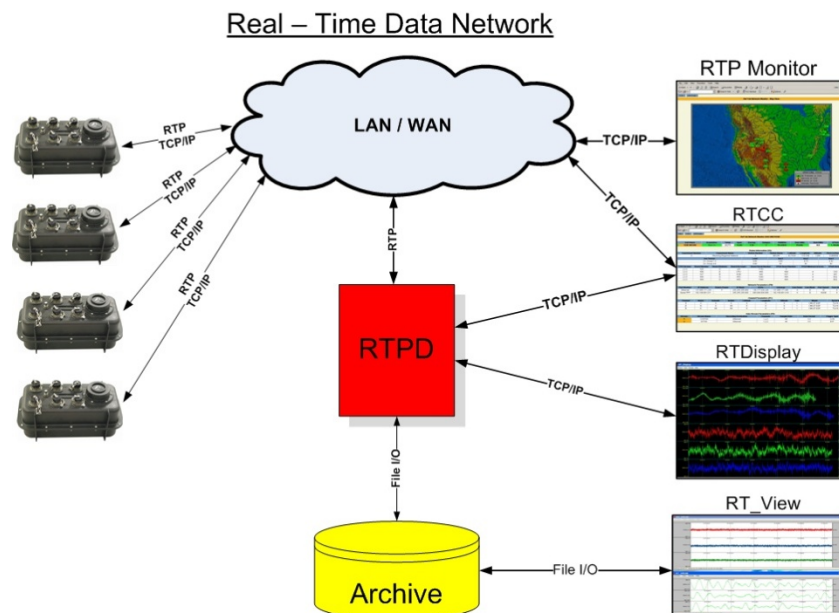


RTPD Protocols

RTP and Client

Version A

5/21/2008



This REF TEK manual describes the protocols used by RTPD, the REF TEK telemetry server. REF TEK Protocol (RTP) is used to communicate between REF TEK recorders and RTPD. The RTPD Client Protocol is used by programs that attach as clients to RTPD.

Copyright© 2008 Refraction Technology, Inc.

All rights are reserved. No part of this manual may be reproduced, copied or transmitted in any form outside the approved recipient's organization without written permission from Refraction Technology Inc.

Printed in USA.

**Refraction Technology
1600 Tenth Street
Suite A
Plano, Texas 75074**

Tel: 214-440-1265

Fax: 972-578-0045
www.reftek.com

About this manual:

This RTPD Protocols Technical Reference manual provides a detailed overview of RTP and Client protocols. It covers the following broad operational topics:

- RTP Protocol
- RTPD Client Protocol

Revision History:

Revision	Date	Reason for change	Pages
0.1	03/14/08	Initial release	All
A	05/20/08	Update to new format	All

CF Card Replacement:

Due to the large variability of CF cards available on the world market and the resulting problems with compatibility due to memory layout, signal structuring and power requirements, Refraction Technology cannot guarantee a CF card will work in a REFTEK data recorder unless it is sold through REFTEK itself. REFTEK ensures compatibility through communications with CF manufacturers and rigorous in-house testing. Some CF manufacturers refuse to provide adequate information or factory controls to ensure that the product being sold today is the same as the product sold earlier under the same part number. CF cards not purchased from REFTEK may work at one temperature but not at another, or may fail all together.

Software Version:

Current software and documentation is available on our web site. Some early units may require hardware modifications to use the latest software. Contact REF TEK if you have any queries on the compatibility of your unit(s) and the current software release.

Firmware Update:

To update firmware from the FTP site

1. Login to our FTP site at: <ftp.reftek.com/pub> as:
User name: Anonymous
Password: Your E-mail address
2. Find the 130 firmware at <ftp.reftek.com/pub/130/cpu/prom>.
3. Download the zip file of the most recently released firmware version.

Update firmware:

Updating firmware in a 130 DAS requires the presence of a firmware file on an installed Compact Flash device.

1. On power-up, the 130 checks the Compact Flash for the presence of 'main.s3' in the root directory.
2. If the 'main.s3' file is present on the Compact Flash, the 130:
 - a. Reads the file.
 - b. DELETES the file.
 - c. Re-programs the internal flash memory.

Note: DO NOT DISTURB THE UNIT DURING THIS PROCESS.

Follow these steps to update the firmware of a 130 DAS:

1. Unzip the 'main.s3' file from the downloaded zip file of the most recently released firmware.
2. Copy the desired firmware image to the root of the Compact Flash as 'main.s3' using a PC with a Compact Flash reader or ftp into the 130 DAS, with a Compact Flash installed, in binary mode.
3. With the Compact Flash with the main.s3 image installed in the 130 DAS, issue a reset command.

(a) If you are at the 130 DAS:

1. Issue a Reset command from a PDA running PFC_130 or Physically disconnect and reconnect power to the unit.
2. Observe the LCD for the following messages:

READING DISK DO NOT DISTURB
WRITING FLASH DO NOT DISTURB

3. The 130 DAS resets and returns to normal messaging.

(b) If you are remotely connected to a 130 DAS via telemetry mode:

1. If you are connecting remotely by a TCP connection:
 - a. **First connect**
 - b. **Discover the unit**
 - c. **Acquire status**
2. Issue a reset command from the Status screen.
3. Delete the unit from the Station List screen.
4. Wait at least 5 minutes.
5. At the Connections screen (reconnect id using a TCP connection) issue a Station Discovery again to discover the 130 DAS station.

Note: DO NOT DISTURB THE UNIT until the start-up LCD message reappears.

Notation Conventions

The following notation conventions are used throughout Ref Tek documentation:

Notation	Description
ASCII	Indicates the entry conforms to the American Standard Code for Information Interchange definition of character (text) information.
Binary	Indicates the entry is a raw, numeric value.
Hex	Indicates hexadecimal notation. This is used with both ASCII characters (0 – 9, A – F) and numeric values.
BCD	Indicates the entry is a numeric value where each four bits represents a decimal digit.
FPn	Indicates the entry is the ASCII representation of a floating-point number with n places following the decimal point.
<n>	Indicates a single 8-bit byte. When the contents are numeric, it indicates a hexadecimal numeric value; i.e. <84> represents hexadecimal 84 (132 decimal). When the contents are capital letters, it represents a named ASCII control character; i.e. <SP> represents a space character, <CR> represents a carriage return character and <LF> represents a line feed character.
MSB	Most Significant Byte of a multi-byte value.
MSbit	Most Significant Bit of a binary number.
LSB	Least Significant Byte of a multi-byte value.
LSbit	Least Significant Bit (bit 0) of a binary number.
YYYY	Year as a 4-digit number
DDD	Day of year
HH	Hour of day in 24-hour format
MM	Minutes of hour
SS	Seconds of minute
TTT	Thousandths of a second (milliseconds)
IIII	Unit ID number

n, nS	nano, nanoSecond; $10^{-9} = 0.000000001$
u, uS	micro, microSecond; $10^{-6} = 0.000001$
m, mS	milli, milliSecond; $10^{-3} = 0.001$
K, KHz	Kilo, KiloHertz; $10^3 = 1,000$
M, MHz	Mega, MegaHertz; $10^6 = 1,000,000$
G, GHz	Giga, GigaHertz; $10^9 = 1,000,000,000$
Kb, KB	Kilobit, KiloByte; $2^{10} = 1,024$
Mb, MB	Megabit, MegaByte; $2^{20} = 1,048,576$
Gb, GB	Gigabit, GigaByte; $2^{30} = 1,073,741,824$

Related Manuals:

