Contribution Number

GIBSON: Global IP-Based Service-Oriented Network Architecture Overview and IMS User Case

August 8, 2006

Contributor: Ping Pan, Tom Nolle

Organization: Hammerhead Systems, CIMI Corp.

Author

Address

Address

City/State/Zip

Phone

Fax

E-mail: ppan@hammerheadsystems.com, tnolle@cimicorp.com

Working Group (if applicable)

Abstract

GIBSON (Global IP-Based Service-Oriented Network) is an architecture that is focused on providing data-plane service provisioning and management in the context of IPsphere. One of its key objectives is to interface with business routing at network edge/border to achieve end-to-end (or edge-to-edge) per-user-flow service guarantees.

In this document, we will provide an outline of the GIBSON architecture, and illustrate its operation in multi-provider IMS environment.

Declaration of IPR

IPsphere Forum disclaimer (copyright and IP).

IPsphere FORUM

THE BUSINESS OF IP

Introduction and Motivation

Providing new services within the existing IP infrastructure will face the following challenges:

1. Access/metro and backbone networks may belong to different carriers or business entities. For example, the access networks may belong to wireless service providers, while the backbone networks may belong to a national or global carrier that provide data transport services to multiple access or metro networks. There will be technology differences among providers and also often between the metro/access and core networks of the same provider.
2. There will be a considerable variability in the "value" of service relationships and thus in the per-service handling that can be justified. Some sessions will be handled individually (video, for example) and others will likely be handled in aggregated form (voice).
3. Also, there may be regulatory issues such as intercept/surveillance that will have to be applied, or that will have to be routed around to avoid.
4. Since user traffic is transported as IP packets throughout the network, the backbone carriers may not have the ability or incentive to provide special treatment to *important* user flows. Subsequently, "hot-potato" type of routing polices are applied to inter-carrier traffic. The end users can only rely on application-level congestion and flow control, such as TCP, to regulate traffic. This practice will not likely to scale as end-user applications become more bandwidth-intensive and delay-sensitive.
5. Services will have to be created at network edge and border. Service providers may offer new services, such as voice, video, security and VPN, from network edge. Given the competition from application service providers, the operation cost must be manageable.

We illustrate the potential problems in the context of IMS below:

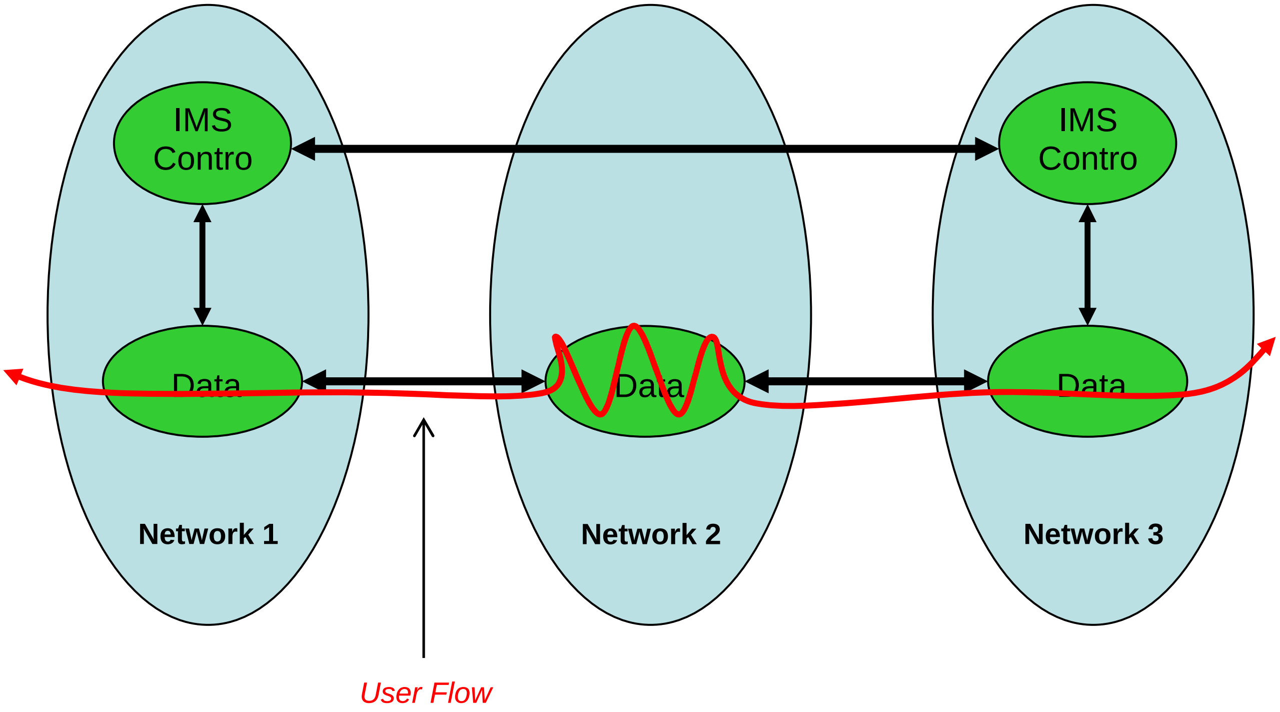

Figure-1: Current multi-provider IMS operation

As shown in Figure-1, IMS in Network 1 and 3 negotiate with each other to establish a session, say, a video session on a real-time event. Since the two IMS domains (1 and 3) may not be directed connected, the traffic may pass through a third party network (Network 2). In this case, Network 2 has no knowledge of the importance of the traffic, and will treat it as an ordinary flow which subjects to drop and delay. Note that in multi-carrier environment, the standardized QoS mechanism (e.g. DiffServ marking), will be difficult to enforce beyond the boundary of a single domain.

When we look into the problems more closely, we can derive the following:

1. Network edge must provide extensive data flow processing capability:
    a. The data flows may be in many format types depending on the services: Ethernet VLAN, TCP, RTP, MPEG and HTTP, etc.
    b. There may be many data flows (in the range of millions) at various granularity
    c. Not all the flows need to have special treatment. However, for some of the important traffic, service guarantees may include rate and delay guarantee, traffic shaping, encryption, redundancy and protection, performance monitoring, rate adaptation, traffic acceleration, address remapping, etc.
2. Traffic forwarding at network boundary (edge or border) depends on business policies. However, it may also be difficult or even impossible to apply non-technical routing metrics to selection of pure IP paths, and so it will be difficult to insure that business routing decisions made by IPsphere's SMS Admin function will actually be carried out. For high-value services like leased lines, there is also a need to know where the service flows are going.
    a. The policies are driven by bilateral or multi-lateral business arrangement
    b. Within core network, the policies may be static and long-lasting
    c. At network access edge, the policies may be somewhat dynamic depending on service and user behavior
    d. The required business policies may have little relevance with IP routing
3. There must exist some type of logical entity, such as IPsphere SSS, that is responsible for the binding of service control-plane and data-plane:
    a. To guarantee QoS on data flows, the data-plane must be able to gather service parameters (such as the ones from SIP/SDP) from control-plane. Note that, in case of IMS, control messages and data packets do not necessarily traverse through the same path. Thus, it requires the logical entity, like IPsphere SMS, to correlate flow information between CSCF and packet switches.

GIBSON Architecture Overview

GIBSON (Global IP-Based Service-Oriented Network) architecture is to address the following:

1. Open interface for business service creation and provisioning
2. Operate in both intra-provider and inter-provider environment
3. Provide consistent edge-to-edge per-flow forwarding behavior
4. Flow type agnostics – capable of processing flows in any format
5. Independent of underlying network transport tunneling mechanism
6. Applicable on all service devices, with less dependency on IP routing

Figure-2 illustrates the GIBSON architecture:

The GIBSON endpoints (or GIBSON-Enabled Nodes) are the devices that are responsible for processing user data flows by interfacing with IPsphere SMS child. Between the GIBSON endpoints, there could be one or multiple networks. The GIBSON endpoints always operate at network edge and/or border.

The GIBSON endpoints are interconnected via one or multiple "transport tunnels", which can be used to aggregate and transport data flows. Typical transport tunnels are MPLS LSP's, Ethernet VLAN trunks, SONET cross-connects and the newly defined PBB/PBT.

