

RFC1939 - Protocollo POP - ver. 3

Indice

| | |
|--------------------------------------------------------------------------------------------------------------------------------|----|
| RFC1939 - Protocollo POP - ver. 3..... | 1 |
| Stato di questo Documento..... | 2 |
| Introduzione | 2 |
| Una breve digressione..... | 2 |
| Funzionamento di base | 2 |
| Stato di AUTORIZZAZIONE ("Authorization")..... | 4 |
| QUIT | 5 |
| Stato di TRANSAZIONE ("Transaction") | 5 |
| STAT..... | 5 |
| LIST [msg]..... | 6 |
| RETR msg | 7 |
| DELE msg..... | 7 |
| NOOP | 8 |
| RSET | 8 |
| Stato di AGGIORNAMENTO ("Update")..... | 8 |
| QUIT | 8 |
| Comandi POP3 Opzionali..... | 9 |
| TOP msg n..... | 9 |
| UIDL [msg]..... | 10 |
| USER name..... | 11 |
| PASS string | 11 |
| APOP name digest..... | 12 |
| Considerazioni Operative..... | 13 |
| Riassunto dei comandi POP3..... | 14 |
| Esempio di una sessione POP3..... | 15 |
| Formato dei Messaggi | 16 |
| Riferimenti | 16 |
| Considerazioni sulla Sicurezza | 16 |
| Riconoscimenti | 17 |
| Indirizzi degli Autori | 17 |
| Differenze rispetto alla RFC 1725..... | 17 |
| Appendice A : The MD5 Message-Digest Algorithm..... | 18 |
| Executive Summary | 18 |
| Appendice B : CODICE ASCII (American Standard Code for Information Interchange) . Errore. Il segnalibro non è definito. | |
| <i>Caratteri di controllo del codice ASCII.....</i> Errore. Il segnalibro non è definito. | |
| <i>Significato dei caratteri di controllo del codice ASCII.....</i> Errore. Il segnalibro non è definito. | |

Traduzione dal documento originale in lingua Inglese :

RFC1939 Myers & Rose Standards Track POP3 - May 1996

curata dal prof.: Cleto Azzani IPSIA "Moretto" BRESCIA (Giugno 2002)

Stato di questo Documento

Questo documento specifica una traccia di protocollo standard nel mondo Internet, e richiede osservazioni, proposte o suggerimenti per il suo miglioramento. Per favore ci si riferisca all'edizione corrente di "Internet Official Protocol Standards" (STD 1) per lo stato di standardizzazione di questo protocollo. Non esistono vincoli alla distribuzione di questo documento.

Introduzione

Sui più piccoli nodi nel mondo Internet spesso non è conveniente e nemmeno possibile mantenere un sistema di gestione dei messaggi (MTS). Per esempio, una workstation può non avere risorse sufficienti (velocità del processore, spazio su disco limitato) per permettersi un servizio SMTP [RFC821] e il relativo sistema di consegna della posta locale residente e in funzione 24 ore al giorno.

Analogamente, può essere costoso (o impossibile) mantenere un PC interconnesso ad una rete con protocollo IP per lungo tempo (il nodo spreca risorse note come la "connettività").

Nonostante questo, è spesso molto utile essere in grado di manipolare posta su questi piccoli nodi, e supportare uno "user agent" (UA) cui siano affidati i compiti di "mail handling". Per risolvere questo problema, un nodo che può supportare MTS offre un servizio di maildrop a nodi meno dotati. Il Protocollo POP3 (Post Office Protocol)- ver. 3 permette ad una workstation di accedere dinamicamente a una maildrop su un sistema di servizio host in modo semplice. Di solito, questo vuole dire che il protocollo POP3 è usato per permettere ad una workstation di recuperare la posta che il server ha temporaneamente in deposito.

POP3 non è dedicato ad eseguire operazioni di manipolazione complessa della posta sul server; normalmente, la posta è scaricata e poi è cancellata. Un più avanzato (e complesso) protocollo, IMAP4 è discusso nel documento [RFC1730].

Per la rimanente parte di questo promemoria, il termine "client-host" o più brevemente "client" si riferisce ad un PC che si avvale del servizio POP3, mentre il termine "server host" o più brevemente "server" si riferisce ad un PC che fornisce il servizio POP3.

Una breve digressione

Questo promemoria non specifica come un "client" possa trasferire messaggi all'interno del sistema di posta, anche se un metodo coerente con la filosofia di questo promemoria è presentato qui di seguito:

Quando lo "user agent" (UA) su un "client" desidera introdurre un messaggio nel sistema di trasporto, stabilisce una connessione SMTP con il suo "host relay" e gli invia tutta la posta. Questo "host relay" può essere, ma non è necessario che sia, il POP3 server. Naturalmente, "host relay" deve accettare posta per consegnarla a destinatari arbitrari, funzionalità non richiesta a tutti i server SMTP.

Funzionamento di base

Inizialmente, il "server" POP3 si pone in ascolto sulla porta TCP 110. Quando un "client" desidera avvalersi del servizio, stabilisce una connessione TCP con il "server" POP3. Non appena il collegamento è stabilito, il server POP3 spedisce un messaggio di saluto. Il client ed il server POP3 scambiano poi comandi e risposte (rispettivamente) finché il collegamento o viene chiuso oppure viene interrotto.

