Master Kurs Rechnernetze Computer Networks IN2097

Prof. Dr.-Ing. Georg Carle
Dr. Thomas Fuhrmann

Institut für Informatik
Technische Universität München
http://www.net.in.tum.de

SIP

- Part 2 -

Credits:
Julie Chan, Vovida Networks.
Christian Hoene, University of Tübingen
Milind Nimesh, Columbia University

SIP

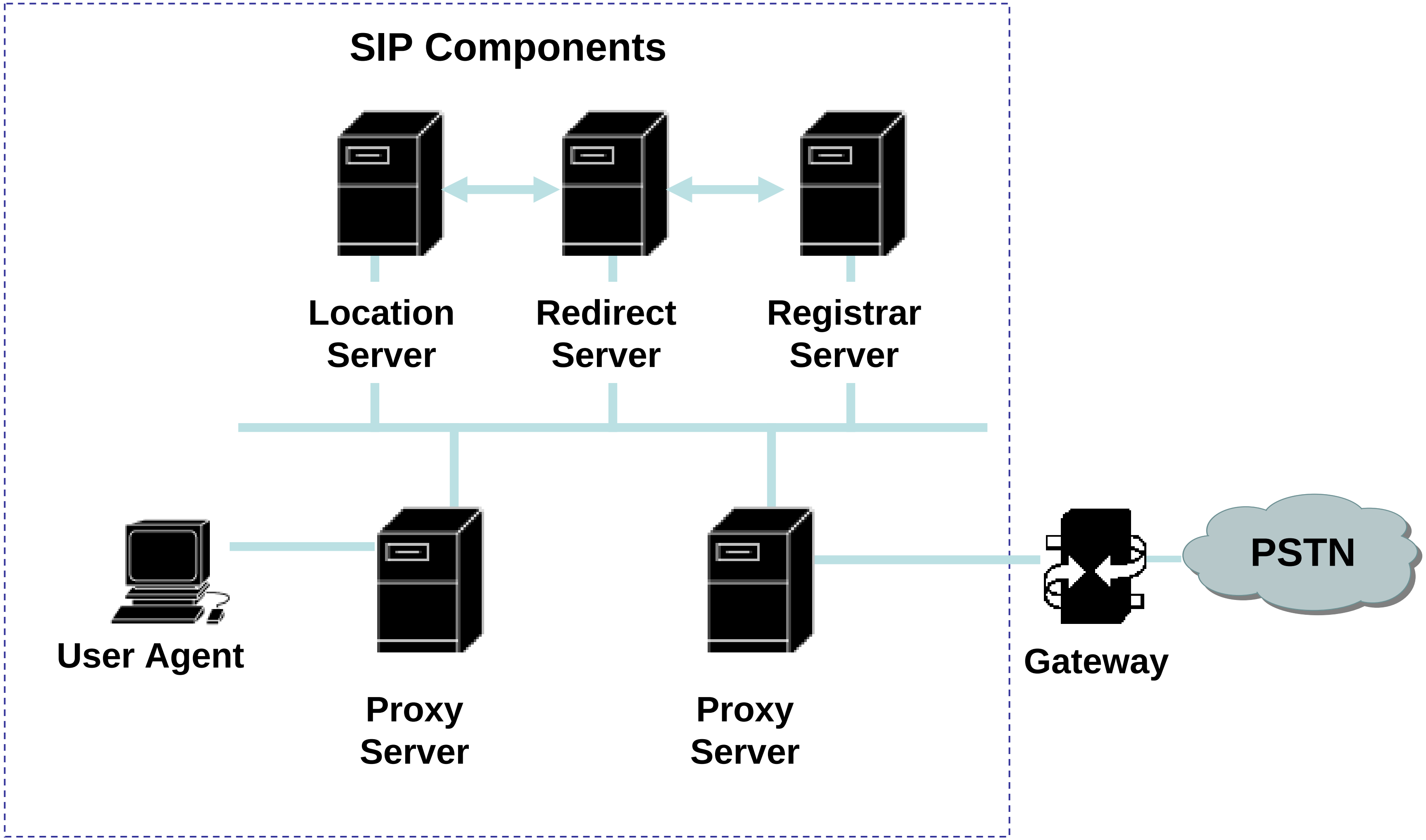
Repetition

- IETF RFC 2543: Session Initiation Protocol –
  An application layer signaling protocol that defines initiation, modification and termination of interactive, multimedia communication *sessions* between users.
- Sessions include voice, video, chat, interactive games, and virtual reality.
- SIP is a text-based protocol, similar to HTTP and SMTP.

SIP consists of a few RFCs

RFC	Description
2976	The SIP INFO Method
3361	DHCP Option for SIP Servers
3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)
3311	The Session Initiation Protocol UPDATE Method
3420	Internet Media Type message/sipfrag
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
3323	A Privacy Mechanism for the Session Initiation Protocol (SIP)
3428	Session Initiation Protocol Extension for Instant Messaging
3326	The Reason Header Field for the Session Initiation Protocol (SIP)
3327	Session Initiation Protocol Extension for Registering Non-Adjacent Contacts
3329	Security Mechanism Agreement for the Session Initiation Protocol (SIP) Sessions
3313	Private Session Initiation Protocol (SIP)Extensions for Media Authorization
3486	Compressing the Session Initiation Protocol
3515	The Session Initiation Protocol (SIP) Refer Method
3319	Dynamic Host Configuration Protocol (DHCPv6)Options for Session Initiation Protocol (SIP) Servers
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3608	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration
3853	S/MIME AES Requirement for SIP
3840	Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)
3841	Caller Preferences for the Session Initiation Protocol (SIP)
3891	The Session Inititation Protocol (SIP) 'Replaces' Header
3892	The SIP Referred-By Mechanism
3893	SIP Authenticated Identity Body (AIB) Format
3903	An Event State Publication Extension to the Session Initiation Protocol (SIP)
3911	The Session Inititation Protocol (SIP) 'Join' Header
3968	The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)
3969	The Internet Assigned Number Authority (IANA) Universal Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)
4032	Update to the Session Initiation Protocol (SIP) Preconditions Framework
4028	Session Timers in the Session Initiation Protocol (SIP)
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)
4168	The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)
4244	An Extension to the Session Initiation Protocol (SIP) for Request History Information
4320	Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) non-INVITE Transaction
4321	Problems identified associated with the Session Initiation Protocol's (SIP) non-INVITE Transaction
4412	Communications Resource Priority for the Session Initiation Protocol (SIP)
4488	Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription
4508	Conveying Feature Tags with Session Initiation Protocol (SIP) REFER Method
4483	A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages
4485	Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP)

SIP Architecture



User Agents

- An application that initiates, receives and terminates calls.
  - User Agent Clients (UAC) – An entity that initiates a call.
  - User Agent Server (UAS) – An entity that receives a call.

  - Both UAC and UAS can terminate a call.

Proxy Server

- An intermediary program that acts as both
  a server and a client
  to make requests on behalf of other clients.
- Requests are serviced internally or passed on,
  possibly after translation, to other servers.
- Interprets, rewrites or translates a request message
  before forwarding it.

Registrar Server

- ❑ A server that accepts REGISTER requests.
- ❑ The register server may support authentication.
- ❑ A registrar server is typically co-located with a proxy or redirect server and may offer location services.

Redirect Server

- A server that accepts a SIP request, maps the address into zero or more new addresses and returns these addresses to the client.
- Unlike a proxy server, the redirect server does not initiate its own SIP request.
- Unlike a user agent server, the redirect server does not accept or terminate calls.
- The redirect server that generates 3xx responses to requests it receives, directing the client to contact an alternate set of URIs.
- In some architectures it may be desirable to reduce the processing load on proxy servers that are responsible for routing requests, and improve signaling path robustness, by relying on redirection.
- Redirection allows servers to push routing information for a request back in a response to the client, thereby taking themselves out of the loop of further messaging for this transaction while still aiding in locating the target of the request. When the originator of the request receives the redirection, it will send a new request based on the URI(s) it has received. By propagating URIs from the core of the network to its edges, redirection allows for considerable network scalability.

