Your Short Cut to Knowledge

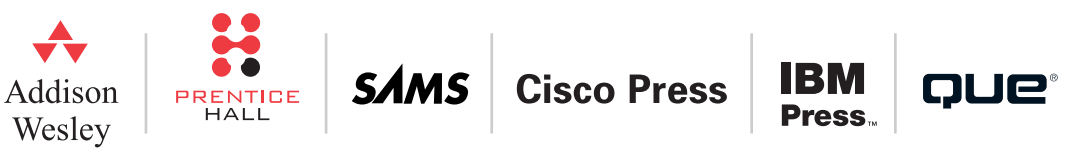
The following is an excerpt from a Short Cut published by one of the Pearson Education imprints.

Short Cuts are short, concise, PDF documents designed specifically for busy technical professionals like you.

We've provided this excerpt to help you review the product before you purchase. Please note, the hyperlinks contained within this excerpt have been deactivated.

Tap into learning—NOW!

Visit **www.informit.com/shortcuts** for a complete list of Short Cuts.



Application Protocols

HTTP

- HTTP is a request/response protocol between clients (user agents) and servers (origin servers).
- An HTTP client initiates a request by establishing a TCP connection to a particular port on a remote host (port 80 by default). Resources to be accessed by HTTP are identified using Uniform Resource Identifiers (URI or URL) using the http: or https: URI schemes.
- HTTP supports authentication between clients and servers, which involves sending a clear-text password (therefore, it is not considered secure). HTTP is disabled by default on Cisco routers but can be enabled for remote monitoring and configuration.

Configuring HTTP

- Use the **ip http access-class** command to restrict access to certain selected IP addresses and **ip http authentication** to allow only certain users to access the Cisco router via HTTP.
- If you choose to use HTTP for management, issue the **ip http access-class** *access-list-number* command to restrict access to appropriate IP addresses. As with interactive logins, the best choice for HTTP authentication is to use a TACACS+ or RADIUS server. Avoid the use of the enable password as an HTTP password.
- The **ip http server** command is used to enable an HTTP server. If a secure HTTP connection is required, **ip http secure-server** needs to be configured on the router. The default port 80 can be changed by using the command **ip http port** *port-number*. Varying forms of authentication for login can be set using the **ip http authentication** [**enable | local | tacacs**] command. However, the default login method is to enter the hostname as the username and the enable or secret password as the password. If local authentication is specified by using **username** *username* **privilege** [**0**-**15**] **password** *password*, the access level on the Cisco router is determined by the privilege level assigned to that user.

Simple Mail Transfer Protocol

- Simple Mail Transfer Protocol (SMTP) is a text-based protocol usually used by two mail servers to exchange e-mail whereby users can retrieve this mail by using any mail clients such as Outlook, Eudora, or Pine. Mail clients use various protocols such as Post Office Protocol 3 (POP3) to connect to the server.

- SMTP uses well-known ports TCP port 25 and UDP port 25. The client and SMTP server send various commands when communicating. Table 3-1 lists some of the SMTP commands and their purpose.

TABLE 3-1 SMTP commands

Command	Function
HELLO (HELO)	Identifies the SMTP client to the SMTP server.
MAIL (MAIL)	Initiates a mail transaction in which the mail data is delivered to an SMTP server, which is then either delivered to mailboxes or passed to another system via SMTP.
RECIPIENT (RCPT)	Identifies an individual recipient of the mail data; multiple use of the command is needed for multiple users.
DATA (DATA)	Identifies the lines following the command (such as the MAIL command) as the mail data in ASCII character codes.
SEND (SEND)	Initiates a mail transaction in which the mail data is delivered to one or more terminals.
SEND OR MAIL (SOML)	Initiates a mail transaction in which the mail data is delivered to one or more terminals or mailboxes.
SEND AND MAIL (SAML)	Initiates a mail transaction in which the mail data is delivered to one or more terminals and mailboxes.
RESET (RSET)	Aborts the current mail transaction. Any stored sender, recipients, and mail data must be discarded, and all buffers and state tables must be cleared. The receiver must send an OK reply.
VERIFY (VRFY)	Verifies whether a user exists; a fully specified mailbox and name are returned.
NOOP (NOOP)	Specifies no action other than that the receiver sent an OK reply.
QUIT (QUIT)	Closes the transmission channel; the receiver must send an OK reply.

