Protocollo SMTP

Introduzione

Simple Mail Transfer Protocol (SMTP) is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred. It is a client-server protocol, where the client transmits an email message to the server. Either an end-user's email client, a.k.a. MUA (Mail User Agent), or a relaying server's MTA (Mail Transfer Agents) can act as an SMTP client.

An email client knows the outgoing mail SMTP server from its configuration. A relaying server typically determines which SMTP server to connect to by looking up the MX (Mail eXchange) DNS record for each recipient's domain name, the part of the email address to the right of the at sign (@). Conformant MTAs (not all) fall back to a simple A record in the case of no MX. Some current mail transfer agents will also use SRV records, a more general form of MX, though these are not widely adopted. (Relaying servers can also be configured to use a smart host.)

The SMTP client initiates a TCP connection to server's port 25 (unless overridden by configuration.) It is quite easy to test an SMTP server using the telnet program.

SMTP is a "push" protocol that does not allow one to "pull" messages from a remote server on demand. To do this a mail client must use POP3 or IMAP. Another SMTP server can trigger a delivery in SMTP using ETRN.

SMTP is the de facto standard for e-mail transmission across the Internet. Formally SMTP is defined in RFC 821 (STD 10) as amended by RFC 1123 (STD 3) chapter 5. The protocol used today is also known as ESMTP and defined in RFC 2821.

Fonte: Wikipedia - http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Utilizzo

Il protocollo client/server per l'invio della posta elettronica richiede che vi sia un software client (che permette all'utente di redigere una messaggio di posta elettronica, specificando mittente, destinatario, oggetto, contenuto, eventuali allegati etc.) e un software server in grado di recepire il messaggio da parte di un mittente e di consegnarlo al server che gestisce la casella di posta (*mailbox*) del/dei destinatario/i.

In genere, i fornitori di connettività provvedono anche a fornire l'accesso a un server SMTP per permettere ai propri clienti (e solo a quelli) di inviare posta elettronica; chi possiede un collegamento modem o ADSL casalingo, oltre ai normali parametri per configurare la connessione, ha ricevuto dal proprio fornitore di connettività anche l'indicazione del server SMTP da utilizzare per l'invio della posta. Per un uso professionale di tale servizio, ad esempio per enti e aziende, si preferisce adottare servizi dedicati in *outsourcing* oppure si provvede all'installazione e alla configurazione di un server interno dedicato all'invio della posta (tipicamente installato in DMZ).

Nell'esperienza di laboratorio il server SMTP per l'invio della posta è il PC del docente, identificato da un indirizzo IP e dall'equivalente nome host (*nota: chiedere la docente questi dati*). Tale server è configurato per operare il cosiddetto "*relay*" della posta senza operare restrizioni in base a un ben

determinato dominio Internet di gestione. Tale pratica è vivamente sconsigliata nell'utilizzo reale ma necessaria per effettuare le esercitazioni di laboratorio.

Per poter capire il funzionamento del protocollo SMTP si effettuerà un invio di e-mail "manuale" (utilizzando una connessione diretta alla porta TCP/25 del server) e un invio tramite client dedicato. Per ogni esercizio si richiede la cattura e l'analisi del traffico generato tramite Wireshark.

Nota

Per poter verificare il corretto invio del messaggio e-mail è necessario possedere un indirizzo e-mail reale al quale poter accedere per visionare il messaggio di posta inviato (meglio se accessibile anche direttamente via POP3 e non solo tramite webmail...). Nel caso non si abbia un indirizzo da poter utilizzare è possibile chiedere al docente l'attivazione momentanea di un indirizzo e-mail su un dominio di servizio ("tennici.it").

Il protocollo SMTP prevede che l'invio del messaggio di posta avvenga a partire da una fase di presentazione per proseguire poi con una serie di invii di informazioni tra il client (che utilizza gli appositi comandi del protocollo) e il server (che notifica l'avvenuta ricezione o l'eventuale errore riscontrato); la comunicazione avviene quindi in modalità "testuale" e utilizza i seguenti comandi (non sono riportati tutti i comandi; si rimanda al comando "HELP" e alle relative RFC):