1. I Comandi nel protocollo POP3 sono costituiti da una parola chiave (case-insensitive), eventualmente seguita da da uno o più argomenti.
2. Tutti i comandi terminano con la coppia CRLF (CR Carriage Return #13; LF Line Feed #10).
3. Le Parole-chiave e gli argomenti sono costituiti da caratteri ASCII stampabili.
4. Le Parole chiave e gli argomenti sono separati da un unico carattere SPACE.
5. Le Parole chiave sono lunghe tre o quattro caratteri. Ciascun argomento può essere lungo fino a 40 caratteri.
6. Le risposte nel protocollo POP3 sono costituite da un "indicatore di stato" ed una parola chiave possibilmente seguite da informazioni supplementari.
7. Tutte le risposte si chiudono con la coppia di caratteri ASCII CRLF.
8. Le Risposte possono essere costituite da un massimo di 512 caratteri compresa la coppia CRLF che termina. Sono definiti per ora indicatori di stato:
 - a. positivo (+OK ")
 - b. negativo ("-ERR").
9. Il "server" deve spedire i messaggi di risposta "+OK " e "-ERR" in lettere maiuscole.

Le risposte ad alcuni comandi sono di tipo multi-linea. In questi casi, indicati in dettaglio nella parte che segue, dopo avere spedito la prima linea della risposta ed un CRLF, vengono spedite altre linee supplementari ognuna terminante con la coppia CRLF. Quando tutte le linee della risposta sono state spedite, viene spedita una linea finale o conclusiva costituita da un "byte" terminale (codice decimale 046, ".") e dalla coppia CRLF. Se una linea della risposta multi-linea inizia con il byte terminale, in quella linea viene inserita una coppia CRLF prima del byte terminale.

Dal lato client in caso di risposta multi-linea, il client verifica se la linea inizia con il byte terminale; in tal caso e se i bytes seguenti sono diversi dalla coppia CRLF, il primo byte (quello terminale) viene rimosso. Nel caso in cui i bytes seguenti siano appunto la coppia CRLF, allora la risposta dal POP server è terminata e la linea che contiene ".CRLF" non è considerata parte della risposta multi-linea.

Una sessione POP3 avanza attraverso un numero di stati durante suo periodo di vita. Una volta che il collegamento TCP è stato aperto ed il server POP3 ha spedito il saluto, la sessione entra nello stato di AUTORIZZAZIONE. In questo stato, il client deve farsi riconoscere dal server POP3. Una volta che il client ha superato questa fase, il server acquisisce le risorse associate al maildrop del client, e la sessione entra nello stato di TRANSAZIONE. In questo stato, il client richiede azioni da parte del server POP3. Quando il client ha inoltrato al server il comando QUIT, la sessione entra nello stato di AGGIORNAMENTO. In questo stato, il server POP3 rilascia alcune risorse acquisite durante lo stato TRANSAZIONE e risponde "goodbye". La connessione TCP viene definitivamente chiusa.

Un server deve essere in grado di rispondere ad un comando non riconosciuto, ad un comando non ancora implementato oppure a un comando sintatticamente non valido rispondendo con un indicatore di stato negativo.

Un server deve essere in grado di rispondere ad un comando fornito quando la sessione è in uno stato non corretto rispondendo con un indicatore di stato negativo

Non c'è nessun metodo generale per un client, di distinguere tra un server su cui non è stato implementato un comando opzionale ed un server che non è in grado o è impossibilitato ad elaborare il comando.

Un server POP3 può essere dotato di un sistema di “autologout a tempo” nel caso in cui perduri uno stato di inattività da parte di una connessione. Tale temporizzatore deve avere almeno una durata di 10 minuti.

Il ricevimento di un qualsiasi comando dal client durante l'intervallo deve riassetare il conteggio del tempo di autologout per inattività.

Quando il tempo scade, la sessione non entra nello stato di AGGIORNAMENTO il server DEVE chiudere il collegamento TCP senza rimuovere alcun messaggio e senza spedire alcuna risposta al client.

Stato di AUTORIZZAZIONE (“Authorization”)

Una volta che il collegamento TCP è stato aperto da un client POP3, il server POP3 invia una linea di benvenuto al client. Questa può essere una qualunque risposta positiva. Un esempio potrebbe essere :

S: +OK POP3 server ready

La sessione POP3 ora è nello stato di AUTORIZZAZIONE. Il client deve ora identificarsi presso il server POP3. Due metodi di autenticazione verranno descritti più avanti in questo documento: la combinazione dei comandi USER e PASS e il comando APOP. Altri metodi di autenticazione sono descritti nel documento [RFC1734]. Mentre non esiste un unico e solo meccanismo per autenticarsi, è evidente che un server POP3 deve supportare almeno un meccanismo di autenticazione.

Una volta che il server POP3 ha determinato, attraverso l'uso di uno dei metodi di autenticazione descritti, che il client ha diritto di accesso alla propria maildrop, il server POP3 richiede un “accesso esclusivo” alla maildrop, necessario per prevenire modifiche o rimozioni di messaggi prima che la sessione passi nello stato di AGGIORNAMENTO.

