Internet Engineering Task Force
Internet Draft
draft-ietf-iptel-glp-00.txt
February 16, 1999
Expires: August 1999

IPTEL WG
Matt Squire
Nortel Networks

A Gateway Location Protocol

STATUS OF THIS MEMO

1 Abstract

Given a gateway and a (possibly empty) list of gateway attributes, the "gateway location problem" is to find a gateway serving the given phone number that satisfies the attribute set. This problem has also been referred to as the "call routing problem" as the answer returned may not be an IP-PSTN gateway but an intermediate signaling server.

Part of the solution to this problem is the maintenance and distribution of the call routing tables. This document describes a protocol for maintaining a distributed call routing database across multiple administrative domains. The protocol uses the Server Cache Synchronization Protocol (SCSP) to maintain the distributed database. This document describes the problem of gateway location and a potential solution that uses SCSP as the foundation for distributing the call routing tables.

2 Overview of the Gateway Location Problem

A gateway is a device providing connectivity between the PSTN and an IP network. A telephone call that originates from an IP device, or that passes through an IP network, and that terminates on the PSTN, must traverse a gateway. There may be multiple gateways in the network through which a particular call could egress the network. An important step in the evolution of IP telephony is automating the choice of an egress gateway for a particular call.

The general gateway location problem is described in the Gateway Location Framework [GLP-FR], and the position of the Gateway Location Protocol (GLP) relative to other IP telephony protocols and entities is defined. This framework is summarized here, but the reader is referred to [GLP-FR] for a fuller description.

In the framework, End Users (EUs) are entities with IP connectivity and with the ability to place phone calls to users on the PSTN. EUs may be users with IP telephony equipment or may be gateways from the PSTN to an IP network. Gateways are the devices that translate between an IP network and the PSTN. Location Servers (LSs) are the logical entities that maintain knowledge of the gateways, and Signaling Servers (SSs) are the entities which forward and process signaling messages. Common signaling protocols are SIP [SIP] and H.323 [H323]. Signaling servers forward (route) signaling messages while location servers maintain the information on which these forwarding decisions are made.

GLP is defined as an inter-domain protocol, where an IP Telephony Administrative Domain (ITAD) is a collection of IP telephony resources under the control of a single administrative authority. LSs participate in the GLP to maintain this database of gateways across multiple ITADs. Another protocol, the intra-domain protocol, may be used by LSs within a domain to further distribute this information. The use of possibly different inter-domain and an intra-domain protocols is analogous to the use of the Border Gateway Protocol (BGP) [BGP] and the Open Shortest Path First (OSPF) [OSPF] protocol to maintain routing tables between and within autonomous systems (IP routing domains). Note that just as BGP can be used within an autonomous system, GLP can be use within an ITAD. Using GLP within an ITAD provides reliability and scaleability for inter-domain communications by permitting multiple border routers.

LSs learn about the gateways within their domain through an out-of-band mechanism. Another protocol, the front-end protocol, is used by EUs to access the LS database in order to route a call toward the PSTN. The GLP places no restrictions on the front-end or intra-domain protocols.

3 Comparison of Call Routing and IP Routing

To better understand the problem of call routing, we first compare it with the well-understood problem of IP routing.

IP routing tables are made up of a collection of routing table entries. For basic IP routing, each entry consists of a destination address, an address mask, a next-hop router, and a path-length. All packets targeted to a destination covered by the combination of the destination address and address mask are forwarded to the next-hop router. The cost to reach the destination is given by path-length.

Whenever there are multiple entries that cover a single destination, the more specific entry (with the longer address mask) is used to route the packet. There are mechanisms defined for aggregating and forwarding routing information. For example, when advertising a route entry received from one neighbor to another neighbor, the router may increment the path-length before transmitting the advertisement. Also, when a router receives multiple routes to a particular destination, it may discard entries with a longer path-length as these represent non-optimal routes.

Call routing is similar but has several important distinctions. The call routing infrastructure is overlayed on the IP infrastructure, but the two routing realms are independent. Location Servers, which maintain the call routing tables, and Signaling Servers, which forward the signaling messages, are distinct logical entities (however, a single device may perform both functions). The IP telephony data (the packetized voice) is not routed using the LS/SS combination. It is forwarded as normal IP packets and need not be routed through any signaling server. Peer LSs need not be physically adjacent.

Call routing tables are made up of a collection of call routing objects. A call routing object is a more complex version of an IP routing table entry. Like an IP routing table entry, a call routing object includes a set of destination addresses and a next hop. In this case, the set of destination addresses is given by upper and lower bound telephone numbers, and the next-hop is the next-hop signaling server (which may in fact be a gateway). In IP routing, the cost represents a path cost (ie a relative measurement of the distance/delay between two points). In call routing, the cost of a route is an optional attribute of a call routing object, and the cost of a route is dependent on may variables other than the path (the cost charged by a gateway to service a call, the quality of the service given by the network and gateway, etc).

A call routing object may also include any number of additional

attributes. These might include the signaling protocols supported by the next-hop SS for this destination, the telephony features provided for this destination, the speech codecs understood for this destination, the encryption algorithms supported for this destination, etc. The set of attributes is open-ended and destination specific. As such, defining a standard set of rules for aggregating and forwarding call-routing objects is itself a difficult problem.

In IP routing, given any destination address, there is a simple rule for determining the routing table entry that should be applied. Namely, find the routing table entry with the longest matching prefix. Such a rule does not exist in the context of call routing. Prefix length is not the most significant variable in determining the best suited routing object. Call routing objects are multi-attributed, as such there can certainly be more than one entry that applies to a particular destination. For example, a particular phone number may be reachable via a SIP server at one destination or via a H.323 server at another destination. Multiple matching entries could be used by a server to load-balance between several possible destinations.

