# STANDARD OPERATING PROCEDURES FOR HOLDING COURT PROCEEDINGS THROUGH VIDEO CONFERENCING

## 1. METHODS OF VIDEO CONFERENCING

a) **Offsite/Remote Location Video Conferencing -** In this type of Video Conferencing the host Court is connected to the Advocates/Litigants present at a remote location i.e. their respective home or office. Such Video Conferencing is done through internet/cloud.

**ILLUSTRATION**

In GR Case Number 1/2020 pending before the Court of S.D.J.M. the Prosecution Counsel and the Defence counsel express desire to appear from remote location i.e. say from the office of the Public Prosecutor and private chamber respectively. A web link shall be created for VC with the Court of S.D.J.M. and shall be provided to the said Advocates. When the relevant proceeding commences, the Court and the Advocates mentioned above can remain connected to the Virtual Court Room through internet (by remaining at their respective remote locations) and participate therein by using the aforementioned link.

b.) **Onsite Video Conferencing -**

In this type of Video Conferencing all the participants are in the same premises (Court building) but in different rooms. We essentially have to provide this type of VC facility to those Advocates and litigants who cannot on their own arrange resources for Video Conferencing. Particular location/locations is/are to be earmarked for this purpose in the concerned Court building. We may call them **Advocates Points** for the sake of reference. There may be as many Advocate Points for the number of Court which shall function through Video Conferencing or there may be lesser number of such points with scheduling done to let more than one Court use the same Advocate Point by scheduling the proceeding time of their respective cases by way of mutual arrangement.

When proceeding commences, the Court (Presiding Officer) and the corresponding Advocates Point can remain connected through video conferencing but this time the connectivity can be through both i.e. LAN based Jitsi or cloud (internet) based Jitsi.

LAN connectivity in Onsite Video Conferencing can be conveniently achieved by installing *Jitsi* Open source Video conferencing software in a separate local server of the Judgeship, so that there would be no requirement of internet to hold Onsite Video Conferencing as *Jitsi* Video Conferencing software would now be available in LAN of that Court Complex.

c.) **Mixed Mode Video Conferencing -**

If any particular case involves Advocates / Parties some of whom want to appear both, from home as well through Onsite VC facility, then in such case the connection has to be made through Cloud *Jitsi* and even though some Advocates/Parties may be at Advocate Point in the Court building, they as well as the Advocates appearing from home/office have to be connected through cloud Jitsi by using internet.

## 2. NETWORK CONNECTIVITY

Steps are being taken to install Jitsi in separate local servers (which are not Live CIS servers) of various Judgeships for ensuring proper Onsite Video Conferencing. (Please refer to Annexure – A below for Manual/Guide for Installing Jitsi in local server)

For ensuring proper Offsite/Remote Location Video Conferencing, steps are also being taken for allowing IPs of all concerned Court Complexes to access *Cloud Jitsi* on MPLS network.

## 3. INFRASTRUCTURE

a. Establishing Advocate Points for Onsite Video Conferencing – This may be any Court Room or Bar Association hall depending on availability.

One way of having adequate number of Advocates Points may be to explore using empty courtrooms. Alternatively, if only Advocates Point is available, cases of various Courts can be scheduled one after another so that Advocates can appear for their respective cases in the single Advocates Point in a Court Complex.

b. Hardware – Desktop, LAN Connectivity, Camera, Microphone, Speaker. If possible power back up may be provided to prevent abrupt termination of Video conferencing in case of power failure.

If most Courtrooms already have hardware, means may be explored to provide hardware to Advocates Point only.

Desktop Computer with Camera (either with inbuilt microphone or separate microphone) and external speaker (if such speaker is not already available in the computer) may be provided to Court points and Advocates point. It may please be remembered that every Presiding Officer is expected to have an official laptop which may have inbuilt camera and microphone as well as speaker. Wherever necessary, these laptops can be conveniently used by concerned Presiding Officer for Video Conferencing at Court side.

## 4. NATURE OF VIRTUAL PROCEEDINGS

Pending finalization of Rules in this regard, at present only such proceedings may be conducted through video conferencing which do not involve recording of evidence rather which involve making of oral submissions by Advocates/Parties. E.g. bail hearing, misc. applications, final arguments in trial etc. (This list is only suggestive).

