LEARN

Lanka Education and Research Network

LEARN Zoom Good Practices Guide (http://learn.zoom.us)

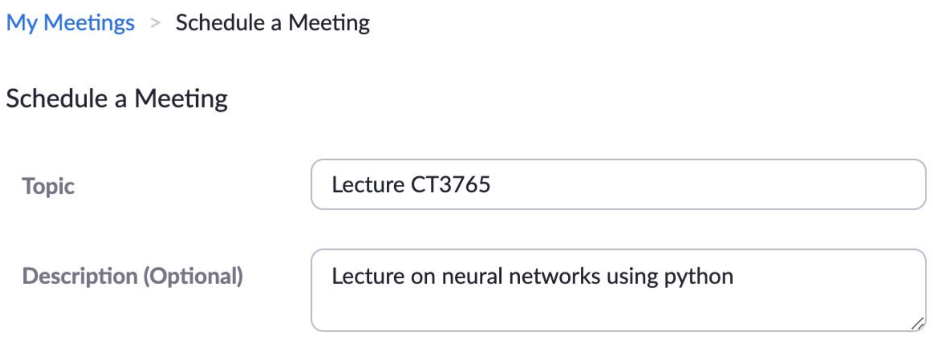
LEARN has hosted Zoom servers within our premises (Zoom On-Premise deployment). This means, that those who are starting a meeting via https://learn.zoom.us will have their meeting data traffic routed to the LEARN hosted servers which will not consume additional data from your ISP provided data bundle. However, since learn.zoom.us is hosted in Zoom cloud (which is hosted outside the country), each such meeting will consume a little data (a maximum of a few MBs) for authentication and sharing metadata.

We would like all members to note that although these services are coming free of charge for them, it is NOT free for all. LEARN is bearing the cost of these licenses and both LEARN and the ISPs are bearing the cost for the data charges. Therefore, both LEARN and the ISPs are incurring cost to provide this service free for the users and kindly requesting all the users to use it with more responsibility.

During the Zoom meetings, we request the users to always keep only screen sharing with video thumbnail while assuring others keep both microphone and video turned off unless they are talking. Such a meeting will consume about 10 times lesser data than a meeting with all the videos and mics on with large size video. Therefore, please avoid overloading the system with good practices. Further, if the data is charged, for an economical meeting as recommended, it should cost a user less than Rs 10/hour compared a meeting without careful use of the technology that will cost ten times more.

Here are some guidelines we made for ALL users to follow for the best use of the limited resources we have.

1. Appropriate meeting *Topic* and the *Description* should be added to briefly explain the official purpose of the meeting. Otherwise, the meeting could be terminated by the authority and audited.



