THIRD QUIZ ANSWERS

COSC 6360
October 28, 2019

Version A

First question

- How does Raft ensure that all newly elected leader are ***up to date***?

First question

- How does Raft ensure that all newly elected leader are ***up to date***?

  - □ ***Servers never vote for a candidate whose log is not as up to date as their own log.***

Second question

- How does SSH use ***HMAC SHA*-1**?

Second question

- How does SSH use ***HMAC SHA*-1**?
  - ***SSH uses HMAC SHA-1 to verify that the data exchanged between the client and the server were not tampered by a third party.***

Third question

- If Alice knows the ***public key*** of Bob, how can she send a secret message to Bob?

Third question

- If Alice knows the ***public key*** of Bob, how can she send a secret message to Bob?
  - ***She will encrypt her message with the public key of Bob.***
    - *Deciphering the message requires the knowledge of the secret key of Bob*.

Fourth question

- Why is the BitTorrent ***chunk selection policy*** poorly suited to streaming applications?

Fourth question

- Why is the BitTorrent ***chunk selection policy*** poorly suited to streaming applications
  - □ ***The BitTorrent chunk selection policy makes downloaders select the rarest chunks without regard to any timing constraints.***

Fifth question

- Consider a ***RAID level 5*** disk array with ten disks.
- How many disk reads and disk writes will be required to update the value of a single block assuming we ***already know*** the previous value of the block being updated?

  □ **Answer: ____ reads and ___ writes.**

Fifth question

- Consider a ***RAID level 5*** disk array with ten disks.
- How many disk reads and disk writes will be required to update the value of a single block assuming we ***already know*** the previous value of the block being updated?

  - **Answer: one read~~s~~ and two writes.**

Explanation

- We have the old value of the data block d_{old}
- We read the old value of the parity block p_{old}
- We compute the new value of the parity block
  - □ $p_{new} = d_{old} \oplus d_{new} \oplus p_{old}$
- We write to disk
  - □ The new value of the data block d_{new}
  - □ p_{new}

