第6篇

应用层协议原理

第23章

文件传输协议

在互联网中我们经常需要在远端主机和本地服务器之间传输文件，文件传输协议提供的应用服务满足了我们的这种需求。FTP(File Transfer Protocol，文件传输协议)是互联网上文件传输的标准协议，FTP 使用 TCP 作为传输协议，支持用户的登录认证及访问权限的设置。互联网上另一种常用的文件传输协议是 TFTP(Trivial File Transfer Protocol)协议，TFTP 是一种简单的文件传输协议，不支持用户的登录认证，也不具备复杂的命令。TFTP 使用 UDP 作为传输协议，并具有重传机制。接下来我们将对这两种传输协议进行介绍。

23.1 本章目标

学习完本章，应该能够达到以下目标。

(1) 掌握 FTP 协议基础知识。
(2) 熟悉 FTP 协议文件传输模式。
(3) 熟悉 FTP 数据传输方式。
(4) 掌握 TFTP 协议基础知识。
(5) 掌握 FTP 与 TFTP 相关配置方法。

23.2 FTP 协议

23.2.1 FTP 协议介绍

FTP 用于在远端服务器和本地主机之间传输文件，是 IP 网络上传输文件的通用协议。在万维网(World Wide Web，WWW)出现以前，用户使用命令行方式传输文件，最通用的应用程序就是 FTP。虽然目前大多数用户在通常情况下选择使用 E-mail 和 Web 传输文件，但是 FTP 仍然有着比较广泛的应用。

FTP 采用客户端/服务器的设计模式，承载在 TCP 协议之上。FTP 功能强大，拥有丰富的命令集。FTP 支持对登录服务器的用户名和口令进行验证，可以提供交互式的文件访问，允许客户指定文件的传输类型，并且可以设定文件的存取权限。

通过 FTP 进行文件传输时，需要在服务器和客户端之间建立两个 TCP 连接：FTP 控制连接和 FTP 数据连接。FTP 控制连接负责 FTP 客户端和 FTP 服务器之间交互 FTP 控

制命令和命令执行的应答信息，在整个 FTP 会话过程中一直保持打开；而 FTP 数据连接负责在 FTP 客户端和 FTP 服务器之间进行文件和文件列表的传输，仅在需要传输数据的时候建立数据连接，数据传输完毕后终止。

FTP 服务器把文件列表通过数据连接发送到客户端，而不是在控制连接上使用多行应答。这样的好处是避免了行的有限性对文件列表大小的限制，并且用户可以把文件列表以文件的方式保存，而不仅仅只在终端上显示出来。

如图 23-1 所示，FTP 服务器启动后，FTP 服务打开 TCP 端口号 21 作为侦听端口，等待客户端的连接。客户端随机选择一个 TCP 端口号作为控制连接的源端口，主动发起对 FTP 服务器端口号 21 的 TCP 连接。控制连接建立后，FTP 客户端和 FTP 服务器之间通过该连接交互 FTP 控制命令和命令执行的应答信息。

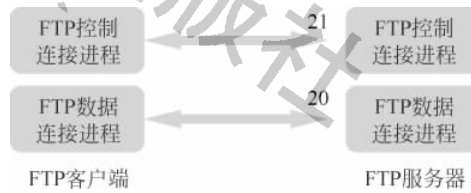

图 23-1　FTP 双连接方式

对于相同的一个文件，不同的操作系统可能会有不同的存储表达方式。为了在不同操作系统之间进行文件传输，确保文件能够准确无误地传送到对方，而不会引起格式上的误解，所以 FTP 协议定义了不同的文件传输模式，适应于传输不同类型的文件。FTP 协议共定义了 4 种文件传输模式，分别介绍如下。

1. ASCII 模式

ASCII 模式是默认的文件传输模式。发送方把本地文件转换成标准的 ASCII 码，然后在网络中传输；接收方收到文件后，根据自己的文件存储表达方式而把它转换成本地文件。ASCII 文件传输模式通常适用于传输文本文件。

2. 二进制模式

二进制模式也称为图像文件传输模式。发送方不做任何转换，把文件按照比特流的方式进行传输。二进制文件类型通常适用于传送程序文件。

3. EBCDIC 模式

EBCDIC 模式要求文件传输的两端都是 EBCDIC 系统。

4. 本地文件模式

本地文件模式是在具有不同字节大小的主机间传输二进制文件。每一字节的比特数由发送方规定。对使用 8 位字节的系统来说，本地文件以 8 位字节传输就等同于二进制文件传输。