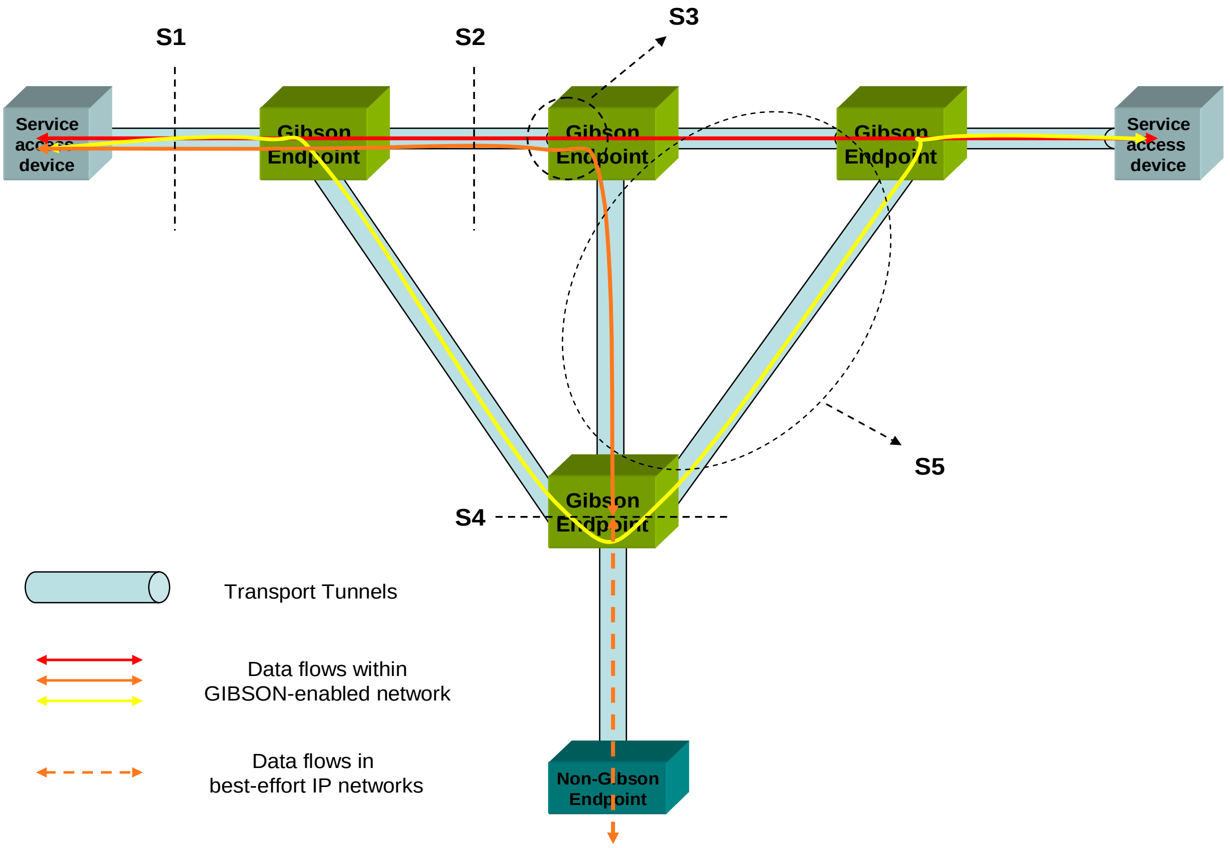

Figure-2: GIBSON architecture overview

The GIBSON endpoints can handle data flows in any format, and encapsulate them in the form of Pseudowires, as defined in IETF [PWE3]. The reason for choosing Pseudowires is due to the following considerations:

- Most important of all, Pseudowires are transport-agnostic in they can support IP and Ethernet, and can even remap to optical. Gibson Pseudowires also recognize multipoint transport behavior and can exploit it at the service level to facilitate multipoint services
- IP-friendly: Pseudowires are provisioned and controlled via IP control plane
- Flow type agnostic: Pseudowires can encapsulate any type of data flows. As defined today, Pseudowires can encapsulate Layer-1 flows in SONET/SDH format (the technique is known as Circuit Emulation), Layer-2 flows such as ATM, Frame Relay, PPP and Ethernet, and IP
- Application-awareness: In the context of GIBSON, Pseudowires can be used to encapsulate application-aware streams such as RTP and MPEG. Application-awareness will enable the GIBSON endpoints to leverage a number of techniques for congestion control, rate adaptation and protection

- Tunnel type independent: PWE3 multi-hop [MHOP] and switching [SWITCH] techniques enable the providers to provision Pseudowires over multiple networks and tunnels types.
- SLA capable: Pseudowire technique can provide QoS [MHOP], protection and restoration [PROTECTION] and congestion control [CONGESTION] functionality at per-flow basis.