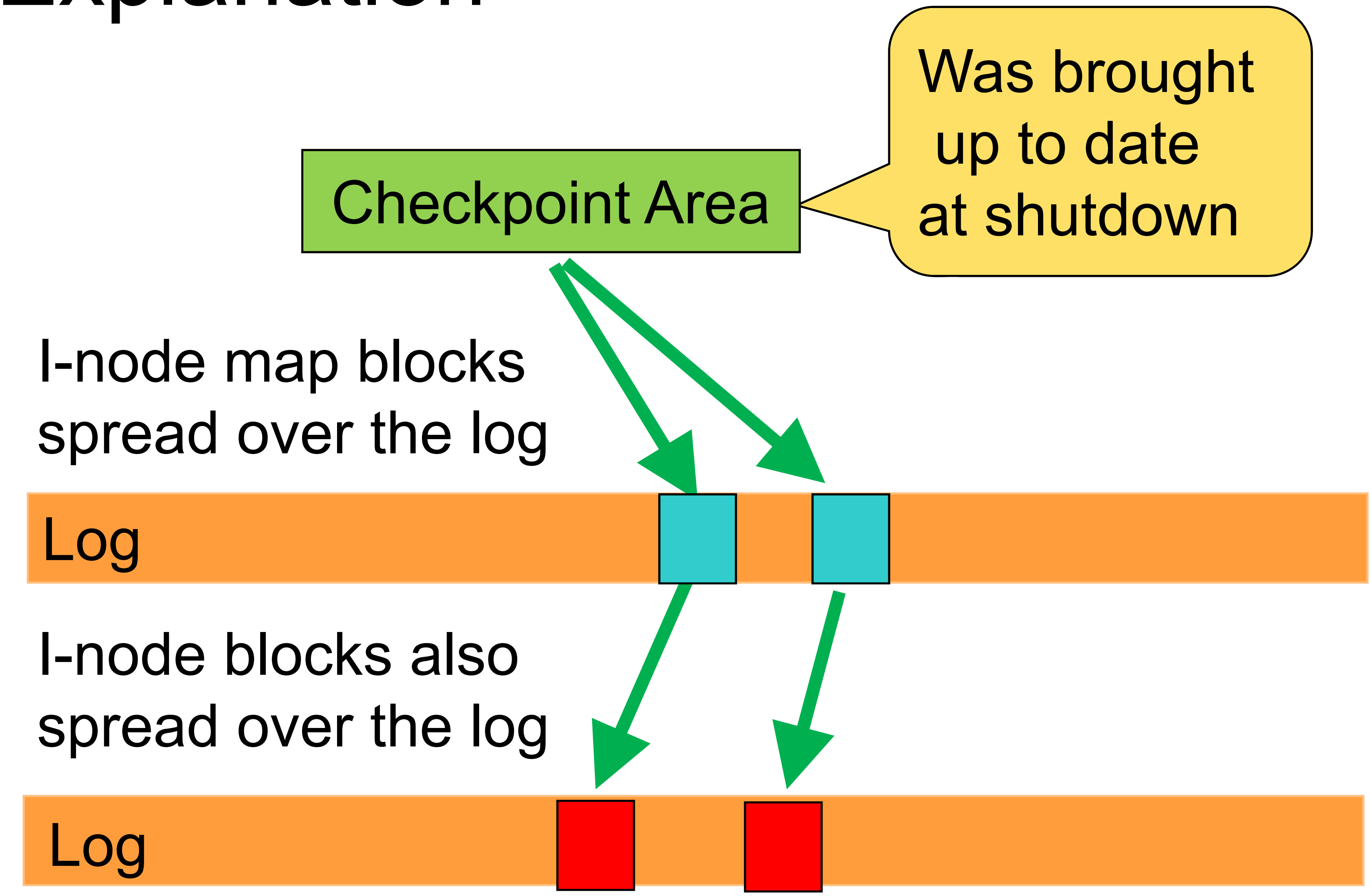
Sixth question

- Consider a ***log-structured file system*** (LFS) that is being accessed ***immediately after*** the system has been rebooted.
- Assuming that a final checkpoint was taken when the system was powered down, which steps must be taken to access a specific i-node.

Sixth question

- Fetch *specific block of i-node map block addresses*
  located in checkpoint area
- Fetch *specific i-map block*
  whose address is given by *block of i-node map block addresses*
- Fetch i-node block whose address is given by *i-map block*

Explanation



Checkpoint Area

Was brought up to date at shutdown

I-node map blocks spread over the log

Log

I-node blocks also spread over the log

Log

Seventh question

- Why does NFS use ***stateless servers***?

Seventh question

- Why does NFS use ***stateless servers***?
  - ***NFS use stateless servers because stateless servers can be restarted after a crash without impacting user behavior***.

Seventh question

- What is their ***main drawback***?

