Introduction to SIP

Stanley Wu (吳建澄)
skyeyester@gmail.com

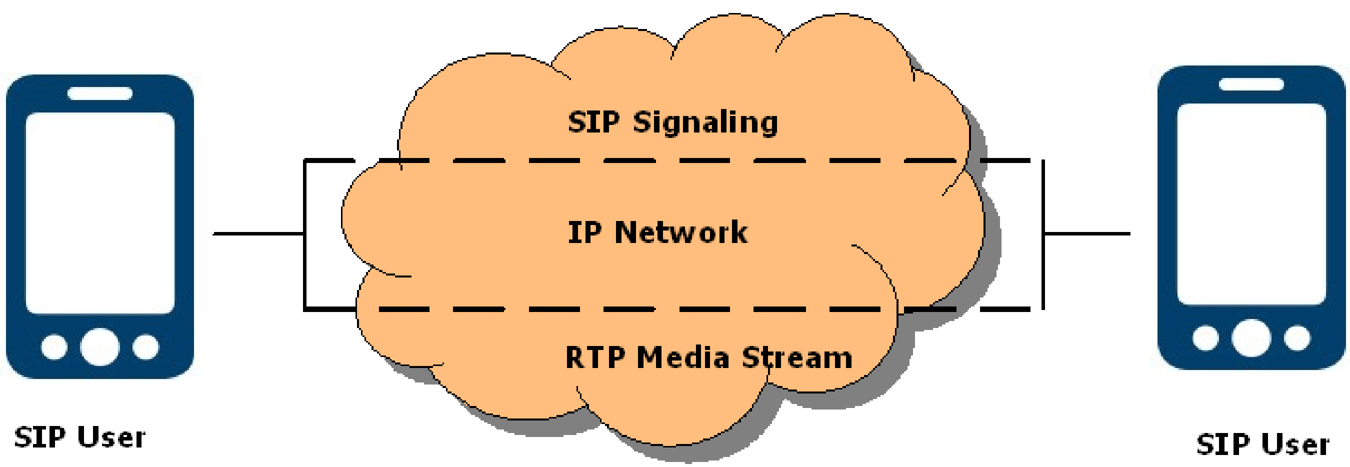
Dec. 12, 2015

Outline

- Introduction
- SIP Signaling
  - Request/Response
- SIP Logical Entities
- Basic Call Flow
- SIP Message Syntax Overview
  - Start Line
  - Message Header
- SIP Correlated Protocols
- SIP Signaling and VoIP analysis using a Wireshark Packet Analyzer

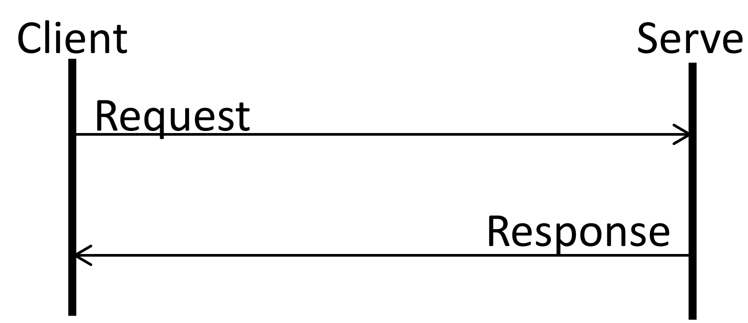
Introduction

- Session Initiation Protocol (SIP)
- SIP enable Internet Endpoints (Clients) to discover and establish a session between each other
  - ✓ A signaling protocol (application-layer control protocol)
  - ✓ For creating, modifying, and terminating sessions
  - ✓ Separate signaling and media streams
  - ✓ All kind of real-time multimedia types, such as voice, video or text messages



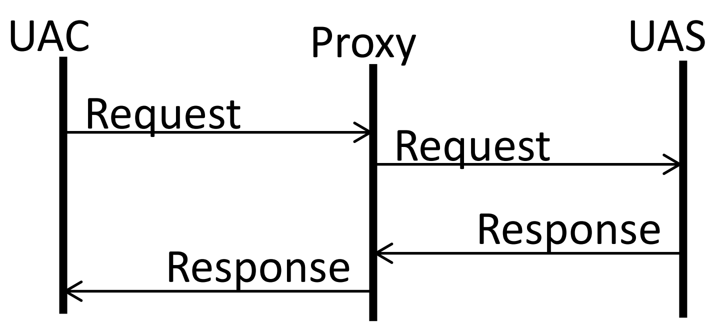
SIP Signaling

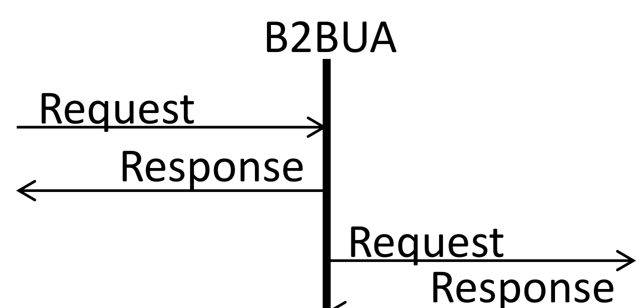
- SIP Message
  - SIP is a text-based protocol and uses the UTF-8 charset.
  - A SIP signaling is either a request message from a client to a server, or a response message from a server to a client.
    - **Request:** A SIP message sent from a client to a server, for the purpose of invoking a particular operation.
    - **Response:** A SIP message sent from a server to a client, for indicating the status of a request sent from the client to the server.
- SIP Addressing (URI)
  - E-mail like
  - user@host
  - sip:Alice@taipei.com



SIP Logical Entities

- User Agent (UA): An endpoint
  - User Agent Client (UAC): sends requests, receives responses
  - User Agent Server (UAS): receives requests, sends responses
- Proxy server: A network host that proxies requests and responses,
  - i.e., acts as a UAC and as a UAS.
- Redirect server: a UAS that redirects request to other servers.
- Back-to-back User Agent: a UAS linked to a UAC
  - Acts as a UAS and as a UAC linked by some application logic





Request Method

Name	Message Capability
INVITE	The user is begin invited to participate in a session.
ACK	The client has received a final response to an INVITE.
OPTIONS	The server is begin queried as to its capabilities.
BYE	The user terminated the session.
CANCEL	It cancels a pending request (not completed request).
REGISTER	It conveys the user’s location information to a SIP server.