C.f. iterative (non-recursive) DNS queries

Location Server

- A location server is used by a SIP redirect or proxy server to obtain information about a called party's possible location(s).

- A location Server is a logical IP server that transmits a Presence Information Data Format - Location Object, or PIDF-LO.
- A PIDF-LO is an XML Scheme specifically for carrying geographic location of a Target.
- As stated in RFC 3693, location often must be kept private.
  The Location Object (PIDF-LO) contains rules which provides guidance to the Location Recipient and controls onward distribution and retention of the location.

SIP Messages – Methods and Responses

SIP components communicate by exchanging SIP messages:

SIP Methods:

- INVITE – Initiates a call by inviting user to participate in session.
- ACK - Confirms that the client has received a final response to an INVITE request.
- BYE - Indicates termination of the call.
- CANCEL - Cancels a pending request.
- REGISTER – Registers the user agent.
- OPTIONS – Used to query the capabilities of a server.
- INFO – Used to carry out-of-bound information, such as DTMF (Dual-tone multi-frequency) digits.

SIP Responses:

- 1xx - Informational Messages.
- 2xx - Successful Responses.
- 3xx - Redirection Responses.
- 4xx - Request Failure Responses.
- 5xx - Server Failure Responses.
- 6xx - Global Failures Responses.

SIP Headers

- SIP borrows much of the syntax and semantics from HTTP.
- A SIP messages looks like an HTTP message: message formatting, header and MIME support.
- An example SIP header:

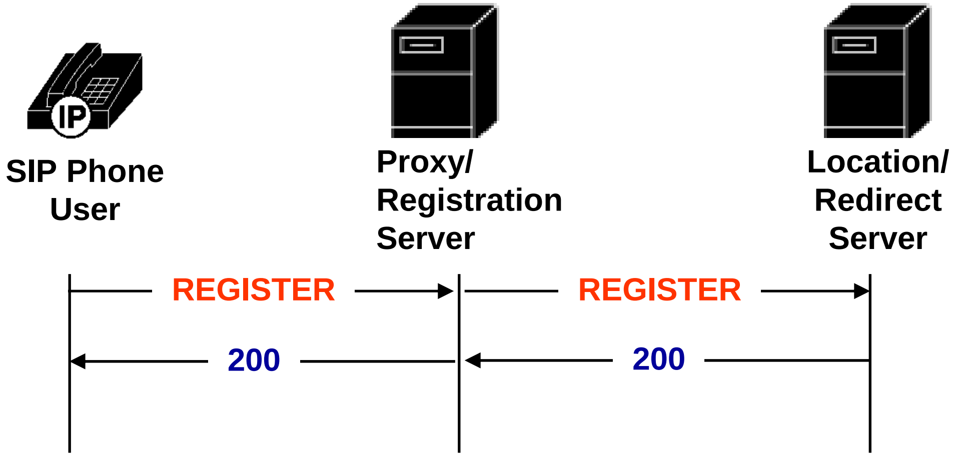
```
----------------------------------------------------------------
                        SIP Header
----------------------------------------------------------------
INVITE sip:5120@192.168.36.180 SIP/2.0
Via: SIP/2.0/UDP 192.168.6.21:5060
From: sip:5121@192.168.6.21
To: <sip:5120@192.168.36.180>
Call-ID: c2943000-e0563-2a1ce-2e323931@192.168.6.21
CSeq: 100 INVITE
Expires: 180
User-Agent: Cisco IP Phone/ Rev. 1/ SIP enabled
Accept: application/sdp
Contact: sip:5121@192.168.6.21:5060
Content-Type: application/sdp
```

SIP Addressing

- The SIP address is identified by a SIP URL, in the format: user@host.
- Examples of SIP URLs:
  - sip:user@domain.com
  - sip:user@192.168.10.1
  - sip:14083831088@domain.com

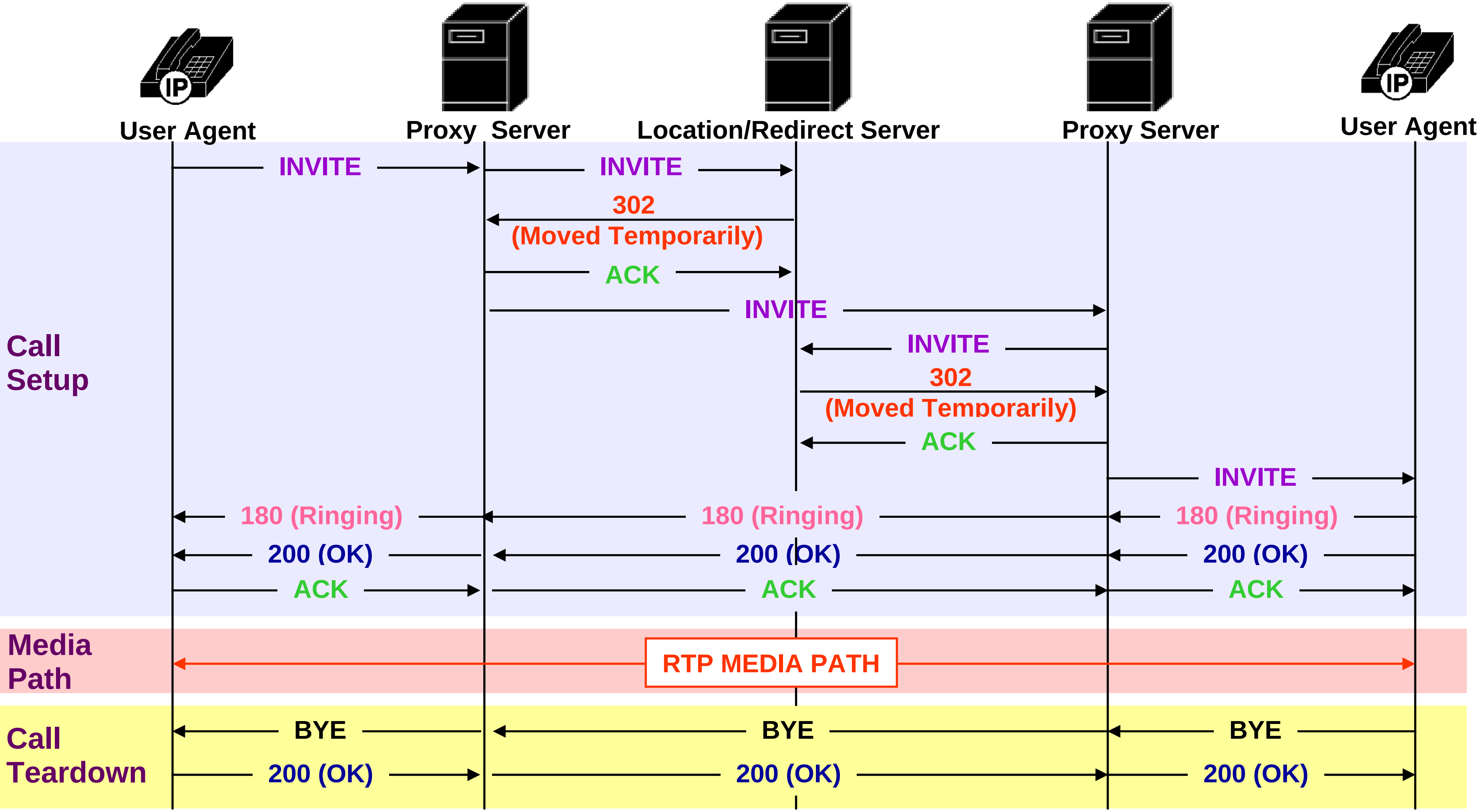
Registration

- Each time a user turns on the SIP user client (SIP IP Phone, PC, or other SIP device), the client registers with the proxy/registration server.
- Registration can also occur when the SIP user client needs to inform the proxy/registration server of its location.
- The registration information is periodically refreshed and each user client must re-register with the proxy/registration server.
- Typically the proxy/registration server will forward this information to be saved in the location/redirect server.