130-SMA System Documents	Number	PDF file
130-SMA Startup (Command Line)	Doc-SMA-Ops	130SMA_startup.pdf
Data Utilities Users Guide	Doc-Datautils	130_utilities.pdf
130-SMA Command Interface	Number	PDF file
130 Cmd Line - Theory of Operations	Doc-CmdL-Theory	130_CLtheory.pdf
130 Cmd Line - Release Notes	Doc-CmdL-Release	130_CLRN.pdf
130 Cmd Line - Reference	Doc-CmdL-Ref	130_CLcmd.pdf
130 Cmd Line - Recording Format	Doc-CmdL-Record	130_CLrecord.pdf
130-SM GUI Users Guide	Doc-130-SMGui	RT130SM.pdf
130-SMA Board Documents	Number	PDF file
RT608-B01 3 Channel 24-Bit A/D	Doc-130-RT608	RT608r.pdf
RT608-B02 6 Channel 24-Bit A/D	Doc-130-RT608	RT608r.pdf
RT506-B04 - CPU	Doc-130-RT506	RT506r.pdf
RT530 - B01 Lid Interconnect	Doc-130-RT530	RT530r.pdf
RT570 - B01 MicroDrive/Flash	Doc-130-RT570	RT570rB01.pdf
RT535 - Mass Memory Board	Doc-130-RT535	RT535rB01.pdf
Optional Manuals	Number	PDF file
SNDP Installation and Users Guide	SNDP-OP-003	SNDPUser.pdf
SNDP Reference Guide	SNDP-S-002	SNDPRef.pdf
RTCC Command / Control Users Guide	RTCC-S-006	RTCC.pdf
RT_Display Users Guide	RTD-S-007	RTDisplay.pdf
RT_View Users Guide	RTV-S-005	RTView.pdf
RTPMonitor Installation and Users Guide	RTPM-S-008	RTPM.pdf
RTPD Installation and Users Guide	RTPD-OP-005	RTPD.pdf
(part of RTPD manual) RTP Protocol		
Accelerometers		
131A-02/3 3G Triaxial Accelerometer	Doc-131A-03/2	131A023.pdf
131A-02/2 3G Triaxial Accelerometer	Doc-131A-02/2	131A022.pdf
131A-01/3 4G Triaxial Accelerometer	Doc-131B-01/3	131B013.pdf
131B-01/1 4G Unixial Accelerometer	Doc-131B-01/1	131B011.pdf

REF TEK Support and update notifications

As a valued user of REF TEK equipment we would like to provide the best support possible by keeping you up to date with our product updates.

If you would like to be notified of any REF TEK product updates please spend a couple of minutes to register with the REF TEK customer support team.

To register, either send an email to updates@reftek.com giving us your name and REF TEK product you currently have or fill out our online registration form at www.reftek.com/registration

Once we register your contact we will only send necessary notifications via email. The same notifications will be shown on our website's www.reftek.com/support page

**Thanks,
Your REF TEK support team**

Contents

1	RTP Protocol Reference	1
1.1	RTP Protocol	1
1.1.1	Introduction	1
1.2	Design Goals	2
1.3	Example Application	3
1.4	RTP Encapsulation.....	4
1.4.1	RTP Protocol Field	5
1.4.2	RTP Packet Codes	5
1.4.3	RTP Sequence Numbers	6
1.4.4	RTP Unit ID Field	6
1.4.5	RTP Length Field	6
1.5	RTP Operation	7
1.5.1	Phase Diagram	7
1.5.2	Down	8
1.5.3	Server Discovery	8
1.5.4	Synchronize	9
1.5.5	Up	9
1.6	RTP Server Discovery	10
1.6.1	The Discovery Process	10
1.6.2	Network Issues.....	11
1.6.3	Discovery Class Packets	12
1.7	RTP Link Synchronization	14
1.7.1	Synchronization Class Packets	14
1.7.2	The Link Synchronization Automaton	16
1.7.3	State Transition Table.....	17
1.7.4	States	18
1.7.5	Events.....	19
1.7.6	Actions	20
1.7.7	Counters and Timers	20
1.8	RTP Data Transfer.....	21
1.8.1	Data Class Packets.....	21
1.8.2	RTP Sequence Numbers	22
1.8.3	RTP Outbound Processing.....	24
1.8.4	RTP Inbound Processing.....	27
1.9	RTP Server Discovery Through Cisco Routers	29

2	RTPD Client Protocol	31
2.1	RTPD/Client Connection Overview	31
2.2	Client Connection to RTPD.....	31
2.3	Opening a Connection	32
2.3.1	Receiving Messages.....	34
2.3.2	Sending Command Packets	35
2.3.3	Connection Session	36
2.4	Closing A Connection.....	37
2.5	Other Message Payloads	38
2.6	RTP Log.....	39

Figure 1 Example Network.....	3
Figure 2 Layers VS Interfaces	3
Figure 3 RTP Connection Phases.....	7
Figure 4 RTP Sequence Space	22
Figure 5 Sequence Number Comparison to Zero	23
Figure 6 0 to 1 Compare	24



1 RTP Protocol Reference

1.1 RTP Protocol

1.1.1 Introduction

This document defines the REF TEK Protocol (RTP). **RTP** is designed to provide the application with a full-duplex, packet-oriented, reliable, transport over UDP network connections. The reader is assumed to have a working understanding of the TCP/IP protocol suite and networking concepts in general.

RTP is typically used in server-client fashion although this is by no means required. Typically there will be a server application running on a IP host somewhere on the network. Clients will attach themselves to the server to send and receive data. The client is typically an embedded system that attaches to the network through an asynchronous serial interface using Point-to-Point protocol however other interfaces will be implemented in the future. The server is typically an application program running on a host and accesses the network via UDP sockets provided by the IP stack on the local operating system.

The first implementation of **RTP** was on the RT422C Asynchronous Communications Card for the REF TEK 72A series Data Acquisition Systems (DAS) and the server application **RTPD**. **RTPD** and its associated software run on Windows 98, NT, 2000, XP ,Linux, and Solaris (Intel and Sparc). Throughout this document we will cover some of the details of this implementation and use it to illustrate various design concepts.

1.2 Design Goals

The following were the goals of the design for RTP:

- **Entirely platform independent**

All data values are stored in network byte order. Can be Implemented on any hardware platform or OS that provides an IP protocol stack.

- **Encapsulate the application data completely**

Not have any dependency on the contents of any particular application data packet. That is to say that the protocol will be completely unaware of what it is transporting to the peer. The only requirement placed on the application is that the data packet be 1024 bytes or less in size.

- **Self-contained and self-configuring at the client**

The protocol stack must discover or be assigned all necessary parameters to operate from the network. No configuration information will be stored by embedded implementations nor will any higher level application configure or control it. The higher level application simply submits data packets to be sent as they are ready and will always be willing to receive data. However, the higher level application must respond to flow control from RTP to avoid loss of data.

- **Both the server and client must initiate the connection on-demand**

When the application has data to send the connection will be established if needed simply by submitting the data packet to be sent. If the connection is down, both must respond to link establishment by the peer at all times. There does not need to be an administratively opened or closed state, it is always administratively open.

- **Recover from loss of connection without data loss**

If a client is sending data to the server and the connection is lost momentarily, it will reestablish the link and resume sending data. No data may be lost or passed on out of order by the server. Momentary loss of connection will mean less than five minutes for purposes of the protocol.

- **Deal with long, thin, pipes effectively**

It must be capable of high utilization (>90%) of slow (9.6k), high latency (>1 second), connections such as VSAT links. We will use deep queues (16 slots) and adaptive retransmission time-out to achieve this goal.

- **Small and relatively simple implementation**

It must be suitable for embedding in dedicated communications hardware for REF TEK recording systems.

- **Function at the application layer**

Uses the standard UDP Socket API on the server system. All network traffic will be UDP datagram to/from the REF TEK port number, port 2543. This port is the well-known REF TEK port and is registered with the Internet Assigned Numbers Authority (IANA) for use with both UDP and TCP. UDP broadcasts will be used only during link establishment and will not be sent more frequently than one packet every ten seconds per client.

1.3 Example Application

Throughout this document we will use the example system shown in Figure 1 to illustrate the details of **RTP**.

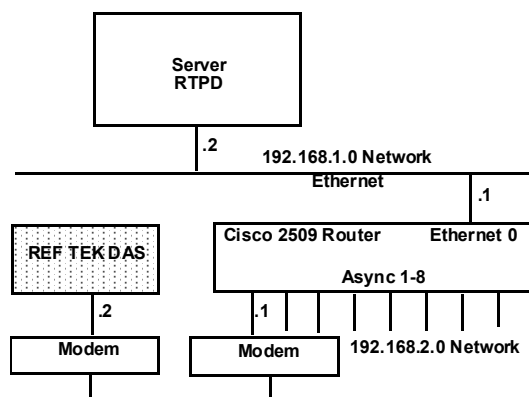


Figure 1 Example Network

This setup consists of two class C networks interconnected by a router. The client is on one network (192.168.2) and connects to the router through an asynchronous serial interface using PPP. The server is on the other network (192.168.1). The router routes traffic between the two networks.

The DAS sends its recording format data to the server as it is acquired. The server sends command format packets to the DAS and receives responses as data packets.

Figure 1 above and 2 show a schematic representation of the example network.