## 5. GENERAL PROCEDURE FOR INFORMING ADVOCATES AND CONDUCTING PROCEEDINGS THROUGH VIDEO CONFERENCING

i. Advocates and Parties may be intimated about Video Conferencing Courts through a general notice which should contain the location for Advocates Point where they will appear and make their oral submission through video conferencing to the concerned Court.

ii. A dedicated email ID should be created where Advocates/parties desirous of appearing from home/office etc can submit their willingness in this regard alongwith case details for which they intend to appear. If they intend to appear through Onsite Video Conferencing, then they must also clearly state this fact in their email.

iii. If request is for appearing through Onsite VC then they must be intimated the location where such Onsite VC facililty has been arranged.

iv. If request is for appearing from home/office then VC link has to be provided to such Advocates by reply e-mail.

v. System Officers/System Assistants and DSAs/TSAs alongwith concerned Court staff should be involved to regulate VC proceedings (Onsite/Offsite) for the concerned Courts.

vi. A Helpline Number should be notified to assist Advocates/Parties who intend to appear before Courts through VC.

*N.B. For any clarification or guidance, Technical Personnel may be directed to contact Central Project Coordinator at 8763332660 immediately.*

## ANNEXURE -A
## SELF HOSTING GUIDE (ON UBUNTU 16.04 SERVER)

This guide helps you host your own Jitsi Server on a separate local servers (which are not Live CIS servers)

*Required packages and repository updates. Make sure your system is up-to-date and required packages are installed. Retrieve the latest package versions across all repositories*

```
#sudo apt-get update
```

**Ensure support is available for apt repositories served via HTTPS*

```
#sudo apt install apt-transport-https
```

*GNU privacy guard - a free PGP replacement (new v2.x).GnuPG is GNU's tool for secure communication and data storage. It can be used to encrypt data and to create digital signatures.*

```
#sudo apt-get update -y
#sudo apt-get install -y gnupg2
```

*On Ubuntu systems, Jitsi requires dependencies from Ubuntu's universe package repository. To ensure this is enabled, run this command:*

```
#sudo apt-add-repository universe
```

**Retrieve the latest package versions across all repositories*

```
#sudo apt-get update
```

Enable Curl in Ubuntu System

```
#sudo apt-get install libssl-dev
#sudo apt-get install curl
```

*Add the Jitsi package repository and update the list of available packages.This will modify your Debian or Ubuntu system package sources to make available the Jitsi Meet packages.*

```
#curl https://download.jitsi.org/jitsi-key.gpg.key | sudo sh -c 'gpg --dearmor > /usr/share/keyrings/jitsi-keyring.gpg'
```

```
#echo 'deb [signed-by=/usr/share/keyrings/jitsi-keyring.gpg] https://download.jitsi.org stable/' | sudo tee /etc/apt/sources.list.d/jitsi-stable.list > /dev/null
```

**Retrieve the latest package versions across all repositories*

```
#sudo apt-get update
```

*Setup and configure firewall. The following ports need to be open in your firewall, to allow traffic to the Jitsi Meet server:*

- *80 TCP - for SSL certificate verification / renewal with Let's Encrypt*
- *443 TCP - for general access to Jitsi Meet*
- *4443 TCP - for fallback network video/audio communications (when UDP is blocked for example)*
- *10000 UDP - for general network video/audio communications*
- *22 TCP - if you access you server using SSH (change the port accordingly if it's not 22)*

