Università di Genova *Telematica 2*
Facoltà di Ingegneria

1. Servizi Multimediali e Qualità del Servizio (QdS) su IP

1.8 Session Initiation Protocol (SIP)

Prof. Raffaele Bolla

SIP – *Session Initiation Protocol*

- Definito dagli RFC 3261-3265 (e da molti altri) in ambito IETF.
- Rappresenta la soluzione VoIP proveniente dal mondo Internet, alternativa allo standard H.323.
- L'approccio SIP, al contrario di quello H.323, è fortemente decentralizzato.
- SIP è più di un protocollo di segnalazione per VoIP: permette di creare sessioni tra due entità.

SIP – *Session Initiation Protocol*

- SIP è un protocollo di tipo testuale
  - basato su HTTP e SMTP.
- La funzione principale è quella di creare w gestire "sessioni" tra gli utenti.
- SIP crea una comunicazione *peer-to-peer*
  - non vengono identificati master/slave,
  - la comunicazione avviene comunque con un paradigma client-server
    - » Il ruolo di server viene assegnato sulla base di chi inizia la sessione.

Caratteristiche generali

- SIP nasce nell'ambito IETF
  - gruppo di lavoro di volontari;
  - collaborazione a livello mondiale
    - » esperti in tutte le aree della tecnologia Internet.
- Lo standard è basato sulla sperimentazione
  - gli sviluppatori creano le nuove proposte implementando le loro idee;
  - le nuove funzionalità entrano a far parte dello standard solo dopo essere state giudicate "mature"
    - » numerosi test di funzionamento ed interoperabilità.

Caratteristiche generali

- SIP permette di:
  - localizzare gli utenti;
  - creare sessioni;
  - registrare la presenza degli utenti;
  - trasportare diversi tipi di segnalazione: descrizioni di sessioni, *instant messaging*, JPEG, e codifiche MIME.
- SIP è particolarmente adatto per applicazioni che utilizzano il concetto di sessione (non solo VoIP):
  - sistemi virtuali distribuiti;
  - giochi in rete (Quake II/III);
  - videoconferenze.

Caratteristiche generali

- SIP non è:
  - un protocollo di trasporto;
  - un meccanismo di QoS;
  - un protocollo di controllo dei gateway o per *Remote Procedure Call* (RPC);
  - un rimpiazzo dei protocolli per PSTN;
  - una mera implementazione di VoIP
    - » in questo è molto distante da H.323, il quale specifica protocolli per tutti gli aspetti relativi all'applicazione VoIP (segnalazione, trasporto, controllo, ecc.).

Caratteristiche alla base del SIP

- L'infrastruttura segue il modello IP
  - intelligenza e stato concentrate nei dispositivi terminali;
  - il *core* della rete mantiene al più uno stato temporaneo;
  - vantaggi: minore necessità di CPU e memoria nei server, affidabilità e scalabilità (non esiste un unico punto critico).
- Supporto per UDP
  - *set-up* più rapido, minor informazioni di stato.

Caratteristiche alla base del SIP

- Estensibilità
  - la gamma dei servizi futuri non può essere nota
    - » rendere la segnalazione indipendente dal servizio;
  - lezione dell'HTTP
    - » HTTP non è più limitato all'HTML: e-commerce, servizi bancari, film, ecc.
    - » le applicazioni crescono, il protocollo rimane lo stesso;
  - i progettisti SIP hanno sfruttato l'esperienza HTTP.

Funzionalità

- Instaurazione chiamate voce su IP
  - servizi PSTN tradizionali (PBX);
  - preferenze degli utenti (media, lingua, mobilità).
- Instaurazione conferenze multimediali.
- Gestione della mobilità (*number portability*)
- Notifica eventi (iscrizione/notifica)
  - presenza;
  - *instant communications*.
- Messaggistica testuale e generica.
- Trasporto segnalazione
  - controllo delle chiamate (attesa, parcheggio, ...).
- Servizi integrati con la rete PSTN.

Elementi

- ***Endpoint***
  - realizzano il protocollo SIP;
  - sono host "*fully qualified*";
  - esistono due tipologie di apparati:
    - » **dispositivi utente**: telefoni, PC;
    - » ***gateway*** verso altre reti: PSTN, H.323;
  - la parte che realizza il protocollo viene definita User Agent (hw o applicativi):
    - » UA client (originano richieste SIP);
    - » UA server (originano risposte SIP).
  - la funzionalità client/server può essere variata spesso nel corso di una sessione.

Elementi

- ***Server***
  - sono dispositivi intermediari all'interno delle rete SIP
    - » supportano gli utenti per inizializzare le sessioni e altre funzioni;
  - sono solo intermediari per la segnalazione
    - » non sono in grado di gestire il flusso dei media
  - in genere intervengono su richiesta di un *endpoint*
    - » possono anche effettuare operazioni autonome;
  - possono essere senza stato
    - » tempi di risposta molto rapidi,
    - » non rappresentano un punto critico in caso di rottura o malfunzionamento;

Elementi

- l'RFC 2543 definisce 3 tipologie di server:
  - » ***proxy SIP***
    - ✓ agiscono come intermediari nella segnalazione inoltrando le richieste,
    - ✓ possono mantenere uno stato della connessione;
  - » ***redirect server***
    - ✓ redireziona una richiesta;
  - » ***registrar server***
    - ✓ accetta registrazioni da parte degli utenti;
    - ✓ mantiene traccia della locazione degli utenti (come l'HLR nelle reti GSM);
- possono essere co-locati sulla stessa macchina;

Elementi

- gli *endpoint* possono localizzare i server tramite:
  - » una configurazione esplicita dell'indirizzo IP del server (***outbound proxy***),
  - » una URL SIP del dominio (***inbound proxy***),
  - » l'utilizzo di un indirizzo multicast (per es. per i ***registrar server***),
  - » l'intermediazione di altri server (per es. un *outbound proxy* per raggiungere un *registrar server*).

Elementi

- ***Location server***
  - consiste in un database contenente informazioni relativa agli utenti (indirizzi IP, URL, script, preferenze) e alla locazione di proxy, gateway e altri location server
    - » SQL, LDAP, Corba, tecnologie proprietarie…
  - di norma non viene contattato direttamente dagli utenti
    - » i server SIP utilizzano protocolli non-SIP per interagire con i location server.

Funzionalità

- Indirizzamento stile web/telefonico.
- Registrazione dei dispositivi.
- Sicurezza.
- Redirezione delle chiamate.
- Proxy.
- Forking.
- Rendezvous e presenza
  - rendezvous attivi o passivi.

Funzionalità

- Mobilità
  - diversi apparati/reti di accesso.
- Preferenze dell'utente
  - chiamante: tipo di servizio, modalità di fruizione del servizio, raggiungibilità di parte degli utenti (esclusioni di numerazioni/servizi);
  - chiamato: gestione delle chiamate (in base al chiamante, giorno e data, dispositivo di comunicazione preferito).
- Controllo dell'instradamento dei messaggi.

Richieste e risposte

- SIP prevede un funzionamento client/server, simile a quello dell'HTTP.
- I client effettuano delle richieste (*metodi*) ai server che possono essere di due tipi:
  - metodi base (RFC 2543): INVITE, ACK, BYE, CANCEL, REGISTER, OPTIONS;
  - altri metodi: estensioni al protocollo definite in RFC successivi.
- I server forniscono delle *risposte* che*:*
  - consistono in codici numerici,
  - derivano da quelle definite per HTTP.

Richieste e risposte

Classi di risposte

Classe	*Descrizione*
1xx	Informativo: la richiesta è in fase di elaborazione ma non ancora completa.
2xx	Successo: la richiesta è stata completata con successo.
3xx	Redirezione: la richiesta deve essere inoltrata ad un'altra locazione.
4xx	Errore del client: la richiesta deve essere riformulata in modo corretto.
5xx	Errore del server: la richiesta non può essere completata dal server, ma può essere inoltrata ad un'altra locazione.
6xx	Fallimento globale: la richiesta è fallita e non può essere riprovata di nuovo.

SIP/IP

- I messaggi SIP possono essere inviati su IP utilizzando qualsiasi protocollo di trasporto (TCP, UDP o altri):
  - **UDP**: è la scelta più comune perché:
    - » SIP possiede dei meccanismi di recupero di errore integrati
    - » minor *overhead* nei proxy;
    - » massima dimensione dei pacchetti minore;
  - **TCP**: scelta meno frequente perché introduce un maggior *overhead* per il *setup* di una connessione, per contro:
    - » può multiplare diversi flussi di segnalazione su un'unica linea
    - » può essere utilizzato con SSL;
  - **SCTP**: nuovo protocollo che introduce comunque un certo *overhead* per il *setup* di una connessione ma permette la gestione
    - » Degli indirizzi di *fallback*;

Le funzioni di SIP

- Risoluzione degli indirizzi.
- Funzioni relative ad una sessione
  - instaurazione, modifica, termine e cancellazione della sessione,
  - negoziazione dei media,
  - segnalazione durante la chiamata,
  - controllo della chiamata,
  - instaurazione di chiamate con QoS.
- Funzioni non relative ad una sessione
  - mobilità,
  - trasporto di messaggi,
  - notifica di eventi,
  - autenticazione.

Le funzioni di SIP

- **Risoluzione degli indirizzi.**
- Funzioni relative ad una sessione
  - instaurazione, modifica, termine e cancellazione della sessione,
  - negoziazione dei media,
  - segnalazione durante la chiamata,
  - controllo della chiamata,
  - instaurazione di chiamate con QoS.
- Funzioni non relative ad una sessione
  - mobilità,
  - trasporto di messaggi,
  - notifica di eventi,
  - autenticazione.

Indirizzamento

- Gli utenti sono individuati con una URL:

  sip:alice@unige.it

  sip:+1-613-555-1212@wcom.com; user=phone
  - lo spazio degli indirizzi risulta praticamente illimitato.
- L'indirizzo può contenere numeri di telefono, fax, parametri (tipo terminale, protocollo di traporto), cifre post-dialing:

  sip:+1-613-555-1212@wcom.com; user=phone; postd=pp32
- Si possono utilizzare anche le URL per i numeri telefonici (globali o locali):

  tel:+390103532057

  tel:+390103532057; phone-context=+39010353

  fax:+390103532154

Indirizzamento

- Un utente in genere ha una sola URL del tipo:

  utente@dominio
- La localizzazione dell'utente avviene tramite l'associazione

  utente@dominio ↔ utente@host

  contenuta nel ***location server***.

Identificazione degli utenti

- Attualmente esiste un elevato numero di reti di comunicazione
  - PSTN, cellulare, Internet.
- La tradizionale forma di indirizzamento identifica i terminali piuttosto che gli utenti
  - l'email rappresenta già un'evoluzione di questo concetto;
  - un utente risponde normalmente a più numeri a seconda del terminale e di dove si trova.
- L'evoluzione attuale mira ad associare un identificativo unico a tutte le persone.

Indirizzamento

Identificazione degli utenti

- Per individuare i singoli individui si può utilizzare
  - una URI (***Universal Locator Identifier***), come negli indirizzi email:
    - » è più menmonica dei numeri;
    - » è molto flessibile;
    - » lo spazio di indirizzamento è praticamente illimitato.
  - un numero, come nella numerazione telefonica E.164
    - » rappresenta una soluzione attualmente più diffusa;
    - » praticamente qualsiasi dispositivo di comunicazione comprende una tastiera numerica a 12 cifre (10 cifre, "#", "*").

Indirizzamento

Indirizzamento gerarchico E.164: ENUM

- L'ampia diffusione delle reti telefoniche tradizionali (PSTN, cellulare) e la necessità di integrazione verso di esse ha portato l'IETF a standardizzare un meccanismo di risoluzione degli indirizzi E.164 mediante DNS (ENUM, RFC 3761).
- Il meccanismo si articola su tre livelli gerarchici:
  - la root DNS: e164.arpa;
  - autorità ENUM nazionali;
  - server proxy SIP per l'instradamento delle chiamate.

Indirizzamento

ENUM – *Top Level Domain*

- Il dominio e164.arpa rappresenta il *Top Level Domain* (TLD) del sistema ENUM.
- I client DNS effettuano una *query* al TLD dopo aver trasformato l'identificativo E.164:
  - al numero E.164 vengono tolti tutti caratteri che non sono cifre;
  - le cifre sono scritte in ordine inverso e separate da ".";
  - il dominio principale e164.arpa viene aggiunto;
  - es.: +39-010-3532057 ⇒ 7.5.0.2.3.5.3.0.1.0.9.3.e164.arpa.
- La risoluzione del sottodominio viene delegata in base alle disposizioni delle diverse autorità nazionali
  - possono essere identificate diverse "sottozone" (es. 010).

Indirizzamento

ENUM – Secondo livello

- I server primari reindirizzano le richieste ai server DNS ENUM (secondo livello).
- I server DNS ENUM realizzano l'effettiva risoluzione dell'indirizzo attraverso l'informazione contenuta nei record NAPTR (*Naming Authority Pointer)* che:
  - In generale permettono di specificare delle regole attraverso le quali è possibile rielaborare il nome da risolvere e interrogare un server successivo;
  - nel caso di ENUM questi record traducono un E.164 in una URL;
  - es: +39-010-3532075

```
$ORIGIN 5.7.0.2.3.5.3.0.1.0.9.3.e164.arpa.
NAPTR 10 100 "u" "E2U+sip" "!^.*$!sip:lelus@unige.it!" .
NAPTR 10 110 "u" "E2U+smtp" "!^.*$!mailto:lelus@unige.it!" .
NAPTR 10 120 "u" "E2U+tel" "!^.*$!tel:+39-010-3532075!" .
```


Indirizzamento

ENUM – Terzo livello

- Il terzo livello di risoluzione può essere un server DNS o un altro tipo di entità
  - dipende in maniera sostanziale dall'applicazione.
- Nel caso di SIP l'entità deve avere determinate caratteristiche:
  - sicurezza: gli utenti devono poter modificare solo i propri record (autenticazione);
  - dinamicità: i dati degli utenti possono cambiare molto rapidamente (*real time*).
- Un *registrar server* assolve a queste funzionalità
  - mantiene una corrispondenza aggiornata sulla attuale presenza e posizione degli utenti;
  - mantiene una lista delle preferenze degli utenti.

Indirizzamento

Identificazione degli utenti

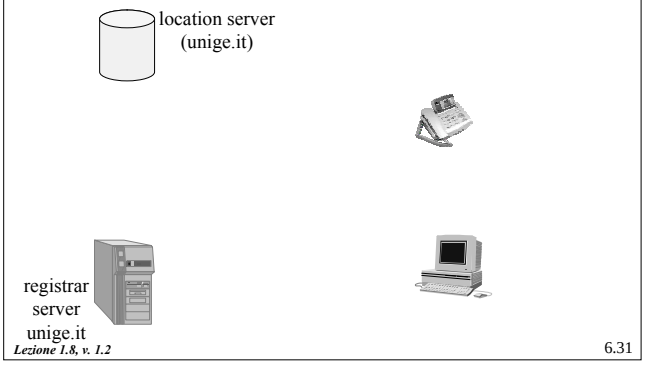
- La risoluzione degli alias degli utenti può avvenire:
  - tramite un sistema simile al precedente
    - » utilizzo dei record NAPTR,
    - » massima flessibilità;
  - tramite i record SRV (SeRVice) del DNS
    - » es.:

```
_sip._tcp  SRV  0   0   5060   sipserver.unige.it
           SRV  1   0   5060   sipbackup.unige.it
```

    - » è possibile gestire la priorità (*backup*) ed il "peso" (*load balancing*).
- In entrambi i casi è possibile utilizzare un *registrar server* per localizzare l'utente e utilizzare le sue preferenze.

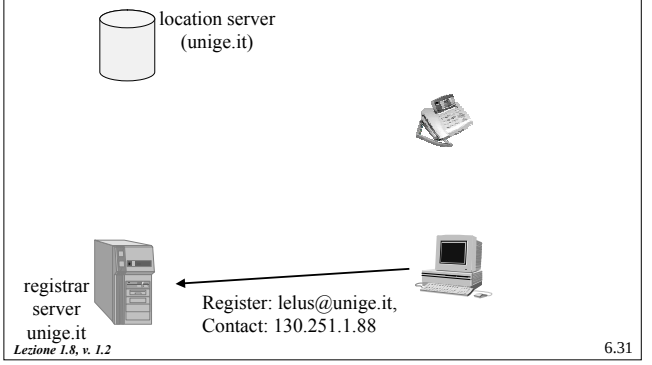
Indirizzamento

Registrazione



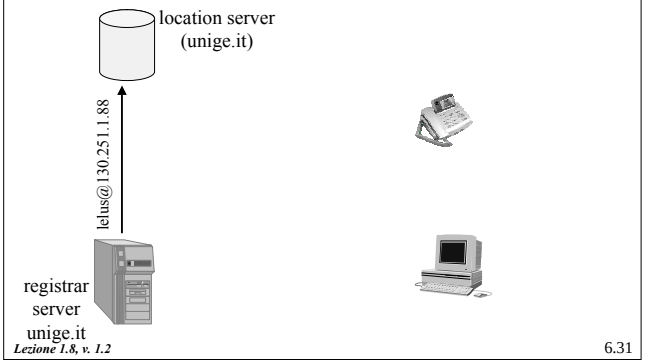
Indirizzamento

Registrazione



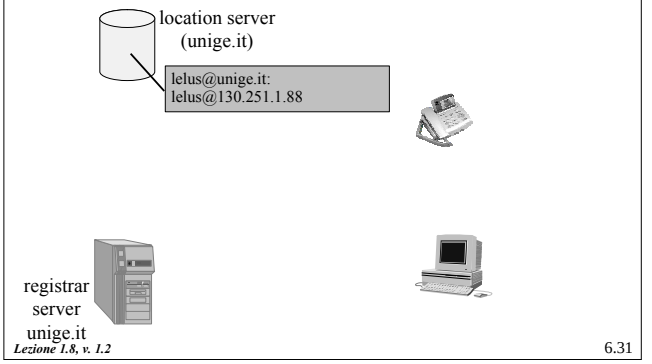
Indirizzamento

Registrazione



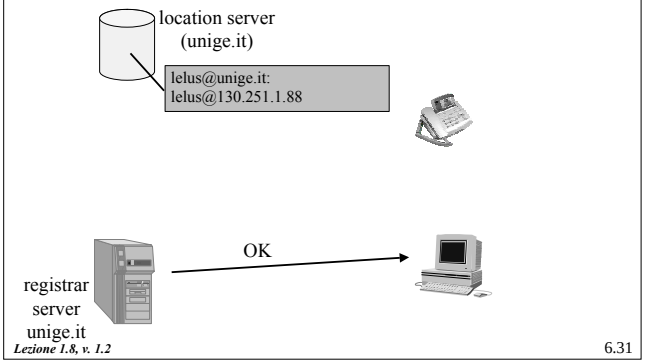
Indirizzamento

Registrazione



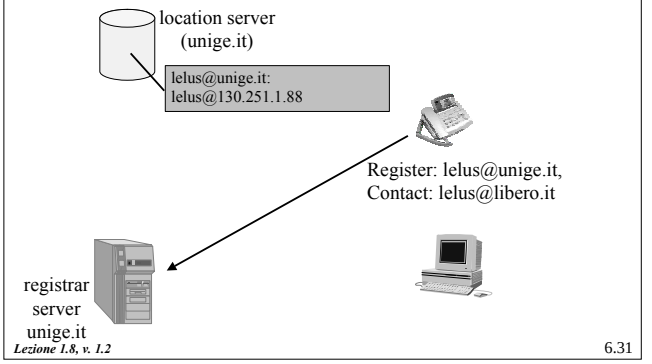
Indirizzamento

Registrazione



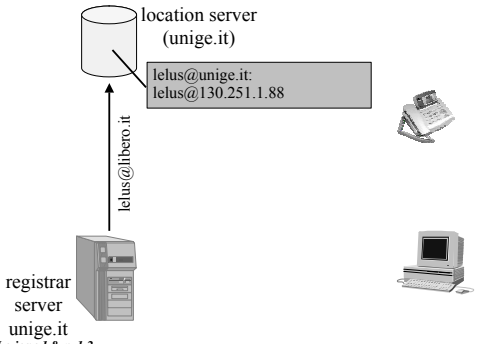
Indirizzamento

Registrazione



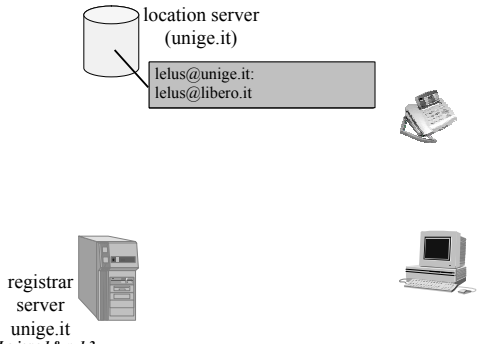
Indirizzamento

Registrazione



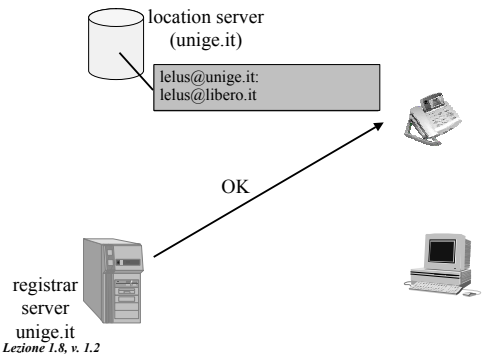
Indirizzamento

Registrazione



Indirizzamento

Registrazione



Le funzioni di SIP

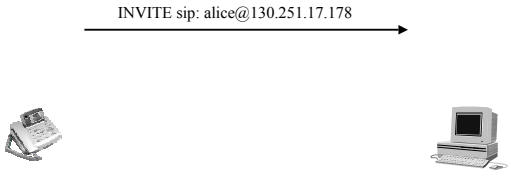
- Risoluzione degli indirizzi.
- Funzioni relative ad una sessione
  - instaurazione, modifica, termine e cancellazione della sessione,
  - negoziazione dei media,
  - segnalazione durante la chiamata,
  - controllo della chiamata,
  - instaurazione di chiamate con QoS.
- Funzioni non relative ad una sessione
  - mobilità,
  - trasporto di messaggi,
  - notifica di eventi,
  - autenticazione.

