XMPP :Extensible Messaging Presence Protocol

Prof SRN Reddy@ IGDTUW

XMPP

X : It means e**X**tensible.

M: XMPP is designed for sending **Messages** in real time. It has very **efficient push mechanism** compared to other protocols.

P : It determines **Presence** whether you are online/offline/busy. It indicates the state.

P : XMPP is a protocol, that is, a set of standards that allow systems to communicate with each other.

- Used for streaming XML elements over a network in order to exchange messages and presence information in close to real time.
- This protocol is mostly used by instant messaging applications like WhatsApp
- XMPP is a open source project which can be changed or extended according to the need.
- Security: native support for pluggable authentication (via SASL) and leading-edge security (via TLS)

Features

- XMPP is based on client-server architecture
- Clients don’t communicate directly, they do it with the help of server
- There is no centralized XMPP server
- Each XMPP client is identified by JID (Jabber ID).
- JID identifies you on the **Jabber** network.

XMPP

- Powerful, open sourse , secure, standards-based application layer protocol.
- It is a freely-available technology for real-time communication
- Used for a wide range of applications including
  - instant messaging
  - presence
  - collaboration
  - voice and video calling
  - Internet of Things[m2m]
  - tactical military messaging
  - mobile cloud push etc.
- XMPP is also well suited to machine-to-machine signaling systems

- **Open** — free, open, public, and easily understandable;
- **Components-** multiple implementations exist in the form clients, servers, server components, and code libraries.
- **Standard** — the Internet Engineering Task Force (IETF) has formalized the core XML streaming protocols as an approved instant messaging and presence technology.
- **Proven** —There are tens of thousands of XMPP servers running on the Internet today, and millions of people use XMPP for instant messaging through public services such as Google Talk and XMPP deployments at organizations worldwide.
- **Decentralized** - anyone can run their own XMPP server, enabling individuals and organizations to take control of their communications experience.
- **Secure** — any XMPP server may be isolated from the public network (e.g., on a company intranet) and robust security using SASL and TLS has been built into the core XMPP specifications. bar even further.
- **Extensible** — using the power of XML, anyone can build custom functionality on top of the core protocols; to maintain interoperability, common extensions are published in the XEP series, but such publication is not required and organizations can maintain their own private extensions if so desired.
- **Flexible** — XMPP applications beyond IM include network management, content syndication, collaboration tools, file sharing, gaming, remote systems monitoring, web services, lightweight middleware, cloud computing
- **Diverse** — a wide range of companies and open-source projects use XMPP to build and deploy real-time applications and services

Applications

Google: Google Cloud Messaging.

Facebook: Facebook Chat integration.

North Atlantic Treaty Organization (NATO): Tactical Chat(TC). [TC is a near-real-time, multi-participant **means** of textually communicating among military units for predominantly jam free communications, similar to radio voice communications, over the internet].

Thousands of companies: **I**nstant messaging.

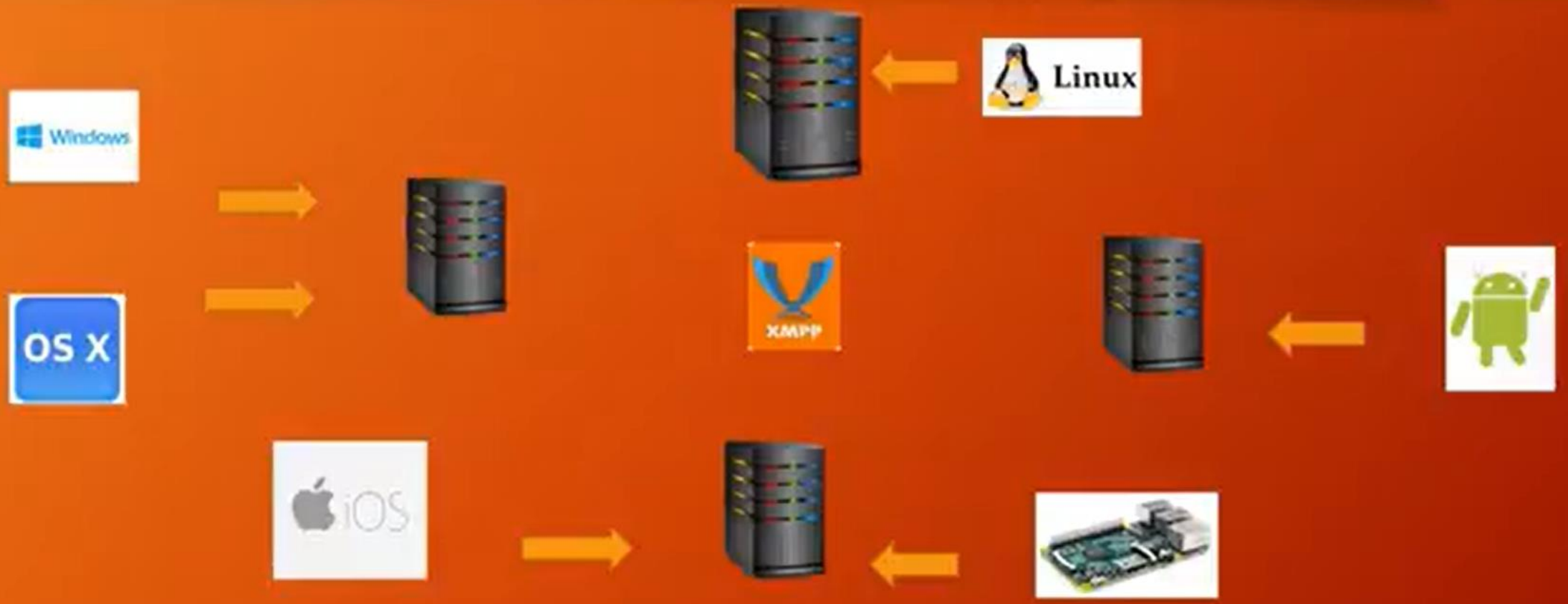
Millions of devices: **I**nterconnecting.