SMTP Commands:	
HELO *sendinghostname*	This command initiates the SMTP conversation. The host connecting to the remote SMTP server identifies itself by it's fully qualified DNS host name.
EHLO *sendinghostname*	An alternative command for starting the conversation. This states that the sending server wants to use the extended SMTP (ESMTP) protocol.
MAIL From: <*source email address*>	This is the start of an email message. The source email address is what will appear in the "From:" field of the message.
RCPT To: <*destination email address*>	This identifies the receipient of the email message. This command can be repeated multiple times for a given message in order to deliver a single message to multiple receipients.
SIZE=*numberofbytes*	The size command tells the remote sendmail system the size of the attached message in bytes. If ommited, mail readers and delivery agents will try to determine the size of a message based on indicators such as them being terminated by a "." on a line by themselves and headers being sent on a line separated from body text by a blank line. But these methods get confused when you have headers or header like information embedded in messages, attachements, etc.
DATA	This command signifies that a stream of data, ie the email message body, will follow. The stream of data is terminated by a "." on a line by itself.
QUIT	This terminates an SMTP connection. Multiple email messages can be transfered during a single TCP/IP connection. This allows for more efficient transfer of email. To start another email message in the same session, simply issue another "MAIL" command.
VRFY *username*	This command will request that the receiving SMTP server verify that a given email username is valid. The SMTP server will reply with the login name of the user. This feature can be turned off in sendmail because allowing it can be a security hole. VRFY commands can be used to probe for login names on a system. See the security section below for information about turning off this feature.
EXPN *aliasname*	EXPN is similar to VRFY, except that when used with a distribution list, it will list all users on that list. This can be a bigger problem than the

	"VRFY" command since sites often have an alias such as "all".
Subject: Cc: Reply-To:	Email header lines are not SMTP commands per se. They are sent in the DATA stream for a message. Header lines appear on a line by themselves, and are separated from the body of a message by a blank line.

L'instaurazione della comunicazione è riportata in Figura 1.

