Protocols supported in Sena products

Technical Tutorial

2002 – 12 - 06

Table of Contents

1. Introduction

A Protocol defines the rules for sending blocks of data (each known as a Protocol Data Unit (PDU)) from one node in a network to another node. Protocols are normally defined in a layered manner and provide all or part of the services specified by a layer of the OSI reference model. A protocol specification defines the operation of the protocol and may also suggest how the protocol should be implemented. It consists of three parts:

- Definition of Protocol Control Information (PCI) format, which forms the PDU header
- Definition of procedures for transmitting and receiving PDUs
- Definition of services provided by the protocol layers

A protocol also defines the procedures which determine how the PDU will be processed at the transmit and receive nodes. The procedures specify the valid values for the PCI fields, and the action be taken upon reception of each PCI value (usually based on stored control information). Protocols are generally described using a layered architecture known as the OSI reference model. The purpose of this document is to give technical readers a basic overview of the Protocol specifications.

.

2. ARP

ARP (Address Resolution Protocol) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. The physical machine address is also known as a Media Access Control or MAC address

How ARP Works

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine.

If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

3. IP (Internet Protocol): -

IP (Internet Protocol) specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

How IP works

For example when you send an e-mail note or a Web page, the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

4. ICMP

ICMP (Internet Control Message Protocol) is an extension to the Internet Protocol (IP) defined by RFC 792. ICMP is a message control and error-reporting protocol between a host server and a gateway to the Internet.

For Example:

- PING command uses ICMP to test an Internet connection.
- A router uses ICMP to notify the sender that its destination node is not available.

5. TCP

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. In other words, IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

How TCP works

For example, when an HTML file is sent to you from a Web server, the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end (the client program in your computer), TCP reassembles the individual packets and waits until they have arrived to forward them to you as a single file.

6. UDP

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.

7. Telnet

Telnet is a terminal emulation protocol commonly used on the Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer. Telnet enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password.

8. DNS

Domain Name System (or Service) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

9. Dynamic DNS

Dynamic DNS is the ability to automatically update a DNS server when an IP address is automatically assigned (typically from DHCP) to a network device. A dynamic DNS (domain name system) service is a company that charges a small fee to allow a user
connecting to the Internet with a dynamic IP address.

10. HTTP

HTTP (Hyper Text Transfer Protocol) is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. In other words, HTTP is the set of rules for exchanging files.

For example, when you enter a URL like www.sena.com in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page www.sena.com. Web browsers typically default to the HTTP protocol. For example, typing www.sena.com is the same as typing http://www.sena.com.

11. SMTP

SMTP (Simple Mail Transfer Protocol) is a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP.

12. BOOTP

The Bootstrap Protocol allows a host to configure itself dynamically at boot time. This protocol provides 3 services.

a. IP address assignment.
b. Detection of the IP address for a serving machine.
c. The name of a file to be loaded and executed by the client machine.

13. DHCP

DHCP (Dynamic Host Configuration Protocol) assigns IP addresses dynamically from an IP address pool, which is managed by the network administrator. Once the user disconnects from the Internet, their dynamic IP address goes back into the IP address pool so it can be assigned to another user. Even if the user reconnects immediately, odds are they will not be assigned the same IP address from the pool.

In the dynamic IP mode, users don't have to specify all the parameters manually such as IP addresses of the VTS, the network subnet mask, the gateway computer and the domain name server computers. This means VTS receives a different IP address each time it
boots up. For the DHCP environment, Dynamic DNS protocol support has been provided to the VTS. Managers may access the VTS by using domain name.

14. PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection. PPPoE can be used to have an office or building-full of users share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a local area network.

15. SNMP V1 & V2 (MIB II)

SNMP (Simple Network Management Protocol) is the protocol governing network management and the monitoring of network devices and their functions.

16. SSH

Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. Secure Shell, sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely.

SSH (Secure Shell) is a popular, robust, TCP/IP-based product for network security and privacy, supporting strong encryption and authentication.

17. Kerberos

Kerberos is designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message. Kerberos is a secure method for authenticating a request for a service in a computer network.

Briefly and approximately, here's how Kerberos works:

- Suppose you want to access a server on another computer (which you may get to by sending a Telnet or similar login request). You know that this server requires a Kerberos "ticket" before it will honor your request.
- To get your ticket, you first request authentication from the Authentication Server (AS). The Authentication Server creates a "session key" (which is also an encryption key) basing it on your password (which it can get from your user name) and a random value that represents the requested service. The session key is effectively a "ticket-granting ticket."
- You next send your ticket-granting ticket to a ticket-granting server (TGS). The TGS may be physically the same server as the Authentication Server, but it's now performing a different service. The TGS returns the ticket that can be sent to the server for the requested service.
- The service either rejects the ticket or accepts it and performs the service.
- Because the ticket you received from the TGS is time-stamped, it allows you to make additional requests using the same ticket within a certain time period (typically, eight hours) without having to be re-authenticated. Making the ticket valid for a limited time period make it less likely that someone else will be able to use it later.

18. RADIUS

Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

19. TACACS+

TACACS (Terminal Access Controller Access Control System) is an authentication protocol that was commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

In spite of its name, TACACS+ is an entirely new protocol. TACACS+ and RADIUS have generally replaced the earlier protocols in more recently built or updated networks. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP).

20. Protocols Supported in Sena Products

Below table shows the list of protocols supported by the Sena Products.

20.1. Protocols supported by HelloDevice Lite Series

Specification	HelloDevice Lite Series
Protocols Supported	ARP, IP/ICMP TCP/IP Telnet DHCP client PPPoE

20.2. Protocols supported by HelloDevice Pro Series

Specification	HelloDevice Pro Series
Protocols Supported	ARP, IP/ICMP TCP, UDP Telnet DNS, SMTP DHCP client PPPoE

20.3. Protocols supported by HelloDevice Super Series

Specification	HelloDevice Super Series
Protocols Supported	ARP, IP/ICMP TCP, UDP Telnet DNS, Dynamic DNS HTTP, SMTP DHCP client PPPoE SNMP V1 & V2

20.4. Protocols supported by IALink100

Specification	IALink100
Protocols Supported	ARP, IP/ICMP TCP, UDP Telnet DNS, SMTP DHCP client PPPoE

20.5. Protocols supported by IALink100-MODBUS

Specification	IALink100-MODBUS
Protocols Supported	ARP, IP/ICMP TCP Telnet DNS DHCP client MODBUS

20.6. Protocols supported by POSLink

Specification	POSLink
Protocols Supported	ARP, IP/ICMP TCP, UDP Telnet DHCP client PPPoE

20.7. Protocols supported by UPSLink

Specification	UPSLink
Protocols Supported	ARP, IP/ICMP TCP, UDP Telnet DNS, Dynamic DNS SMTP DHCP client PPPoE NTP

20.8. Protocols supported by VTS

Specification	VTS
Protocols Supported	ARP, IP/ICMP TCP, UDP Telnet DNS, Dynamic DNS HTTP, SMTP BOOTP/DHCP client PPPoE, SSH, Kerberos, TACACS+, LDAP SNMP V1 & V2 (MIB II)