FTP

FTP allows users to transfer files from one host to another. FTP is a TCP-based connection-oriented protocol and uses port 21 to open the connection and port 20 to transfer data. FTP uses clear-text authentication. FTP clients can be configured for two modes of operation, PORT (active) mode and PASV (passive) mode.

Figure 3-1 shows an overview of FTP modes of operation between an FTP client and FTP server for both the active and passive mode.

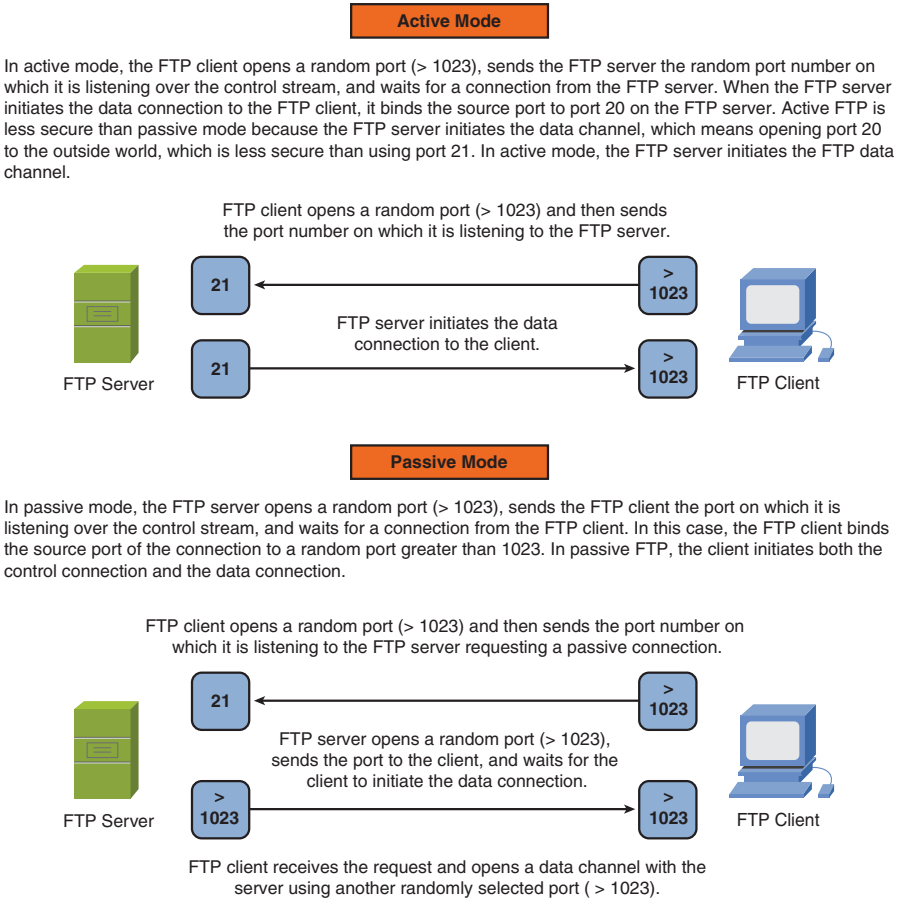


FIGURE 3-1 Overview of FTP operation and operating modes

Domain Name System

Domain Name System (DNS) is a name resolution protocol used to translate hostnames to IP addresses and vice versa. A DNS server is a host that is running the DNS service, and it is configured to do the translation for the user transparently using TCP/UDP port 53. TCP port 53 is also used for DNS zone transfers. UDP 53 is used for DNS lookups and browsing.