IETF: For internal meetings of voice and video data.

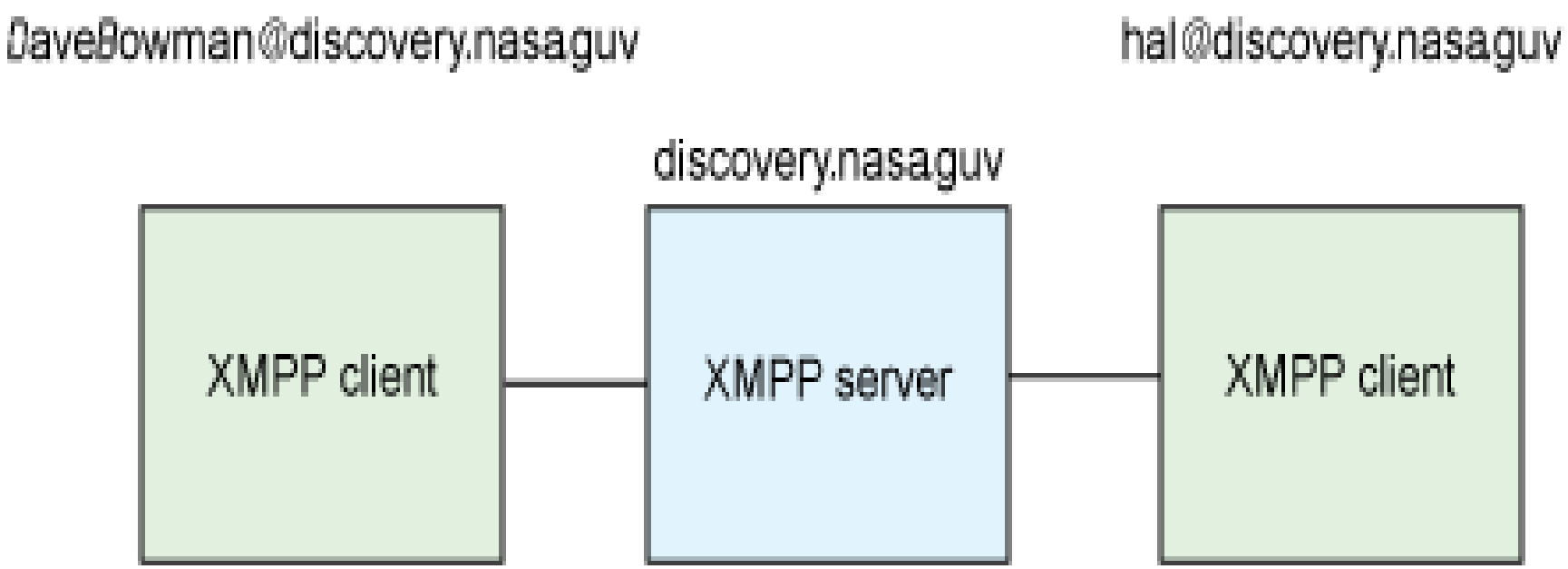
XMPP Support

- Send and receive messages with other users.
- Check and share presence status
- Manage subscriptions to and from other users.
- Manage contact list
- Block communications(receive message, sharing presence status, etc) to specific users.

