Workgroup:	Internet Engineering Task Force
Internet-Draft:	draft-royer-phoenix-00
Published:	21 January 2025
Intended Status:	Informational
Expires:	25 July 2025
Author:	DM. Royer, Ed.
	RiverExplorer Games LLC

Phoenix: Lemonade Risen Again

Abstract

NOTE: This is just getting started, not ready for submission yet.

Email and MIME messages account for one the largest volumes of data on the internet. The transfer of these MIME message has not had a major updated in decades. Part of the reason is that it is very important data and altering it takes a great deal of care and planning.

This application transport can also transfer non-MIME data. It can be used as an XDR transport, or for opaue data (blobs of known or unknown data) transport.

Another major concern is security and authentication. This proposal allows for existing autnentication to continue to work.

This is a MIME message transport that can facilitate the transfer of any kind of MIME message. Including email, calendaring, and text, image, or multimedia MIME messages. It can transfer multipart and simple MIME messages.

The POP and IMAP protocols are overly chatty and now that the Internet can handle 8-bit transfers, there is no need for the overly complex text handling of messages.

This proposal includes a sample implementation. (https://github.com/RiverExplorer/Phoenix) Which also includes a gateway from this proposal to existing system. Thunderbid and Outlook plugins are part of the sample implementation.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 July 2025.

Copyright Notice

Table of Contents

1. Introduction

On the Internet, just about everything is a MIME object and there are many ways to transport MIME. This document specifies a new application level MIME transport mechanism and protocol. This document does not specify any new or changed MIME types.

Transporting MIME objects is generally done in one of two ways: (1) Broadcasting, (2) Polling. Both methods often require some form of authentication, registration, and selecting of the desired material. These selection processes are essentially a form of remote folder management. In some cases you can only select what is provided, and in others you have some or a lot of control over the remote folders.

In addition to other functions, this specification defines a remote and local folder management. This remote folder management is common with many type of very popular protocols. This design started by looking at the very popular IMAP and POP protocols.

An additional task is transporting the perhaps very large MIME objects. Some MIME objects are so large that some devices may default to looking at only at parts of the MIME object. An example is an email message with one or more very large attachments, where the device may default to not download the large attachment without a specific request from the user.

Some objects are transported as blocks of data with a known and fixed size. These are often transported with some kind of search, get, and put commands. In effect these are folder and file commands

Other MIME objects are transported in streams of data with an unspecified size, such as streaming music, audio, or video. This specification describes how to use existing protocols to facilitate the data streaming. And again, these are folder and file commands.

A MIME object can be a simple object, or it may contain many multipart sections of small to huge size. These sections can be viewed as files in the containing MIME object.

By implementing this specification application developers can use the techniques to manage local and remote files and folders. Remote email or files are the same thing in this specification. The sections of MIME object with multipart sections are viewed as files in the MIME object. You can interact with the entire folder, or just the files within it.

MIME objects have meta data, and they are called headers. Files and folders have meta data, and they are called file attributes. This specification does not mandate any meta data, it allows for a consistent transport of existing meta data.

File and folder meta data is a complex task that can involve access control lists and permissions. This specification defines a mechanism to transport this meta data, it does not define the meta data.

And this specification provides for the ability to define both protocol extensions and the creating of finer control for specific commands that may evolve over time.

This examples compares current folder and file manipulations to how it can be used in this protocol with email.

- You can search for file names. You can search email for: sender, subject, and more.
- You can search for file contents. You can search for email message contents.
- You can create, delete, and modify files. You can create, delete, and modify email messages.
- You can create, delete, and modify folders. You can create, delete, and modify email folders.

What this specification defines:

- How to use existing authentication implementations or use new ones.
- This specification describes a standard way to perform file operations that are remote to the application and agnostic to purpose of data being transported.
- Specifies a way to migrate from some existing protocols to Phoenix. Provides links to sample implementations.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Terms and Definition used in this proposal

The following is a list of terms with their definitions as used in this specification.

AdminCmd
: A general term for any administrative command. Administrative and auditing operations. This list includes commands for authorized users to configure, query logs, errors, possibly user activity.

AuthCmd
: A general term for any authentication command. Authentication and authorization operations. These operations authenticate users and verity their authorization access.

CMD
: A specific protocol operation, or command. They are broken down into, AdminCmd, AuthCmd, FileCmd, and ProtoCmd.

Command, CMD
: Each packet contains a command. This command is also in the reply to the command. Not all commands have a reply. These are called a CMD or command.

FileCmd
: A general term for any file command. File and folder operations. This include creating, getting, modifying, deleting, moving, and renaming files.

Media Type
: Each MIME object has a media type that identifies the content of the object. This specification does not add, remove, or alter any MIME media type;

MIME
: This protocol transports MIME objects. This specification does not remove or alter any MIME objects;

Packet
: A packet is a blob of data that has a header (its length) followed by a Phoenix command with all of its values and parameters. Packets flow in both directions and asynchronously. Commands can be sent while still waiting for other replies. Each endpoint may send commands to the other endpoint without having to be prompted to send information.

Parameter
: Most commands have values that are associated with them. These values are called parameters. For example, the create folder command has the name of the new folder to be created as a parameter.

ProtoCmd
: A general term for all protocol commands. This also includes commands that do not fall into one of the other catagories described here in this definistions section.

SEQ, Command Sequence, CMD_SEQ
: Each command has a unique identifier, a sequence number. All replies to a command include the same sequence number as the original command. In this way replies can be matched up with their original command.

SSL
: For the purpose of this specification, SSL is interchangable with TLS. This document uses the term TLS. The sample implementation uses both SSL and TLS because the legacy UNIX, Linux, Windows, and OpenSSL code uses the term SSL as well as TLS.

TLS
: A way of securely transporting data over the Internet. See RFC-xxxx.

XDR
: RFC-4506 specifies a standard and compatible way to transfer binary information. This protocol uses XDR to transmit a command, its values and any parameters and replies. The MIME data, the payload, is transported as XDR opaque, and is unmodified.

3. Commands Summary

The endpoint that initiates the connection is called the client. The endpoint that is connected to, is called the server. The client is the protocol authority, and the server responds to client commands as configured or instructed by the client.

This section provides an overview of the basic commands. Each command has a detailed section in this specification.

When a command is sent to the remote endpoint and received, the remote endpoint determines if the connection is authenticated or authorized to perform the command. If not supported, or not authorized, a NotSupported command is send as a reply. The NotSupported command sent back has the same Sequence number that was in the original command.

Many commands are only valid after authentication.

When the client connects to a server it immediately sends its pre authentication capabilities to the server. Or an Auth command.

When the server gets a new connection followed by a pre authentication capability command, it immediately sends its pre authentication capabilities to the client.

When the client and server have had a relationship, the client may send an Auth Command to initiate the authorization and does not send its pre authentication capability list to the server. It then waits for the Auth reply from the server.

- If the client gets an Auth reply that is positive, it sends its post authentication capability list to the server.
- If the client gets an Auth reply that is negative, it sends its pre authentication capability list to the server.

When a servers first received packet is a Auth command, It processes the Auth command and sends the Auth reply.

- If the Auth reply is positive, then it also sends it post authentication capability list.
- If the Auth reply is negative, then it sends its pre authentication capability list to the client.

A server may automatically send its pre authentication capability list to the client upon initial connection. Or it may wait to see if it gets a pre authentication capability list, or an Auth command.

If the client sends an Auth command as its first packet, it may get the pre authentication capability from the server before the Auth reply. Simply process both.

3.1. Protocol Commands Summary

In addition to the protocols listed in this specification. Additional protocols and commands can be added in the future. They must follow the same framework listed here.

This protocol connects two endpoints over a network and facilitates the secure and authorized transfer of MIME objects.

This is a binary protocol. The payload can be anything, text or binary. This protocol was designed to reduce the number of back and forth requests and replies between the client and server. By using XDR as the format for transferring binary control information it is portable to any computer architecture. Appendix XXX has the rpcgen definition for the protocol defined in this specification.