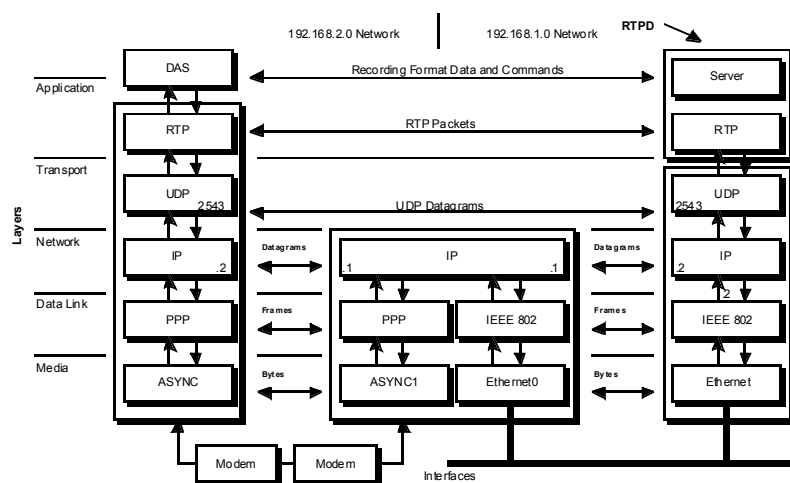


Figure 2 Layers VS Interfaces

Data from the DAS flows down through the stack to the interface at the bottom and across the wire to the router. The router forwards the packet to its Ethernet interface and on to the server. It then flows up through the stack at the server to the application.

Note: In a router packets only come up the stack to the network layer and are routed. At the transport layer and above, the client views the connection from end-to-end and is unaware of any routing or interface issues. From the network layer down, only the next-hop host is visible and at the network layer all forwarding issues are dealt with.

1.4 RTP Encapsulation

Application data is encapsulated by **RTP** for transport across the network and de-capsulated upon arrival. This is accomplished by prep ending an eight byte packet header, that contains the additional data required by the protocol to perform error-correction and various control functions, to the data packet.

The RTP header has the following form:

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	
8	Data...			

All values in any **RTP** packet are stored in network byte order. When transmitted on the network, bytes are sent from bit 0 to bit 7, multi-byte values are sent LSB first, MSB last. This is also known as big-endian byte order and is the same as specified for the entire TCP/IP protocol family.

The **RTP** packet is further encapsulated within a UDP datagram as it passes through the transport layer on its way down the protocol stack. All UDP encapsulated **RTP** packets will typically be sent to and received from the well-known REF TEK port number 2543. However, the server may serve clients on ephemeral ports if so desired.

1.4.1 RTP Protocol Field

The Protocol field is used to identify the contents of this UDP datagram as a **RTP** packet. The **RTP** protocol number is 0x4023. An early version of **RTP** was implemented at the network layer directly on top of PPP at the data link layer for use over dedicated asynchronous serial links (RT422A and B). The 0x4023 protocol was registered as a PPP protocol number with IANA at that time. We have used the same value here simply because we already have this number and it will serve this purpose adequately.

1.4.2 RTP Packet Codes

The Code field is an 8 bit unsigned integer that is used to identify the type of **RTP** packet. Up to 256 types of packets may be used by **RTP**.

There are currently nine different packet types that fall into three classes:

- Data packets used to transport data over the connection to the peer.
- Server Discovery packets used by a client to find a server.
- Synchronization packets used to synchronize the sequence numbers used at each end of the connection for error-correction.

The table below lists the types of packets currently defined for **RTP**.

Code	Binary code	Name	Description
0x0	00000000	Data	Application data (payload).
0x01	00000001	DataAck	Data acknowledgement, data packet accepted by peer
0x04	00000100	Sync	Synchronize outbound sequence number.
0x05	00000101	SyncAck	Acknowledgement of sequence number.
0x06	00000110	USync	Unconditional synchronize.
0x07	00000111	USyncAck	Acknowledgement of unconditional synchronization
0x08	00001000	SvrInquiry	Server discovery inquiry.
0x09	00001001	InquireAc	Server acknowledgement.
0x0B	00001011	InquireNak	Server negative acknowledgement.

All codes not listed are reserved for future use. Note that as defined, bit 0 of the code field may be interpreted as the "ack bit", bit 1 as the "unconditional bit", bit 2 as the "sync bit", and bit 3 as the "discovery bit".

The three classes of packets can be easily distinguished by checking bits 2 and 3 of the code field. If bit 2 is set, this is a synchronization packet, bit 3 indicates a server discovery packet, otherwise it is data.

1.4.3 RTP Sequence Numbers

The Sequence Number field is an 8 bit unsigned integer that is used to correct transmission errors. The value of this field ranges from 0 to 255.

As each data packet is sent, the sequence number increments. The receiving end generates an acknowledgment packet for each packet that is accepted with the same sequence number and sends it back to the sender. The sender then knows that packet has been successfully transported to the peer.

The sequence number is used by the receiver to reorder packets, detect duplicate packets, and detect old packets. More details about data transfer can be found in RTP Data Transfer below.

1.4.4 RTP Unit ID Field

The Unit ID field is a 16 bit unsigned integer that identifies the application at the peer. In the case of the RT422C card, this is the DAS unit ID number. However, the purpose of this number is to identify the peer at the opposite end of the connection, which is not necessarily a DAS. This field should be thought of as a peer, or connection, number.

1.4.5 RTP Length Field

The length field is a 16 bit unsigned integer number of bytes in the RTP packet including the **RTP** header. This means that if there are 0 data bytes, the length field will be set to 8.

1.5 RTP Operation

In order for a client to move data across the network to a server, it must connect to the network, discover the address of the server, and then synchronize sequence numbers.

In order to accomplish this, RTP goes through several distinct phases.

1. **Down**, the link is not available for data transfer.
2. **Server Discovery**, the client is looking for the server.
3. **Synchronization**, client and server are synchronizing sequence numbers.
4. **Up**, the link is available for data transfer.
5. If a server wishes to **connect** to a client, it must **synchronize** but it will not need to discover the client's address, so the discovery phase is simply skipped.

1.5.1 Phase Diagram

Figure 3 shows the relationships between these phases.

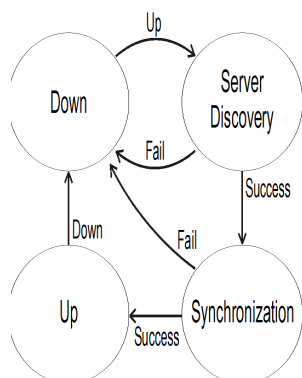


Figure 3 RTP Connection Phases

1.5.2 Down

While **RTP** is in the Down phase, the connection is not available for data transfer. The connection begins and ends in this phase.

One of two events signals that the connection should be established. If the application submits a data packet for transfer, the lower layers are opened if necessary, and **RTP** proceeds to the Server Discovery phase. Clients will also respond an incoming connection, that is, the transport layer signals an Up event. Servers are generally always connected to the network and respond to Server Inquiry packets to establish inbound connections.

1.5.3 Server Discovery

This is the only aspect of **RTP** that follows a client-server model and allows a client to discover its server. This mechanism meets the self-configuration requirements put forth in the design goals above.

Clients must discovery the IP address and port number (the endpoint) that the server will use to service its connection. Once connected to the network, the client periodically sends Server Inquiry packets containing the endpoint as subnet-directed broadcasts to the well-known REF TEK port. If the client has never been connected, the endpoint is 0.0.0.0:2543, if it has, it is the endpoint last used. The server listens for these broadcasts and responds with a InquireAck if the endpoint is correct or a InquireNak that contains the endpoint that it desires.

Once the client receives as InquireAck from the server, it proceeds to the Synchronize phase.

Servers simply skip this entire phase and proceed directly to the Synchronize phase. The server must always accept and respond to Discovery packets that it receives.

1.5.4 Synchronize

In order to perform error-correction, each end of the connection must notify the other of the sequence number of the next Data packet that it will send and receive acknowledgement. This can be accomplished by a finite-state automaton and is covered in detail below.

Note that there are two synchronize packets defined, Sync, and USync. The normal Sync, sometimes referred to as a warm Sync indicates that there has been a previous connection and we are attempting to resume that connection. The unconditional or USync, sometimes referred to as a cold Sync indicates that the sender has never been connected and that the receiver should not attempt to resume any connection.

Once an **Ack**, either **SyncAck**, or **USyncAck**, has been both sent and received, **RTP** proceeds to the Up phase. While in the Synchronize phase, no Data class packets are allowed to be transferred. Any Data class packets received are silently discarded.

1.5.5 Up

While **RTP** is in the Up phase, data may flow across the connection. All types of **RTP** packets are allowed and data moves across the connection error-free.

1.6 RTP Server Discovery

Server Discovery is a mechanism used by **RTP** clients to discover the IP address and UDP port number that the server will use to service its connection. This mechanism is the only aspect of **RTP** that employs the client-server model.