My Meetings > Schedule a Meeting

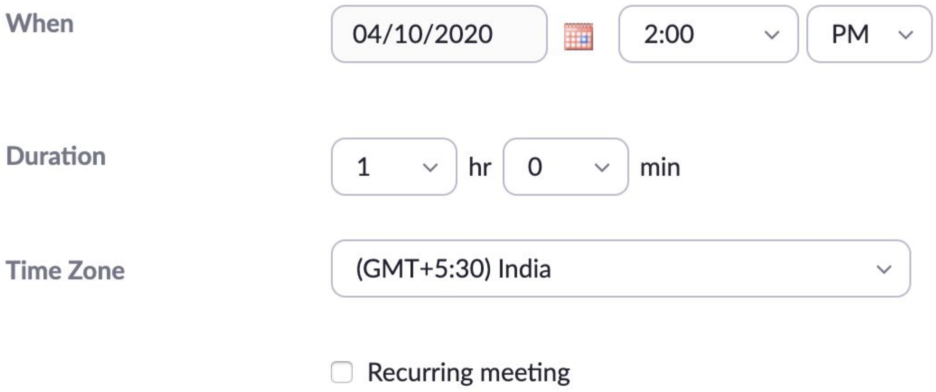
Schedule a Meeting

Topic: Lecture CT3765

Description (Optional): Lecture on neural networks using python

Figure: Example Topic and Description

2. Define the exact start time and duration. If it is a recurrence meeting, mention it too.



When 04/10/2020 2:00 PM

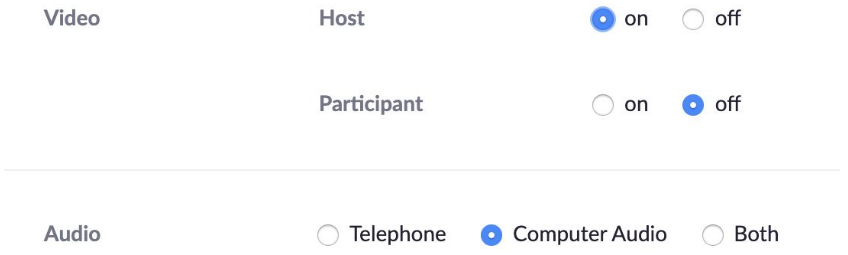
Duration 1 hr 0 min

Time Zone (GMT+5:30) India

☐ Recurring meeting

Figure: Example Time/Duration

3. When Configuring Video Audio Options, make sure you off participant's video on login and to select Computer Audio as the Audio method

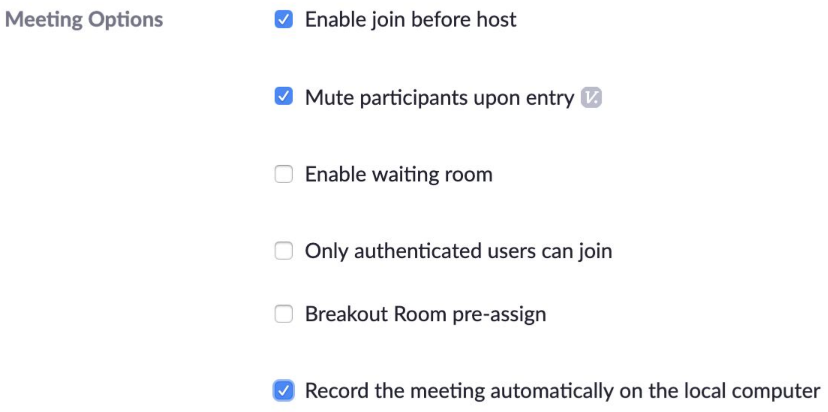


Video Host ● on ○ off

Participant ○ on ● off

Audio ○ Telephone ● Computer Audio ○ Both

4. On rest of the functions;
   Enable Join Before Host
   Mute participants upon entry
   Record meetings automatically on local computer



Meeting Options

☑ Enable join before host

☑ Mute participants upon entry

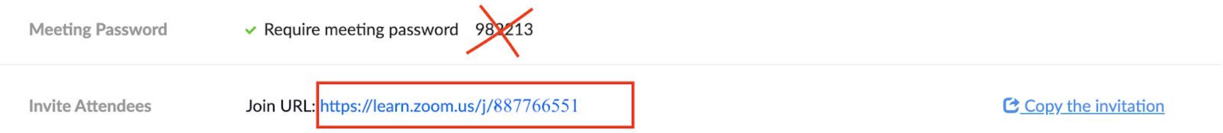
☐ Enable waiting room

☐ Only authenticated users can join

☐ Breakout Room pre-assign

☑ Record the meeting automatically on the local computer

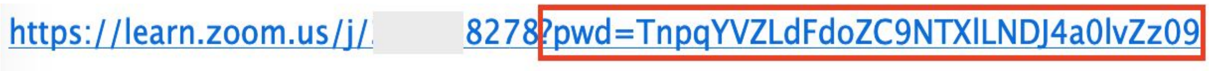
5. Use a password for the meeting and share it by other means (SMS, WhatsApp group, etc) without posting it on the same email of meeting invitation. Meeting Join URL is more than enough when inviting students.



