System Administration Guide, Volume 3

Previous: Protocol Layers and the OSI Model **Next**: How the TCP/IP Protocols Handle Data Communications

TCP/IP Protocol Architecture Model

The OSI model describes an idealized network communications protocol family. TCP/IP does not correspond to this model directly, as it either combines several OSI layers into a single layer, or does not use certain layers at all. The following table shows the layers of the Solaris implementation of TCP/IP, listed from topmost layer (application) to lowest (physical network).

Table 4-2 TCP/IP Protocol Stack

OSI Ref. Layer No.	**OSI Layer Equivalent**	**TCP/IP Layer**	**TCP/IP Protocol Examples**
5,6,7	Application, Session, Presentation	Application	NFS, NIS+, DNS, `telnet` , `ftp` , `rlogin` , `rsh` , `rcp` , RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP
3	Network	Internet	IP, ARP, ICMP
2	Data Link	Data Link	PPP, IEEE 802.2
1	Physical	Physical Network	Ethernet (IEEE 802.3) Token Ring, RS-232, others

The table shows the TCP/IP protocol layers, their OSI Model equivalents, and examples of the protocols available at each level of the TCP/IP protocol stack. Each host involved in a communication transaction runs its own implementation of the protocol stack.

Physical Network Layer

The physical network layer specifies the characteristics of the hardware to be used for the network. For example, it specifies the physical characteristics of the communications media. The physical layer of TCP/IP describes hardware standards such as IEEE 802.3, the specification for Ethernet network media, and RS-232, the specification for standard pin connectors.

Data-Link Layer

The data-link layer identifies the network protocol type of the packet, in this case TCP/IP. It also provides error control and "framing." Examples of data-link layer protocols are Ethernet IEEE 802.2 framing and Point-to-Point Protocol (PPP) framing.

Internet Layer

This layer, also known as the network layer, accepts and delivers packets for the network. It includes the powerful Internet protocol (IP), the Address Resolution Protocol (ARP) protocol, and the Internet Control Message Protocol (ICMP) protocol.

IP Protocol

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for:

- **IP addressing** - The IP addressing conventions are part of the IP protocol. (Chapter 5, Planning Your TCP/IP Network describes IPv4 addressing in detail and Chapter 14, Overview of IPv6 describes IPv6 addressing in detail.)
- **Host-to-host communications** - IP determines the path a packet must take, based on the receiving host's IP address.
- **Packet formatting** - IP assembles packets into units known as **IP datagrams**. Datagrams are fully described in "Internet Layer".
- **Fragmentation** - If a packet is too large for transmission over the network media, IP on the sending host breaks the packet into smaller fragments. IP on the receiving host then reconstructs the fragments into the original packet.

Previous releases of the Solaris operating environment implemented version 4 of the Internet Protocol, which is written IPv4. However, because of the rapid growth of the Internet, it was necessary to create a new Internet Protocol with improved capabilities, such as increased address space. This new version, known as version 6, is written IPv6. The Solaris operating environment supports both versions, which are described in this book. To avoid confusion when addressing the Internet Protocol, the following convention is used:

- When the term IP is used in a description, the description applies to both IPv4 and IPv6.
- When the term IPv4 is used in a description, the description applies only to IPv4.
- When the term IPv6 is used in a description, the description applies only to IPv6.

ARP Protocol

The Address Resolution Protocol (ARP) conceptually exists between the data link and Internet layers. ARP assists IP in directing datagrams to the appropriate receiving host by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

ICMP Protocol

Internet Control Message Protocol (ICMP) is the protocol responsible for detecting network error conditions and reporting on them. ICMP reports on:

- Dropped packets (when packets are arriving too fast to be processed)
- Connectivity failure (when a destination host can't be reached)
- Redirection (which tells a sending host to use another router)

The " `ping` Command" contains more information on the operating system commands that use ICMP for error detection.

Transport Layer

The TCP/IP transport layer protocols ensure that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets. This type of communication is known as "end-to-end." Transport layer protocols at this level are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

TCP Protocol

TCP enables applications to communicate with each other as though connected by a physical circuit. TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discreet packets. This transmission consists of a starting point, which opens the connection, the entire transmission in byte order, and an ending point, which closes the connection.

TCP attaches a header onto the transmitted data. This header contains a large number of parameters that help processes on the sending machine connect to peer processes on the receiving machine.

TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts. TCP is therefore considered a "reliable, connection-oriented" protocol.

UDP Protocol

UDP, the other transport layer protocol, provides datagram delivery service. It does not provide any means of verifying that connection was ever achieved between receiving and sending hosts. Because UDP eliminates the processes of establishing and verifying connections, applications that send small amounts of data use it rather than TCP.

Application Layer

The application layer defines standard Internet services and network applications that anyone can use. These services work with the transport layer to send and receive data. There are many applications layer protocols, some of which you probably already use. Some of the protocols include:

- Standard TCP/IP services such as the `ftp` , `tftp` , and `telnet` commands
- UNIX "r" commands, such as `rlogin` and `rsh`

- Name services, such as NIS+ and Domain Name System (DNS)
- File services, such as the NFS service
- Simple Network Management Protocol (SNMP), which enables network management
- RIP and RDISC routing protocols

Standard TCP/IP Services

- **FTP and Anonymous FTP** - The File Transfer Protocol (FTP) transfers files to and from a remote network. The protocol includes the `ftp` command (local machine) and the `in.ftpd` daemon (remote machine). FTP enables a user to specify the name of the remote host and file transfer command options on the local host's command line. The `in.ftpd` daemon on the remote host then handles the requests from the local host. Unlike `rcp`, `ftp` works even when the remote computer does not run a UNIX-based operating system. A user must log in to the remote computer to make an `ftp` connection unless it has been set up to allow anonymous FTP.

  You can now obtain a wealth of materials from **anonymous FTP servers** connected to the Internet. These servers are set up by universities and other institutions to make certain software, research papers, and other information available to the public domain. When you log in to this type of server, you use the login name `anonymous`, hence the term "anonymous FTP servers."

  Using anonymous FTP and setting up anonymous FTP servers is outside the scope of this manual. However, many trade books, such as **The Whole Internet User's Guide & Catalog**, discuss anonymous FTP in detail. Instructions for using FTP to reach standard machines are in *System Administration Guide, Volume 1*. The ftp(1) man page describes all `ftp` command options, including those invoked through the command interpreter. The ftpd(1M) man page describes the services provided by the daemon `in.ftpd`.

- **Telnet** - The Telnet protocol enables terminals and terminal-oriented processes to communicate on a network running TCP/IP. It is implemented as the program `telnet` (on local machines) and the daemon `in.telnet` (on remote machines). Telnet provides a user interface through which two hosts can communicate on a character-by-character or line-by-line basis. The application includes a set of commands that are fully documented in the telnet(1) man page.

- **TFTP** - The trivial file transfer protocol (`tftp`) provides functions similar to `ftp`, but it does not establish `ftp`'s interactive connection. As a result, users cannot list the contents of a directory or change directories. This means that a user must know the full name of the file to be copied. The tftp(1) man page describes the `tftp` command set.

UNIX "r" Commands

The UNIX "r" commands enable users to issue commands on their local machines that are actually carried out on the remote host that they specify. These commands include

- `rcp`
- `rlogin`
- `rsh`

Instructions for using these commands are in rcp(1), rlogin(1), and rsh(1) man pages.

Name Services

Two name services are available from the Solaris implementation of TCP/IP: NIS+ and DNS.

- **NIS+** - NIS+ provides centralized control over network administration services, such as mapping host names to IP and Ethernet addresses, verifying passwords, and so on. See *Solaris Naming Administration Guide* for complete details.

- **Domain Name System** - The Domain Name System (DNS) provides host names to the IP address service. It also serves as a database for mail administration. For a complete description of this service, see *Solaris Naming Administration Guide*. See also the in.named(1M) man page.

File Services

The NFS application layer protocol provides file services for the Solaris operating environment. You can find complete information about the NFS service in Chapter 29, Solaris NFS Environment.

Network Administration

The Simple Network Management Protocol (SNMP) enables you to view the layout of your network, view status of key machines, and obtain complex network statistics from graphical user interface based software. Many companies offer network management packages that implement SNMP; SunNet Manager™ software is an example.

Routing Protocols

The Routing Information Protocol (RIP) and the Router Discovery Protocol (RDISC) are two routing protocols for TCP/IP networks. They are described in "Routing Protocols".

Previous: Protocol Layers and the OSI Model **Next**: How the TCP/IP Protocols Handle Data Communications