

Figure 1 shows the computer network of a company NIS limited. In this network, there are six routers connecting many LANs (not shown) together. The only LAN shown in the figure is connecting routers R1 and R2, and it consists of six Ethernet switches (with their Bridge ID given). In order to provide layer 2 redundancy, the Spanning Tree Protocol (STP) is run by the switches. The figure also shows the STP cost of each layer 2 link. **Note that Figure 1 will be used by all questions in this paper.**

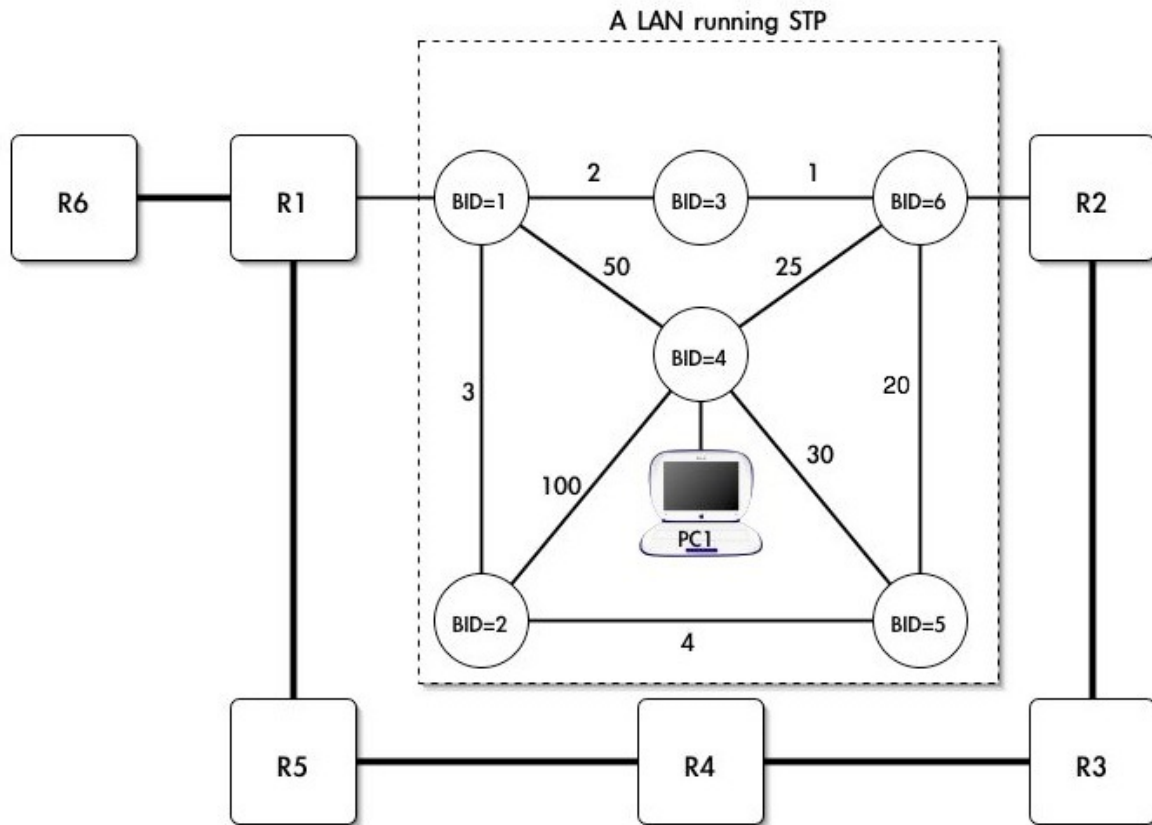


Figure 1 – The computer network of NIS limited.

Question 1 (23 marks)

In this question, please assume that all routers run a Distance Vector routing protocol.

- a) A hacker, using PC1, successfully compromises the Ethernet switch with BID=4. He wants to capture the network infrastructure signaling sending between R1 and R2. He knows that the signaling is sent by using the Ethernet Broadcast address.
 - i) Show the original spanning tree of the LAN when STP is run.
 - ii) Discuss (with good reason) whether the hacker needs to influence the STP topology in order to capture the signaling sent between R1 and R2. If it is needed, explain how he could do that.

[8 marks]

- b) After capturing the signaling, the hacker knows that the routers are running a distance vector routing protocol. He then wants to launch Man-In-The-Middle (MITM) attack.
- i) Can he launch MITM attack by using ARP poisoning? If your answer is yes, show the ARP tables of R1 and R2 *after* the attack. (Given: IP addresses of R1, R2 and PC1 are IP-R1, IP-R2 and IP-PC1 respectively. MAC addresses of R1, R2 and PC1 are MAC-R1, MAC-R2 and MAC-PC1 respectively.)
- ii) Discuss, by showing the appropriate contents of ARP messages, how he can poison the ARP tables of R1 and R2. The format of an ARP message is given for your reference:

Ethernet	
Destination:	
Source:	
Type:	ARP
ARP	
Opcode	
Sender MAC	
Sender IP	
Target MAC	
Target IP	

[13 marks]

- c) Suppose the hacker compromises also R1. He then makes R1 to send packets sourced from R2 and destined at R6 back to R2. What is the name of this attack?

[2 marks]