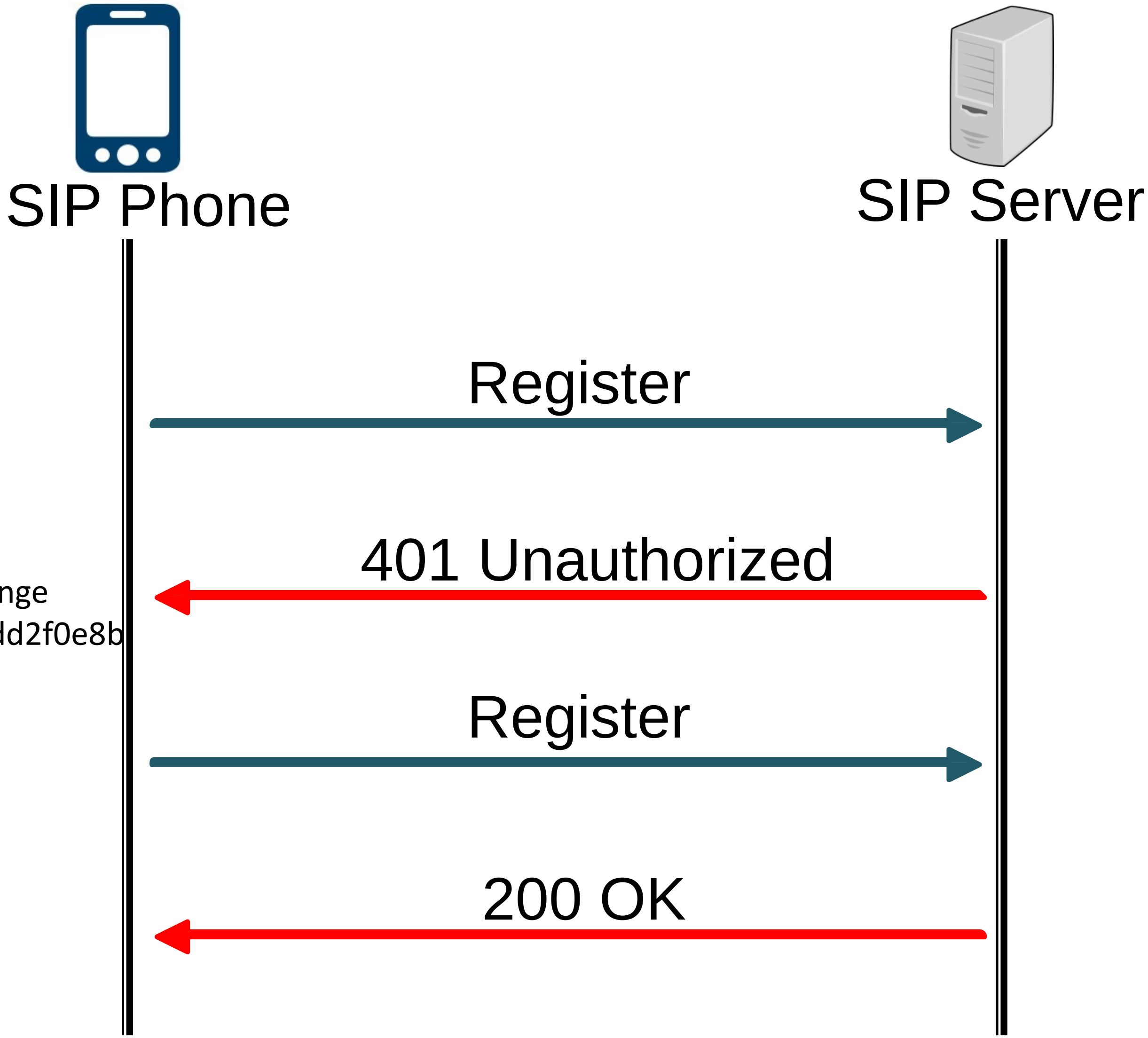
Request Method (cont.)

Name	Message Capability
SUBSCRIBE	installs a subscription for a resource
NOTIFY	informs about changes in the state of the resource
MESSAGE	delivers an Instant Message
INFO	used to transport mid-session information
PUBLISH	publication of presence information
UPDATE	changes the media description (e.g. SDP) in an existing session
REFER	used for call transfer, call diversion, etc.
PRACK	acknowledges a provisional response for an INVITE request