Setup delle connessioni

Connessione diretta tra terminali

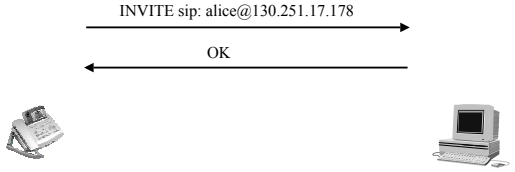
Setup delle connessioni

Connessione diretta tra terminali



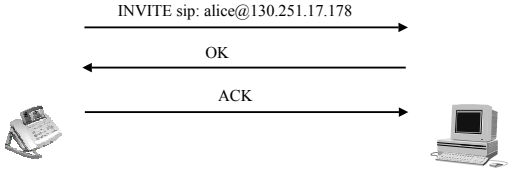
Setup delle connessioni

Connessione diretta tra terminali



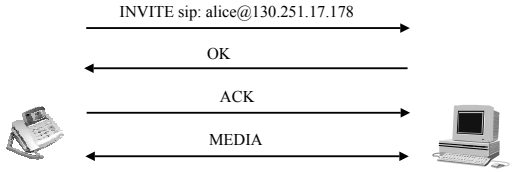
Setup delle connessioni

Connessione diretta tra terminali



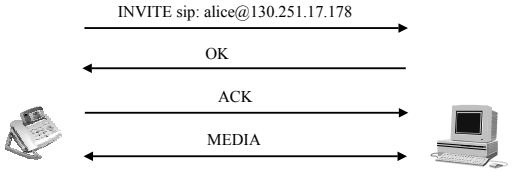
Setup delle connessioni

Connessione diretta tra terminali



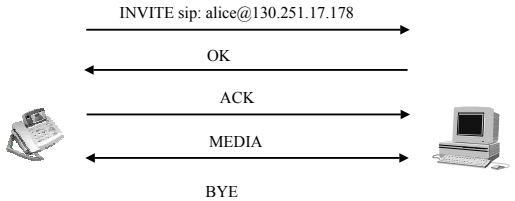
Setup delle connessioni

Connessione diretta tra terminali



Setup delle connessioni

Connessione diretta tra terminali

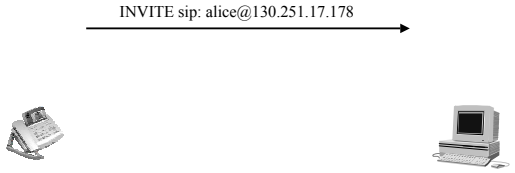


Setup delle connessioni

Connessione diretta tra terminali

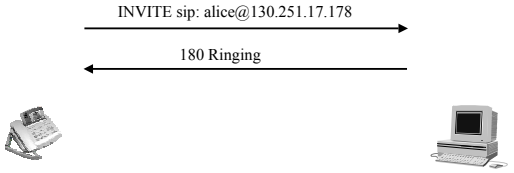
Setup delle connessioni

Connessione diretta tra terminali



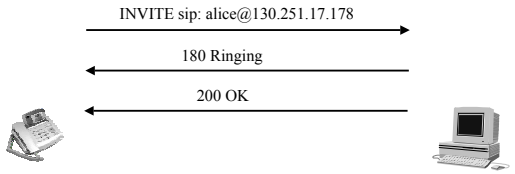
Setup delle connessioni

Connessione diretta tra terminali



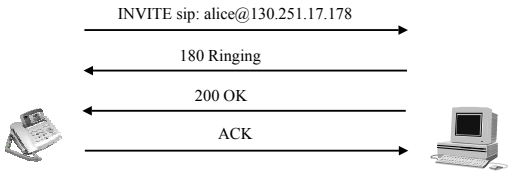
Setup delle connessioni

Connessione diretta tra terminali



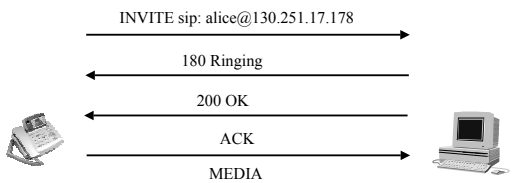
Setup delle connessioni

Connessione diretta tra terminali



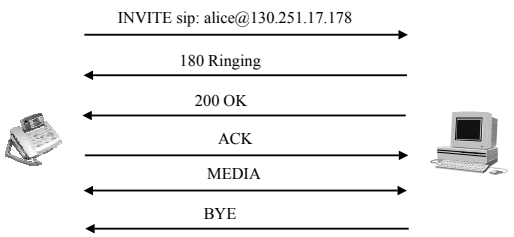
Setup delle connessioni

Connessione diretta tra terminali



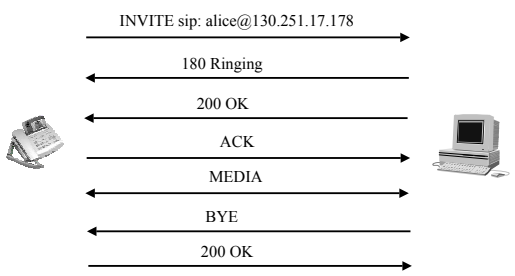
Setup delle connessioni

Connessione diretta tra terminali



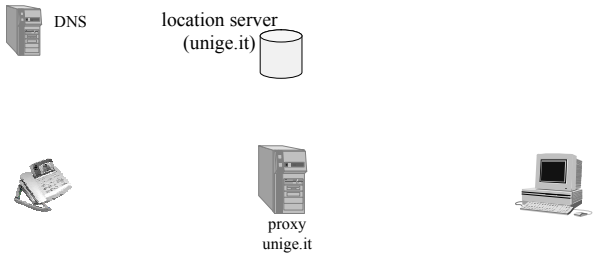
Setup delle connessioni

Connessione diretta tra terminali



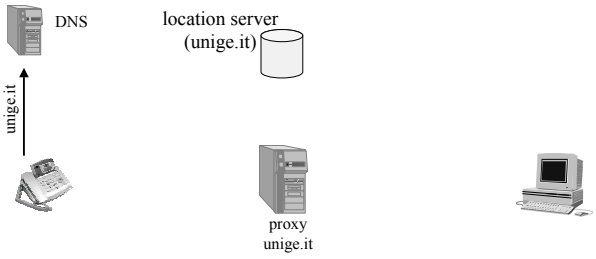
Setup delle connessioni

Connessione tramite proxy



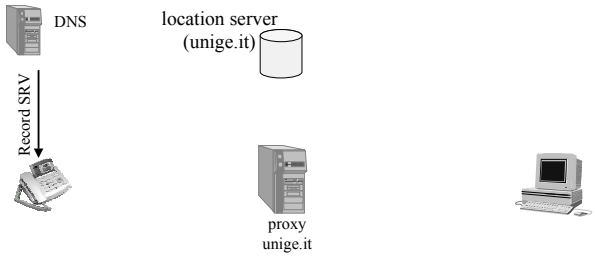
Setup delle connessioni

Connessione tramite proxy



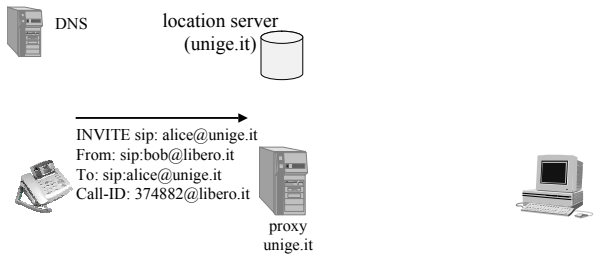
Setup delle connessioni

Connessione tramite proxy



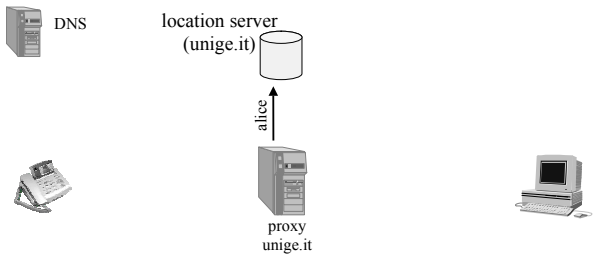
Setup delle connessioni

Connessione tramite proxy



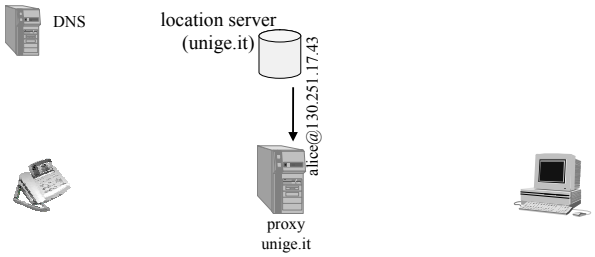
Setup delle connessioni

Connessione tramite proxy



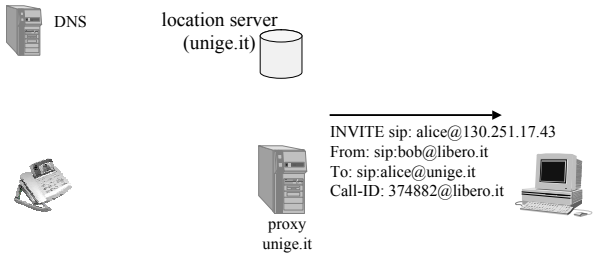
Setup delle connessioni

Connessione tramite proxy



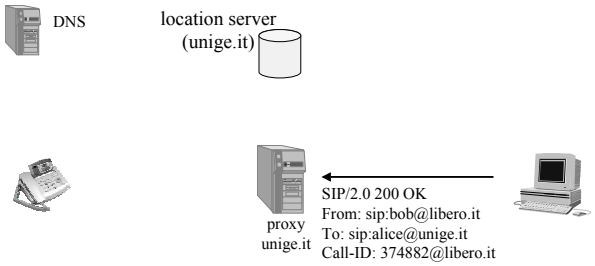
Setup delle connessioni

Connessione tramite proxy



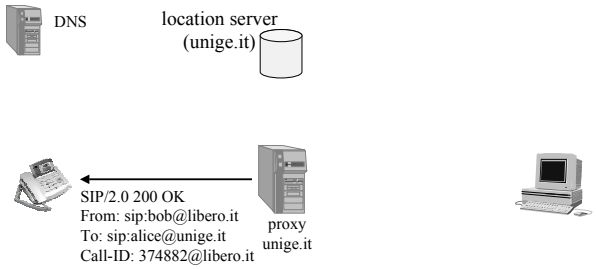
Setup delle connessioni

Connessione tramite proxy



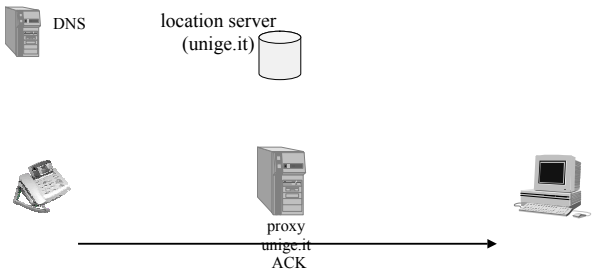
Setup delle connessioni

Connessione tramite proxy



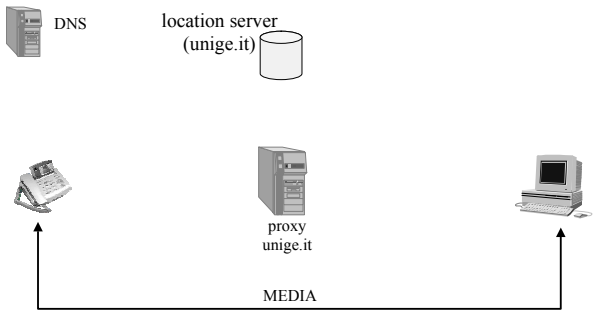
Setup delle connessioni

Connessione tramite proxy



Setup delle connessioni

Connessione tramite proxy



I Proxy

- Rappresentano dei punti di Rendez-vous in cui cercare gli utenti
  - la loro presenza consente la mobilità degli utenti.
- I *proxy* inoltrano le richieste verso gli utenti finali, utilizzando informazioni disponibili presso i *location server*.
- Effettuano il routing della segnalazione
  - verso terminali, altri proxy, server redirect;
  - consentono alle funzioni di routing di essere programmabili
    - » preferenze degli utenti, AAA, controllo dei firewall.

I Proxy

- Si possono individuare due modalità differenti:
  - *stateless proxy;*
  - *forking proxy.*

I Proxy
Stateless Proxy

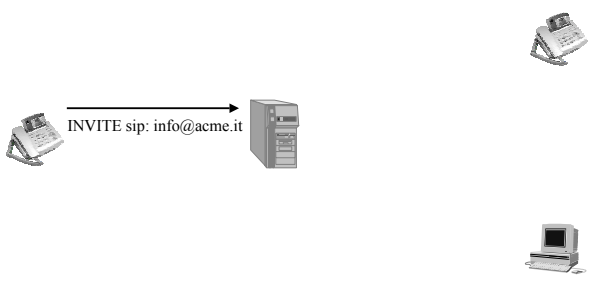
- I proxy mantengono lo stato solo durante una transazione SIP
  - inoltrano il messaggio INVITE verso la destinazione finale e la risposta OK verso la sorgente, senza tener traccia della sessione;
    - » INVITE e OK seguono lo stesso percorso,
    - » ACK può seguire una altra strada, a meno che non sia usata l'opzione *route recording*.
- I proxy SIP non mantengono traccia delle connessioni attive.
- Sarebbe anche possibile mantenere uno stato della connessione
  - in questo caso si perderebbe il vantaggio della scalabilità.

I Proxy
Forking Proxy

- Permettono di poter inviare le richieste a più utenti:
  - in sequenza (se non si ha risposta);
  - in parallelo (il primo che risponde instaura la sessione).

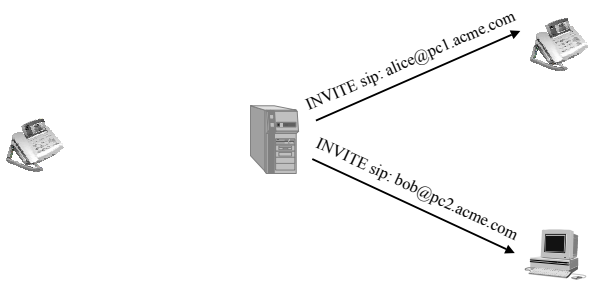
I Proxy
Forking parallelo

I Proxy
Forking parallelo



I Proxy

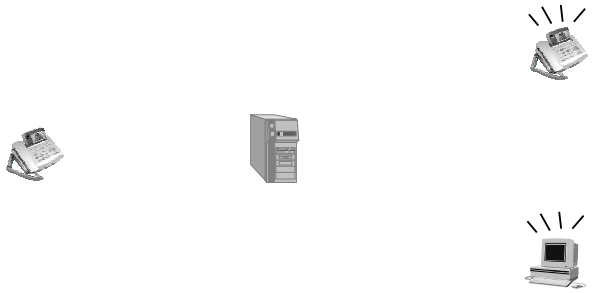
Forking parallelo



R. Bolla Telematica 2, n. o.

I Proxy

Forking parallelo

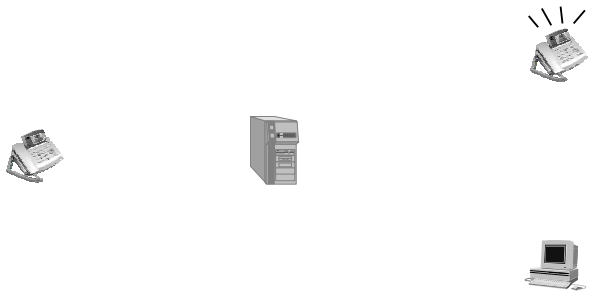


Lezione 1.8, v. 1.2 6.40

R. Bolla Telematica 2, n. o.

I Proxy

Forking parallelo

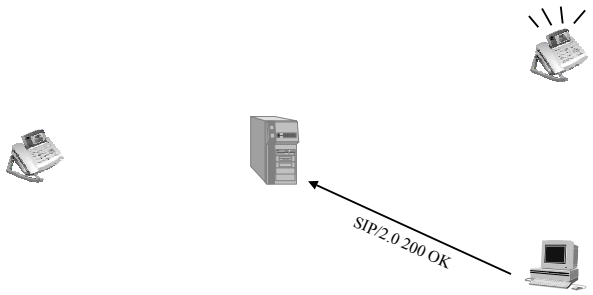


Lezione 1.8, v. 1.2 6.41

R. Bolla Telematica 2, n. o.

I Proxy

Forking parallelo

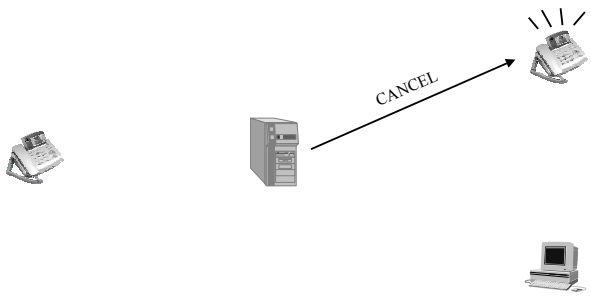


Lezione 1.8, v. 1.2 6.41

R. Bolla Telematica 2, n. o.

I Proxy

Forking parallelo

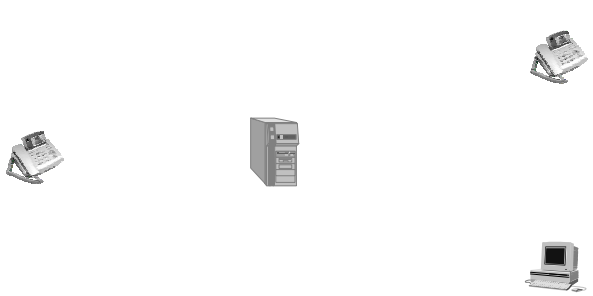


Lezione 1.8, v. 1.2 6.41

R. Bolla Telematica 2, n. o.

I Proxy

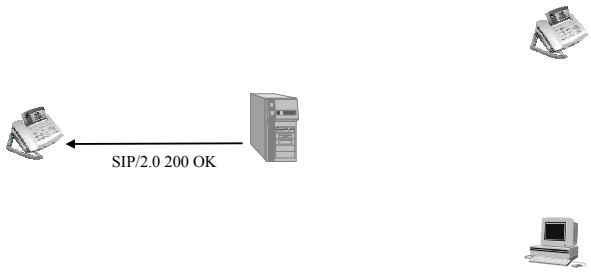
Forking parallelo



Lezione 1.8, v. 1.2 6.42

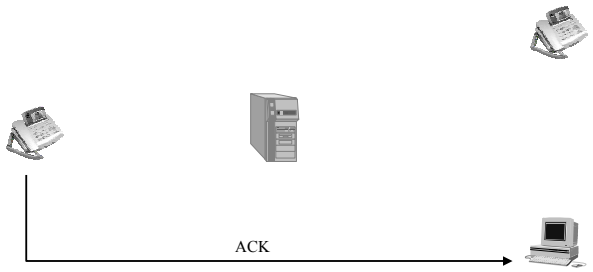
I Proxy

Forking parallelo



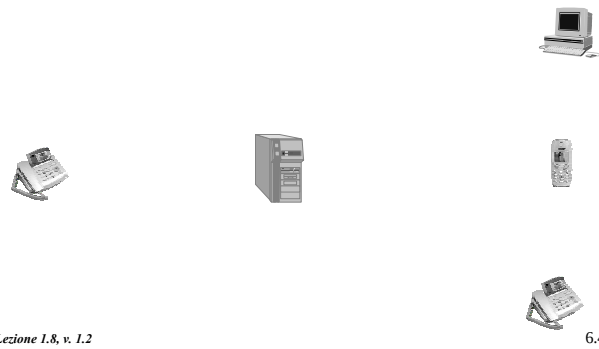
I Proxy

Forking parallelo



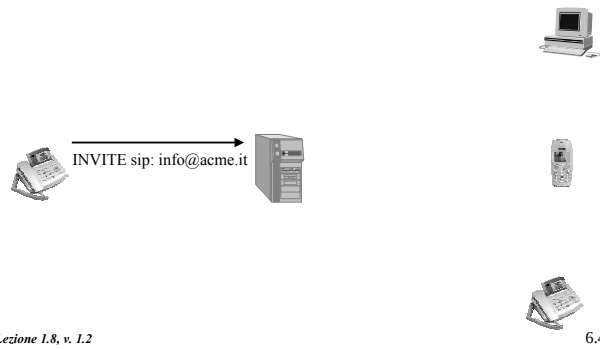
I Proxy

Forking sequenziale



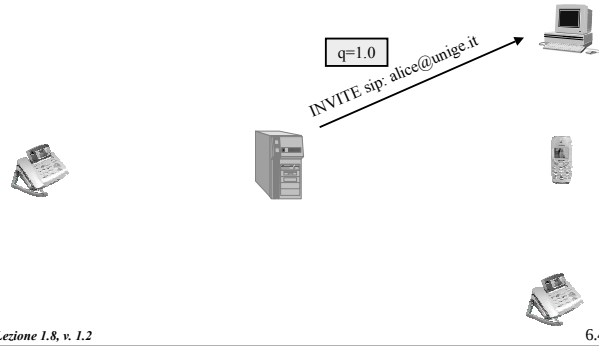
I Proxy

Forking sequenziale



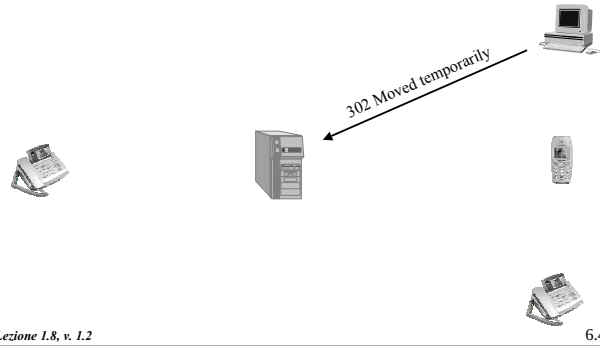
I Proxy

Forking sequenziale



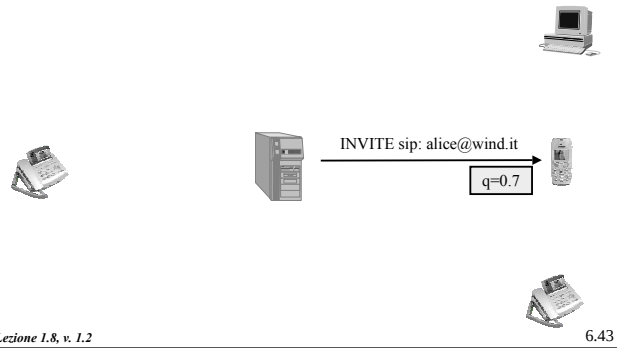
I Proxy

Forking sequenziale



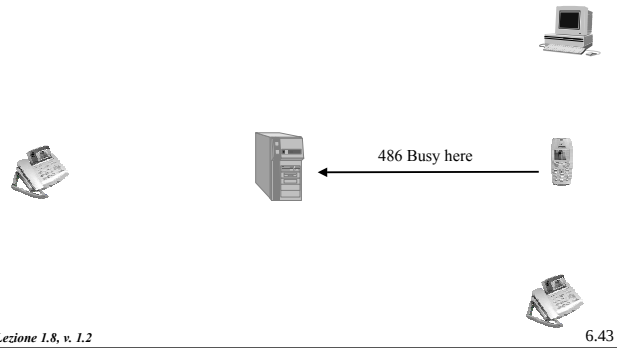
I Proxy

Forking sequenziale



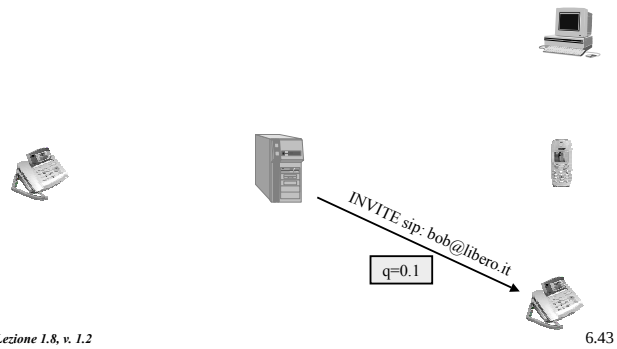
I Proxy

Forking sequenziale



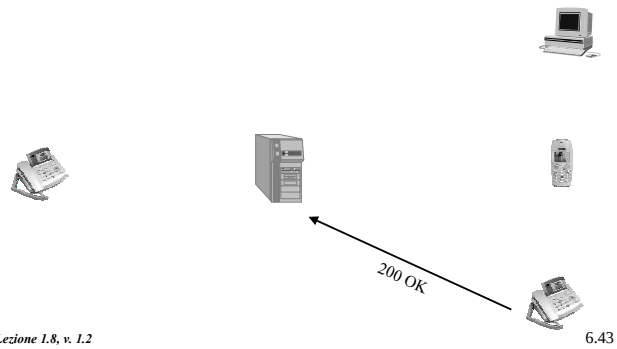
I Proxy

Forking sequenziale



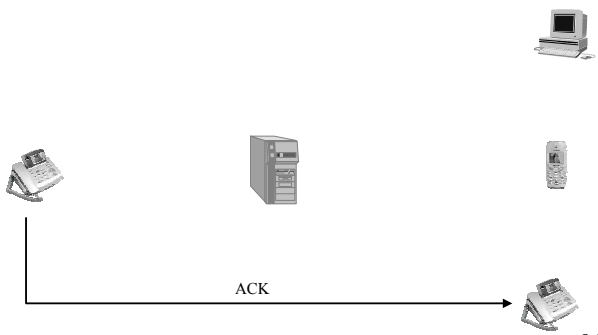
I Proxy

Forking sequenziale



I Proxy

Forking sequenziale



I Proxy

Outbound proxy

- Il proxy esaminato in precedenza viene definito "inbound proxy"
  - gestisce le connessioni in arrivo agli utenti;
  - gestisce un solo dominio.
- A volte vengono utilizzati anche "outbound proxy"
  - gestisce tutte le connessioni in uscita da un dominio;
  - permette di realizzare funzioni di emergenza (localizzazione chiamate 118 più vicino);
  - interagisce con eventuali firewall;
  - consente di instradare le chiamate;
  - permette di tariffare gli utenti.

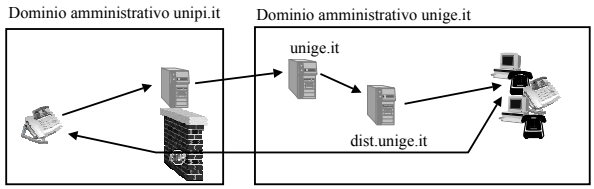
I Proxy

Outbound proxy

- I terminali devono conoscere l'indirizzo del proxy
  - configurazione manuale;
  - configurazione automatica (DHCP, TFTP).
- In generale, diversi server (proxy) possono essere attraversati
  - ad es. un unico proxy aziendale può distribuire la segnalazione a diversi server dipartimentali;
  - un utente può inoltrare le proprie chiamate verso un altro terminale;
  - i server devono essere in grado di evitare i loop.

I Proxy

Outbound proxy e catena di proxy



L'outbound proxy permette l'attraversamento del firewall

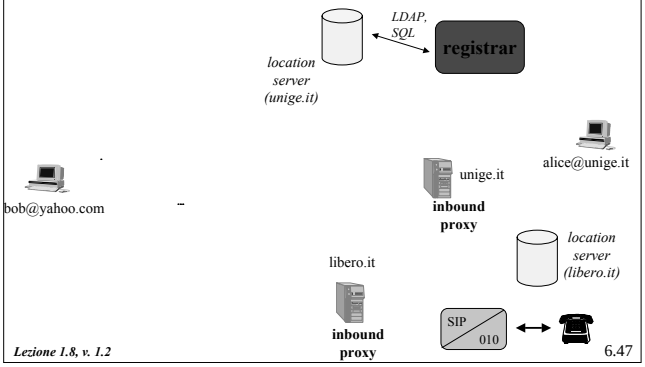
Il proxy unige.it identifica un proxy che serve il singolo dipartimento

Il proxy dist.unige.it distribuisce la segnalazione ai terminali e riceve le loro registrazioni.

Segnalazione e media possono seguire percorsi completamente diversi.

