Computer Networks and Distributed Systems

Solutions to Questionnaire about STP and the intro to IP

Based on textbook "*Conceptual Computer Networks*" (WIP) by José María Foces Morán and José María Foces Vivancos

Context

- STP and Intro IP

1. Contrast the concept of Spanning Tree Protocol (STP) and the Spanning Tree Algorithm

   The Spanning Tree Algorithm takes as its input a graph and obtains a tree that preserves its connectivity without any loops. This algorithm can be executed by a single microprocessor or in a distributed infrastructure.

   The Spanning Tree Protocol is comprised of a set of valid messages exchanged by switches that support the Spanning Tree Algorithm. In a distributed manner, a network's switches exchange STP messages in order for them to agree on which links to deactivate so as to break existing loops.

2. Can frames *proliferate* in Switched Ethernet networks?

   a. Discuss why *frame proliferation* is to be avoided altogether
   b. Can IP packets proliferate when IP networks have loops? Compose a tentative response to this question, for the time being, since we will treat this topic when we take up IP forwarding.

3. What's the basic structure of a Bridge Configuration Message?

Assume a bridge B0 is sending its configuration message, the structure of this message is:
(B0's ID, ID of the bridge B0 believes is the root, Minimum distance from B0 to the root bridge)

4. What is the IEEE standard for Spanning Tree Protocol?

IEEE standard 802.1D

5. Assume a Switched Ethernet network that contains a few loops and that all its constituent switches are STP-capable. When the switches are powered up, each sends its initial configuration message to all their directly-connected switches, so all of them begin to agree upon which switch is root. This process continues until all the switches agree a root switch, each has elected their own root port and, finally, all the switches connected to each LAN elect a *designated bridge port.* Assume this process has finished and the STP instance is stable across the whole network, then respond to the following questions:

a. Does the root send any BPDUs (Bridge Protocol Data Units)? Explain the purpose of those BPDUs, if any?

When the STP has converged, the root bridge periodically sends its configuration message to its neighboring switches, which in turn, will send it to all its neighbors. This process guarantees that the root switch's configuration message will reach the farthest switches in the network, which will become aware all links keep being operational.

b. Do switches other than root *send* any BPDUs?

In the stable state described in the problem statement, only the root switch will send its configuration message.

c. Assume STP has disabled all the ports of a switch, could we power it off and expect the network to keep functioning ok? Please, discuss this.

The switch should remain powered up so it can reactivate some of its links if needed in case of failure of other links in order to preserve connectivity

d. *Where* is a BPDU encapsulated into?

BPDUs are encapsulated in Ethernet frames which destination address is multicast address reserved for representing all the switches in this network

e. What is the Ethertype of a BPDU?

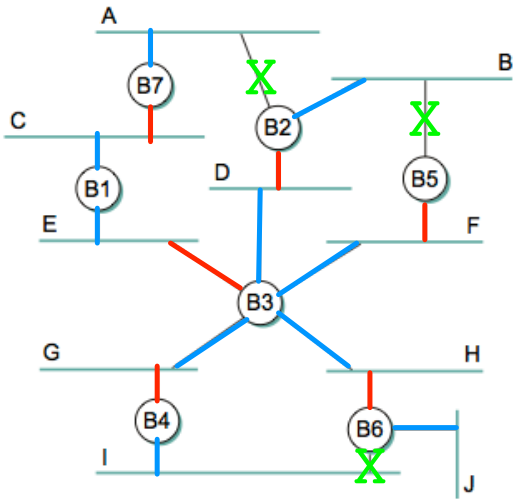
0x42

f. When a new BPDU is generated by root or forwarded by any other switch, what is the contents of the Destination MAC field of the Ethernet frame that encapsulates it? And the Source MAC?

The destination MAC contains a special, muilticast address which meaning is "all bridges". The source address is the address on that port of the bridge that is sending the config message.

6. Solve the following exercises from textbook chapter 3: 13, 14,18, 19 and 23

Ex. 13:

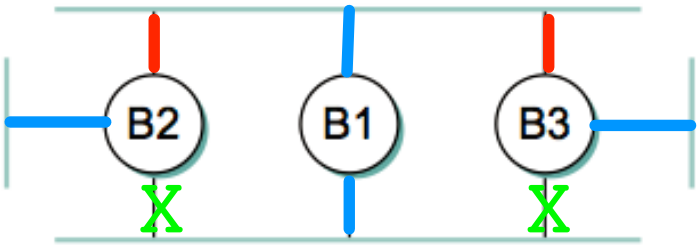


1. Root is B1
2. Root ports marked in red
3. Designated ports marked in blue

Disabled ports marked with a green X

Ex. 14: *Suppress bridge B1 and its two links from the network diagram, then, recompute the spanning tree. In this case B2 will result elected as root bridge.*

