6 2 10.0.3.2 10.0.3.2 2960 0x80000003 0x22b3 2 10.0.3.4 10.0.3.4 746 0x80000005 0x03c2 2 10.0.4.4 10.0.4.4 2048 0x80000002 0x56ad 1 10.0.4.5 10.0.4.5 368 0x80000005 0x8e11 2 10.0.5.1 10.0.5.1 32 0x80000006 0xf6c8 2 10.0.5.2 10.0.5.2 1006 0x80000004 0xf6d3 2 10.0.5.4 10.0.5.4 187 0x80000008 0x4a8d 1 10.0.6.6 10.0.6.6 737 0x80000005 0x2b82 2 10.0.6.7 10.0.6.7 153 0x80000005 0x7f3f 2

Net Link States (Area 0.0.0.1)

Link ID ADV Router Age Seq CkSum 10.0.1.2 10.0.1.2 516 0x80000002 0x61c4 10.0.2.3 10.0.5.1 293 0x80000009 0xcd0f 10.0.3.3 10.0.5.1 32 0x80000004 0x9f56 10.0.4.4 10.0.3.4 746 0x80000001 0xbd52 10.0.5.8 10.0.5.4 408 0x80000008 0x626f 10.0.6.7 10.0.6.7 370 0x80000001 0x837e

6.4 Pick a single link state advertisement packet captured by Wireshark, and describe how to interpret the information contained in the link state advertisement.

Update packets contain numbers of LSA and the time that the LSA entries stay there. In addition, they also show the number of links which are Stub and Transit.

6.5 How quickly are OSPF messages sent after the cable is disconnected?

It took 19 seconds for the OSPF update message.

6.6 How many OSPF messages are sent?

15 OSPF messages including Hello and ack packets before the connection.

6.7 Which type of OSPF packet is used for flooding link state information?

The OSFP update messages.

6.8 Describe the flooding of LSAs to all routers.

From time to time, each router will broadcast LSAs to surrounding hosts using OSPF update. Hosts that got updated will answer with an acknowledgement message.

6.9 Which type of encapsulation is used for OSPF packets (TCP,UDP or other)?

It is using IP (Internet Protocol)

6.10 What is the destination address of OSPF packets?

The broadcast address.

6.11 Can you confirm that the link state databases are identical? Compare the output of the command show ip ospf database from the Cisco routers and the Linux PCs.

It can be confirmed, that all databases are identical.

7 Part 6: Defining multiple areas in OSPF

7.1 Include the Wireshark output in your report showing, if any, the different types of OSPF packets that you did not observe in Part 5.

There were LS requests and DB Descr. seen.
$OSPFVersion : 2 MessageType : DBDescr.(2) OSPFVersion : 2 MessageType : LSRequest(3)$

7.2 Include the output of the link state databases saved in Step 5.

The output can be found in directory exercice6.

7.3 Compare the link state databases to those saved in Part5. Which differences do you note?

Instead of the link state databases being all equals, the hosts only know information about their own area relying on border gateways to reach different areas.

7.4 Which information do routers in Area 1 have about Area2? Which information do they have about the backbone area (Area 0)?

None about area 2 routers. They only have information about the area 0 borderline router connection area 1 to area 0.

7.5 How much information do the routers in the backbone area (Area 0) have about the topology of Area 1 and Area 2?

They only possess information about area 1 or 2 and area 0 including the other vorderline router, but do not know information about area 2 or 1 (vice versa).

7.6 How do the IP routers in Area 1 know how to forward traffic to Area 2?

They will send their traffic to their gefault gateway, in that case the borderline router.

7.7 Explain the output of the command show ip ospf border-routers in Step 5.

$i10.0.1.1[1]via10.0.2.1, FastEthernet0/1, ABR, Area1, SPF11$

The output shows the borderline router between area 1 and 0.

8 Part 7: Basic BGP configuration and BGP convergence

8.1 Describe the different types of BGP messages that you observe in the Wireshark window on PC4.

KeepAlive: Message sent by a network device to inform neighbors that the virtual circuit is still active.

8.2 Notice that BGP transmits messages over TCP connections. What is a reason that BGP uses TCP to transmit its messages?

TCP is used to establish a reliable connection. One session is established between each peet for each BGP session. No routing information can be exchanged until the TCP session has been established. This implies that each BGP speaker must have working IP connectivity between them first, which is usually provided by a directly connected interface or the IGP.

8.3 What is the IP address of the next-hop attribute for AS 100 on Router2?

10.0.4.1/28

8.4 What are the BGP peers in this topology?

Router1, Router2 and Router3.

8.5 Which BGP message(s) contain(s) the AS-PATH information? Include a BGP message to illustrate your answer.

BGP update messages contan the AS-PATH informaton.

$UPDATEMessageMarker : 16bytesLength : 52bytesType : UPDATEMessage(2)Unfeasibler$
$0bytesTotalpathattributelength : 25bytesPathattributesORIGIN : IGP(4bytes)Flags :$
$0x40(Well-known, Transitive, Complete)0..... = Well-known.1..... =$
$Transitive..0..... = Complete...0.... = Regularlength$

8.6 Use the saved output to provide a brief explanation of how the routers find the proper path between the autonomous systems.

They constantly trade AS-PATH information, which contains the next hop to get to other destinations.

$NEXT_HOP : 10.0.4.1(7bytes)Flags : 0x40(Well-known, Transitive, Complete)0..... =$
$Well-known.1..... = Transitive..0..... = Complete...0.... = RegularlengthTypecode :$
$NEXT_HOP(3)Length : 4bytesNexthop : 10.0.4.1(10.0.4.1)$

8.7 Describe how the BGP routers learn that a link is down.

From the only notification message of BGP packets, we found out that there is Error Code stated that Hold Timer is expired. Here, routers must maintain a TCP session with their neighbors since we were using BGP and AS topology. If a TCP session is terminated for any reason, the routing

information learnt from that session is deleted. All routing updates contain the originating AS number. In our lab result, it seems like AS200 tried to keep TCP session with AS100 but since AS100 was disconnected, it was notified and it sent update to AS300.

8.8 Which BGP messages indicate that there is a link problem? Include a BGP message.

BGP update and notification messages.