IGS

SESSION 3:
REAL-TIME DATA/
PRODUCT EXCHANGE

Position Paper for the Session Real-time Data/Products Exchange

Mark Caissy, NRCan, and Ron Muellerschoen, JPL

INTRODUCTION:

The Ottawa workshop will provide an opportunity for us to share our knowledge and experiences in real-time data and product generation. The objective of this session is to lay down the foundation needed to facilitate a free flowing exchange of real-time data and products among IGS members. We will begin this process by developing recommendations for the design of a data and products exchange prototype and set a course for its implementation. The goal is to have in place a reliable, robust and manageable system of data and products exchange coming from a global network of multidisciplinary real-time tracking stations.

This document addresses the requirements for the design of a system that will allow the real-time exchange of GPS data and products within the IGS community, using the open Internet as a transport medium. The paper will focus on the main objectives in phase one of the IGS RTWG's Charter, namely the implementation of a prototype real-time data distribution system and the adoption of a real-time exchange format for GPS data on the open internet.

DISCUSSION

We have been asked to design and implement a data and products exchange prototype that will meet our above-stated goals. We must therefore attempt to see where we want to be several years from now and make every effort to ensure that our prototype design will fit into our vision for the future. We must also be inclusive, that is we must involve as many members of the IGS as possible through the sharing of real-time enabling technologies. By doing so, we will involve all interested members of the IGS community in real-time activities.

The remainder of this section will be for the discussion of the requirements considered necessary for the implementation of a data and products exchange prototype.

Requirements of a Data and Products Exchange Prototype

Routing

See note #1 at the end of the paper

Routing is the managed process of directing data packets from one node to another on a path to their final destination. At the lowest layer, dedicated hardware routers manage the routing of packets for all traffic on the Internet. It is recommended that at the

application layer, the highest layer, special purpose applications be used to allow data to be forwarded from a data center to others via a connectionless UDP unicast. It will be the responsibility of these applications to respond to data requests from external users of the data. Initially, all requests for data will be serviced. Should this service prove to be over subscribed, so that the data centers cannot respond to all requests, or the centers bandwidth is being consumed due to excessive traffic, access control shall be implemented as described below.

See notes #2 & #3 at the end of the paper

Access Control, Confidentiality, and Data Integrity:

Due to the openness of the Internet, it is prudent to assess the prototype security requirements. Access control is considered important and it is recommended that access control be implemented as necessary accordingly to each facilities capabilities and concerns. Access control may be handled at the hardware level with dedicated firewalls, at the OS level using methods such as IP-chains, or higher up in the application layer.

Data confidentiality may be addressed through the use of encryption technology. However, we do not recommend encrypting the data at this time. The prototype is considered to be an open system and hence accessible to all. Encrypting the data creates an exclusive environment and is therefore not conducive to an open system.

Data integrity is considered a compulsory matter to address. Data integrity or authenticity can be provided through the use of a message authentication code (MAC) sometimes referred to as a cryptographic checksum. A MAC insures that data has not been altered along its transmission path, but moreover a MAC also enables one to verify that data came from the intended source. The MAC, represented as a bit-string, is a function of the data, and a secret key shared by the sender and the receiver. A MAC is typically attached to the end of a packet. MACs can vary in bit length depending on the required level of authentication assurance. A 16 byte MAC provides strong authentication of a received message and is recommended for the prototype.

Functionality / Logical Design

The data is to be distributed within a robust and reliable environment capable of real-time distribution of data and products on the Open Internet. The data from the real-time tracking stations will flow into the data centers. A mechanism shall be in place to inject the data being shared by the data center into the routing application. The routing application is required to listen for requests from users and based on the request take the required action. These actions will in the beginning be restricted to sending data or continuing to send data. Later actions may be required in dealing with a request to retransmit missed packets.

Since the recommended protocol (UDP unicast) is connectionless, the sender (server) will not know when the receiver (client) has shut down. The server shall stop sending data to the client after a reasonable timeout period (on the order of several minutes). In order to continue receiving data, the client must periodically make requests of the server. These requests shall also be unicast UDP packets.