*If you are using ufw, you can use the following commands:*

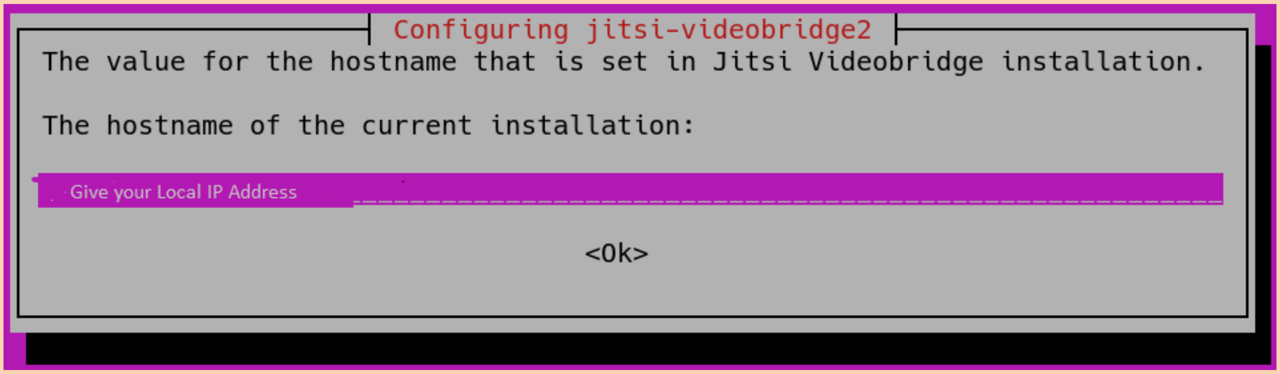
```
#sudo ufw allow 80/tcp
#sudo ufw allow 443/tcp
#sudo ufw allow 4443/tcp
#sudo ufw allow 10000/udp
#sudo ufw allow 22/tcp
#sudo ufw enable
```

*Make sure the firewall status with:*

```
#sudo ufw status verbose
```

**<u>INSTALL Jitsi Meet</u>**

```
#apt-get -y install jitsi-meet
```

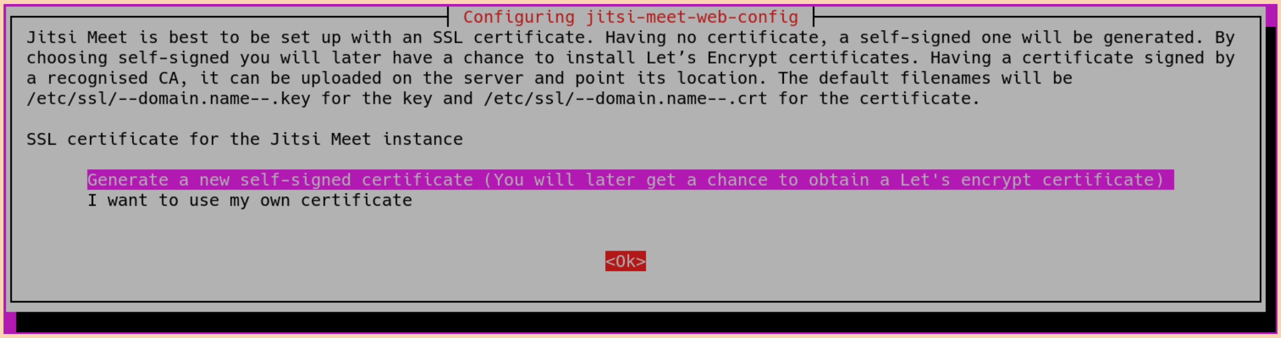


```
Configuring jitsi-videobridge2
The value for the hostname that is set in Jitsi Videobridge installation.

The hostname of the current installation:

Give your Local IP Address

                              <Ok>
```



```
Configuring jitsi-meet-web-config
Jitsi Meet is best to be set up with an SSL certificate. Having no certificate, a self-signed one will be generated. By
choosing self-signed you will later have a chance to install Let’s Encrypt certificates. Having a certificate signed by
a recognised CA, it can be uploaded on the server and point its location. The default filenames will be
/etc/ssl/--domain.name--.key for the key and /etc/ssl/--domain.name--.crt for the certificate.

SSL certificate for the Jitsi Meet instance

      Generate a new self-signed certificate (You will later get a chance to obtain a Let's encrypt certificate)
      I want to use my own certificate


                                                          <Ok>
```

Generate a new self-signed certificate option

*Generate a Let's Encrypt certificate (optional, recommended)*

**#sudo /usr/share/jitsi-meet/scripts/install-letsencrypt-cert.sh**

While asking for email address press enter

**UNINSTALL**

**#sudo apt purge jigasi jitsi-meet jitsi-meet-web-config jitsi-meet-prosody jitsi-meet-turnserver jitsi-meet-web jicofo jitsi-videobridge2**

Sometimes the following packages will fail to uninstall properly:

- jigasi
- jitsi-videobridge

When this happens, just run the uninstall command a second time and it should be ok. The reason for the failure is that sometimes the uninstall script is faster than the process that stops the daemons. The second run of the uninstall command fixes this, as by then the jigasi or jitsi-videobridge daemons are already stopped.

****