SIP Messages:
REGISTER – Registers the address listed in the To header field.
200 – OK.

Simplified SIP Call Setup and Teardown



SIP – Design Framework

- SIP was designed for:
  - Integration with existing IETF protocols.
  - Scalability and simplicity.
  - Mobility.
  - Easy feature and service creation.

Integration with IETF Protocols

- Other IETF protocol standards can be used to build a SIP based application. SIP can works with existing IETF protocols, for example:
  - RSVP - to reserve network resources.
  - RTP Real Time Protocol - to transport real time data and provide QOS feedback.
  - RTSP Real Time Streaming Protocol - for controlling delivery of streaming media.
  - SAP Session Advertisement Protocol - for advertising multimedia session via multicast.
  - SDP Session Description Protocol – for describing multimedia sessions.
  - MIME – Multipurpose Internet Mail Extension – describing content on the Internet.
  - COPS – Common Open Policy Service.
  - OSP – Open Settlement Protocol.

Scalability and Simplicity

- Scalability:
  The SIP architecture is scalable, flexible and distributed.
  - Functionality such as proxying, redirection, location, or registration can reside in different physical servers.
  - Distributed functionality allows new processes to be added without affecting other components.

- Simplicity:
  SIP is designed to be:
  - “Fast and simple in the core.”
  - “Smarter with less volume at the edge.”
  - Text based for easy implementation and debugging.

Feature Creation

- SIP can support these features and applications:
  - Basic call features (call waiting, call forwarding, call blocking etc.).
  - Unified messaging (the integration of different streams of communication - e-mail, SMS, Fax, voice, video, etc. - into a single unified message store, accessible from a variety of different devices.)
  - Call forking.
  - Click to talk.
  - Presence.
  - Instant messaging.
  - Find me / Follow me.

Feature Creation (2)

- A SIP based system can support rapid feature and service creations.
- For example, features and services can be created using:
  - Call Processing Language (CPL).
    - Jonathan Lennox, Xiaotao Wu, Henning Schulzrinne: RFC3880
    - Designed to be implementable on either network servers or user agents. Meant to be simple, extensible, easily edited by graphical clients, and independent of operating system or signalling protocol. Suitable for running on a server where users may not be allowed to execute arbitrary programs, as it has no variables, loops, or ability to run external programs.
    - Syntactically, CPL scripts are represented by XML documents.
  - Common Gateway Interface (CGI).
    - A standard for interfacing external applications with information servers, such as Web servers (or SIP servers).
      A CGI program is executed in real-time, so that it can output dynamic information.

References

- For more information on SIP:
- IETF
  - http://www.ietf.org/html.charters/sip-charter.html
- Henning Schulzrinne's SIP page
  - http://www.cs.columbia.edu/~hgs/sip/

Location Information and IETF GeoPriv Working Group

credits:

Milind Nimesh, Columbia University

Location Information

- Describes physical position of a person or device:
  - geographical
  - civic (i.e., address)
  - descriptive (eg. library, airport)
- Formatting and transfer of location information – relatively easy
- Privacy and security – complex
- Application:
  - emergency services
  - resource management
  - social networking
  - search
  - navigation

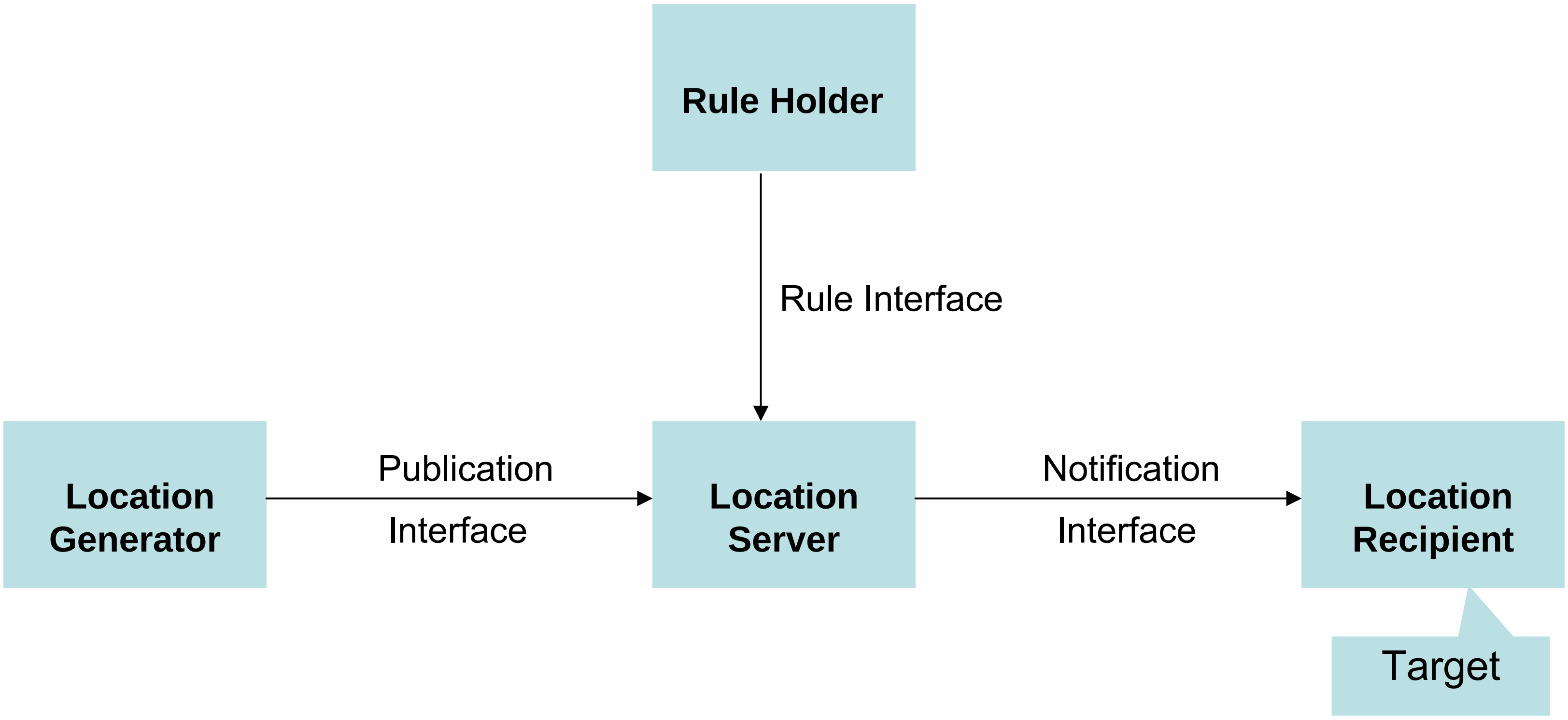
IETF Geopriv Working Group

- ❑ Geographic Location/Privacy working group

- ❑ Primary tasks for this working group
  - ▪ assess authorization, integrity and privacy requirements
  - ▪ select standardized location information format
    - • enhance format → availability of security & privacy methods
  - ▪ authorization of: requester, responders, proxies