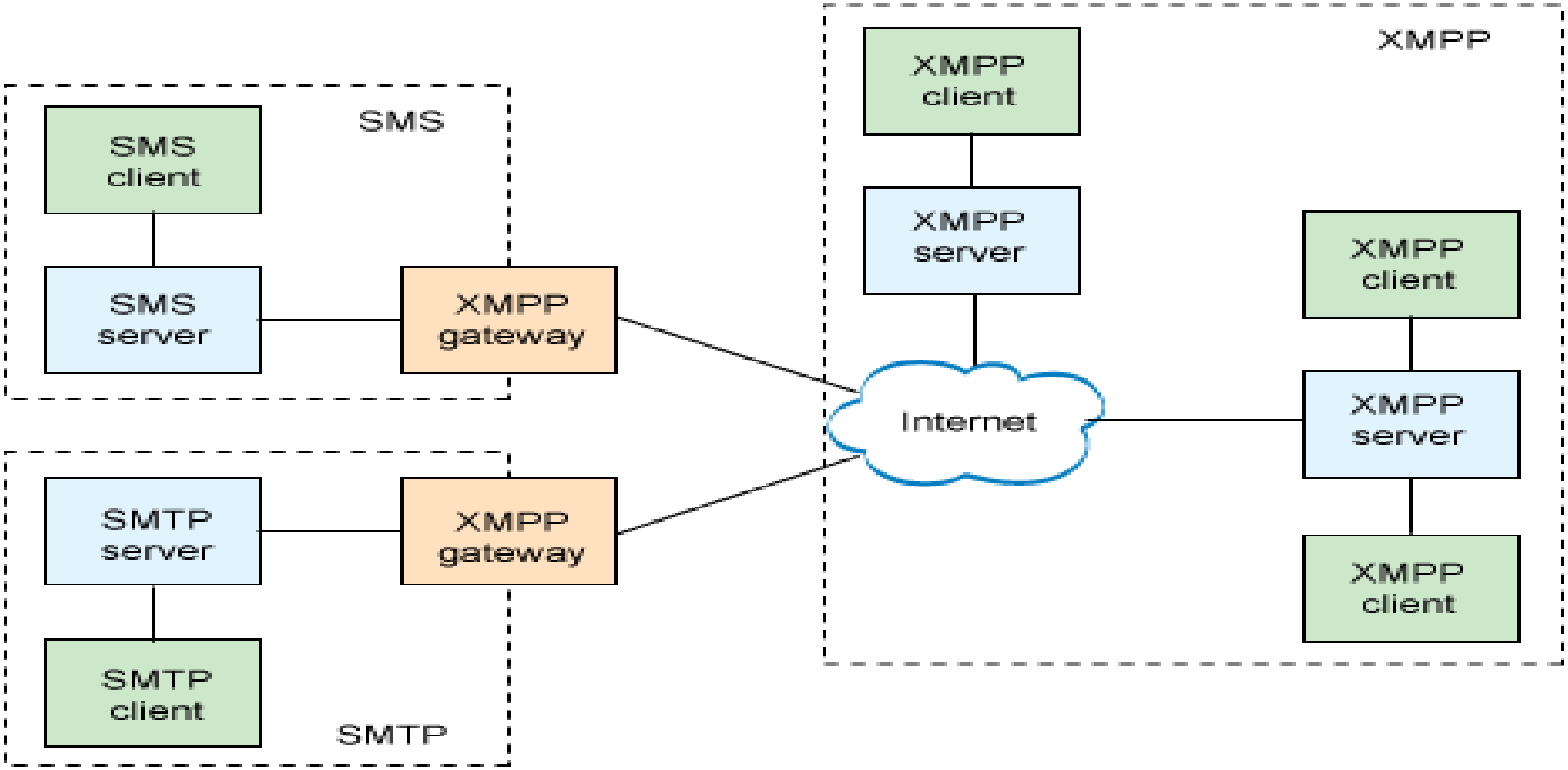
User Experience



CSC Architecture[4]



Complex Architecture[4]