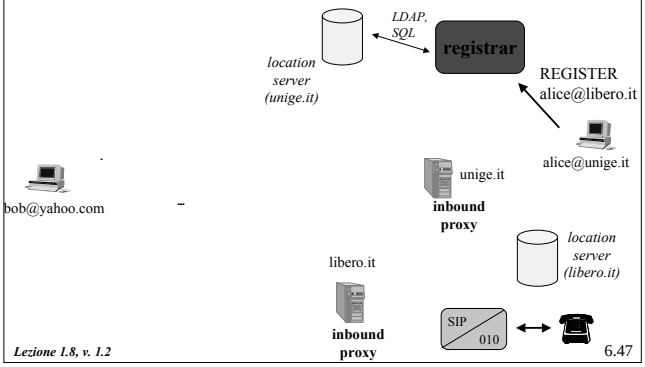
Setup delle connessioni

Redirect



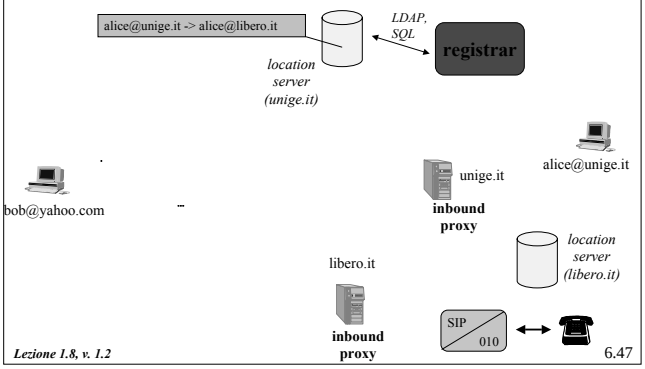
Setup delle connessioni

Redirect



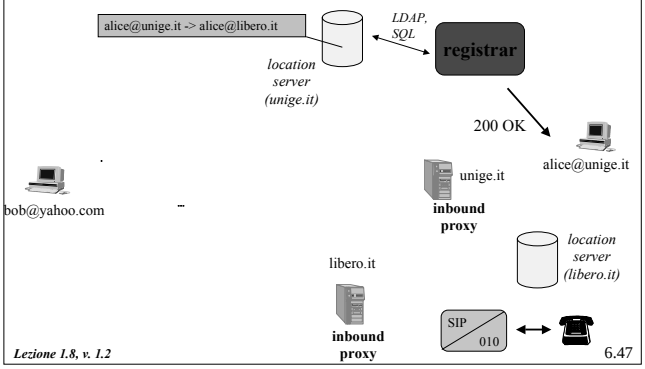
Setup delle connessioni

Redirect



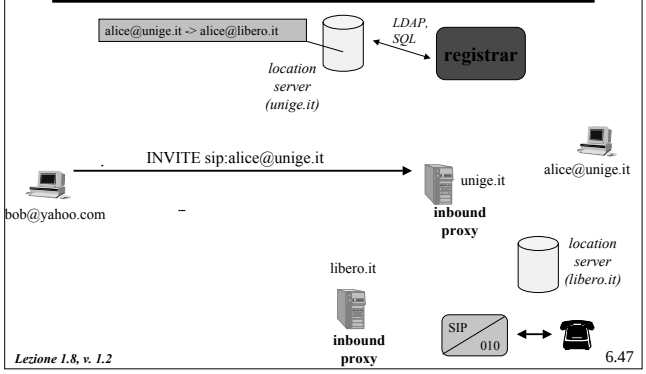
Setup delle connessioni

Redirect



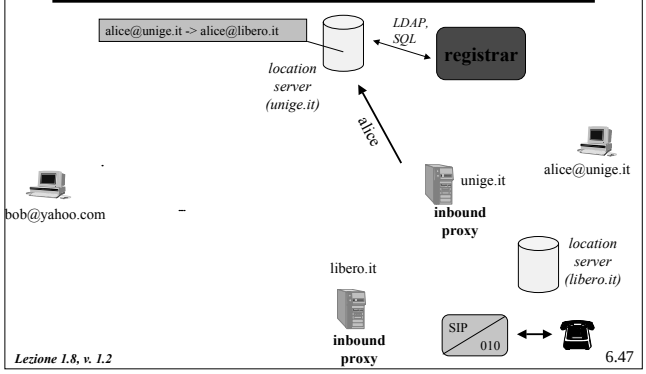
Setup delle connessioni

Redirect



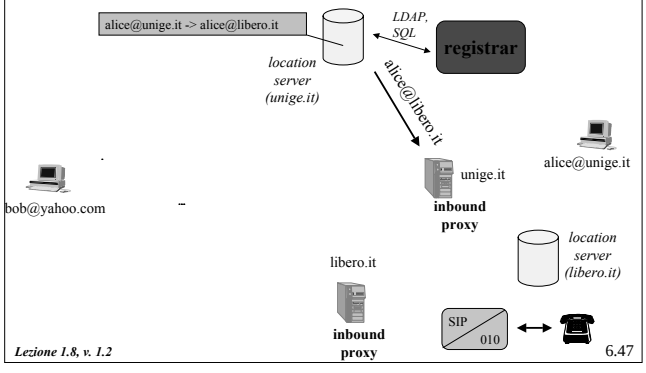
Setup delle connessioni

Redirect



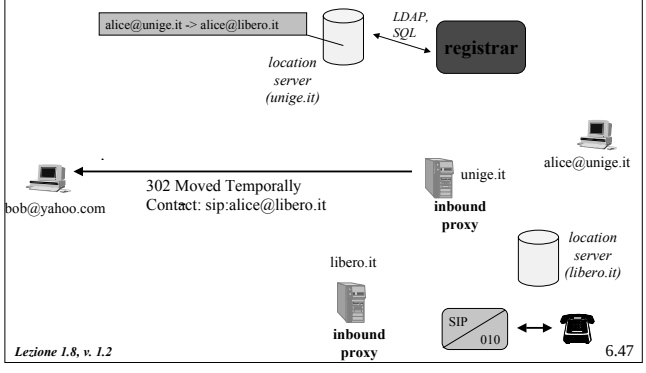
Setup delle connessioni

Redirect



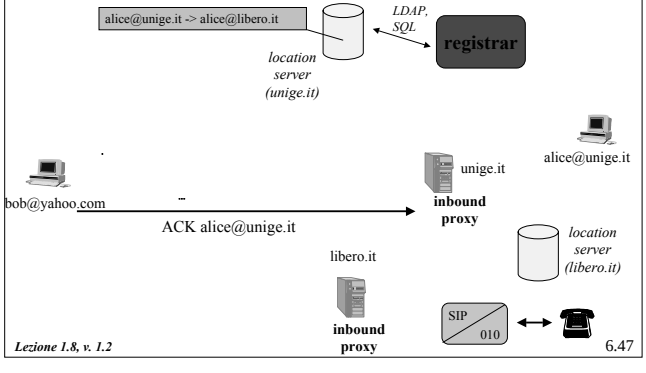
Setup delle connessioni

Redirect



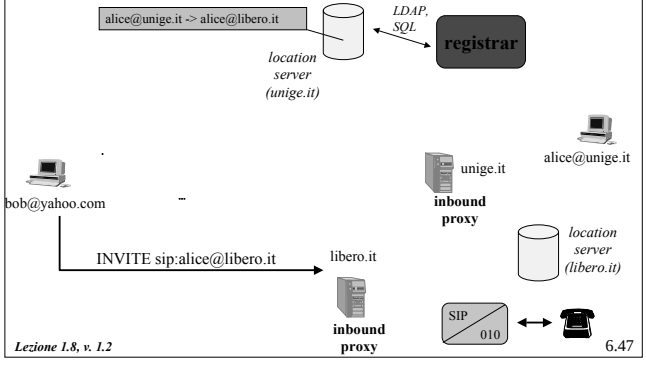
Setup delle connessioni

Redirect



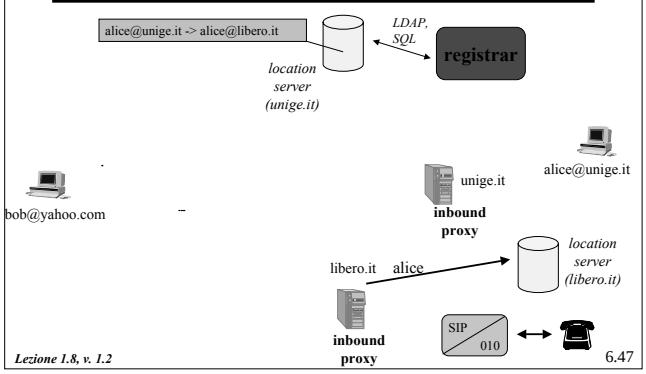
Setup delle connessioni

Redirect



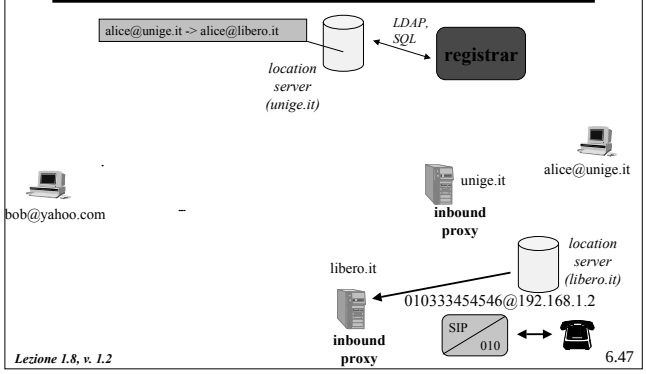
Setup delle connessioni

Redirect



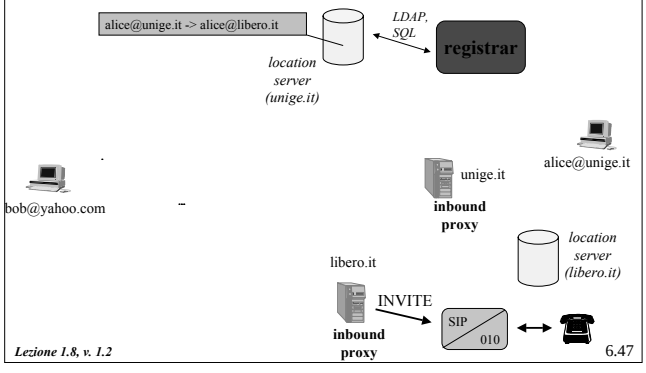
Setup delle connessioni

Redirect



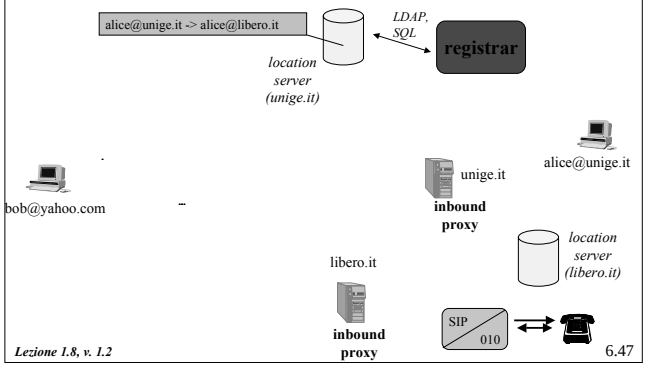
Setup delle connessioni

Redirect



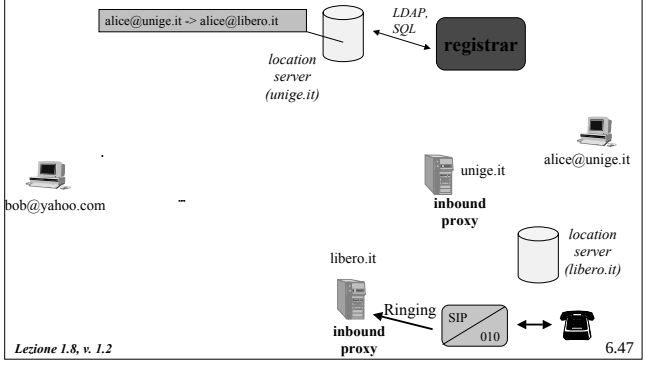
Setup delle connessioni

Redirect



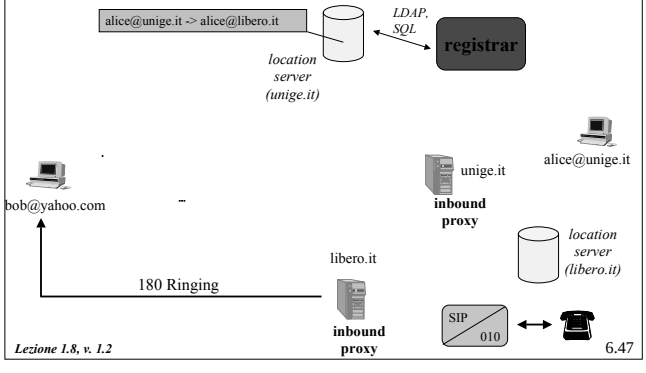
Setup delle connessioni

Redirect



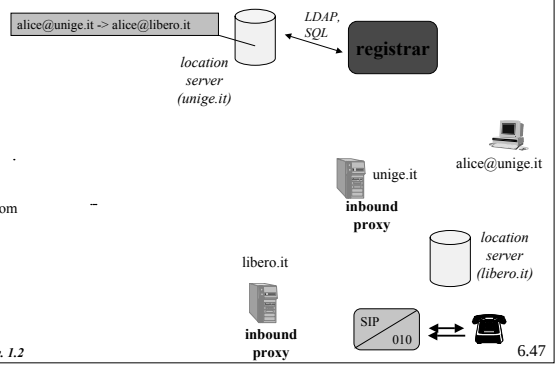
Setup delle connessioni

Redirect



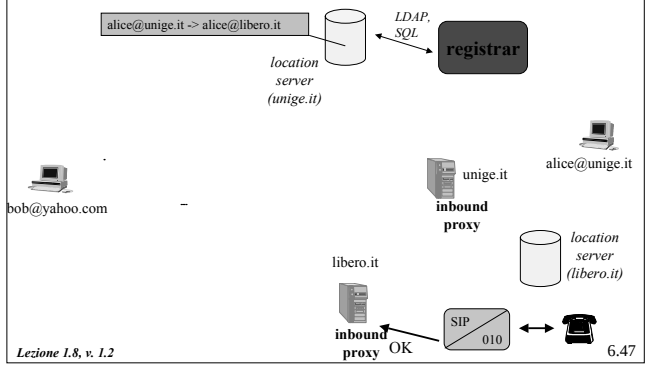
Setup delle connessioni

Redirect



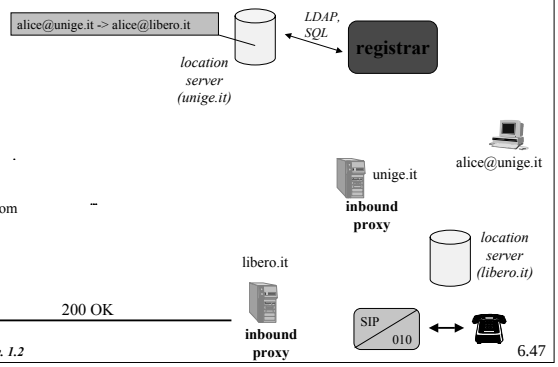
Setup delle connessioni

Redirect



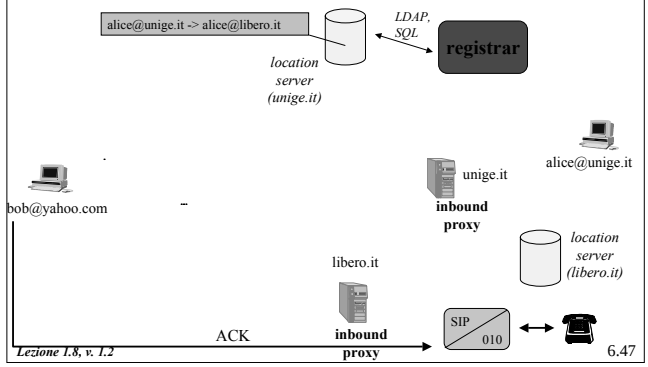
Setup delle connessioni

Redirect



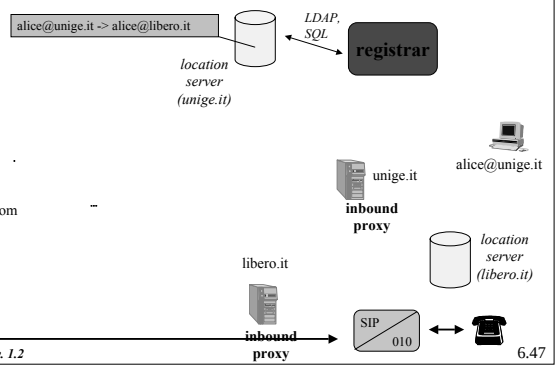
Setup delle connessioni

Redirect



Setup delle connessioni

Redirect

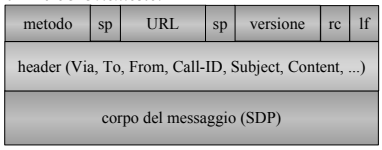


Redirect

- Un server SIP può effettuare l'operazione di proxy o redirect.
- Il comportamento può essere configurato
  - staticamente,
  - dinamicamente.
- La redirezione è utile nel caso cambi il provider
  - il chiamante può direttamente chiamare il nuovo alias la prossima volta;
  - senza stato.
- L'operazione di proxy è utile nel caso sia necessario utilizzare il forking, AAA, controllo del firewall
  - il generale, il proxy permette un maggior controllo al server.

SIP – Formato dei messaggi

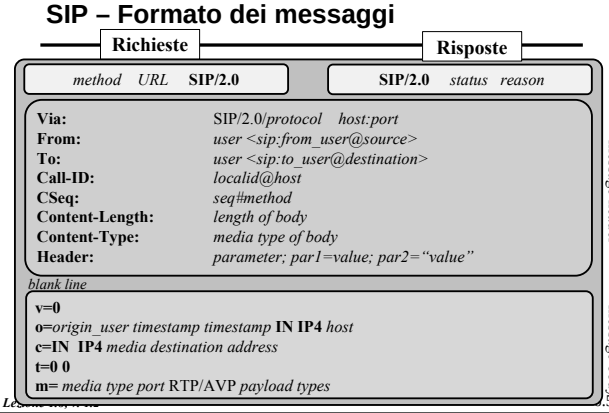
- Il SIP utilizza un formato dei messaggi analogo a quello dell'HTTP.
- Il client invia delle ***richieste***:



Metodo: INVITE, ACK, OPTIONS, BYE, CANCEL, REGISTER.

- Il server invia delle ***risposte***:

SIP – Formato dei messaggi



Metodi di SIP

Richieste (RFC 2543)

Metodo	*Descrizione*
INVITE	Richiesta di instaurazione di una sessione.
ACK	Conferma l'instaurazione della sessione.
BYE	Termina la sessione.
CANCEL	Annulla una ricerca precedente (INVITE).
OPTIONS	Richiesta delle funzionalità supportate.
REGISTER	Registrazione presso un location server.

Metodi di SIP

Estensioni alle richieste

Metodo	*Descrizione*
INFO	Segnalazione durante la sessione.
COMET	Requisito soddisfatto.
PRACK	ACK provvisorio.
SUBSCRIBE	Sottoscrizione ad un evento
NOTIFY	Notifica agli iscritti.
REFER	Chiede al ricevitore di effettuare una richiesta SIP (trasferimento di chiamata).

Metodi di SIP

Richieste SIP - Esempi

```
INVITE sip:picard@wcom.com SIP/2.0
Via: SIP/2.0/UDP host.wcom.com:5060
From: Alan Johnston
<sip:alan.johnston@wcom.com>
To: Jean Luc Picard <sip:picard@wcom.com>
Call-ID: 314159@host.wcom.com
CSeq: 1 INVITE
```

Identificano univocamente la richiesta.

- **`Via:`** l'instradamento della richiesta.
- **`Call-ID:`** identificativo univoco generato dal client.
- **`CSeq:`** Command Sequence Number
  - generato dal client;
  - incrementato ad ogni richiesta successiva.

Metodi di SIP

Richieste SIP - Esempi

```
INVITE sip:picard@wcom.com SIP/2.0
Via: SIP/2.0/UDP host.wcom.com:5060
From: Alan Johnston <sip:alan.johnston@wcom.com>
To: Jean Luc Picard <sip:picard@wcom.com>
Call-ID: 314159@host.wcom.com
CSeq: 1 INVITE
Contact: sip:alan.johnston@wcom.com
Subject: Where are you these days?
Content-Type: application/sdp
Content-Length: 124

v=0
o=ajohnston 5462346 332134 IN IP4 host.wcom.com
s=Let's Talk
t=0 0
c=IN IP4 10.64.1.1
m=audio 49170 RTP/AVP 0 3
```

Descrizione della sessione (SDP)

Metodi di SIP

Risposte

Informational	*Success*	*Redirection*	*Client Failure*
100 Trying 180 Ringing 181 Call forwarded 182 Queued 183 Session Progress	200 OK	300 Multiple Choices 301 Moved Perm. 302 Moved Temp. 380 Alternative Serv.	400 Bad Request 401 Unauthorized 403 Forbidden 404 Not Found 405 Bad Method 415 Unsupp. Content 420 Bad Extensions 486 Busy Here

Server Failure	*Global Failure*
500 Server Error 501 Not Implemented 503 Unavailable 504 Timeout	600 Busy Everwhere 603 Decline 604 Doesn't exist 606 Not Acceptable

Metodi di SIP

Risposte SIP - Esempi

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP host.wcom.com:5060
From: Alan Johnston
<sip:alan.johnston@wcom.com>
To: Jean Luc Picard
<sip:picard@wcom.com>
Call-ID: 314159@host.wcom.com
CSeq: 1 INVITE
```

- **`Via, From, To, Call-ID`**, e **`CSeq`** sono copiati esattamente dalla Richiesta.
- **`To`** e **`From`** NON SONO INVERTITI!

Metodi di SIP

Risposte SIP - Esempi

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP host.wcom.com
From: Alan Johnston <sip:alan.johnston@wcom.com>
To: Jean Luc Picard <sip:picard@wcom.com>
Call-ID: 314159@host.wcom.com
CSeq: 1 INVITE
Contact: sip:picard@wcom.com
Subject: Where are you these days?
Content-Type: application/sdp
Content-Length: 107

v=0
o=picard 124333 67895 IN IP4 uunet.com
s=Engage!
t=0 0
c=IN IP4 11.234.2.1
m=audio 3456 RTP/AVP 0
```

Descrizione della sessione (SDP)

Metodi di SIP

Richieste e Risposte SIP - Esempi

```
INVITE sip:bob@macrosoft.com SIP/2.0
From: sip:alice@wonderland.com
To: sip:bob@macrosoft.com
Call-ID: 3232@wonderland.com
CSeq: 42 INVITE
Content-Type: application/sdp
v=0
o=user1 536 2337 IN IP4 h3.wonderland.com
c=IN IP4 h3.wonderland.com
m=audio 3456 RTP/AVP 0 1
m=video 4000 RTP/AVP 38 39
```

alice@wonderland.com chiama bob@macrosoft.com

```
SIP/2.0 200 OK
From: sip:alice@wonderland.com
To: sip:bob@macrosoft.com
Call-ID: 3232@wonderland.com
CSeq: 42 INVITE
Content-Type: application/sdp
v=0
o=user1 535 687637 IN IP4  m.macrosoft.com
c=IN IP4 h3.wonderland.com
m=audio 1200 RTP/AVP 0 1
m=video 0 RTP/AVP
```

bob accetta l'audio ma rifiuta il video

Metodi di SIP

Negoziazione dei media

- SIP non prevede meccanismi per la negoziazione dei media
  - per tale scopo si utilizza SDP;
  - recenti proposte hanno suggerito l'utilizzo di XML
    - » SIP è più semplice e veloce da elaborare.
- L'offerta dei media viene fatta nell'INVITE dal chiamante, il chiamato specifica la sua scelta nel messaggio 200 OK
  - l'offerta può essere chiesta al chiamato non specificando niente nell'INVITE.

SIP/SDP

- SIP non sempre utilizza tutti i campi dell'SDP
  - *Version* (v), *Subject* (s) e *Time* (t) non sono utilizzati.
- Dopo l'instaurazione della connessione ulteriori negoziazioni dei media possono avvenire in fase di modifica della sessione.
- Le capacità descrittive dell'SDP sono limitate
  - la successiva versione (SDPng) avrà più avanzate capacità descrittive e di negoziazione.

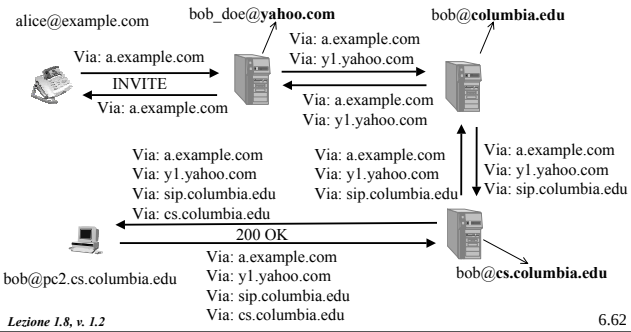
Metodi di SIP

Instradamento delle risposte

- Le Richieste SIP sono instradate tramite le URL.
- Le Risposte SIP vengono inviate sullo stesso percorso a ritroso
  - senza mantenere uno stato nei proxy;
  - utilizzando l'informazione in "**Via:**".
- Alcuni proxy dovrebbero rimanere nel percorso delle Richieste
  - firewall, proxy anonimizzatori, proxy per gw PSTN;
  - è possibile memorizzare il percorso di INVITE con **Record-Route** e forzarlo sulle successive Richieste con **Route**.

Metodi di SIP

Instradamento delle risposte

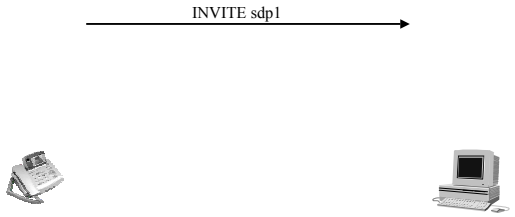


Modifica della sessione

- Una volta instaurata,una sessione può essere modificata da una nuova sequenza INVITE/OK/ACK (re-INVITE)
  - può essere effettuata solo dopo l'ACK della fase iniziale;
  - deve avere gli stessi "**From:**" "**To:**" e "**Call-ID:**" dell'INVITE originale;
  - se la re-INVITE fallisce o non viene accettata, la sessione SDP originale rimane valida fino al termine della sessione.