在 4 种文件传输模式中，ASCII 模式和二进制模式是使用最广泛的两种传输模式，几乎所有 FTP 服务器都支持这两种文件类型，而 EBCDIC 和本地文件模式已经基本不再使用，因此大部分服务器都不提供这两种模式的支持。

23.2.2　FTP 数据传输方式

在 FTP 数据连接过程中，有两种数据传输方式：主动方式和被动方式。

FTP 主动传输方式也称为 PORT 方式，是 FTP 协议最初定义的数据传输方式。采用主动方式建立数据连接时，FTP 客户端会通过 FTP 控制连接向 FTP 服务器发送 PORT 命令，PORT 命令携带如下格式的参数(A1，A2，A3，A4，P1，P2)。其中 A1，A2，A3，A4 表示

需要建立数据连接的主机 IP 地址；而 P1 和 P2 表示客户端用于传输数据的临时端口号，临时端口号的数值为 256×P1＋P2。当需要传送数据时，服务器通过 TCP 端口号 20 与客户端提供的临时端口建立数据传输通道，完成数据传输。在整个过程中，由于服务器在建立数据连接时主动发起连接，因此被称为主动模式。

1. FTP 主动方式建立连接过程

FTP 主动方式建立连接的过程如下。

阶段一：建立控制通道 TCP 连接，如图 23-2 所示。

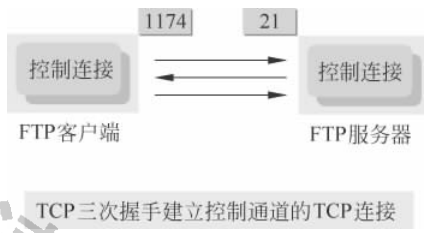

图 23-2 FTP 主动方式阶段一

(1) FTP 客户端以随机端口(图 23-2 中是 1174)作为源端口，向 FTP 服务器的 TCP 端口 21 发送一个 TCP SYN 报文，开始建立 TCP 连接。

(2) FTP 服务器收到 SYN 报文后发送 SYN ACK 报文给客户端，源端口为 TCP 端口 21，目的端口为 FTP 客户端使用的随机端口 1174。

(3) FTP 客户端收到 FTP 服务器发送的 SYN ACK 报文后，向 FTP 服务器回送一个 ACK 报文，完成 TCP 三次握手，建立 FTP 控制连接。

阶段二：主动方式参数传递，如图 23-3 所示。

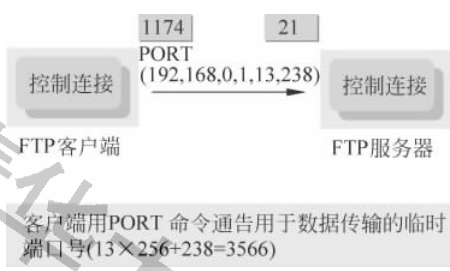

图 23-3 FTP 主动方式阶段二

当 FTP 客户端希望请求文件列表或者需要同服务器进行文件传输时，FTP 客户端会通过已经建立好的控制通道向服务器发送 PORT 命令，命令中包含了自己的 IP 地址和端口号。在图 23-3 中，IP 地址是 192.168.0.1，端口号是 13×256＋238＝3566。

阶段三：建立数据通道 TCP 连接，如图 23-4 所示。

(1) FTP 服务器向 FTP 客户端发送一个 SYN 报文，主动建立 TCP 连接。通信的源端口为 FTP 服务器的 TCP 端口号 20，目的端口为客户端在 PORT 命令中发送给服务器的端口号 3566。

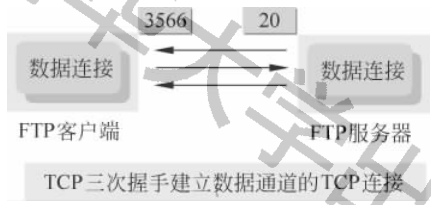

图 23-4　FTP 主动方式阶段三

(2) FTP 客户端以端口号 3566 为源端口,20 为目的端口向 FTP 服务器发送一个 SYN ACK 报文。

(3) FTP 服务器端向 FTP 客户端发送一个 ACK 报文,完成 TCP 三次握手,建立数据通道的 TCP 连接。

阶段四:数据传输,如图 23-5 所示。

图 23-5　FTP 主动方式阶段四

(1) 数据通道连接建立后,FTP 客户端与 FTP 服务器利用该通道进行数据的传输。

(2) 数据传输完毕后,由发送数据的一方发送 FIN 报文,关闭这条数据连接。如果 FTP 客户端需要打开新的数据连接,则可以通过控制通道发送相关命令再次建立新的数据传输通道。