- ❑ Goal: transferring location information: private + secure

Geopriv Entities



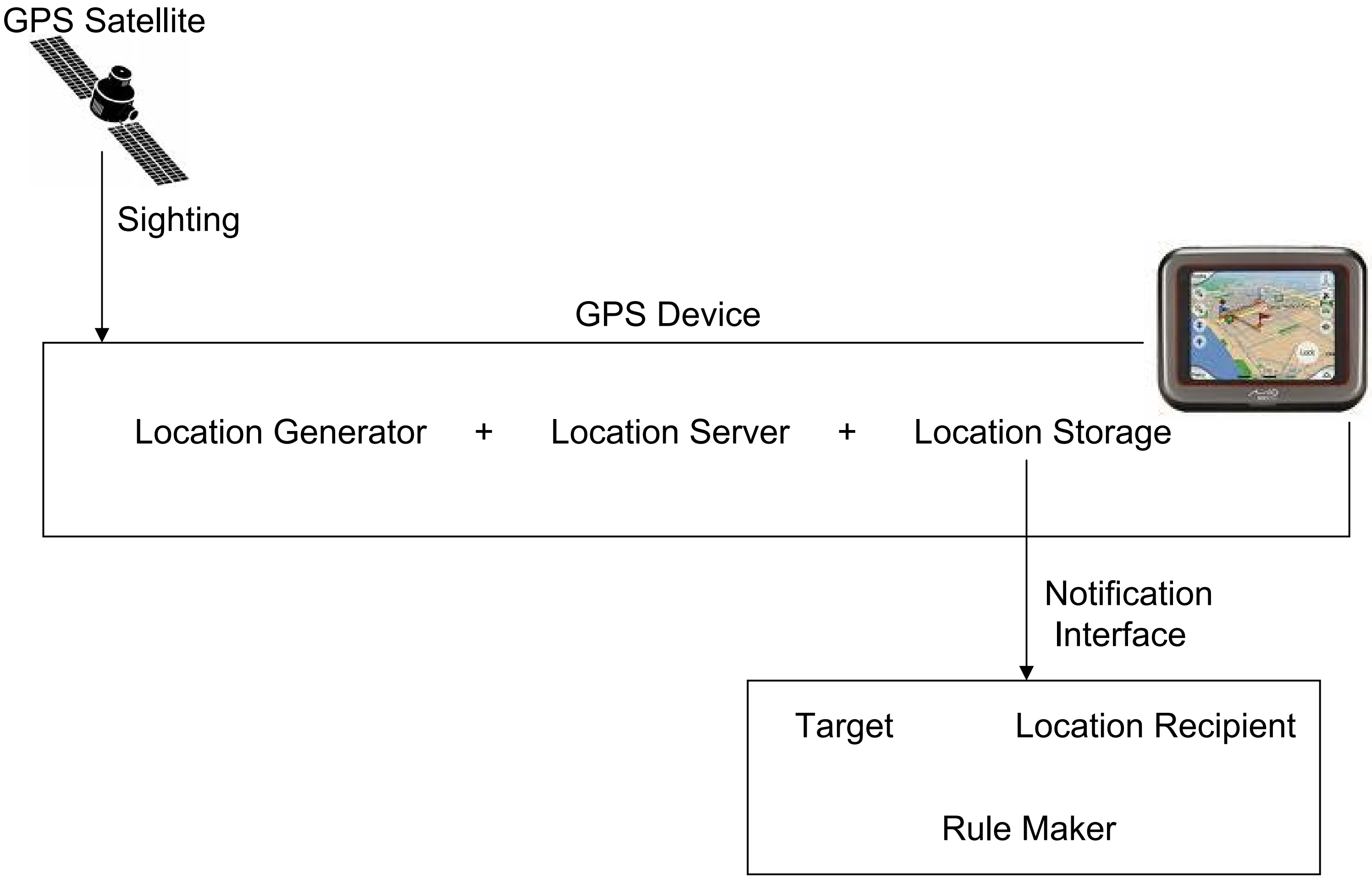
Geopriv Terminology

- ❑ Location Object: conveys location information + privacy rules
- ❑ Rule Maker: creates rules → governs access to location information
- ❑ Target: person/entity whose location communicated
- ❑ Using Protocol: protocol carrying location object
- ❑ Viewer: consumes location information but does not pass information further

Geopriv Requirements

- ❑ Secure transmission of location objects
- ❑ User controlled privacy rules
- ❑ Filtering location information
- ❑ Location object carries core set of privacy rules
- ❑ Ability of user to hide real identity