One can also examine the scaleability of call routing versus IP routing. For the Internet, all routers must be interconnected. Each routing table must contain an applicable entry for every Internet address. The collection of SSs on the Internet need not be (and most likely will never be) connected. A likely scenario is that a set of IP telephony providers will combine resources to form a confederation whose signaling servers and location servers communicate. Different confederations will most likely not share call routing data, implying a collection of independent call routing confederations. So although a call routing table may contain an entry covering every phone number on the PSTN, any particular LS/SS only propagates information about/to gateways within its confederation.

4 GLP Model

GLP is analogous to BGP in that it is used to distribute (call) routing information between domains. As such, BGP is used as the model for GLP.

At its core, BGP is a combination of link-state and distance-vector routing protocols whose aggregation and filtering rules are partially specified by the protocol itself and partially specified by a set of local policies for that BGP speaker. BGP speakers may have internal and external links to BGP speakers in its or other domains. A BGP

link is a communication between two peer BGP speakers. Behavior over internal and external links is slightly different. Within a domain, all BGP speakers use a combination of a mesh or route reflectors to achieve complete connectivity. BGP speakers maintain an inbound and outbound routing table for each link, as well as a local routing table used in their own routing decisions. When a link is first established, BGP synchronizes each speaker's outbound routing table with its peer's inbound routing table. After this synchronization, only updates traverse across the link.

The Server Cache Synchronization Protocol (SCSP), on the other hand, is a generalization of OSPF in that it accomplishes database synchronization on multiple servers by flooding information received from one neighbor to all other neighbors. However, if an SCSP flooding domain is restricted to a pair of neighbors, then SCSP behaves much like BGP. Both protocols exchange hello messages between peers, perform an entire transfer of the database upon detecting a new peer, and only exchange incremental updates after the initial synchronization. GLP applies SCSP to the inter-domain problem of gateway location by limiting the inter-domain flooding group to a pair of peer speakers from adjacent ITADs. In other words, the flooding aspects of SCSP are not used on inter-ITAD links.

To this end, a Location Server belongs to a number of Server Groups (SGs). Each SG corresponds to a collection of servers whose databases are to be synchronized. When a SG spans domains, it likely consists of only two LSs and provides bidirectional connectivity between the LSs. This is analogous to two peer BGP speakers over an external BGP link. For internal links, however, the possibilities are more flexible. Within a domain, a Server Group may consist of multiple LSs interconnected with an arbitrary topology. This provides a much more flexible and robust intra-domain connectivity than BGP meshes and route reflectors.

The set of SGs to which a particular LS belongs, the set of servers forming a Server Group, and the topology of interconnection within a SG are all determined administratively. Since GLP is defined as an inter-domain protocol, no neighbor discovery is provided.

SCSP is used to maintain a distributed and synchronized database over all servers in a Server Group. This database consists of the information required to route calls across the network. As in BGP, the database can be logically partitioned into inbound and outbound databases. The LS has an internal Policy Information Base (LS-PIB) that defines how to compute the outbound databases given the set of inbound databases. The LS also has a local database that it uses to make call forwarding decisions. The contents of the local database is also determined by applying the LS-PIB policy to the inbound

databases.

The GLP model is depicted in Figure 1, where LSs LS-A1 through LS-A3 are in one administrative domain, and LSs LS-B1 through LS-B2 are in another ITAD. In this example, the SGs are {LS-A1, LS-A2, LS-A3}, {LS-A3, LS-B1}, and {LS-B1, LS-B2}. Note that the topology in administrative domain A is not complete. SCSP provides synchronization across arbitrary connected topologies.