如果客户端处于防火墙内部,主动方式可能会遇到问题。因为客户端提供的端口号是随机的,防火墙并不知道。而为了安全起见,通常防火墙只会允许外部主机访问部分内部已知端口,阻断对内部随机端口的访问,从而造成无法建立 FTP 数据连接。此时,需要使用 FTP 被动方式来进行文件传输。

被动方式也称为 PASV 方式。FTP 控制通道建立后,希望通过被动方式建立数据传输通道的 FTP 客户端会利用控制通道向 FTP 服务器发送 PASV 命令,告诉服务器进入被动方式传输。服务器选择临时端口号并告知客户端,一般采用如下形式命令:Entering Passive Mode(A1,A2,A3,A4,P1,P2)。其中 A1,A2,A3,A4 表示服务器的 IP 地址;P1,P2 表示服务器的临时端口号,数值为 256×P1+P2。当需要传送数据时,客户端主动与服务器的临时端口建立数据传输通道,并完成数据传输。在整个过程中,由于服务器总是被动接收客户端的数据连接,因此被称为被动方式。

采用被动方式时,两个连接都由客户端发起。一般防火墙不会限制从内部的客户端发出的连接,所以这样就解决了在主动方式下防火墙阻断外部发起的连接而造成无法进行数据传输的问题。

2. FTP 被动方式建立连接过程

FTP 被动方式建立连接的过程如下。

阶段一：建立控制通道 TCP 连接，如图 23-6 所示。

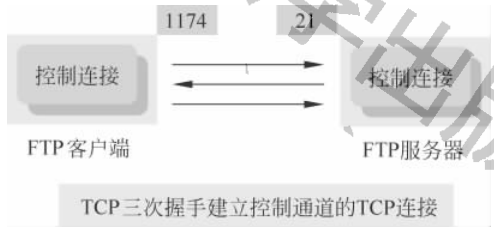

图 23-6 FTP 被动方式阶段一

(1) FTP 客户端以随机选择的临时端口号(图 23-6 中是 1174)作为源端口向 FTP 服务器 TCP 21 端口发送一个 TCP SYN 报文，开始建立 TCP 连接。

(2) FTP 服务器收到 SYN 报文后发送 SYN ACK 报文给客户端，源端口为 TCP 21 端口，目的端口为 FTP 客户端使用的随机端口号 1174。

(3) FTP 客户端收到 FTP 服务器发送的 SYN ACK 报文后，向 FTP 服务器回送一个 ACK 报文，完成 TCP 三次握手建立 FTP 控制连接。

阶段二：被动方式参数传递，如图 23-7 所示。

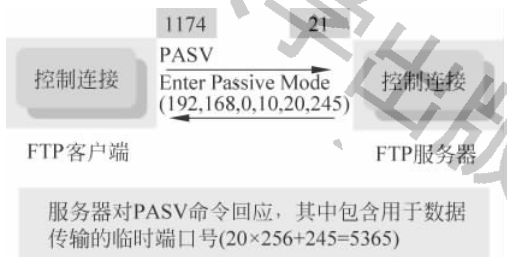

图 23-7 FTP 被动方式阶段二

当 FTP 客户端希望请求文件列表或者需要同服务器进行文件传输时，FTP 客户端会通过已经建立好的控制通道向服务器发送 PASV 命令，告诉服务器进入被动模式。服务器对客户端的 PASV 命令应答，应答中包含了服务器的 IP 地址和一个临时端口信息。在图 23-7 中，IP 地址是 192.168.0.10，端口号是 20×256+245=5365。

阶段三：建立数据通道 TCP 连接，如图 23-8 所示。

图 23-8 FTP 被动方式阶段三

(1) 此时,FTP 客户端已经得知 FTP 服务器使用的临时端口号是 5365。FTP 客户端以随机选择的临时端口号(图 23-8 中是 3789)作为源端口,向 FTP 服务器的端口 5365 发送一个 SYN 报文,主动建立 TCP 连接。

(2) FTP 服务器端发送 SYN ACK 给 FTP 客户端,目的端口为客户端自己选择的端口 3789,源端口为 5365。

(3) FTP 客户端向 FTP 服务器端发送 ACK 消息,完成 TCP 三次握手,建立数据通道的 TCP 连接。

阶段四:数据传输,如图 23-9 所示。

图 23-9　FTP 被动方式阶段四

(1) 数据通道连接建立后,FTP 客户端与 FTP 服务器利用该通道进行数据的传输。

(2) 数据传输完毕后,由发送数据的一方发送 FIN 报文,关闭这条数据连接。如果 FTP 客户端需要打开新的数据连接,则可以通过控制通道发送相关命令再次建立新的数据传输通道。