Ex. 18:

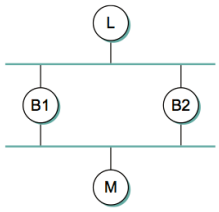


1. Root is B1
2. Root ports marked in red
3. Designated ports marked in blue

Disabled ports marked with a green X

Ties are broken by considering the lowest numbered port at each switch which are assumed to be the upper ports at each switch

Ex. 19: *When M sends to L, both switches learn M and flood the frame, assuming neither knows which port iL connected to. The flooded frame sent by B1 will be received by B2 and, viceversa, the frame flooded by B2 will be received by B1, then the switches will re-learn M assuming it is connected to the upper port and flood it again, assuming neither knows where L is connected to. This proliferation of frames will create sort of a broadcast storm, though, the involved frames are unicast frames.*



Ex. 23: *Ports of real switches have MAC addresses that allow them to break ties when two or more ports of a switch are connected to the same LAN –the least numbered (MAC) port is selected as designated bridge port on that LAN, for example.*

7. Solve exercises 1, 2 and 3 from Exam no. 3 in the following document:
   http://paloalto.unileon.es/cn/CN-ExRefSol2013.pdf

The mentioned exam document contains the solutions to questions 1,2, and 3 of exam no. 3

8. How many different IP addresses can be obtained by using IPv4?

   IPv4 uses 32-bit IP addresses, therefore the maximum number of IPs is 2^{32} = 4G IPs

9. What is CIDR? Can you explain the meaning of the CIDR prefix in the following IP address? 193.146.101.46/20

   CIDR stands for Classless Interdomain Routing, it superseded the classful addressing scheme in which three IP address classes were available for Unicast traffic.

   The CIDR prefix /20 in the above IP address means that the high 20 bits of the address represent the network number and that, therefore, the remaining 32 – 20 = 12 bits are used for numbering the hosts contained in that network.

10. What are the most important fields of an IPv4 packet mentioned in the lecture?
    Regarding the lecture mentioned in the context, above, the most important field of an IP packet are the Protocol (A layer-three multiplexing key), the source IP and the destination IP and the payload.

11. What's an IP block?
    According to the definition provided in the Lab session, an IP block is a block of consecutive IP addresses whose size is an integral power of two and whose initial address is divisible by the block's size.

12. Calculate the prefix number (Network number) and the IP broadcast address of the IP block to which 192.168.1.50/25 belongs. How do you derive the *Network Mask* from the CIDR prefix?

    The mask contains a block of 25 bits 1 and a block of 32-25 bits 0, therefore the mask is: 255.255.255.128

    For computing the IP block's prefix number (Initial or base address) we apply the bitwise AND operation between the given IP and the mask:

```
  192.168.  1. 50
& 255.255.255.128
  ---------------
  192.168.  1.  0
```

    For calculating the broadcast address, we add to the prefix number (Network number or base address) the size of the IP block minus 1:

```
  192.168.  1.  0
+             127
  ---------------
  192.168.  1.127
```

13. Explain the facets that constitute the IP Service Model

Please, consult textbook pg. 206 and 207

14. Consult the structure of an IP packet (Textbook, presentation) and respond to these questions:

a. Can you provide three instances of protocols that can be encapsulated into IP? Write down the standard multiplexing key's values

TCP (6), UDP (17), ICMP (1)

b. How many IP addresses are contained in an IP packet?

Two IPs are contained within an IP packet: the source IP and the destination IP

c. Do you remember that Ethernet's MTU is 1500Bytes?

Yes, original Ethernet's MTU is 1500Bytes or 12000 bits

d. What's the biggest IP packet that can be encapsulated into an Ethernet frame?

Since an IP packet using no options is 20Bytes in size, the biggest IP packet to be encapsulated into an Ethernet frame is 1500Bytes – 20Bytes = 1460Bytes.

e. What is IP fragmentation and what is its purpose?

IP packets can grow to sizes far bigger than those of the Ethernet, then, when an IP must traverse a link whose MTU is smaller than the IP packet's size, the router proceeds to fragment it. IP fragmentation consists of a router breaking down an incoming, big IP packet into several IP packets consistent with the link's MTU. Several IP packet's fields serve for controlling where in the original IP packet lays each fragment: Ident, flag MF and offset.