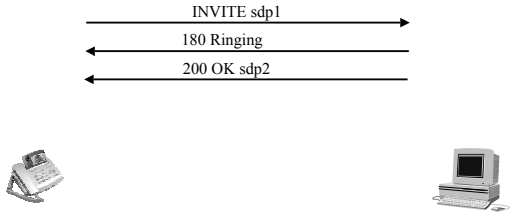
Modifica della sessione

Modifica della sessione

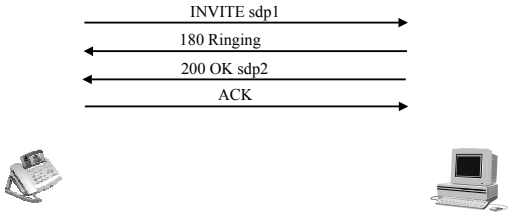


Modifica della sessione

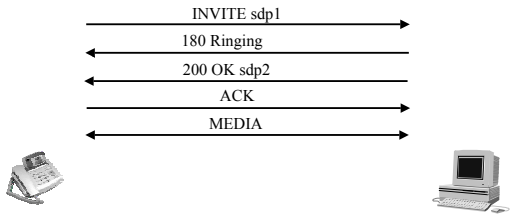
Modifica della sessione



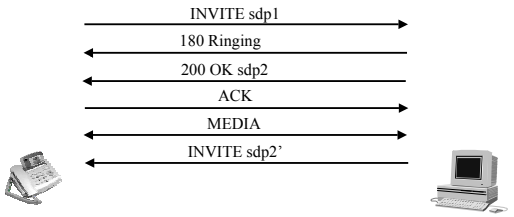
Modifica della sessione



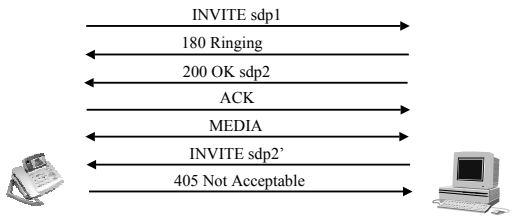
Modifica della sessione



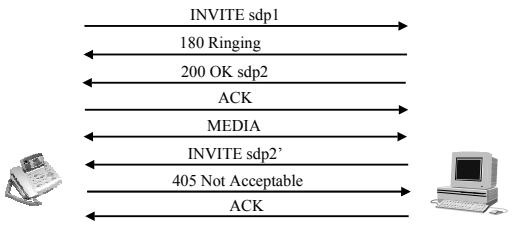
Modifica della sessione



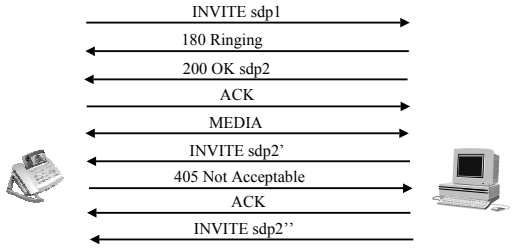
Modifica della sessione



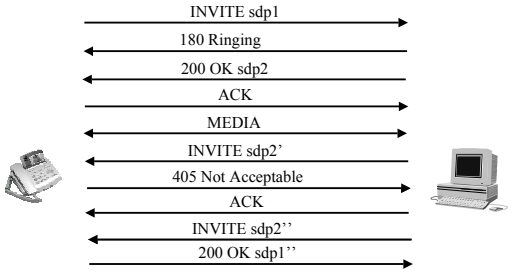
Modifica della sessione



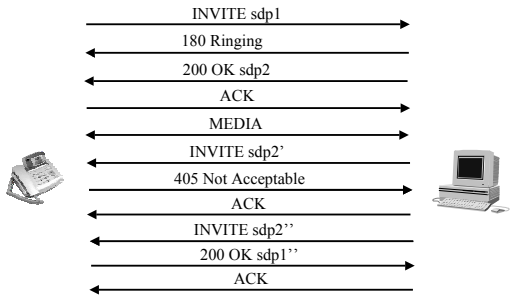
Modifica della sessione



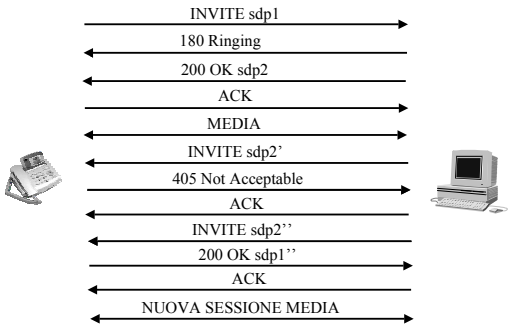
Modifica della sessione



Modifica della sessione



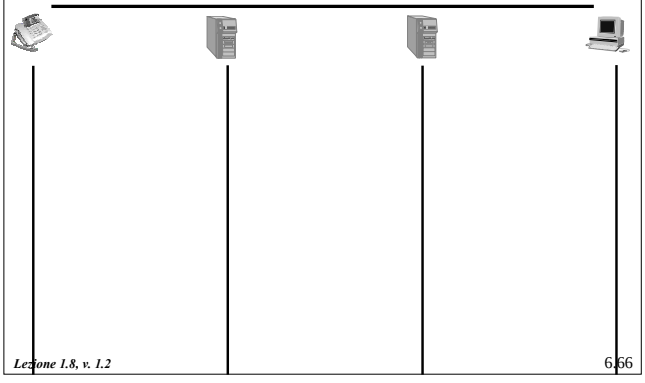
Modifica della sessione



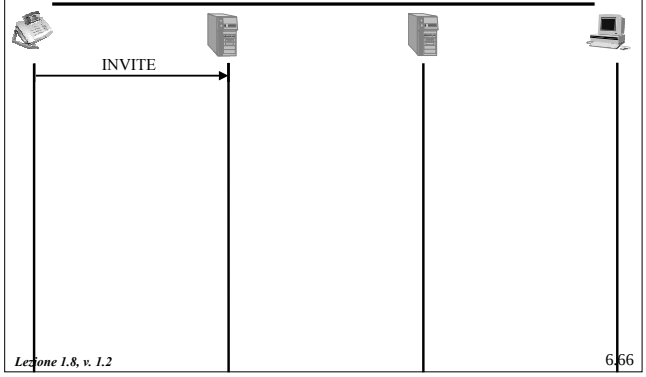
Termine e Cancellazione della sessione

- Termine della sessione
  - avviene a sessione attiva;
  - invio di BYE con riferimento alla sessione attiva.
- Cancellazione della sessione
  - la chiamata viene terminata prima dell'instaurazione della sessione
    - » per es. se utente non risponde;
  - la cancellazione avviene *hop-by-hop* con l'invio di CANCEL.

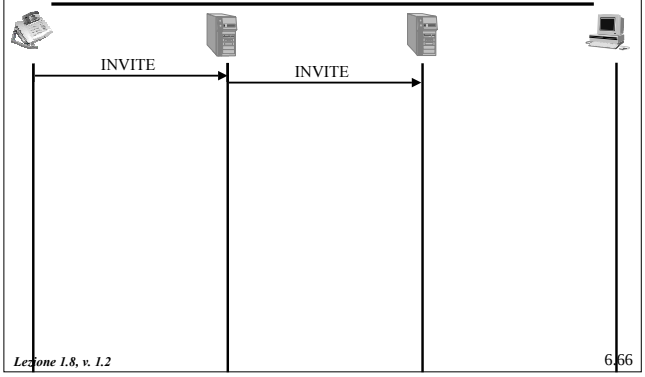
Cancellazione della sessione



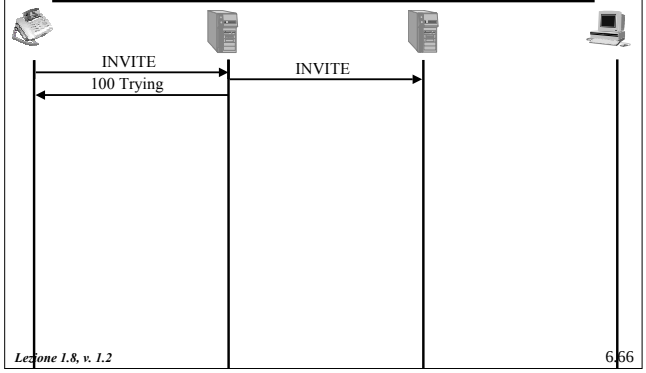
Cancellazione della sessione



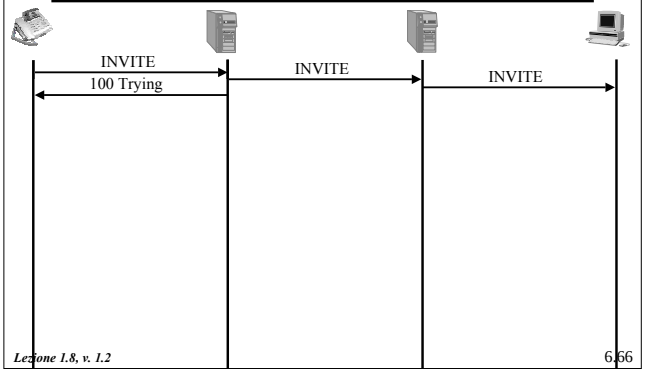
Cancellazione della sessione



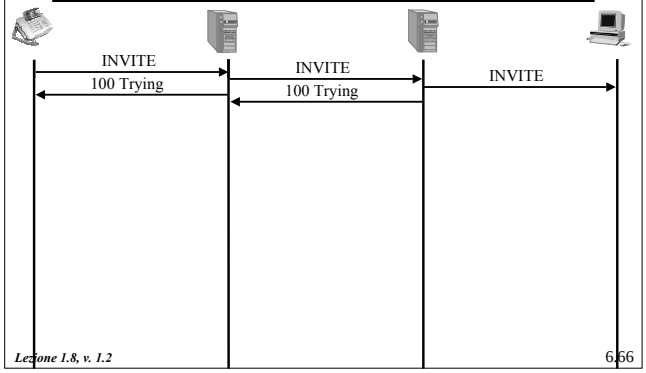
Cancellazione della sessione



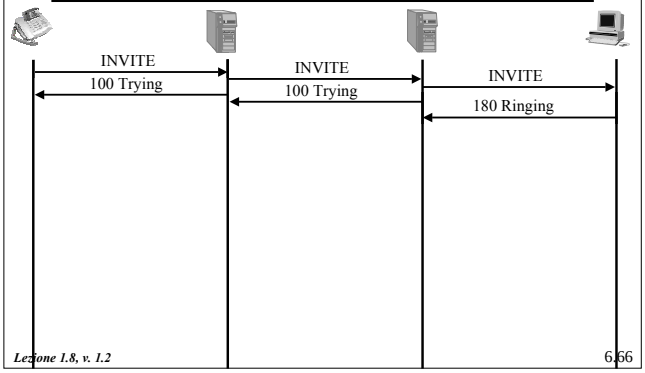
Cancellazione della sessione



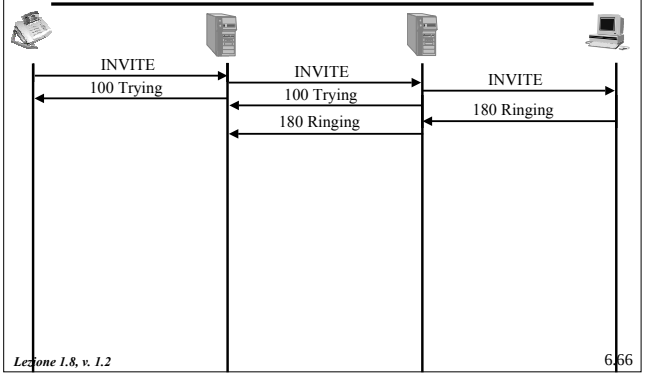
Cancellazione della sessione



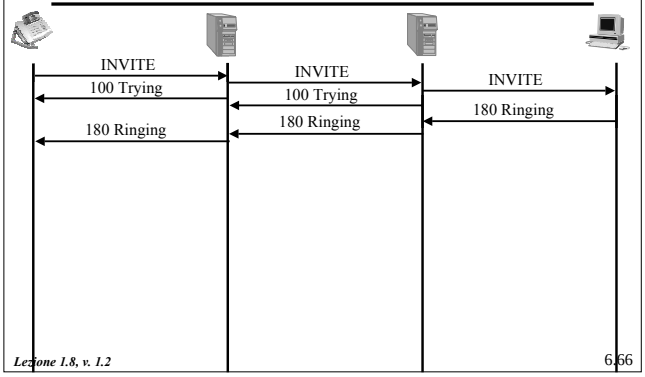
Cancellazione della sessione



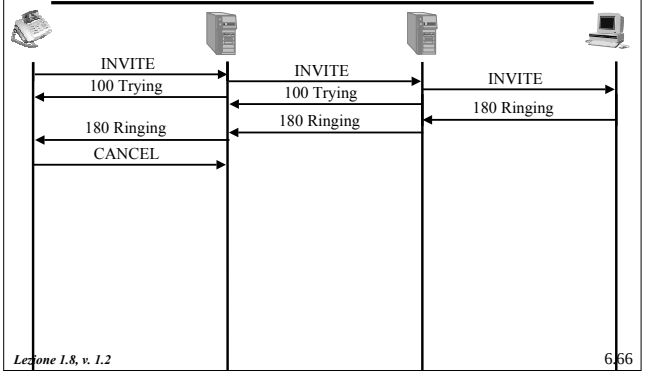
Cancellazione della sessione



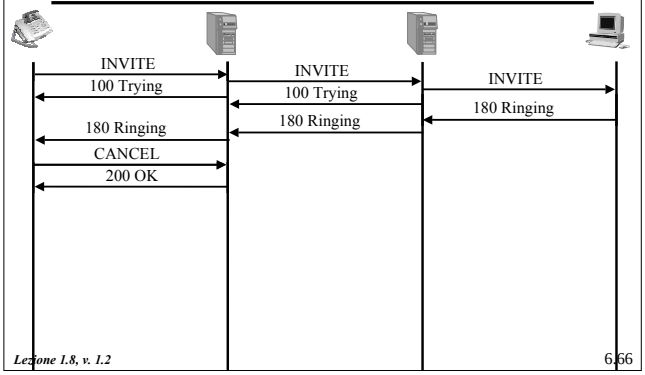
Cancellazione della sessione



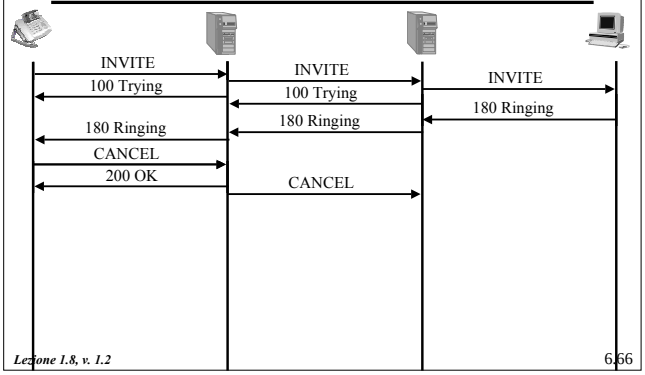
Cancellazione della sessione



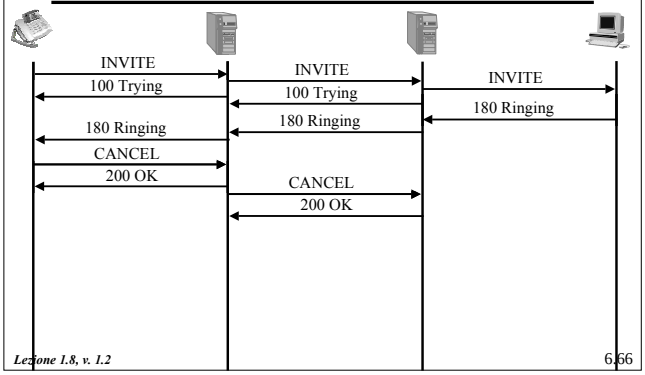
Cancellazione della sessione



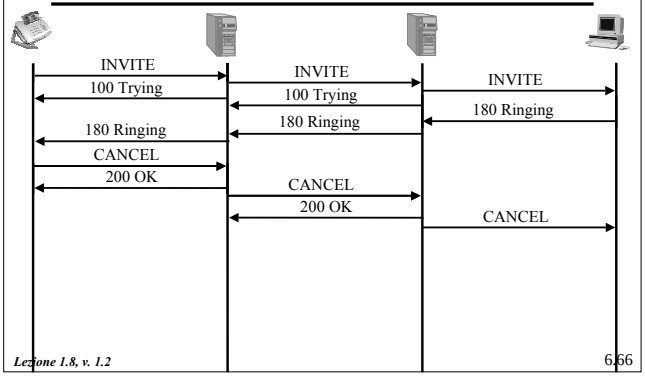
Cancellazione della sessione



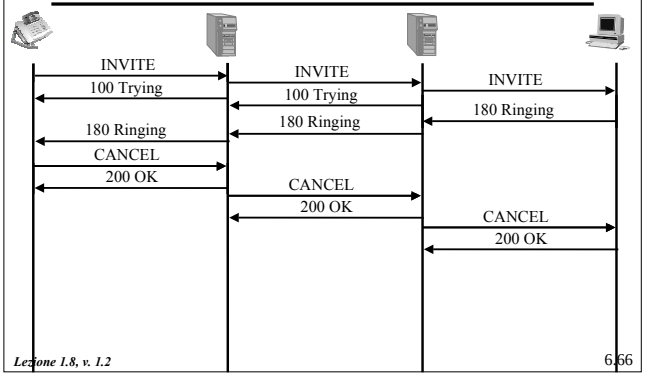
Cancellazione della sessione



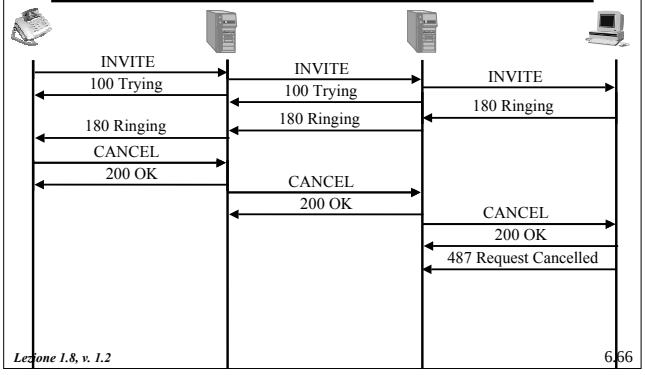
Cancellazione della sessione



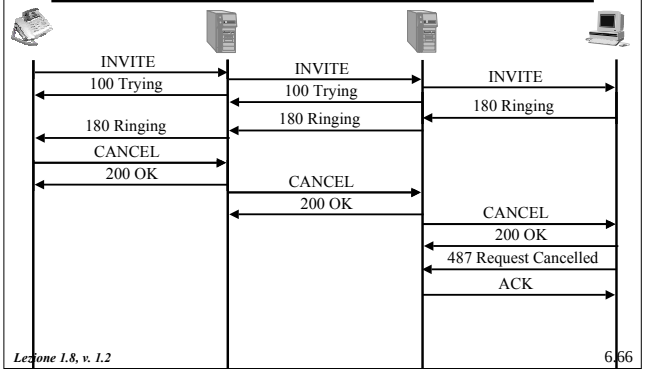
Cancellazione della sessione



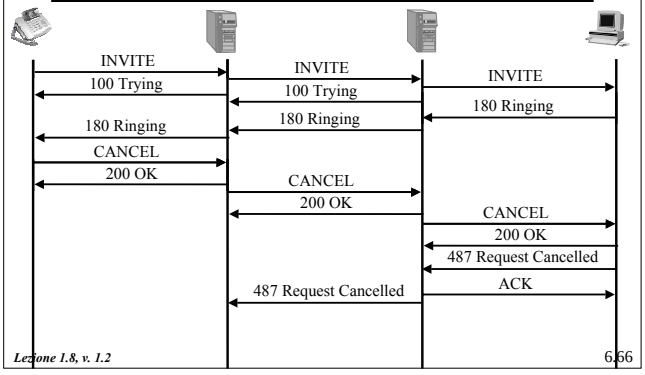
Cancellazione della sessione



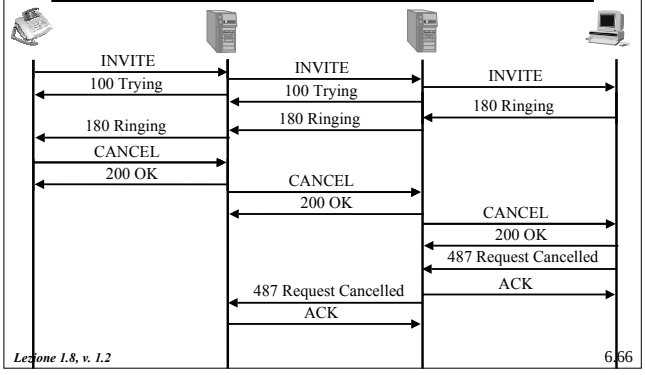
Cancellazione della sessione



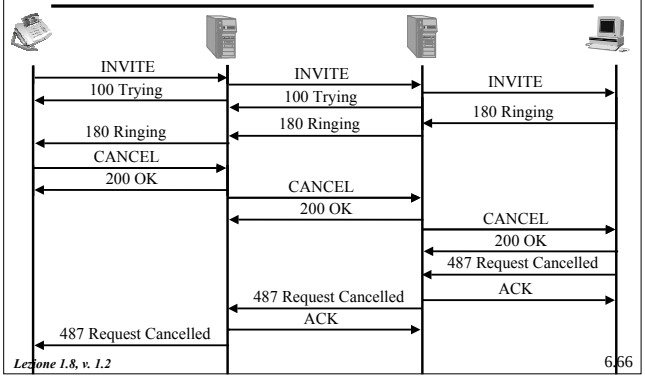
Cancellazione della sessione



Cancellazione della sessione

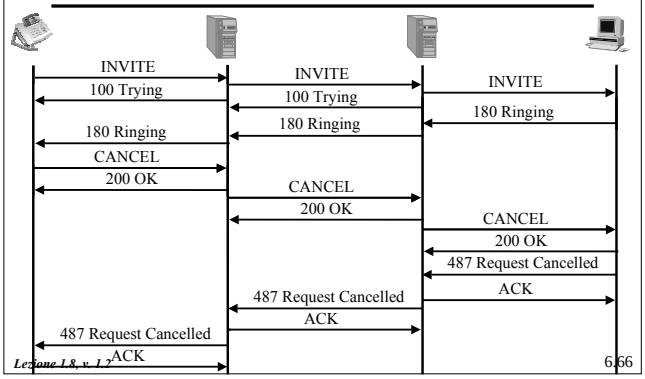


Cancellazione della sessione



R. Bolla Telematica 2, n. o.

Cancellazione della sessione



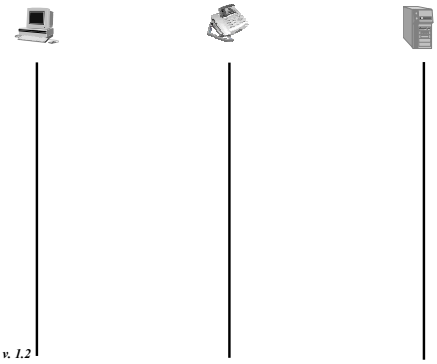
R. Bolla Telematica 2, n. o.

Segnalazione durante la sessione

- *Midcall Signaling*
  - consiste in segnalazione tra due endpoint che non cambia i parametri della sessione;
  - utilizzo il metodo INFO.
- *Call Control*
  - nell'architettura SIP il controllo delle comunicazioni viene effettuato end-to-end;
  - la possibilità di controllare la chiamata da una terza parte può essere utile:
    - » per es. centri di distribuzione chiamate agli utenti;
  - due possibilità di effettuare il controllo
    - » riceve la richiesta e inizia una nuova sessione con la terza parte;
    - » utilizzo del metodo REFER per instaurare la nuova connessione.

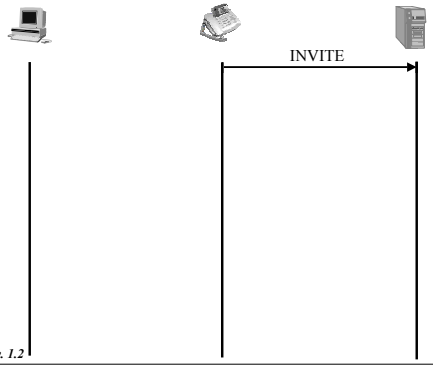
R. Bolla Telematica 2, n. o.

Metodo REFER



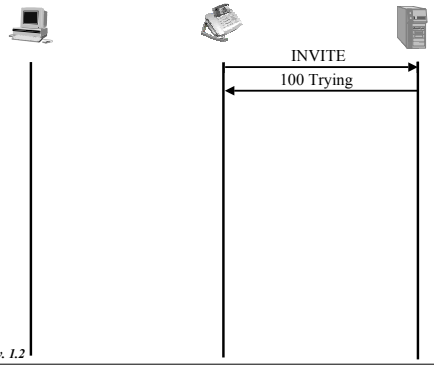
R. Bolla Telematica 2, n. o.

