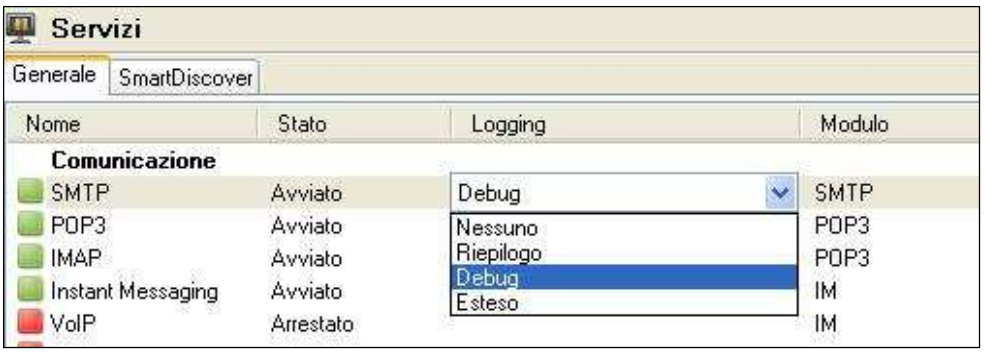
Registrazione delle attività e diagnostica di base delle problematiche di mancata ricezione

Ciascun servizio di IceWarp Server permette di impostare un livello di registrazione dell'attività che mantenga traccia di ciò che accade sullo specifico servizio, allo scopo di individuare le problematiche di funzionamento del mail server e porvi soluzione.

Impostazioni generali di logging

Per ciascun servizio si può quindi scegliere fra una registrazione di tipo riepilogativo e una invece decisamente più dettagliata (Debug, Esteso). Per avere informazioni tali da diagnosticare la maggior parte delle problematiche si consiglia di attivare il logging a livello *Debug*.



I log vengono salvati al percorso definito in [Sistema > Memorizzazione > Cartelle > Percorso log].
I file prodotti avranno nomi che variano a seconda del loro contenuto e del periodo di tempo al quale si riferiscono. L'iniziale indica il tipo di log (es: c: Web, e: Errori, p: Pop, s: Smtp, m: Imap) e la restante parte del nome corrisponde alla data in formato “aaaammgg” ed eventualmente un indice crescente nel caso in cui i log siano stati “spezzati”.
E' infatti possibile (nonché decisamente consigliato per sistemi con alto volume di traffico) fare in modo che raggiunta una certa dimensione nella creazione del file di log esso venga chiuso e ne venga creato uno nuovo di modo da non creare file di dimensioni troppo elevate sfavorendo la portabilità e consultabilità delle informazioni [Sistema > Registrazione attività > Generale > Ruota i file di log quando le dimensioni superano].
E' anche possibile alleggerire l'operazione di scrittura dei log definendo una cache ed è possibile impostare la cancellazione automatica dei file più vecchi di un determinato periodo, mantenendo un archivio dei file cancellati se lo si desidera.

SMTP

Il log di SMTP mantiene traccia di tutte le sessioni passate dal mail server, siano esse di tipo Server (con IceWarp Server che agisce come **ricevente**) o Client (IceWarp Server che agisce come **mittente**).
Tramite la consultazione del log SMTP è possibile, nella norma, stabilire il motivo per il quale un determinato messaggio non è stato ricevuto.

Di seguito l'esempio di una sessione Client e della relativa sessione Server (sul server remoto) andate a buon fine:

- Client

```
SYSTEM          [1140] 10:47:14 Client session Message id OSA88513 item 201110051047140042.tm$
SYSTEM          [1140] 10:47:14 Client session DNS query 'icewarp.it' 0 (2) [OK - 1]
SYSTEM          [1140] 10:47:14 Client session Connecting to 'mail.icewarp.it'
89.186.73.168   [1140] 10:47:14 Client session Connected, local IP= 192.168.26.218
89.186.73.168   [1140] 10:47:14 Client session <<< 220 mail.fastflow.it ESMTP IceWarp 10.3.4 (2011-09-22); Wed, 05 Oct 2011 10:47:12 +0200
89.186.73.168   [1140] 10:47:14 Client session >>> EHLO localhost
89.186.73.168   [1140] 10:47:14 Client session <<< 250 HELP
89.186.73.168   [1140] 10:47:14 Client session >>> STARTTLS
89.186.73.168   [1140] 10:47:14 Client session <<< 220 2.0.0 Ready to start TLS
89.186.73.168   [1140] 10:47:14 Client session SSL: Not verified (18) - proceed anyway
89.186.73.168   [1140] 10:47:14 Client session >>> EHLO localhost
89.186.73.168   [1140] 10:47:14 Client session <<< 250 HELP
89.186.73.168   [1140] 10:47:14 Client session >>> MAIL From:<admin@icewarpdemo.com> SIZE=589 TRANSID=<20111005104714004 2@icewarpdemo.com>
89.186.73.168   [1140] 10:47:14 Client session <<< 250 2.1.0 <admin@icewarpdemo.com>... Sender ok
89.186.73.168   [1140] 10:47:14 Client session >>> RCPT To:<test@icewarp.it>
89.186.73.168   [1140] 10:47:14 Client session <<< 250 2.1.5 <test@icewarp.it>... Recipient ok
89.186.73.168   [1140] 10:47:14 Client session >>> DATA
89.186.73.168   [1140] 10:47:14 Client session <<< 354 Enter mail, end with "." on a line by itself
89.186.73.168   [1140] 10:47:14 Client session >>> 589 bytes (overall data transfer speed=293275 B/s)
89.186.73.168   [1140] 10:47:15 Client session <<< 250 2.6.0 589 bytes received in 00:00:00; Message id OSA57912 accepted for delivery
89.186.73.168   [1140] 10:47:15 Client session *** <admin@icewarpdemo.com> <test@icewarp.it> 1 589 00:00:00 OK OSA88513
89.186.73.168   [1140] 10:47:15 Client session >>> QUIT
89.186.73.168   [1140] 10:47:15 Client session <<< 221 2.0.0 mail.fastflow.it closing connection
89.186.73.168   [1140] 10:47:15 Client session Disconnected
```

A fianco di ogni riga della sessione client vi è l'indirizzo del server. Sulla prima riga della sessione è invece indicato l'IP locale dal quale è stata inizializzata la sessione (*local IP*) mentre sulla riga seguente vi è la presentazione del Server di sessione che definisce il protocollo che si intende usare (*ESMTP*).
Seguono il blocco di indirizzamento del messaggio, durante il quale viene assegnato un *TRANSID*, che accompagnerà questo messaggio fino a destinazione, e quello di trasferimento alla fine del quale il server prende in carico il messaggio per la consegna.
Una volta concluso il trasferimento del messaggio viene riportata una riga di riepilogo (***) sulla quale viene anche assegnato un *Message id*.

- Server

```
192.168.26.42  [0EC4] 10:47:13 Connected, local IP=192.168.26.218
192.168.26.42  [0EC4] 10:47:13 >>> 220 localhost ESMTP IceWarp 10.3.4; Wed, 05 Oct 2011 10:47:13 +0200
192.168.26.42  [0EC4] 10:47:13 <<< EHLO icewarpdemo.com [127.0.0.1]
192.168.26.42  [0EC4] 10:47:13 >>> 250-localhost Hello icewarpdemo.com [192.168.26.42], pleased to meet you.
192.168.26.42  [0EC4] 10:47:13 <<< MAIL FROM:<admin@icewarpdemo.com>
192.168.26.42  [0EC4] 10:47:13 >>> 250 2.1.0 <admin@icewarpdemo.com>... Sender ok
192.168.26.42  [0EC4] 10:47:13 <<< RCPT TO:<test@icewarp.it>
192.168.26.42  [0EC4] 10:47:13 >>> 250 2.1.5 <test@icewarp.it>... Recipient ok; will forward
192.168.26.42  [0EC4] 10:47:13 <<< DATA
192.168.26.42  [0EC4] 10:47:13 >>> 354 Enter mail, end with "." on a line by itself
192.168.26.42  [0EC4] 10:47:13 <<< 387 bytes (overall data transfer speed=383859 B/s)
192.168.26.42  [0EC4] 10:47:13 Start of mail processing
192.168.26.42  [0EC4] 10:47:13 *** <admin@icewarpdemo.com> <test@icewarp.it> 1 382 00:00:00 OK OSA88513
192.168.26.42  [0EC4] 10:47:13 >>> 250 2.6.0 382 bytes received in 00:00:00; Message id OSA88513 accepted for delivery
192.168.26.42  [0EC4] 10:47:13 <<< quit
192.168.26.42  [0EC4] 10:47:13 >>> 221 2.0.0 localhost closing connection
192.168.26.42  [0EC4] 10:47:13 Disconnected
```