Response Code

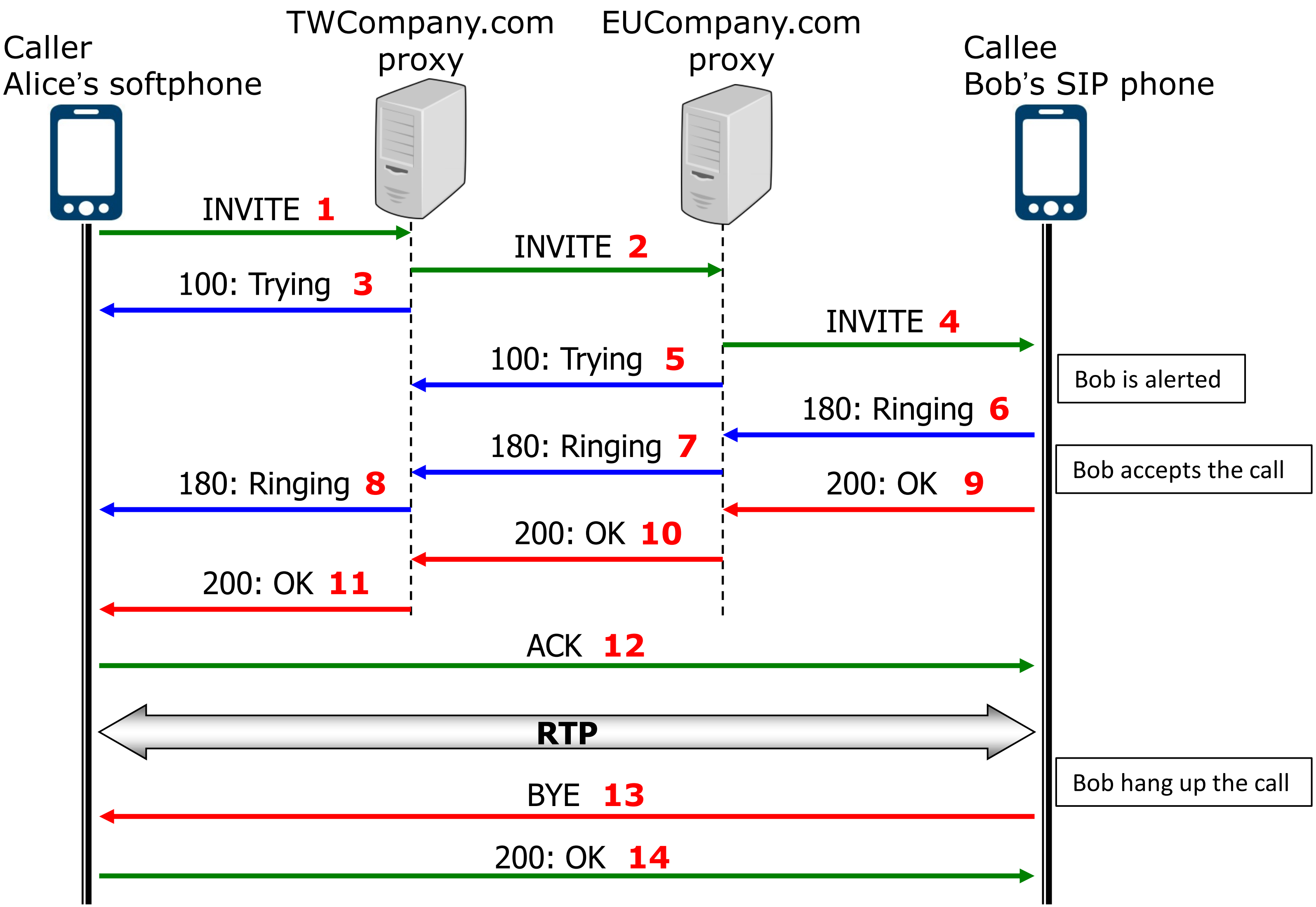
Serial Number	Status Code	Message Capability
1xx	Provisional	request received, continuing to process the request, **e.g. 100 Trying**
2xx	Success	the action was successfully received, understood, and accepted, **e.g. 200 OK**
3xx	Redirection	further action needs to be taken in order to complete the request, **e.g. 302 Moved Temporarily**
4xx	Client Error	the request contains bad syntax or cannot be fulfilled at this server, **e.g. 486 Busy Here**
5xx	Server Error	the server failed to fulfill an apparently valid request, **e.g. 501 Not Implemented**
6xx	Global Failure	the request cannot be fulfilled at any server, **e.g. 604 Does Not Exist Anywhere**

Basic Call Flow (Register)