Seventh question

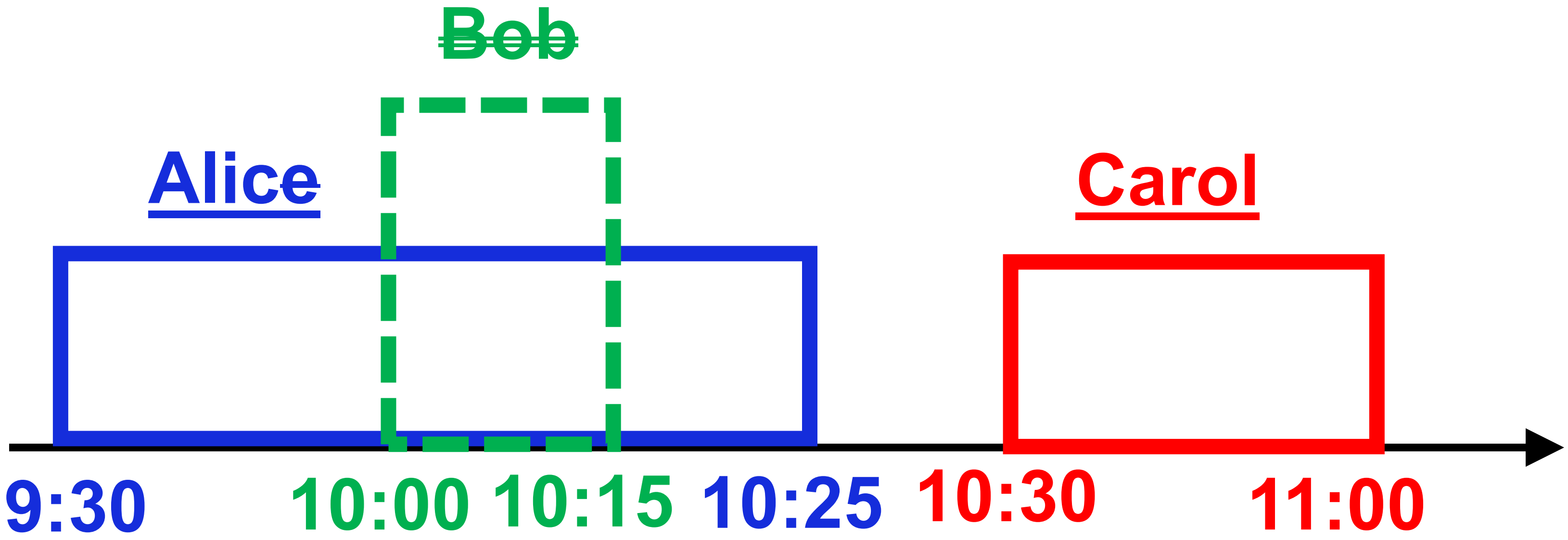
- What is their ***main drawback***?
    - ***Stateless servers cannot detect whether***
        - ***A single client accesses a given file***
        - ***Multiple clients access the file***

Seventh question

- Consider a distributed file system implementing ***close-to-open consistency***. Assuming that
  - □ Alice opens the file at 9:30 AM, modifies it and closes it at 10:25 AM,
  - □ Bob opens the file at 10:00 AM, modifies it and closes it at 10:15 AM,
  - □ Carol opens the file at 10:30 AM, modifies it and closes it at 11:00 AM.

Seventh question

- Which of these three users would see his or her changes incorporated in the final version of the file?



Version B

First question

- Which technique does Raft use to reduce the risk of ***split votes*** in ***leader elections***?

First question

- Which technique does Raft use to reduce the risk of ***split votes*** in ***leader elections***?
  - ***Raft uses randomized election timeouts to increase the chances that a single follower will detect the loss of the leader before the others.***

Second question

- How does SSH use ***HMAC SHA*-1**?

Second question

- How does SSH use ***HMAC SHA*-1**?
  - ***SSH uses HMAC SHA-1 to verify that the data exchanged between the client and the server were not tampered by a third party.***

Third question

- If Alice knows the ***public key*** of Bob, how can Bob send her signed messages?

Third question

- If Alice knows the ***public key*** of Bob, how can Bob send her signed messages?
  - ***He will encrypt his messages with his secret key .***
    - *Anyone can decipher these messages.*
    - *Only Bob can have written them.*

Fourth question

- Why is the BitTorrent ***chunk selection policy*** poorly suited to streaming applications?

Fourth question

- Why is the BitTorrent ***chunk selection policy*** poorly suited to streaming applications
  - ***The BitTorrent chunk selection policy makes downloaders select the rarest chunks without regard to any timing constraints.***

Fifth question

- Consider a ***RAID level 5*** disk array with ten disks.
- How many disk reads and disk writes will be required to update the value of a single block assuming we ***do not know*** the previous value of the block being updated?

  - □ **Answer: ____ reads and ___ writes.**

Fifth question

- Consider a ***RAID level 5*** disk array with ten disks.
- How many disk reads and disk writes will be required to update the value of a single block assuming we ***already know*** the previous value of the block being updated?
  - □ **Answer: two reads and two writes.**

Explanation

- We read
  - □ The old value of the data block d_{old}
  - □ The old value of the parity block p_{old}
- We compute the new value of the parity block
  - □ $p_{new} = d_{old} \oplus d_{new} \oplus p_{old}$
- We write to disk
  - □ The new value of the data block d_{new}
  - □ p_{new}