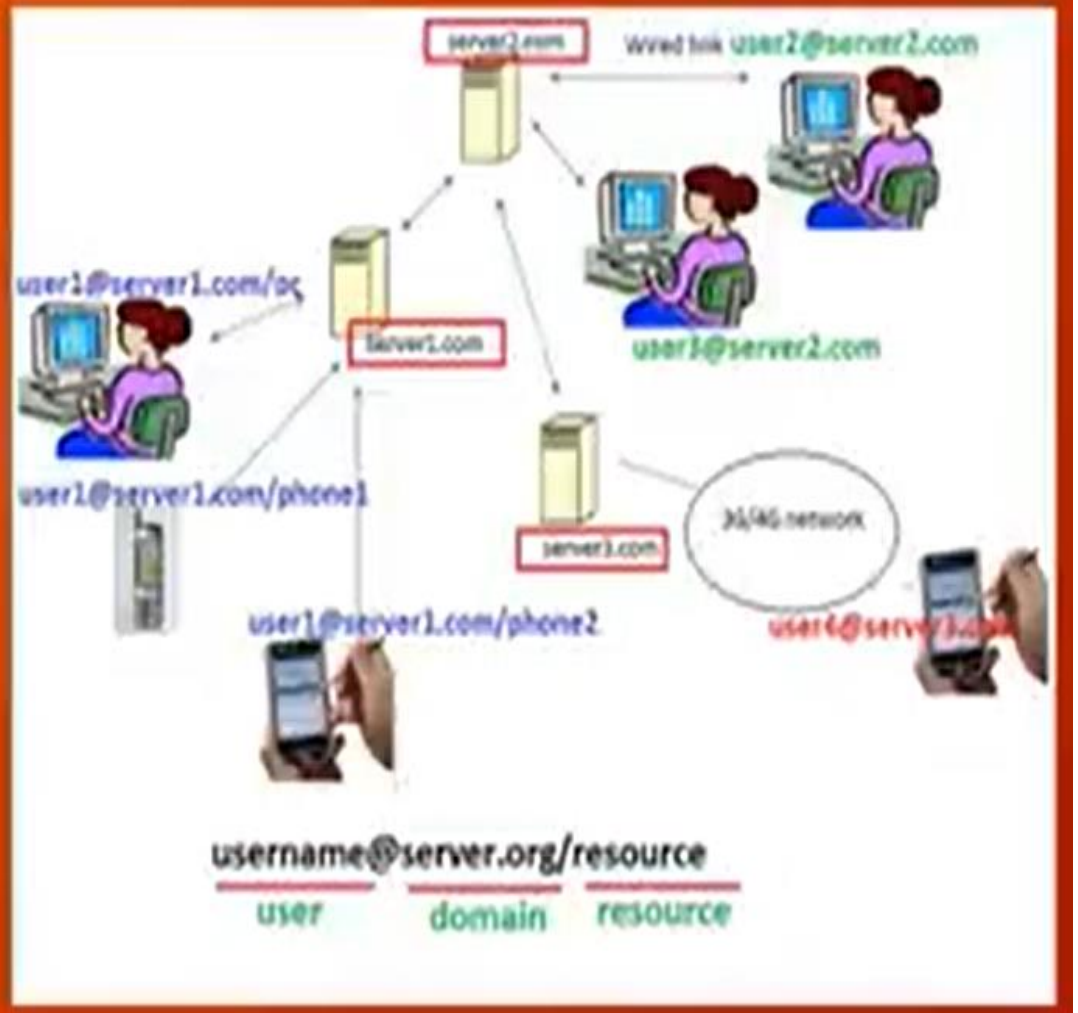
Addressing

- All XMPP entities are addressable on the network
- XMPP Client addresses look like email addresses. Think “user@server.org