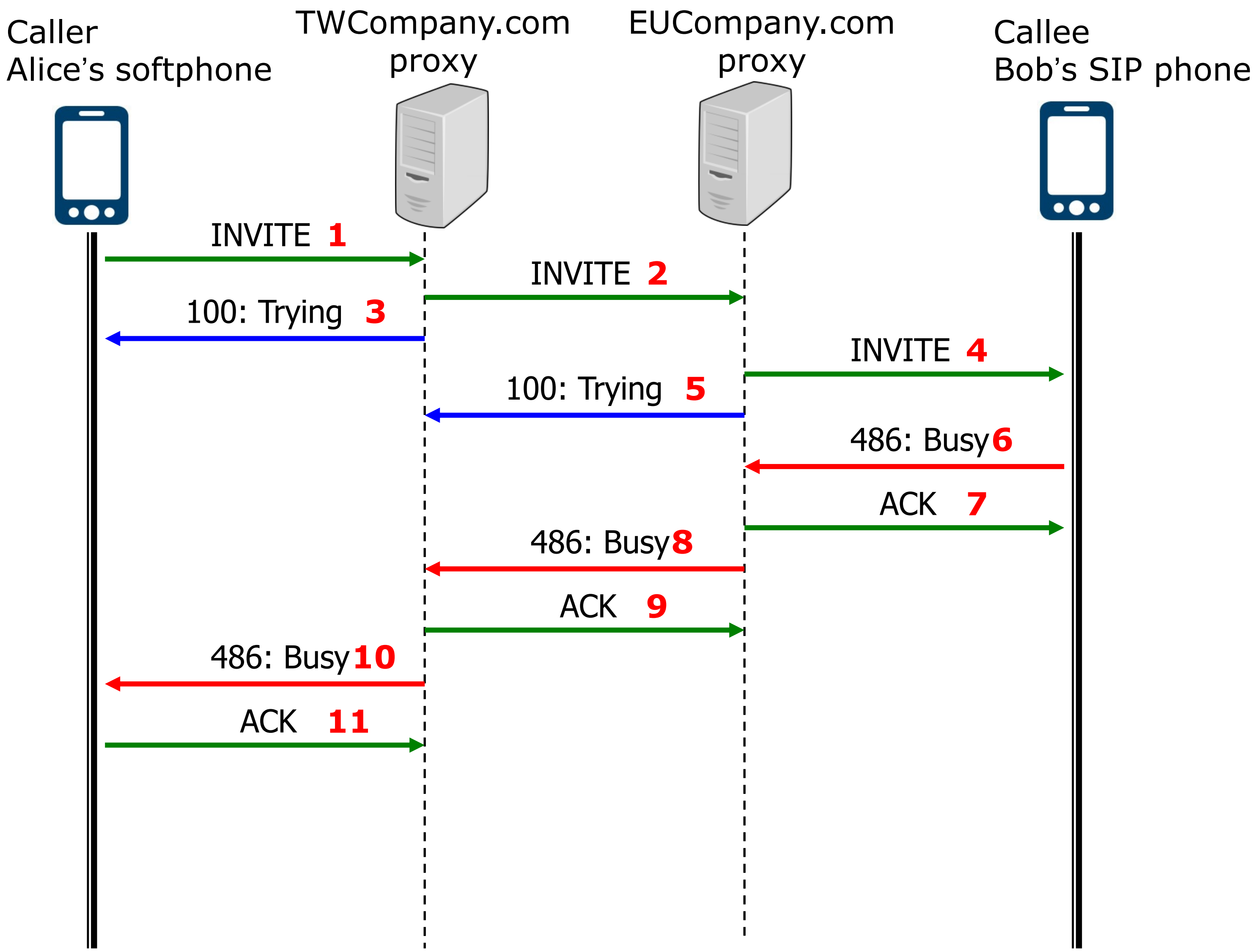


401 Unauthorized
Authentication challenge
nonce="dcd98b7102dd2f0e8b
11d0f600bfb0c093"

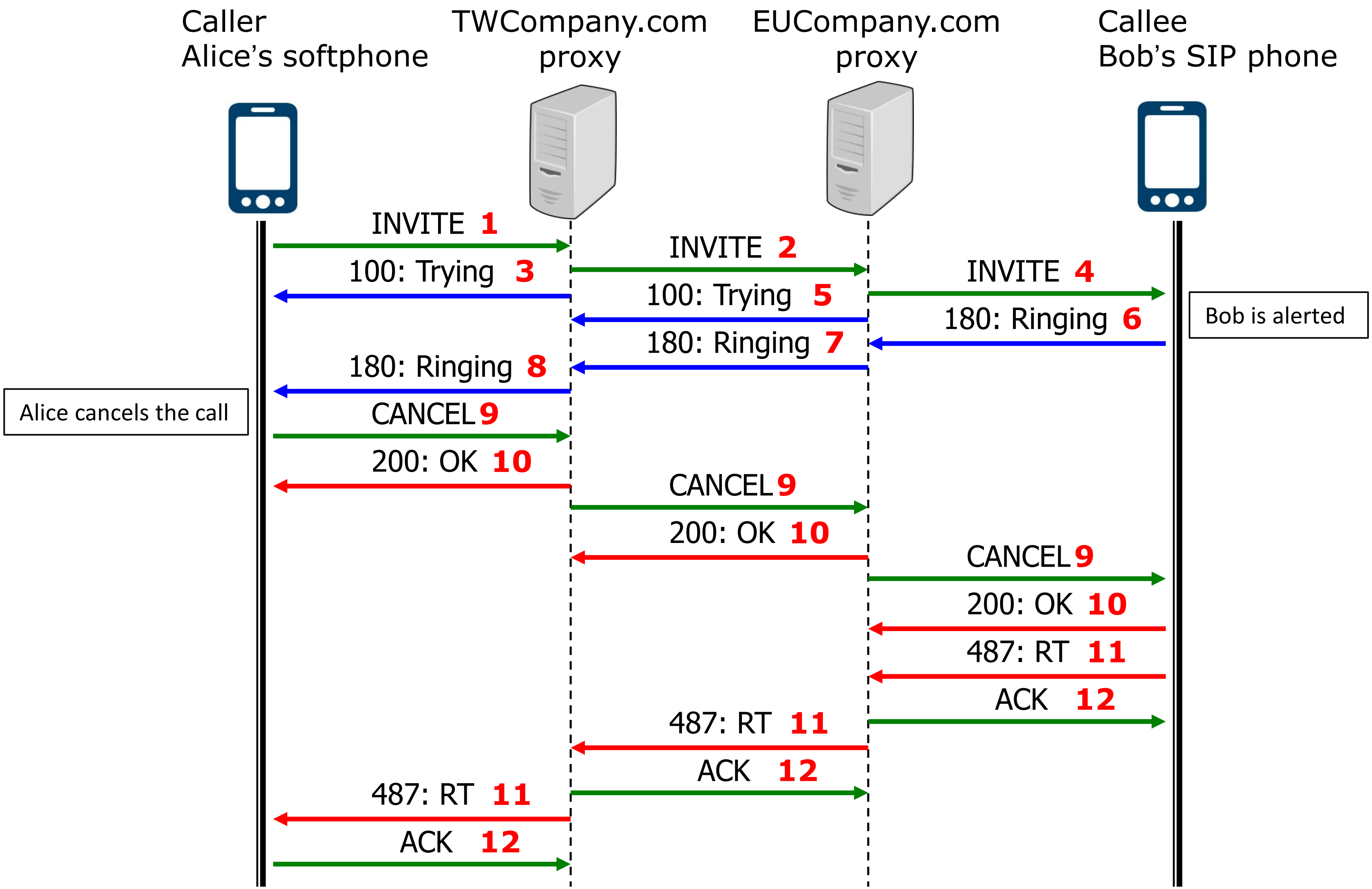
Basic Call Flow (Answer)



Basic Call Flow (Busy)



Basic Call Flow (Cancel)



PS: Request Terminated (RT)

SIP Message Syntax Overview

- Text-based
  - Use the UTF-8 charset (RFC 2279)
  - Syntax similar to HTTP/1.1 (RFC 2616)

```
generic-message = start-line
                  *message-header
                  CRLF
                  [message-body]
```

Start Line

start-line = Request-line | Status-line

Request-Line = **Method** SP **Request-URI** SP **SIP-Version** CRLF

Ex: **INVITE sip:Alice@TWCompany.com SIP/2.0**

Status-Line = **SIP-Version** SP **Status-Code** SP **Reason-Phrase** CRLF

Ex: **SIP/2.0 200 OK**

Message Header

```
message-header = ( general-header
                 | request-header
                 | response-header
                 | entity-header)
```

- General Header
  - Be applied to both request and response messages
- Entity Header
  - Define information about the message body
- Request Header
  - Allow the client to pass additional information about the request
- Response Header
  - Allow the server to pass additional information about the response

Message Header (cont.)

General-headers	Entity-headers	Request-headers	Response-headers
Accept	Content-Disposition	Authorization	Authenticateion-Info
Accept-Encoding	Content-Encoding	Max-Forwards	Error-Info
Accept-Language	Content-Language	Priority	Min-Expires
Alert-Info	Content-Length	Proxy-Authorization	Proxy-Authenticate
Allow	Content-Type	Proxy-Require	Retry-After
Call-ID		Route	Unsupported
Call-Info		Subject	Warning
Contact			WWW-Authenticate
CSeq			
Date			
Encryption			
MIME-Version			
Organization			
Expires			
From			
Record-Route			
Reply-To			
Require			
Supported			
Timestamp			
To			
Via			

Request Message Format

Command name	Request URI	Protocol version
Call-id: value		
Via: value		
From: value		
To: value		
Contact: value		
Cseq: value		
Content-Length: value		
Max-Forward: value		
Content-Type: value		
CRLF		
SDP		