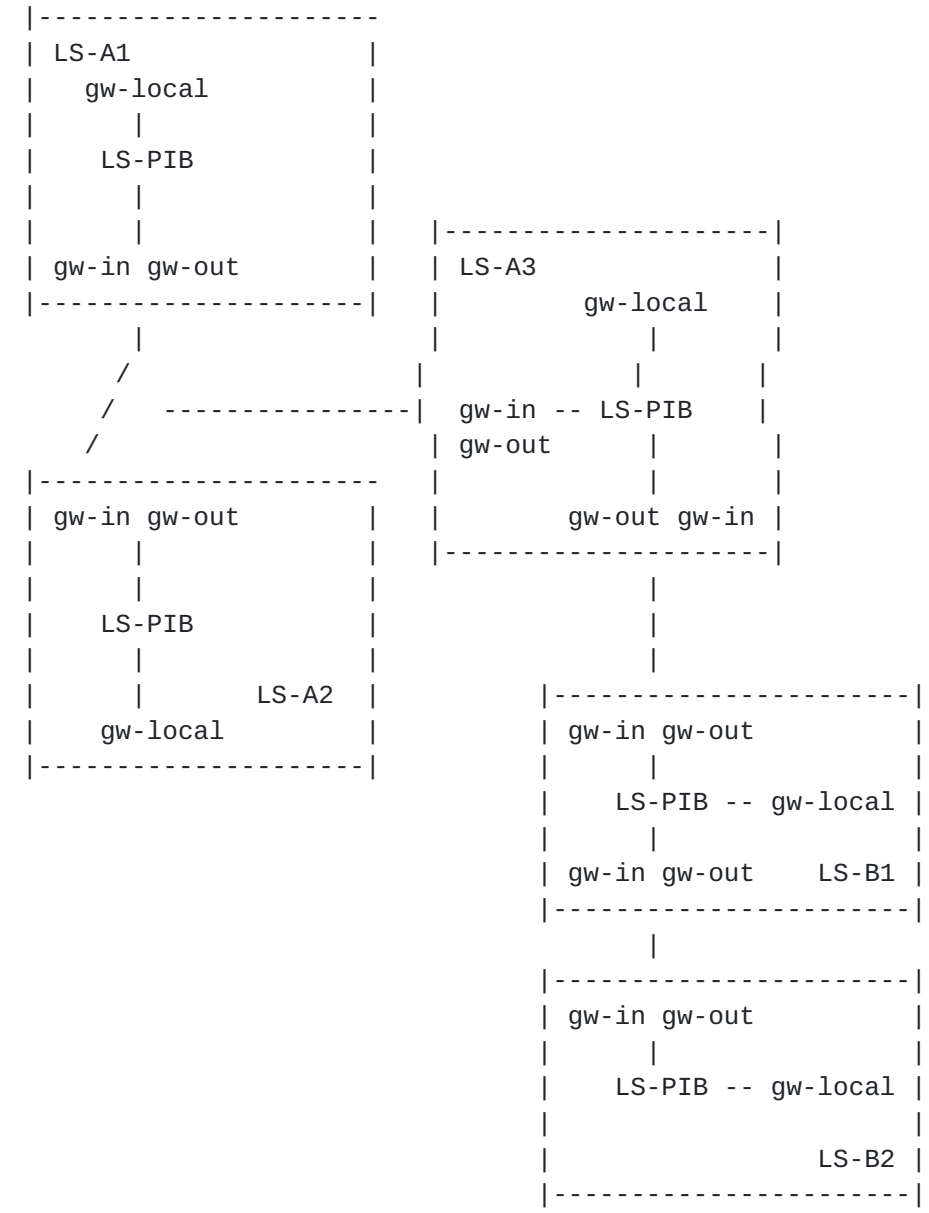


Figure 1 GLP Model

The form and function of the LS policies is not defined in this document. We believe that the most appropriate policies will be developed over time and through implementation innovation and experience. The multi-attributed nature of a gateway makes it difficult to define a satisfactory set of policies for aggregating and filtering the collection of gateways forwarded to each neighbor.

5 SCSP

The Server Cache Synchronization Protocol (SCSP) [SCSP] solves the general problem of server synchronization and cache replication. SCSP synchronizes the caches of a set of servers of a particular protocol bound to a particular server group. In the case of GLP, SCSP is used to synchronize the call routing database of all servers within a SG. The SG may consist of two servers (for example, an inter-ITAD SG may consist of one LS from each of two domains) or may be more general (for example, when used between the border LSs within a particular ITAD).

SCSP uses the combination of a Protocol ID (PID) and a Server Group ID (SGID) to identify both the protocol for which the servers are being synchronized as well as the instance of that protocol. In our case, the PID identifies the protocol as GLP.

Editor's Note. We need to get an SCSP PID for GLP.

SCSP assumes a the underlying network is a Non-Broadcast Multiple Access (NBMA) network. For GLP, the NMBA network is any IP network providing TCP connectivity. GLP could also operate directly over other NBMA networks (such as ATM AAL5, Frame Relay, etc), but the specifics of such behavior is not detailed here.

5.1 SCSP Operation

SCSP has three phases. The first phase serves to establish connectivity between directly connected neighbors. This phase is known as the Hello Phase. The second phase is the Cache Alignment phase, where directly connected servers quickly exchange the contents of their entire database. The third phase is the Cache State Update phase, where servers only transmit updates of their local database to their directly connected peers, and servers flood received database elements to other directly connected peers within the same SG. Note that this flooding operation permits a more general intra-domain topology than BGP which requires a combination of meshes and route reflectors.

5.1.2 Hello Phase

In the Hello Phase, directly connected LSs exchange hello messages in order to establish bidirectional connectivity between peers.

After connectivity is established, hello messages continue to be exchanged in order to indicate the status of the peer. Hello messages have two fields which control the frequency of the hello messages and the time before a neighbor is declared inoperable. Hello messages are sent every HelloInterval seconds. A peer is considered dead if no hello message has been received for HelloInterval*DeadFactor seconds. For GLP, hello messages must not be transmitted more than once per second. The suggested value for the HelloInterval is 30 seconds. The suggested value of DeadFactor is 3.

Editor's Note. One shortcoming of SCSP is that the Hello Protocol is not particularly extendible. There is nothing like version or feature negotiation during the Hello Phase. Is version/feature negotiation required for GLP?

5.1.2 Cache Alignment Phase

During the Cache Alignment phase, peer servers synchronize the contents of their entire database. During Cache Alignment, peer servers first exchange a summary of their database. After the summary exchange, a server requests data elements from their peers based on that summary information. Cache Alignment ends when peer servers have synchronized their databases for the first time.

After first aligning its GLP database with a peer, an LS shall execute its local policies to determine if any of its advertised databases, or its local database, have changed. Any resulting changes to an advertised route must be synchronized with the affected neighbor(s).

5.1.3 Cache State Update Phase

During the Cache Update phase, adjacent LSs exchange only changed or updated data elements. When something happens at an LS to change the set of advertised call routing elements to a peer, an LS must propagate this change to its neighbor. The neighbor acknowledges the newly received elements.

When an LS is informed of an updated or new call routing data

element, it must execute its local policies to determine if the set of local or advertised call routes has been changed. If so, then these changes must be propagated to the affected neighbor(s).

5.2 GLP Specific SCSP Fields

SCSP has generic and protocol specific aspects. This section details the GLP specific fields and formats for use within SCSP.

GLP runs over a NBMA network of TCP connections. During initialization, servers establish TCP connections to their configured set of peers. By default, SCSP over TCP uses TCP port XXXX. This port value should be configurable at an LS. It is a straightforward exercise to run GLP over other types of NBMA networks, or to extend SCSP/GLP over a network with multicast ability. However, due to the inter-domain aspects of GLP, multicast is not recommended.

