Modulo 8: Applicativi

Parte 5: FTP e TFTP

Introduzione a FTP

- Storia

Introduzione a FTP (1)

- Protocollo di trasferimento dati tra macchine connesse attraverso una rete che supporta TCP/IP.
- Il primo standard FTP (RFC 114) nasce nel 1971, in ARPANet.
- Lo definizione dello standard attuale ad opera dell'IETF (RFC 959) e' del 1985.

Introduzione ad FTP (2)

- Si basa sul modello client/server:
  - Il server FTP viene eseguito sulla macchina che accede fisicamente ai file e attende richieste.
  - Il client FTP si collega al server e puo' richiedere al server operazioni inerenti il trasferimento dati.
- Il trasferimento dati ed il controllo delle operazioni avviene via TCP
- Il server ascolta sulla porta TCP 21

Le connessioni FTP

- Per ogni sessione FTP sono necessarie due connessioni TCP tra client e server:
  - Control connection, connessione attraverso la quale vengono iviati i comandi e le risposte del server
  - Data connection, connessione attraverso la quale vengono iviati dati veri e propri

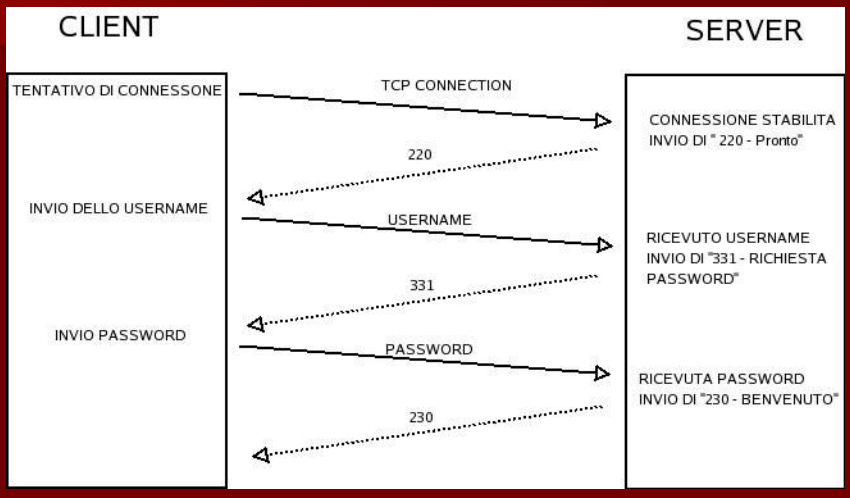
Control connection (1)

- Il canale di controllo o control connection vinene stabilito dal client che utilizza una porta TCP locale (> 1024) per connettersi alla porta 21 del server.
- La connessione richiede una sessione di autenticazione (access control) tramite username e password seguita da una resource selection (il server decide quali risorse mettere a disposizione del utente)

Control connection (2)

- La sessione di autenticazione avviene in modo semplice tramite l'invio di username e password tramite i comandi USER e PASS e delle relative risposte del server.
- Una volta verificate le credenziali dell'utente il server configura il tipo di accesso associato (permessi di scrittura e lettura su diversi tipi di file o directory).
- Tramite il comando ACCT il client puo' decidere a quale tipo di account locale (del server) essere associato.

Control connection (3)



Control connection (3)

- E' diffusa la pratica di consentire un accesso anonimo (anonymous FTP), generalmente richiedendo come username "anonymous" e come password un indirizzo email
- I client ftp utilizzano email fasulle:
  - Firefox: mozilla@example.com
  - Wget: wget@

Data connection (1)

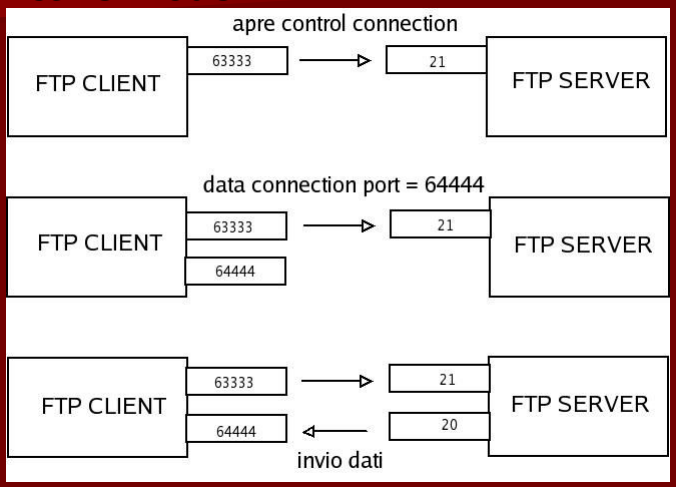
- Il canale di trasferimento dati o data connection viene stabilito dopo l'autenticazione ma solo nel momento in cui vi siano dati da trasmettere (directory listing, file trasfert)
- La connessione dati puo' essere stabilita in due modi: active mode o passive mode