After the connection is successful and authenticated, ether endpoint may send commands to the other endpoint. When the server initiates an unsolicited command, it could be a any kind of notification or message for the client side application or the user. It could be reporting errors or updates to previous client initiated commands.

All commands initiated from the client have even numbered command sequence numbers. All commands initiated from the server have odd numbered command sequence numbers.

Some commands expect a command reply. Other commands do not expect a command reply. An example of a command that expects a reply is the ping command. An example of a command that does not expect a reply is the keep-alive command. Conceptually there are two kinds of commands:

Directive commands: A directive type command expects the other endpoint to process the command and possibly reply with some results. An example could be: Send me an index of my emails in my InBox. The client would expect a result. Another example is a bye command, once sent, no reply is expected.

Request commands: A request type command may or might not have any reply. For example, a keep-alive command is a request to not timeout and has no reply. And a send new email notifications command would expect zero or more replies and it would not require them, as they might not happen.

These are not specific protocol entities, these concepts will be used to describe the expected behavior when one of these are transmitted.

3.1.1. Packet Summary

All commands are sent in a packet. A packet has two parts:

1. The packet header.
2. The packet body.

The packet header has one value, the total length of the packet body, and payload sent as an unsigned 64-bit integer in network byte order. The length does not include its own length. It is the total length that follows the length value.

The packet body is divided into three parts:

1. Command sequence (SEQ).
2. The Command (CMD).
3. The command specific data (Payload).

3.1.1.1. Command Sequence Number (SEQ)

The Command SEQ is a 32-bit unsigned integer sent in network byte order. This SEQ is an even number when initiated from the client, and an odd number when initiated from the server.

The first SEQ value sent from the client is zero (0) and is incremented by two each time.

The first SEQ value sent from the server is one (1) and is incremented by two each time.

In the event an endpoint command SEQ reaches its maximum value, then its numbering starts over at zero (0) for the client and one (1) for the server. An implementation must keep track of outstanding commands and not accidentally re-issue the same SEQ that may still get replies from the other endpoint.

3.1.1.2. The Command (CMD)

The command is a predefined enumerated 32-bit unsigned integer sent in network byte order. The value (in hex) 0xFFFFFFFF is reserved for extensions if the 32-bit range is exhausted.

3.1.1.3. The Payload (Payload)

The payload has no predefined length, other what what is specified for the CMD in the packet. It could be zero to vary large in size. It could be opaque data, or it could be data that is XDR encoded. The contents are specific to the CMD specified in the in the packet body.

3.1.2. Packet Reply Summary

All replies to a command are also a command packet. They contain the same command SEQ and command as the original packet. The endpoint recognizes it is a reply because:

- The command SEQ matches one that is waiting a reply.
- When the client gets an even numbered SEQ, it can only be a reply.
- When the server gets an odd numbered SEQ, it can only be a reply.

Some commands have zero to many replies. Each of these multiple replies contains the same SEQ as the original command. An example, the client sends a request to be notified when new email arrives and uses command SEQ 20. Each time a new email arrives, a reply will be sent from the server with a command SEQ of 20. And over time, the client may get many with a SEQ of 20 as new emails arrive on the server.

3.2. Administration Commands Summary

Implementations are not required to implement any ADMIN command. A client will know the server supports one or more ADMIN commands when it gets its post authentication capability command from the server.

Administrative command can be used to configure, audit, and manage the remote endpoint. Administrative command can be used to configure, audit, and manage user access.

3.2.1. Administration Capability Definitions

Implementations MUST NOT send the ADMIN capability in the pre authorization CAPABILITY list.

Implementations that support any administration command MAY include ADMIN capability in the post authentication CAPABILITY list. An implementation may decide that only specified and authorized users may issue administrative commands and send only those authenticated users the ADMIN capability.

The ADMIN capability include the list of ADMIN commands the user is allowed to perform. For example, if a user only has permission to only view user lists, then only the USER_LIST ADMIN capability will be provided.

The capability name is also the command name to use when invoking that capability.

When a user attempts to send a commmand they are not authorized to send, the remote endpoint will reply with a NotSupported command with its sequence number set to the sequence number from offending command.

3.2.2. Administration of users.

The following operations are defined for administration.

Command and Capability Name	Brief Description.
USER_CREATE	May create a new user. And also the command to create a user.
USER_DELETE	May delete a user. And the command to delete a user.
USER_RENAME	May rename a user. And the command to rename a user.
USER_LIST	May list users and their capabilities. And the command to list users.
USER_PERMISSIONS	May update other users permissions. And the command to view and set user permissions.
SERVER_SHUTDOWN	May shutdown the server. And the command to shutdown the server.
SERVER_LOGS	May view the server logs. And the command to view server logs.
SERVER_KICK_USER	May logout a user. And limit when they can use the server again. And the command to kick and limit a user.
SERVER_MANAGE_BANS	May manage IP and user bans. And the command to manage ban users an IP addresses.
SERVER_VIEW_STATS	May view server statistics. And the command to view statistics.

Command and Capability Name	Brief Description.
SERVER_CONFIGURE	May configure the server. If sent with a VIEW_ONLY parameter, then the user may only view the configuration information. And the command to view and alter the server configuration information.

Table 1

3.3. Authentication Commands Summary

TODO

3.4. Calendar Commands Summary

These command are based on iCalendar and iTIp.

3.5. Capability Commands Summary

This section

3.6. EMail Commands Summary

These commands allow for the fetching and submission of EMail messages

3.7. File and Folder Commands Summary

The file operations (FileOp) have protocol names. Here are their protocol names and a breif description.

Implementations are not required to support any or all of these commands.

Op Name	Brief Description.
FOLDER_CAPABILITY	When sent as a command, request the list of folder commands supported. When sent as a reply, includes the list of folder commands supported.
FOLDER_CREATE	Create a new folder. Also the name of the capability for this permission.
FOLDER_COPY	Copy a folder. Also the name of the capability for this permission.
FOLDER_DELETE	Delete a folder. Also the name of the capability for this permission.
FOLDER_RENAME	Rename a folder. Also the name of the capability for this permission.

Op Name	Brief Description.
FOLDER_MOVE	Move a folder. Also the name of the capability for this permission.
FOLDER_SHARE	Share a folder. Also the name of the capability for this permission.
FOLDER_LIST	List folders and files. Also the name of the capability for this permission.
FILE_CREATE	Create a new file. Also the name of the capability for this permission.
FILE_COPY	Copy a file. Also the name of the capability for this permission.
FILE_DELETE	Delete a file. Also the name of the capability for this permission.
FILE_RENAME	Rename a file. Also the name of the capability for this permission.
FILE_MOVE	Move a file. Also the name of the capability for this permission.
FILE_SHARE	Share a file. Also the name of the capability for this permission.
FILE_GET	Get a file. Also the name of the capability for this permission.
FILE_MODIFY	Modify the contents of an existing file. Also the name of the capability for this permission.

Table 2

3.8. KeepAlive Command Summary

The KeepAlive command is sent to the server from the client. It requests the server not time out. The server may honor or ignore the request.

The Phoenix protocol is designed to transfer data and a server may handle a small subsets of what is possible. Which is why the server decides what is an important command while determining idle timeout.

When the server sends the post authentication capabilities to the client, it includes an IdleTimeout capability that includes the number of seconds it allows for idle time. If no significant action has been taken by the client, as determined by the server, in that time the server may timeout and close the connection.

The KeepAlive command tells the server that the client wishes the server not to time out as long as a KeepAlive or other command is sent to the server before IdleTimeout seconds have passed.

An IdleTimeout capability can be a positive number, zero, or a negative number.

- A positive number is the maximum idle time in seconds before the server terminates the connection.

- When the IdleTimeout is zero (0), the server does not timeout.
- When the IdleTimeout is less than zero (< 0), it means it ignores KeepAlive and it will idle out in the absolute value of the IdleTimeout value in seconds. For example, a value of (-300) means it will ignore KeepAlive and timeout when the server determines nothing significant has happened in 5 minutes (300 seconds).

Servers that are not threaded or can not reply to simultaneous or overlapping commands, MUST set their IdleTimeout to zero (0) or a negative number.