Se la condizione di blocco è acquisita con successo, il server POP3 risponde con un indicatore di stato positivo. La sessione POP3 ora entra nello stato TRANSAZIONE, con nessun messaggio contrassegnato come cancellato. Se la maildrop non può essere aperta per qualche ragione (per una condizione di blocco non può essere raggiunta; al client viene negato l'accesso alla propria maildrop, oppure la maildrop non può essere analizzata), il server POP3 risponde con un indicazione di stato negativo. (Se è stata acquisita una condizione di blocco ma il server POP3 intende rispondere con una indicazione di stato negativa, il server POP3 deve rilasciare la condizione di blocco prima di rigettare il comando).

Dopo avere restituito una indicazione di stato negativa, il server può chiudere la connessione. Se il server non chiude la connessione, il client può o inviare al server un nuovo comando di autenticazione e ripartire quindi da capo, oppure inviare al server il comando QUIT.

Dopo che il server POP3 ha aperto la maildrop, assegna un numero progressivo ad ogni messaggio, e annota la dimensione di ciascun messaggio espressa in bytes. Al primo messaggio viene assegnato il numero “1”, al secondo il numero “2”, e così via fino all'ultimo cui viene assegnato il numero “n”. Nei comandi e nelle risposte previste dal protocollo POP3, le informazioni di tipo numerico vengono riportate in base-10 (i.e., decimale).

Ecco il sommario per il comando QUIT quando usato nello Stato di "AUTORIZZAZIONE" :

QUIT

Argomenti: nessuno
Restrizioni : nessuna
Possible Risposte : +OK

Esempio :

C: QUIT
S: +OK dewey POP3 server signing off

Stato di TRANSAZIONE ("Transaction")

Una volta che il client si è autenticato correttamente presso il server POP3 e che il server POP3 ha bloccato ed aperto l'appropriata maildrop, la sessione POP3 passa in modalità di TRANSAZIONE .

Il client può ora fornire uno qualsiasi dei seguenti comandi (anche ripetutamente). Dopo ciascun comando, il server POP3 restituisce una risposta. Eventualmente il client fornisce il comando QUIT e la sessione POP3 passa nello stato di AGGIORNAMENTO. Sono qui elencati tutti i comandi POP3 validi in stato di TRANSAZIONE :

STAT

Argomenti: nessuno
Restrizioni: può essere inoltrato solamente in stato di TRANSAZIONE

Discussione:

Il server POP3 fornisce una risposta positiva con un messaggio (costituito da una riga) contenente informazioni riguardo alla maildrop. Questa riga viene chiamata "drop listing" per quella maildrop.

Per semplificare l'analisi delle risposte, tutti i server POP3 si devono attenere ad un formato standard per le "drop listing". Le risposte positive sono costituite dalla sequenza "+OK" seguita da un solo carattere "SPACE" (\$20 dec. 32), il numero dei messaggi contenuti nella maildrop, un carattere "SPACE", e la dimensione della maildrop espressa in bytes. In questo documento non vengono formulate ipotesi particolari su ciò che segue la dimensione della maildrop. La implementazione minima pertanto dovrà prevedere una coppia CRLF che determinano il "fine-linea". Implementazioni più avanzate possono includere altre informazioni.

NOTA: Questa RFC scoraggia FORTEMENTE implementazioni del protocollo che forniscano informazioni supplementari nella "drop listing". Altre caratteristiche, opzionali verranno discusse in seguito per consentire al "client" di analizzare i messaggi contenuti nella maildrop.

Si noti che, i messaggi con il contrassegno "DELETED" (marked as deleted) non vengono riportati nel totale.

Possibili Risposte:

+OK nn mm

Esempio :

C: STAT

S: +OK 2 320

LIST [msg]

- *Argomenti:* Un "message-number" (opzionale), che, se presente non si può riferire ad un messaggio con il contrassegno "DELETED".
- *Restrizioni :* può essere inoltrato solamente in stato di *TRANSAZIONE*

Discussione:

Se viene fornito un parametro corretto dopo il comando "LIST", il server POP3 darà una risposta positiva restituendo una linea contenente le informazioni specifiche riferite a quel messaggio. Questa linea viene chiamata "scan listing" relativa a quel messaggio. Se, non viene fornito alcun parametro, e il server POP3 restituisce una risposta positiva, la risposta in questo caso è di tipo multi-linea.

Dopo la sequenza iniziale "+OK", per ciascun messaggio contenuto nella maildrop, il server POP3 risponde con una linea contenente le informazioni riferite ad ogni singolo messaggio.

Se non esiste alcun messaggio nella maildrop, il server POP3 risponde con nessuna "scan listing"; fornisce semplicemente la risposta positiva, seguita da una linea contenente il byte terminale (codice decimale 046, ".") e la coppia CRLF.

Per semplificare l'analisi delle risposte, tutti i server POP3 si devono attenere ad un formato standard per le "scan listing". Una "scan listing" è costituita da il numero progressivo del messaggio entro la maildrop, seguita da un solo carattere "SPACE" (\$20 dec. 32), e dalla dimensione esatta del messaggio espressa in bytes. I metodi per calcolare la dimensione esatta del messaggio sono descritti nella sezione "Formato del Messaggio" più avanti. In questo documento non vengono formulate ipotesi particolari su ciò che segue la dimensione esatta del messaggio nella "scan listing".