Metodo REFER

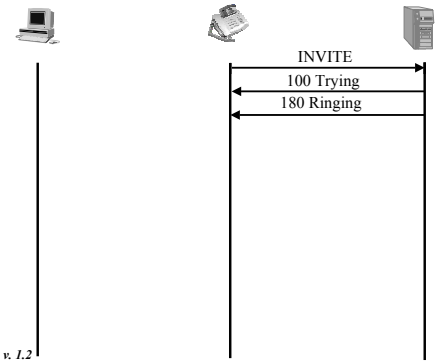


R. Bolla Telematica 2, n. o.

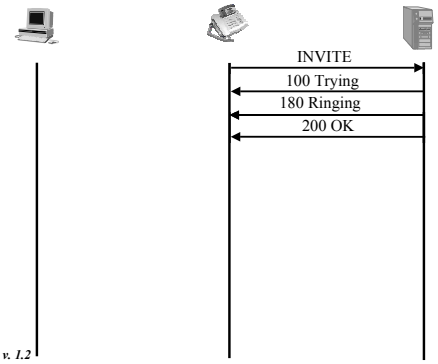
Metodo REFER



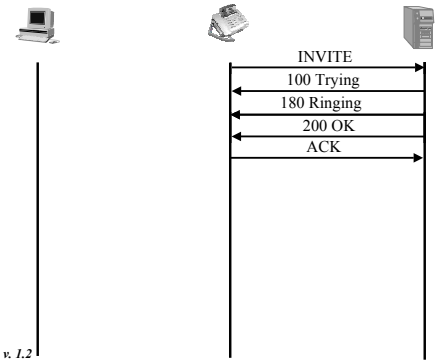
Metodo REFER



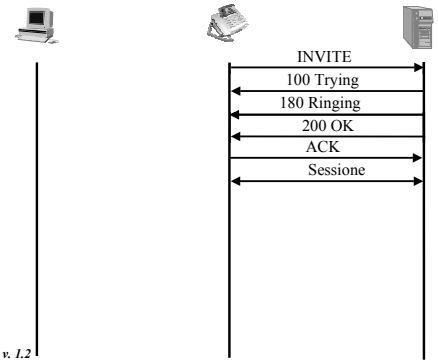
Metodo REFER



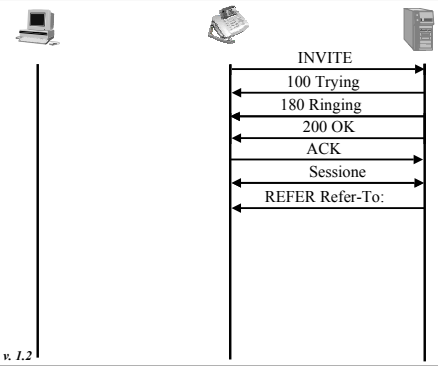
Metodo REFER



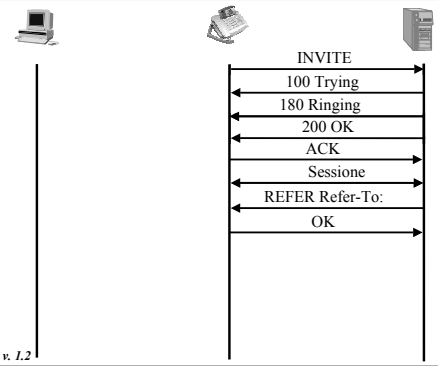
Metodo REFER



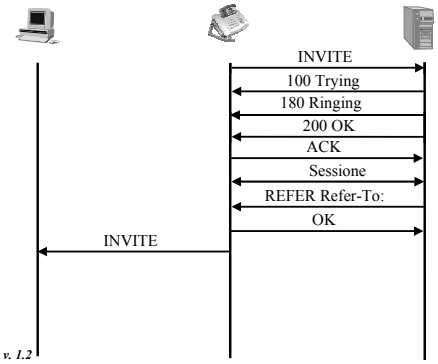
Metodo REFER



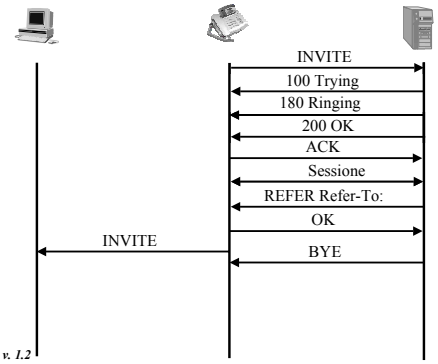
Metodo REFER



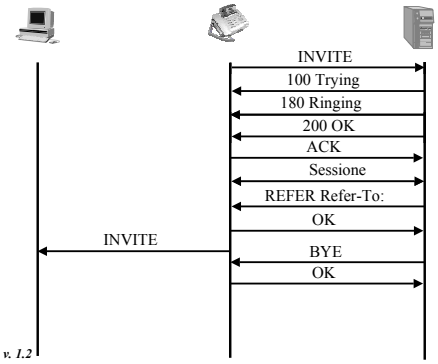
Metodo REFER



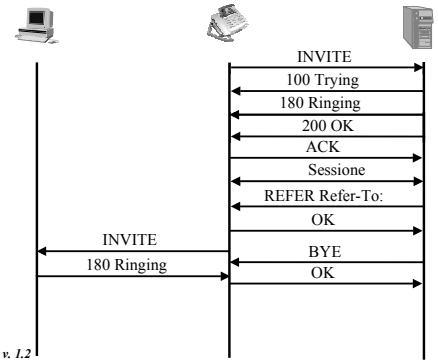
Metodo REFER



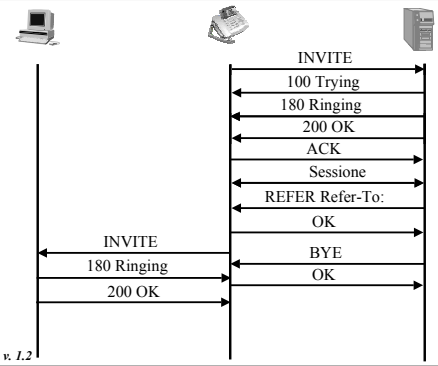
Metodo REFER



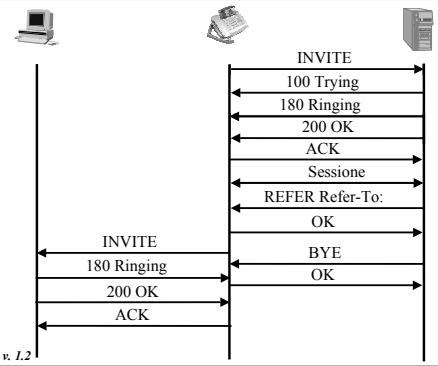
Metodo REFER



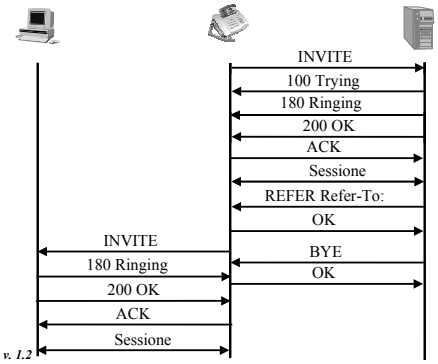
Metodo REFER



Metodo REFER



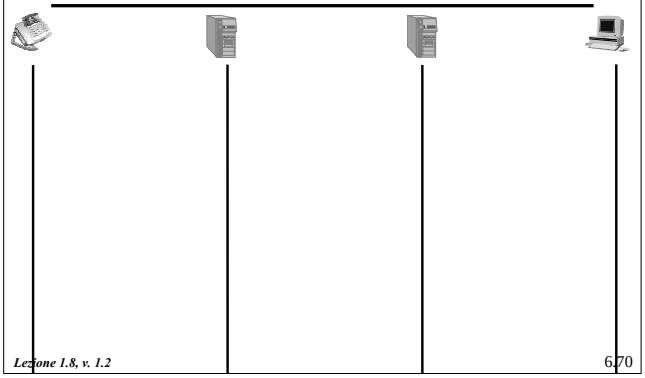
Metodo REFER



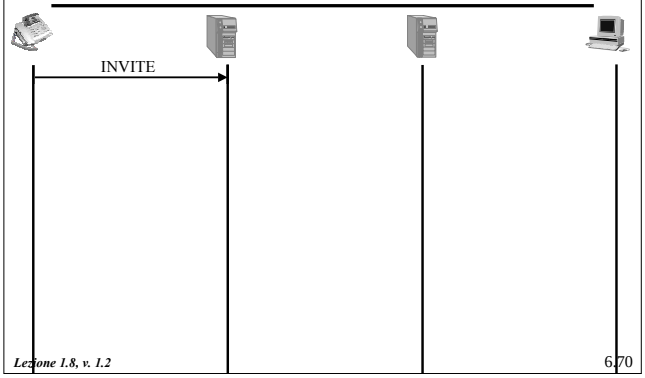
Qualità del servizio

- La gestione della qualità del servizio richiede tre estensioni a SIP
  - *Early Media*, per poter inserire SDP nel messaggio "183 Session Progress";
  - *Reliable Provisional Responses*, permette di rilevare la perdita di alcuni messaggi (ad es. un Provisional Response ACK –PRACK- viene inviato in risposta al messaggio 183);
  - il metodo COMET (*preCOnditions MET*), che conferma la disponibilità dei prerequisisti di QoS.
- La QoS può essere gestita tramite
  - RSVP nel caso di IntServ;
  - campo TOS con DiffServ.

