Objectives:

- Describe the structure of a routing table.
- Describe how a router determines a path and switches packets.

Intro:

After receive a call from OCP Enterprises, you place a visit to their office to check the problem. According to the complaint made during the phone call, parts of their network are not able to reach each other. The reported problems are listed below:

1. PC1 is not able to reach PC4 with no packets being successfully sent/received between those PCs.
2. PC1 is not able to reach PC5, PC6 or PC7.
3. PC1 and PC3 reach network 3 but PC2 does not.

Topology:
The Scenario:

The topology is relatively simple and you decide to examine each problem separately.

Problem 1 – PC1 fails reaching PC4

You take a look on the topology handed to you (shown above) and, from PC1, you send a few packets to PC4 using the ping command. You watch while all packets are being dropped.

You check PC1’s IP information configuration and it looks good: PC1 has a valid IP address belonging to R1’s network 1 and PC1’s default gateway is the R1’s interface connected to network 1.

In order to identify the failure point, you decide to issues pings to closer devices. You issue another ping from PC1 but this time targeting R1’s fa0/0 and watch them being successfully received by R1.

The successful ping from PC1 to R1 fa0/0 (PC1’s default gateway) means the path from PC1 to R1 is working fine (at a OSI Layer 3, at least)

Based on the topology shown above, you move forward and ping R2’s interface Se0/0 from PC1. All pings fail.

Looks like R2 has wrong routing information regarding network 1 but you still need a few more tests to make sure.

Question 1:

Could you give one reason why is it too early to blame R2’s routing table?

Answer: At this point there is no guarantee that the serial link between R1 and R2 is up. A problem in R1’s side of the serial link could bring the link down, keep PC1 from reaching PC4 and R2 would have no blame on it.

You issue a ping from R1 to R2’s serial 0/0. Since the pings were successful, you assume R2 must have some wrong information regarding network 1 placed on its routing table.

Question 2:

How the successful ping from R1 to R2 raised the odds of problems in R2’s routing table?

Answer: The successful pings from R1 to R2 serial 0/0 ensure that link is fine. Network 1 is direct connected to R1 and therefore, R1 must know how to reach network 1. Because the entire path between PC1 and R2 is ok at layer 1 and 2 levels, on this case, chances are R2 routing information is the failure point.
As a last test, you issue a **ping** from R2 to PC1 and watch them fail.

A quick look at R2’s routing table reveals the problem:

**Routing Information Known by R2:**

<table>
<thead>
<tr>
<th>Destination Network</th>
<th>Address of the Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.4.0/24</td>
<td>[directly connected]</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>[directly connected]</td>
</tr>
<tr>
<td>192.168.5.0/24</td>
<td>[directly connected]</td>
</tr>
<tr>
<td>192.168.1.0/24</td>
<td>192.168.5.1</td>
</tr>
</tbody>
</table>

**Question 3:**

Which problem on R2’s routing table keeps PC1 from reaching PC4?

**Answer:** *R2 has no route to reach network 1. In other words, R2 does not know how to send packets to network 1.*

**Question 4: (Challenge Question)**

If a ping from R1 to PC4 was issued would it be successful? Explain.

**Answer:** Yes, it would. *R2 doesn’t know how to reach network 1 (192.168.1.0/24) but it knows how to reach R1 because R1 lays in one of R2’s direct connected networks (192.168.5.0/24). R2’s routing information showed above has network 5 included on it.*

You notice the problem in R2 and manually add a static route to network 1 using R1’s interface serial0/0 IP address (192.168.5.1) as the next hop. R2’s updated routing information looks like the table shown below:

**R2’s Manually Updated Routing Information**

<table>
<thead>
<tr>
<th>Destination Network</th>
<th>Address of the Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.4.0/24</td>
<td>[directly connected]</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>[directly connected]</td>
</tr>
<tr>
<td>192.168.5.0/24</td>
<td>[directly connected]</td>
</tr>
<tr>
<td>192.168.1.0/24</td>
<td>192.168.5.1</td>
</tr>
</tbody>
</table>
A ping from PC1 to PC4 is issued and it is successful this time. Problem 1 is solved.

Problem 2 – PC1 fails reaching PC5, PC6, PC7 or any device on Network 3

Problem 2 on the report given to you via telephone claims PC1 is not able to reach PC5 or PC6. Because network 3 is also under R2, a lack of a route to network 1 into R2’s routing table could also be causing problem 2. You issue a few pings but just to realize PC1 is still not able to reach PC5, PC6 or any other device on network 3.