La implementazione minima pertanto deve prevedere una coppia CRLF che determinano il "fine-linea". Implementazioni più avanzate possono includere altre informazioni desunte da ulteriori analisi sul messaggio

NOTA: Questa RFC scoraggia **FORTEMENTE** implementazioni del protocollo che forniscano informazioni supplementari nella "scan listing". Altre caratteristiche, opzionali verranno discusse in seguito per consentire al "client" di analizzare i messaggi contenuti nella maildrop.

Si noti che, i messaggi con il contrassegno "DELETED" (marked as deleted) non vengono elencati.

Possibili Risposte:

- +OK scan listing follows
- ERR no such message

Esempi :

C: LIST

S: +OK 2 messages (320 octets)

S: 1 120

S: 2 200

S: .

...

C: LIST 2

S: +OK 2 200

...

C: LIST 3

S: -ERR no such message, only 2 messages in maildrop

RETR msg

- *Argomenti: Un "message-number" (obbligatorio), che, non si può riferire ad un messaggio con il contrassegno "DELETED".*
- *Restrizioni: può essere inoltrato solamente in stato di TRANSAZIONE*

Discussione:

Se il server POP3 fornisce una risposta positiva, allora la risposta data è di tipo multi-linea. Dopo la sequenza iniziale "+OK", il server POP3 invia il messaggio corrispondente al "message-number" fornito, prestando attenzione a introdurre il carattere terminale (come accade in tutte le risposte di tipo "multi-linea").

Possibili Risposte:

+OK message follows

-ERR no such message

Esempi:

C: RETR 1

S: +OK 120 octets

S: <the POP3 server sends the entire message here>

S: .

DELE msg

- *Argomenti: Un "message-number" (obbligatorio), che, non si può riferire ad un messaggio con il contrassegno "DELETED".*
- *Restrizioni: può essere inoltrato solamente in stato di TRANSAZIONE*

Discussione:

Il server POP3 assegna al messaggio il contrassegno "DELETED". Qualsiasi riferimento futuro al "message-number" associato a tale messaggio, in un comando POP3 genera un errore. Il server POP3, non cancella il messaggio fino a che la sessione POP3 non entra nello stato "DI AGGIORNAMENTO".

Possibili Risposte:

+OK message deleted

-ERR no such message

Esempi:

C: DELE 1

S: +OK message 1 deleted

...

C: DELE 2

S: -ERR message 2 already deleted

NOOP

- *Argomenti: nessuno*
- *Restrizioni: può essere inoltrato solamente in stato di TRANSAZIONE*

Discussione:

Il server POP3 non fa nulla, risponde semplicemente con una risposta di tipo positivo.

Possibili Risposte:

+OK

Esempi:

C: NOOP

S: +OK

RSET

- *Argomenti: nessuno*
- *Restrizioni: può essere inoltrato solamente in stato di TRANSAZIONE*

Discussione:

Viene tolto il contrassegno "DELETED" a tutti i messaggi marchiati "DELETED" dal server POP3. Il server restituisce poi una risposta positiva.

Possibili Risposte:

+OK

Esempi:

C: RSET

S: +OK maildrop has 2 messages (320 octets)

Stato di AGGIORNAMENTO ("Update")

Quando il client fornisce il comando QUIT nello stato TRANSAZIONE, la sessione POP3 entra nello stato di AGGIORNAMENTO. (Si noti che se il comando QUIT viene inviato al server nello stato di AUTORIZZAZIONE, la sessione POP3 termina; non entra in stato di AGGIORNAMENTO).

Se una sessione termina per ragioni diverse dall'aver ricevuto il comando QUIT da parte del client, la sessione POP3 non entra nello stato di AGGIORNAMENTO e il server non deve rimuovere alcun messaggio dalla maildrop.

QUIT

- *Argomenti: nessuno*
- *Restrizioni: nessuna*

Discussione:

Il server POP3 rimuove tutti i messaggi con il contrassegno "DELETED" dalla maildrop e risponde specificando lo stato dell'operazione. Se si è verificato un errore, come ad esempio una riduzione di risorse (ad es.: connettività), mentre è in corso la rimozione dei messaggi, può accadere che alcuni o nessun messaggio con il contrassegno "DELETED" venga rimosso dalla maildrop. In nessun caso il server può rimuovere messaggi senza il

contrassegno "DELETED". Sia che la rimozione abbia avuto successo oppure no, il server rilascia l'accesso esclusivo alla maildrop e chiude la connessione TCP.

Possibili Risposte:

- +OK
- ERR some deleted messages not removed

Esempi:

- C: QUIT
- S: +OK dewey POP3 server signing off (maildrop empty)
- ...
- C: QUIT
- S: +OK dewey POP3 server signing off (2 messages left)
- ...

Comandi POP3 Opzionali

I comandi POP3 discussi più avanti devono essere supportati da tutte le implementazioni minime del server POP3. I comandi opzionali descritti di seguito, permettono ad un client POP3 una grande libertà nella manipolazione dei messaggi, mantenendo una semplice implementazione del protocollo POP3 a livello server.