RTP servers must listen on UDP port 2543, the well-known REF TEK port, for **RTP** Server Inquiry packets from clients. Clients send these packets as subnet-directed broadcasts. These packets carry as data the endpoint that will be used by the **RTP** server to service the connection.

1.6.1 The Discovery Process

After a client has successfully attached to the network (an Up from the transport layer), it begins periodically (typically every ten seconds) broadcast a Server Inquiry packet to the REF TEK port. This will continue until successful discovery is achieved or the network connection goes down.

When a server receives a Server Inquiry packet, it examines the contents of the packet, specifically the Unit ID, and endpoint, and either reactivates a previous connection for the Unit or establishes a new connection for the Unit. If the connection is reestablished, the server can simply send an InquireAck to the peer. If a new connection is being activated, the server sends an InquireNak to the peer that contains the endpoint that the client must use to communicate with the server. Note that the server should unicast the Ack packet to the source endpoint of the Server Inquiry packet.

When a client receives an InquireAck from a server, it simply uses the endpoint within the packet and proceeds to the Synchronize phase. When a client receives an InquireNak from a server, it broadcasts a new Server Inquiry packet containing the new endpoint and the process continues.

A client will not leave the Discovery phase until it receives an InquireAck or the transport layer signals a down event. This mechanism ensures that the server and the client agree on the server's endpoint. If a packet is lost during this process it will still result in successful discovery.

1.6.2 Network Issues

Because the client broadcasts **Server** Inquiry packets, there can be problems in your network caused by routers not forwarding these packets to other networks. It is required that the server be visible to the client through subnet-directed broadcasts in order for the server discovery process to succeed.

If the server and client both reside on the same network, this is not an issue. However, in the real world, this may not be the case. In the case of our example system (see Figure B - 1 on page B-87), the server is on the other side of a router and measures must be taken to insure that the discovery process can succeed.

Note: the following aspects of the Server Inquiry packet:

- **They are always a subnet-directed broadcast. In our example, a class C network, they are sent to 192.168.2.255.**
- **They are always a UDP packet broadcast to the well-known REF TEK port (2543).**

Given this information, routers generally can be configured to allow limited forwarding of these broadcasts. In our example, the router is configured to forward only UDP packets destined for port 2543 to the subnet-directed broadcast address (192.168.1.255) of the other network and this solves the problem. The responses from the server are unicast back to the client and need no special attention.

Most routers provide this ability because various protocols, such as BOOTP, must provide this same type of functionality by employing UDP broadcasts.

See the section below for the configuration of a Cisco 25xx router that handles the issues in the example network.

1.6.3 Discovery Class Packets

The three packets used in the server discovery process in detail are:

- **ServerInquiry** - Packet is sent as a subnet-directed UDP broadcast to the well-known REF TEK port (2543). The endpoint of the server is carried in the packet as six bytes of data. It is used by the client to query the server as to the server endpoint to use for the RTP connection.

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	
8	Server IP Address			
12	Port #			

Label	Description
Code:	0x08 (SvrInquiry)
Unit ID:	The unit ID of the client. The server will use this to identify the client.
Length:	14
Server IP Address:	32 bit unsigned integer IP address of the server. If unknown, 0.0.0.0, otherwise, the address last used for the RTP connection.
Port #:	16 bit unsigned port number of server. If unknown, 2543 (0x09EF), otherwise, the UDP port last used for the RTP connection.

Note: The sequence numbers used for Discovery and Synchronize class packets should be distinct from that used for Data class packets. During the discovery phase, the sequence number is simply used to match inquiries with responds. The client must increment the sequence number each time it sends a SvrInquiry packet.

The server must use the same sequence number in its response, either InquireAck, or InquireNak.

- **InquireAck** - Packet is a positive server response to a SvrInquiry packet from a client. It is used to confirm the server endpoint to be used by the client for the RTP connection.

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	
8	Server IP Address			
12	Port #			

Label	Description
Code:	0x09 (InquireAck)
Unit ID:	The unit ID of the client. The server will use this to identify the client.
Length:	14
Server IP Address:	32 bit unsigned integer IP address of the server.
Port #:	16 bit unsigned port number of server.

The sequence number is the sequence number of the inquiry packet for which this packet is the response. Together, the Server IP Address and Port number make up the server endpoint to be used by the client for the **RTP** connection.

- **InquireNak** - Packet is a negative server response to a SvrInquiry packet from a client. It is used to communicate to the client the server endpoint that must be used for the RTP connection.

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	
8	Server IP Address			
12	Port #			

Label	Description
Code:	0x0B (InquireNak)
Unit ID:	The unit ID of the client. The server will use this to identify the client.
Length:	14
Server IP Address:	32 bit unsigned integer IP address of the server.
Port #:	16 bit unsigned port number of server.

The sequence number is the sequence number of the inquiry packet for which this packet is the response. Together, the Server IP Address and Port number make up the server endpoint to be used by the client for the **RTP** connection.

1.7 RTP Link Synchronization

RTP link synchronization is a process whereby an **RTP** implementation notifies its peer of its outbound sequence number. Each end of an **RTP** connection maintains two sequence numbers, which are the inbound and outbound sequence numbers. Each end is only responsible for synchronizing the outbound sequence number with the peer.

The process is complete when each end has both sent and received an acknowledgment packet from the peer. A finite-state-automaton (FSA) is provided that will accomplish this process.

During the synchronization process, the outbound sequence number is the number of the first data packet that will be sent to the peer. The inbound sequence number is the number of the next packet that will be forwarded to the application by **RTP**.

1.7.1 Synchronization Class Packets

There are four synchronization class packets. They are presented in detail below. None of these packets carry data, that is, there is no additional data beyond the **RTP** header.

The four synchronization packets are:

- **Sync** - Packet is used to inform the peer of the sequence number that will be used on the next data packet that it will receive. This is a "normal" Sync, this means there was a previous connection to the peer and that the peer should check to see if the sequence number falls within its inbound sequence space. If it does, the connection is resumed, otherwise the action is the same as for USync (see below).

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	

Label	Description
Code:	0x04 (Sync)
Sequence:	Local outbound sequence number.
Unit ID:	The unit ID of local RTP.
Length:	8

- **SyncAck** - Packet is used to acknowledge a Sync packet received from the peer. The packet can be created by simply copying the received Sync, changing its code to SyncAck, and reflecting it back to the peer.

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	

Label	Description
Code:	0x05 (SyncAck)
Sequence:	Peer's outbound sequence number.
Unit ID:	The unit ID of the peer RTP.
Length:	8

- **USync** - or **unconditional synchronize** packet, is used to inform the peer that it has never been successfully connected to the peer and has no out-of-order data in its outbound queue. The peer must flush any pending out-of-order data that might be in its inbound queue and set its inbound sequence number.

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	

Label	Description
Code:	0x06 (USync)
Sequence:	Local outbound sequence number.
Unit ID:	The unit ID of local RTP.
Length:	8

- **USyncAck** - Packet is used to acknowledge a USync packet received from the peer. The packet can be created by simply copying the received USync, changing its code to SyncAck, and reflecting it back to the peer.

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	

Label	Description
Code:	0x07 (USyncAck)
Sequence:	Peer's outbound sequence number.
Unit ID:	The unit ID of the peer RTP.
Length:	8

1.7.2 The Link Synchronization Automaton

Here is presented a finite-state-automaton (FSA) that will drive the link synchronization process.

The FSA is defined by events, actions, and state transitions. Events include: reception of external signals such as open and close commands and signals from lower layers, reception of RTP synchronization class packets, and the expiration of the restart timer. Actions include: communicating with the lower layers and transmitting packets to the peer.

The following table summarizes the events handled and actions taken by the automaton.

Actions:		Events:	
tls	This layer start.	Up	Lower layer is up.
tlf	This layer finished.	Down	Lower layer is down.
tlu	This layer up.	Open	Open the connection.
tld	This layer down.	Close	Close the connection.
irc	Initialize restart counter.	TO+	Time-out with restart counter > 0.
ssp	Send synchronize packet.	TO-	Time-out with restart counter = 0.
sap	Send sync acknowledge packet.	RSP	Received synchronize packet.
		RAP	Received sync acknowledge packet.

1.7.3 State Transition Table

The complete state transition table follows. States are indicated horizontally and events are read vertically. State transitions and actions are represented in the form action/next-state. Multiple actions are separated by commas and may continue on the next line. The dash indicates an illegal action.