Come si può notare questa sessione è esattamente lo “specchio” di quella precedentemente riportata.
A fianco di ogni riga della sessione server vi è l'IP a partire dal quale la connessione è stata stabilita. Chiaramente questo indirizzo non corrisponde all'indirizzo locale riportato nella sessione client, dato che tale informazione non è accessibile all'esterno della rete locale.
L'indirizzo IP mostrato a fianco della dicitura *local IP* in questa sessione indica invece l'indirizzo del server.

Procediamo ora analizzando alcune particolari sessioni SMTP che possono risultare di non immediata interpretazione e cerchiamo all'interno di esse una chiave di lettura.

Sessioni incomplete

Se una sessione non viene portata correttamente a termine significa che il trasferimento del messaggio non è avvenuto. Il mancato successo viene in alcuni casi segnalato tramite la dicitura “INCOMPLETE-SESSION” in una riga di riepilogo dopo la quale avviene la disconnessione.
Ci sono numerosi motivi per i quali una sessione può essere incompleta e il motivo risulta nella maggior parte dei casi facilmente determinabile grazie ai messaggi di errore della tipologia 5xx che sono quasi sempre accompagnati da una breve dicitura esplicativa.
Altre volte invece il motivo del fallimento della sessione non è chiaramente specificato e pertanto può essere necessario dedurlo per mezzo di altri elementi e osservando come si svolge la sessione.

Vediamo alcuni esempi:

```
SYSTEM          [1B6C] 12:03:40 Client session Message id WTQ78139 item 20110913120339l673.tm$
SYSTEM          [1B6C] 12:03:40 Client session DNS query 'arrigonovelli.it' 0 (1) [OK - 2]
SYSTEM          [1B6C] 12:03:40 Client session Connecting to 'mx.arrigonovelli.it'
SYSTEM          [1B6C] 12:04:01 Client session Could not connect to 'mx.arrigonovelli.it(62.149.128.72)'
SYSTEM          [1B6C] 12:04:01 Client session *** <user@icewarpdemo.com> <info@arrigonovelli.it> 1 32304 00:00:00 INCOMPLETE-SESSION WTQ78139
SYSTEM          [1B6C] 12:04:01 Client session Disconnected
```

La sessione Client sopra riportata fallisce a causa dell'impossibilità di stabilire la connessione con l'indirizzo IP associato al record MX risultante dalla query DNS.

```
127.0.0.1       [0208] 16:20:47 Connected, local IP=127.0.0.1
127.0.0.1       [0208] 16:20:47 >>> 220 localhost ESMTP IceWarp 10.3.2; Thu, 01 Sep 2011 16:20:47 +0200
127.0.0.1       [0208] 16:20:47 <<< EHLO [127.0.0.1]
127.0.0.1       [0208] 16:20:47 >>> 250-localhost Hello [127.0.0.1] [127.0.0.1], pleased to meet you.
127.0.0.1       [0208] 16:20:47 <<< QUIT
127.0.0.1       [0208] 16:20:47 >>> 221 2.0.0 localhost closing connection
127.0.0.1       [0208] 16:20:47 *** <> <> 0 0 00:00:00 INCOMPLETE-SESSION
127.0.0.1       [0208] 16:20:47 Disconnected
```

Questo estratto mostra invece una sessione nella quale non è stato trasferito alcun messaggio, senza che ciò costituisca un malfunzionamento. Il sistema remoto, infatti, subito dopo aver inizializzato la sessione, l'ha terminata con il comando QUIT, senza dar luogo alle consuete fasi di indirizzamento e di trasferimento dei messaggi. I codici di risposta del server sono tutti di classe 2xx, che indica responsi positivi. L'esito "INCOMPLETE-SESSION", pertanto, non indica necessariamente una situazione di errore.