As shown in Figure-2, GIBSON operation can be described in five areas:

S1 - Access Interface

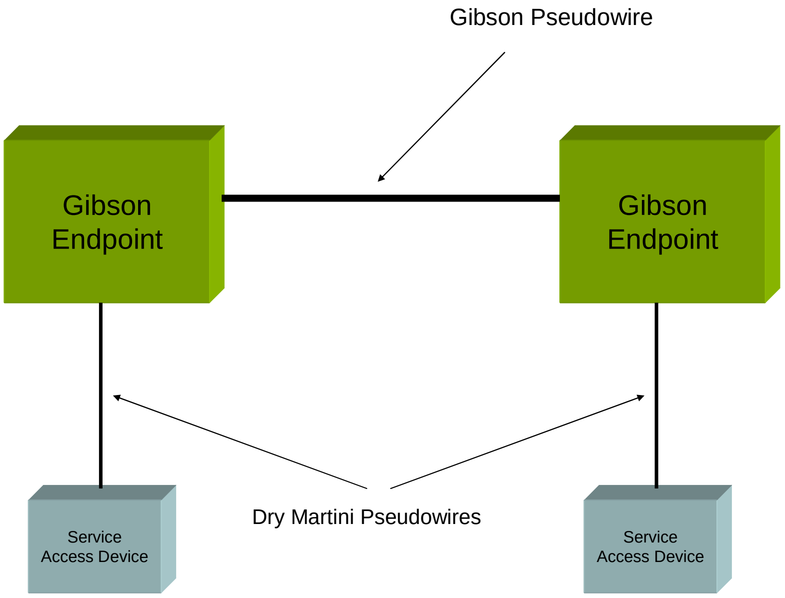

Figure-3: GIBSON S1 interface

This is where GIBSON Endpoints aggregate user flows from service access devices. The service access devices may include a wide range of equipment including IP DSLAM, PON, SONET/SDH MSPP and wireless base-stations. The service access devices do not need to be fully IP routing capable. Instead, they need to be efficient in supporting the services that they are designed to do.

Service access devices can deliver user flows in native format (such as VLAN), or construct the flows as standard Pseudowires.

Upon the reception of user flows from service access devices, the GIBSON endpoints can either convert the flows in native format to Pseudowires, or, most conveniently, switch the incoming Pseudowires as GIBSON Pseudowires.

Since the access network topology is relatively simple, the service access devices do not need to be routers. Therefore, there is little use in running complex IP routing and signaling protocols to setup Pseudowires over MPLS networks, as defined by IETF [PWE3-CTRL]. The access devices may use a much simpler approach in Pseudowire setup as defined in [Dry-Martini].

IPsphere SMS controls the initiation, maintenance and termination of GIBSON Pseudowires at each GIBSON Endpoint. This implies that the service providers have the full-control of edge-to-edge user flows. Further, by interfacing with business database through SMS, the providers can readily provide subscription, monitoring and accounting services at data-plane level.

S2 – Data Aggregation

Between two GIBSON endpoints, user data flows are aggregated into transport tunnels. As described previously, the transport tunnel could be any type preferred by the service providers. It could be MPLS LSP established via RSVP-TE or LDP in core networks, and could be Ethernet PBT tunnels in metro networks.

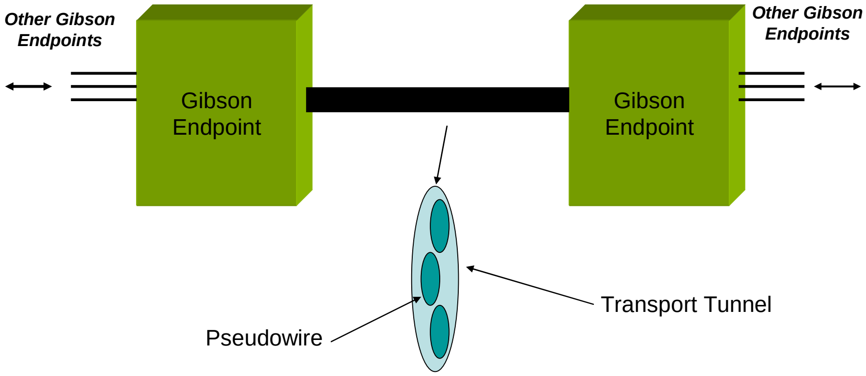

Figure-4: GIBSON S2 interface

The Pseudowire aggregation process may be bounded by the business policies distributed via IPsphere SMS. The policies may determine the allocation of Pseudowires into transport tunnels, and the modification of transport tunnels to accommodate the Pseudowire network resource consumption.