Data connection (2)

- In active mode il client si connette al server sulla porta 21 (control connection) e, prima del trasferimento dati, si mette in ascolto su una porta TCP (>1024).
- Il client notifica al server, attraverso la connessione di controllo, il numero di porta su cui si e' messo in ascolto
- Il server si connette con la porta suddetta dalla porta 20 aprendo cosi' la data connection
- Inizia il trasferimento dati.

Data connection (3)

- Active mode FTP

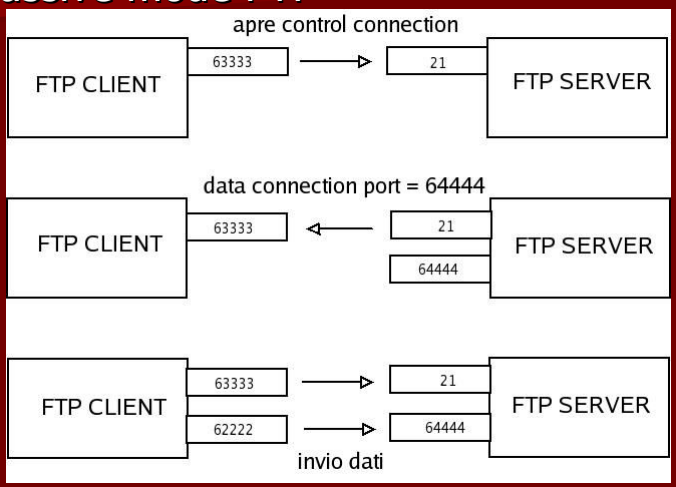


Data connection (3)

- In passive mode apre la control connection sulla porta 21 del server. Il server, alla richiesta di trasmissione dati, apre una porta TCP (>1024) e trasmette attraverso la connessione di controllo il numero della porta.
- Il client si connette alla porta suddetta aprendo cosi' la data connection.
- Inizia il trasferimento dati.

Data connection (5)

- Passive mode FTP



Data connection (5)

- L'active mode e' piu' indicato dal punto di vista della sicurezza del server (solo due porte utilizzabili 20/TCP e 21/TCP)
- Il passive mode permette connessioni con il client dietro NATting (e' il client ad iniziare la connessione di trasferimento dati)
- Esistono soluzioni di *connection tracking* che permettono di adattare il NATting all'active mode FTP

Tipi di trasmissione dati

- Quando la data connection e' stata stabilita, la trasmissione dei dati puo' avvenire in 3 modi:
  - Stream mode: i dati vengono inviati bit a bit e la trasmissione finisce quando la connessione viene interrotta
  - Block mode: i dati vengono divisi in blocchi e racchiusi in frame FTP. E' utile in quanto permette una verifica della trasmissione
  - Compress mode: la trasmissione viene compressa mediante un algoritmo rudimentale. E' utile solo se i dati non sono gia' compressi

Formato dei dati (1)

- E' possibile in FTP definire il tipo di dati che devono essere trasmessi. Esistono due tipologie principali:
  - ASCII: file di testo strutturati secondo la codifica ASCII. La trasmissione avviene per carattere. Utile quando i sistemi operativi condificano in maniera diversi alcuni caratteri speciali (es.: Unix vs. Windows)
  - Binary: file generici. La trasmissione avviene bit a bit, senza che l'applicativo tenti di interpretare il contenuto

Formato dei dati (2)

- Esistono altri due formati (EBCDIC e local) ma non sono quasi piu' utilizzati.
- E' importante non trasmettere dati binari in ASCII mode, in quanto verrebbero corrotti.
- Alcune implementazioni di FTP tentano di riconoscere automaticamente il formato dei dati.