Editor's Note. We need to get a SCSP TCP port assigned.

Editor's Note. It is not obvious that TCP is the only or the right choice for the transport layer. RUTS? An encrypted transport? Other possibilities?

The scope of a SCSP flooding domain is controlled by the combination of Server Group ID (SGID) and Protocol ID (PID). For GLP, the PID is XXXX. The assignment of the SGID for a specific set of servers is a local decision.

Editor's Note. We need to get a SCSP GLP PID assigned.

Servers within a SG of SCSP must have unique server identifiers. These identifiers are used to indicate the source and recipient of each SCSP message, as well as the originator of a data element within the distributed database. For GLP, this identifier is an IP address unique to the LS. The identifier is 4 octets in length.

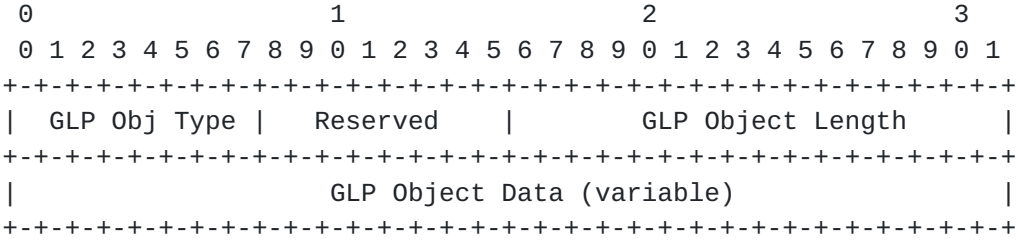
Each data element within a SCSP database can be identified by the combination of the Originator ID (the server which sourced the data element) and the Cache Key. The Cache Key is an identifier for the data element chosen such that the combination of Originator ID and Cache Key uniquely identifies this element. Servers use this identification method when determining if a received data element is a 'new' object or another version of an existing object. The Cache Key is variable length in SCSP. For GLP, the length of the Cache Key is 4. The Cache Key is a 4-octet field chosen by the originator of a data element such that the uniqueness condition is guaranteed.

SCSP also defines a 'newness' criteria for database elements. When a server receives a data element from a peer, and that new element matches an existing element in both the Originator ID and Cache Key, then the server examines the Sequence Number of the element to determine which version of the element is newer. Sequence Numbers can be used to refresh aging database elements.

The format of the data elements synchronized by SCSP for GLP is given in Section 5.2.1.

5.2.1 Generic GLP Data Object Format

SCSP synchronizes individual database elements to all servers within a Server Group. In SCSP, a database element is represented as a Cache State Advertisement (CSA). Each CSA contains a CSA header followed by a protocol specific part containing the actual data. The protocol specific part of a GLP CSA has the following generic format.



The fields are defined as follows.

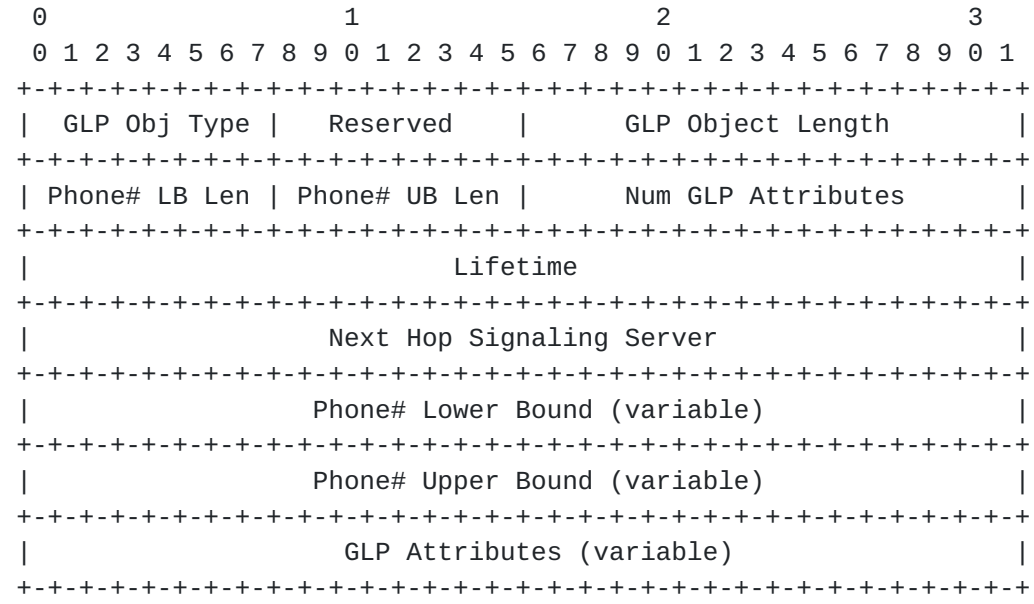
GLP Obj Type.
This field defines the type of GLP object. This specification defines the following GLP Object Types.
1 - GLPv1.0 Call Routing Object

GLP Object Length.
The Length of the GLP Object, from the start of the GLP Object Type field to the end of the CSA data. For alignment purposes, all GLP objects should be padded to have even length.

CSA Data.
The data specific to this instance of the object. The format of the data depends on the object type.

5.2.2 GLP Call Routing Object Format

The GLP Call Routing Object (CRO) forms the basis for internet call routing. The GLP CRO associates a range of telephone numbers with an IP address. A CRO can be used to route signaling messages to phone numbers that lie within the range specified by the lower and upper bound telephone numbers. When forwarding a signaling message for a phone number in the specified range, a signaling server or user agent may forward the signaling message to the Next Hop Signaling Server specified in the CRO. The Next Hop Signaling Server may represent an actual gateway or a transit signaling server. Whether the CRO represents an actual gateway or a transit SS cannot be determined from the CRO.