23.3　TFTP 协议

23.3.1　TFTP 协议介绍

TFTP 也是用于在远端服务器和本地主机之间传输文件的,相对于 FTP,TFTP 没有复杂的交互存取接口和认证控制,适用于客户端和服务器之间不需要复杂交互的环境。

TFTP 采用客户端/服务器设计方式,承载在 UDP 协议上,TFTP 服务器使用众所周知的端口号 69 侦听 TFTP 连接。由于 UDP 本身不能提供可靠的数据传输,因此 TFTP 使用自己设计的超时重传机制确保数据正确传送。TFTP 只能提供简单的文件传输能力,包括文件的上传和下载。TFTP 也不像 FTP 那样拥有一个庞大的命令集,不支持文件目录列表功能,也不能对用户的身份进行验证和授权。

TFTP 协议传输是由客户端发起的。当需要下载文件时,由客户端向 TFTP 服务器发送读请求包,然后从服务器接收数据,并向服务器发送确认;当需要上传文件时,由客户端向 TFTP 服务器发送写请求包,然后向服务器发送数据,并接收服务器的确认。

与 FTP 类似,TFTP 传输文件有两种模式:netascii 模式和 octet 模式。octet 传输模式对应于 FTP 中的二进制模式,用于传输程序文件;netascii 模式对应于 FTP 中的 ASCII 模式,用于传输文本文件。

23.3.2 TFTP 协议报文

TFTP 共有 5 种协议数据报文，分别为读请求报文、写请求报文、数据报文、确认报文和错误报文。每种报文的头两个字节是操作码字段。对于读请求(RRQ)和写请求(WRQ)，操作码字段分别为 1 和 2，文件名字段说明客户要读或写的位于服务器上的文件，文件名字段以 0 字节作为结束。方式字段填写的是一个 ASCII 码字符串 netascii 或 octet(可大小写任意组合)，同样以 0 字节结束。操作码为 3 的报文是数据报文，数据报文中包含两个字节的块编号，块编号需要在确认报文中使用。操作码为 4 的报文是数据的确认报文。操作码为 5 的报文是差错报文，它用于服务器不能处理读请求或写请求的情况。在文件传输过程中读和写差错也会导致传送这种报文，数据传输随即停止，差错报文不会被确认，也不会重传。

23.3.3 TFTP 文件传输过程

TFTP 进行文件传输时，将待传输文件看成由多个连续的文件块组成。每一个 TFTP 数据报文中包含一个文件块，同时对应一个文件块编号。每次发完一个文件块后就等待对方的确认，确认时应指明所确认的块编号。发送方发完数据后如果在规定的时间内收不到对端的确认那么发送方就要重新发送数据。发送确认的一方如果在规定时间内没有收到下一个文件块数据，则重发确认报文。这种方式可以确保文件的传送不会因某一数据的丢失而失败。

每次 TFTP 发送的数据报文中包含的文件块大小固定为 512 字节，如果文件长度恰好是 512 字节的整数倍，那么在文件传送完毕后，发送方还必须在最后发送一个不包含数据的数据报文，用来表明文件传输完毕。如果文件长度不是 512 字节的整数倍，那么最后传送的数据报文所包含的文件块肯定小于 512 字节，这正好作为文件结束的标志。

TFTP 的文件传输过程以 TFTP 客户端向 TFTP 服务器发送一个读请求或写请求开始。读请求表示 TFTP 客户端需要从 TFTP 服务器下载文件，写请求表示客户端需要向服务器上传文件。

如图 23-10 所示，TFTP 客户端需要从 TFTP 服务器下载文件时，会向 TFTP 服务器发送一个读请求报文，包含需要下载的文件名信息和文件传输的模式(netascii 或 octet)。如果这个文件可以被客户端下载，那么服务器回应一个数据报文，报文中包括文件的第一个文件块，块编号为 1。客户端收到块编号为 1 的数据报文后，返回一个确认报文，报文中的块编号为 1。服务器收到确认后继续发送块编号为 2 的数据报文，客户端回应块编号为 2 的