Clients MUST NOT send KeepAlive commands to a server that has an IdleTimeout of zero (0) or negative (< 0).

Clients MUST NOT send KeepAlive commands to the server until at least 75% of the idle time has passed since the last command has been sent to the server.

A server may terminate a connection if the server implementation determines that KeepAlive commands are arriving to quickly.

3.9. Ping Command Summary

The ping command only sent when the client implementation has determined it has waited too long for a command reply. The ping command is only initiated from the client. It is not valid for the server to send a ping command to a client.

The ping command MUST NOT be the first command sent to the server. It should only be sent when the client implementation determines it has waited too long for a reply.

If the server supports the ping command, then a PING capability is sent in the pre authentication capability command.

Sometimes servers are unavailable and can go down. A server could be down for maintenance, or in a shutdown mode. It might limit the number of simultaneous connections. It might be very busy. The packets might not be making it to the server because of network issues.

When a ping command is received by the server:

- When the server did not send PING capability to the client. Then the server replies with a NotSupported packet with the sequence number the same as in the ping command.
- When the server has not yet received an authentication command, the server replies with a NotSupported packet with the sequence number the same as in the ping command.
- When the server has received an authentication command, and has not yet replied to an authentication command. Then the server sends a ping reply, with the same sequence number that was in the ping command. This could happen when the client implementation had determined it has waited too long for an authentication reply.
- When the client is authenticated, and when the server is available for processing commands. Then the server replies with a ping reply with the same sequence number. This could happen when the client implementation had determined it has waited too long for an expected reply.

If the server is alive and not available, the server will reply with a NotSupported command, with its sequence number set to the sequence number in the ping command.

If a connected and authenticated client has been waiting for a reply or for some other reason needs to determine if the server is still available. It can send a ping command. If the server is still available, it sends a ping reply. If it is no longer available for any reason, it sends a NotSupported reply.

Endpoints MUST NOT send a ping command if they are awaiting the results of a previously sent ping command.

Endpoints MUST NOT send more than two ping commands per minute.

Clients and servers must give priority to ping commands. If possible, reply as soon as it receives the command.

The server MAY consider too many ping commands as a malfunctioning or malicious client and terminate the connection.

Servers that are not threaded or can not reply to simultaneous or overlapping commands, MUST NOT include PING in their capability command.

3.10. S/MIME Commands Summary

4. Over the Wire Protocol Detail

This section specifies the details of what is transmitted over the network.

All protocol data transmitted between the endpoints is sent in network byte order.

All payload data transmitted between the endpoints is sent in original format. The payload consent is seen as an opaque blob of data within a command packet.

When a command packet is received by ether endpoint it: (1) Checks the command sequence number to determine if it is a reply or not. (2) If it is a reply, it looks at the command and dispatches it to the implementations commands reply code. (3) If is not a reply, it looks at the command and dispatches it to the implementations command code.

A command and all of its replies, use the same format as described here.

A packet has a 64-bit unsigned integer in network byte order that is set to the octet count of all of the data that follows this length value. The shortest packet is 16 octets in size, with a length value set to 8. With 8 octets for the length, and 8 octets for the packet.

Followed by a 32-bit unsigned integer in network byte order that is the command sequence number.

Followed by a 32-bit unsigned integer in network byte order that is the command.

Followed by zero or more octets of payload data.

There is no space, padding, or line endings between the parts of the packet. The payload is sent without any modification and is not encoded or transformed in any way. A packet is shown here vertically only to aid in readability.

```
+-----------------------------------------------------------------+
| ...64-bit.unsigned.integer.length ..............................|
+-----------------------------------------------------------------+
| ...32-bit.unsigned.command.SEQ...|
+----------------------------------+
| ...32-bit.unsigned.command.CMD...|
+----------------------------------+
| payload.....
```

The payload size and format varies for each command. The details of the payload content, and the format of that content, is described in each specific CMD section.

An implementation can send, receive, and dispatch packets within its implementation by looking at the length, SEQ, and CMD, then passing the payload to code that can handle that payload.

- Read in a 64-bit value. - Convert the value from network byte order, to host byte order. This is the total length of the data that follows. - Read in length octets into the packet payload. - Get the 32-bit value in the payload, it is the SEQ in network byte order. - Convert the SEQ from network byte order, to host byte order. - Get another 32-bit value in the payload, it is the CMD in network byte order. - Convert the CMD from network byte order, to host byte order. - Dispatch the CMD with SEQ and all of the data that follows to implementation

The following is pseudo code that explains how processing incoming XDR data can be handled:

```
// Where:
//  uint64_t, is a 64-bit unsigned integer.
//  uint32_t, is a 32-bit unsigned integer.
//  uint8_t *, is a pointer to 8-bit data.
//  XDR, is an XDR object.
//
//  CmdPacket, is an object that represents all commands
//  and replies.
//
//  NOTE: See the sample implementation.
//
uint64_t   NetLength;
uint64_t   PacketLength;
uint8_t *  Data;
uint8_t *  DataPointer;
XDR        Xdr;
CmdPacket  Packet;

// Read the length and convert to host byte order.
//
```

```
read(FromClientSocket, &NetLength, sizeof(uint64_t));
PacketLength = ntohll(NetLength);

// Allocate PacketLength data, and read it.
//
Data = new uint8_t[PacketLength]
DataPointer = Data;

// Initialize the XDR deserializer.
//
xdrmem_create(&Xdr, Data, PacketLength, XDR_DECODE);

// Decode the received data into a Packet.
//
if (xdr_CmdPacket(&Xdr, &Packet)) {

  // If the lowest bit is set, it is an odd number.
  //
  if (Packet.Sequence & 0x01) {
    SequenceIsEvenNumber = false;
  } else {
    SequenceIsEvenNumber = true;
  }

  // The client sends even numbered sequences, and the server
  // sends the same even numbers sequence in the reply to
  // the command.
  //
  // If a client gets an odd numbered sequence, it is a command
  // from the other endpoint.
  //
  // The server sends odd numbered sequences, and the client
  // sends the same odd numbers sequence in the reply to
  // the command.
  //
  // If a server gets an even numbered sequence, it is a
  // command from theother endpoint.
  //
  if (WeAreTheClient) {
    if (SequenceIsEvenNumber) {
      DispatchReply(Packet);
    } else {
      DispatchCommandFromOtherEndpoint(Packet);
    }
  } else {
    if (SequenceIsEvenNumber) {
      DispatchCommandFromOtherEndpoint(Packet);
    } else {
      DispatchReply(Packet);
    }
  }
}
```

5. IANA Considerations

This memo includes no request to IANA. [CHECK]

6. Security Considerations

This document should not affect the security of the Internet. [CHECK]

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[exampleRefMin] Surname [REPLACE], Initials [REPLACE]., "Title [REPLACE]", 2006.

[exampleRefOrg] Organization [REPLACE], "Title [REPLACE]", 1984, <http://www.example.com/>.

Appendix A. Administrative Enumerated Binary Values

Phoenix is a binary protocol. Each value is sent as an unsigned 32-bit integer in xdr format.

The values for the commands are arbitrary and were assigned as created. There is no plan or origination to the numbers. There is no priority or superiority to any value. The table is sorted by name, not value.

The values are not unique. They are only unique within the context in which they are used.

Some of these values are reused for other commands. For example USER_CREATE is both an (a) AUTH capability reply informing the user that they have permission to create a user with the (b) USER_CREATE command.

Some values may be reused if they are parameter arguments to other commands. For example xxxxxx.

Decimal Value	Command / Capability Name	Brief Description.
x	USER_CERT	Manage a users certificate.
x	USER_CREATE	When sent in a capability reply USER_CREATE informs the user that they have permission to create users. When sent as a command the USER_CREATE instructs the other endpoint to create a named user.
x	USER_DELETE	Delete a user.
x	USER_LIST	List users and their capabilities.
x	USER_PERMISSIONS	Update user permissions.
x	USER_RENAME	Rename a user.
x	USER_RESET	Used to coordinate resetting a users authentication information.
4294967296	Reserved for future expansion.	4294967296 has a hex value of: 0xffffffff

Table 3

Appendix B. Authentication Enumerated Binary Values

Phoenix is a binary protocol. Each value is sent as an unsigned 32-bit integer in xdr format.