Comandi interni al protocollo (1)

- Attraverso la connessione di controllo il client invia al server una serie di istruzioni o protocol commands. Ad ogni comando segue una risposta del server.
- I comandi si dividono in 3 gruppi:
  - Access control commands: fanno parte della procedura di login e gestiscono l'acesso alle risorse
  - Transfer parameter command: specificano i parametri di trasferimento e di connessione (tipo di dati, active, passive)
  - FTP service command: tutti i comandi che permettono di eseguire materialmente la trasmissione dei dati

Comandi interni al protocollo (2)

- La struttura dei comandi e' la stessa di TELNET
- Ogni comando e' una stringa seguita da un parametro

Access control command

Nome	Comando	Parametri	Descrizione
Account	ACCT	<account-information>	Alcuni server richiedono un account per accessi specifici, ad esempio per memorizzare file
Password	PASS	<password>	Invia la password dell'utente
Logout	QUIT		Disconnette l'utente e chiude la connessione di controllo.
Change to parent directory	CDUP		Cambia la directory di lavoro corrente con quella di livello superiore
Change working directory	CWD	<pathname>	Cambia la directory di lavoro sul server
Reinitialize	REIN		Resetta tutti i parametri, termina le connessioni dati.
Structure mount	SMNT	<pathname>	Inserisce la struttura di file specificata
User Name	USER	<username>	Identificazione dell'utente richiesta dal server

Transfer parameter commands

Trasfer mode	MODE	<mode-code>	Modalità di trasferimento (S=stream, B=block, C=compressed). Il valore di default è S
Representation type	TYPE	<type-code>	Tipo di rappresentazione dei dati (A=ASCII, I=binary). Il valore di default è A
Passive	PASV		Configura la connessione dati in passive mode
Data port	PORT	<host-port>	Indirizzo internet dell'host e indirizzo TCP della porta, per la connessione dati in active mode

Service commands (1)

Nome	Comando	Parametri	Descrizione
Abort	ABOR		Termina la connessione per il trasferimento dei dati
Allocate	ALLO	<decimal-integer>	Alcuni server lo richiedono per riservare spazio sufficiente per contenere i nuovi file da trasferire
Append (with create)	APPE	<pathname>	Obbliga il server ad accettare i dati inviati tramite la connessione dati e salvarli in un file. Se il file esiste già i dati vengono aggiunti, altrimenti il file viene creato *ex-novo*
Delete	DELE	<pathname>	Cancella dal server il file specificato
Help	HELP	<string>	Restituisce informazioni sul comando specificato
List	LIST	<pathname>	Se l'argomento indica un file, elenca le proprietà del file; se l'argomento è una directory, il server trasferisce una lista di file nella directory

Service commands (2)

Make directory	MKD	<pathname>	Crea sul server la directory indicata
Name list	NLST	<pathname>	Elenca il contenuto della directory indicata
Noop	NOOP		Indica nessuna azione tranne l'invio di un Ok dal server
Restart	REST	<marker>	Riprende il trasferimento file dall'offset indicato
Retrieve	RETR	<pathname>	Obbliga il server a spedire una copia del file all'utente/server dall'altra parte della connessione
Remove directory	RMD	<pathname>	Rimuove dal server la directory specificata
Rename from	RNFR	<pathname>	Indica il vecchio nome del file da rinominare. Deve essere immediatamente seguito da un RNTO

Service commands (3)

Rename to	RNTO	<pathname>	Indica il nuovo nome del file da rinominare, indicato dal comando RNFR
Site parameters	SITE	<string>	Comando usato dal server per fornire servizi specifici del suo sistema che sono essenziali per il trasferimento dei file ma non sufficientemente universali per essere inclusi come comandi del protocollo
Status	STAT	<pathname>	È una risposta inviata dal server: durante il trasferimento di file contiene lo stato dell'operazione
Store	STOR	<pathname>	Obbliga il server ad accettare i dati inviati tramite la connessione dati e salvarli
Store unique	STOU	<pathname>	Obbliga il server ad accettare i dati inviati tramite la connessione dati e salvarli con un nome univoco
System	SYST		Restituisce il sistema operativo in uso sul server

FTP replies (1)