Events /state	0-Closed	1-Stopped	2-Sync-sent	3-Ack-rcvd	4-Ack-sent	5-Opened
Up	irc, ssp/2	irc, ssp/2	–	–	–	–
Down	1	1	1	1	1	tld/1
Open	tls/1	tls/1	2	3	4	tld, irc, ssp/2
Close	tlf/0	tlf/0	tlf/0	tlf/0	tlf/0	tld, tlf/0
TO+	–	–	ssp/2	ssp/2	ssp/4	–
TO -	–	–	tld, tlf/1	tld, tlf/1	tld, tlf/1	–
RSP	–	irc, ssp, sap/4	sap/4	sap, tlu/5	sap/4	tld, ssp, sap/4
RAP	–	irc, ssp/2	irc/3	ssp/2	irc, tlu/5	tld, irc, ssp/2

The states in which the restart timer is running are identified by the presence of the TO events.

If the link has never been in the Opened state (it is “cold”), unconditional Syncs and Sync Acks (USync, USyncAck) are sent to the peer, otherwise regular Syncs and SyncAcks are sent.

The Closed state (0) differs from the Stopped state (1) only in that the link is dropped (tlf) before the transition to Closed. In either state an incoming connect brings this layer up. This allows the application to use the Open and Close events as initiate and drop the link commands respectively. The automaton is in the Closed state only when the application commands it. It is in the stopped state due some external factor such as loss of carrier.

1.7.4 States

The following is a brief description of each **FSA** state.

State	Description
Closed (0)	In this state, RTP has not been initialized and the transport layer is not up. No packets can be sent or received in this state. An RTP implementation should issue an open event as soon as possible at startup. The restart timer is not running.
Stopped (1)	In this state the transport layer is not up. The FSA will begin to synchronize the link when the transport layer signals an Up event. An Open event will cause the start action to initiate the connection. The restart timer is not running.
Sync-sent (2)	In this state a Sync (or USync) has been sent to the peer but a SyncAck (or USyncAck) has not been received. The restart timer is running and the Sync packet will be sent again upon its expiration.
Ack-rcvd (3)	In this state a Sync has been sent to and a SyncAck has been received from the peer. However, no Sync has been received and no Sync-Ack has been sent. The restart timer is running and the Sync packet will be sent again upon its expiration.
Ack-sent (4)	In this state a Sync and a SyncAck have been sent to the peer. No SyncAck has been received. The restart timer is running and the Sync will be sent again if it expires.
Opened (5)	In this state a SyncAck has been both sent to and received from the peer. The connection is now synchronized and ready to transfer data. The RTP connection is Up and the restart timer is not running.

1.7.5 Events

FSA actions and state transitions are caused by events. The following is a brief summary of the events handled by the **FSA**.

Event	Description
Up	This event comes from the transport layer to indicate that the network will now accept traffic. On clients, this event is intercepted to initiate the server discovery process and upon successful completion is then sent to the FSA to cause the link to synchronize.
Down	This event comes from the transport layer to indicate that the connection to the network is down and unavailable for traffic. This causes the FSA to transition to the Stopped state.
Open	This event comes from the application and indicates that it desires to send data across the link. If the transport layer is not up, it causes action to initiate the connection to the network. If the FSA is already opened, this event causes re synchronization.
Close	This event comes from the application and indicates that the connection should be dropped. The connection to the network is broken and the FSA transitions to the Closed state.
Time-out TO+,TO-	These events occur when the restart timer expires. The restart timer is used to time the response to Sync packets.
	The TO+ event indicates that the restart timer expired with the restart counter greater than zero. The restart is decremented and the packet is retransmitted.
	The TO- event indicates that the restart timer expired with the restart counter equal to zero. The link is recycled, that is, the connection to the network is dropped, then reestablished. Note that this causes server discovery to happen again before synchronization.
Received Sync Packet (RSP)	This event occurs when a Sync (or USync) packet is received from the peer. If the packet is a Sync, the sequence number within the packet is checked against the inbound sequence space, if it is within the space, it is simply Ack'ed. If not, it is treated as a USync.
	If the packet is a USync, the inbound queue is flushed and the inbound sequence number is set to the sequence number within the USync packet. Because this informs the us that the peer is "cold", this forces the local system to be "cold" as well. The local outbound queue must be examined for non-contiguous packets.
	If any are found, they must be discarded and the outbound sequence number must be set to the oldest contiguous packet in the outbound queue and a USync must be transmitted.
Received SyncAck packet (RAP)	This event occurs when a SyncAck (or USyncAck) is received from the peer. If the sequence number in the packet doesn't match that of the last transmitted Sync (or USync) the packet must be discarded.

1.7.6 Actions

Actions are taken by the automaton as events occur. The following is a brief description of the various actions that may be taken by the **FSA**.

Action	Descriptions
Illegal Action (-)	This is an action that should never occur in a properly implemented automaton. This indicates an internal error that needs to be corrected.
This Layer Start (tls)	This action causes initiation of the connection to the network. Usually this simply causes an Open event to the transport layer which in turn opens the layers on down the stack.
This Layer Up (tlu)	This action occurs as the synchronization process is successfully completed and is used to perform whatever task is required at that point. This is the last action taken as the connection comes opened and may be used to notify the application the RTP connection is now ready for traffic.
This Layer Down (tld)	This action occurs when the connection is no longer ready to carry data traffic. It is the first action taken as RTP leaves the Up phase and can be used to notify the application that the connection is down.
This Layer Finished (tlf)	This action causes disconnection from the network. This is the last action taken before entering the Down phase.
Initialize Restart Counter (irc)	This action set the restart counter to the appropriate retry value. This is typically 10.
Send Sync Packet (ssp)	This action is used to create a Sync or USync packet and send it to the peer.
	For a normal Sync , the sequence number of the packet is the number of the oldest packet in the outbound queue.
	For a USync , the outbound queue must be checked and any non-sequential packets discarded before the oldest packet sequence number is used.
Send SyncAck Packet (sap)	This action is used to create a SyncAck or USyncAck packet and send it to the peer. The packet can be created by copying the received Sync or SyncAck, changing the code to an Ack (set bit 0), and reflect the packet to the peer.

1.7.7 Counters and Timers

The **RTP FSA** makes use of one counter, the restart counter, and one timer, the restart timer. The restart counter is decremented each time that as **Sync** or **USync** packet is sent. Expiration of the restart timer causes the TO events that cause retransmission of these packets.

By default the restart timer should be set to six (6) seconds and the restart counter should be set to 10.

1.8 RTP Data Transfer

The primary purpose of **RTP** is to transfer data. The requirements are, in order;

- Provide error-free transfer across the network.
- Efficient utilization of the available bandwidth.

The transport layer (**UDP**) provides a simple, packet oriented, best-effort service to **RTP**. UDP packets may arrive at the peer out of order or not at all.

In order to meet these requirements, **RTP** employs an acknowledgement mechanism, 16 slot queues to allow streaming transmission (up to 16 packets may be sent before receiving acknowledgement) on the outbound side, and reorder of packets on the inbound side. In addition to this queuing, an adaptive retransmission time-out scheme is used to insure that lost packets are retransmitted as soon as possible and helps to reduce the need for deep queues.

1.8.1 Data Class Packets

Application data packets are encapsulated in RTP Data packets for transport across the network. The Data packet is complemented by the DataAck packet which is sent by the peer to indicate that it has accepted the Data packet.

Data

The Data packet is used to transport application data packets to the peer. Each packet is assigned a sequence number as they are received from the application and are delivered at the peer application in that same order.

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	
8	Application Data...			

Label	Description
Code:	0x00 (Data)
Sequence #:	Senders outbound sequence number.
Unit ID:	The unit ID of the sending RTP.
Length:	8 + length of application data.
Application Data:	0 to 1024 bytes of payload data.

DataAck

The DataAck packet is sent by the receiving RTP to indicate the acceptance of the associated Data packet. The sender of the Data packet takes reception of this DataAck packet to indicate that the packet has been successfully transported and can now be disposed of.

	0	1	2	3
0	Protocol (0x4023)		Code	Sequence #
4	Unit ID (0000-9999)		Length	

Label	Description
Code:	0x01 (DataAck)
Sequence:	Received Data packet sequence number.
Unit ID:	The unit ID of the RTP that is the source of the Data packet.
Length:	8

Note: An ack can be created by copying the RTP header of the Data packet, changing its code to DataAck and length to 8, and reflecting the packet to the peer.

1.8.2 RTP Sequence Numbers

Every data packet sent across an RTP connection is assigned an 8 bit sequence number. This number is assigned as packets are accepted from the application by the sending RTP and reflect the order in which the application submitted them. RTP will deliver these packets in this same order to the application at the opposite end of the connection.

Because RTP is full-duplex, each end must maintain a set of sequence numbers, one for inbound and one for outbound packets. For each direction on the connection there is an available sequence space. This is the range of sequence numbers that are currently active in one direction.