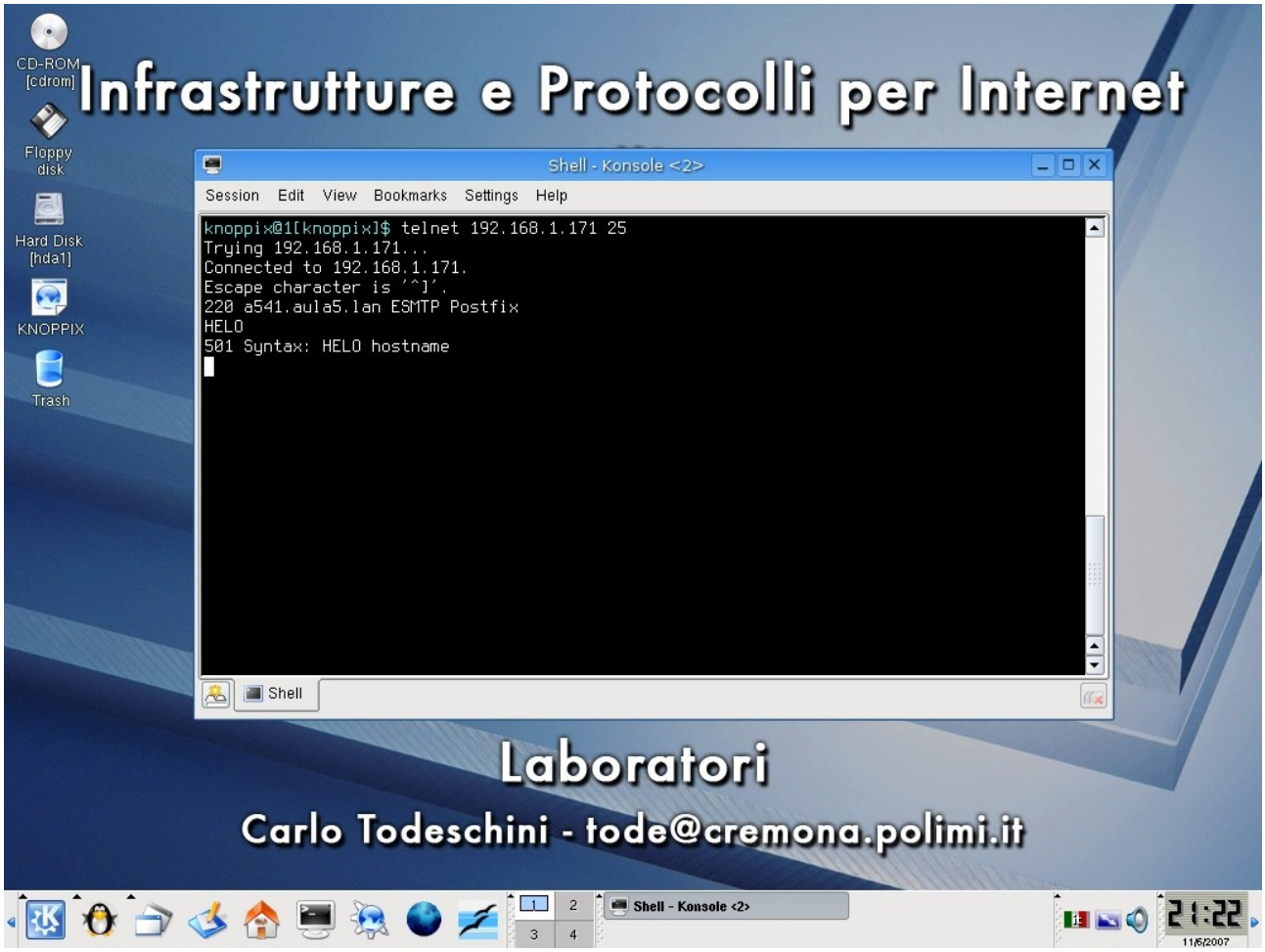

Fig. 1: esempio di inizio di una sessione di telnet con utilizzo del protocollo SMTP

Quindi, per simulare una connessione SMTP è necessario instaurare la seguente sessione “telnet” sulla porta 25: in neretto è riportato l'input che va dato simulando la parte client.
Si consiglia di inviare un messaggio e-mail ad un proprio account esistente e attivo, dal quale si possa poi, tramite webmail, controllarne l'avvenuta ricezione.

`# telnet a541.aula5.lan 25`
`Trying 192.168.1.171...`
`Connected to 192.168. 1.171.`
`Escape character is '^]'.`
`220 a541.aula5.lan ESMTP Postfix`
	Tramite il programma telnet viene contattato il server SMTP sulla porta TCP/25
	E' possibile notare dal messaggio la keyword ESMTP che indica che il server supporta le SMTP Service Extensions

`HELO polimi.it` `250 a541.aula5.lan`	*Il client si identifica tramite il comando helo (sostituire polimi.it*

	con il proprio)
MAIL FROM: tode@cremona.polimi.it 250 2.1.0 Ok	*E' necessario specificare un indirizzo e-mail che abbia un dominio reale altrimenti il server rifiuta il dato. Impostare, ad esempio, il proprio indirizzo e-mail*
RCPT TO: tode@tennici.it 250 2.1.5 Ok	*E' necessario specificare un indirizzo e-mail di destinazione; ad esempio utilizzare l'indirizzo di un collega*
DATA 354 End data with <CR><LF>.<CR><LF>	*Con il comando DATA inizia l'inserimento del corpo della mail*
From: "Carlo Todeschini – Poli" <tode@cremona.polimi.it> **To: "Carlo Todeschini – Tennici" <tode@tennici.it>** **Subject: Prova di invio** **Questo e' un test di invio di una e-mail tramite protocollo SMTP.** **Ciao,** **tode** **.**	*Ogni parametro dati che compone l'e-mail va scritto su un'unica riga, terminandola con un "a capo". Il comando "." (punto), seguita da un " a capo", termina l'inserimento del messaggio*
250 2.0.0 Ok: queued as XXXXXXXXXXXX	*Il server SMTP accetta il messaggio per il delivery*
QUIT 221 2.2.0 Bye	*La connessione TCP termina e si ritorna al prompt*

A questo punto è necessario accedere, tramite il proprio programma di posta oppure l'applicazione webmail, alla propria mailbox per leggere il messaggio arrivato. Nota: la ricezione del messaggio nella mailbox di destinazione può richiedere tempo oppure può essere scartata dal server di destinazione in quanto considerata SPAM.

Esercizio 1

Eseguire la connessione indicata sopra e catturare il traffico con Wireshark. Verificare che la comunicazione è effettivamente riconosciuta come "traffico SMTP".

Ora è possibile impostare un programma client per l'invio/ricezione della posta tra quelli a disposizione in Knoppix. Ad esempio, è possibile configurare "KMail" (come mostrato in figura 2) specificando la propria identità (menu "Settings >> Configure KMail >> Identities"), facendo attenzione a configurare un indirizzo e-mail esistente, e il server di posta in uscita (menu "Settings >> Configure KMail >> Accounts >> Sending"; per questo occorre cancellare il server esistente e crearne uno nuovo, di tipo SMTP, con i dati già a conoscenza).