DNS is a hierarchical database where the data is structured in a tree, with the root domain, ".", at the top, and various subdomains branch out from the root much like the directory structure of a UNIX or Windows file system. Cisco routers can be configured for DNS so that users can simply type a hostname versus an IP address. Local names can also be configured for devices. A name server stores information about its domain in the form of several different kinds of resource records, each of which stores a different kind of information about the domain and the hosts in the domain. Resource records are traditionally text entries stored in different files on the domain name server. The Cisco DNM Browser is a graphical utility that enables you to edit these records via a graphical interface, reducing the chance of errors in the text files. A router will not provide DNS server responses to client devices such as PCs or UNIX hosts. Table 3-2 describes the different record types.

TABLE 3-2 Different record types

Record type	Function
Start of Authority (SOA)	Required for every domain. Stores information about DNS itself for the domain.
Name Server (NS)	Stores information used to identify the name servers in the domain that store information for that domain.
Address (A)	Stores the hostname and IP address of individual hosts and is used to translate hostnames to IP addresses.
Canonical Name (CNAME)	Stores additional hostnames, or aliases, for hosts in the domain.
Mail Exchange (MX)	Stores information about where mail for the domain should be delivered.
Pointer (PTR)	Stores the IP address and hostname of individual hosts and is used to translate IP addresses to hostnames in a reverse DNS lookup.
Host Information (HINFO)	Stores information about the hardware for specific hosts.
Well Known Services (WKS)	Stores information about the various network services available from hosts in the domain.
Text Information (TXT)	Stores up to 256 characters of text per line.
Responsible Person (RP)	Stores information about the person responsible for the domain.

TFTP

TFTP uses UDP port 69 to transfer files between devices. Data transfer occurs between two UDP ports, where one is the source and the other the destination. TFTP is considered to possess weak security because the TFTP packet has no fields to authenticate with username and password. Therefore, security is enabled by predefinition of directories and filenames of files to be transferred to the TFTP server. This allows the remote hosts to transfer the file to the remote TFTP client. Security is reliant on the application and not the operating system. TFTP is widely used for upgrading Cisco IOS images on Cisco routers, Cisco switches, and Cisco security devices.

Network Time Protocol

Network Time Protocol (NTP) is used for accurate timekeeping and can, for example, reference atomic clocks that are present on the Internet. NTP is capable of synchronizing clocks within milliseconds and is a useful protocol when reporting error logs (for instance, from Cisco routers, Cisco switches, and Cisco security devices). NTP is useful for security/incident event correlation across multiple security devices and helps to determine the exact time of the event. For NTP, the defined ports are UDP port 123 (connectionless) and TCP port 123 (guaranteed, connection-oriented). NTP applications typically use only UDP port 123.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) is a protocol that defines the method by which data stored in a directory is accessed and how the data is represented in the directory service. Finally, LDAP defines how data is added and exported using LDIF. LDAP runs over TCP/IP or other connection-oriented protocols. RFC 2251 defines the functional specifications of LDAP. LDAP stores information where each entry is a collection of predefined attributes that has a globally unique DN (distinguished name). The DN enables reference to unique records. Directory structure in LDAP is similar to DNS, with a tree structure with the root at the head of the tree. Refer to the RFC for more information about LDAP models. LDAP is based on the client/server model. The server farm of LDAP servers constitutes the directory information tree (DIT). When the client queries the DIT for information, the DIT either responds or relays the query to another LDAP server in the DIT.

Syslog

Syslog is typically used for computer system management and security auditing. Using syslog, the sender sends a small text message that is less than 124 bytes to the syslog receiver or server. These messages can be sent via UDP or TCP. By default, Cisco routers send syslog messages to their logging server with a default facility of *local7*. The messages can be logged to the console, monitor, syslog server, or internal buffer. Logging levels can also be set when logging messages. Table 3-3 describes the logging levels and keywords that can be used to set the logging levels. The highest level of message is level 0, emergencies. The lowest level is level 7, debugging, which also displays the greatest number of messages.

TABLE 3-3 Message logging keywords and levels

Level	Keyword	Description
0	**emergencies**	System is unusable.
1	**alerts**	Immediate action is needed.
2	**critical**	Critical condition exists.
3	**errors**	Error condition exists.
4	**warnings**	Warning condition exists.
5	**notification**	Normal but significant condition exists.
6	**informational**	Informational messages.
7	**debugging**	Debugging messages.