NOTA : Questa RFC incoraggia fortemente la implementazione di questi comandi anzichè appesantire la consistenza delle "scan listing" e delle "drop listing" fornite dal server. In breve, la filosofia di questa RFC è di potenziare il client POP3 aumentandone l'intelligenza ma mantenere semplice la implementazione del server POP3.

TOP msg n

- *Argomenti:* Un "message-number" (obbligatorio), che, non si può riferire ad un messaggio con il contrassegno "DELETED" e un numero "n" non negativo di linee (richiesto).
- *Restrizioni:* può essere inoltrato solamente in stato di **TRANSAZIONE**

Discussione:

Se il server POP3 fornisce una risposta positiva, allora la risposta data è di tipo multi-linea. Dopo la sequenza iniziale "+OK", il server POP3 invia le intestazioni (headers) del messaggio, la linea vuota che separa le intestazioni dal corpo del messaggio, e successivamente il numero di linee indicate nel corpo del messaggio, prestando attenzione a introdurre il carattere terminale (come accade in tutte le risposte di tipo "multi-linea").

Se il numero di linee richiesto dal client è maggiore il numero di linee del corpo del messaggio, il server POP3 invia l'intero messaggio.

Possibili Risposte:

- +OK top of message follows
- ERR no such message

Examples:

- C: TOP 1 10

S: +OK

S: <il server POP3 invia le intestazioni del messaggio, una linea vuota, e le prime 10 linee del corpo del messaggio>

S: .

...

C: TOP 100 3

S: -ERR no such message

UIDL [msg]

- *Argomenti:* Un "message-number" (obbligatorio), che, non si può riferire ad un messaggio con il contrassegno "DELETED".
- *Restrizioni:* può essere inoltrato solamente in stato di TRANSAZIONE

Discussione:

Se è stato fornito un parametro dopo il comando UIDL e il server POP3 fornisce una risposta positiva tale risposta giunge al client con una linea contenente informazioni riguardo a quel messaggio. Questa linea viene chiamata "unique-id listing" per quel messaggio. Se nessun argomento viene fornito ed il server POP3 fornisce una risposta positiva, allora la risposta data è di tipo multi-linea. Dopo la sequenza iniziale "+OK", il server POP3, per ciascun messaggio contenuto nella maildrop, risponde con una linea contenente informazioni per quel messaggio.

Per semplificare l'analisi delle risposte, tutti i server POP3 si devono attenere ad un formato standard per le "unique-id listing". Una "unique-id listing" è costituita dal "message-number" di quel messaggio seguito da un solo carattere "SPACE" (\$20 dec. 32), e dall'identificatore univoco "unique-id" del messaggio; nessuna altra informazione viene ulteriormente accodata. Lo "unique-id" o identificatore univoco di un messaggio è una stringa arbitraria determinata a livello di server; essa è costituita da un numero di caratteri compresi fra 1 e 70 scelti nel campo compreso fra il valore esadecimale \$21 (0x21) e il valore esadecimale \$7E (0x7E), che in modo univoco identifica un messaggio all'interno di una maildrop e che si mantiene inalterato durante l'intera sessione. Questa persistenza è richiesta anche se una sessione termina senza entrare nello stato di AGGIORNAMENTO.

Il server NON DEVE MAI riutilizzare l'identificatore "unique-id" in una determinata maildrop, finchè l'entità associata a quell'identificatore esiste. I messaggi con il contrassegno "DELETED" non vengono elencati.

Mentre è in genere preferibile, nelle implementazioni server, memorizzare i valori arbitrari assegnati "unique-id" nella maildrop, le specifiche di questo documento prescrivono di calcolare "unique-id" con tecniche di "hash" sul messaggio. I clients devono essere in grado di gestire correttamente situazioni in cui due copie identiche di un messaggio in una maildrop sono individuate dal medesimo "unique-id".

Possible Responses:

+OK unique-id listing follows

-ERR no such message

Examples:

C: UIDL

S: +OK

S: 1 whqtswo00WBw418f9t5JxYwZ

S: 2 QhdPYR:00WBw1Ph7x7

S: .

...

C: UIDL 2

S: +OK 2 QhdPYR:00WBw1Ph7x7

...

C: UIDL 3

S: -ERR no such message, only 2 messages in maildrop

USER name

- *Argomenti: una stringa di identificazione della mailbox (obbligatoria) che però ha significato SOLO su quel server;*
- *Restrizioni: può essere inviato al server in stato di AUTORIZZAZIONE dopo la riga di benvenuto del server POP3 o dopo una sequenza USER/PASS che non si è conclusa con successo.*

Discussione:

Per autenticarsi utilizzando la combinazione di comandi USER e PASS, il client deve inviare al server per primo il comando USER. Se il server POP3 risponde con un messaggio di stato positivo, ("+OK"), allora il client può fornire sia il comando PASS per completare l'autenticazione, sia il comando QUIT per terminare la sessione POP3.

Se, al contrario, il server POP3 risponde con un messaggio di stato negativo ("-ERR") al comando USER, allora il client può inviare un nuovo comando di autenticazione, oppure può inviare il comando QUIT. Il server può restituire una risposta positiva anche se la mailbox non esiste; il server può restituire una risposta negativa se la mailbox esiste ma non consente una autenticazione con password in chiaro.