GLP Object Type.
Equals 1.

GLP Object Length.
A CRO object has variable length but the length must be even.

Phone Number Lower Bound Length.
The length of the Lower Bound Phone Number field.

Phone Number Upper Bound Length.
The length of the Upper Bound Phone Number field.

Number of GLP Attributes.
The number of GLP attributes in this CRO.

Lifetime.
The number of seconds that this call-routing object is valid. CROs

must be aged in the database and removed when their lifetime expires. Similarly, an originator must refresh CROs before they expire in a peer. A CRO can be refreshed by incrementing the Sequence Number of a CRO and synchronizing the updated CRO CSA with the peer.

Next Hop Signaling Server.
The IP address of the next hop signaling server that is associated with this call routing object. When using this call routing object to route a call, signaling messages are sent to this address.

Editor's Note. Should probably have a more general concept of a protocol address (ie have a protocol type and a protocol address). This would permit the same protocol to be used for routing calls over other networks (IPv6).

Phone Number Lower Bound.
The lower bound of the telephone number range defined by this CRO. The sytax of this field is:

phone-number-bound = +1*phone-digit phone-digit = DIGIT

This format is similar to the format for a global telephone number as defined in SIP [4] without visual separators. This format facilitates efficient comparison with the internationalized format of a phone number.

Editor's Note. This representation does not permot 'local' phone number formats. Local formats seem dangerous when one the concept of local can be different for the client and server.

Phone Number Upper Bound.
The upper bound of the telephone number range defined by this CRO. The lower and upper bounds may refer to phone numbers in different country codes and have different lengths. A phone number is covered by a particular CRO if

lb <= p <= ub

where p is the international version of the phone number and the comparison is performed using a string comparison function. For example,

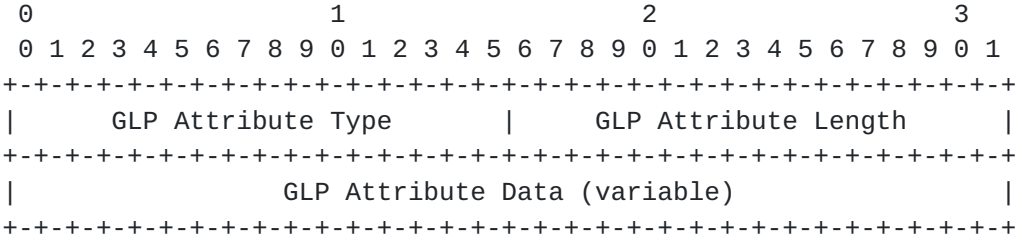
+1919 <= +19199929048 <= +1919993

Editor's Note. We could also make the phone numbers and next hop server into attributes (ie have the type, length, value format). Preferences anyone?

GLP Attributes.
The collection of attributes associated with this call routing object. For alignment purposes, this field starts on the first even-octet boundary after the previous field.

5.2.3 Generic GLP Attribute Format

A CRO may contain any number of GLP Attributes. Attributes provide additional information about the call routing object. Each GLP Attribute has the following generic format.



GLP Attribute Type.

GLP Attributes provide additional information that can be used to restrict the call routing path applicable to a specific signaling sequence. The following attribute types are defined in this specification.

1 - Supported Signaling Protocols
2 - Pricing
3 - Gateway Provider
4 - Next Hop Provider
5 - Supported Codecs
6 - Capacity
7 - Time-to-live

GLP Attribute Length.

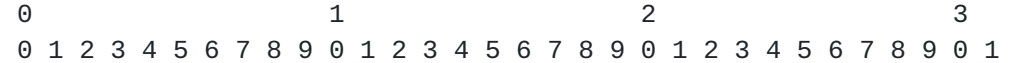
The length of this attribute from the start of the type field. The length must be even.

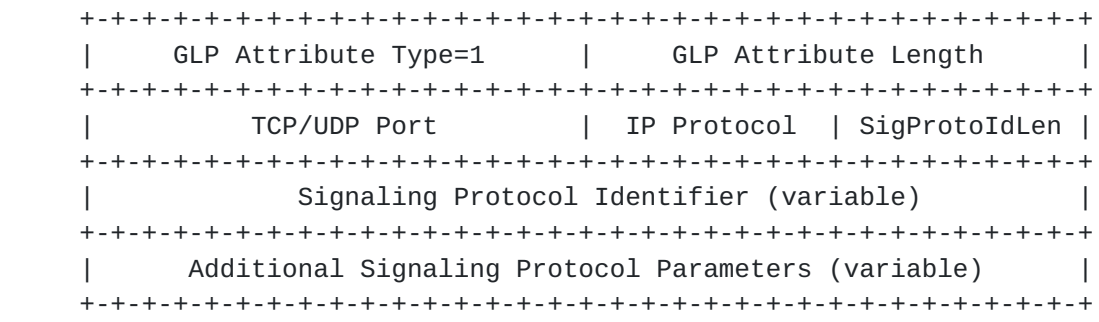
GLP Attribute Data.

The data specific to this attribute. The data format for each attribute is given in the following sections.

5.2.3.1 Supported Signaling Protocol Attribute

The Supported Signaling Protocol Attribute gives a signaling protocol supported for the CRO address range by the CRO next hop. There can be multiple instances of this attribute in a CRO CSA when a next hop can be contacted for the same phone numbers using multiple signaling protocols.





GLP Attribute Type.
Equals 1.