Headers

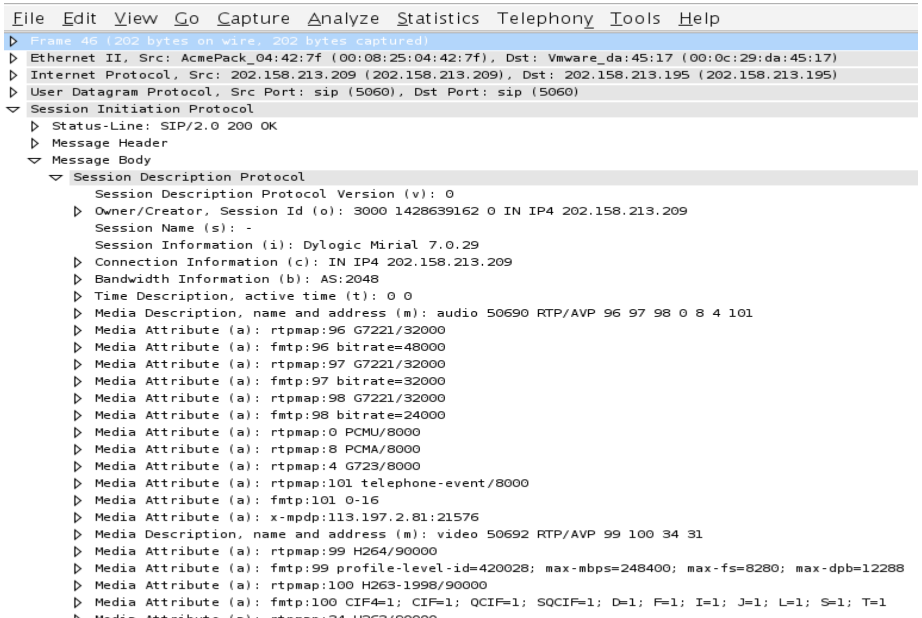
Parameter line

Request Message Example

- INVITE

Request-URI

INVITE sip:**<u>bob@biloxi.com</u>** SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142



Request Message Example (cont.)

- The attribute mechanism “a=“ is the primary means for extending SDP and tailoring it to particular applications or media.
- An example SDP description is:
- v=0
- o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
- s=SDP Seminar
- i=A Seminar on the session description protocol
- u=http://www.example.com/seminars/sdp.pdf
- e=j.doe@example.com (Jane Doe)
- c=IN IP4 224.2.17.12/127
- t=2873397496 2873404696
- a=recvonly
- **m=audio 49170 RTP/AVP 0**
- **m=video 51372 RTP/AVP 99**
- a=rtpmap:99 h263-1998/90000

Session description
v= (protocol version)
o= (originator and session identifier)
s= (session name)
i=* (session information)
u=* (URI of description)
e=* (email address)
p=* (phone number)
c=* (connection information -- not required if included in all media)
b=* (zero or more bandwidth information lines)
One or more time descriptions ("t=" and "r=" lines; see below)
z=* (time zone adjustments)
k=* (encryption key)
a=* (zero or more session attribute lines)
Zero or more media descriptions

Time description
t= (time the session is active)
r=* (zero or more repeat times)

Media description, if present
m= (media name and transport address)
i=* (media title)
c=* (connection information -- optional if included at session level)
b=* (zero or more bandwidth information lines)
k=* (encryption key)
a=* (zero or more media attribute lines)

Response Message Format

SIP/Protocol version	Response header
Call-id: value	
Via: value	
From: value	
To: value	
Contact: value	
Cseq: value	
Content-Length: value	
Max-Forward: value	
Content-Type: value	
CRLF	
SDP	

Headers

Parameter line

Response Message Example

- 200 OK

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP TWCompany.com:5060;branch=z9hG4bK8542.1
Via: SIP/2.0/UDP 140.113.102.103:5060;branch=z9hG4bK45a35h76
To: Alice <sip:alice.t@TWCompany.com>;tag=24019385
From: Bob <sip:bob.t@EUCompany.com>;tag=312345
Call-ID: 105637921@100.101.102.103
CSeq: 1 INVITE
Contact: sip:alice@140.201.202.203
Content-Type: application/sdp
Content-Length: 173

v=0
o= Alice 2452772446 2452772446 IN IP4 200.201.202.203
s=SIP Call
c=IN IP4 200.201.202.203
t=0 0
m=audio 56321 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

SIP Correlated Protocols

- Media information
  - SDP (Session Description Protocol) is responsible for setting the media attribute.
    - ✓ For example, setting the session port (port) and encoding (codec)
  - ✓ RTP （Real-time Transport Protocol）is the voice in a call or the video in a video call.
  - ✓ SRTP（Secure RTP) Since RTP can be intercepted and decoded easily by any network capture. SRTP uses AES as encryption to protect the voice

Session Description Protocol (SDP)

- SDP is a session description protocol for multimedia sessions
- SDP is used to describe the set of media streams, codecs, and other media related parameters supported by either party.
- All SIP implementations MUST support SDP, although they can support other bodies
- Used by other protocols than SIP: RTSP, SAP, etc.
- SDP was initially developed to support multicast sessions in the Internet. Gradually tailored for SIP purposes.

SDP Format

- Each field in the SDP message falls into one of the following categories:
  - Session name
  - Time the session is active
  - Media in the session and information required to receive the media
  - Information about bandwidth
  - Contact info for the responsible person
- Fields in SDP messages have the format <field code>=<value>. The field code is always a single letter.