Question 5:

How Problem 1 (lack of a route to network 1 into R2’s routing table) could also be causing Problem 2?

Answer: Because any packet traveling from network 3 towards network 1 has to go through R2, if R2 has no route to network 1 (cause of problem 1) would keep packets originated on network 3 from reaching network 1.

Following the troubleshoot process, you check PC5, PC6 and PC7 IP configuration and it is correct: all three devices have unique IP addresses belonging to network 3 and their default gateways option are set to 192.168.3.1 (R2’s fa0/1 interface IP address). You issue pings from PC5, PC6 and PC7 to R2’s fa0/1 interface; they are all successful.

Successful pings from network 3 devices toward R2 fa0/1 interface mean that the segment linking R2 to network 3 is working fine. Based on tests conducted during problem 1 troubleshooting, the serial link between R1 and R2 can also be considered ok.

Still based on problem 1 troubleshooting, R2 has a route to network 1 (manually added by you) and network 1 devices IP configuration is ok.

You decide to check R1’s routing table. R1’s routing information is shown below:

R1’s Routing Information

<table>
<thead>
<tr>
<th>Destination Network</th>
<th>Address of the Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.0/24</td>
<td>[directly connected]</td>
</tr>
<tr>
<td>192.168.4.0/24</td>
<td>192.168.5.2</td>
</tr>
<tr>
<td>192.168.5.0/24</td>
<td>[directly connected]</td>
</tr>
</tbody>
</table>

Again, a quick look on R1’s routing information reveals the problem: R1 has no route to network 3 (192.168.3.0/24) and therefore, doesn’t know how to reach that network.
Since there is no routing protocol running on OCP's network, you manually add the missing route again. Now R1’s routing table (manually updated) looks like the table shown below:

**R1’s Manually Updated Routing Information**

<table>
<thead>
<tr>
<th>Destination Network</th>
<th>Address of the Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.0/24</td>
<td>[directly connected]</td>
</tr>
<tr>
<td>192.168.4.0/24</td>
<td>192.168.5.2</td>
</tr>
<tr>
<td>192.168.5.0/24</td>
<td>[directly connected]</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>192.168.5.2</td>
</tr>
</tbody>
</table>

On R1’s updated routing table, a route to network 3 (192.168.3.0/24) using R2’s serial 0/0 interface (192.168.5.2) as next hop, was added.

Again, you issue a few **pings** from PC1 to network 3 devices but this time they are all successful.

**Problem 3 – PC1 and PC3 reach network 3 but PC2 does not.**

To ensure problem 2 was completely solved, you decide to issue **pings** from PC2 and PC3 to network 3 but even though **pings** from PC1 and PC3 work fine, all **pings** from PC2 to network 3 fail.

**Question 6:**

Based on troubleshooting done on both previous problems, what would be your first guess to find the problem? Explain.

**Answer:** Since PC1 and PC3 are able to reach network 3, R1 and R2 are correctly routing packets between network 1 and 3. From a routing perspective, chances are the problem relates to PC2 itself.

**Note:** Packet filtering could cause problem 3 as well but it isn't being covered and studied at this document.

From PC2, you issue **pings** to different network 3 devices but with no success. Still from PC2 you issue **pings** to R1’s fa0/0. All the pings from PC2 to R1 fail but pings from PC1 and PC3 to R1’s fa0/0 are successful.

You check PC2’s IP configuration and find the problem: PC2 default gateway is set to 192.168.4.1 which is the IP address of R2’s fa0/0 interface. Since a default gateway is the network device used to reach remote networks, it must be an address **within the local network**.
You also notice PC2 has an IP address from network 4 configured (192.168.4.11/24). OCP’s people tell you know PC2 use to part of network 4, had to be moved to network 1 but nobody changed its IP configuration.

You issue a few pings from PC2 to different network 3 devices after changing default gateway information to 192.168.1.1 and the IP address to 192.168.1.2/24. The pings are now successful. Problem 3 is solved.

Note: If PC2 IP configuration was correct, the next point to check would be PC2’s cabling.

**Question 7 (Challenge Question)**

Would a network device (a user PC, for example) configured with no default gateway information, still be able to communicate to other devices? Explain.

**Answer:** Yes it would. With no default gateway information, such device wouldn’t be able to reach remote networks but would still communicate with other network devices located inside its local network. A default gateway (or default route) is only used while sending/receiving packets to/from a remote network.