Since there may be different data types (ie: GPS, meteorological, seismic etc) originating from a station, data requests may be required to be data type specific. Users should only receive data of the type they have requested from a centers accumulator (server). It may prove easier for data centers to distribute different data types on different ports, that is, set up parallel servers on separate channels for the different data types. This is the approach taken by JPL to distribute gps data, broadcast ephemeris, almanac information, ionosphere/timing information, and global differential corrections. It is recommended that different data types be made available on different port numbers.

Physical Network Topology

As a starting point for the prototype network, the raw data may be requested from the agency controlling the stations from which the data accumulates. This provides a very direct path for the data from the source to the end user. The data centers should strive to have redundant Internet services and servers providing access to identical data flows, (Figure 1 in prep). In this way all data accumulators/distributors can be viewed as being at the same level.

As the physical network grows in stations and users, distributed servers may be required to limit the demands placed on data centers supplying the real-time data. One possible scenario is the incorporation of global data centers in the role of global real-time data distribution centers (Figure 2 in prep). These distribution centers would be chosen because of their reliability/redundancy and Internet bandwidth. Careful consideration must be given to the design of such a hierarchical system, as there are drawbacks to this approach including single points of failure at any of the nodes of the hierarchy. Should one node fail, the higher nodes will not have access to the data being processed by the lower nodes. Another drawback is the management of this type of system. Should nodes accidentally feed back to lower nodes, packets will endlessly be circulated in a loop. It is not recommend that distributed servers be implemented at this time.

Performance and Scalability

It is envisioned that the network will begin small and grow to the required numbers over time. It is therefore important to not limit the prototype's potential performance or scalability. Bandwidth restrictions and Internet performance will play a factor here.

Reliability Requirements

The system must be designed carefully for reliability and high availability. The network software and hardware infrastructure should have the necessary redundancy to prevent disruption of the network because of failure of network or server components. Tracking station outages will make their data unavailable and makes geographical redundancy necessary. Data center outages will make all data routed through them unavailable. The concept of primary and secondary data centers will be important for the future growth of the system.

Network Management Monitoring and Maintenance

A critical requirement of the solution is to minimize the level of effort required to manage and troubleshoot the prototype and the future fully functional distribution system.

Data distribution centers are responsible for the maintenance and monitoring of connections with the outside world, as well as administering tracking stations or sub-networks under their umbrella.

It is recommended that a RT-network-coordinator monitor and report back to the data centers on: accessibility (is the data there), reliability (how often is the data not there), and integrity (is the data usable). The integrity of the data may be implemented by sampling the data at a configurable frequency and post-processing the results.

Formats

Due to the phased approached of constructing the prototype network, different data formats shall be accommodated. This is considered the quickest way in which to proceed to a prototype where real data is flowing. The format of the data will be known by information contained in a message wrapper. See "Design Requirements for Data Wrappers". Format translation functions will be required at the user end.

In later revisions, it may be possible to limit the data formats to a handful, if not down to one. Recommended format(s) shall be designed to minimize bandwidth consumption without compromising the resolution of the data to a point where products become negatively impacted. In the case of GPS data, dynamic range compression techniques may be employed for bandwidth minimization. For example, JPL's soc format makes certain assumptions of the data characteristics, such as reasonable magnitudes of multipath and exploits the ionospheric phase and group delay differences among the data types. See for example: http://gipsy.jpl.nasa.gov/igdg/papers/. Other examples of GPS data compression will be investigated.

Sharing of Expertise

It is recommended that centers with expertise in accessing data directly from receivers to putting the data on-line share their experiences and practices with others. It should be realized that some centers are restricted from open-sourcing code and from providing executable code. Additionally, it must be understood that centers have limited resources in providing expertise.

Design Requirements for Data Wrappers

We introduce the concept of a "data wrapper". The "data wrapper" shall consist of minimally a header, and a MAC trailer.