Possibili risposte :

+OK name is a valid mailbox

-ERR never heard of mailbox name

Esempio :

C: USER frated

S: -ERR sorry, no mailbox for frated here

...

C: USER mrose

S: +OK mrose is a real hoopy frood

PASS string

- *Argomenti: una password specifica della mailbox su quel server (obbligatoria)*
- *Restrizioni: deve essere inviato al server nello stato di AUTORIZZAZIONE immediatamente dopo un comando USER accettato dal server*

Discussione

Quando il client invia il comando PASS, il server POP3 utilizza la coppia di parametri inviati con la sequenza di comandi USER e PASS per determinare se quel client è autorizzato ad accedere a quella appropriata maildrop. Poiché il comando PASS prevede

esattamente un unico parametro, un server POP3 deve considerare i caratteri SPACE posti all'interno del parametro come parte integrante della password piuttosto che separatori fra parametri diversi.

Possibili risposte:

- +OK maildrop locked and ready
- ERR invalid password
- ERR unable to lock maildrop

Esempio:

```
C: USER mrose
S: +OK mrose is a real hoopy frood
C: PASS secret
S: -ERR maildrop already locked
...
C: USER mrose
S: +OK mrose is a real hoopy frood
C: PASS secret
S: +OK mrose's maildrop has 2 messages (320 octets)
```

APOP name digest

- *Argomenti: una stringa di identificazione della mailbox e una "MD5 digest string" (obbligatorie entrambe)*
- *Restrizioni: può essere inviato al server in stato di AUTORIZZAZIONE dopo la riga di benvenuto del server POP3 o dopo una sequenza USER/PASS che non si è conclusa con successo.*

Discussione: Di norma, una sessione POP3 inizia con la coppia di messaggi USER/PASS. Ciò comporta che sia lo user-id sia la password relativa viaggiano in chiaro sulla rete. In caso di utilizzo non continuativo del protocollo POP3, non si va incontro a gravi rischi. Tuttavia, in molte implementazioni di client POP3 questi si connettono al server periodicamente per verificare se nella mailbox è giunta nuova posta. Perciò, il rischio di cattura della password è molto marcato. Si richiede quindi un metodo alternativo di autenticazione che abbandoni lo schema originario che prevede di inviare in chiaro sulla rete le password. Il comando APOP fornisce queste funzionalità. Un server POP3 che implementa il comando APOP invia, nella "riga di benvenuto" indirizzata al client dopo l'apertura della connessione TCP, un "timestamp" una sorta di contrassegno temporale. La sintassi del "timestamp" corrisponde al 'msg-id' indicato nel documento [RFC822], and DEVE essere diverso ogni volta che il server POP3 invia una riga di benvenuto al client. Ad esempio, in caso di implementazione UNIX nel quale viene utilizzato un processo UNIX diverso per ogni istanza del servizio POP3, la sintassi è la seguente :

```
<process-ID.clock@hostname>
```

dove 'process-ID' è il valore decimale del PID del processo, clock è l'espressione decimale del clock di sistema, e "hostname" rappresenta il nome di dominio della macchina su cui il server POP3 è in esecuzione. Il client POP3 prende nota del "timestamp", e invia il comando APOP al server. Il parametro "name" ha la stessa semantica di "name" nel comando USER; il parametro "digest" è calcolato dal client applicando l'algoritmo MD5 descritto nel documento [RFC1321] ad una stringa costituita dal "timestamp" e

comprensiva delle parentesi angolari (< e >) seguita da un codice segreto noto solamente al client e al server POP3. Bisogna prestare molta attenzione per evitare che la divulgazione non autorizzata del codice segreto dia la possibilità a chi è maleintenzionato di intromettersi sul servizio di posta. Il parametro "digest" è un valore a 16 bytes, viene inviato in formato esadecimale, utilizzando i caratteri minuscoli del codice ASCII.

Quando il server POP3 riceve il comando APOP, verifica il "digest" trasmesso dal client; se esso è corretto, il server risponde positivamente al client e passa in stato di TRANSAZIONE, in caso contrario il server rimane nello stato di "AUTORIZZAZIONE". Si tenga presente che maggiore è la lunghezza del codice segreto utilizzato nell'algoritmo MD5, maggiore è la difficoltà di risalire ad esso. Perciò i codici segreti devono essere stringhe di caratteri e/o numeri relativamente lunghe (considerevolmente più lunghe di quella indicata nell'esempio che segue).