Meeting Password ✓ Require meeting password ~~982213~~

Invite Attendees Join URL: https://learn.zoom.us/j/887766551

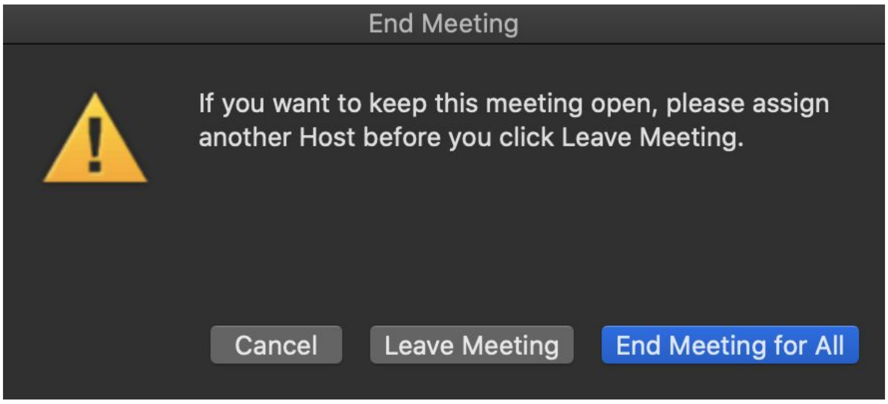
6. If your Meeting URL contains "?pwd=....." after the meeting id digits, remove the whole part starting from "?" symbol before sharing.



https://learn.zoom.us/j/[redacted]8278?pwd=TnpqYVZLdFdoZC9NTXlLNDJ4a0lvZz09

7. Each meeting consumes expensive technology and resources (computing, storage, network bandwidth). Therefore the facility should be optimally used.

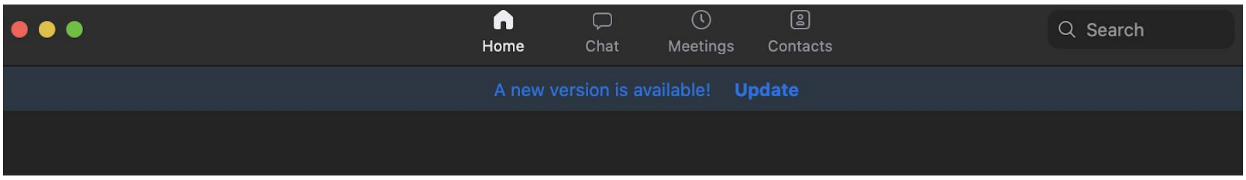
   The meeting should be ended for all participants when finished to free up the resources



If you want to keep this meeting open, please assign another Host before you click Leave Meeting.

8. Zoom system provides complete auditing information. Therefore, we are able to see any miss appropriations and miss-use of the system. Due to the nature of the system, please apply the fair use policy at all times. We have no other option than reporting violators to the authorities.

9. If you are using desktop/mobile app, update the zoom installation as frequently as possible to avoid threats



A new version is available! Update

Here is a guide from PC Magazine Regarding Securing Zoom.

10 WAYS TO SECURE ZOOM!

1 Use a Unique ID for Large or Public Zoom Calls

When you schedule a Zoom meeting, look for the Meeting ID options and choose Generate Automatically. Doing so plugs up one of the biggest holes that Zoom-bombers can exploit.

2 Require a Meeting Password

One way to protect the meeting is to require a password. You can give the password out only to those who have replied and seem credible. To password-protect a meeting, start by scheduling a meeting and checking the box next to Require meeting password.

3 Create a Waiting Room

When participants log into the call, they see a Waiting Room screen, the host, lets them in. You can let people in all at once or one at a time, which means if you see names you don't recognize in the Waiting Room, you don't have to let them in at all.

4 Only the Hosts Should Share Their Screen

Make sure your settings indicate that the only people allowed to share their screens are hosts.You can enable this setting in advance as well as during a call.

5 Create an Invite-Only Meeting

Only people who can join the call are those you invited, and they must sign in using the same email address you used to invite them.

6 Lock a Meeting Once It Starts

While the meeting is running, navigate to the bottom of the screen and click Manage Participants. The Participants panel will open. At the bottom, choose More > Lock Meeting.

7 Kick Someone Out or Put Them on Hold

During the call, go to the participants pane on the right. Hover over the name of the person you want to boot and when options appear, choose Remove.

8 Disable Someone's Camera

If someone is being rude or inappropriate on video, the host can open the Participants panel and click on the video camera icon next to the person's name.

9 Prevent Animated GIFs and Other Files in the Chat

In the chat area of a Zoom meeting, participants can share files, including images and animated GIFs—if you let them.

10 Disable Private Chat

Open Settings in the Zoom web app (it's not in the desktop app). On the left side, go to Personal > Settings. Then click In Meeting (Basic). Scroll until you see Private chat. When the button is gray, it's disabled.

Info Credit: https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing

Design: Liberty Leadership Development, LLC