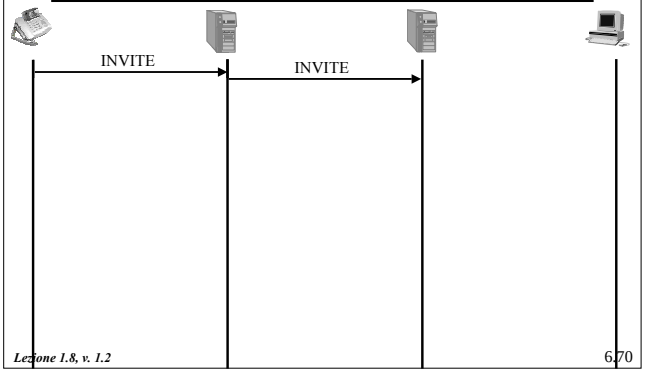
Qualità del servizio



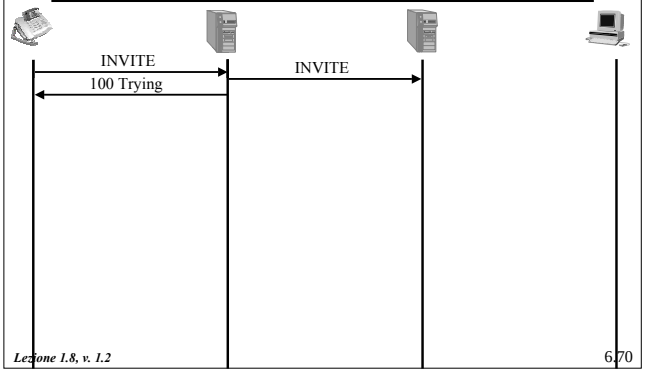
Qualità del servizio



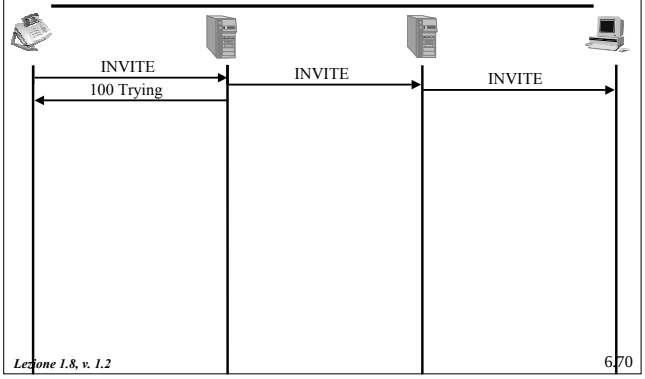
Qualità del servizio



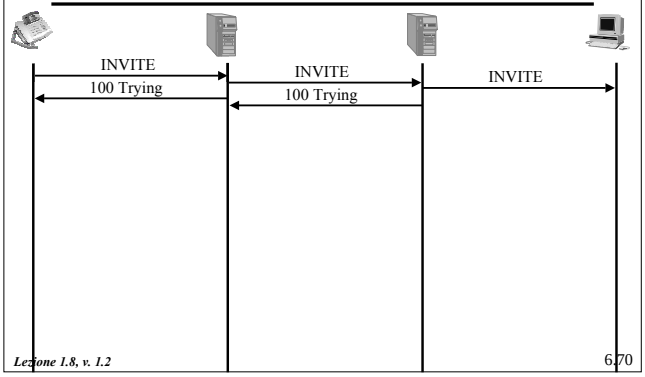
Qualità del servizio



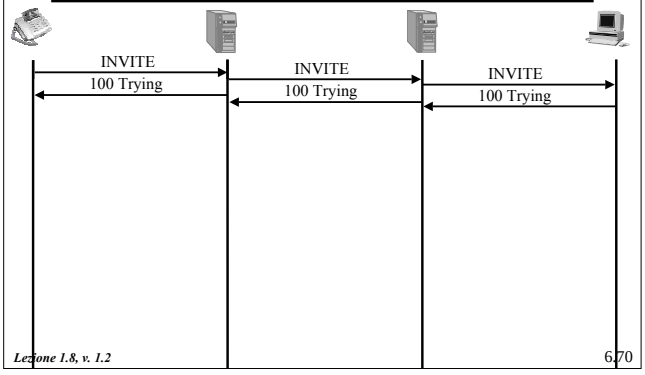
Qualità del servizio



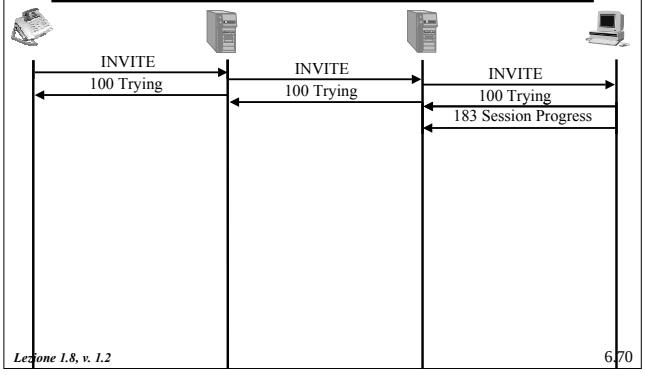
Qualità del servizio



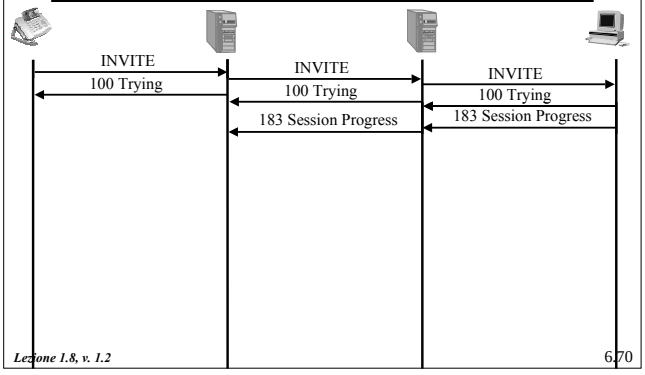
Qualità del servizio



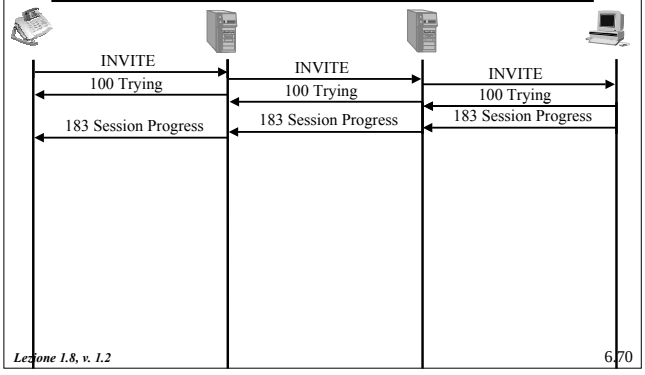
Qualità del servizio



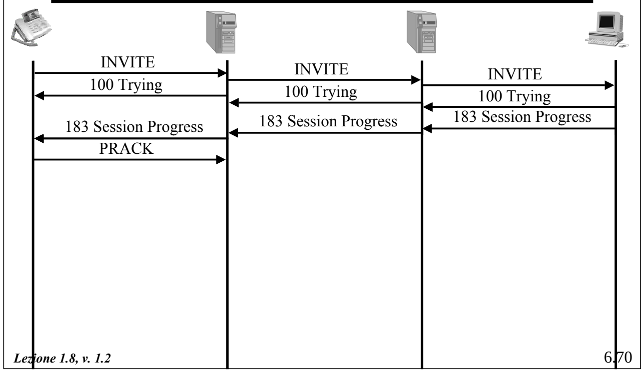
Qualità del servizio



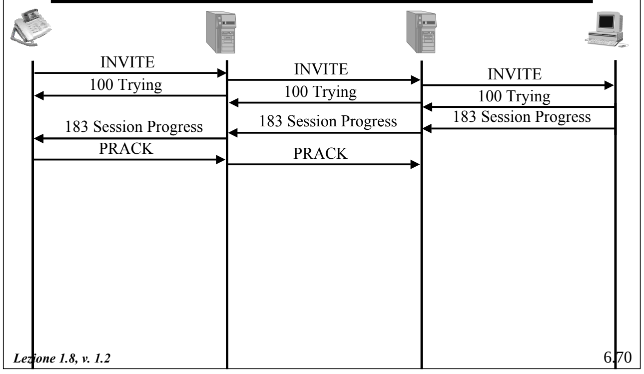
Qualità del servizio



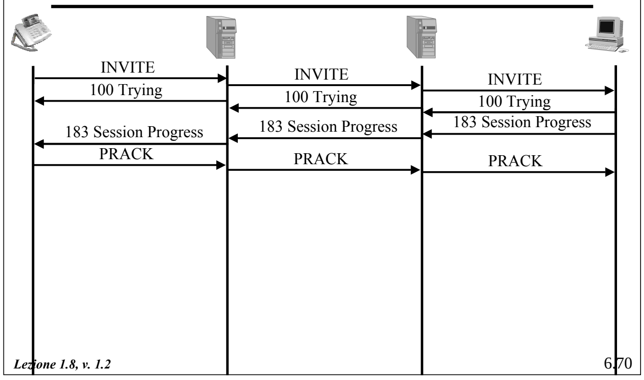
Qualità del servizio



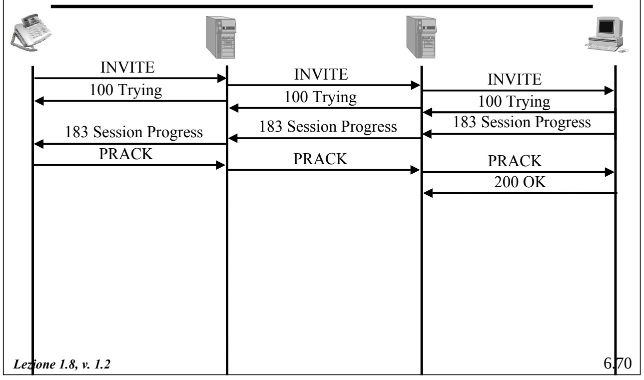
Qualità del servizio



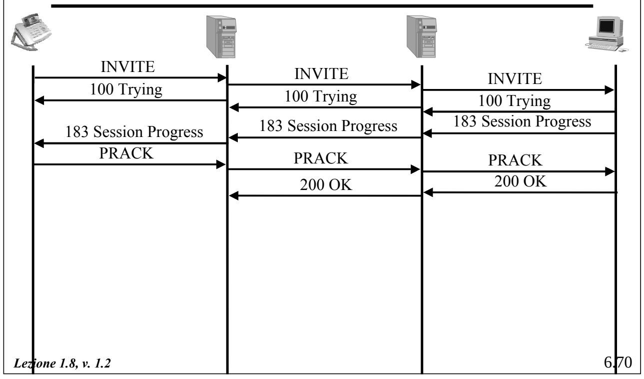
Qualità del servizio



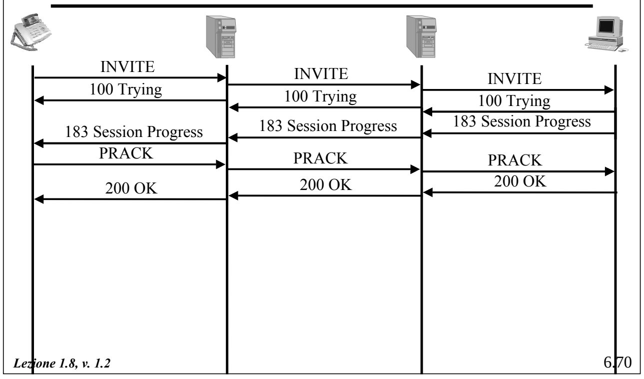
Qualità del servizio



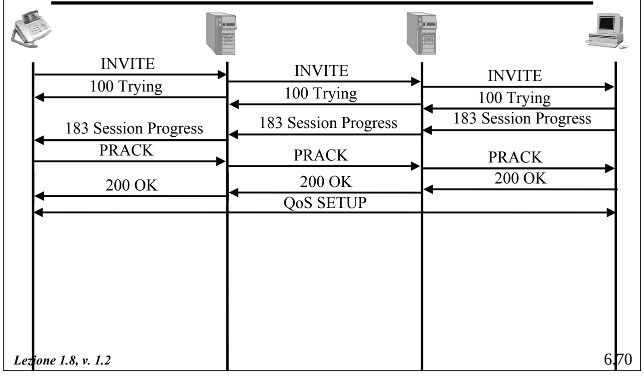
Qualità del servizio



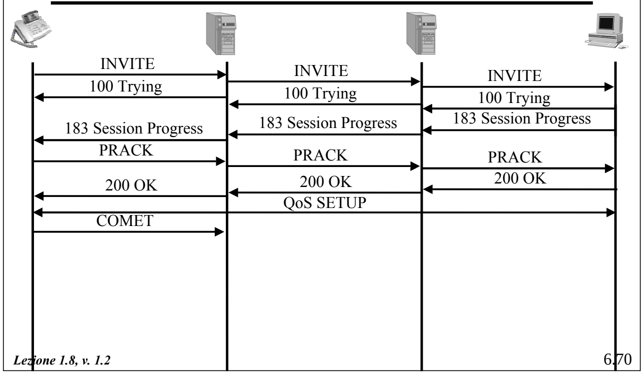
Qualità del servizio



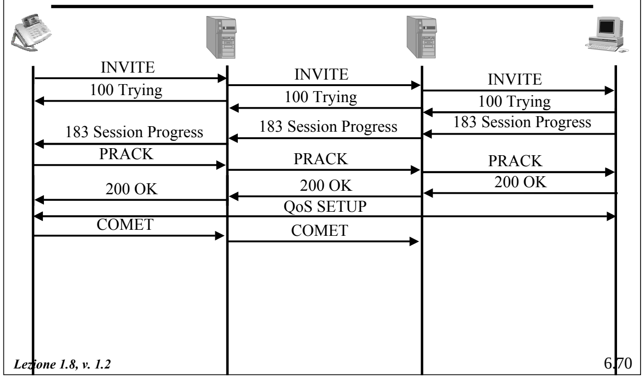
Qualità del servizio



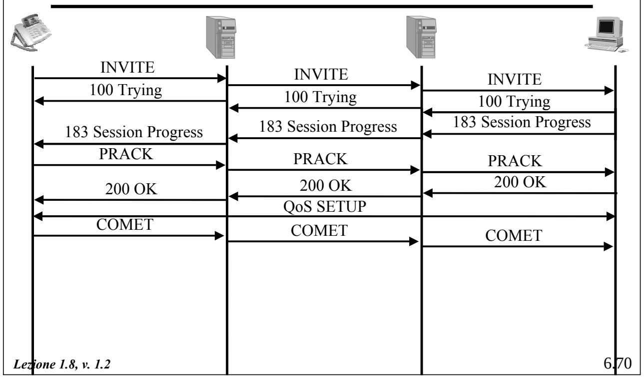
Qualità del servizio



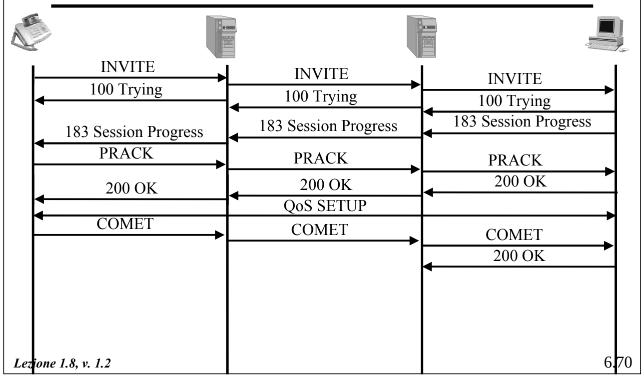
Qualità del servizio



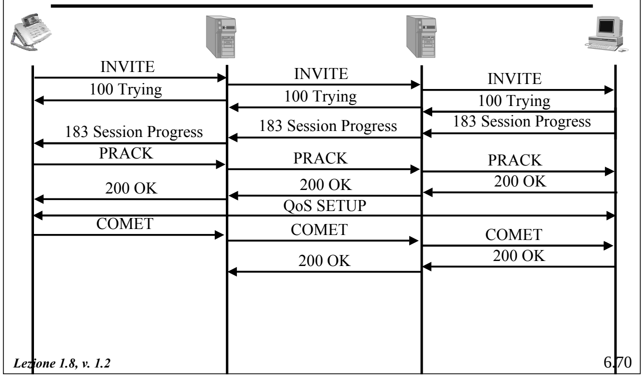
Qualità del servizio



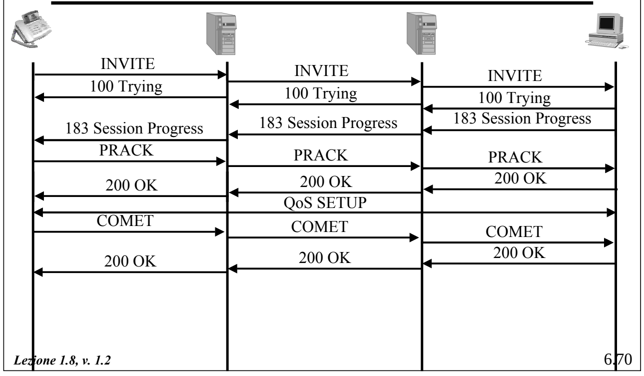
Qualità del servizio



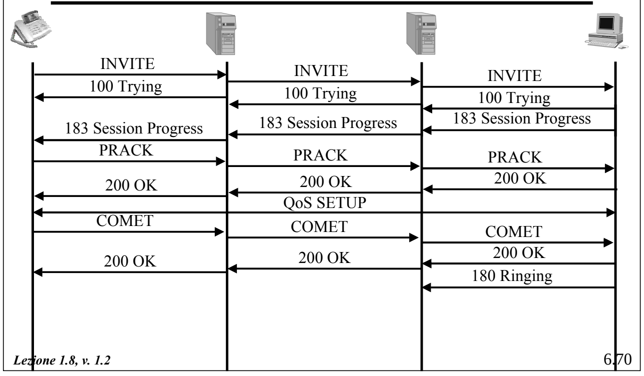
Qualità del servizio



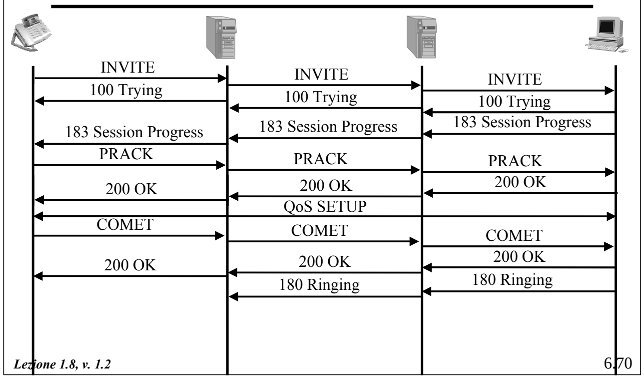
Qualità del servizio



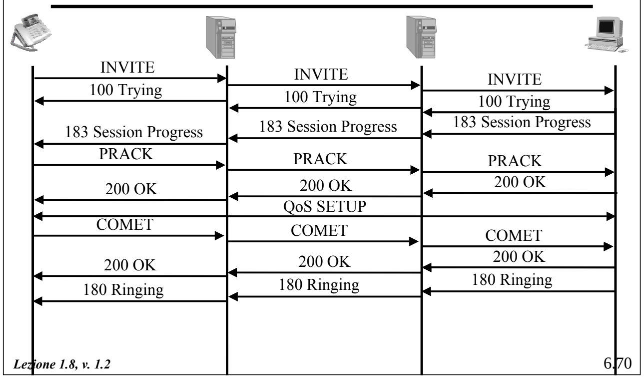
Qualità del servizio



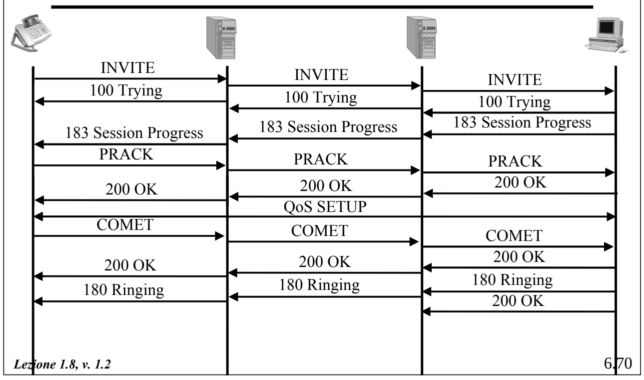
Qualità del servizio



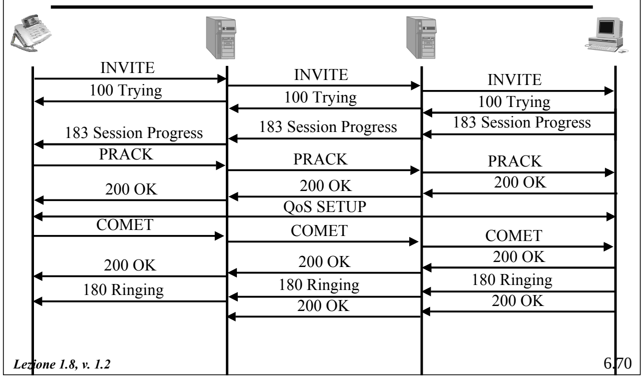
Qualità del servizio



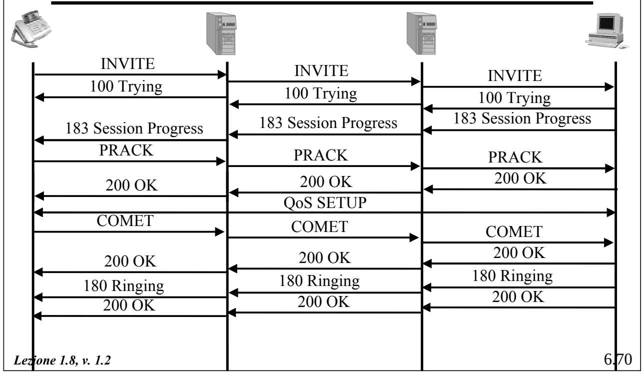
Qualità del servizio



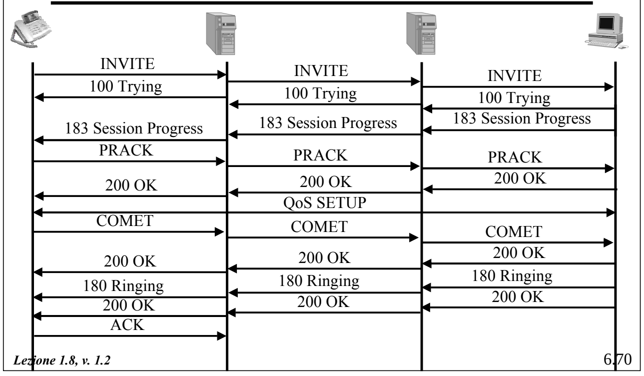
Qualità del servizio



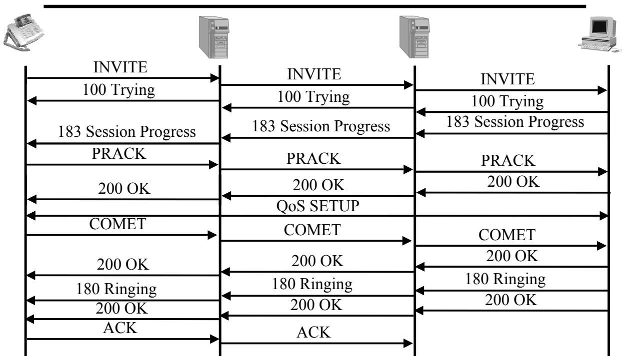
Qualità del servizio



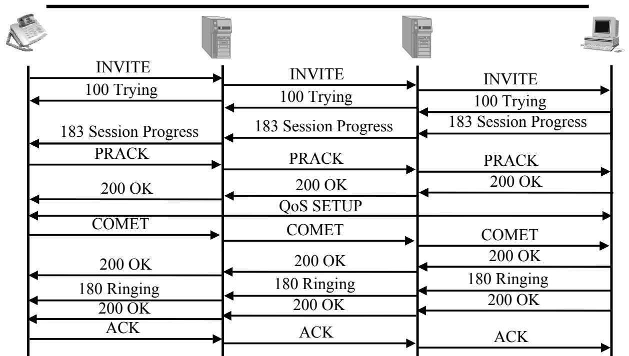
Qualità del servizio



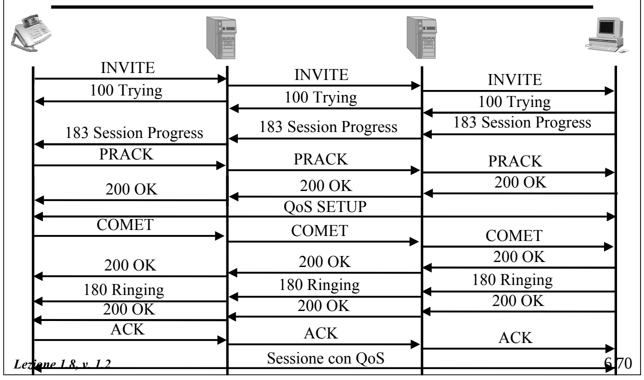
Qualità del servizio



Qualità del servizio



Qualità del servizio



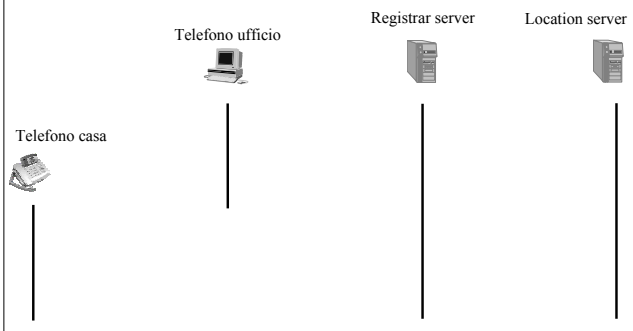
Le funzioni di SIP

- Risoluzione degli indirizzi.
- Funzioni relative ad una sessione
  - instaurazione, modifica, termine e cancellazione della sessione,
  - negoziazione dei media,
  - segnalazione durante la chiamata,
  - controllo della chiamata,
  - instaurazione di chiamate con QoS.
- Funzioni non relative ad una sessione
  - mobilità,
  - trasporto di messaggi,
  - notifica di eventi,
  - autenticazione.

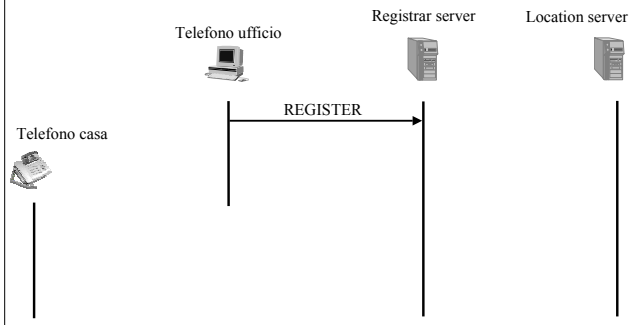
Mobilità in SIP

- La mobilità degli utenti è permessa grazie alla registrazione.
- Il processo di registrazione è simile a quanto avviene nelle reti cellulari
  - con SIP, però, si registrano gli utenti invece dei terminali.
- La registrazione avviene con il metodo REGISTER
  - il terminale in questione non deve implementare necessariamente SIP (PSTN)
    - » in questo caso per la registrazione si utilizzano altri sistemi (web, email. meccanismi automatici a tempo);
  - il protocollo per la registrazione verso il location server non è SIP.

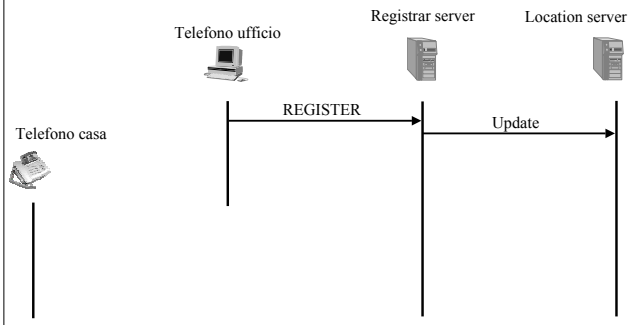
Mobilità in SIP



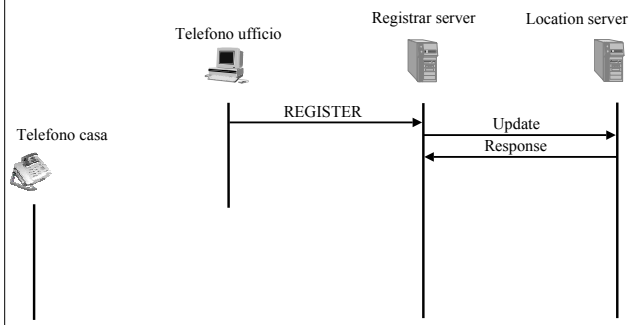
Mobilità in SIP



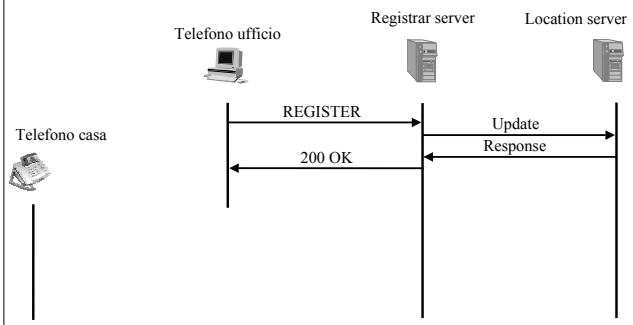
Mobilità in SIP



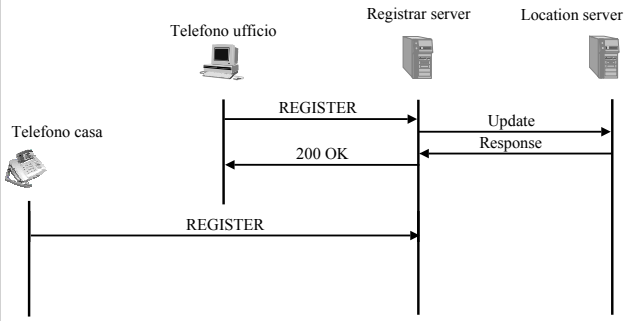
Mobilità in SIP



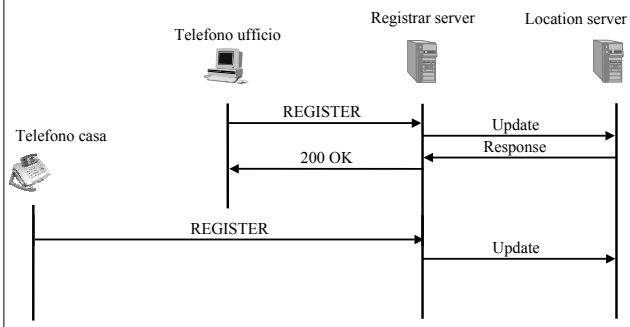
Mobilità in SIP



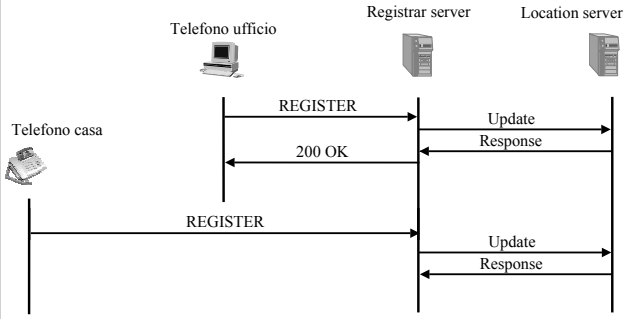
Mobilità in SIP



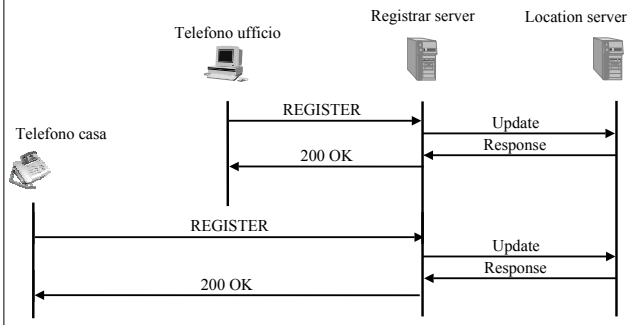
Mobilità in SIP



Mobilità in SIP



Mobilità in SIP



Mobilità in SIP

```
REGISTER sip:registrar.unige.it SIP/2.0
Via: SIP/2.0/UDP 208.251.99.12:5069
To: Utente A <sip:utenteA@unige.it>
From: Utente A <sip:utenteA@unige.it>
Call-ID: a5-32-43-12-77@208.251.99.12
CSeq: 1 REGISTER
Contact: <sip:utenteA@208.251.99.12>;class=personal
Contact: <sip:utenteA-mess@voicemail.provider.com;feature=voicemail
Contact: <sip:+39010222222@gateway.com;user=phone>;class=business
Contact: <sip:+39333989892@cellular.com;user=phone>;mobility=mobile
Contact: <tel:+39010444444>
Contact: mailto:utenteA@unige.it
Content-Length: 0
```


Mobilità in SIP

```
REGISTER sip:registrar.unige.it SIP/2.0
Via: SIP/2.0/UDP 208.251.99.12:5069
To: Utente A <sip:utenteA@unige.it>
From: Utente A <sip:utenteA@unige.it>
Call-ID: a5-32-43-12-77@208.251.99.12
CSeq: 1 REGISTER
Contact: <sip:utenteA@208.251.99.12>;class=personal
Contact: <sip:utenteA-mess@voicemail.provider.com;feature=voicemail
Contact: <sip:+39010222222@gateway.com;user=phone>;class=business
Contact: <sip:+39333989892@cellular.com;user=phone>;mobility=mobile
Contact: <tel:+39010444444>
```

Estensioni parametriche a Contact (User Preferences). Permettono ad un client di ottenere informazioni relative al device identificato dall'URL.

Mobilità in SIP

```
REGISTER sip:registrar.unige.it SIP/2.0
Via: SIP/2.0/UDP 208.251.99.12:5069
To: Utente A <sip:utenteA@unige.it>
From: Utente A <sip:utenteA@unige.it>
Call-ID: a5-32-43-12-77@208.251.99.12
CSeq: 1 REGISTER
Contact: <sip:utenteA@208.251.99.12>;class=personal
Contact: <sip:utenteA-mess@voicemail.provider.com;feature=voicemail
Contact: <sip:+39010222222@gateway.com;user=phone>;class=business
Contact: <sip:+39333989892@cellular.com;user=phone>;mobility=mobile
Contact: <tel:+39010444444>
Contact: mailto:utenteA@unige.it
Content-Length: 0
```

In genere gli indirizzi vengono provati in ordine.

Il client può specificare preferenze sul tipo di indirizzo da ricevere o da evitare.

Il client può anche esprimere la preferenza circa una ricerca sequenziale o parallela.

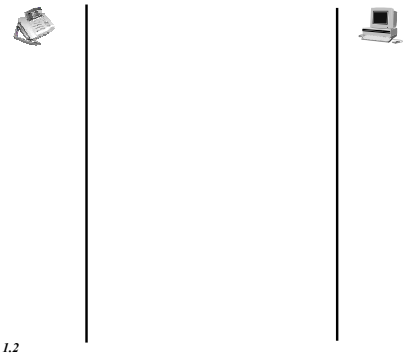
Trasporto di messaggi

- Il metodo MESSAGE consente di recapitare un messaggio al destinatario di una URI senza instaurare una sessione.
- Si utilizzano URI di tipo im anziché sip.
- Una risposta "200 OK" deve essere generata dal ricevente.

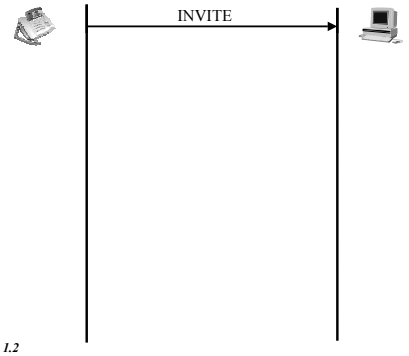
```
MESSAGE im:matteo@unige.it SIP/2.0
Via: SIP/2.0/UDP 130.251.1.99
To: matteo <im:matteo@unige.it>
From: lelus <im:lelus@unige.it>
Call-ID: 32-42-43-32@130.251.1.99
CSeq: 1 MESSAGE
Content-Type: text/plain
Content-Length: 15

Ciao, come stai?
```

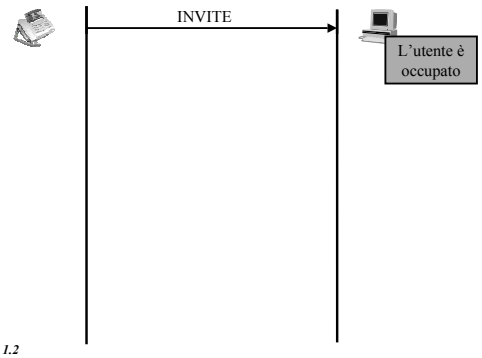

Sottoscrizione di eventi e notifiche



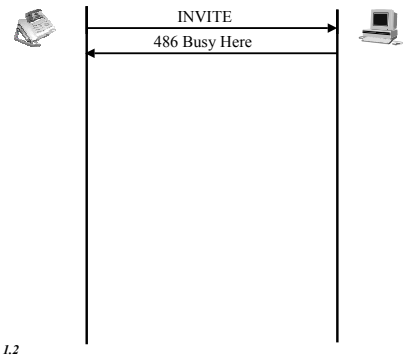
Sottoscrizione di eventi e notifiche



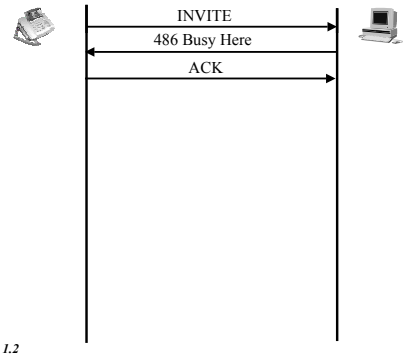
Sottoscrizione di eventi e notifiche



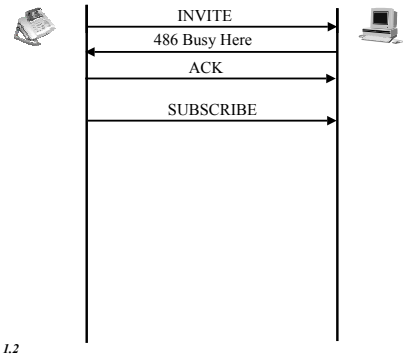
Sottoscrizione di eventi e notifiche



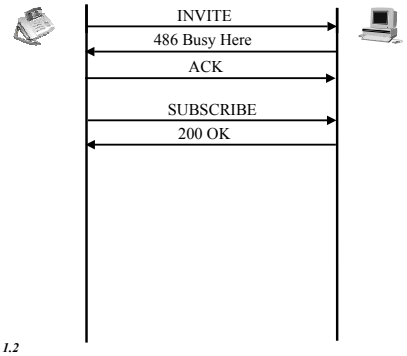
Sottoscrizione di eventi e notifiche



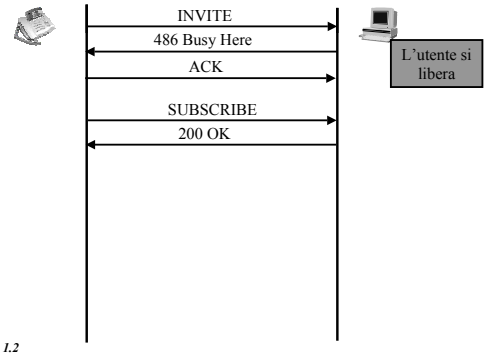
Sottoscrizione di eventi e notifiche



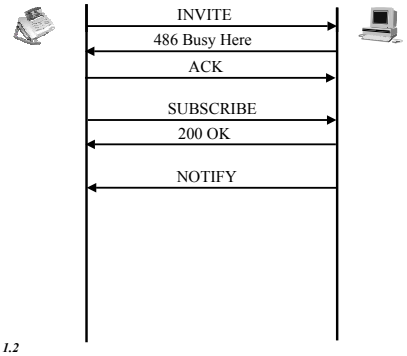
Sottoscrizione di eventi e notifiche



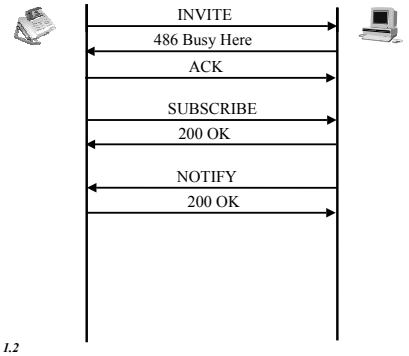
Sottoscrizione di eventi e notifiche



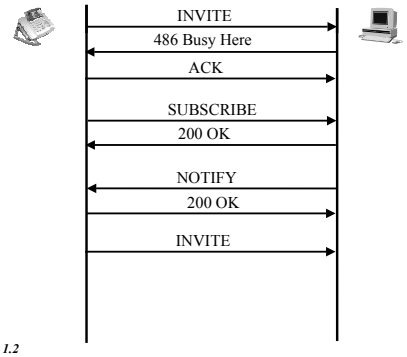
Sottoscrizione di eventi e notifiche



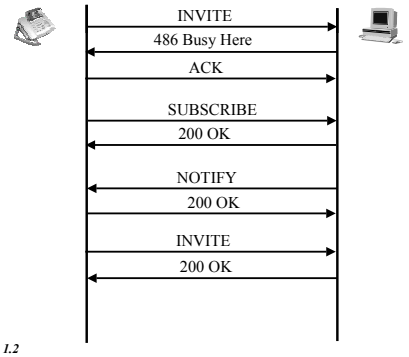
Sottoscrizione di eventi e notifiche



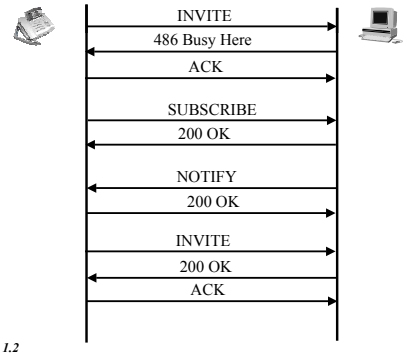
Sottoscrizione di eventi e notifiche



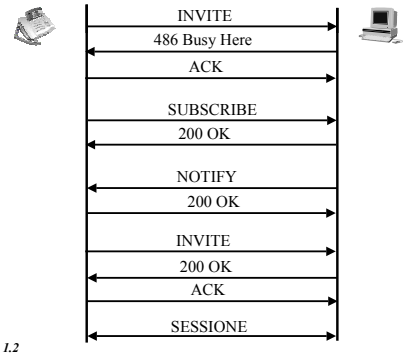
Sottoscrizione di eventi e notifiche



Sottoscrizione di eventi e notifiche



Sottoscrizione di eventi e notifiche



Sottoscrizione di eventi e notifiche

```
SUBSCRIBE: sip:matteo@unige.it SIP/2.0
Via: SIP/2.0/UDP 130.251.1.77
To: lelus <sip:lelus@unige.it>
From: matteo <sip:matteo@unige.it>
Call-ID: a3-32-4-55-44@130.251.1.77
CSeq: 1 SUBSCRIBE
Event: Available
Content-Length: 0
```

Sottoscrizione

Notifica

```
NOTIFY: sip:lelus@unige.it SIP/2.0
Via: SIP/2.0/UDP 130.251.15.7
To: matteo <sip:matteo@unige.it>
From: lelus <sip:lelus@unige.it>
Call-ID: 434566633@130.251.15.7
CSeq: 5 NOTIFY
Event: Available
Content-Length: 0
```


Sicurezza

- SIP prevede tre meccanismi di sicurezza delle comunicazioni
  - autenticazione;
  - riservatezza;
  - firma elettronica.