Possibili Risposte:

+OK maildrop locked and ready

-ERR permission denied

Esempio:

S: +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>

C: APOP mrose c4c9334bac560ecc979e58001b3e22fb

S: +OK maildrop has 1 message (369 octets)

In questo esempio, il codice segreto è rappresentato dalla stringa di caratteri 'tanstaaf'. L'algoritmo MD5 viene perciò applicato alla stringa:

<1896.697170952@dbc.mtview.ca.us>tanstaaf

che produce il valore "digest" :

c4c9334bac560ecc979e58001b3e22fb

Considerazioni Operative

Dato che alcune delle caratteristiche opzionali descritte in precedenza sono state incorporate nel protocollo POP3, si è accumulata una certa esperienza utilizzandole soprattutto su sistemi commerciali applicati su larga scala in campi dove la maggior parte degli utenti non sono relazionati fra di loro. In queste situazioni e in altre utenti e venditori di client POP3 hanno scoperto che utilizzando il comando UIDL senza utilizzare il comando DELE può portare ad pensare di avere realizzato versione semplificata di "maildrop come deposito semi-permanente" funzionalità presente nel protocollo IMAP. Naturalmente, le altre caratteristiche del protocollo IMAP quali l'interrogazione su una connessione esistente per stabilire se vi sono nuovi messaggi e il supporto di cartelle multiple sul server, non sono presenti nel protocollo POP3.

Queste caratteristiche usate in questo modo da utenti occasionali, hanno causato il diffondersi della abitudine a lasciare depositati, sul server, messaggi già letti in grande quantità. Questo comportamento non può essere accettato dal punto di vista di chi amministra il server mail. La situazione è inoltre aggravata dal fatto che le limitate possibilità del protocollo POP3 non permettono una manipolazione efficiente delle maildrop che hanno centinaia o migliaia di messaggi. Di conseguenza, si raccomanda agli operatori di server multi-utente, specialmente a quelli destinati al servizio di posta elettronica nei quali l'utente accede alla maildrop attraverso il protocollo POP3 di tenere in considerazione le seguenti possibilità :

Imporre un limite massimo alla maildrop di ciascun utente

Uno svantaggio di questa scelta è che l'accumulazione eccessiva di messaggi può impedire all'utente di ricevere i nuovi nella maildrop. I siti che scelgono questa opzione devono informare gli utenti, attraverso appropriati messaggi inseriti nella maildrop, che lo spazio a disposizione sta per esaurirsi.

Adottare regole riguardo alla giacenza dei messaggi di posta sul server

I siti sono liberi di stabilire politiche locali riguardo alla permanenza dei messaggi di posta sul server sia per quanto riguarda i messaggi letti sia per quelli non letti. Per esempio, un provider di servizi di posta potrebbe decidere di cancellare i messaggi non letti dopo un periodo di 60 gg. di giacenza sul server e quelli letti dopo un periodo di 7 giorni. Le cancellazioni dei messaggi sono al di fuori degli scopi del protocollo POP3 e non sono da considerare violazioni al protocollo. Gli amministratori del servizio di posta, devono rendere gli utenti consapevoli delle regole vigenti in tema di giacenza dei messaggi sul server.

I Client non devono assolutamente pensare che la cancellazione dei messaggi sia una operazione automatica affidata al server ma devono continuare ad usare il messaggio DELE quando ciò è necessario.

E' opportuno notare che, limitare il tempo di permanenza dei messaggi sul server può creare confusione nella comunità degli utenti dato che, i client POP3 hanno opzioni di configurazione che prevedono di lasciare la posta sul server opzione che però di fatto non è supportata dal server.

Una caso speciale di regole di gestione della posta è quello che prevede che il messaggio possa essere scaricato solamente una volta dal server perché immediatamente dopo viene cancellato. Questo modo di funzionare può essere implementato via software sul server attivando la seguente procedura : " A seguito di un POP3 login da parte di un client che ha concluso con un comando QUIT, cancella tutti i messaggi scaricati durante la sessione POP3 utilizzando il comando RETR".

E' importante non cancellare i messaggi in caso di una anormale conclusione della connessione (ad es.: in assenza del comando QUIT ricevuto dal client) perché il client potrebbe non avere ricevuto o non avere memorizzato in modo corretto e completo il messaggio. I server che implementano la regola del "download-and-delete" devono disabilitare o limitare le funzioni previste dal comando TOP, dato che può essere utilizzato come metodo alternativo per effettuare il download dei messaggi dal server.

Riassunto dei comandi POP3

Set minimo dei comandi POP3 :

USER name *validi in stato di AUTORIZZAZIONE*
PASS string
QUIT

STAT *valid in the stato di TRANSAZIONE*
LIST [msg]
RETR msg
DELE msg
NOOP

RSET
QUIT

Comandi POP3 Opzionali:

APOP name digest *valido in stato di AUTORIZZAZIONE*
TOP msg n *valido in stato di TRANSAZIONE*
UIDL [msg]

Risposte del server POP3:

+OK
-ERR

Note that with the exception of the STAT, LIST, and UIDL commands, the reply given by the POP3 server to any command is significant only to "+OK" and "-ERR". Any text occurring after this reply may be ignored by the client.

Esempio di una sessione POP3

S: <wait for connection on TCP port 110>
C: <open connection>
S: +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C: APOP mrose c4c9334bac560ecc979e58001b3e22fb
S: +OK mrose's maildrop has 2 messages (320 octets)
C: STAT
S: +OK 2 320
C: LIST
S: +OK 2 messages (320 octets)
S: 1 120
S: 2 200
S: .
C: RETR 1
S: +OK 120 octets
S: <the POP3 server sends message 1>
S: .
C: DELE 1
S: +OK message 1 deleted
C: RETR 2
S: +OK 200 octets
S: <the POP3 server sends message 2>

S: .
C: DELE 2
S: +OK message 2 deleted
C: QUIT
S: +OK dewey POP3 server signing off (maildrop empty)
C: <close connection>
S: <wait for next connection>

Formato dei Messaggi

Tutti i messaggi trasmessi durante una sessione POP3 si suppone siano conformi allo standard per i messaggi di testo su Internet descritti nel documento [RFC822]. E'importante notare che il conteggio dei bytes relativi ad un messaggio effettuato sul server può essere diverso dal conteggio dei bytes assegnato a quel messaggio; ciò è dovuto alle convenzioni locali per designare l'EOL (end of line).