GLP Attribute Length.
Variable, even length.

TCP/UDP Port.
The TCP/UDP port that should be used to contact the next-hop when using the specified signaling protocol.

IP Protocol.
Indicates whether TCP (0x06) or UDP (x11) should be used to contact the next hop when using this signaling protocol.

Signaling Protocol Identifier Length.
The length of the Signaling Protocol Identifier field.

Signaling Protocol Identifier.
Identifies a signaling protocol that can be used to contact phone numbers in the CRO's phone number range using the specified next hop. The Signaling Protocol Identifier format is:
sig-proto-id = "SIP" | "H323"

Editor's Note. Is there a standard method of expressing signaling protocols like SIP or H.323 within a message? Couldn't find them registered with IANA.

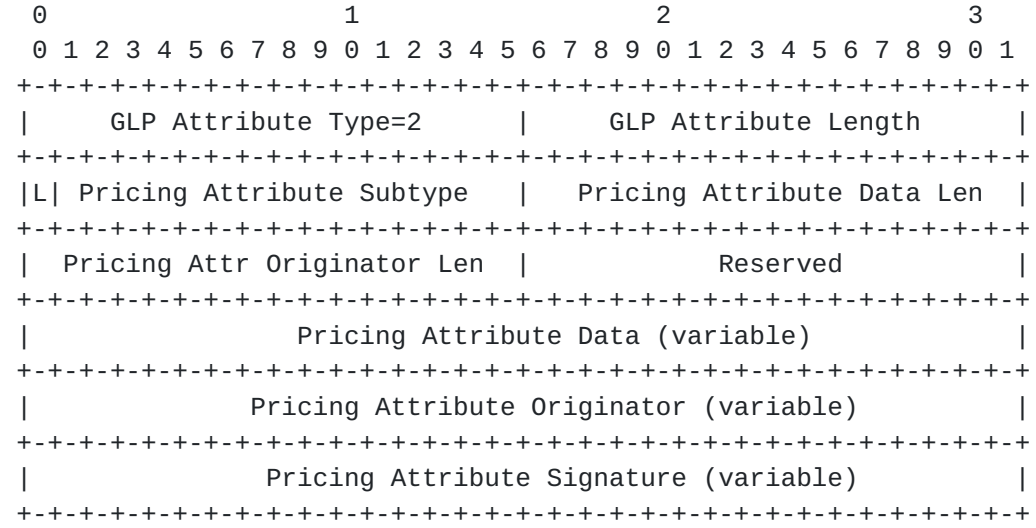
Additional Signaling Protocol Parameters.
This field can be used to specify additional signaling parameters needed to establish a connection using this signaling protocol to the specified next hop. This attribute should contain only those signaling parameters required to establish a connection that cannot be expressed by any other GLP attribute. Many signaling parameters can be negotiated during the signaling process. It is recommended that negotiable signaling parameters are not included in this attribute. Limiting the number of signaling parameters improves scaleability of the protocol. The format of this field is dependent on the signaling protocol.

Editor's Note. The goal of this last field is to allow the expression of any attributes that need to be given in order to allow the signaling to work. Since signaling protocols are evolving, we can't cover everything in attributes. This gives a back door to get needed information into the database. If this approach is acceptable, then we need to define the formats of this field for SIP & H.323.

5.2.3.2 Pricing Attribute

The purpose of the Pricing Attribute is to provide information on how much a call to a phone number in the CRO's telephone range would cost a user. The pricing attribute is sub-typed to yield several methods of expressing the pricing details.

The End Users must recognize the pricing attribute cannot be taken as a guarantee of a particular service for a particular price. Other factors may influence the actual amount a user is charged for a service. Pricing structures may have too many variables to guarantee the accuracy of this data to the end user. For example, the cost of a call through a gateway may depend upon the source of the call (ie are you a customer of ISP-X?). The cost may also depend upon the negotiated media capabilities. Such variables complicate the pricing structures. Other protocols (AAA, OTP, RSVP, etc) must perform the authentication, negotiation, accounting, etc. required to actually negotiate and authorize the final charge for the phone service. There can be at most one Pricing Attribute in a CRO.



GLP Attribute Type.
Equals 2.

GLP Attribute Length.
Variable, even length.

Pricing Attribute Subtype.
The subtype may have either local significance or be a registered subtype with IANA. Local subtypes have the L-flag set, while IANA registered subtypes have the L-flag cleared. The purpose of the local subtypes is so that within a ITAD, or within a confederation of ITADs, a pricing structure can be expressed in method that can be automatically interpreted by a program (such as the LS policy decision process) to better automate the choice of next hop. The format of the data section differs for each subtype.

The set of currently defined subtypes is:
1 - Text
2 - URL

Editor's Note. Any other suggestions on how to do pricing?

Pricing Attribute Data Length.
The length of the Pricing Attribute Data Field. Must be even.

Pricing Attribute Originator Length.
The length of the Pricing Attribute Data Field. Must be even.

Pricing Attribute Data.
The formats for the Pricing Attribute Data are given in subsequent sections.

Pricing Attribute Originator.
The originator of the Pricing Attribute. A LS should not propagate a CRO if the originator of the pricing attribute is not trusted.

Editor's Note. Any suggestions on how to handle representation of the originator? Company name? Web page? Contact information? Some ITAD numeric representation?

Pricing Attribute Signature.
A digital signature that can be used to authenticate the the validity of the pricing data. In the event of a false advertisement, the source of the false advertisement can be traced. The pricing attribute signature is calculated over the entire Pricing Attribute. The pricing attribute may be signed before being advertised by an LS. If an LS does not alter the Pricing attribute data, it must not alter the originator or the signature. If an LS does modify the Pricing attribute data, it must put itself as the originator and may sign the message as well.