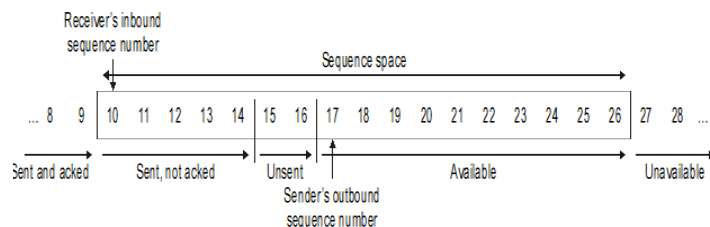


Figure 4 RTP Sequence Space

The sender should not send packets with sequence numbers that are outside of the sequence space. The sender tracks the sequence space as starting at the oldest unacknowledged packet to that sequence number plus the depth of the queues (16).

The receiver tracks the sequence space from the inbound sequence number, the sequence number of the next packet that will be sent to the application, to that number plus the depth of the queue, again, 16. The receiver will accept, that is acknowledge, all packets up to and including the end of the sequence space. Packets with sequence numbers less than the inbound sequence number are old packets which have already been received and are discarded. Packets that already exist in the queue are duplicates and again are discarded. Packets greater than the end of the sequence space are in error and are not accepted, that is, they are not acknowledged and will be retransmitted by the sender. Properly implemented, RTP should never send packets that are greater than the end of the sequence space.

- Modular Arithmetic with Sequence Numbers - RTP must deal with the fact that the 8 bit integer sequence has a limited range of 0 to 255. Once 28 (256) packets have been sent, the sequence number will wrap from 255 back to 0. Given that the sequence space is limited to 16, this can easily be dealt with by employing modular arithmetic to compare sequence numbers.
- Sequence Number Comparisons - RTP sequence numbers are defined as an unsigned 8 bit integer. The following C language macros compare RTP sequence numbers:

```
typedef INT8 signed char;
```

```
#define SEQ_LT(a, b) ((INT8)((a) - (b)) < 0)
#define SEQ_LE(a, b) ((INT8)((a) - (b)) <= 0)
#define SEQ_GT(a, b) ((INT8)((a) - (b)) > 0)
#define SEQ_GE(a, b) ((INT8)((a) - (b)) >= 0)
```

When comparing two sequence numbers, we can simply subtract one from the other and interpret the result as a signed integer. This resulting relationship to zero is the relationship of the one sequence number (a) to the other (b).

This is somewhat counterintuitive. For example, if we compare 255 to 0, we find the 255 is less than zero.



Figure 5 Sequence Number Comparison to Zero

Figure B - 6 shows a somewhat more intuitive way to visualize the circular nature of RTP sequence numbers.

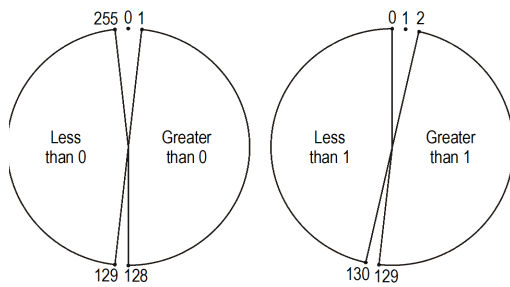


Figure 6 0 to 1 Compare

1.8.3 RTP Outbound Processing

Application data packets submitted to **RTP** for transport across the network to the peer are encapsulated in **RTP** Data packets and added to the outbound queue. Each entry in the queue is called a slot and along with the **RTP** Data packet it has a counter and a timer associated with it. The counter is used to count the number of times that this packet has been sent and the timer is the elapsed time since it was last sent. There must be at least 16 slots available in the outbound queue.

There are two global values that are associated with outbound data, they are; the current outbound sequence number, and the current retransmission interval.

1.8.3.1 Enqueuing Outbound Data Packets

The queue is kept in order of sequence numbers and represents the currently occupied portion of the sequence space. The queue is typically implemented as a linked list of structures in memory. The head slot in the queue is the oldest, that is, the lesser sequence number, and the tail is the newest.

Before **RTP** enqueues an outbound packet, it must check that there is room in the sequence space for that packet. This is easily accomplished by comparing the sequence number of the head slot (the oldest unacknowledged packet) plus 16 with the current outbound sequence number. If the current outbound sequence number is less than the head number plus 16, then the packet may be enqueued, otherwise, the outbound queue is full and the application must wait.

New packets are assigned the current outbound sequence number and it is then incremented. The new packet is placed in the tail slot of the queue, its counter is set to 10, and its timer is initialized.

1.8.3.2 Sending Outbound Data Packets

Packets are transmitted by examining the queue from head to tail and sending the first packet that either has never been sent (counter equal to 10) or has an elapsed time since last sent greater than the retransmission time-out. This insures that packets that need retransmission will get it in a timely manner.

As each slot of the queue is examined, several checks are made. First, if the counter on any packet is zero, there is a major problem with the connection to the network and it should be dropped and reestablished. Second, if the elapsed time since last sent is greater than the retransmit interval or the counter is equal to 10, the packet is to be sent. After the packet is sent, its counter is decremented, its timer restarted, and we repeat the procedure starting at the head of the queue, not the next slot.

If we reach the tail of the queue, no packets are ready to be sent so we simply repeat the procedure starting at the head slot again.

1.8.3.3 Dequeuing Outbound Data Packets

As DataAck packets are received, the outbound queue is examined for the sequence number contained in the DataAck packet. If the corresponding Data packet is in the outbound queue, it is dequeued. The elapsed time since sent is the effective round-trip time to the server and may be used to implement adaptive retransmission.

1.8.3.4 Adaptive Retransmission Time-out

Adaptive retransmit is a mechanism that keeps the retransmission interval set to a realistic value so that RTP does not stall or retransmit unnecessarily. The idea is to update the retransmission interval each time that a packet is dequeued from the outbound queue using a running average over some number of packets plus some time for overhead.

This is very helpful on connections with long round trip times. If the retransmission interval is too long, when a Data or DataAck packet is lost, RTP will send all packets in the outbound queue and then stall waiting for the missing DataAck to arrive before retransmitting the Data packet again. Conversely, if the interval is too short, it will retransmit Data packets before the DataAck can make the trip back and squander the bandwidth available on the connection.

Adaptive retransmit helps by insuring that Data packets needing retransmission are sent again quickly and insures that there are no more packets in the outbound queue at any given time than are absolutely necessary.

The following C language function will compute the retransmission interval based on the round trip time measured for the last packet transferred:

```
typedef signed long INT32;      /* 32 bit signed */
typedef unsigned long UINT32;   /* 32 bit unsigned */

#define RETRANS_MAX              (10 * SECOND_MS)
#define RETRANS_MIN              (500 * MSECOND_MS)
#define RETRANS_C                 4
#define RETRANS_M                 2

UINT32 ComputeRetransInterval( UINT32 round_trip, UINT32 *retrans_interval )
{
    INT32 a, t, c;

    /* Compute average interval over last C packets by recursive
       approximation. The result is the minimum plus M times the
       average constrained to less than the maximum.

       round_trip = round trip time measured for last packet in ms.
       retrans_interval = pointer to the current retransmission interval in ms.

       return value = value of new retransmission interval.
    */

    t = (INT32)RETRANS_MIN + ((INT32)round_trip * (INT32)RETRANS_M);
    a = (INT32)*retrans_interval;
    c = (INT32)RETRANS_C;

    a = (a + ((t - a) / c));

    if (a > RETRANS_MAX)
        a = RETRANS_MAX;

    *retrans_interval = (UINT32)a;

    return(*retrans_interval);
}
```

If an error occurs and **RTP** retransmits a Data packet, it cannot be sure if the DataAck that it receives is for the last or the first packet sent. This means that measures must be taken to ensure that the retransmission interval is not allowed to decrease without limit. The code above will not allow it to decrease to less than 500 ms. However, a sudden change in the condition of the connection can still cause problems.

A simple solution is to check the counter on Data packets before they are dequeued. If the packet has been transmitted more than three times, it is likely that the interval needs to be increased. Rather than recompute the interval, it should be doubled and then constrained to be less than the maximum value (10 seconds).

The following C language function will increase the retransmission interval as described.

```
UINT32 IncreaseRetransInterval( UINT32 *retrans_interval )
{
    /* Double the retransmission interval */
    *retrans_interval *= 2;

    if( *retrans_interval > RETRANS_MAX )
        *retrans_interval = RETRANS_MAX;

    return( *retrans_interval );
}
```

1.8.4 RTP Inbound Processing

As Data packets are received from the network, they are inserted into the inbound queue. This queue is maintained in order of packet sequence number. As with the outbound queue, the head slot contains the packet with the lesser sequence number.