S3 – Pseudowire Routing

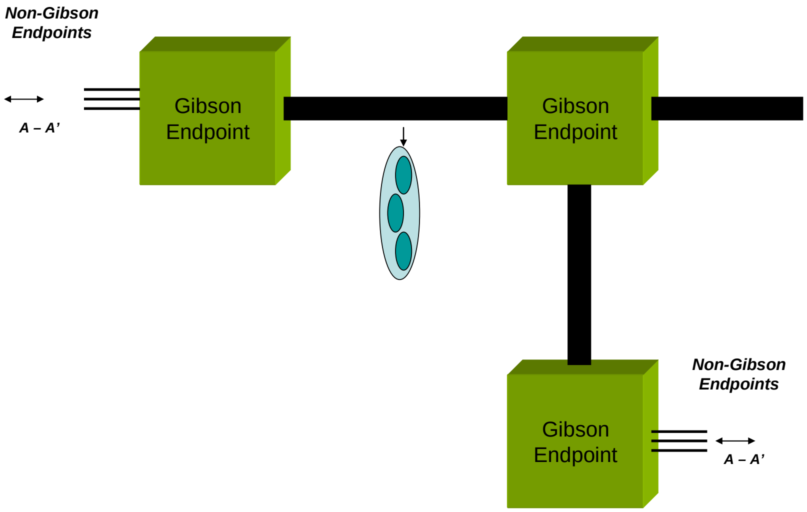

Figure-5: GIBSON S3 interface

Within the network, the intermediate GIBSON endpoints will terminate the transport tunnels, and switch the Pseudowires into another set of tunnels toward their destination. At GIBSON Pseudowire setup time, each Pseudowire request message will carry information such as QoS, protection and congestion control data and user flow information.

In case of IMS, the user flow and QoS information will be derived from SDP, and translated and encoded by the Pseudowire-initiating GIBSON endpoints into the setup messages. The transit GIBSON endpoints will use this information for routing.

GIBSON Pseudowire routing involves business policies. There are a number of methods for GIBSON Pseudowire routing:

- The first method is that providers download a set of business policies to the GIBSON endpoints through SMS
- The second method is to have the GIBSON endpoints querying business database through SMS, upon the reception of Pseudowire setup requests
- Finally, the providers may simply use MP-BGP (i.e. 2547bis) to distribute GIBSON capability within the network. The GIBSON endpoints can learn about the topology for Pseudowire forwarding. Note that this may be the preferred method for forwarding non-GIBSON-enabled Pseudowires.