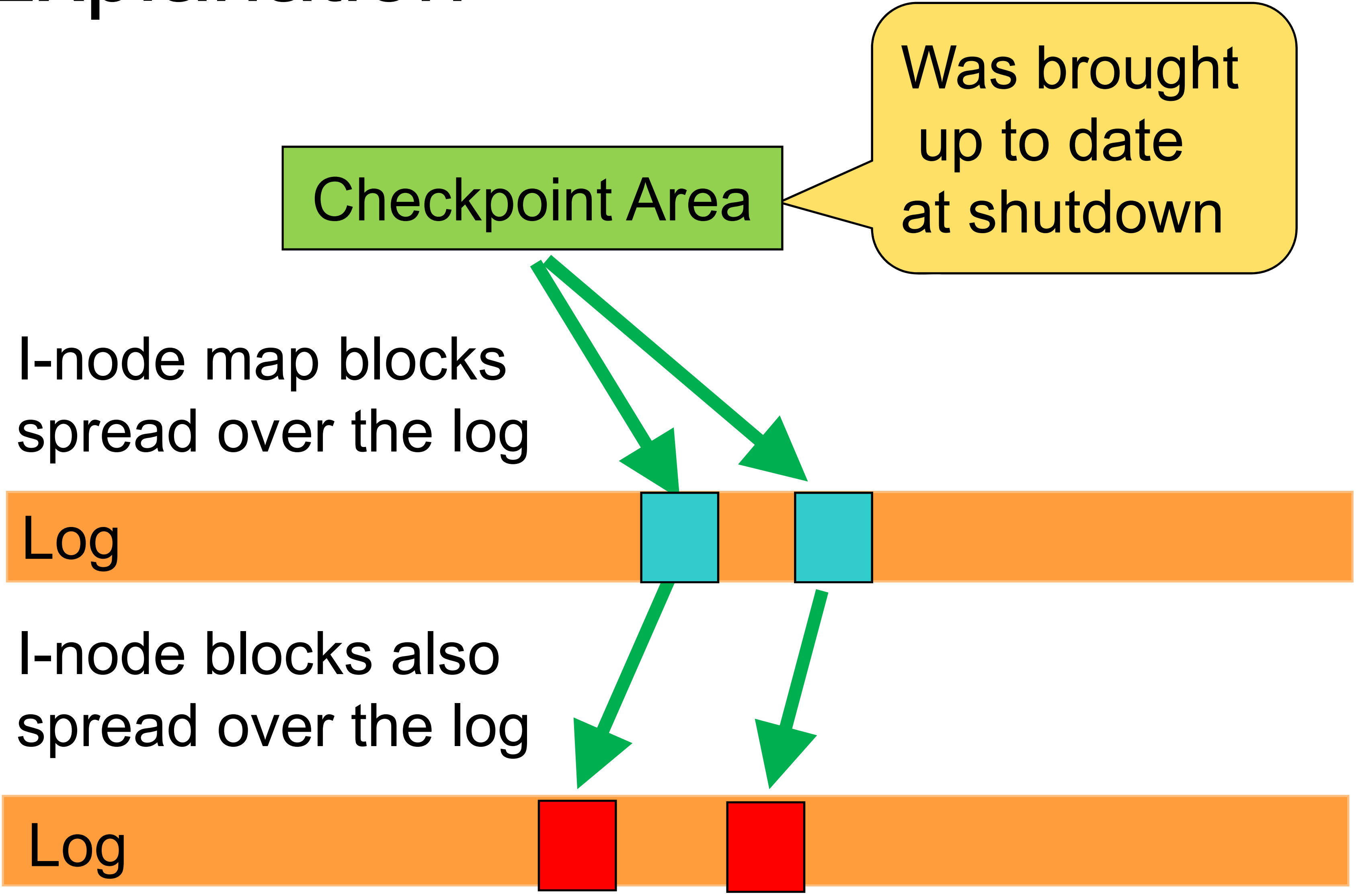
Sixth question

- Consider a ***log-structured file system*** (LFS) that is being accessed ***immediately after*** the system has been rebooted.
- Assuming that a final checkpoint was taken when the system was powered down, which steps must be taken to access a specific i-node.