See note #4 at the end of the paper

We highlight as an example, NRCan's message header

```
typedef struct _udpRelayMsgHdr_t {
   unsigned char          sync1;       /*  1 byte  */
   unsigned char          sync2;       /*  1 byte  */  Serial or Wireless requirement
   unsigned short         msgType;     /*  2 bytes */  Message Type
   unsigned short         cntrl;       /*  2 bytes */  Control Bits (Special Purpose)
   unsigned short         stationID;   /*  2 bytes */
   struct timeval         timestamp;   /*  8 bytes */ Network performance
   unsigned short         msgSeq;      /*  2 bytes */  Sequence Number
   unsigned short         msgSize;     /*  2 bytes */  Message Size including MAC
   unsigned short         dataSize;    /*  2 bytes */  DataSize
   unsigned short         reserved;    /*  2 bytes */
} udpRelayMsgHdr_t;                    /*----------*/
                                       /* 24 bytes */
```

The header information is followed by the data and the MAC is then appended.

The msgTypes include control packets and data packets and each data packet has an associated data format. Initially control packets shall be request packets to start or continue data service.

The stationID will indicate which station the request packet is requesting. A default stationID is recommended to indicate that all station data from the data center is being requested. These control packets shall originate from the clients requesting data. The station ID is unique to the controlling agency that is accumulating the data.

The msgSeq number is an incremental number attached to each data packet on a per station ID basis. Its period must be defined.

The "msgSize" indicates the total number of bytes in the message including the data and MAC, while the "dataSize" variable indicates how many bytes are in the data block.

The MAC is generated based on publicly available functions shared at both the send and receive ends. Generating and verifying a MAC has in NRCan's experience required very low (negligible) overhead.

Other control packets can be later defined to be requests for retransmission of missed packets. For these types of requests, the stationID and msgSeq number are meaningful.

The msgType for data packets shall contain information relating to the format of the data block. Data packets shall either be labeled original packets (default) or retransmitted data packets resulting from retransmission requests. This again is for later development.

In addition to this, in order to respond to station changes on the fly it may be necessary to transmit a station reference number. Should the station configuration change (like antenna heights or clock steering), the user needs to know this on the fly, and take the appropriate actions.

RECOMMENDATIONS

It is recommended that the IGS community and the RTWG in particular move forward on two fronts with the goal of completing phase 1 of the RTWG's charter as quickly as possible.

1) Involve the broadest membership as possible from within the IGS community.

   In order to achieve this we should: (beginning at the workshop)
   a. Identify interested agencies.
   b. Identify enabling technologies within the broad membership that can be shared.

2) Move forward on the development of the prototype.
   - By giving consideration to:

     i. The use of UDP unicast at the application level for directing data packets between data centers and users.

     ii. To the use of a MAC to ensure data integrity.

     iii. The use of different port numbers for different data types available at a data center.

iv. The adoption of a wrapper for the data formats including a structure for request packets.

v. Use the simplest physical network structure starting with data being available only from controlling data centers.

- Incorporating additional requirements identified during the workshop and deemed necessary for the prototype development.

Proposed Next Steps

In a short period of time, the RTWG shall:

i. Recommend a wrapper for the data formats, including a structure for request packets.
ii. Recommend port numbers in the range of the IANA Registered Ports (1024 to 49151) that have not already been registered by IANA (Internet Assigned Numbers Authority). See for example: http://www.iana.org/assignments/port-numbers

The RTWG shall make a request to IANA to register these port numbers. This step is generally done when trying to establish a new standard. It ensures that other legitimate Internet users will not ship packets on the same port number to your computer.

Centers will be asked to make a subset of their real-time data stream available with the interface defined by our initial prototype requirements. It is recommended that this data shall be made available within 3 months after the wrapper, request packets, and port numbers have been defined.

NOTES:

Note 1: As described we do not consider this to be an authoritative description of TCP/IP. It is limited to the authors' current knowledge and experiences. Please bring to the attention of the authors any errors in our understanding that you may encounter, both for our own edification and to incorporate into future revisions of this paper.

Note 2: TCP and UDP are the two predominant transport layer protocols. Both use IP as their network layer. TCP provides a reliable transport layer, whereas UDP sends and receives datagrams (hence its name User Datagram Protocol) on a best effort basis. UDP does not guarantee that the datagram ever gets to its final destination. UDP is considered connectionless, and is a many-to-one and one-to-many protocol. The many-to-one aspect can be used to easily build data accumulators. Multiple applications, lets call them clients, can send UDP packets to a central receiver, typically known as a server. Servers do not need to know of the existence of their clients a priori, but clients must know what servers exist on the network. On the outgoing side, the one-to-many aspect can be used

to build data distributors. Here the data accumulator can respond to data requests, and forward copies of its data packets to multiple IP destinations. TCP on the other hand establishes a reliable connection between two IP addresses. It is a one-to-one protocol. It is possible but more difficult to build a many-to-one and one-to-many architecture using TCP. This generally requires either multiple socket instantiations, or forking dedicated processes for each connection. JPL's original data accumulators and data distributors were TCP based. These were abandoned in favor of UDP due to the high overhead required of TCP. TCP proved not to be an effective transport layer to many parts of the world where link layers were not well established.