S4 – Pseudowire Termination

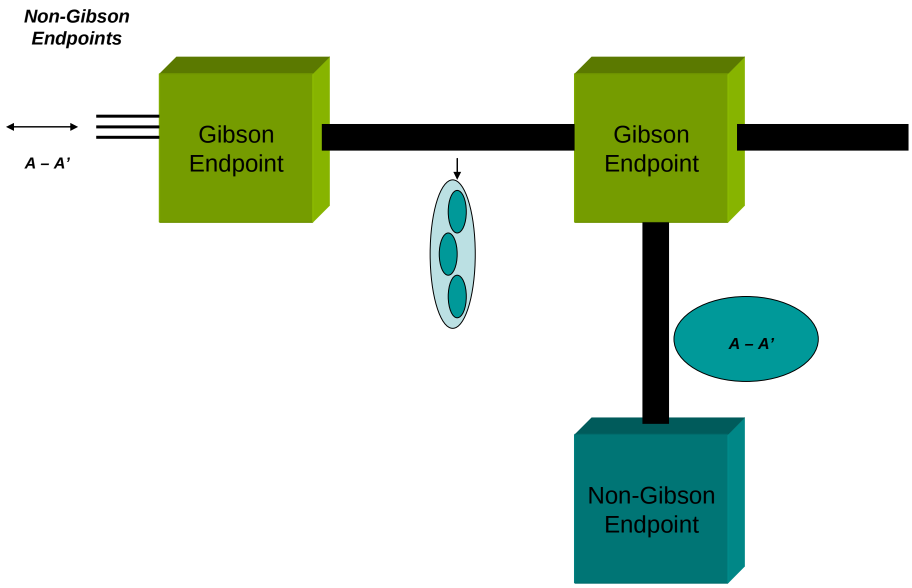

Figure-6: GIBSON S4 interface

When interfacing with Non-GIBSON-enabled nodes, the GIBSON endpoints will terminate the Pseudowires and forward the original users traffic. Since there will be no service guarantees beyond this point, the service providers will be notified about partial service guarantees on data flows. Flow information carried at Pseudowire setup time will permit the terminating process to map the flow correctly onto the egress network.

S5 - Multipoint Transport

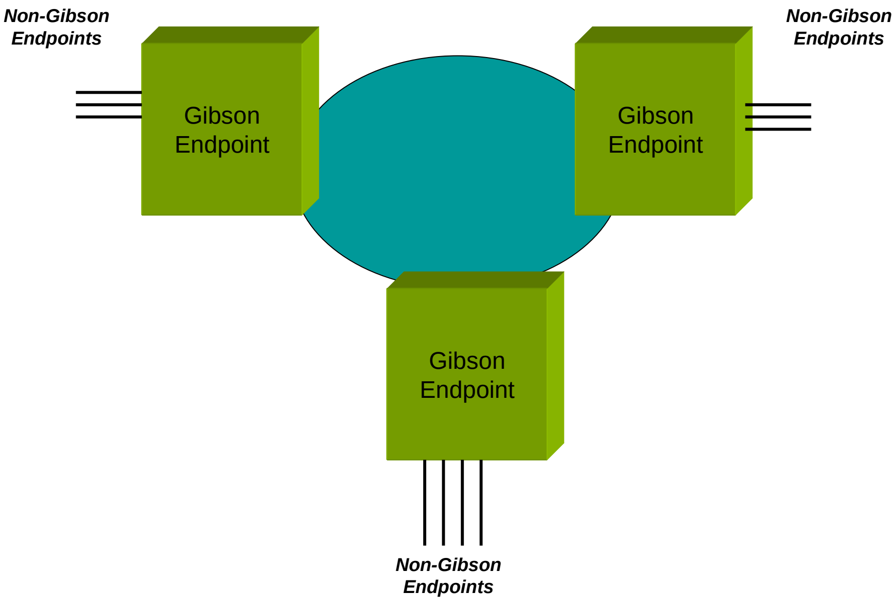

Figure-7: GIBSON S5 interface

The GIBSON endpoints can interface with IPsphere SMS to discover network topology. In turn, it can use the standard VPN mechanism, such as 2547bis option 2(b), VPWS and IPLS to construct point-to-multipoint VPN networks. Note that the Pseudowire is not multipoint in itself, but it can be routed over a multipoint transport process.

At network boundary, GIBSON endpoints will terminate the Pseudowires and forward data packets.

A User Case for IMS

In an earlier section we outlined some specific issues associated with IMS routing. How would IPsphere and GIBSON architecture overcome the problems?