The values for the commands are arbitrary and were assigned as created. There is no plan or origination to the numbers. There is no priority or superiority to any value. The table is sorted by name, not value.

The values are not unique. They are only unique within the context in which they are used.

Some of these values are reused for other commands. For example USER_CREATE is both an (a) AUTH capability reply informing the user that they have permission to create a user with the (b) USER_CREATE command.

Some values may be reused if they are parameter arguments to other commands. For example xxxxxx.

Decimal Value	Command / Capability Name	Brief Description.
x	AUTH_TODO	xxx.

Decimal Value	Command / Capability Name	Brief Description.
xxx	AUTH_xxx	xxx.
4294967296	Reserved for future expansion.	4294967296 has a hex value of: 0xffffffff

Table 4

Appendix C. File and Folder Enumerated Binary Values

Phoenix is a binary protocol. Each value is sent as an unsigned 32-bit integer in xdr format.

The values for the commands are arbitrary and were assigned as created. There is no plan or origination to the numbers. There is no priority or superiority to any value. The table is sorted by name, not value.

The values are not unique. They are only unique within the context in which they are used.

Some of these values are reused for other commands. For example USER_CREATE is both an (a) AUTH capability reply informing the user that they have permission to create a user with the (b) USER_CREATE command.

Some values may be reused if they are parameter arguments to other commands. For example xxxxxx.

Decimal Value	Command / Capability Name	Brief Description.
x	FILE_TODO	xxx.
xxx	FILE_xxx	xxx.
4294967296	Reserved for future expansion.	4294967296 has a hex value of: 0xffffffff

Table 5

Appendix D. Protocol Enumerated Binary Values

Phoenix is a binary protocol. Each value is sent as an unsigned 32-bit integer in xdr format.

The values for the commands are arbitrary and were assigned as created. There is no plan or origination to the numbers. There is no priority or superiority to any value. The table is sorted by name, not value.

The values are not unique. They are only unique within the context in which they are used.

Some of these values are reused for other commands. For example USER_CREATE is both an (a) AUTH capability reply informing the user that they have permission to create a user with the (b) USER_CREATE command.

Some values may be reused if they are parameter arguments to other commands. For example xxxxxx.

Decimal Value	Command / Capability Name	Brief Description.
x	PROTO_TODO	xxx.
xxx	PROTO_xxx	xxx.
4294967296	Reserved for future expansion.	4294967296 has a hex value of: 0xffffffff

Table 6

Appendix E. RPCGEN protocol specification

The following is the extendable RPCGEN specification for the Phoenix protocol defined in this document.

E.1. RPCGEN - Acl

```
%#ifdef BUILDING_LIBPHOENIX
%#include "Types.hpp"
%#else
%#include <RiverExplorer/Phoenix/Types.hpp>
%#endif

#ifdef RPC_HDR
%/**
% * The Acl_Cmd ...
% */
#endif
class Acl
{
        int Todo;
};
```

E.2. RPCGEN - Administration

```
%#ifdef BUILDING_LIBPHOENIX
%#include "Types.hpp"
%#else
%#include <RiverExplorer/Phoenix/Types.hpp>
%#endif

#ifdef RPC_HDR
%/**
% * The Administratoin Commands
% */
#endif
enum AdministrativeCommands_e
{
        USER_CREATE = 0,
        USER_DELETE = 1,
        USER_RENAME = 2,
        USER_LIST = 3,
        USER_PERMISSIONS = 4,
        SERVER_SHUTDOWN = 5,
        SERVER_LOGS = 6,
        SERVER_KICK_USER = 7,
        SERVER_MANAGE_BANS = 8,
        SERVER_VIEW_STATS = 9
};

#ifdef RPC_HDR
%/**
% * The Administratoin Command ...
% */
#endif
class Administration
{
        int Todo;
};

#ifdef RPC_HDR
%/**
% * The Administratoin Reply Command ...
% */
#endif
class AdministrationReply
{
        int Todo;
};
```

E.3. RPCGEN - Authenticate

```
%
%#ifdef BUILDING_LIBPHOENIX
%#include "Types.hpp"
%#else
```

```
%#include <RiverExplorer/Phoenix/Types.hpp>
%#endif

#ifdef RPC_HDR
%/**
% * Authentication is initiated by the endpoing doing the inital
% * connection, to the endpoint it is connecting to.
% *
% * The start of the authentication process take one of two
% * directions:
% *
% * (1) New account, new client, or new authentication mechanism being
% * attempted.
% *
% * (2) - Existing account from a previously used client using a
% * previously known to work (from the clients point of view) authentication
% * mechanism.
% *
% * New is divided up into (1.a) unknown or new account or (1.b) known
account.
% *
% * (1.a) New, known account:
% * Just after the network connection is made, the client sends its
% * pre authentication capabilities to the server, then waits
% * for the pre authentication capabilities packet to arrive from
% * the server. The server supplied pre authentication packet includes
% * the authentication mechanisms it suppots.
% *
% * (1.b) New, unknown account:
% * Starts off like (a), then checks the servers capability set for
% * "allow-new-accounts". If provided, then the sign-up procedure is
% * followed. (sign-up documentation below). Followed by an authentication
% * to verify it worked.
% *
% * If "allow-new-accounts" is not provided, then the account information
% * must be aquired by methods external to this protocol.
% *
% * @note
% * Allowing new users to sign up using this protocol can be site
% * specific and may include procedures external to this protocol
% * such as visiting web sites or other external verification processes.
% *
% * @note
% * For security and anti-junk user accounts, many site may choose not enable
% * "allow-new-accounts". For servers internal to orginazations or on secure
% * networks this might be enabled.
% *
% * (2) Existing or known:
% * Just after the network connection is made, the client sends its
% * pre authentication capabilities to the server. Then without
% * waiting sends any first step authentication data to the server.
% * These are two separate packets each unique and independent.
% *
% * In both cases:
% * Authentication proceeds.
% */
#endif
struct AuthMD5
```

```
{
        string Account<>;
        string Md5Password<>;
};

struct Authenticate
{
        AuthMD5 Md5;
};

struct AuthenticateReply
{
        bool_t  Accepted;
};
```