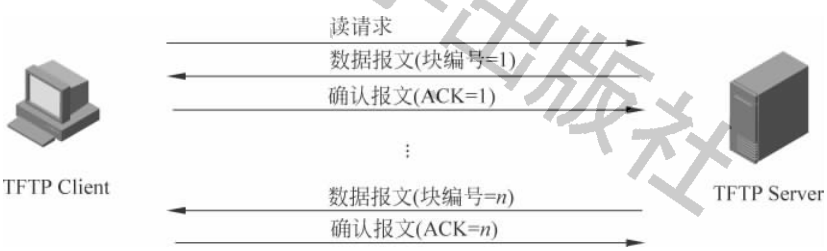

图 23-10 TFTP 下载文件过程

确认报文。这个过程周而复始，直至文件全部传输完毕。除了最后一个数据报文可含有不足 512 字节的数据，其他每个数据报文均含有 512 字节的数据。当客户端收到一个不足 512 字节的数据报文后，就知道它收到了最后一个数据分组。

如图 23-11 所示，TFTP 客户端需要向 TFTP 服务器上传文件时，会向 TFTP 服务器发送一个写请求报文，包含需要在服务器上保存的文件名信息和文件传输模式（netascii 或 octet）。如果这个文件可以被客户端上传，那么服务器回应一个块编号为 0 的确认报文。客户端继续发送块编号为 1 的数据报文，服务器返回块编号为 1 的确认报文。然后客户端继续发送块编号为 2 的数据报文，服务器返回块编号为 2 的确认报文。以此类推，直至文件全部传输完毕。

图 23-11　TFTP 上传文件过程

23.4　配置 FTP 与 TFTP

23.4.1　FTP 客户端配置

路由器可以作为 FTP 客户端，建立设备与远程 FTP 服务器的连接，访问远程 FTP 服务器上的文件。

在用户视图下用以下命令来登录远程 FTP 服务器。

ftp *ftp-server* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** { *interface-name* | *interface-type interface-number* } | **ip** *source-ip-address* }]

命令中常见参数含义如下所述。

（1）*ftp-server*：FTP 服务器的主机名或 IP 地址。

（2）*service-port*：远端设备提供 FTP 服务的 TCP 端口号，取值范围为 0～65535，默认值为 21。

（3）**vpn-instance** *vpn-instance-name*：指定 FTP 服务器所属的 VPN。

（4）**source**{ **interface** {*interface-name*|*interface-type interface-number*} | **ip** *source-ip-address* }：指定建立 FTP 连接时使用的源地址。

在上述命令中，如果不指定任何参数，则只进入 FTP 客户端视图，不登录 FTP 服务器。

如果指定参数，系统会提示用户输入登录 FTP 服务器的用户名和密码。如果用户名和密码正确，则登录成功，并进入 FTP 客户端视图；否则，登录失败。

在登录到 FTP 服务器后，通常会查看服务器上的目录和文件，以确定需要下载的文件名。在 FTP 视图下查看 FTP 服务器上目录和文件，其命令如下：

ls remotefile [*localfile*]

然后可以指定所需要下载的文件和下载到本地后的文件名,其命令如下:

get remotefile [*localfile*]

也可以上传本地文件到远程 FTP 服务器上,命令如下:

put *localfile* [*remotefile*]

在下载完成后,在 FTP 视图下用命令断开与 FTP 服务器之间的连接。

bye

其他会经常使用的命令如表 23-1 所示。

表 23-1 其他常用命令表

命 令	操 作
binary	设置 FTP 文件传输的模式为二进制模式
pwd	显示远程 FTP 服务器上的工作目录
cd pathname	切换远程 FTP 服务器上的工作路径
put localfile [remotefile]	上传本地文件到远程 FTP 服务器

23.4.2 FTP 服务器端配置

当路由器作为 FTP 服务器时,可进行如下配置。

第 1 步:在系统视图下启动 FTP 服务器功能。

ftp server enable

因为默认情况下,FTP 服务器功能处于关闭状态,所以必须使能 FTP 服务。

第 2 步:创建本地用户并设置相应的密码、服务类型、权限级别等参数。

创建本地用户并进入本地用户视图。

local-user *user-name* [**class** { **manage** | **network** }]

在本地用户视图下设置当前本地用户的密码。

password { **hash** | **simple** } *password*

在本地用户视图下设置服务类型。

service-type { **ftp** | { **ssh** | **telnet** | **terminal** } }

23.4.3 FTP 配置示例

图 23-12 为配置路由器作为服务器端和客户端的示例。图中作为 FTP 服务器的路由器接口 IP 地址是 10.0.0.1。

配置路由器作为 FTP 服务器端。