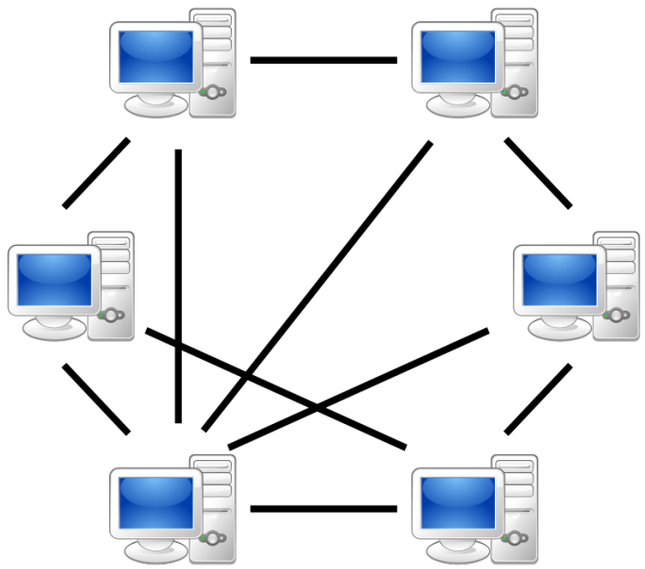
waag
technology & society

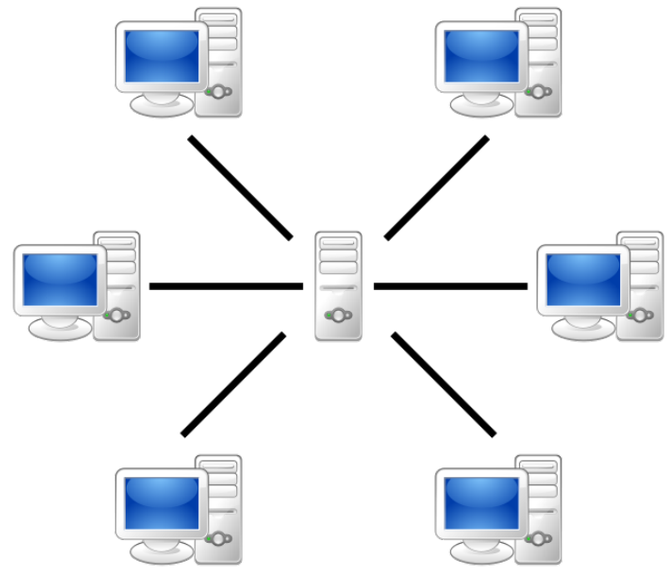
Video Conference tools

Stefano Bocconi
stefano@waag.org

Network architecture



Peer to peer



Client server

- In peer to peer, no server -> no external party that sees your data
- More private, not necessarily more secure

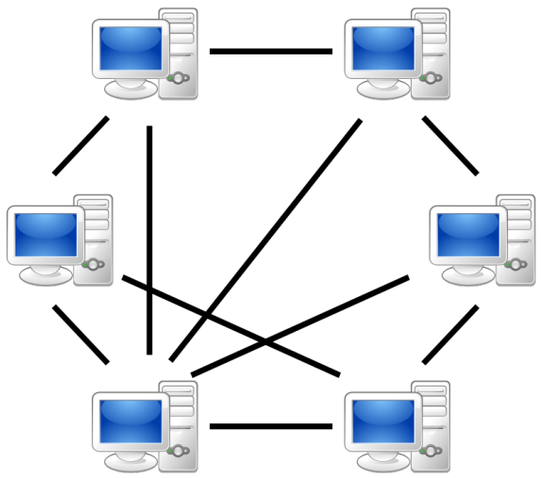
Two phases

1) Find each other, call and be called

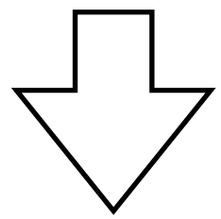
2) Communicate with each others

created by freepik

Find each other - peer to peer

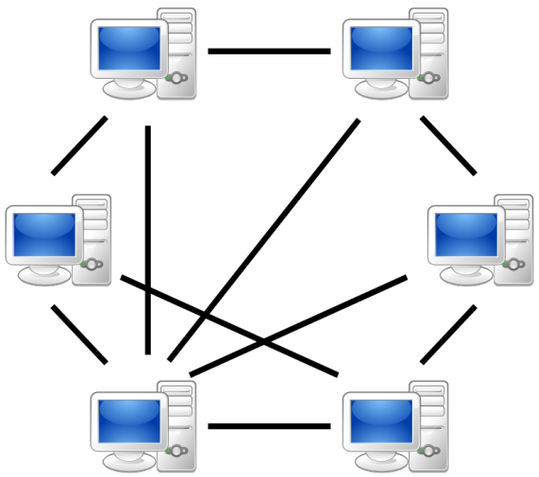


- Each node keeps track of who the other nodes are
- Each node listens for incoming calls