Note 3: An alternative to UDP unicast is UDP multicast. NRCan's internal data distribution is based on UDP multicast. Although UDP multicast is ideally suited for our purposes, the Internet as a whole, specifially IPv4, does not currently support IP multicast across subnets. Version 6 of IP will fully support UDP multicast routing, but it is not known by the authors how and when the world's link layers will permit IPv6 packet routing If we could use multicast technology, all the operating real-time stations would send their data to a global multicast group, which is in essence a virtual IP address. A multicast client could subscribe to this multicast group and would automatically be forwarded the data. Internet routers using IGMP (Internet Group Management Protocol) would determine optimally how to route the data. In the case of multiple requests coming from almost similar clients, routes are constructed so that only one packet transverses a majority of the distance. At the last possible router, the packets are duplicated and sent off to separate destinations. It can be thought of as a branching architecture where branches grow out of other branches due to clients joining the multicast group. The drawback to this is an all-or-nothing data feed, in which case the "all" may overwhelm the client's bandwidth. The client is at the mercy of whatever has been placed in the multicast group and has no say as to what packets it would like to receive.

Note 4: The words "header", "wrapper", "upper-data layer" shall refer to some higher layer of the underlying data format.

NRCan's Internet Global Positioning System Data Relay (iGPSDR)

K. Macleod and M. Caissy - Geodetic Survey Division, natural Resources Canada
R. Fong - TesserNet Inc.
V. Forgues and T. Erskine - SourceWorks Consulting Inc.

Natural Resources Canada (NRCan), Geodetic Survey Division (GSD) has been operating the Canadian Real-Time Active Control System (CRTACS) since 1996. The CRTCACS comprises a Real-Time Master Active Control Station (RTMACS) and a network of continuously operating GPS data acquisition stations, called Real-Time Active Control Points (RTACPs).

The RTMACS receivers RTACP observation data every second and ephemeris data upon update. At designated intervals (every 2 seconds) the RTMACS computes wide area GPS corrections. The GPS correction product derived by the RTMACS is known as the Canadian GPS□C service.

The CRTACS is enabled by a managed frame relay wide are network (WAN). The managed frame relay network is very reliable and unfortunately the cost associated with the frame relay network is also very high. With a core network of frame relay stations NRCan decided to develop a less expensive data collection application to densify and extend the network. The WAN networking technology option that was chosen was the Internet.

The Internet provides economical real-time (less than 1.5 seconds) data collection capability. However, data transmitted over the open Internet is not secure and the quality of service is not predictable. To ensure that the data sent over the open Internet is secure a message authentication code (MAC) is used. The MAC insures that the messages are not altered in transit. To enhance security the data can also be encrypted so that unauthorized users cannot read the message content. The reliability and bandwidth of the Internet has improved significantly since its inception. In North America the backbone of the Internet is very reliable and has excess capacity. Until recently, connecting to the Internet has been problematic. However, with the availability of high speed Digital Subscriber Lines (DSL) Internet access is no longer as significant an issue. NRCan has a managed Asymmetric Digital Subscriber Line (ADSL) dedicated to real-time GPS data and correction collection and distribution. The dedicated ADSL will contribute to the overall quality of the Internet real-time data collection project.

NRCan built an Internet Global Positioning System Data Relay (iGPSDR) application to facilitate the routing of GPS data and corrections over the open Internet to a large number of National and International users. The iGPSDR securely routes data from source to relay, relay to relay, and relay to destination. Redundancy and quality of service features have been built into the iGPSDR. Since networks and data formats can change over time, the iGPSDR can be configured at run time thereby enabling uninterrupted service. If a network of iGPSDRs is built the bandwidth required to move data can be minimized and the reliability maximized.