E' anche possibile che una sessione non venga portata a termine a causa della decisione di una delle due parti coinvolte di abbandonare la comunicazione.
Nel caso mostrato di seguito è il server locale ad abbandonare, a causa della inattività prolungata del sistema remoto:

```
79.38.14.7 [05DC] 18:07:04 Connected, local IP=10.0.0.20
79.38.14.7 [05DC] 18:07:04 >>> 220 smtp.example.it ESMTP IceWarp 10.3.1; Thu, 25 Aug 2011 18:07:04 +0200
79.38.14.7 [05DC] 18:07:04 <<< EHLO localhost
79.38.14.7 [05DC] 18:07:04 >>> 250-smtp.example.it Hello localhost [79.38.14.7], pleased to meet you.
250-ENHANCEDSTATUSCODES
250-SIZE
250-EXPN
250-ETRN
250-ATRN
250-DSN
250-CHECKPOINT
250-8BITMIME
250-AUTH PLAIN LOGIN DIGEST-MD5 CRAM-MD5 GSSAPI
250-STARTTLS
250 H
79.38.14.7 [05DC] 18:07:04 <<< MAIL FROM:<admin@icewarpdemo.com> SIZE=19687
79.38.14.7 [05DC] 18:07:04 >>> 250 2.1.0 <admin@icewarpdemo.com>... Sender ok
79.38.14.7 [05DC] 18:07:04 <<< RCPT TO:<test@example.it>
79.38.14.7 [05DC] 18:07:04 >>> 250 2.1.5 <test@example.it>... Recipient ok
79.38.14.7 [05DC] 18:07:04 <<< DATA
79.38.14.7 [05DC] 18:07:04 >>> 354 Enter mail, end with "." on a line by itself
79.38.14.7 [05DC] 18:12:09 <<< 2736 bytes (overall data transfer speed=9 B/s)
79.38.14.7 [05DC] 18:12:09 *** <admin@icewarpdemo.com> <test@example.it> 1 0 00:00:00 TIMEOUT IYG80904
79.38.14.7 [05DC] 18:12:09 Disconnected
```

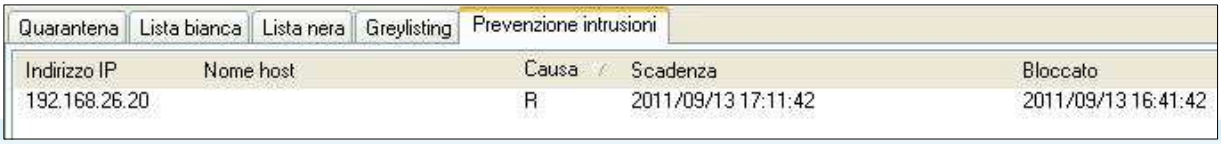
La sessione fallisce per timeout della connessione. Come è facile notare, il tempo che intercorre tra l'inizio del trasferimento ed il TIMEOUT è esattamente di 5 minuti, il che fornisce una chiara indicazione sulle impostazioni del server.
Di default l'impostazione del tempo di inattività dopo il quale le sessioni SMTP devono andare in timeout è infatti di 300 secondi (5 minuti). Tale impostazione è contenuta nella variabile *c_system_adv_protocols_sessiontimeout* accessibile da console API.

Ci sono poi situazioni nelle quali qualcosa interviene a bloccare la sessione. Può essere ad esempio il caso del sistema di *Prevenzione intrusioni* delle varie modalità di controllo che esso implica.