E.4. RPCGEN - Capability

```
%
%#ifdef BUILDING_LIBPHOENIX
%#include "Types.hpp"
%#else
%#include <RiverExplorer/Phoenix/Types.hpp>
%#endif

#ifdef RPC_HDR
%/**
% * The Capability command informs the other endpoint about
% * its capabilities.
% *
% * This is done once at connection time.
% * And once after authentication is successful.
% * All other attempts will get a NotSupported_Cmd reply.
% *
% * A single capability is a string key, and a string value.
% * The value for each capability is described in its own
% * section.
% *
% * A capability value may contain one or more values, each separated
% * as defined in the capability description.
% * It is suggested that a comma (HEX 2C) be used. Except when
% * that would complicate the capability value.
% * In all cases, the capability value is defined separately for
% * each capability.
% *
% * If the capability list does not include the capability name,
% * then it is not supported.
% *
% * If the reply contains the capability name, then
% * its associated value will be used to determine the
% * extent of its support.
% *
% * Capability keys MUST BE processed in all lower case.
% * If a capability arrives in upper or mixed case,
% * the receiver MUST covert then check to see if that is
% * valid. This prevents capabilities with the same name
```

```
% * and varying case from being used.
% *
% * Capability values SHOULD BE in all lower case.
% * Except when the capability itself contains values
% * that must be upper or mixed case.
% *
% * Capabilties that have a boolean value, SHOULD use
% * 'true' or 'false' and not 'yes', 'no' or other variations of true or
false.
% *
% * Capabilties that have a enabled or disabled value, SHOULD use
% * 'enabled' or 'disabled' and not 'yes', 'no' or other variations of
% * enabled or disabled.
% *
% */
#endif

class Capability
{
        ArrayOfStrings  Supported<>;
};

#ifdef RPC_HDR
%/**
% * Capability FolderCapabilities_e Capabilities that
% * apply to folder or directories.
% *
% * Folder capabilites should not be provided in pre-authentication
% * capability packets.
% *
% * @note
% * Not call capabilities are applicable to all endpoints, files,
% * folders, users, or specific commands. Read the associated
% * command and capability specifications to understand each
% * operation.
% *
% * The capability specifies the endpoing is capable of the
% * function. It may be further restriced by who is authenticated
% * or acess control lists (ACLs) on specific associated items.
% *
% * <ul>
% * <li>CanList: Has a key of "canlist" and has a boolean value.
% * -When true, then a list of files and folders can be accessed.
% * -When false, then only already known named files and folders can be
accessed.
% * </li>
% *
% * <li>CanSubscribe: Has a key value of "cansubscribe" and has
% * a boolean value.
% * -When true, then this server supports unsolicited push notifcations.
% * -When false, then no unsolicited push notifcations can not be sent
% * from this endpoint.
% * </li>
% *
% * <li>CanCreate: Has a key value of "cancreate" and has a boolean value.
% * -When true, then this endpoint supports creating folders.
% * -When false, this endpoint does not support creating folders.
% * <li>
```

```
% *
% * <li>CanRemove: Has a key value of "canremove" and has a boolean value.
% * -When true, this endpoint supports removing folders.
% * -When fales, this endpoint does not support removing foldres.
% * <li>
% *
% * <li>CanRename: Has a key value of "canrename" and has a boolean value.
% * When true, this endpoint supports renaming folders.
% * When false, this endpoint does not support renaming folders.
% * <li>
% *
% * <li>CanCopy: Has a key value of "cancopy" and has a boolean value.
% * When true, this endpoint supports copying folders.
% * When false, this endpoint does not support copying folders.
% * <li>
% *
% * <li>CanSearch: Has a key value of "cansearch" and has a boolean value.
% * When true, this endpoint supports searching folders names using posix
regex expressions
% * When false, this endpoint does not support searching folders.
% * <li>
% *
% * <li>Acls: Has a key value of 'acls' and has a string value.
% * When supplied, the endpoint supports at least one acl type.
% * The types currely defined in the Acls_e enumeration.
% */
#endif

enum FolderCapabilities_e
{
        CanList,
        CanSubscribe,
        CanCreate,
        CanRemove,
        CanAppend,
        CanRename,
        CanUpdate,
        CanCopy,
        CanSearch,
        Acls
};

enum Acls_e
{
        OwnerRW_t,
        OwnerRO_t,
        GroupRW_t,
        GroupRO_t,
        OtherRW_t,
        OtherRO_t,
        NamedListRW_t,
        NamedListRO_t
};
```

E.5. RPCGEN - Folder

```
%
%#ifdef BUILDING_LIBPHOENIX
%#include "Types.hpp"
%#include "MetaData.hpp"
%#else
%#include <RiverExplorer/Phoenix/Types.hpp>
%#include <RiverExplorer/Phoenix/MetaData.hpp>
%#endif

#ifdef RPC_HDR
%/**
% */
#endif

enum Folder_e
{
        FolderCreate_Cmd = 0,
        FolderCreateReply_Cmd = 1,
        FolderCopy_Cmd = 2,
        FolderCopyReply_Cmd = 3,
        FolderDelete_Cmd = 4,
        FolderDeleteReply_Cmd = 5,
        FolderRename_Cmd = 6,
        FolderRenameReply_Cmd = 7,
        FolderMove_Cmd = 8,
        FolderMoveReply_Cmd = 9,
        FolderShare_Cmd = 10,
        FolderShareReply_Cmd = 11,
        FolderList_Cmd = 12,
        FolderListReply_Cmd = 13,
        FileCreate_Cmd = 14,
        FileCreateReply_Cmd = 15,
        FileCopy_Cmd = 16,
        FileCopyReply_Cmd = 17,
        FileDelete_Cmd = 18,
        FileDeleteReply_Cmd = 19,
        FileRename_Cmd = 20,
        FileRenameReply_Cmd = 21,
        FileMove_Cmd = 22,
        FileMoveReply_Cmd = 23,
        FileShare_Cmd = 24,
        FileShareReply_Cmd = 25,
        FileGet_Cmd = 26,
        FileGetReply_Cmd = 27
};

#ifdef RPC_HDR
%/**
% * @class FolderCreate CmdFolder.hpp <RiverExplorer/Phoenix/CmdFolder.hpp>
% * @addtogroup Folder
% *
% * The full path is the path from the top of the users virtual
% * home folder, and includes the folder name.
% *
```

```
% * The path separator is the '/' (UTF-8 value 0x2f) character.
% *
% * The root folder is "/".
% */
#endif
class FolderCreate
{
        string  FullPath<>;
};

#ifdef RPC_HDR
%/**
% * @class FolderCreateReply CmdFolder.hpp <RiverExplorer/Phoenix/
CmdFolder.hpp>
% * @addtogroup Folder
% * The reply for CreateFolder, Success is set to true if the
% * folder was created. Otherwise it is set to false.
% */
#endif
class FolderCreateReply
{
        bool_t  Success;
};

#ifdef RPC_HDR
%/**
% * @class FolderCopyr CmdFolder.hpp <RiverExplorer/Phoenix/CmdFolder.hpp>
% * @addtogroup Folder
% *
% * The full original path is the path from the top of the users virtual
% * home folder, and includes the folder name. And names
% * the folder to copy from.
% *
% * The full destination path is the path from the top of the users virtual
% * home folder, and includes the folder name.
% * And names the folder that will have a copy of FullOriginalPath
% * placed into.
% *
% * When recursive is false, only the contents are copied
% * and not any directories.
% *
% * When recursive is true, the contents are copied
% * and recursively copies all directories in the original path directories
% * to the new destination.
% *
% * The path separator is the '/' (UTF-8 value 0x2f) character.
% *
% * The root folder is "/".
% */
#endif
class FolderCopy
{
        string  FullOriginalPath<>;
        string  FullDestinationPath<>;
        bool_t  Recursive;
};

#ifdef RPC_HDR
```

```
%/**
% * @class FolderCopyReply CmdFolder.hpp <RiverExplorer/Phoenix/
CmdFolder.hpp>
% * @addtogroup Folder
% *
% * The reply for CopyFolder, Success is set to true if the
% * folder was copied into FillToPath. Otherwise it is set to false.
% *
% * A false indicates that nothing was copied.
% * A true indicates that everything was copied.
% *
% * Must fail and leave the original structure in place
% * on any failure, and return false.
% */
#endif
class FolderCopyReply
{
        bool_t  Success;
};

class FolderDelete
{
        int todo;
};

class FolderDeleteReply
{
        int todo;
};

class FolderRename
{
        int todo;
};

class FolderRenameReply
{
        int todo;
};

class FolderMove
{
        int todo;
};

class FolderMoveReply
{
        int todo;
};

class FolderShare
{
        int todo;
};

class FolderShareReply
{
        int todo;
```

```
};

class FolderList
{
        int todo;
};

class FolderListReply
{
        int todo;
};

class FileCreate
{
        int todo;
};

class FileCreateReply
{
        int todo;
};

class FileCopy
{
        int todo;
};

class FileCopyReply
{
        int todo;
};

class FileDelete
{
        int todo;
};

class FileDeleteReply
{
        int todo;
};

class FileRename
{
        int todo;
};

class FileRenameReply
{
        int todo;
};

class FileMove
{
        int todo;
};

class FileMoveReply
```

```
{
        int todo;
};

class FileShare
{
        int todo;
};

class FileShareReply
{
        int todo;
};

class FileGet
{
        int todo;
};

class FileGetReply
{
        int todo;
};

union FolderCmdData switch (Folder_e FCmd)
{
 case FolderCreate_Cmd:
         FolderCreate * FolderCreateFolder;

 case FolderCopy_Cmd:
         FolderCopy * FolderCopyData;

 case FolderDelete_Cmd:
         FolderDelete * FolderDeleteData;

 case FolderRename_Cmd:
         FolderRename * FolderRenameData;

 case FolderMove_Cmd:
         FolderMove * FolderMoveData;

 case FolderShare_Cmd:
         FolderShare * FolderShareData;

 case FolderList_Cmd:
         FolderList * FolderListData;

 case FileCreate_Cmd:
         FileCreate * FileCreateData;

 case FileCopy_Cmd:
         FileCopy * FileCopyData;

 case FileDelete_Cmd:
         FileDelete * FileDeleteData;

 case FileRename_Cmd:
         FileRename * FileRenameData;
```

```
 case FileMove_Cmd:
         FileMove * FileMoveData;

 case FileShare_Cmd:
         FileShare * FileShareData;

 case FileGet_Cmd:
         FileGet * FileGetData;

};

union FolderReplyData switch (Folder_e FCmd)
{
 case FolderCreateReply_Cmd:
         FolderCreateReply * FolderCreateReplyData;

 case FolderCopyReply_Cmd:
         FolderCopyReply * FolderCopyReplyData;

 case FolderDeleteReply_Cmd:
         FolderDeleteReply * FolderDeleteReplyData;

 case FolderRenameReply_Cmd:
         FolderRenameReply * FolderRenameReplyData;

 case FolderMoveReply_Cmd:
         FolderMoveReply * FolderMoveReplyData;

 case FolderShareReply_Cmd:
         FolderShareReply * FolderShareReplyData;

 case FolderListReply_Cmd:
         FolderListReply * FolderListReplyData;

 case FileCreateReply_Cmd:
         FileCreateReply * FileCreateReplyData;

 case FileCopyReply_Cmd:
         FileCopyReply * FileCopyReplyData;

 case FileDeleteReply_Cmd:
         FileDeleteReply * FileDeleteReplyData;

 case FileRenameReply_Cmd:
         FileRenameReply * FileRenameReplyData;

 case FileMoveReply_Cmd:
         FileMoveReply * FileMoveReplyData;

 case FileShareReply_Cmd:
         FileShareReply * FileShareReplyData;

 case FileGetReply_Cmd:
         FileGetReply * FileGetReplyData;

};
```

```
#ifdef RPC_HDR
%/**
% * An XML representation of a file, not the
% * contents, but the information about the file.
% *
% * - Meta: Is an array of MetaData.
% * - Name: This is the name excluding the path.
% * - Size: This is the full size of the file.
% * The FLAG_... symbols are symbolic names
% */
#endif

class FileInformation
{
        MetaData        Meta<>;
        string          Name<>;
        uint64_t        Size;
        uint32_t        FlagBits;
};

#ifdef RPC_HDR
%/**
% * An XML representation of a folder
% *
% * - Meta: Is an array of MetaData.
% * - Name: This is the name excluding the path.
% * - Folders: An array of information about folders within this folder.
% * - Files: An array of information about files in this folder.
% */
#endif
class FolderInformation
{
        MetaData                Meta<>;
        string                  Name<>;
        FolderInformation       Folders<>;
        FileInformation         Files<>;
};

class Folder
{
        FolderCmdData Data;
};

class FolderReply
{
        FolderReplyData Data;
};
```