Sicurezza

Autenticazione

- L'autenticazione può essere rivolta da un client a:
  - un proxy (*proxy-authentication*),
    - » utile, ad es. per controllare l'accesso ad un gateway verso PSTN;
  - un altro endpoint.
- I meccanismi di autenticazione derivano dal quelli in uso per HTTP.
- Diversi tipi di autenticazione:
  - Basic, password passata in chiaro;
  - Digest, si basa su un meccanismo *challenge/response* con un segreto condiviso
    - » username e password;
  - Certificate;
  - SSL, SSH, solo per TCP.

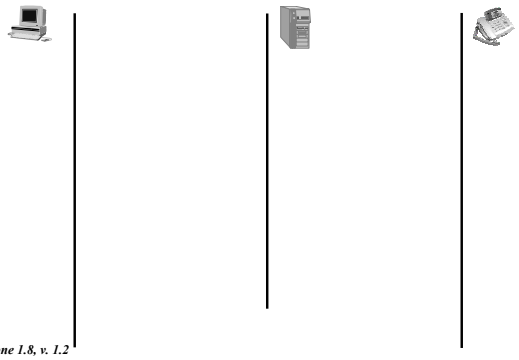
Sicurezza

Autenticazione

- L'autenticazione consiste in un MD5 del digest fornito nel *challenge* e di una combinazione di username/password
  - il digest viene restituito in una *response;*
  - l'MD5 non è tra gli algoritmi migliori
    - » il livello di sicurezza è adeguato all'applicazione,
    - » il tempo necessario per violarlo è superiore al tempo utile dell'informazione.

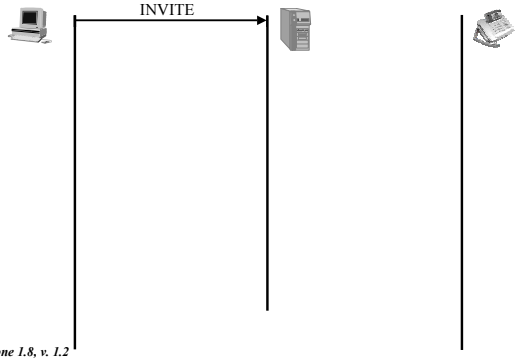
Sicurezza

Autenticazione



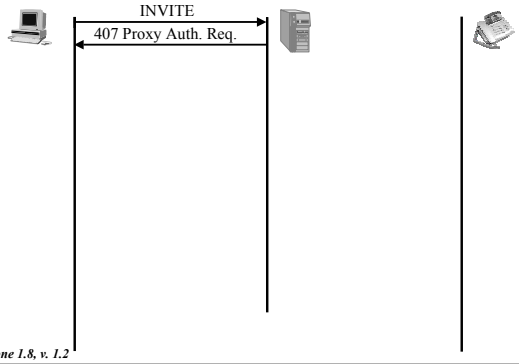
Sicurezza

Autenticazione



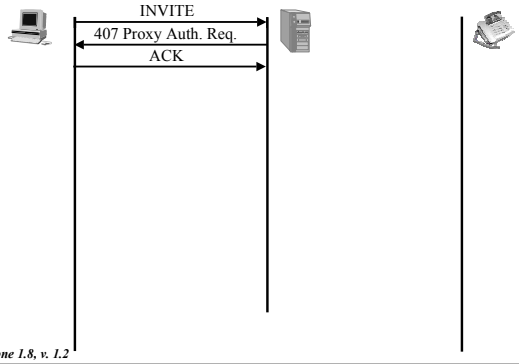
Sicurezza

Autenticazione



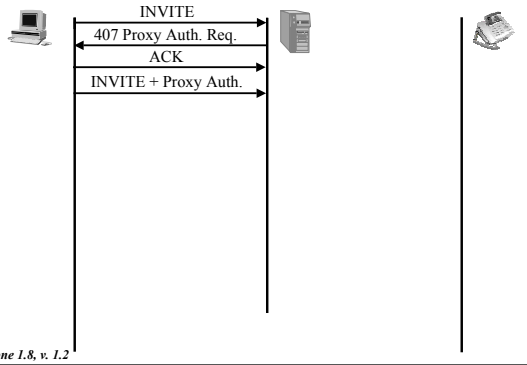
Sicurezza

Autenticazione



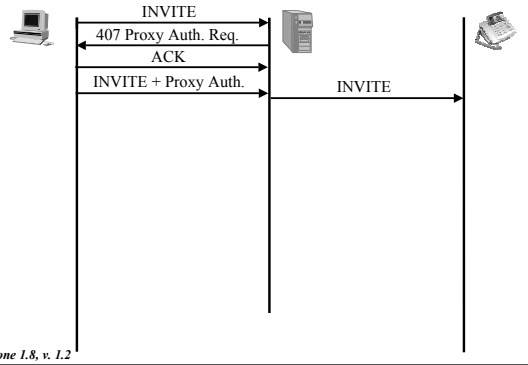
Sicurezza

Autenticazione



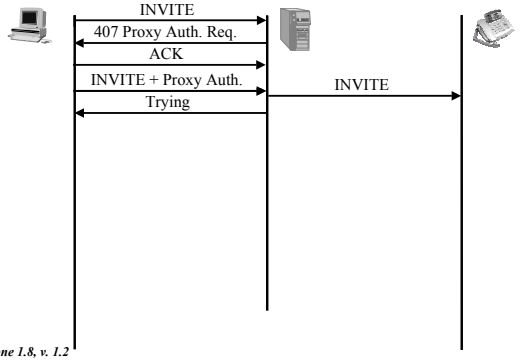
Sicurezza

Autenticazione



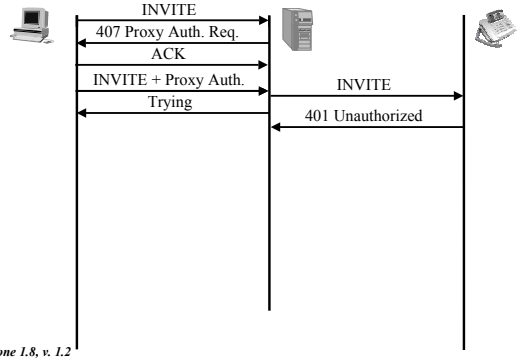
Sicurezza

Autenticazione



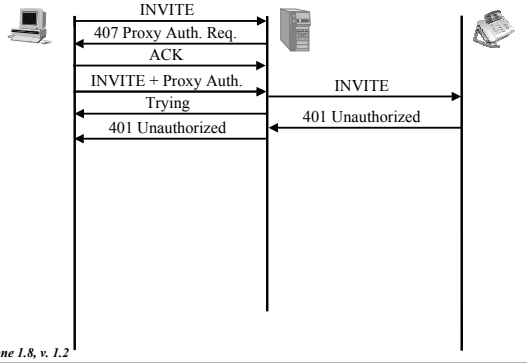
Sicurezza

Autenticazione



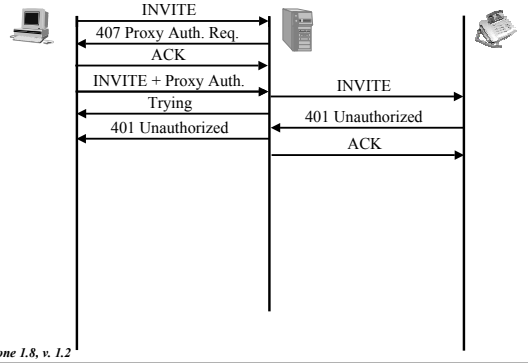
Sicurezza

Autenticazione



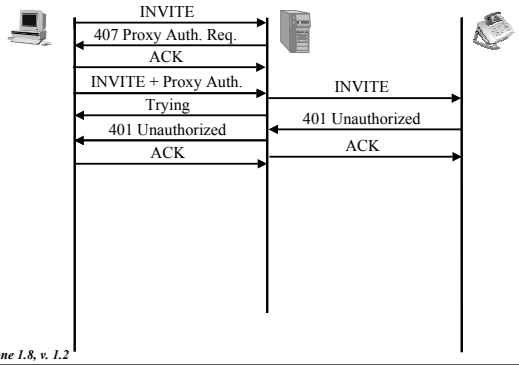
Sicurezza

Autenticazione



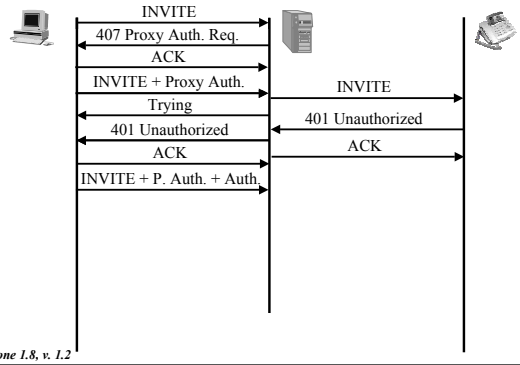
Sicurezza

Autenticazione



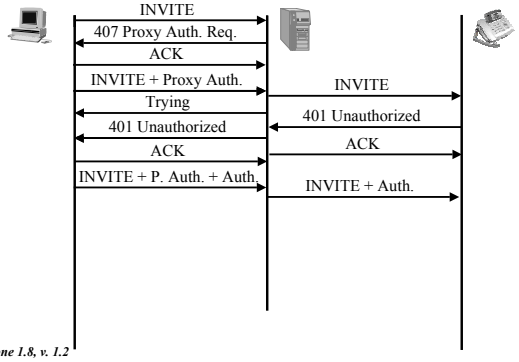
Sicurezza

Autenticazione



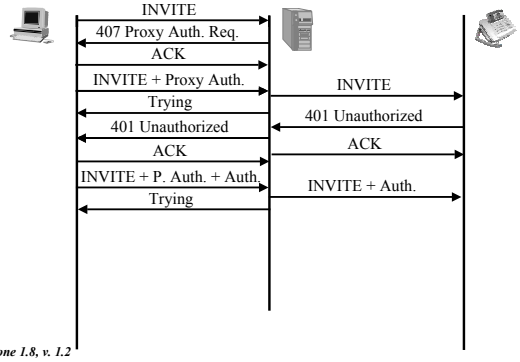
Sicurezza

Autenticazione



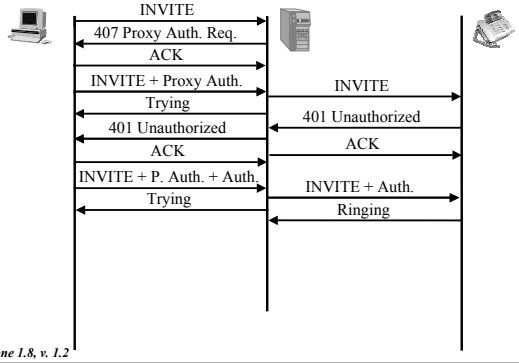
Sicurezza

Autenticazione



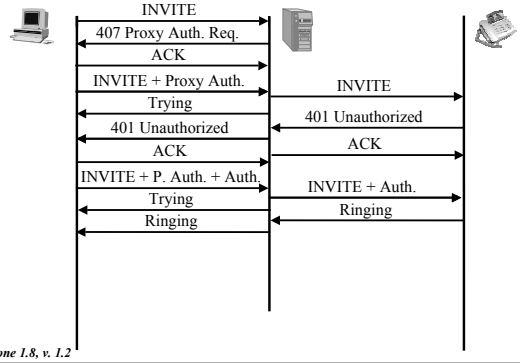
Sicurezza

Autenticazione



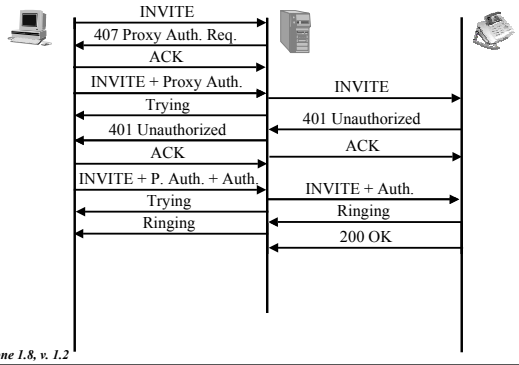
Sicurezza

Autenticazione



Sicurezza

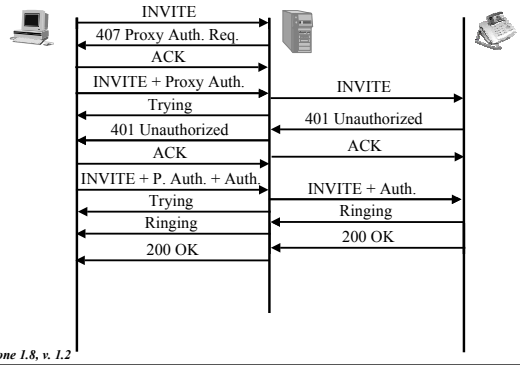
Autenticazione



R. Bolla Telematica 2, n. o.

Sicurezza

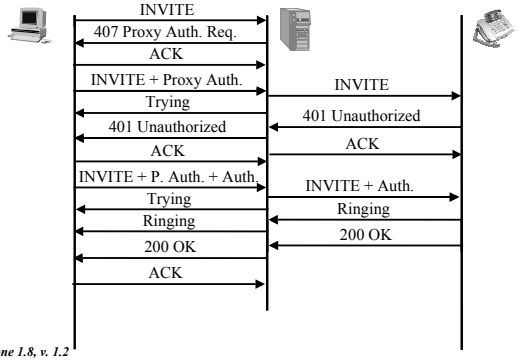
Autenticazione



R. Bolla Telematica 2, n. o.

Sicurezza

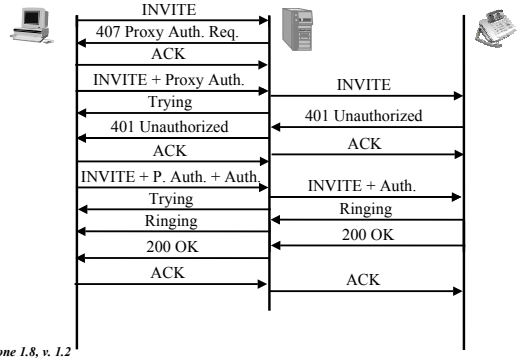
Autenticazione



R. Bolla Telematica 2, n. o.

Sicurezza

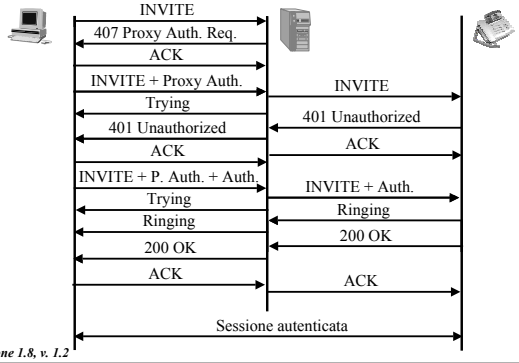
Autenticazione



R. Bolla Telematica 2, n. o.

Sicurezza

Autenticazione



R. Bolla Telematica 2, n. o.

Sicurezza

Cifratura

- La cifratura SIP assume due forme:
  - *hop by hop*: l'intero pacchetto viene cifrato
    - » IPSec, TLS;
    - » non è necessario un supporto SIP per questa cifratura;
  - *end-to-end*: il messaggio SIP è parzialmente cifrato
    - » non tutti i campi possono essere cifrati (proxy intermedi);
    - » per la cifratura si può usare per es. PGP.

SIP e sicurezza delle reti

- L'utilizzo di SIP, come H.323, deve risolvere tutta una serie di problematiche connesse con l'utilizzo di dispositivi di sicurezza
  - NAT;
  - firewall.

SIP e sicurezza delle reti

NAT

- L'indirizzo IP appare in diversi campi dei pacchetti SIP:

```
INVITE sip:picard@wcom.com SIP/2.0
Via: SIP/2.0/UDP 192.16.8.1:50
From: Alan Johnston <sip:alan.johnston@wcom.com>
To: Jean Luc Picard <sip:picard@wcom.com>
Call-ID: 314159@192.16.8.1
CSeq: 1 INVITE
Contact: sip:alan.johnston@192.16.8.1
Subject: Where are you these days?
Content-Type: application/sdp
Content-Length: 124

v=0
o=ajohnston 5462346 332134 IN IP4 host.wcom.com
c=IN IP4 192.16.8.1
m=audio 49170 RTP/AVP 0 3
```


R. Bolla Telematica 2, n. o.

SIP e sicurezza delle reti

NAT

- L'indirizzo IP appare in diversi campi dei pacchetti SIP:

INVITE sip:picard@wcom.com SIP/2.0
Via: SIP/2.0/UDP 192.16.8.1:50
From: Alan Johnston <sip:alan.johnston@wcom.com>
To: Jean Luc Picard <sip:picard@wcom.com>
Call-ID: 314159@192.16.8.1
CSeq: 1 INVITE
Contact: sip:alan.johnston@192.16.8.1
Subject: Where are you these days?
Content-Type: application/sdp
Content-Length: 124

v=0
o=ajohnston 5462346 332134 IN IP4 host.wcom.com
c=IN IP4 192.16.8.1
m=audio 49170 RTP/AVP 0 3

Lezione 1 6.84

R. Bolla Telematica 2, n. o.

SIP e sicurezza delle reti

NAT

- L'indirizzo IP appare in diversi campi dei pacchetti SIP:

INVITE sip:picard@wcom.com SIP/2.0
Via: SIP/2.0/UDP 192.16.8.1:50
From: Alan Johnston <sip:alan.johnston@wcom.com>
To: Jean Luc Picard <sip:picard@wcom.com>
Call-ID: 314159@192.16.8.1
CSeq: 1 INVITE
Contact: sip:alan.johnston@192.16.8.1
Subject: Where are you these days?
Content-Type: application/sdp
Content-Length: 124

v=0
o=ajohnston 5462346 332134 IN IP4 host.wcom.com
c=IN IP4 192.16.8.1
m=audio 49170 RTP/AVP 0 3

Lezione 1 6.84

R. Bolla Telematica 2, n. o.

SIP e sicurezza delle reti

NAT

- L'indirizzo IP appare in diversi campi dei pacchetti SIP:

INVITE sip:picard@wcom.com SIP/2.0
Via: SIP/2.0/UDP 192.16.8.1:50
From: Alan Johnston <sip:alan.johnston@wcom.com>
To: Jean Luc Picard <sip:picard@wcom.com>
Call-ID: 314159@192.16.8.1
CSeq: 1 INVITE
Contact: sip:alan.johnston@192.16.8.1
Subject: Where are you these days?
Content-Type: application/sdp
Content-Length: 124

v=0
o=ajohnston 5462346 332134 IN IP4 host.wcom.com
c=IN IP4 192.16.8.1
m=audio 49170 RTP/AVP 0 3

Lezione 1 6.84

R. Bolla Telematica 2, n. o.

SIP e sicurezza delle reti

NAT

- L'indirizzo IP appare in diversi campi dei pacchetti SIP:

INVITE sip:picard@wcom.com SIP/2.0
Via: SIP/2.0/UDP 192.16.8.1:50
From: Alan Johnston <sip:alan.johnston@wcom.com>
To: Jean Luc Picard <sip:picard@wcom.com>
Call-ID: 314159@192.16.8.1
CSeq: 1 INVITE
Contact: sip:alan.johnston@192.16.8.1
Subject: Where are you these days?
Content-Type: application/sdp
Content-Length: 124

v=0
o=ajohnston 5462346 332134 IN IP4 host.wcom.com
c=IN IP4 192.16.8.1
m=audio 49170 RTP/AVP 0 3

Lezione 1 6.84

SIP e sicurezza delle reti

NAT - Problemi

- La presenza del NAT comporta una serie di problematiche dovute alla sostituzione degli indirizzi IP:
  - la risposta alla richiesta non può essere instradata verso chi l'ha originata **(Via:)**;
  - eventuali richieste future da parte del chiamato non potranno raggiungere il chiamante (**Contact:**);
  - i pacchetti RTP inviati dal chiamato non raggiungeranno il chiamante (parametro "c" in SDP).
- Anche i numeri delle porte (5060 e 49170) potrebbero essere cambiate dal NAT, impedendo il corretto scambio di segnalazione/media.

SIP e sicurezza delle reti

NAT - Soluzioni

- Possibili soluzioni:
  - un proxy che si accorge della sostituzione, inserisce il nuovo indirizzo IP nell'intestazione **Via:**, in modo che il pacchetto possa tornare correttamente al chiamante attraverso il NAT
    - » è necessario che il NAT mantenga un'assegnazione statica degli indirizzi per tutta la durata della sessione
      - ✓ usando TCP questo non rappresenta un requisito critico;
  - utilizzo di una connessione TCP permanente per tutta la durata della connessione, per le eventuali richieste da parte del chiamato;
  - utilizzo di un flusso RTP simmetrico (il chiamato ignora le informazioni SDP).

SIP e sicurezza delle reti

Firewall - Problemi

- L'interazione di SIP con i firewall dipende dal protocollo di trasporto utilizzato:
  - UDP:
    - » le richieste possono essere inviate all'esterno, ma le risposte non possono essere ricevute,
    - » non si possono ricevere chiamate da host esterni,
    - » non si possono ricevere flussi RTP;
  - TCP:
    - » è possibile ricevere le risposte alle richieste inviate (utilizzando la stessa connessione TCP),
    - » non si possono ricevere chiamate da host esterni,
    - » non si possono ricevere flussi RTP.

SIP e sicurezza delle reti

Firewall - Soluzioni

- ALG (Application Level Gateway)
  - l'ALG è un proxy SIP/RTP ritenuto affidabile dal firewall
    - » esegue autenticazioni, validazioni, tariffazioni, …;
  - il firewall lascia passare solo i pacchetti SIP e RTP diretti/provenienti dall'ALG;
  - l'ALG funziona anche con i NAT
    - » gli indirizzi IP nei messaggi SIP sono sostituiti;
  - l'ALG si trova di solito nella DMZ;
  - non sono necessarie modifiche dinamiche nelle politiche di sicurezza del firewall.

SIP e sicurezza delle reti

Firewall - Soluzioni

- Firewall proxy
  - comunica con il firewall/NAT;
  - esegue autenticazione, autorizzazione, ecc;
  - permette l'invio diretto dei media tra gli endpoint:
    - » ricava gli indirizzi IP/porte UDP del flusso RTP dai messaggi SIP,
    - » apre le corrispondenti porte sul firewall,
    - » mantiene traccia delle sostituzioni NAT e modifica di conseguenza l'SDP;
  - alla chiusura della sessione (BYE) il firewall proxy richiude le porte sul firewall e rimuove l'associazione del NAT;
  - il protocollo di comunicazione tra il firewall proxy ed il firewall non è ancora standardizzato (MidCom IETF).

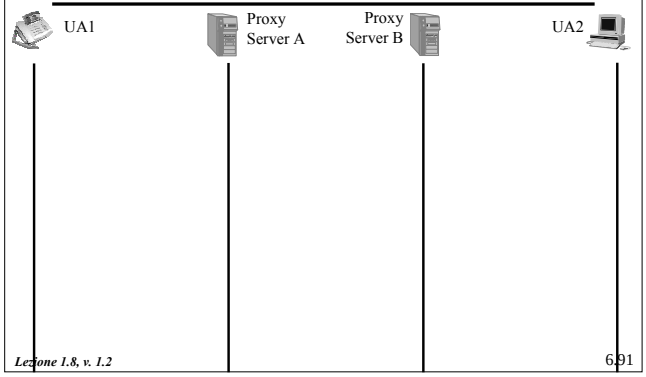
SIP e sicurezza delle reti

Intermediari di sicurezza

- Gli intermediari di sicurezza (ALG, firewall proxy) devono essere sempre attraversati dalla segnalazione
  - l'URL dell'utente deve essere risolta all'indirizzo IP dell'intermediario;
  - la segnalazione deve utilizzare l'opzione *Record-Route* per registrare l'intermediario da attraversare.
- SIP prevede l'utilizzo delle opzioni *Record-Route* e *Route* per memorizzare i proxy da attraversare e forzare il percorso ai successivi messaggi.
- Gli intermediari di sicurezza devono essere impostati come default outbound proxy per tutte richieste in uscita.