- Tipo di server di posta in ingresso: POP3 (v. prossima scheda)
- Indirizzo e-mail: il proprio indirizzo e-mail reale o l'indirizzo appositamente creato dal docente sul server
- Server posta in uscita: <NOME MACCHINA DOCENTE> (senza opzione SSL)
- Server posta in entrata: <NOME MACCHINA DOCENTE> (senza opzione SSL)

Nota: potrà richiedersi una ulteriore configurazione per disabilitare il supporto all'SSL

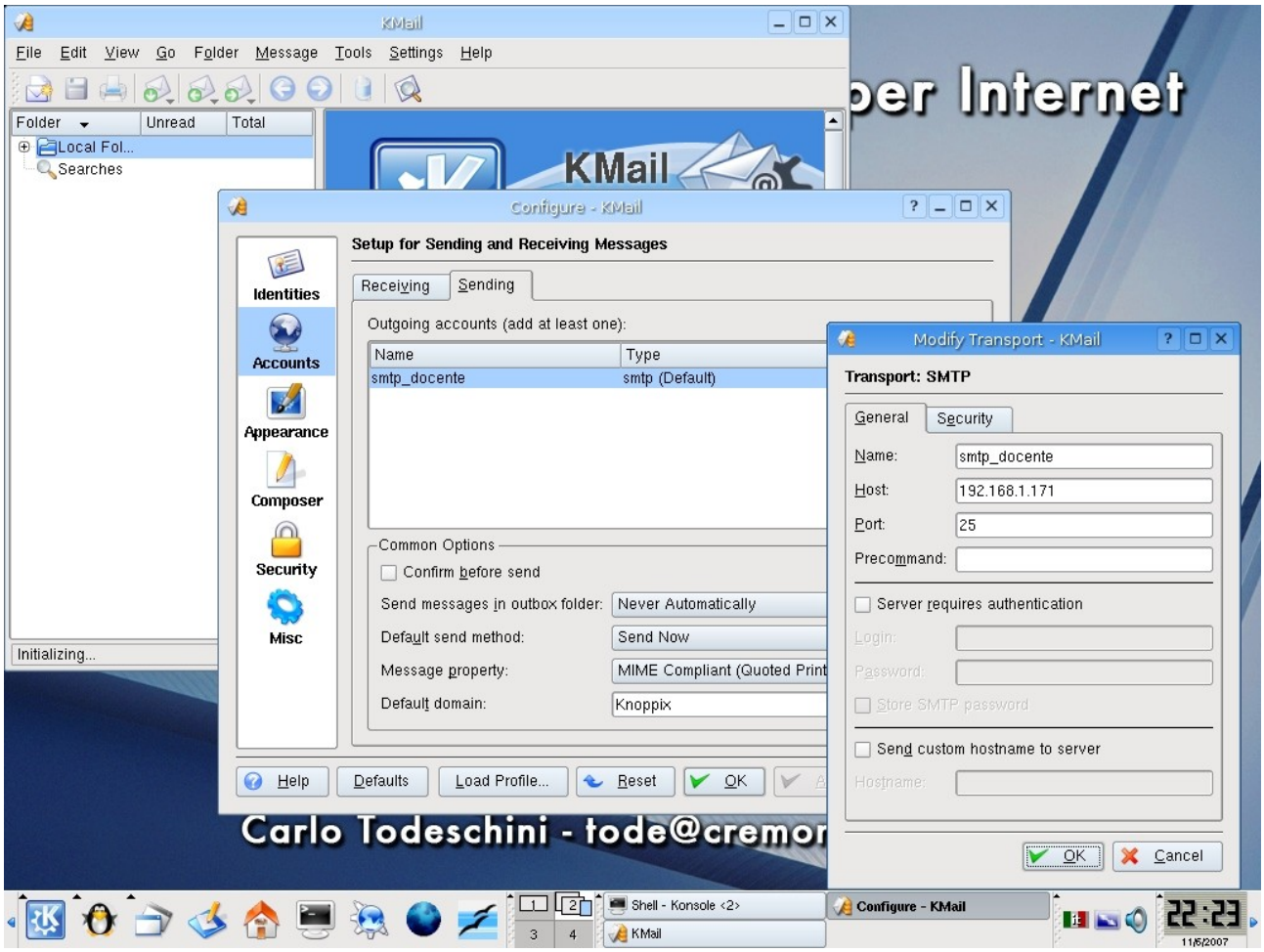

Fig. 2: utilizzo di KMail

Nota: configurare Wireshark per sniffare su tutte le interfacce e non solo su eth0.

Esercizio 2

Eseguire un invio di e-mail con il programma KMail (o equivalente).
Come varia il traffico catturato con Wireshark?