Di seguito un esempio:

```
192.168.26.20   [135C] 16:41:28 >>> 250 2.0.0 Reset state
192.168.26.20   [135C] 16:41:30 <<< rset
192.168.26.20   [135C] 16:41:30 >>> 250 2.0.0 Reset state
192.168.26.20   [135C] 16:41:32 <<< rset
192.168.26.20   [135C] 16:41:32 >>> 250 2.0.0 Reset state
192.168.26.20   [135C] 16:41:34 <<< rset
192.168.26.20   [135C] 16:41:34 >>> 250 2.0.0 Reset state
192.168.26.20   [135C] 16:41:36 <<< rset
192.168.26.20   [135C] 16:41:36 >>> 250 2.0.0 Reset state
192.168.26.20   [135C] 16:41:42 <<< rset
192.168.26.20   [135C] 16:41:42 >>> 250 2.0.0 Reset state
192.168.26.20   [135C] 16:42:00 <<< mail from:<user@icewarpdemo.com>
192.168.26.20   [135C] 16:42:00 >>> 250 2.1.0 <user@icewarpdemo.com>... Sender ok
192.168.26.20   [135C] 16:42:12 <<< rcpt to:<admin@icewarpdemo.com>
192.168.26.20   [135C] 16:42:12 >>> 250 2.1.5 <admin@icewarpdemo.com>... Recipient ok
192.168.26.20   [135C] 16:42:15 <<< data
192.168.26.20   [135C] 16:42:15 >>> 354 Enter mail, end with "." on a line by itself
192.168.26.20   [135C] 16:42:27 <<< 26 bytes (overall data transfer speed=2 B/s)
192.168.26.20   [135C] 16:42:27 Start of mail processing
192.168.26.20   [135C] 16:42:28 *** <user@icewarpdemo.com> <admin@icewarpdemo.com> 1 21 00:00:12 OK WXD75015
192.168.26.20   [135C] 16:42:28 >>> 250 2.6.0 21 bytes received in 00:00:12; Message id WXD75015 accepted for delivery
192.168.26.20   [135C] 16:42:30 <<< quit
192.168.26.20   [135C] 16:42:30 >>> 221 2.0.0 localhost closing connection
192.168.26.20   [135C] 16:42:30 Disconnected
192.168.26.20   [135C] 16:42:32 Connected, local IP=192.168.26.20
192.168.26.20   [135C] 16:42:32 >>> 421 4.7.1 Intrusion prevention active for [192.168.26.20][R]
192.168.26.20   [135C] 16:42:32 *** <> <> 0 0 00:00:00 INCOMPLETE-SESSION
192.168.26.20   [135C] 16:42:32 Disconnected
```

In questo caso la prevenzione intrusioni è stata attivata da una sessione all'interno della quale è stato inviato 6 volte il comando RSET. La sessione si conclude correttamente con il trasferimento del messaggio ma al tentativo di apertura di una nuova sessione SMTP a partire dallo stesso IP viene notificato l'errore 421 e la specifica ragione per cui il sistema di Prevenzione intrusioni è entrato in funzione (*R: "exceeding RSET command count"*).
La presenza dell'IP nella lista di quelli bloccati è verificabile al percorso [Stato > Code spam > Prevenzione intrusioni].



Mancata ricezione causa Antispam

```
'<user@icewarpdemo.com>' '<user2@icewarpdemo.com>' 1 score 2,01 reason [SpamAssassin=1,01,Other=1,00:Body=R,Live=N] action NONE
'<user2@icewarpdemo.com>' '<user3@icewarpdemo.com>' 1 score 2,01 reason [SpamAssassin=1,01,Other=1,00:Body=R,Live=N] action NONE
'<user@icewarpdemo.com>' '<user4@icewarpdemo.com>' 1 score 1,90 reason [SpamAssassin=0,90,Other=1,00:Body=R,Live=N] action NONE
'<test@icewarp.it>' '<user@icewarpdemo.com>' 1 score 7,81 reason [SpamAssassin=5,31,Other=2,50:Body=PR] action SPAM
```

Nel log Antispam è possibile verificare come ciascun messaggio che transiti sul server venga esaminato dal motore Antispam e classificato a seconda del punteggio assegnatogli dalle varie procedure di controllo.
In corrispondenza di ogni messaggio viene quindi mostrato il punteggio da esso raggiunto e la conseguente azione intrapresa dal sistema (NONE, REJECT, DELETE, SPAM, QUARANTINE).

L'azione intrapresa conseguentemente all'assegnazione di punteggio può quindi portare anche a provvedimenti drastici, quali l'eliminazione del messaggio o il respingimento della sessione.

La riga evidenziata nell'estratto precedentemente riportato si riferisce ad un messaggio classificato come SPAM. Tale classificazione è dovuta a tre assegnazioni di punteggio che concorrono al raggiungimento di 7,81. Le tre componenti sono:

- SpamAssassin: software che fa uso di un insieme complesso di regole attivabili/disattivabili da interfaccia di amministrazione;
- Other: somma dei punteggi assegnati dalle regole della sezione [Antispam > Varie];
- Body: Codici definiti nella documentazione del software (P: parti testo e html non corrispondenti, R: consegna diretta, nessun server intermediario);
- Live: Antispam Live.