5.2.3.2.1 Text

This Pricing Attribute subtype contains a textual description of a pricing strategy. The intent of this subtype is that this description can be displayed to an end user. The character set is ISO 10646 using UTF-8 encoding [UTF8].

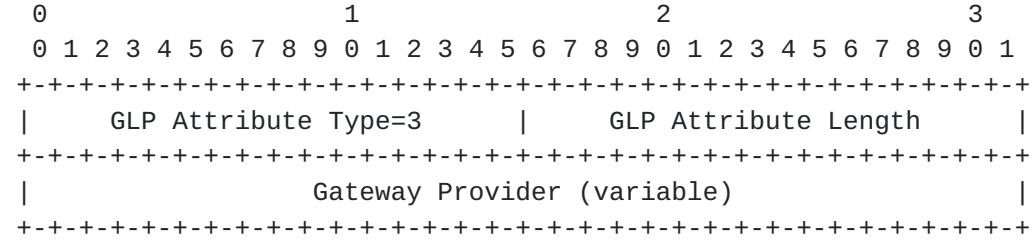
Editor's Note. If we want this, do we need to worry about language concerns? I'd prefer to let language concerns be handled by the URL sub-type and let this sub-type be simple character representations.

5.2.3.2.2 URL

This Princing Attribute sub-type contains a URL from which additional pricing data may be retrieved. The intent of this subtype is that the URL may contain data that can be displayed to the end user or used by some automated selection process. A pricing structure may be given in multiple languages using an HTTP URL and language negotiation as specified in HTTP [HTTP1.1]. URL formats are defined in [URL].

5.2.3.3 Gateway Provider

The Gateway Provider attribute specifies the owner/provider of an egress gateway to the PSTN indicated by this CRO. The provider of a gateway may be used when selecting how to route a particular call. There may be multiple Gateway Provider attributes in a CRO.



GLP Attribute Type.
Equals 3.

GLP Attribute Length.
Variable, even length.

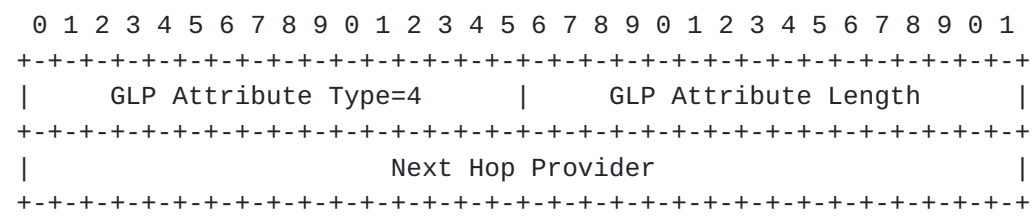
Gateway Provider.
The Gateway Provider field specifies the owner/provider of the

egress gateway for this CRO.

Editor's Note. We are now presented with the question of how to represent an Internet telephony service provider. Two obvious possibilities are using a numeric representation along the lines of a BGP AS, or using a string representation along the lines of DNS. Could we use DNS names or do we need a new type of name? Maybe a URL?

5.2.3.4 Next Hop Provider

The next hop provider attribute specifies the owner/provider of the next hop SS specified by this CRO. Like the Gateway Provider attribute, the Next Hop Provider may be used when deciding how to route a particular call. A single Next Hop Provider attribute must be in every CRO.



GLP Attribute Type.
Equals 4.

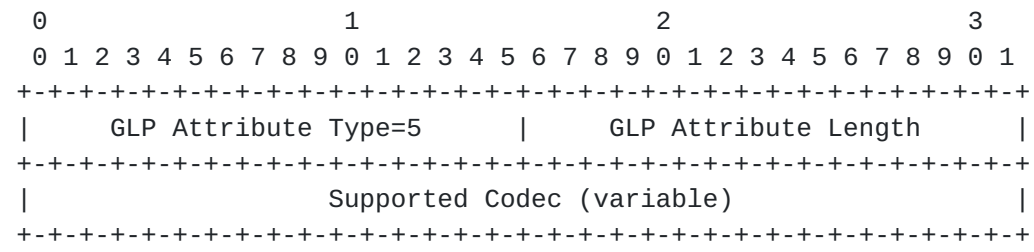
GLP Attribute Length.
Variable, even length.

Next Hop Provider.
The Next Hop Provider field specifies the owner/provider of the provider of the next hop signaling server listed in the CRO. A single Next Hop Provider attribute must exist in every CRO.

Editor's Note. Again have to worry how to represent providers.

5.2.3.5 Supported Codec

This attribute is used to specify the codecs that are supported by an egress gateway that can be reached via the next hop in this CRO. There may be multiple Supported Codec attributes in a CRO.



GLP Attribute Type.
Equals 5.

GLP Attribute Length.
Variable, even length.