Esercizio 3

Eseguire un invio di e-mail con il programma KMail (o equivalente) inserendo un allegato nel testo della e-mail.
Come varia il traffico catturato con Wireshark?
Come viene gestito l'invio dell'allegato?

Nota

La parte che segue è facoltativa.

Sul Knoppix dei laboratori è già installato un server SMTP: Smail-3. Si consiglia di sostituirlo con il server "Postfix" (scaricabile dal sito del docente nella pagina dedicata "Pacchetti .deb di supporto"; salvare il pacchetto "postfix*" nella dir "/tmp/") con i seguenti comandi:

```
# apt-get remove smail
[...]
# dpkg -i /tmp/postfix_2.5.2-2_i386.deb
[...]
```

Durante la fase di installazione che segue al lancio di questo comando verranno richieste alcune configurazioni: scegliere sempre le opzioni di default proposte.

Al termine è necessario verificare che il demone sia attivo, utilizzando i comandi "nmap" oppure "netstat", sulla porta 25/TCP, dedicata al protocollo. A questo punto il server è in attesa di connessioni da parte di client remoti; con la semplice configurazione adottata, il server è in grado di accettare messaggi e-mail da altri server di posta indirizzati ai propri utenti locali.

Si può quindi procedere alla creazione di ulteriori utenti dotati di mailbox sulla macchina server in uso con il comando:

```
# adduser <NOME UTENTE>
[...]
```

A seguito del comando appena impartito verranno richiesti alcuni parametri per la configurazione dell'account, compresa la password di autenticazione. A questo punto è possibile inviare una e-mail, a uno degli utenti appena creati, dalla propria macchina oppure inviare un messaggio a uno degli utenti che un collega ha creato sulla sua macchina, connettendosi direttamente al server SMTP che questo ha attivato e configurato.

Per simulare una connessione SMTP è necessario instaurare la seguente sessione "telnet" sulla porta 25. Il server utilizzato non effettua "*relay*" per cui è possibile inviare messaggi e-mail indirizzati solo agli utenti locali del "server".

```
# telnet a5xx.aula5.lan 25

Trying 192.168.xxx.xxx...
Connected to 192.168.xxx.xxx (192.168.xxx.xxx).
Escape character is '^]'.
220-Knoppix Smail-3.2.0.115 (#2 2005-Mar-28)
220-ready at Wed, 7 Jun 2006 23:22:37 +0200 (CEST)
220 ESMTP supported
```

Tramite il programma telnet viene contattato il server SMTP sulla porta TCP 25
E' possibile notare dal messaggio ESMTP Service che il server supporta le SMTP Service Extensions

```
HELO a5xx.aula5.lan
250 Knoppix Hello a5xx.aula5.lan (yyy.yyy.yyy from address
[192.168.xxx.xxx]).
```

Il client si identifica tramite il comando helo

```
MAIL FROM: tode@cremona.polimi.it
250 2.1.0 tode@cremona.polimi.it Sender Okay.
NOTA: è necessario specificare un indirizzo e-mail che abbia un dominio reale altrimenti il server rifiuta il dato

RCPT TO: utente
250 2.1.0 'utente' Recipient Okay.
NOTA: sostituire a 'utente' uno degli utenti creati sulla macchina su  cui gir il server SMTP.

DATA
Inizia l'inserimento del corpo della mail (NOTA: non lasciare spazi tra il campo e il valore)
354 Enter mail, end with "." on a line by itself...

From:Carlo Todeschini
To:Root di Knoppix
Subject:Prova di invio

Questo e' un test di invio di una e-mail tramite
protocollo SMTP.

Ciao,
tode
.
250 2.6.0 Mail accepted, queue ID m1Fo5VV-00017NC on Knoppix.
Il comando "." punto termina l'inserimento del messaggio; Il server SMTP lo accetta

QUIT
221 2.2.0 Knoppix closing connection
Connection closed by foreign host.
La connessione TCP termina e si ritorna al prompt
#
```

E' possibile verificare che il *delivery* delle e-mail è avvenuto senza problemi visualizzando il contenuto del file "`/var/spool/mail/<UTENTE>`"; in questa directory vengono memorizzate le *mailbox* relative a tutti gli *account* memorizzati sul server; si tratta di file di testo che riportano, in un unico file, tutte le e-mail ricevute per un dato account.

Esercizio 4 ***(facoltativo)***

Coordinarsi con un collega e testare l'invio di messaggi e-mail utilizzando il server SMTP installato sulla macchina del collega.

Approfondimenti

- *RFC 2821 - Simple Mail Transfer Protocol*: ftp://ftp.rfc-editor.org/in-notes/rfc2821.txt