SDP Format (mandatory fields)

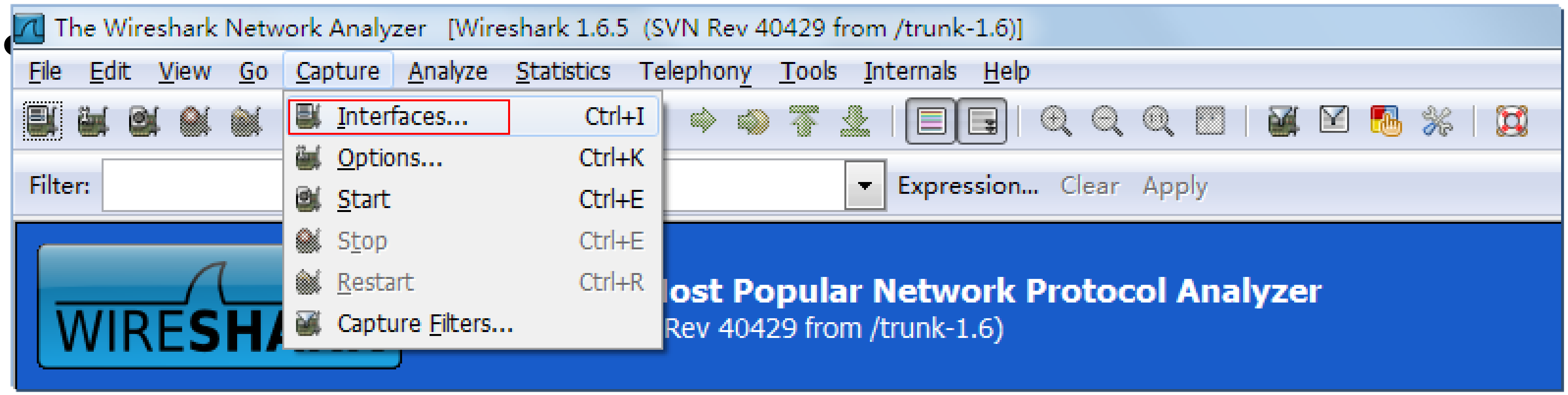
Field	Meaning	Format
v=	protocol version	v=0
o=	session owner and identifier	o=<username> <session id> <version> <network type> <address type> <address> In our example message above, the field was: o=root 1821 1821 IN IP4 10.10.1.99 ("IN" stands for Internet, "IP4" means IP version 4 address)
s=	session name	s=<session name> In our example, this was just: s=session
t=	time the session is active	t=<start time> <stop time> Even though this is a mandatory field in SDP, it is not very meaningful for SIP — it is not easy to predict the duration of a call. Usually, both values are the same. In our example, we have just "t=0 0". The times are decimal Network Time Protocol values (in seconds since the year 1900). In applications other than SIP, the SDP message can contain several "t= " lines, specifying additional periods of time when the session will be active.
m=	media type, format, and transport address	m=<media> <port> <transport> <format list> In our example message, this is: m=audio 11424 RTP/AVP 0 8 101 The <media> is either "audio" or "video" (if the call contained both audio and video, there would be two "m=" lines). The <port> should always be even (the even port is used by RTP and the next odd port by RTCP). <transport> is usually "RTP/AVP", denoting the RTP protocol with the profile for "Audio and Video Conferences with Minimal Control" (seeRFC3551). Under the AVP, the code 0 denotes G.711 uLaw, 8 stands for G.711 ALaw, 3 denotes the GSM codec, and for example the G.729 codec is denoted by 18. These codes appear in the <format list> part, and their order denotes the codec preferences of the given user agent. In our example, G.711 uLaw (code 0) is the most preferred codec and G.711 ALaw is the second most preferred. The codes not specified in the AVP can be introduced on a dynamic basis which is the case of the code 101 in our example message.

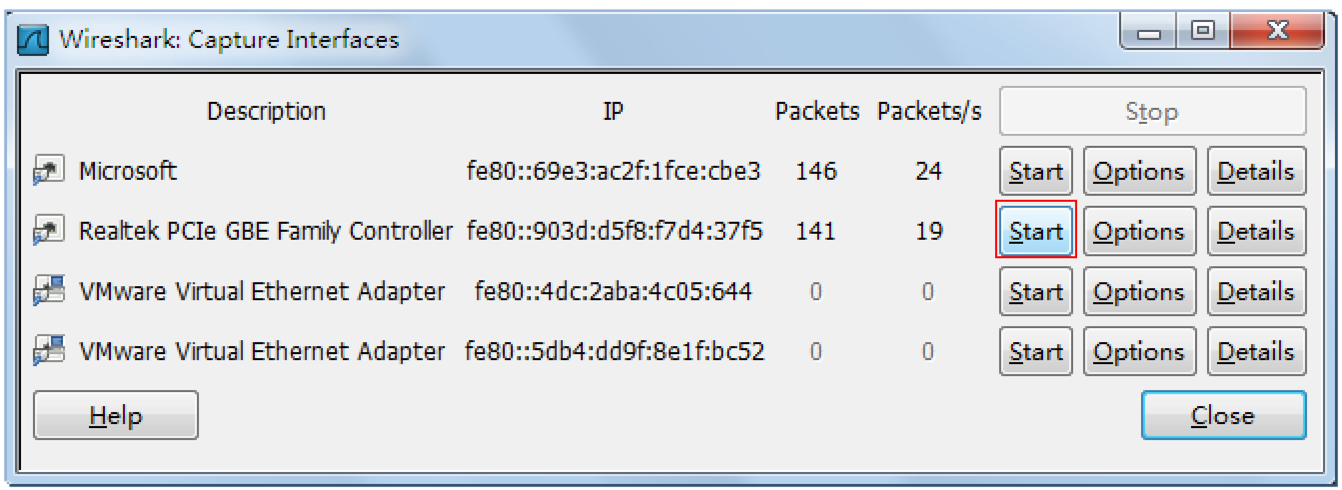
SDP Format (optional fields)

Field	Meaning	Format
c=	connection information	**c=<network type> <address type> <connection address>** In our example message, the field is as follows: c=IN IP4 10.10.1.99 This field is "semi-optional". It must appear either at the session level (like in our example) where it is valid for the entire session, or it must be included as a part of the "m=" field (after the <format list> part).
i=	session information	**i=<textual description>** The session information may appear at the session level or within the "m=" field (like the "c=" field above).
k=	encryption key	**k=<method>:<encryption key> or k=<method>** This parameter may appear at the session level or within the "m=" field.
a=	session attributes	**a=<attribute> or a=<attribute><value>** The SDP message may contain zero or several session attributes. There's quite a number of possible attributes and we will look at them below. Like the other optional fields in this table, "a=" may appear either at the session level or within the "m=" field. The session-level option is the usual one as is the case in our example message.