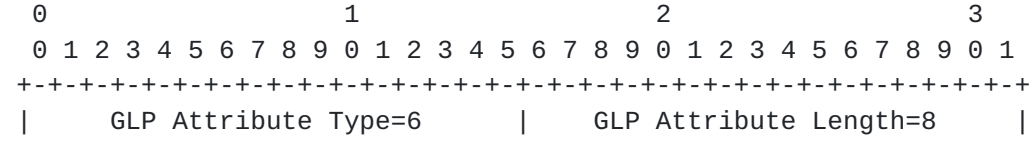
Supported Codec.
Specifies an algorithm for the encoding and decoding of packetized voice. The set of registered codec names is maintained by IANA [RFC1890]. Non-registered codecs are indicated by preceding the name with "X-". The format for the Supported Codecs field is:

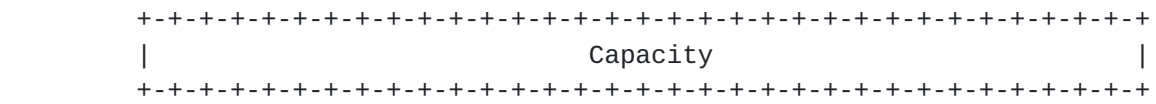
supported-codec ; see [RFC1890]

5.2.3.6 Capacity

Gateways may have varying capabilities with regard to the number of phone calls that can be simultaneously processed. The capacity of a gateway may be limited by link speed, memory, the number of circuits, etc. The Capacity Attribute allows administrators to assign gateways a metric representative of their capacity. The Capacity Attribute is a relative metric to be used across a confederation of ITADs. The determination of the capacity of a gateway as communicated by this attribute is an administrative matter. The unitless nature of the Capacity Attribute makes it impossible to compare the capacity of two gateways in different Internet telephony confederations. This attribute can be used to load-balance connections between a set of satisfactory next-hops. Note that this metric is NOT a path cost, but a relative measurement of the capacity of the egress gateway(s). This attribute is not intended to indicate any aspects of the real-time load on the gateway(s). This attribute may be modified by intermediate LSs when performing aggregation or filtering of CROs. Only one Capacity Attribute is permitted in a CRO.

The format of the Capacity attribute is given below.





GLP Attribute Type.
Equals 6.

GLP Attribute Length.
Equals 8.

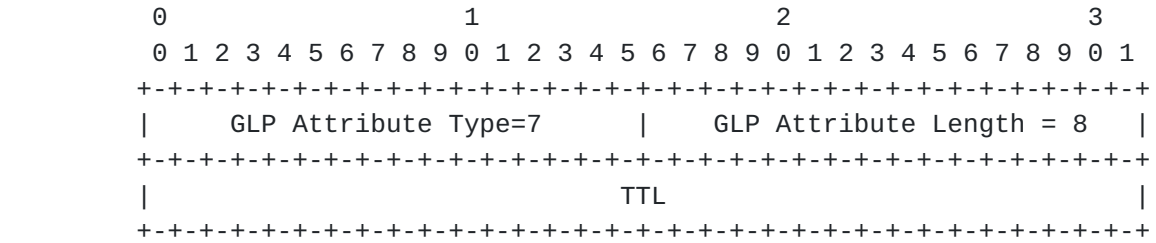
Capacity.
A relative measurement of the capacity of the egress gateway(s) represented by the call routing object. Represented as a 32-bit unsigned integer. A larger value in the Capacity field represents a CRO with more egress gateway capacity. The capacity of a gateway(s) is a relative value and cannot be used for comparison between different Internet telephony confederations.

Editor's Note. We could define some unit(s) for the capacity metric. For example, bandwidth, maximum circuits, etc. Defining multiple units complicates the comparison of two capacities (ie is 10 Mbps greater than 20 circuits?), but makes the measurement more concrete. Suggestions?

5.2.3.7 Time-To-Live

The TTL attribute is used to prevent loop detection. A LS must decrement the TTL of a CRO that it advertises to a peer in another administrative domain. When aggregating multiple inbound CROs into a single outbound CRO, the aggregated CRO must have a TTL less than all of the CROs that served as input for the outbound CRO. CROs with a TTL of zero must be ignored on receipt and should not be transmitted. Each CRO must contain a single TTL attribute.

The format for the TTL Attribute is:



GLP Attribute Type.
Equals 7.

GLP Attribute Length.
Equals 8.

TTL.
The number of intermediate LSs through which this CRO may be forwarded. The default value for CROs originated within the local ITAD is XXXX (?).

Editor's Note. Might be better to use a loop detection algorithm more like BGP where we record the route of every entry. Preferences?

Editor's Note. SCSP doesn't have any error indication defined. Should we try to define one, or just have the application layer deal with errors.

Editor's Note. Instead of including all of the attributes with the call routing information in a single object, we could put each attribute into its own object. This would allow attributes to be updated independently of the base call routing data (ie every update wouldn't have to include the entire CRO), but would require more objects and the correlation of the objects.

6 Security Considerations

SCSP has an Authentication Extension that can be appended to any SCSP message. When included in a SCSP message, the Authentication Extension provides integrity and authentication between directly connected peers. It is recommended that GLP speakers use the Authentication Extension of SCSP to validate incoming GLP messages.

LSs may also wish to provide confidentiality for their transmitted data. To achieve confidentiality, peer LSs may communicate over an encrypted TCP connection.

7 IANA Considerations

- scsp pid - tcp port for scsp?
- signaling protocols
- internet telephony admin domains
- other?

8 Conclusions

9 References

[GLP-FR] J. Rosenberg and H. Schulzrinne, A Framework for a Gateway Location Protocol, Internet Draft, Internet Engineering Task Force, Work in Progress, 1999

[BGP4] Y. Rekhter and T. Li, A border gateway protocol 4 (BGP-4), Request for Comments (Draft Standard) 1771, Internet Engineering Task Force, Mar. 1995. (Obsoletes RFC1654).

[OSPF] OSPF

[SIP] SIP

[H323] H323

[SCSP] SCSP

[HTTP1.1] HTTP 1.1

[UTF8] ISO 10646 in UTF8 (rfc 2279)

[RFC1890] RTP codec names & payload types

[URL] URL formats

[ISO4217] ISO 4217 (currency codes?)

Author's Address

Matt Squire
Nortel Networks
4309 Emporer Blvd
Suite 200
Durham, NC 27703

Phone: (919) 992-9048

msquire@nortelnetworks.com