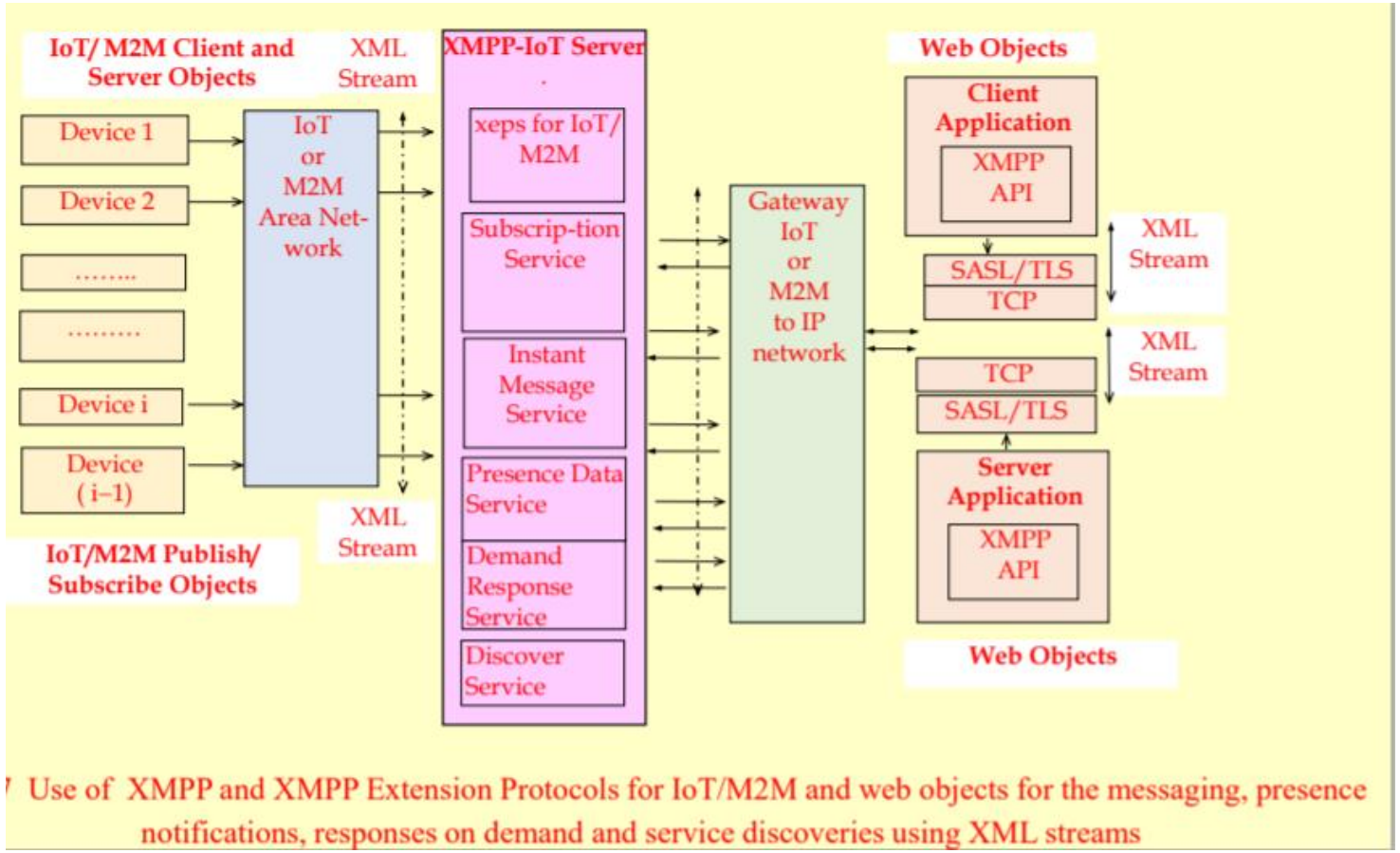
username@server.org/resource

user domain resource

- XMPP Servers are only addressed by the domain part, after the “@” symbol



APPLICTION of XMPP



Use of XMPP and XMPP Extension Protocols for IoT/M2M and web objects for the messaging, presence notifications, responses on demand and service discoveries using XML streams

Pros and Cons of XMPP

Pros

- Addressing scheme to recognize devices on the network
- Client-server architecture
- Decentralized
- Flexible
- Open standards

Cons

- Text-based messaging and no provision for end-to-end encryption
- No provision for quality of service
- The data flow is usually more than 70 per cent of the XMPP protocol server, of which nearly 60 per cent is repeated; the XMPP protocol has a large overhead of data to multiple recipients

Summary

- XMPP is an open, standardized protocol, originally developed to replace proprietary IM networks.
- The XMPP protocol is more than a decade old and quite mature.
- XMPP is great for writing IM applications
- Servers, clients, components, and plug-ins are all parts of XMPP networks
- XMPP addresses, called JIDs, resemble e-mail addresses and decompose into three parts: the local part, the domain, and the resource.
- Full JIDs are the most specific addresses for an entity; for example, darcy@pemberley.lit/ library.
- Bare JIDs are the same as full JIDs without the resource; for example, darcy@pemberley.lit
- Servers will handle stanzas to a client's bare JID, potentially routing them to one or more connected resources.
- Every XMPP session has a life cycle consisting of several phases: connection, stream set up, authentication, the session body, and disconnection.

References

1. https://xmpp.org/about/faq.html
2. https://www.jongbloed.nl/code/inkijkexemplaar/9780470540718/professional-xmpp-programming-with-javascript-and-jquery-engels-jack-moffitt.pdf
3. https://xmpp.org/extensions/xep-0134.pdf
4. https://developer.ibm.com/technologies/messaging/tutorials/x-xmppintro/
5. https://www.youtube.com/watch?v=WktC6vc4WQs [videos]

Q&A

Quiz

SASL: Simple Authentication and Security Layer

TLS: Transport Layer Security