If the head slot of the queue contains the packet with the inbound sequence number, it is dequeued and forwarded to the application. The inbound sequence number is then incremented. This is the mechanism whereby packets are re-ordered before being sent to the application.

There is only one global variable associated with the inbound queue, the current inbound sequence number.

1.8.4.1 Enqueuing Inbound Data Packets

As stated above, the inbound queue is maintained in ascending order of sequence number. Before an inbound Data packet is enqueued, its sequence number is checked as follows:

Is it less than the current inbound sequence number? If so, the packet is old and indicates that the previous DataAck did not make it back to the peer. A DataAck is generated for this new packet and the packet is discarded.

Is it greater than or equal to the current inbound sequence number plus 16? If so the packet is in error and is simply discarded without acknowledgement. The sender has made the error and should retransmit the packet again later.

If the above two tests are false, this packet falls within the sequence space. The packet must now be inserted into the queue in its proper place. If a packet with this sequence number is already in the queue, then this new packet is a duplicate and is discarded.

1.8.4.2 Dequeuing Inbound Data Packets

RTP is always waiting for the Data packet with the inbound sequence number to arrive. This packet is sent to the application and the inbound sequence number is incremented.

Because the inbound queue is maintained in order, the packet of interest will always be in the head slot of the queue. If this packet's sequence number is equal to the inbound sequence number, it is sent to the application, the packet is dequeued, and the inbound sequence number is incremented.

1.9 RTP Server Discovery Through Cisco Routers

As stated in the section above on Server Discovery, if the server and the client are on different networks, the router must be instructed to forward UDP packets destined for the well-know Ref Tek port to the servers network.

The following is the configuration of the Cisco 2509 router shown in figure 1.

```
!  
version 11.3  
no service password-encryption  
!  
hostname RefTek  
!  
username das#7377 password 0 das#7377  
username das#7378 password 0 das#7378  
!  
chat-script reset-USRcourier-v34 "" "at&f1&d2s0=1" "OK"  
chat-script dial-USRcourier-v34 "" "atdt\T" TIMEOUT 60 CONNECT \c  
!  
interface Ethernet0  
  description Interface to 192.168.1.0 network  
  ip address 192.168.1.1 255.255.255.0  
!  
interface Serial0  
  no ip address  
  shutdown  
!  
interface Serial1  
  no ip address  
  shutdown  
!  
interface Async1  
  description DDR connection to RT422 in DAS 7377  
  ip address 192.168.2.1 255.255.255.0  
  ip helper-address 192.168.1.255  
  encapsulation ppp  
  dialer in-band  
  dialer wait-for-carrier-time 60  
  dialer string 3530611  
  dialer-group 1  
  async mode interactive  
  peer default ip address 192.168.2.2  
  no cdp enable  
  ppp authentication pap callin  
!  
interface Async2  
  description Direct connect to RT422 in DAS 7378  
  ip address 192.168.2.1 255.255.255.0  
  ip helper-address 192.168.1.255  
  encapsulation ppp  
  async mode interactive  
  peer default ip address 192.168.2.3  
  no cdp enable  
  ppp authentication pap callin  
!  
ip http server  
ip classless
```

```
ip forward-protocol udp 2543
ip route 192.168.1.0 255.255.255.0 Ethernet0
ip route 192.168.2.2 255.255.255.255 Async1
ip route 192.168.2.3 255.255.255.255 Async2
access-list 101 permit ip any any
access-list 101 deny igrp any host 255.255.255.255
dialer-list 1 protocol ip list 101
!
line con 0
line 1
  autoselect ppp
  script dialer dial-USRcourier-v34
  script reset reset-USRcourier-v34
  login local
  modem InOut
  transport input all
  speed 115200
  flowcontrol hardware
line 2 8
  autoselect ppp
  modem InOut
  flowcontrol hardware
line aux 0
line vty 0 4
  exec-timeout 0 0
  password reftek
  login
!
end
```

This configuration provides for a DAS with an RT422 to be connected directly to the Async2 interface as well as a Dial-on-demand routing (DDR) connection through a modem on the Async1 interface.

The UDP broadcasts are handled by the global statement `ip forward-protocol udp 2543`, and the Async interface statements `ip helper address 192.168.1.255`. These statements cause the router to forward UDP broadcasts received on those interfaces to the subnet directed broadcast address of the 192.168.1.0 network where the server will see them.



2 RTPD Client Protocol

2.1 RTPD/Client Connection Overview

The RTPD to client connection is created using a TCP socket and the **RTP** protocol. RTPD is the server and the client initiates the connection. The **rtp** library encapsulates much of the message handling required to establish a connection and to send and receive messages. The library also handles any of the data conversion required to ensure the message is transmitted in network byte order. This document gives the minimum amount of information necessary to create a client program. The programmer is encouraged to examine and use the rtp library functions when writing their application.

2.2 Client Connection to RTPD

A client program connects to an RTPD server by sending messages to the server's IP address using the port number defined in the server's RTPD.ini file (value of the Port field). The default port number is 2543. The client connection must use the IP address of the first interface card address for the workstation where the server is running.

The structure of the RTP message packets is shown in the table below.

Offset	Description	No. of Bytes	Type and Range
0	Type of message	2	Binary integer 0 – 11 (see table 2).
2	Length of payload	4	Binary integer. Zero if payload is absent.
4	Payload	nnnn	Message Body. nnnn = size in bytes.

The message types are defined in the file <src/include/rtp.h> as show in Table 2. The length of the payload is used to know the size of the payload being transmitted. This length can increase if more data is transmitted in future releases of rtpd or client programs. Therefore, it must be used to ensure messages stay in sync. When establishing a connection to RTPD , there is a protocol version which is passed as the first message. It is used to verify that the handshake protocol, or the number and sequence of messages used to establish a connection, is the same between the client and the RTPD server.

Value	Type Name	Description
0	RTP_MSG_REFTEK	A Reftek (ie, from DAS) packet
1	RTP_MSG_CMDPKT	An RTP command packet
2	RTP_MSG_NOP	Heartbeat message
3	RTP_MSG_ATTR	Connection attribute message
4	RTP_MSG_SOH	State of health request/reply
5	RTP_MSG_START	Start forwarding packets
6	RTP_MSG_STOP	Stop forwarding packets
7	RTP_MSG_FLUSH	Flush buffered but undelivered packets
8	RTP_MSG_BREAK	Break connection
9	RTP_MSG_BUSY	Server busy message
10	RTP_MSG_FAULT	Server fault
11	RTP_MSG_PID	Peer PID message

2.3 Opening a Connection

A client establishes a connection by opening a socket to the server and exchanging a specific sequence of messages. This process has been encapsulated by the `rtp_open()` function. `rtp_open()` opens the socket and calls the `handshake()` function to send these first few messages. These functions are located in the module `<src/lib/rtp/accept.c>`.

The handshake procedure includes three steps: identifying the RTP protocol version used, trading process IDs (PIDs) and establishing the connection attributes.

1. The client sends an empty message (6 bytes in length for the header) using the Client Protocol version number as the message type. RTPD responds with a similar message where the message type is set to the protocol version supported by current RTPD implementation.

Note: The current implementation of RTPD only accepts protocol version 1.

2. The client sends a PID message (`RTP_MSG_PID`) containing its PID number and client name. RTPD responds with its own PID message containing its PID number and name. The id and name are put in the RTPD log when the connection is complete. The PID message is defined in the table below.

Element	Type	Description
PID	UINT32	Process ID
client_name	32 CHAR	Name of program

3. The client sends an ATTRIBUTE message (`RTP_MSG_ATTR`) containing its connection attributes. RTPD responds with an attribute message that may contain changes. The client must use the modified attributes. The connection attributes message is defined in following table.

The connection is open if these three steps finish successfully.

Element	Type	Description
at_dasid	UINT32	DAS "mask"
at_pmask	UINT32	Packet mask
at_smask	UINT32	Stream mask
at_timeo	INT32	I/O timeout interval (for RTPD i/o)
at_block	INT32	Application level block/noblock flag. This element is defined in structure rtp_attr to be of BOOL type. A value of this variable transmits as 1/0 that corresponds to TRUE/FALSE.
at_sndbuf	INT32	TCP/IP transmit buffer size
at_rcvbuf	INT32	TCP/IP receive buffer size
flag	INT32	Bit 0 is clients command privilege 1-allowed 0-not allowed

A structure is defined in <src/include/rtp.h> The names above match the members of the structure rtp_attr. However, the sequence of elements does not correspond identically to their order in the structure.