Scenarios



GPS Satellite

Sighting

GPS Device

Location Generator + Location Server + Location Storage

Notification Interface

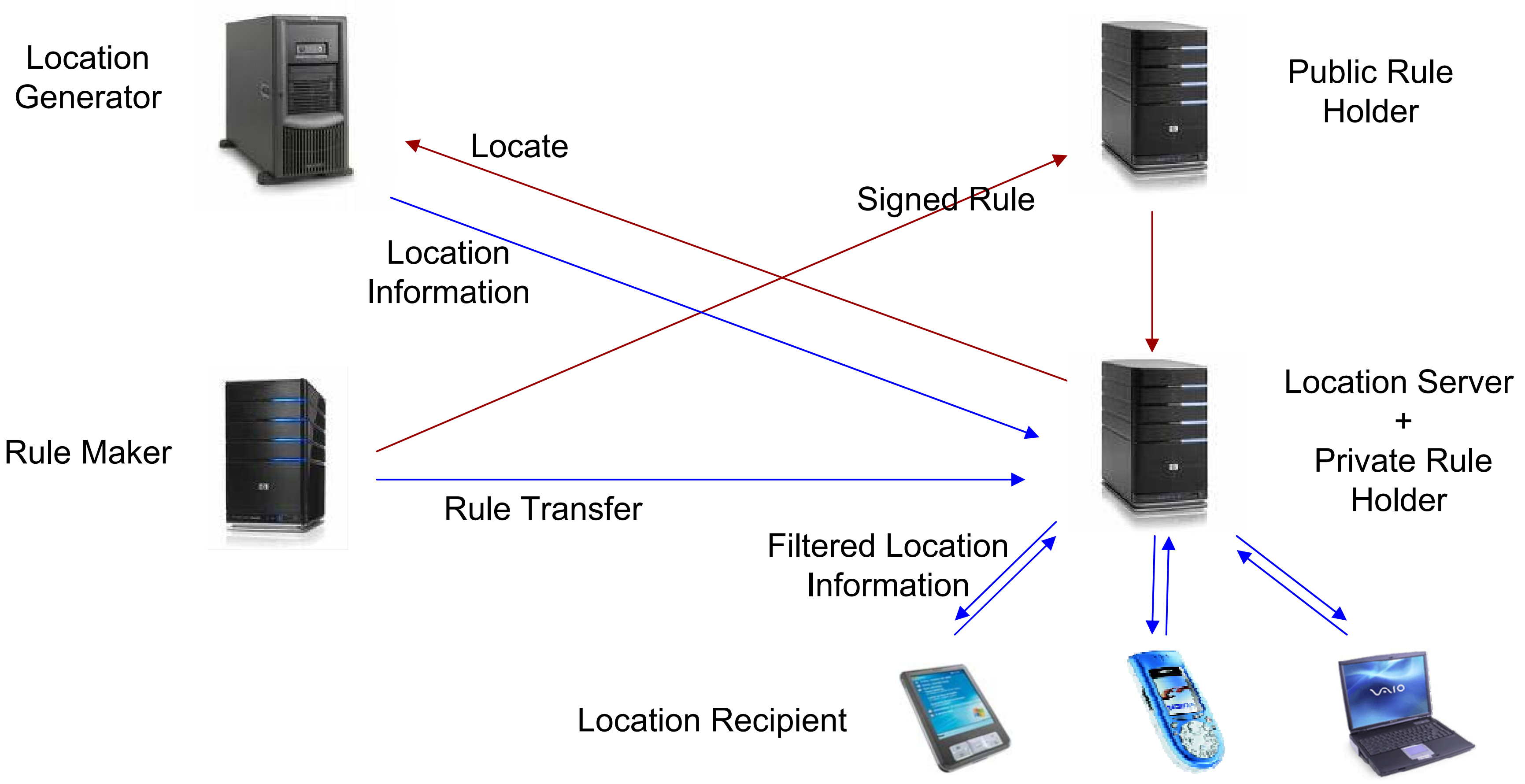
Target

Location Recipient

Rule Maker

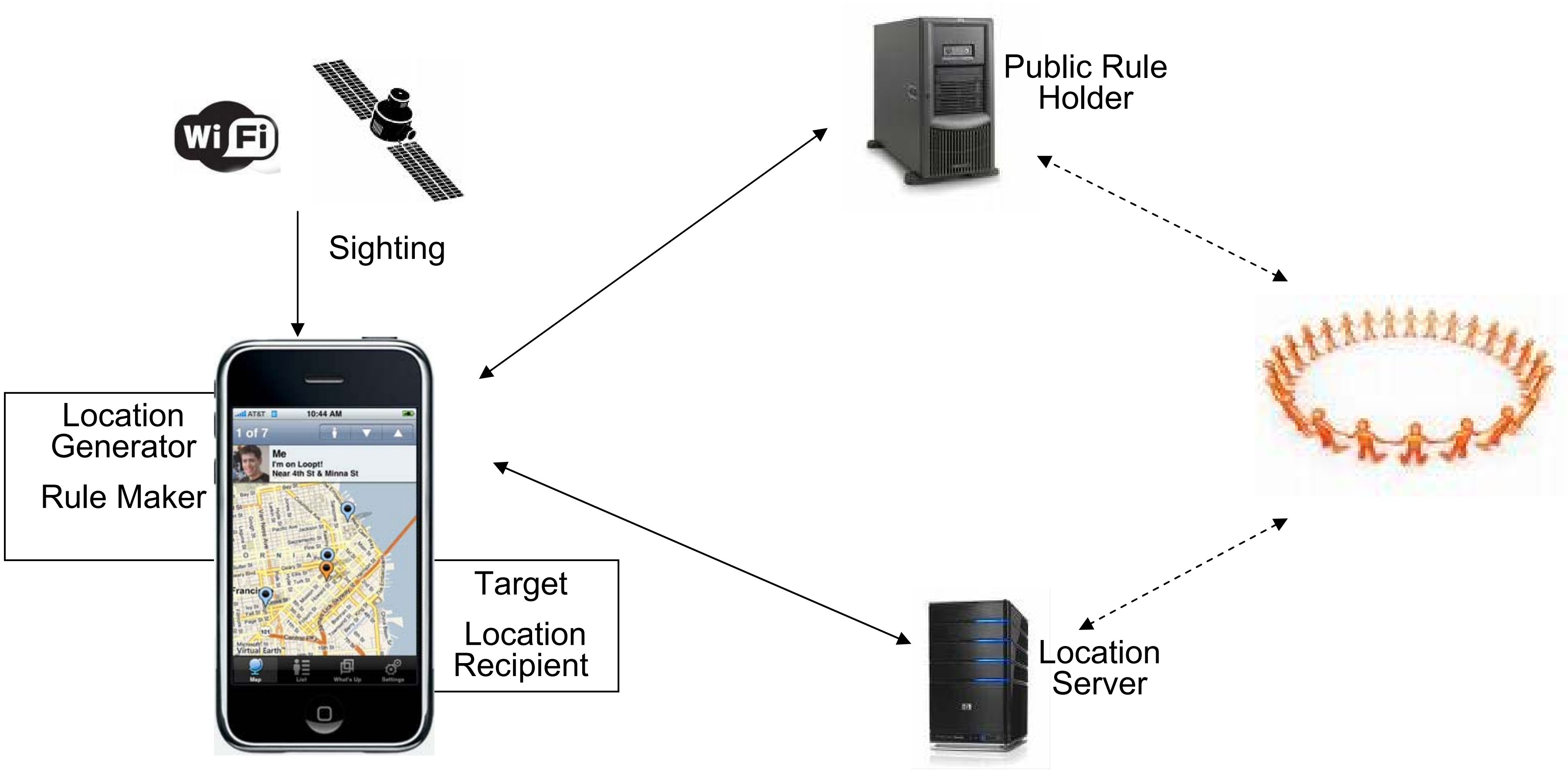
GPS Device with Internal Computing Power: Closed System

Scenarios



Mobile Communities and Location-Based Services

Applications: Social Networking



Sighting

Public Rule Holder

Location Generator

Rule Maker

Target

Location Recipient

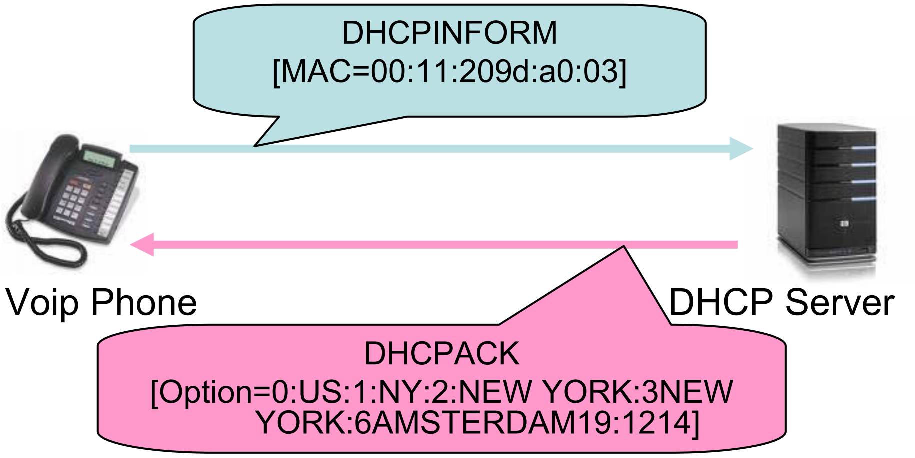
Location Server

Location configuration

- Configuring the location of device
- HTTP Enabled Location Delivery
  - device retrieves location from LIS
  - assumption: device & LIS present in same admin domain
- Link Layer Discovery Protocol - Media Endpoint Discovery
  - LLDP - a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network. IEEE standard 802.1AB-2005 in May 2005.
    Supersedes proprietary protocols like Cisco Discovery Protocol,
  - auto-discovery of LAN policies → plug & play
  - device location discovery
  - cisco discovery protocol
    - switch broadcast switch/port id
    - switch → floor, port → room » room level accuracy
- Modified DHCP server
- Applications → emergency 911, voip, location based applications

DHCP Option for Civic Addresses Configuration

- DHCP Server configures location information of devices
- Mapping: MAC → location
- Issues
  - consistent information
  - geographically valid configuration
- Option 99 → civic address
- Option 123 → geo-coordinate based location information



Security Considerations

- Traffic Analysis
  - attacks on target and privacy violations
- Securing the Privacy Rules
  - rules accessible to LS
  - authenticated using signature
- Emergency Case
  - handling authentication failure
- Identities & Anonymity

Presence Information Data Format - PIDF

- XML based object format, communicates presence information

- PIDF extended to carry geographical information

- Extended PIDF encapsulates
  - preexisting location information formats
  - security & policy control