E.6. RPCGEN - KeepAlive

```
%
%#ifdef BUILDING_LIBPHOENIX
%#include "Types.hpp"
%#else
%#include <RiverExplorer/Phoenix/Types.hpp>
%#endif

#ifdef RPC_HDR
%/**
% * The KeepAlive command sends a packet to the remote endpoint.
% *
% * There is no reply to a KeepAlive command.
% */
#endif
struct KeepAlive
{
        int foo;
};
```

E.7. RPCGEN - NotSupported

```
%
%#ifdef BUILDING_LIBPHOENIX
%#include "Types.hpp"
%#else
%#include <RiverExplorer/Phoenix/Types.hpp>
%#endif

#ifdef RPC_HDR
%/**
% * Not supported. This is sent back to the initiating endpoint
% * when this endpoint does not support the command sent.
% *
% * @note
% * There is no data associated with a NotSupported_Cmd, only the
% * CmdPacket is sent.
% */
#endif

struct NotSupported
{
        int foo;
};

struct NotSupportedReply
{
        int foo;
};
```

E.8. RPCGEN - Ping

```
%
%#ifdef BUILDING_LIBPHOENIX
%#include "Types.hpp"
%#else
%#include <RiverExplorer/Phoenix/Types.hpp>
%#endif

#ifdef RPC_HDR
%/**
% * The Ping command sends a packet to the remote endpoint.
% * The other endpoint does a PingReply with no data.
% *
% * The reply is required.
% */
#endif
class Ping
{
        int foo;
};

#ifdef RPC_HDR
%/**
% * The Ping Reply command sends a packet to the remote endpoint.
% * The other endpoint does a PingReply with no data.
% *
% * The reply is required.
% */
#endif
class PingReply
{
        int foo;
};

#ifdef RPC_HDR
%/**
% * @return a new Ping CmdPacket.
% */
#endif
%namespace RiverExplorer::Phoenix
%{
%class CmdPacket;
%extern CmdPacket * NewPing(CommandSequence Seq);
%}
```