- La risposta ad un comando FTP avviene attraverso un codice di tre cifre (reply code) che puo' essere seguito da una descrizione dipendente dall'implementazione del server
- Ognuna delle tre cifre (x,y,z) ha un significato differente:
  - X: indica il fallimento o il successo di una operazione e gli stati intermedi
  - Y: indica il motivo del fallimento o del successo
  - Z: parametro specifico

FTP replies (2)

Formato codice	significato	descrizione
1yz	Risposta positiva temporanea	Il comando e' stato accettato ma il client deve attendere la risposta definitiva
2yz	Risposta positiva definitiva	Il comando e' stato accettato
3yz	Risposta positiva intermedia	Il comando e' stato accettato ma necessita un'altra azione per essere completato
4yz	Risposta negativa temporanea	Il comando non e' stato accettato ma il problema e' temporaneo
5yz	Risposta negativa definitiva	Il comando non e' stato accettato

FTP replies (3)

Formato codice	significato	descrizione
x0z	Sintassi	Errore di sintassi
x1z	Informazione	Richiesta di ulteriori informazioni
x2z	Connessione	Risposta al tentativo di connessione dati
x3z	Autenticazione	Risposta all'autenticazione o accounting
x4z	Non specificato	---
x5z	Filesystem	Risposta relativa al filesystem locale al server

FTP replies (4)

- Es.: Errore 530 = Errore di autenticazione (username o password errata)
- E' possibile ricevere risposte composte da piu' linee (ad es. i banner di login):

```
230 - Benvenuto in ftp.ge.infn.it
230 -
230 - Sei il #30 utente di 100 ammessi
230 - logged in
```


User interface (1)

- La user interface permette di svolgere azioni, anche complesse, digitando un numero limitato di comandi (es.: copiare ricorsivamente il contenuto di una directory, copia con caratteri speciali)
- Esistono user interface a linea di comando (di solito integrate nei SSOO) o user interface grafiche (GUI)

User interface (2)

- La user interface a linea di comando si lancia digitando il comando "ftp" seguito dall'FQDN del server.
- GUI:
  - Windows: FileZilla, WSFTP, SmartFTP,……
  - Linux: gFTP, Kasablanca, ftpcube,……
  - MacOSX: Fetch, Cyberduck, FTPeel,……

Criticita' di FTP

- FTP non implementa un meccanismo di cifratura dei dati: e' vulnerabile allo sniffing
- Utilizza due connessioni TCP (control e data) quindi e' piu' difficile da gestire dal punto di vista del NATting
- Alta latenza dovuta al numero e al formato dei comandi
- Non possiede un meccanismo di controllo dell'integrita' dei dati
- Non possiede un meccanismo di controllo dell'errore (usa quello di TCP)
- Non trasferisce glio attributi dei file (data di accesso e di modifica)

TFTP

- TFTP (Trivial FTP), nasce per soddisfare l'esigenza di un protocollo di file transfer piu' semplice di FTP che richidesse programmi (client e server) di dimensioni ridotte
- Viene utilizzato da apparecchiature dotate di poca memoria, da PC diskless o da sistemi di installazione remota via PXE
- La versione attuale (TFTP version 2, revision 2) e' descritta dall'RFC1350 del 1992

Differenze tra TFTP ed FTP

- Trasporto: TFTP utilizza UDP come strato di trasporto mentre FTP si basa su TCP
- Comandi: TFTP puo' solo inviare o ricevere dati.
- Formato dei dati: TFTP accetta solo rappresentazione dei dati ASCII o binaria
- Autenticazione: TFTP non ha meccanismo di autenticazione

Connessione TFTP

- Il server TFTP ascolta sulla porta 69/UDP
- Il client invia dati da una porta "A" casuale (>1024)
- Il server decide di rispondere da una porta "B" casuale (>1024) alle richieste del client
- Il controllo ed il trasferimento dati avviene sullo stesso canale identificato dalle due porte "A" e "B"

Problemi di TFTP

- La totale mancanza di sicurezza rende TFTP inadatto ad essere un sostituto di FTP. Deve essere utilizzato in casi particolari
- Avendo un solo canale per il controllo e lo scambio di dati, TFTP ha problemi di performance. Non deve essere utilizzato per trasferimenti grandi moli di dati.