- Your application needs to continuously run: impossible for mobile users
- Nodes come and go, a problem for contact discovery and other features

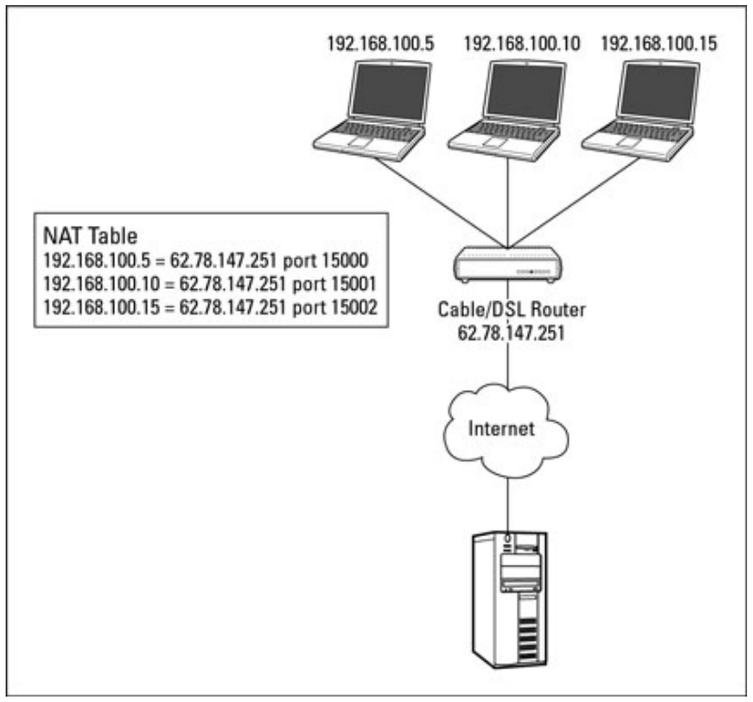
Communicate - peer to peer



- Each node transmit to each other node
- There is not resource bottleneck due to a server, just each node’s limitation in terms of bandwidth and processing power

All good?

Communicate - peer to peer



- **N**etwork **A**ddress **T**ranslation:
  - Your IP address is not visible outside your network
  - It cannot be reached by an external party, unless you initiate the connection

- Two solutions:
- **STUN** only one client behind a NAT -> discover its visible address using an external server
- **TURN**: all traffic goes through an external server
- They both require a …….. server!!

There is always (at least) one server

- **Signalling** might be visible to servers?
  - Less sensitive, but still sensitive?
- **Content** should not be visible to servers!!
- In general there are two types of **security**:
  - **Transport-level encryption** (like HTTPS): safe against snooping of the network traffic, the server sees the content
  - **End to End encryption**: only the endpoints see the content

End to end encryption

- Endpoints need to encrypt the content and manage the encryption keys
- Example of **fake** end to end encryption:
  - The server chooses the **encryption keys** and distributes it to every endpoint (Zoom)
  - The server is one of the **endpoints** because you asked for it (for example when recording the meeting, or allowing people to phone in)
  - **Intelligent server functions** such as detect who is talking, and reduce everybody else's resolution/data rate
- More work for the client side.

Who does End to end encryption?

Open source

- Jitsi: NO (there are plans)
- Jami: YES (a quasi peer to peer solution with 4 servers)
- SylkServer: NO
- Signal: YES (peer to peer communication unless NAT or IP hiding)
- BigBlueButton: NO

Commercial

- Zoom: NO (maybe in the future)
- WebEx: YES but some functionality removes it

You are your server

- Can you run your own server? Or do you trust an organisation that runs a server?
  - Then you should not have servers spying on you
- BUT keep into account that:
  - Well meant volunteers are setting up for ex. Jitsi instances to allow people to communicate during the corona-crisis
  - Many do not have cybersecurity experience.
  - Risk for the safety and privacy of the citizens using these services.

Conclusions

- Pure peer to peer seems not to be possible, but some solutions are more peer to peer than others
- End to End encryption is a good thing, but not easy to implement (right).
- The more you think you need privacy and security, the more you need to be careful with what you choose.
- The homogeneity (all Mac users?) and size of the group is a factor in the solution.

Questions?

Resources

- Why is Jami truly distributed?
- Video Conference Tools