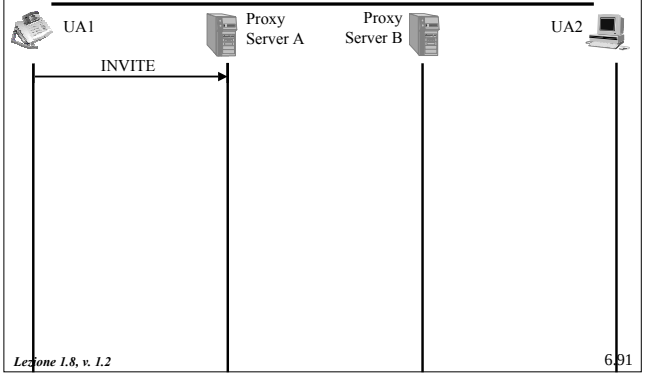
SIP e sicurezza delle reti

Record-Route



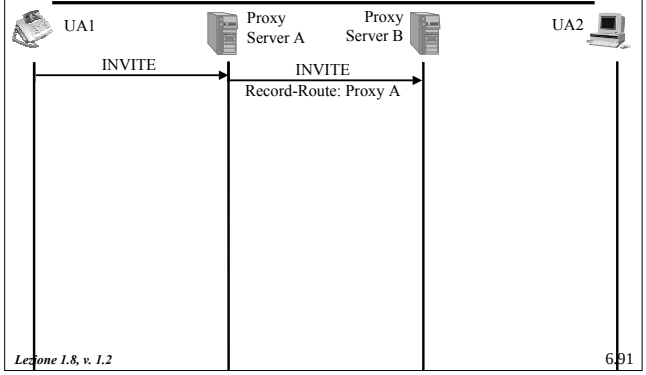
SIP e sicurezza delle reti

Record-Route



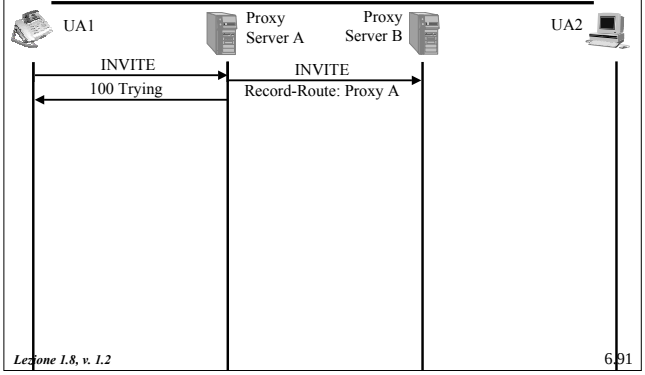
SIP e sicurezza delle reti

Record-Route



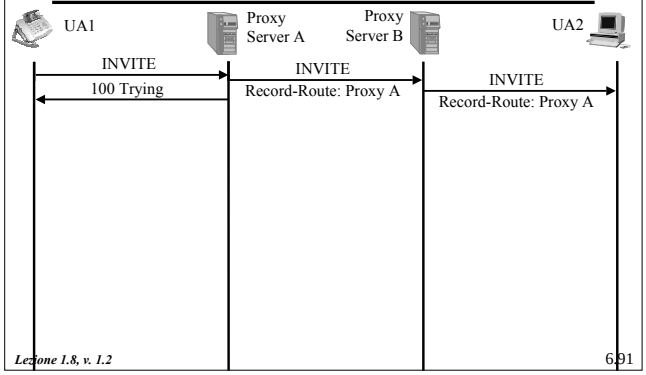
SIP e sicurezza delle reti

Record-Route



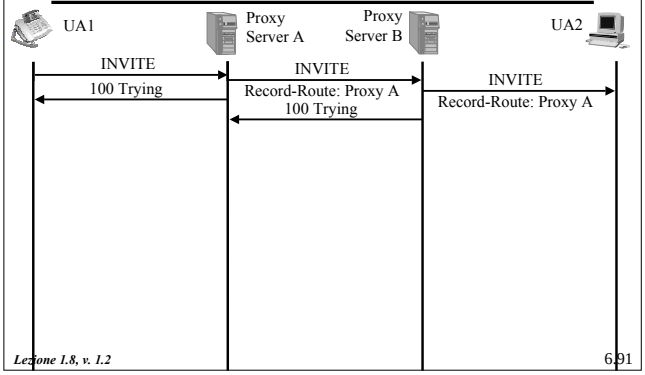
SIP e sicurezza delle reti

Record-Route



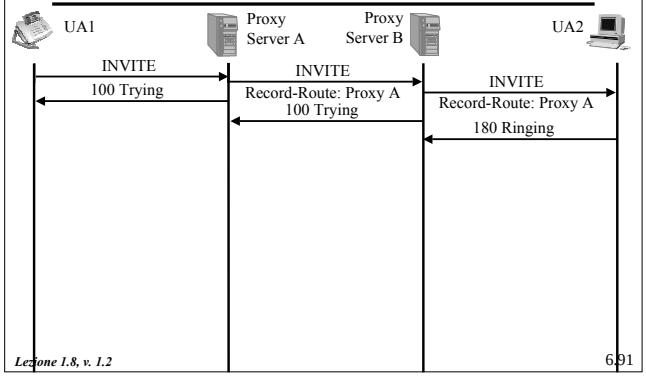
SIP e sicurezza delle reti

Record-Route



SIP e sicurezza delle reti

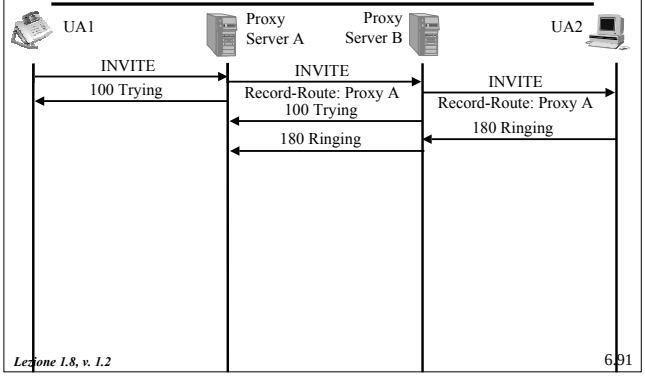
Record-Route



R. Bolla Telematica 2, n. o.

SIP e sicurezza delle reti

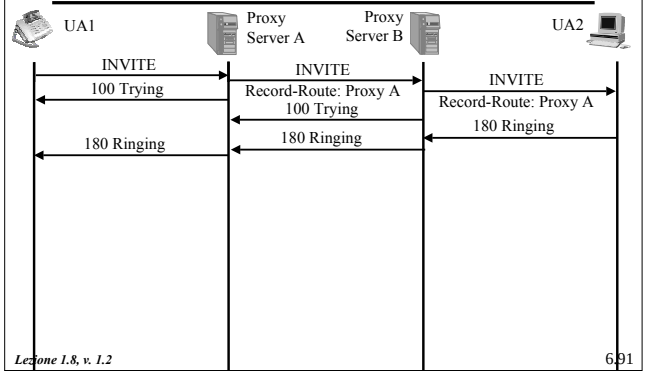
Record-Route



R. Bolla Telematica 2, n. o.

SIP e sicurezza delle reti

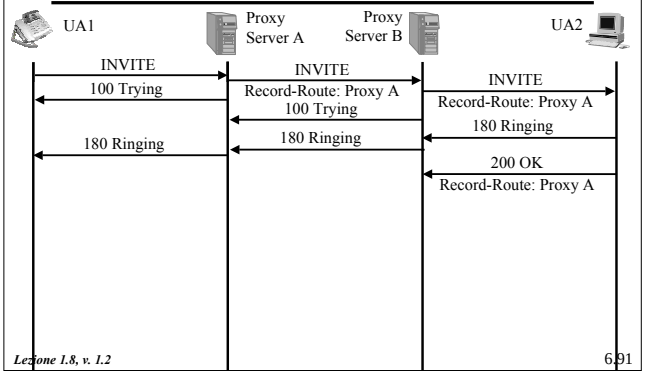
Record-Route



R. Bolla Telematica 2, n. o.

SIP e sicurezza delle reti

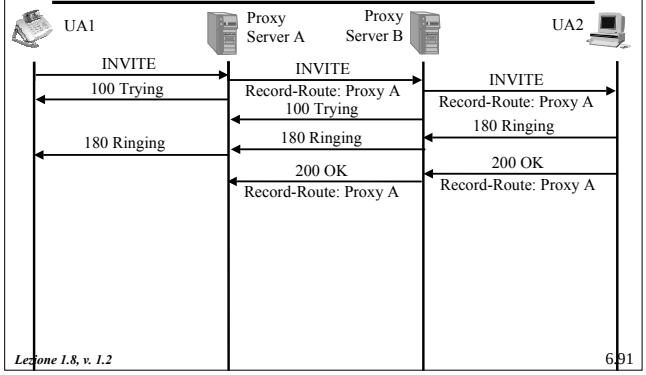
Record-Route



R. Bolla Telematica 2, n. o.

SIP e sicurezza delle reti

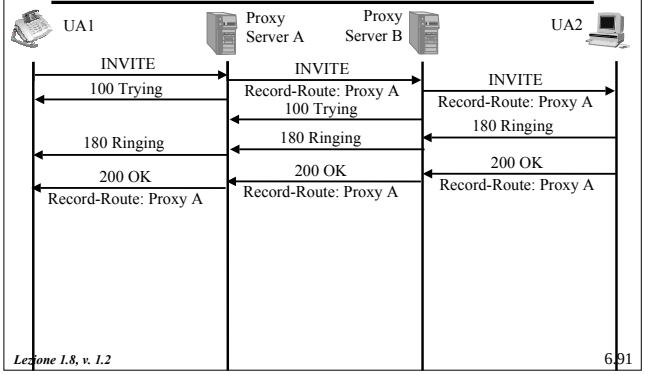
Record-Route



R. Bolla Telematica 2, n. o.

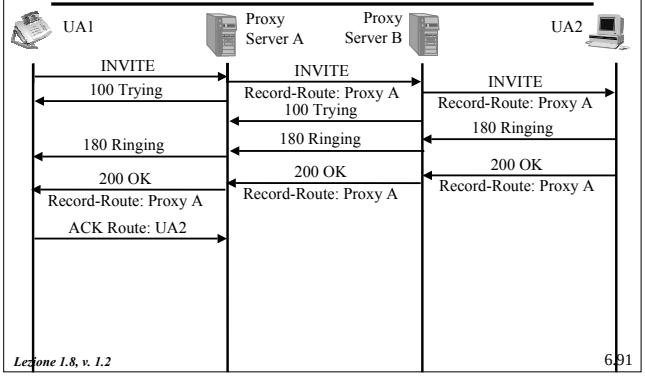
SIP e sicurezza delle reti

Record-Route



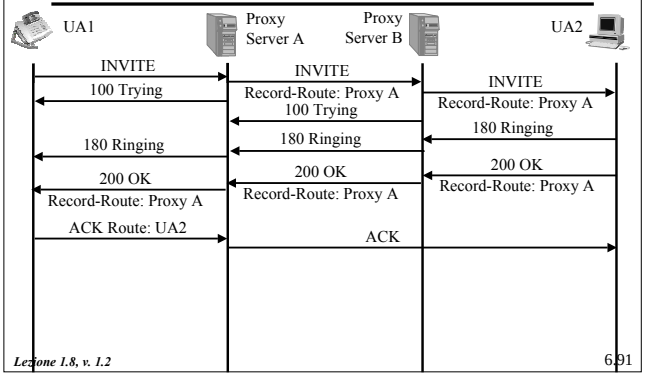
SIP e sicurezza delle reti

Record-Route



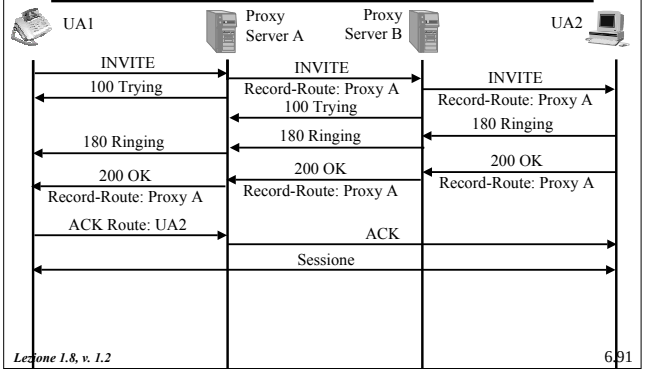
SIP e sicurezza delle reti

Record-Route



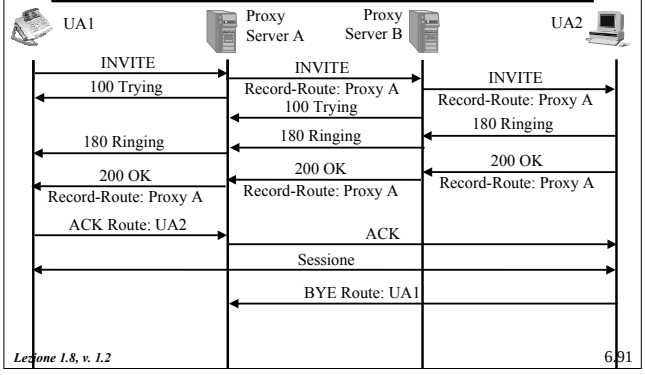
SIP e sicurezza delle reti

Record-Route



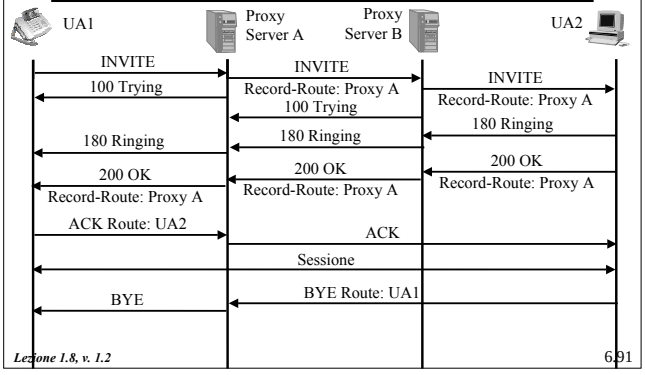
SIP e sicurezza delle reti

Record-Route



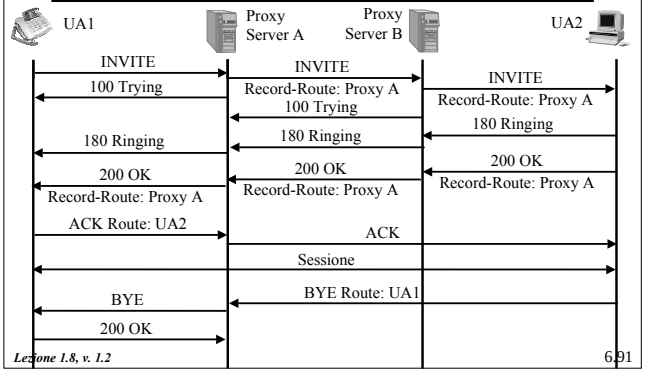
SIP e sicurezza delle reti

Record-Route



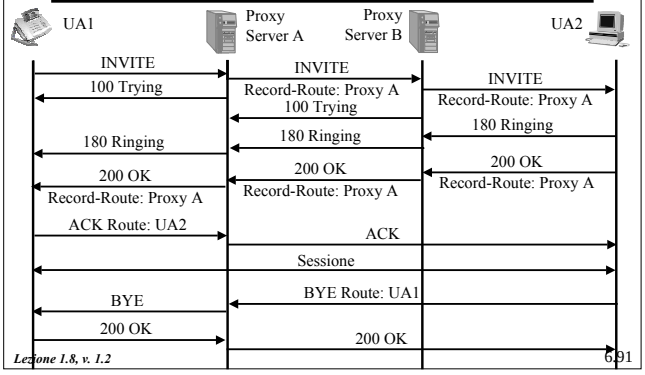
SIP e sicurezza delle reti

Record-Route



SIP e sicurezza delle reti

Record-Route



Privacy

- La privacy è una caratteristica delle attuali reti PSTN
  - blocco della visualizzazione del numero del chiamante;
  - telefoni pubblici.
- SIP non presenta intrinsecamente questa caratteristica
  - l'instaurazione di una sessione richiede lo scambio di dati privati significativi (indirizzo IP).
- La privacy può essere assicurata in SIP utilizzando un *back-to-back user agent* (B2BUA)
  - funziona da "anonymizer" agendo come intermediario tra i terminali remoti;
  - ogni terminale invia(riceve) la segnalazione/media solo al B2BUA.

Creazione di nuovi servizi in SIP

- L'architettura distribuita di SIP permette la realizzazione di nuovi servizi e funzionalità da parte degli utenti
  - call forwarding, integrazione con web o db.
- I servizi possono risiedere
  - nei server/proxy
    - » maggior affidabilità (presenza costante),
    - » necessità e limitazioni dovute al caricamento del software
  - negli agenti chiamati
    - » maggiore libertà realizzativa,
    - » necessità di essere sempre registrati e "on-line";
  - negli agenti chiamanti
    - » è necessario che i server rispondano secondo determinati schemi (es. redirect per un call forwarding).

Creazione di nuovi servizi in SIP

Nuovi metodi e intestazioni

- Nuove funzionalità e servizi possono essere implementati definendo nuove intestazioni e metodi
  - le proposte possono essere sottomesse all'IETF per la standardizzazione.
  - non richiedono il supporto dei server SIP
    - » i proxy che ricevono richieste con metodi sconosciuti le inoltrano.

Creazione di nuovi servizi in SIP

Realizzazione

- *Call Processing Language* (CPL), IETF
  - sviluppato per permettere ad utenti anonimi di inserire i loro servizi su server SIP;
  - basato su XML (eXtensible Markup Language);
  - la struttura prevede l'utilizzo di "etichette" (*tag*), in modo analogo all'HTML
    - » le etichette possono avere "attributi";

Creazione di nuovi servizi in SIP

Call Processing Language

Esempio di uno script per rifiutare le chiamate anonime:

```
<?xml version="1.0"?>
<!DOCTYPE cpl PUBLIC "-//IETF/DTD RFCxxxx CPL 1.0//EN"
"cpl.dtd">

<cpl>
 <incoming>
  <address-switch field="origin" subfield="user">
    <address is="anonymous">
     <reject status="reject"
                  reason="Non accetto chiamate anonime"
/>
    </address>
  </address-switch>
 </incoming>
</cpl>
```

Creazione di nuovi servizi in SIP

Realizzazione

- SIP *Common Gateway Interface* (CGI)
  - analogo al CGI dell'HTTP;
  - rappresenta un'interfaccia, non un linguaggio di programmazione
    - » come linguaggi si possono utilizzare C, Perl, TCL, ecc;
  - buona parte del codice CGI HTTP può essere riutilizzato;
  - mantengono uno stato, in modo da poter associare diverse richieste alla stessa sessione SIP.

Creazione di nuovi servizi in SIP

Realizzazione

- SIP *Application Programming Interfaces* (API)
  - minor overhead, un processo esterno non deve essere creato ogni volta;
  - maggior semplicità per memorizzare stato e timer della session;
  - dipendono dal linguaggio utilizzato;
  - SIP Java Servlets, JAIN.
- SIP e VoiceXML
  - basato su XML;
  - riproduce messaggi, riconosce input (tastiera e vocali), elabora i risultati;
  - non si relazione direttamente con SIP; uno script VoiceXML può essere eseguito insieme ad uno script CPL o CGI per implementare un servizio interattivo.

Preferenze degli utenti

- La telefonia tradizionale PSTN non la possibilità agli utenti di specificare come gestire le singole chiamate
  - questo deriva in gran parte dall'architettura centralizzata di questi sistemi.
- Nelle reti IP (SIP) l'intelligenza è decentralizzata
  - è possibile gestire in modo scalabile le preferenze degli utenti:
    - » chiamare solo caselle vocali,
    - » decidere gli orari in cui ricevere determinati tipologie di chiamate,
    - » specificare i terminali su cui essere chiamato solo in determinate date/orari,
    - » abilitare le comunicazioni IM solo in riunione.

Preferenze degli utenti

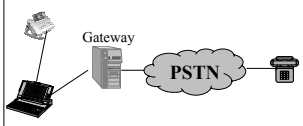
- Ci sono due categorie di preferenze degli utenti:
  - preferenze del chiamante
    - » richieste al server su come cercare la destinazione: proxy, cancel, fork, recurse, parallel, queue;
    - » come gestire le URL: parametri per decidere quali URL accettare/rifiutare;
  - preferenze del chiamato
    - » sono generalmente invocate da un proxy che gestisce la chiamata in arrivo;
    - » l'utente usa REGISTER per caricarle nel server insieme ai servizi desiderati.

Conferenze con SIP

- Le diverse architetture utilizzabili per le conferenze con SIP possono essere distinte sulla base:
  - della segnalazione necessaria per l'instaurazione della conferenza;
  - della modalità con cui i flussi di informazioni sono trasportati e miscelati.
- Ogni modello differisce dagli altri per quanto riguarda:
  - scalabilità della conferenza;
  - flusso di informazioni per partecipare;
  - come e dove i media sono mandati e miscelati;
  - posizionamento della logica: endpoint o server.

Conferenze con SIP

Modelli di conferenza

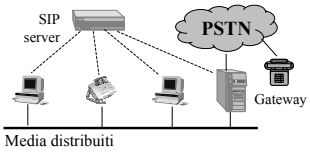


Endpoint mixing

- Piccole conferenze (3-5 partecipanti).
- Un endpoint gestisce la segnalazione e la miscelazione dei media
  - tale endpoint deve essere operativo per tutta la durata della conferenza.

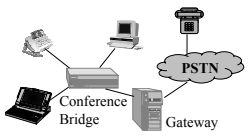
Server SIP e media distribuiti

- Il server SIP stabilisce una maglia completa di flussi RTP tra tutti i partecipanti.
- Ogni partecipante miscela i flussi in ingresso e invia il proprio a tutti gli altri.
- In genere poche stazioni trasmettono contemporaneamente
  - la miscelazione dei flussi richiede una elaborazione limitata.



Conferenze con SIP

Modelli di conferenza



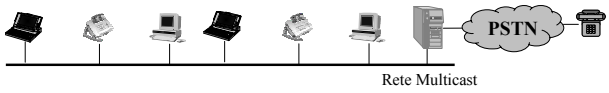
Centralized conference

- Conferenze media dimensione
- Il conference bridge
  - gestisce la segnalazione;
  - riceve e miscela i flussi RTP;
  - comprende il software applicativo per AAA, controllo della controllo della conferenza;
  - invia il flusso dei media a tutti i partecipanti.

- La conferenza può essere:
  - dial-in: i partecipanti si uniscono alla sessione attraverso il Conference Bridge;
  - ad-hoc: la conferenza nasce su invito a partire da una comunicazione tra due terminali o da una conferenza *Endpoint mixing*, passando il controllo al Conference Bridge.

Conferenze con SIP

Modelli di conferenza



Large multicast conference

- Conferenze su larga scala (milioni di utenti).
- Gli utenti aderiscono ad un indirizzo multicast annunciato sul web, via mail, o sono invitati tramite SIP
  - la segnalazione SIP non è strettamente richiesta.

Confronto SIP/H.323

Tabella delle caratteristiche

	H.323	SIP
Architettura	Stack/Centralizzata	Elementi/Distribuita
Origine	ITU	IETF
Trasporto	Principalmente TCP	Principalmente UDP
Codifica	ASN.1	Testuale, simile ad HTTP
Enfasi	Telefonia	Multimedialità
Indirizzi	Alias	URL sip

Confronto SIP/H.323

H.323

- Maggiore complessità, utilizza diversi protocolli per la segnalazione.
- La codifica ASN.1 è complessa da gestire a livello di programmazione.
- Maggiori ritardi nel setup delle comunicazioni.
- Pensato per singole LAN.

SIP

- Un unico protocollo, integrato con servizi già esistenti.
- La codifica testuale è molto semplice da gestire a livello di programmazione ed è simile a quella di RTSP.
- Semplicità nell'instaurazione della connessione.
- Progettato per l'utilizzo in WAN.

Confronto SIP/H.323

H.323

- Gatekeeper e gateway possono essere intasati dalle connessioni TCP.
- Supporto per mobilità e redirezionalità limitato.
- Permette un ampio controllo sulla conferenza (ad es. registrando i partecipanti).

SIP

- I proxy stateless che utilizzano UDP non devono mantenere informazioni di stato sulle connessioni attive.
- Ampio supporto per la mobilità dell'utente.
- Non fornisce controlli addizionali per la conferenza oltre a quelli di base del RTCP.

Coesistenza SIP/H.323

- I terminali SIP e H.323 non possono comunicare tra di loro.
- La realizzazione di un gateway è abbastanza semplice:
  - necessita la traduzione dei soli flussi di segnalazione;
  - i flussi di informazioni non hanno bisogno di traduzione poiché si possono usare gli stessi codec.
- I due protocolli possono coesistere su diversi segmenti di una stessa connessione.