Attribute	Format and Description
rtpmap	**a=rtpmap:<payload type> <encoding name>/<clock rate> [/<encoding parameters>]** This attribute is called "rtpmap" because it defines a mapping from RTP payload codes (which are used in the <format list> in the "m=" field) to a codec name, clock rate, and other encoding parameters. The "rtpmap" field must be used for dynamic payload types (i.e. types that are not predefined in the AVP profile) but it is quite common to use it even for the types that are already defined in the AVP profile. In our example message, one of the "rtpmap" attributes is "a=rtpmap:0 PCMU/8000"
sendrecv	a=sendrecv This attribute means that we are going to both send and receive media. This is the option you will see with SIP, the other options ("sendonly", "recvonly", "inactive", "broadcast") would be highly unusual for a phone call.
ptime	**a=ptime:<packet time>** This parameter describes the length of time (in milliseconds) carried in one RTP packed.
fmtp	**a=fmtp:<format> <format specific parameters>** This option allows to define parameters that are specific for a given format code. SDP does not need to understand the parameters, it only transports them.

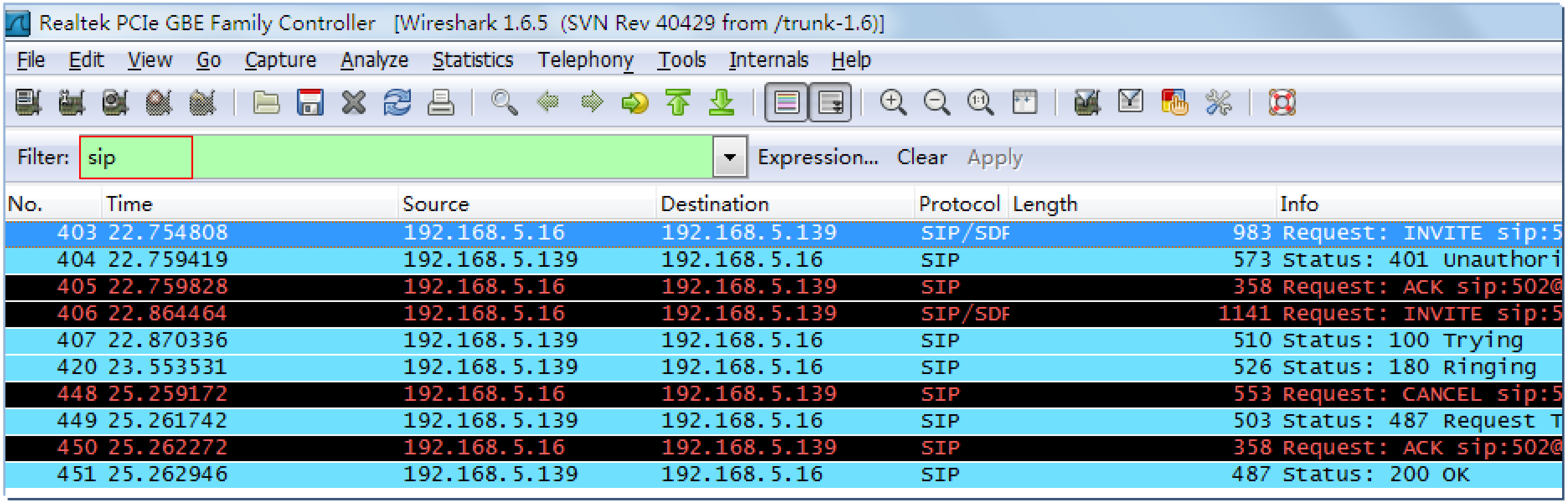
Development Log Tool





Development Log Tool

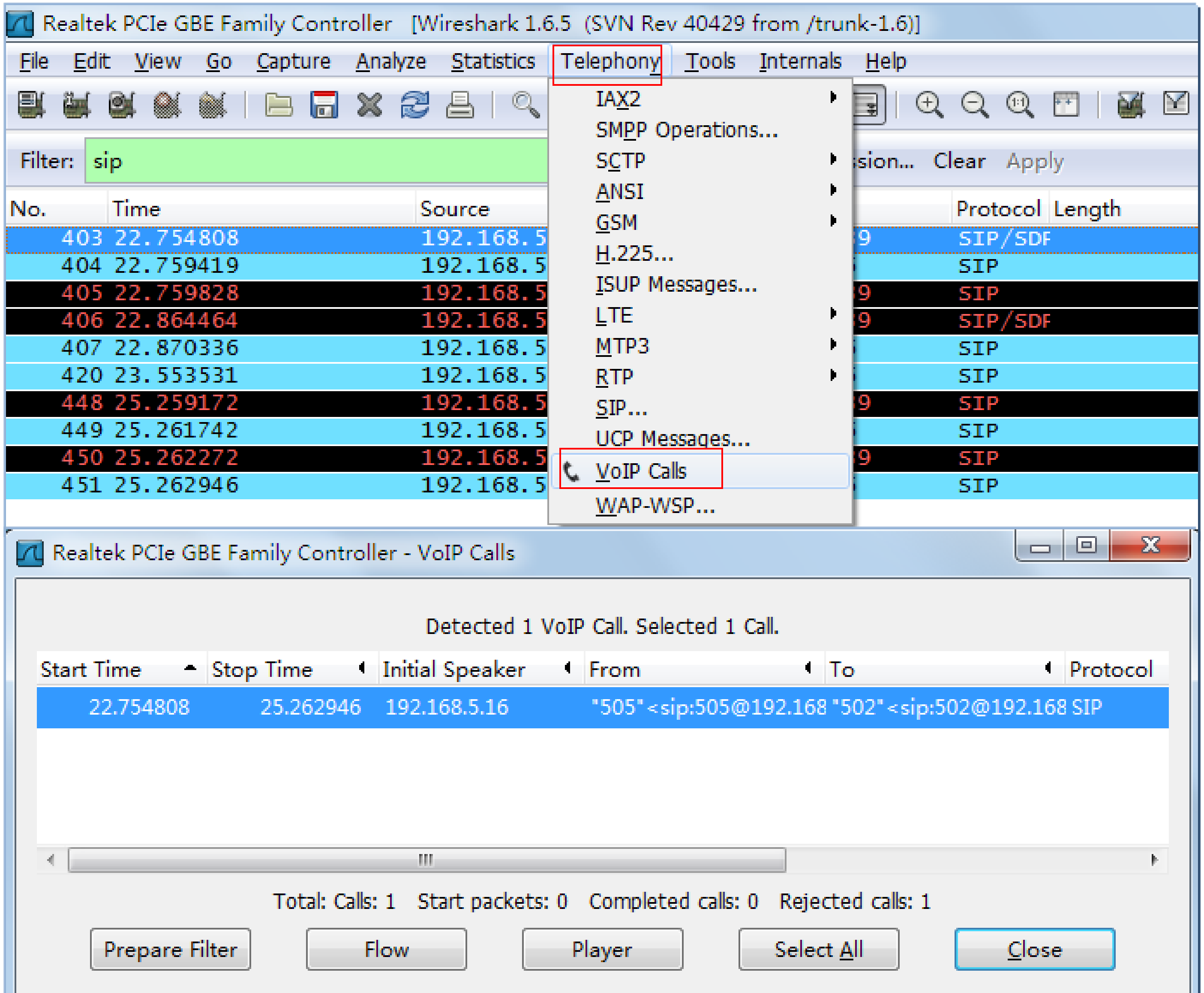