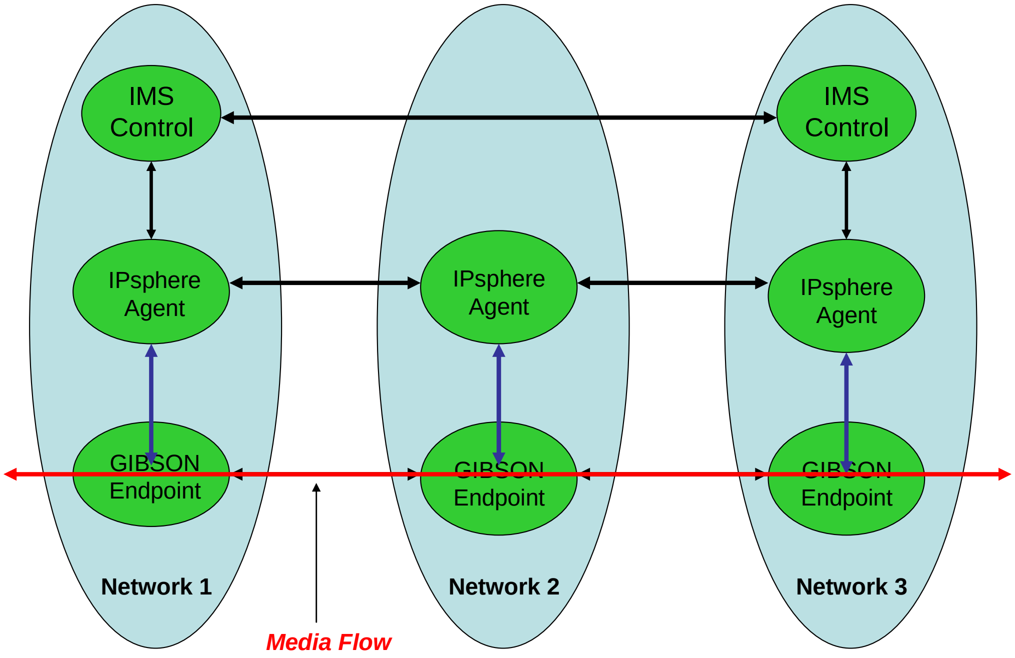

Figure-8: GIBSON Operation in IMS Environment

Figure-8 presents one possible solution:

1. Initially, GIBSON Endpoints in Network 1, 2 and 3 will setup transport tunnels among each others. The tunnel information will be uploaded to the IPsphere Agent.
2. Access networks 1 and 3 have their own IMS (a.k.a. IMS domains). Through IPsphere Agent, the IMS will populate the database (e.g. HSS) with network resource information and transport tunnel identification.
3. The end users in both networks will negotiate multimedia sessions via CSCF. During session negotiation, SDP will distribute the transport tunnel information to the end users.
4. When the sessions have been established, IMS will notify IPsphere Agent about the session data flow information (that is, RTP session) and associated tunnel information.
5. IPsphere Agents distribute the data flow information to the GIBSON Endpoints in Network 1 and 3.
6. For some critical flows, IPsphere Agent will also compute the policy routes between Network 1 and 3, and distribute the routing information to the intermediate GIBSON Endpoints.
7. The GIBSON Endpoints in Network 1 and 3 will setup Pseudowires for user data flows. The Pseudowire type depends on the application itself. In this case, the GEN may choose IP as the default Pseudowire type. The Pseudowire routing information comes from IPsphere Agent.
8. When Pseudowire setup messages have arrived on Network 2, the GIBSON Endpoints would use pre-installed policy routes to direct the Pseudowires toward Network 3.
9. During the Pseudowire setup, the setup messages will carry SLA parameters. The GIBSON Endpoints will process the SLA information, and run admission control algorithms to aggregate Pseudowires into the pre-established transport tunnels.
10. When end-user data traffic in Network 1 and 3 arrive on the GIBSON Endpoints, they will be mapped to the corresponding Pseudowires.

In this approach, two levels of admission control will take care. At control-plane, IPsphere Agents provide network resource information to IMS, which may result in call admission control at SIP setup time. At data-plane, IPsphere Agents provide per-user flow information to GIBSON Endpoints, which will aggregate each user flow in the form of Pseudowire to transport tunnels.

As a result, data flows will have QoS guarantees throughout the network.

Future Work

We need to investigate the interface between IPsphere SMS and GIBSON endpoints. Further we would like to apply the GIBSON architecture in other user cases, such as VPN.

References

[PWE3] http://www.ietf.org/html.charters/pwe3-charter.html

[MHOP] IETF Draft, L. Martini, et al, “Dynamic Placement of Multi Segment Pseudo Wires”, work in progress

[SWITCH] IETF Draft, L. Martini, et al, “Segmented Pseudo Wire”, work in progress

[PROTECTION] IETF Draft, P. Pan, et al, “Pseudowire Protection”, work in progress

[CONGESTION] IETF Draft, P. Pan, et al, “Pseudowire Congestion Control”, work in progress

[Dry-Martini] IETF Draft, P. Pan, et al, “Dry-Martini: Supporting Pseudo-wires in Sub-IP Access Networks”, work in progress

[PWE3-CTRL] IETF RFC 4447, L. Martini, et al, “Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)”