Sixth question

- **Fetch** ***specific block of i-node map block addresses***
  located in checkpoint area
- **Fetch** ***specific i-map block***
  whose address is given by ***block of i-node map block addresses***
- **Fetch i-node block whose address is given by** ***i-map block***

Explanation



Checkpoint Area

Was brought up to date at shutdown

I-node map blocks spread over the log

Log

I-node blocks also spread over the log

Log

Seventh question

- What is the main advantage of ***stateless servers***?

Seventh question

- What is the main advantage of ***stateless servers***?
  - ***NFS use stateless servers because stateless servers can be restarted after a crash without impacting user behavior***

Seventh question

- What is their ***main drawback***?

Seventh question

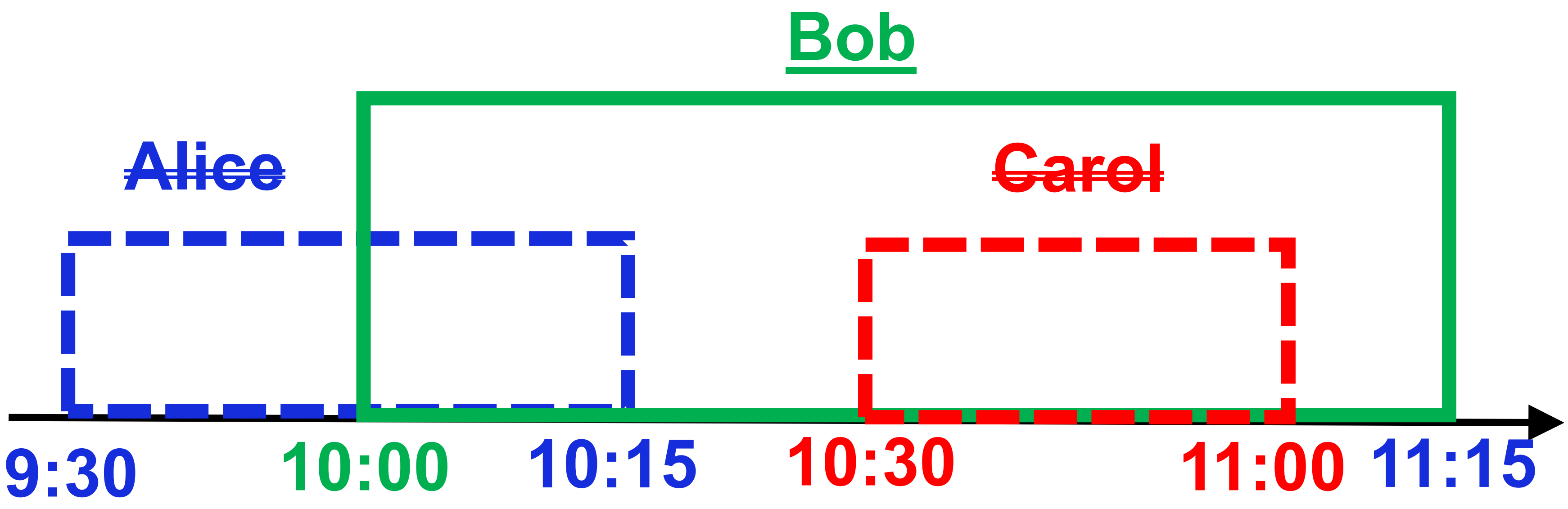
- What is their ***main drawback***?
  - ***Stateless servers cannot detect whether***
    - ***A single client accesses a given file***
    - ***Multiple clients access the file***

Seventh question

- Consider a distributed file system implementing ***close-to-open consistency***. Assuming that
  - Alice opens the file at 9:30 AM, modifies it and closes it at 10:15 AM,
  - Bob opens the file at 10:00 AM, modifies it and closes it at 11:15 AM,
  - Carol opens the file at 10:30 AM, modifies it and closes it at 11:00 AM.

Seventh question

- Which of these three users would see his or her changes incorporated in the final version of the file?


Bob
~~Alice~~
~~Carol~~
9:30
10:00
10:15
10:30
11:00
11:15