Connection for a typical client connection might look as follows:

```
static CHAR  Host   = "localhost"; /*or dot delimited server address*/
static UINT16 Port   = RTP_DEFAULT_PORT;
static UINT16 Retry  = RTP_ERR_NONFATAL;
RTP  *rtp  = (RTP *) NULL;
void main(int argc, char *argv[])
{
    struct rtp_attr attr = RTP_DEFAULT_ATTR;
    attr.at_block = FALSE;
    attr.at_pmask = RTP_PMASK_ALL;
    strncpy(client_name,argv[0],RTP_CLIENT_NAME_LEN);/*for PID msg*/
    if ((rtp = rtp_open(Host, Port, &attr, Retry)) == (RTP *) NULL)
    {
        perror("rtp_open");
        exit(1);
    }
    .
    .
    .
    .
}
```

It should be noted that the rtp_open uses the variable client_name to fill in the program name in the RTP_MSG_PID. If this is not done the name "Client Name not set" will be used.

2.3.1 Receiving Messages

When receiving messages from the server, the message header is received first, and then the message payload is received next based on the size declared in the message header. Therefore, per Table 1, 6 bytes are received, and then a variable number of bytes will be received. The process is encapsulated in the function `rtp_rcv()`. Messages returned from the DAS are placed in messages of type. `RTP_MSG_REFTEK`. The payload of this message is usually a DAS data packet or command response. The data packet is defined by the 130 recording document, RECORDING FORMAT SPECIFICATIONS For REFTEK 130 Data Acquisition Systems. The command response is defined in the 130 command document, COMMAND FORMAT SPECIFICATIONS For REFTEK 130 Data Acquisition Systems.

The library function `rtp_daspkt()` provides an example of using the `rtp_rcv()` function.

```
BOOL rtp_daspkt(
RTP *rtp,
UINT8 *buf, /* payload will be put in this buffer */
INT32 *datlen) /* length of payload will be set */
{
    UINT16 type;
    static CHAR *fid = "rtp_daspkt";

    if (rtp == (RTP *) NULL || buf == (UINT8 *) NULL)
    {
        rtp_log(RTP_ERR, "%s: null input(s)!", fid);
        errno = EINVAL;
        return FALSE;
    }
    while (1)
    {
        /* Get the next message from the server */
        if (!rtp_rcv(rtp, buf, &type, datlen))
        {
            rtp_log(RTP_DEBUG, "%s: rtp_rcv failed", fid);
            return FALSE;
        }

        /* Deal with it */
        if (type == RTP_MSG_REFTEK) /*command response or data packet from
DAS*/
        {
            return TRUE;
        }
        else if (type == RTP_MSG_NOP && !rtp->attr.at_block)
        {
            rtp_log(RTP_DEBUG, "HEARTBEAT received");
            *datlen = 0;
            return TRUE;
        }
        .
        .
        .
    }
}
```

```

    .
    .
    else if (type == RTP_MSG_FAULT)
    {
        rtp_log(RTP_ERR, "server fault!");
        errno = ECONNABORTED;
        rtp->rcv.error = RTP_ERR_FATAL;
        return FALSE;
    }
}
}

```

2.3.2 Sending Command Packets

The DAS command packets are described in the 130 command document, COMMAND FORMAT SPECIFICATIONS For REFTEK 130 Data Acquisition Systems. The DAS packet is the data part of the RTP_MSG_CMDPKT described in Table 5.

The unit id and command length are added so that RTPD can easily extract them and use them to forward to the DAS.

Element	Type	Description
Unit	UINT16	Unit ID
Len	UINT16	Command Packet length
Data	1K max	DAS command packet as described in 130 document

The application only needs to format the DAS command packet and call `rtp_cmdpkt_send()` to send the packet. This function will handle creating the RTP message, encoding the extra data in network byte order before sending it to the RTPD server. Here is an example of sending a command packet. Note that it uses the structure `RTP_CMDPKT` to setup the data to be formatted and sent.

```

VOID Cmd_130(RTP *rtp,
  UINT16 uid, /* DAS unit id */
  char *message) /* command packet to send/
{
  static char *fid = "Cmd_130";
  UINT16      len;
  UINT16      crc;
  char        *p;
  RTP_CMDPKT  cmdpkt;
  BOOL        first = TRUE;

  /* check for valid message */
  if (rtp == (RTP *)NULL)
  {
    fprintf(stderr, "command discarded: NULL RTPD handle!\n");
    return;
  }
}

```

```
if (uid && (uid < 0x9000))
{
    fprintf(stderr, "command discarded: invalid UID (%04X)!\n", uid);
    return;
}
len = strlen((CHAR *)message);
if (len > (256 - 16))
{
    fprintf(stderr, "command discarded: too long!\n");
    return;
}
if (len == 0)
{
    fprintf(stderr, "command discarded: zero length!\n");
    return;
}

/*-----
    create actual command
-----*/
p = cmdpkt.data;
*p++ = RT130_CMND;
*p++ = 0;
sprintf(p, "%04hX%04hu%s", uid, (len+6), message);
len += 8;          /* account for ID & length fields */
crc = Cmd_130_crc(p, len);
len += 2;          /* account for ATTN & rsvd fields */
sprintf(&cmdpkt.data[len], "%04X\r\n", crc);
len += 6;          /* account for CRC & delimiters */
cmdpkt.unit = uid;
cmdpkt.len = len;
rtp_cmdpkt_send(rtp, &cmdpkt);

} /* end of Cmd_130() */
```

2.3.3 Connection Session

During a connection session, RTPD sends a HEARTBEAT message (RTP_MSG_NOP) once a second if no messages were sent to the client during the past second. The REFTEK messages could be DAS recording packets or DAS responses to client commands. This is performed by the RTPD function ClientThread() located in <src/bin/rtpd/client.c>. The HEARTBEAT message currently has a zero length payload.

2.4 Closing A Connection

The client closes an open connection by sending a BREAK message (RTP_MSG_BREAK) to the server and closing the socket. The BREAK message is sent using the `rtp_break()` macro located in `<src/include/rtp.h>`. The socket is closed by the function `rtp_close()` located in `<src/lib/rtp/close.c>`. The BREAK message currently has a zero length payload. Example code follows:

```
VOID graceful_exit(RTP *rtp, UINT16 status)
```

```
{  
    rtp_log(IDLOG_ERR, "shutdown");  
    rtp_break(rtp);  
    rtp_close(rtp);  
    exit((int) status);  
} /* end graceful_exit() */
```

2.5 Other Message Payloads

The following messages currently have a zero length payload:

```
RTP_MSG_FAULT-   logged by RTPD only
RTP_MSG_BUSY  -   logged by RTPD only
RTP_MSG_BREAK -   RTPD returns break & closes connection
RTP_MSG_START -   restarts transmission of data packets
RTP_MSG_STOP  -   stops transmission of data packets
RTP_MSG_SOH   -   logged by RTPD only
RTP_MSG_NOP   -   logged by RTPD only
RTP_MSG_FLUSH -   RTPD flushes pending data packets to client
```

2.6 RTP Log

The rtp library also has a logging function built into it. It is suggested that the programmer use this facility to provide common functionality amongst clients.

The logging facility is initialized as follows:

```
static CHAR *Logfn    = "rtpid.log";
rtp_loginit(Logfn, 0, NULL, "rtpid");
```

Then messages are logged as follows:

```
rtp_log(RTP_INFO, "%s", Version);
```

The first parameter is the message type and can be replaced by one of the following:

```
RTP_LOG_ECHO
RTP_ERR
RTP_WARN
RTP_INFO
RTP_DEBUG
```

ECHO can be used to always display information to the screen. The other three types allow the user to control the amount of information put in the log file. This is controlled by a logging threshold that is set by calling `rtp_loglevel(newlevel)`. If the newlevel is set to `RTP_ERR`, only `RTP_ERR` messages are logged. If `RTP_WARN`, `RTP_ERR` and `RTP_WARN` are displayed. The default level is `RTP_INFO`.

LOG LEVEL	MESSAGE TYPES LOGGED
RTP_ERR	RTP_ERR
RTP_WARN	RTP_ERR & RTP_WARN
RTP_INFO	RTP_ERR,RTP_WARN & RTP_INFO
RTP_DEBUG	RTP_ERR, RTP_WARN,RTP_INFO & RTP_DEBUG

Control of the logging level is often programmed to be selectable. Sample code follows:

```
if (strcasecmp(argv[i], "-v") == 0)
{
    rtp_loglevel(RTP_DEBUG);
}
```