- Protocols capable of carrying XML or MIME types suitable

- Security: MIME-level → S/MIME

PIDF Elements - RFC 3863

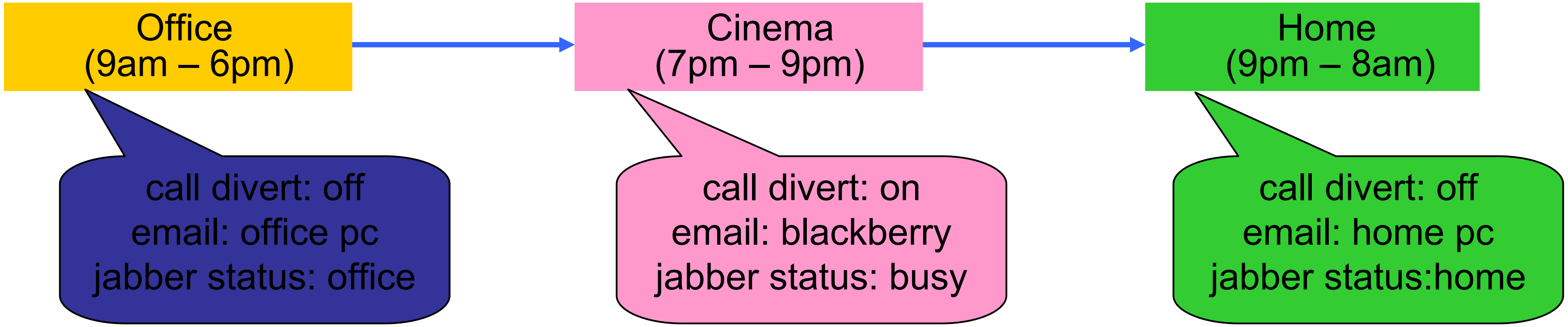
Baseline

- entity
- contact (how to contact the person)
- timestamp
- status
- tuple (provide a way of segmenting presence information)

Extensions

- location-info
- usage-rules
  - retransmission-allowed
  - retention-expires
  - ruleset-reference
  - note-well
- method
- provided-by

Location Type Registry



- Describes places humans or end systems found
- Application
  - define location based actions
  - eg. if loc = “classroom” then cell phone ringer = off
  - eg. if loc = “cinema” then call divert = on
- Location coordinate knowledge ≠ context
- airport, arena, bank, bar, bus-station, club, hospital, library….

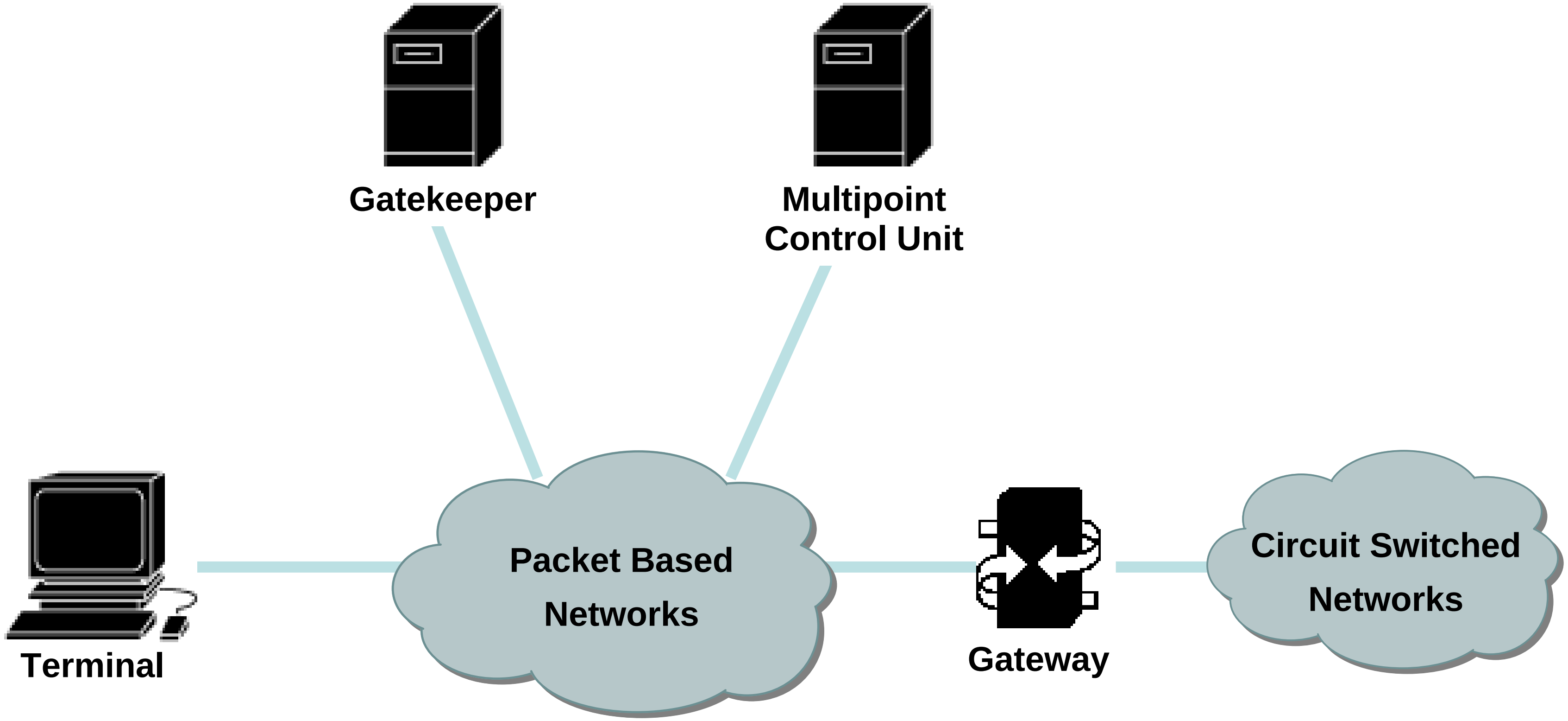
H.323

What is H.323?

- ITU-T Recommendation H.323 Version 4

  Describes terminals and other entities that provide multimedia communications services over Packet Based Networks (PBN) which may not provide a guaranteed Quality of Service. H.323 entities may provide real-time audio, video and/or data communications.
- H.323 framework defines:
  - Call establishment and teardown.
  - Audio visual or multimedia conferencing.

H.323 Components



H.323 Terminals

- H.323 terminals are client endpoints that must support:
  - H.225 call control signaling.
  - H.245 control channel signaling.
  - RTP/RTCP protocols for media packets.
  - Audio codecs.

  - Video codecs support is optional.

H.323 Gateway

- A gateway provides translation:
  - For example, a gateway can provide translation between entities in a packet switched network (example, IP network) and circuit switched network (example, PSTN network).
  - Gateways can also provide transmission formats translation, communication procedures translation, H.323 and non-H.323 endpoints translations or codec translation.

H.323 Gatekeepers

- Gatekeepers provide these functions:
  - Address translation.
  - Admission control.
  - Bandwidth control.
  - Zone management.
  - Call control signaling (optional).
  - Call authorization (optional).
  - Bandwidth management (optional).
  - Call management (optional).
- Gatekeepers are optional but if present in a H.323 system, all H.323 endpoints must register with the gatekeeper and receive permission before making a call.

H.323 Multipoint Control Unit

- MCU provide support for conferences of three or more endpoints.
- An MCU consist of:
  - Multipoint Controller (MC) – provides control functions.
  - Multipoint Processor (MP) – receives and processes audio, video and/or data streams.