- Real-time view sip packet



No.	Time	Source	Destination	Protocol	Length	Info
403	22.754808	192.168.5.16	192.168.5.139	SIP/SDF	983	Request: INVITE sip:5
404	22.759419	192.168.5.139	192.168.5.16	SIP	573	Status: 401 Unauthori
405	22.759828	192.168.5.16	192.168.5.139	SIP	358	Request: ACK sip:502@
406	22.864464	192.168.5.16	192.168.5.139	SIP/SDF	1141	Request: INVITE sip:5
407	22.870336	192.168.5.139	192.168.5.16	SIP	510	Status: 100 Trying
420	23.553531	192.168.5.139	192.168.5.16	SIP	526	Status: 180 Ringing
448	25.259172	192.168.5.16	192.168.5.139	SIP	553	Request: CANCEL sip:5
449	25.261742	192.168.5.139	192.168.5.16	SIP	503	Status: 487 Request T
450	25.262272	192.168.5.16	192.168.5.139	SIP	358	Request: ACK sip:502@
451	25.262946	192.168.5.139	192.168.5.16	SIP	487	Status: 200 OK

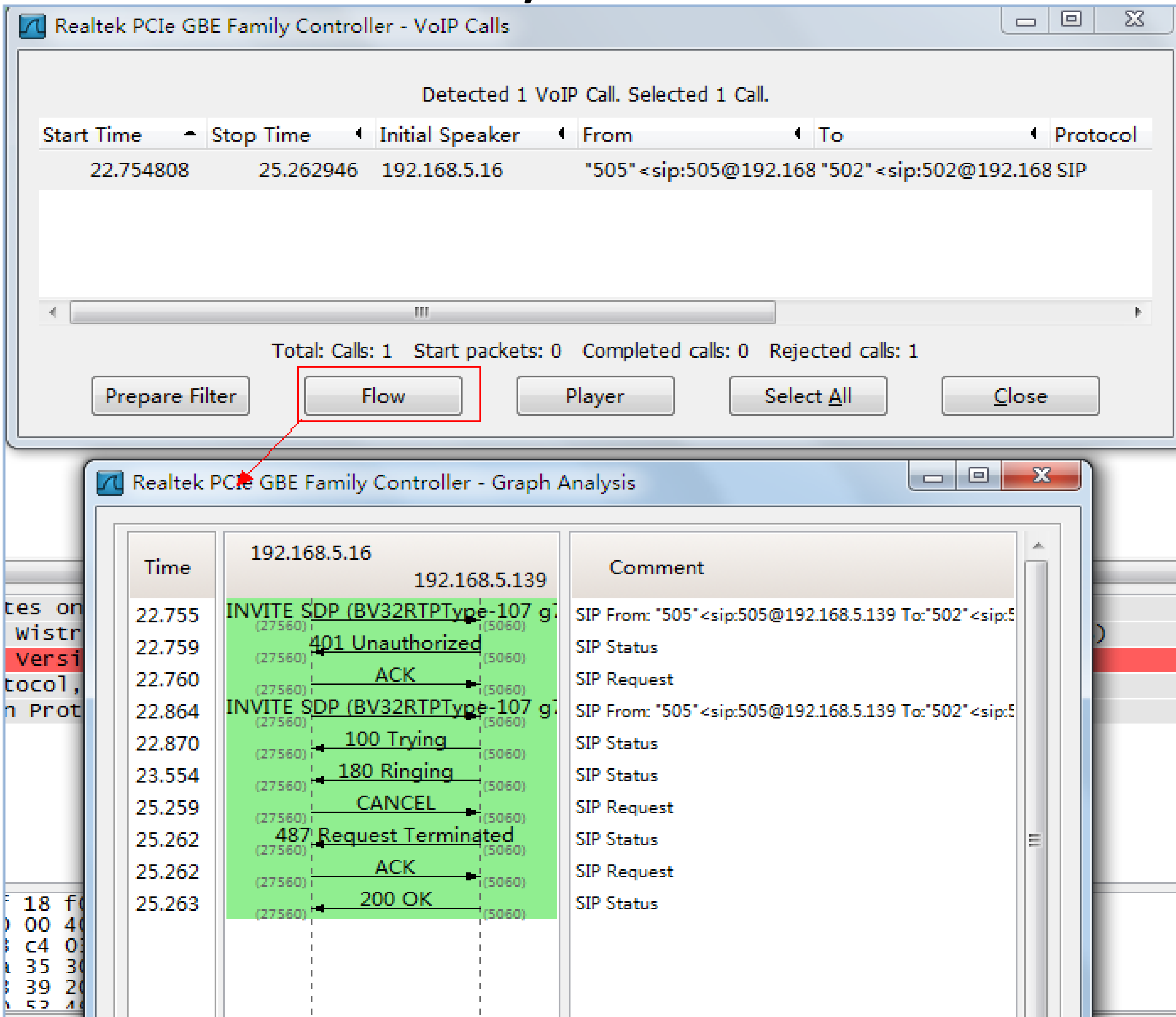
Development Log Tool

- SIP Conversation Analysis



Development Log Tool

- SIP Conversation Analysis



Reference

- Session Initiation Protocol (RFC 3261)
- Session Initiation Protocol Basic Call Flow Examples (RFC 3665)
- The SIP INFO Method (RFC 2976)
- The Session Initiation Protocol Refer Method (RFC 3515)
- Session Description Protocol (SDP) (RFC 3264, 4566)
- Transport Protocol for Real-Time Applications (RTP) (RFC 3550)
- The Secure Real-time Transport Protocol (SRTP) (RFC 3711)
- Wireshark