Generalmente, durante lo stato di AUTORIZZAZIONE della sessione POP3, il server può calcolare la dimensione in bytes di ciascun messaggio quando apre la maildrop. Per esempio, se il server POP3 rappresenta internamente il carattere EOL con un solo carattere, allora è sufficiente che il server conti ciascuno di questi caratteri due volte. Si noti che le linee di messaggio che iniziano con il byte terminale non vanno contati due volte dato che il client POP3 rimuove tutti i caratteri fine linea aggiunti quando esso riceve risposte multi linea.

Riferimenti

[RFC821] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821, USC/Information Sciences Institute, August 1982.

[RFC822] Crocker, D., "Standard for the Format of ARPA-Internet Text Messages", STD 11, RFC 822, University of Delaware, August 1982.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, MIT Laboratory for Computer Science, April 1992.

[RFC1730] Crispin, M., "Internet Message Access Protocol - Version 4", RFC 1730, University of Washington, December 1994.

[RFC1734] Myers, J., "POP3 AUTHentication command", RFC 1734, Carnegie Mellon, December 1994.

Considerazioni sulla Sicurezza

It is conjectured that use of the APOP command provides origin identification and replay protection for a POP3 session. Accordingly, a POP3 server which implements both the PASS and APOP commands should not allow both methods of access for a given user; that is, for a given mailbox name, either the USER/PASS command sequence or the APOP command is allowed, but not both. Further, note that as the length of the shared secret increases, so does the difficulty of deriving it. Servers that answer -ERR to the USER command are giving potential attackers clues about which names are valid. Use of the PASS command sends passwords in the clear over the network. Use of the RETR and

TOP commands sends mail in the clear over the network. Otherwise, security issues are not discussed in this memo.

Riconoscimenti

The POP family has a long and checkered history. Although primarily a minor revision to RFC 1460, POP3 is based on the ideas presented in RFCs 918, 937, and 1081. In addition, Alfred Grimstad, Keith McCloghrie, and Neil Ostroff provided significant comments on the APOP command.

Indirizzi degli Autori

John G. Myers - Carnegie-Mellon University - 5000 Forbes Ave - Pittsburgh, PA 15213

E-Mail: jgm+@cmu.edu

Marshall T. Rose - Dover Beach Consulting, Inc. - 420 Whisman Court - Mountain View, CA 94043-2186

E-Mail: mrose@dbc.mtview.ca.us

Differenze rispetto alla RFC 1725

This memo is a revision to RFC 1725, a Draft Standard. It makes the following changes from that document:

- clarifies that command keywords are case insensitive.
- specifies that servers must send "+OK" and "-ERR" in upper case.
- specifies that the initial greeting is a positive response, instead of any string which should be a positive response.
- clarifies behavior for unimplemented commands.
- makes the USER and PASS commands optional.
- clarified the set of possible responses to the USER command.
- reverses the order of the examples in the USER and PASS commands, to reduce confusion.
- clarifies that the PASS command may only be given immediately after a successful USER command.
- clarified the persistence requirements of UIDs and added some implementation notes.
- specifies a UID length limitation of one to 70 octets.
- specifies a stato indicator length limitation of 512 octets, including the CRLF.
- clarifies that LIST with no arguments on an empty mailbox returns success.
- adds a reference from the LIST command to the Message Format section
- clarifies the behavior of QUIT upon failure
- clarifies the security section to not imply the use of the USER command with the APOP command.
- adds references to RFCs 1730 and 1734
- clarifies the method by which a UA may enter mail into the transport system.
- clarifies that the second argument to the TOP command is a number of lines.

- changes the suggestion in the Security Considerations section for a server to not accept both PASS and APOP for a given user from a "must" to a "should".
- adds a section on scaling and operational considerations

Appendice A : The MD5 Message-Digest Algorithm

Executive Summary

This document describes the MD5 message-digest algorithm. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" (impronta digitale) or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

The MD5 algorithm is designed to be quite fast on 32-bit machines. In addition, the MD5 algorithm does not require any large substitution tables; the algorithm can be coded quite compactly. The MD5 algorithm is an extension of the MD4 message-digest algorithm [1,2].

The MD5 message-digest algorithm is simple to implement, and provides a "fingerprint" or message digest of a message of arbitrary length. It is conjectured that the difficulty of coming up with two messages having the same message digest is on the order of 2^{64} operations, and that the difficulty of coming up with any message having a given message digest is on the order of 2^{128} operations. The MD5 algorithm has been carefully scrutinized for weaknesses. It is, however, a relatively new algorithm and further security analysis is of course justified, as is the case with any new proposal of this sort.