E.9. RPCGEN - Commands

```
%#ifdef BUILDING_LIBPHOENIX
%#include "CppTypes.hpp"
%#else
%#include <RiverExplorer/Phoenix/CppTypes.hpp>
```

```
%#endif

#ifdef RPC_HDR
%/**
% * Command_e: An enumerated list of fetch commands.
% * <ul>
% * <li>
% *     Admin_Cmd - The packet contains an administrative command.
% * </li>
% * <li>
% *     AdminReply_Cmd - The packet contains an administrative command reply.
% * </li>
% * <li>
% *     Auth_Cmd - The packet contains an authentication command.
% * </li>
% * <li>
% *     AuthReply_Cmd - The packet contains an authentication command reply.
% * </li>
% * <li>
% *     Capability_Cmd - The packet contains a capability command.
% * A Capability_Cmd has no reply.
% * </li>
% * <li>
% *     Folder_Cmd - The packet contains a folder command.
% * </li>
% * <li>
% *     FolderReply_Cmd - The packet contains a folder command reply.
% * </li>
% * <li>
% * The NotSupported_Cmd is sent back to
% * the remote endpoint when it sends a command
% * that is not supported.
% * It can be because of access control list,
% * out of sequence, or other error.
% * A Capability_Cmd has no reply.
% * </li>
% * <li>
% *     Ping_Cmd - The packet contains a pint command reply.
% * The reply to a ping is the same packet back.
% * </li>
% * <li>
% *     Proto_Cmd - The packet contains a protocol command.
% * A protocol command is an extension command not built int
% * the core Phoenix protocol.
% * </li>
% * <li>
% *     ProtoReply_Cmd - The packet contains a protocol command reply.
% * </li>
% * <li>
% *     Reserved_Cmd - In the unlikely event that 2^32 commands
% * are ever created, this is an escape to allow more.
% * </li>
% * </ul>
% *
% */
#endif
enum Command_e
{
```

```
        Admin_Cmd = 1,
        AdminReply_Cmd = 2,
        Auth_Cmd = 3,
        AuthReply_Cmd = 4,
        Capability_Cmd = 5,
        Folder_Cmd = 6,
        FolderReply_Cmd = 7,
        NotSupported_Cmd = 8,
        Ping_Cmd = 9,
        Proto_Cmd = 10,
        ProtoReply_Cmd = 11,
        Reserved_Cmd = 0xffffffff
};

#ifdef RPC_HDR
%/**
% * The transport top level is simple.
% * You can Send() a packet and get a packet back.
% * Or you send a notification that receives nothing back.
% * Or you send a broadcast message to all interested participants, with no
% * reply expected.
% */
#endif

#ifdef RPC_HDR

%#ifdef BUILDING_LIBPHOENIX
%#include "CmdAcl.hpp"
%#include "CmdAddMessage.hpp"
%#include "CmdAuthenticate.hpp"
%#include "CmdAdministration.hpp"
%#include "CmdCapability.hpp"
%#include "CmdCopyMessage.hpp"
%#include "CmdFolder.hpp"
%#include "CmdExpunge.hpp"
%#include "CmdGetMessage.hpp"
%#include "CmdKeepAlive.hpp"
%#include "CmdNotSupported.hpp"
%#include "CmdPing.hpp"
%#include "CmdSearch.hpp"
%#include "CmdSubscribe.hpp"
%#include "CmdTimeout.hpp"
%#include "CmdUpdateMessage.hpp"
%#include "Commands.hpp"
%#else
%#include <RiverExplorer/Phoenix/CmdAcl.hpp>
%#include <RiverExplorer/Phoenix/CmdAddMessage.hpp>
%#include <RiverExplorer/Phoenix/CmdAuthenticate.hpp>
%#include <RiverExplorer/Phoenix/CmdAdministration.hpp>
%#include <RiverExplorer/Phoenix/CmdCapability.hpp>
%#include <RiverExplorer/Phoenix/CmdCopyMessage.hpp>
%#include <RiverExplorer/Phoenix/CmdFolder.hpp>
%#include <RiverExplorer/Phoenix/CmdExpunge.hpp>
%#include <RiverExplorer/Phoenix/CmdGetMessage.hpp>
%#include <RiverExplorer/Phoenix/CmdKeepAlive.hpp>
%#include <RiverExplorer/Phoenix/CmdNotSupported.hpp>
%#include <RiverExplorer/Phoenix/CmdPing.hpp>
%#include <RiverExplorer/Phoenix/CmdSearch.hpp>
```

```
%#include <RiverExplorer/Phoenix/CmdSubscribe.hpp>
%#include <RiverExplorer/Phoenix/CmdTimeout.hpp>
%#include <RiverExplorer/Phoenix/CmdUpdateMessage.hpp>
%#include <RiverExplorer/Phoenix/Commands.hpp>
%#endif
#endif

union CmdData switch (Command_e Cmd)
{
 case Admin_Cmd:
        Administration *       AdminData;

 case AdminReply_Cmd:
        AdministrationReply *  AdminReplyData;

 case Auth_Cmd:
        Authenticate           *       AuthData;

 case AuthReply_Cmd:
        AuthenticateReply              *       AuthReplyData;

 case Capability_Cmd:
        Capability             *       CapabilityData;

 case Folder_Cmd:
        Folder *       FolderData;

 case FolderReply_Cmd:
        FolderReply    *       FolderReplyData;

 case NotSupported_Cmd:
        void;

 case Ping_Cmd:
        void;

};

#ifdef RPC_HDR
%/**
% * Set the callback for a command.
% *
% * @param Cmd The command being registered.
% *
% * @param Callback The user supplied callback function.
% *
% * @note
% * It is is recommended that each registered callback be thread safe.
% */
%namespace RiverExplorer::Phoenix
%{
%extern bool Register_Cmd(Command_e Cmd, CommandCallback * Callback);
%}
#endif

#ifdef RPC_HDR
%/**
% * Set the callback for a command.
```

```
% *
% * @param Cmd The command being registered.
% *
% * @param Callback The user supplied callback function.
% *
% * @note
% * It is is recommended that each registered callback be thread safe.
% */
%namespace RiverExplorer::Phoenix
%{
%extern bool Register_Cmd(Command_e Cmd, CommandCallback * Callback);
%}
#endif

#ifdef RPC_HDR
%/**
% * A command consists of:
% * - The enumerated command (Command_e),
% * - An XDR opaque object (length + data).
% * The XDR opaque data was prepared by the Cmd specific code
% * and is set into place for transport.
% */
#endif
struct  CmdPacket
{
        CommandSequence Sequence;
  CmdData Data;
};
```

E.10. RPCGEN - EMail

```
const FLAG_SEEN                         = 0x0001;
const FLAG_ANSWERED             = 0x0002;
const FLAG_FLAGGED              = 0x0004;
const FLAG_DELETED              = 0x0008;
const FLAG_DRAFT                        = 0x0010;
const FLAG_FORWARDED    = 0x0040;
const FLAG_MDNSENT              = 0x0080;
const FLAG_JUNK                         = 0x0100;
const FLAG_NOTJUNK              = 0x0200;
const FLAG_PHISHING             = 0x0400;

#ifdef RPC_HDR
%/**
% * @note
% * The "C" routines return a bool_t, the C++ API return a bool.
% */
%#ifdef BUILDING_LIBPHOENIX
%#include "Types.hpp"
%#include "MetaData.hpp"
%#include "Mime.hpp"
%#else
%#include <RiverExplorer/Phoenix/Types.hpp>
%#include <RiverExplorer/Phoenix/MetaData.hpp>
%#include <RiverExplorer/Phoenix/Mime.hpp>
```

```
%#endif
%#include <string>
%#include <vector>

#endif

#ifdef RPC_HDR
%/**
% * EMail headers are a vector of MetaData.
% *
% * Some examples:
% * @verbatim
% *
% * From: RiverExplorer.USexample.com
% * To: CEO@example.com
% * Subject: The holidays!
% *
% * @endverbatim
% *
% * @note
% * This does not define new or alter existing header types.
% * This is a container to transport them.
% */
#endif
typedef MetaData EMailHeader;
typedef EMailHeader EMailHeaders<>;

#ifdef RPC_HDR
%
%/**
% * An email is a vector of MimeBodyPart
% *
% * @note
% * This does not define new or alter existing mime or email headers.
% * This is a container to transport them.
% */
#endif
typedef MimeBodyPart EMailBodyParts<>;

#ifdef RPC_HDR
%
%/**
% * Check for the existence of a specific Header.
% *
% * @param Headers The Headers that is being processed.
% *
% * @param Key The header name being looked for.
% *
% * @return The number of matches.
% * Returns zero (0) when none are found.
% * Returns ((uint64_t)-1) when Obj or Key are NULL.
% */
%namespace RiverExplorer::Phoenix{
%extern uint64_t * EMail_HasHeader(EMailHeaders * Headers, const char * Key);
%}
#endif

#ifdef RPC_HDR
```

```
%
%/**
% * Get a specific Header.
% *
% * @param Headers The Headers that is being processed.
% *
% * @param Key The header name being looked for.
% *
% * @return A vector of the matches.
% * Will return zero (0) or more matches, in the original order.
% * Will return NULL of Obj or Key are NULL.
% * Will return NULL when Key is not found.
% */
%namespace RiverExplorer::Phoenix{
%extern EMailHeader  * EMail_GetHeader(EMailHeaders * Headers, const char *
Key);
%}
#endif

#ifdef RPC_HDR
%
%/**
% * Headers count.
% *
% * @param Headers The Headers that is being processed.
% *
% * @return The number of EMailHeader in Headers.
% * Returns ((uint64_t)-1) when Headers is NULL.
% */
%namespace RiverExplorer::Phoenix{
%extern uint64_t EMail_GetHeaderCount(EMailHeaders * Headers);
%}
#endif

#ifdef RPC_HDR
%
%/**
% * Headers iterator.
% *
% * @param Headers The Headers that is being processed.
% *
% * @param Which The header to get, the first is zero (0).
% *
% * @return A pointer to the EMailHeader.
% * Returns NULL when Headers or Key is NULL.
% * Returns NULL when Which is not a valid index.
% */
%namespace RiverExplorer::Phoenix{
%extern EMailHeader * EMail_GetHeaderByIndex(EMailHeaders * Headers, uint64_t
Which);
%}
#endif

#ifdef RPC_HDR
%
%/**
% * Common headers names.
% */
```

```
%namespace RiverExplorer::Phoenix{
%extern const char * Date_s;                    /** "Date" */
%extern const char * From_s;                    /** "From" */
%extern const char * Subject_s;         /** "Subject" */
%extern const char * To_s;                              /** "To" */
%}
#endif

#ifdef RPC_HDR
#ifdef __cplusplus
} // End extern "C"
%
#endif
%#ifdef __cplusplus
%namespace RiverExplorer::Phoenix::EMail {
%class Message
%{
% public:
%
%       /**
%        * Message - Default Destructor.
%        */
%       Message();
%
%       /**
%  * Message - Destructor.
%  */
%
%       /**
%  * Get the headers.
%        *
%        * @return All of the headers.
%  */
%       EMailHeaders * Headers() const;
%
% /**
%  * Add a header.
%  *
%  * @param NewHeader The new header to add.
%  */
%  void Add(EMailHeader & NewHeader);
%
% /**
%  * Add a header.
%  *
%  * @param Key The new header to add.
%  *
%  * @param Value The new header value to add.
%  */
%  void Add(std::string Key, std::string Value);
%
% /**
%  * Get the named header.
%  *
%  * @param Key The new header to add.
%  *
%        * @return A vector of all the matches. It will contain
%        * zero or more entries.
```

```
%  *
%  * @note
%  * You MUST delete result when finished or you will have
%        * a memory leak. You MUST NOT delete the
%        * entries in the vector, they are still in the email message.
%  */
%  std::vector<const EMailHeader*>      * Header(std::string Key);
%
% /**
%  * Get the number of body parts.
%  *
%  * @return The number of body parts.
%        */
% const uint64_t Count() const;
%
% /**
%  * Get the body parts.
%  *
%  * @return The body parts.
%  *
%  * @note
%  * Do not delete the results.
%        */
% const MimeBodyPart * Body() const;
%
% /**
%  * Get the nTh body part.
%  *
%  * @param nTh Which to get, first is zero (0).
%  *
%  * @return The body part.
%  * Returns nullptr when nTh does not exist.
%  *
%  * @note
%  * Do not delete the results.
%        */
% const MimeBodyPart * Body(uint64_t nTh) const;
%
% /**
%        * This ID is used as a transport ID between
%        * endpoints to uniquely identify this message for this
%        * account on this server.
%        *
%        * @return The message ID For this message.
%        * A return value of zero (0) indicates that this message
%  * does not have an ID.
%        *
%        * @note
%        * This is NOT the 'Message-ID' in email headers.
%        * This is the ID that uniquely identifies this message to endpoints.
%        *
%        * @note
%        * This ID is unique to the server or message provider and might
%        * not be unique on the client side.
%        * Implementations may wish to provide their own local ID
%        * to uniquely identify this message in their system that is
%        * separate from this ID.
%        */
```

```
% uint64_t ID() const;
%
% /**
%  * Messages in a message store have an ID.
%  * This sets the message ID for this message.
%        *
%        * @param TransportID The transport ID to associate with this
message.
%        * A value of zero (0) indicates that this message
%  * does not have an ID.
%        *
%        * @note
%        * This is NOT the 'Message-ID' in email headers.
%        * This is the ID that uniquely identifies this message to endpoints.
%        *
%        * @note
%        * This ID is unique to the server or message provider and might
%        * not be unique on the client side.
%        * Implementations may wish to provide their own local ID
%        * to uniquely identify this message in their system that is
%        * separate from this ID.
%        */
% void ID(uint64_t StoreID) const;
%};
%} // End namespace EMail
%#endif // class
#endif // RPC_HDR
```