Procediamo esaminando un altro esempio:

```
[0C50] 16:22:58 Connected, local IP=192.168.26.20
[0C50] 16:22:58 >>> 220 localhost ESMTP IceWarp 10.3.3 (2011-09-14); Thu, 15 Sep 2011 16:22:58 +0200
[0C50] 16:23:00 <<< ehlo test
[0C50] 16:23:00 >>> 250-localhost Hello test [192.168.26.20], pleased to meet you.
[0C50] 16:23:07 <<< mail from:<user@icewarpdemo.com>
[0C50] 16:23:07 >>> 250 2.1.0 <user@icewarpdemo.com>... Sender ok
[0C50] 16:23:17 <<< rcpt to:<user2@icewarpdemo.com>
[0C50] 16:23:17 >>> 250 2.1.5 <user2@icewarpdemo.com>... Recipient ok
[0C50] 16:23:21 <<< data
[0C50] 16:23:21 >>> 354 Enter mail, end with "." on a line by itself
[0C50] 16:23:25 <<< 11 bytes (overall data transfer speed=3 B/s)
[0C50] 16:23:25 Start of mail processing
[0C50] 16:23:25 Message for <user2@icewarpdemo.com> not delivered. Reasons:[SpamAssassin=2,01,Other=2,00:Body=BR,ContentFilter=Missing headers], Action:DELETE
[0C50] 16:23:26 *** <user@icewarpdemo.com> <user2@icewarpdemo.com> 1 6 00:00:04 OK YXM31221
[0C50] 16:23:26 >>> 250 2.6.0 6 bytes received in 00:00:04; Message id YXM31221 accepted for delivery
[0C50] 16:23:27 <<< quit
[0C50] 16:23:27 >>> 221 2.0.0 localhost closing connection
[0C50] 16:23:27 Disconnected
```

L'estratto si riferisce ad una sessione di invio di un messaggio che causa l'intervento di un filtro [Posta > Filtri > Filtri sul contenuto].
In questo caso il messaggio viene quindi consegnato come viene appunto confermato nel log (“*accepted for delivery*”) ma unitamente alla sua consegna ne viene disposta la cancellazione e ciò viene segnalato nella stessa sessione SMTP assieme alle ragioni che hanno comportato un'attribuzione di punteggio e al nome del filtro che ha causato l'intervenuto.

Di seguito riportiamo invece una sessione che si riferisce ad un messaggio respinto:

```
192.168.26.20   [1120] 11:48:30 Connected, local IP=192.168.26.20
192.168.26.20   [1120] 11:48:30 >>> 220 localhost ESMTP IceWarp 10.3.3 (2011-09-14); Fri, 16 Sep 2011 11:48:30 +0200
192.168.26.20   [1120] 11:48:30 <<< HELO smtp.test.com
192.168.26.20   [1120] 11:48:30 >>> 250 localhost Hello smtp.test.com [192.168.26.20], pleased to meet you.
192.168.26.20   [1120] 11:48:30 <<< MAIL From:test@icewarp.it
192.168.26.20   [1120] 11:48:30 >>> 250 2.1.0 <test@icewarp.it>... Sender ok
192.168.26.20   [1120] 11:48:30 <<< RCPT To:user@icewarpdemo.com
192.168.26.20   [1120] 11:48:30 >>> 250 2.1.5 <user@icewarpdemo.com>... Recipient ok
192.168.26.20   [1120] 11:48:30 <<< DATA
192.168.26.20   [1120] 11:48:30 >>> 354 Enter mail, end with "." on a line by itself
192.168.26.20   [1120] 11:48:30 <<< 475 bytes (overall data transfer speed=54976852 B/s)
192.168.26.20   [1120] 11:48:30 Start of mail processing
192.168.26.20   [1120] 11:48:31 Message for <user@icewarpdemo.com> not delivered. Reasons:[SpamAssassin=5,31,Other=2,50:Body=PR], Action:REJECT
192.168.26.20   [1120] 11:48:31 *** <test@icewarp.it> <user@icewarpdemo.com> 1 470 00:00:01 SPAM ZSM28130
192.168.26.20   [1120] 11:48:31 >>> 554 5.7.1 Message cannot be accepted, spam rejection
192.168.26.20   [1120] 11:48:32 Disconnected
```

Anche in questo caso la sessione contiene direttamente il riferimento alle attribuzioni di punteggio ma, diversamente da quanto accade nell'esempio precedente, il messaggio non viene preso in consegna.