H.323 is an “Umbrella” Specification

Media

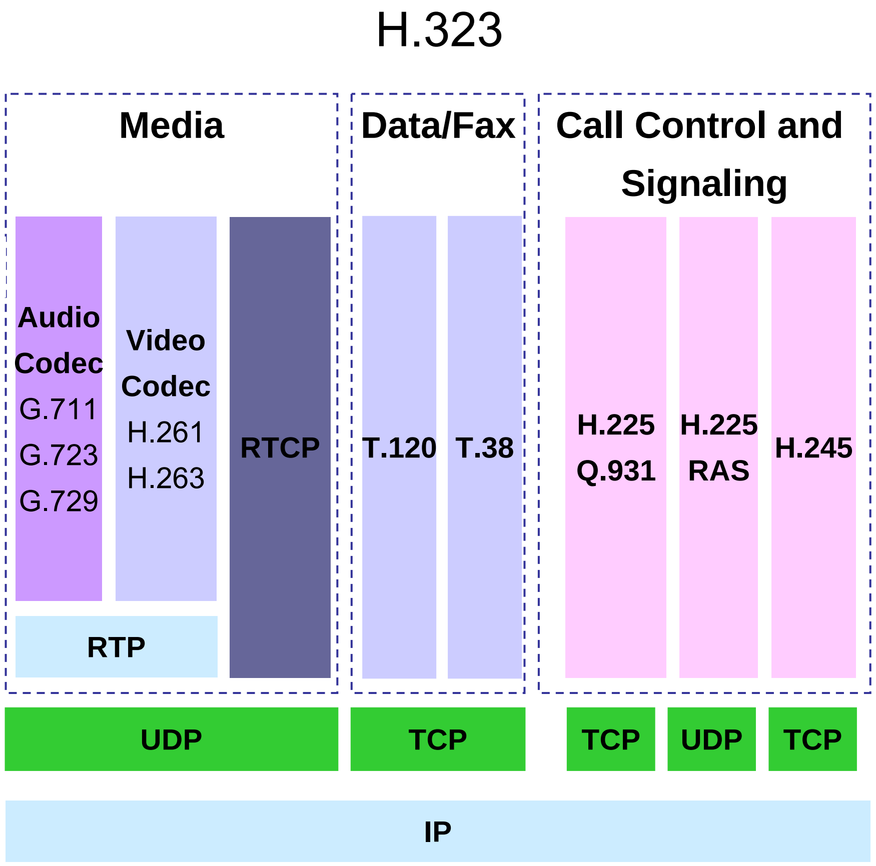
- ❑ H.261 and H.263 – Video codecs.
- ❑ G.711, G.723, G.729 – Audio codecs.
- ❑ RTP/RTCP – Media.

Data/Fax

- ❑ T.120 – Data conferencing.
- ❑ T.38 – Fax.

Call Control and Signaling

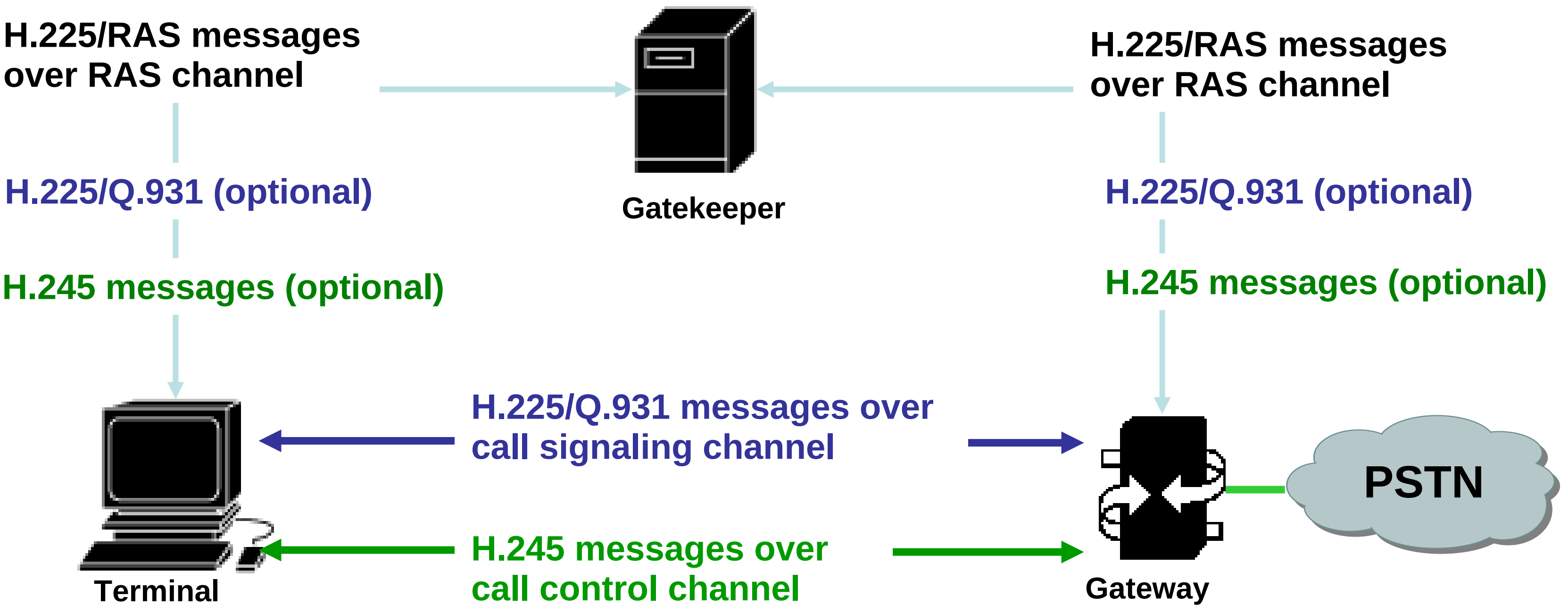
- ❑ H.245 - Capabilities advertisement, media channel establishment, and conference control.
- ❑ H.225
- ❑ Q.931 - call signaling and call setup.
- ❑ RAS - registration and other admission control with a gatekeeper.



Other ITU H. Recommendation that work with H.323

Protocol	Description
H.235	Specifies **security and encryption** for H.323 and H.245 based terminals
H.450.N	H.450.1 specifies framework for supplementary services. H.450.N recommendation specifies supplementary services such as call transfer, call diversion, call hold, call park, call waiting, message waiting indication, name identification, call completion, call offer, and call intrusion.
H.246	Specifies internetworking of H Series terminals with circuit switched terminals.

H.323 Components and Signaling


H.225/RAS messages over RAS channel
H.225/RAS messages over RAS channel
Gatekeeper
H.225/Q.931 (optional)
H.225/Q.931 (optional)
H.245 messages (optional)
H.245 messages (optional)
H.225/Q.931 messages over call signaling channel
H.245 messages over call control channel
Terminal
Gateway
PSTN