E.11. RPCGEN - MIME

```
#ifdef RPC_HDR
%/**
% * @note
% * The "C" routines return a bool_t, the C++ API return a bool.
% */
%#ifdef BUILDING_LIBPHOENIX
%#include "MetaData.hpp"
%#else
%#include <RiverExplorer/Phoenix/MetaData.hpp>
%#endif
%
%/**
% * A MediaType is a string pair as defined
% * at https://www.iana.org/assignments/media-types/media-types.xhtml
% *
% * Some examples:
% * @verbatim
% *
% * text/html
% * application/pdf
% * audio/ogg
% * image/png
% * multipart/mixed
% *
% * @endverbatim
% *
```

```
% * Would have a Key of 'From' and a value of 'RiverExplorer.US@gmail.com'.
% *
% * @note
% * This does not define new or alter existing IANA media types.
% * This is a containter to transport them.
% */
#endif
typedef MetaData MediaType;

#ifdef RPC_HDR
%/**
% * A MIME header is a key/string value.
% */
#endif
typedef MetaData MimeHeader;

#ifdef RPC_HDR
%/**
% * Headers is an array of MimeHeader.
% *
% * Example:
% * @verbatim
% *
% * From: RiverExplorer.US@example.com
% * To: CEO@example.com
% *
% * @endverbatim
% *
% * @note
% * This does not define new or alter existing mime or email headers.
% * This is a containter to transport them.
% */
#endif
typedef MimeHeader MimeHeaders<>;

#ifdef RPC_HDR
%
%/**
% * A MIME object. Has a MediaType, MimeHeaders and data.
% *
% * To use:
% *
% * @code
% *
% * MimeBodyPart        * TheMimeBodyPart;
% *
% * // ...however you fill in or get the MimeBodyPart object data ...
% * //
% * TheMimeBodyPart = GetTheData();
% *
% * uint64_t            Length;
% * const char* TheMediaType = MimeBodyPart_GetMediaType(TheMimeBodyPart);
% * uint8_t             * Data = MimeBodyPart_GetData(TheMimeBodyPart,
&Length);
% * ...
% *
% * // At this point, you have the media-type, Data, and length
% * // of the data.
```

```
% *
% * @endcode
% */
#endif

#ifdef RPC_HDR
%/**
%       * - Type: The media-type of the object.
% * @note
% * Media-type is not duplicated in Headers.
% *
%       * - Headers: The MIME headers.
% *
% * - Data: The data itself.
% * The data is a binary blob without any encoding.
% */
#endif
struct MimeBodyPart
{
        MediaType               Type;
        MimeHeaders Headers;
        IoVec                           Data;
};
```

E.12. RPCGEN - Phoenix

```
/**
 * These are just used below to make the 'program' values
 * more readable.
 */
#define PhoenixProgramNumber 1
#define PhoenixProgramVersion 1
#define PhoenixSendPacket 1
#define PhoenixNotifyPacket 2
#define PhoenixBroadcastPacket 3

program PhoenixProgram
{
        version PhoenixVersion
        {
                CmdPacket Send(CmdPacket) = PhoenixSendPacket;
                void Notifiy(CmdPacket) = PhoenixNotifyPacket;
                void Broadcast(CmdPacket) = PhoenixBoradcastPacket;

        } = PhoenixProgramVersion;
} = PhoenixProgramNumber;
```

E.13. RPCGEN - Types

```
#ifdef RPC_HDR
/**
 * The orignal RPCGEN was "C" only, RPCGEN++ is "C++".
 * C useed bool_t, and C++ uses bool.
 * So this is a wrapper.
```

```
 *
 * @param xdrs An initialized XDR object.
 *
 * @param BValue The address of the bool_t object.
 *
 * @return false if failed.
 */
%namespace RiverExplorer::Phoenix
%{
%extern bool xdr_bool_t(XDR * xdrs, bool_t * BValue);
%}
#endif

#ifdef RPC_HDR
%/**
% * Each command sent, has a command identifier, and a sequence.
% * Each reply to a command has the same CommandID and sequence.
% */
#endif
typedef uint64_t CommandSequence;

#ifdef RPC_HDR
%/**
% * An array of strings.
% */
#endif
typedef string StringType<>;

#ifdef RPC_HDR
%/**
% * An array of strings.
% */
#endif
typedef StringType ArrayOfStrings<>;


#ifdef RPC_HDR
%/**
% * An object to data objects, some of which might
% * be memory mapped.
% *
% * - IsMMapped: When true, Data was memory mapped and not allocated.
% * When false, Data was allocated.
% *
% * - Len The number of octets in Data.
% *
% * - Data A pointer to the data.
% */
#endif
class IovVec
{
        bool_t          IsMMapped;
        uint64_t        Len;
        uint8_t * Data;
};
```

Acknowledgments

Contributors

Thanks to all of the contributors. [REPLACE]

Author's Address

Doug Royer (EDITOR)
RiverExplorer Games LLC
848 N. Rainbow Blvd #1120
Las Vegas, Nevada 89107
United States of America
Phone: 1+714-989-6135
Email: DouglasRoyer@gmail.com
URI: https://RiverExplorer.games