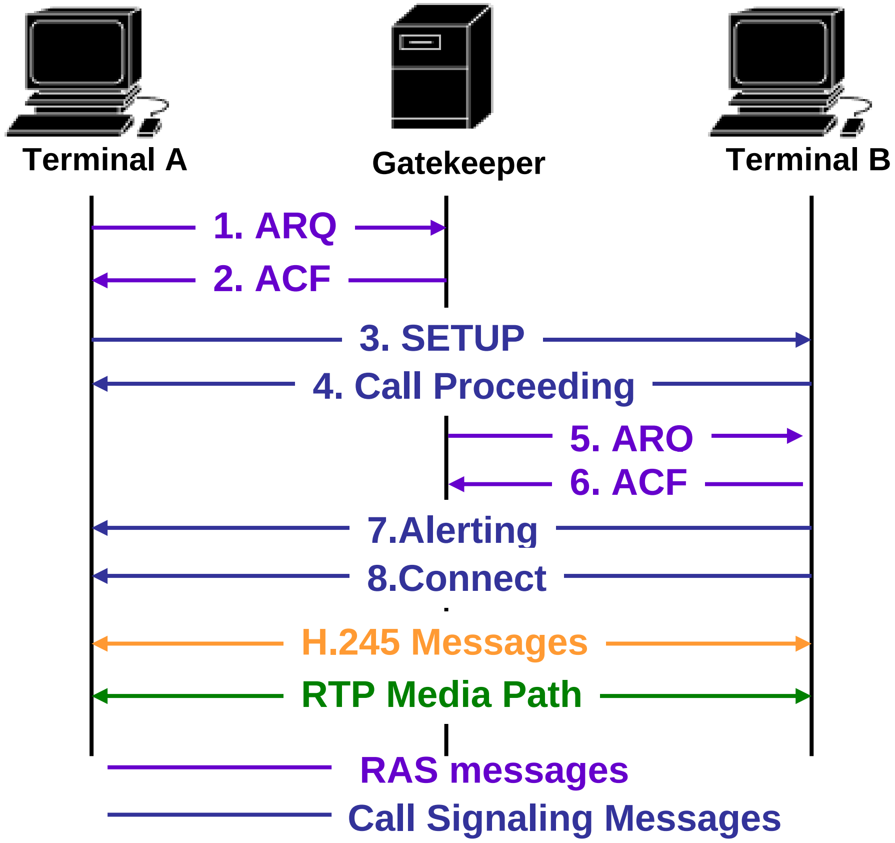
- ❑ H.245 – A protocol for capabilities advertisement, media channel establishment and conference control.
- ❑ H.225 - Call Control.
- ❑ Q.931 – A protocol for call control and call setup.
- ❑ RAS – Registration, admission and status protocol used for communicating between an H.323 endpoint and a gatekeeper.

Process for Establishing Communication

- Establishing communication using H.323 may occur in five steps:
  - Call setup.
  - Initial communication and capabilities exchange.
  - Audio/video communication establishment.
  - Call services.
  - Call termination.

Simplified H.323 Call Setup

- ❑ Both endpoints have previously registered with the gatekeeper.
- ❑ Terminal A initiate the call to the gatekeeper. (RAS messages are exchanged).
- ❑ The gatekeeper provides information for Terminal A to contact Terminal B.
- ❑ Terminal A sends a SETUP message to Terminal B.
- ❑ Terminal B responds with a Call Proceeding message and also contacts the gatekeeper for permission.
- ❑ Terminal B sends a Alerting and Connect message.
- ❑ Terminal B and A exchange H.245 messages to determine master slave, terminal capabilities, and open logical channels.
- ❑ The two terminals establish RTP media paths.



Terminal A

Gatekeeper

Terminal B

1. ARQ

2. ACF

3. SETUP

4. Call Proceeding

5. ARO

6. ACF

7.Alerting

8.Connect

H.245 Messages

RTP Media Path

RAS messages

Call Signaling Messages

Note: This diagram only illustrates a simple point-to-point call setup where call signaling is not routed to the gatekeeper. Refer to the H.323 recommendation for more call setup scenarios.

Versions of H.323

Version	Date	Reference for key feature summary
H.323 Version 1	May 1996	New release. Refer to the specification. http://www.packetizer.com/iptel/h323/
H.323 Version 2	January 1998	http://www.packetizer.com/iptel/h323/whatsnew_v2.html
H.323 Version 3	September 1999	http://www.packetizer.com/iptel/h323/whatsnew_v3.html
H.323 Version 4	November 2000	http://www.packetizer.com/iptel/h323/whatsnew_v4.html

References

- For more information on H.323 refer to:
- ITU-T
  - http://www.itu.int/itudoc/itu-t/rec/index.html
- Packetizer
  - http://www.packetizer.com/iptel/h323/
- Open H.323
  - http://www.openH323.org

Comparing

SIP and H.323

Comparison with H.323

- H.323 is another signaling protocol for real-time, interactive services
- H.323 is a complete, vertically integrated suite of protocols for multimedia conferencing: signaling, registration, admission control, transport, codecs
- SIP is a single component. Works with RTP, but does not mandate it. Can be combined with other protocols, services
- H.323 comes from the ITU (telephony).
- SIP comes from IETF: Borrows much of its concepts from HTTP
  - SIP has Web flavor, whereas H.323 has telephony flavor.
- SIP was based on the KISS principle: Keep it simple stupid. (Remark: after all SIP extensions, this is not any more the case.)

Comparing SIP and H.323 - Similarities

- Functionally, SIP and H.323 are similar. Both SIP and H.323 provide:
  - Call control, call setup and teardown.
  - Basic call features such as call waiting, call hold, call transfer, call forwarding, call return, call identification, or call park.
  - Capabilities exchange.

Comparing SIP and H.323 - Strengths

- H.323 – Defines sophisticated multimedia conferencing. H.323 multimedia conferencing can support applications such as whiteboarding, data collaboration, or video conferencing.
- SIP – Supports flexible and intuitive feature creation with SIP using SIP-CGI (SIP-Common Gateway Interface) and CPL (Call Processing Language).
- SIP – Third party call control is currently only available in SIP. Work is in progress to add this functionality to H.323.

Table 1 - SIP and H.323

Information	SIP	H.323
Standards Body	IETF.	ITU.
Relationship	Peer-to-Peer.	Peer-to-Peer.
Origins	Internet based and web centric. Borrows syntax and messages from HTTP.	Telephony based. Borrows call signaling protocol from ISDN Q.SIG.
Client	Intelligent user agents.	Intelligent H.323 terminals.
Core servers	SIP proxy, redirect, location, and registration servers.	H.323 Gatekeeper.
Current Deployment	SIP is gaining majority of interest.	Widespread, but considered as “legacy technology”.
Interoperability	IMTC sponsors interoperability events among SIP, H.323, and MGCP. For more information, visit: http://www.imtc.org/	

Table 2 - SIP and H.323

Information	SIP	H.323
Capabilities Exchange	SIP uses SDP protocol for capabilities exchange. SIP does not provide as extensive capabilities exchange as H.323.	Supported by H.245 protocol. H.245 provides structure for detailed and precise information on terminal capabilities.
Control Channel Encoding Type	Text based UTF-8 encoding.	Binary ASN.1 PER encoding.
Server Processing	Stateless or stateful.	Version 1 or 2 – Stateful. Version 3 or 4 – Stateless or stateful.
Quality of Service	SIP relies on other protocols such as RSVP, COPS, OSP to implement or enforce quality of service.	Bandwidth management/control and admission control is managed by the H.323 gatekeeper. The H.323 specification recommends using RSVP for resource reservation.

Table 3 - SIP and H.323

Information	SIP	H.323
Security	**Registration -** User agent registers with a proxy server. **Authentication -** User agent authentication uses HTTP digest or basic authentication. **Encryption -** The SIP RFC defines three methods of encryption for data privacy.	**Registration -** If a gatekeeper is present, endpoints register and request admission with the gatekeeper. **Authentication and Encryption -** H.235 provides recommendations for authentication and encryption in H.323 systems.
Endpoint Location and Call Routing	Uses SIP URL for addressing. Redirect or location servers provide routing information.	Uses E.164 or H323ID alias and a address mapping mechanism if gatekeepers are present in the H.323 system. Gatekeeper provides routing information.

Table 4 – SIP and H.323

Information	SIP	H.323
Features	Basic call features.	Basic call features.
Conferencing	Basic conferencing without conference or floor control.	Comprehensive audiovisual conferencing support. Data conferencing or collaboration defined by T.120 specification.
Service or Feature Creation	Supports flexible and intuitive feature creation with SIP using SIP-CGI and CPL. Some example features include presence, unified messaging, or find me/follow me.	H.450.1 defines a framework for supplementary service creation.

Note: Basic call features include: call hold, call waiting, call transfer, call forwarding, caller identification, and call park.