Autoconfiguration Mechanism for IP Telephony Location Servers

SCN-IP Telephony Convergence

Jose Costa-Requena, Ignacio Gonzalez Olias, Raimo Kantola, Nicklas Beijar
Networking Laboratory. Helsinki University of Technology

Abstract: IP Telephony is clearly the service that converges data and real time voice, video over IP networks. This paper shows that the convergence for this specific service is feasible. Nevertheless, it shows that certain technologies trends needs to be solved. The smoothly transition from switched telephony over IP networks can be achieved. This paper analyses a suitable architecture and presents specific enhancements to be implemented in the existing IP Telephony routing protocols. The appropriate auto-configuration and replication mechanism in the proposed architecture will facilitate the data synchronisation across switched and IP technologies. This will promote the convergence of services into IP networks in a seamless manner.

Key words: Location Servers, Synchronisation, TRIP, SCSP, IP Telephony, Routing and Auto-configuration.

1. INTRODUCTION

IP networks were designed to provide an efficient and robust mechanism for transferring data between remote computers. Initially, the information exchanged was mostly computer related data: text documents, files, web content, etc. However, the increasing popularity of this kind of networks is encouraging the development of new services and applications that take advantage of the existing infrastructures. IP telephony, is a clear convergence example of services that traditionally had been provisioned in switched networks. Therefore, it is clearly stated that convergence of data and real time communications will happen over IP networks.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35673-0_28](https://doi.org/10.1007/978-0-387-35673-0_28)

C. McDonald (ed.), *Converged Networking*

© IFIP International Federation for Information Processing 2003

IP Telephony is a service that was traditionally offered using public switched telephone networks (PSTN), and now it has been adapted to the IP networks. Nevertheless, the migration from one approach to another can not take place overnight, both technologies will be interacting for a period of time. This interaction generates new interoperability problems that must be addressed. Data and signalling conversion between both networks is performed by special entities called gateways. Section 2 presents the proposed architecture that solves the problem of gateway location for providing IP Telephony routing information across networks. Section 3 shows the novel auto-configuration module added to enhance their scalability and flexibility features.

2. IP TELEPHONY NETWORKS

IP networks are becoming more popular, IP Telephony (Voice over IP) is being developed in order to take advantage of the existing infrastructures. The next generation of Mobile networks (UMTS [1]) are fully deployed on top of IP networks. The final goal is to completely replace conventional wire or wireless telephony by IP based telephony. Since this process requires some time and effort, it has to be carried out in progressive stages.

At first, IP telephony has been introduced only in private networks, as the technology needed to expand it into public networks is under development. It is expected that IP telephony will be gradually connected to the existing PSTN, meaning that both technologies will be interacting for a period of time. The main part of the current research is focused on this area. A decisive target is to develop reliable and optimal mechanisms to make both networks interact. Several architectures and protocols have been proposed to match the requirements of the new telephony. The Internet Engineering Task Force (IETF) has defined a set of protocols to implement Telephony over IP networks. One of those protocols is the Session Initiation Protocol, SIP [2] that defines the signalling protocol to setup a voice/video session between IP terminals. Another important protocol defined at the IETF is the (Telephony Routing over IP, TRIP) [3]. The TRIP protocol was specified to address the problem of locating the right gateway to perform the signalling conversion, when traversing between switched and IP networks [4].

2.1 Telephony Gateway Location

When a telephone call originated in an IP network needs to be routed to a destination located within the PSTN, it must traverse a device capable of performing data and signaling conversion between different technologies.

This device is called a gateway, and it is situated on the boundary between the IP and PSTN networks, playing a central role in IP-PSTN integration. The operators will have in their administrative domain (IP Telephony Administrative Domain, ITAD) multiple gateways with different features and capacities. The main problem is how to choose an optimal gateway to route every new IP-side originated call towards the PSTN. One solution to this problem could be the use of a global database to store gateway information. Every time a call needs to be routed towards the PSTN, the required information would be retrieved from the database. This solution assumes that every gateway is made available to everyone, and overlooks the possible existence of different operators running different policies.

However, the expected scenario is likely to be rather complex, with many gateway providers operating at the same time and making their gateways available depending on local policies. This means that one specific provider may be willing to let other providers make use of its resources or not, depending on the policy it is running. Thus, the idea of a global database must be discarded since it does not match the real requirements. Instead, providers can make use of the TRIP protocol to exchange information about gateway availability between different domains [5]. TRIP protocol was originally designed on top of the Server Cache Synchronization Protocol (SCSP) [6] that was used to maintain the distributed database of routing information. Figure 1, shows the structure to provide Telephony routing information across switched and IP networks using TRIP.

Figure 1. IP Telephony Interoperability using TRIP

After some discussion, the IETF IPTEL working group decided to include the replication mechanism within the protocol itself. This new version was modeled after the Border Gateway Protocol (BGP4). Nevertheless, the prototype used for implementing the test bed is based on

the original TRIP using SCSP [7]. Thus the replication task is performed by SCSP for both inter and intra domain relationships. Furthermore, the prototype has been enhanced with auto-configuration and security modules [8] to design a new scalable and flexible version of TRIP protocol.

2.2 Synchronisation Module

The TRIP protocol is responsible for distributing gateway availability information between different administrative domains, while the Server Cache Synchronization Protocol (SCSP) performs the required database replication. TRIP is responsible for processing all the routing information from different domains and keep a cache with the information about all the available gateways.

The Server Cache Synchronization Protocol (SCSP) addresses the problem of database synchronization within a set of servers, also called Server Group (SG). The server under scrutiny is called Location Server (LS), and it is connected to one or more Direct Connected Servers (DCS). Any other protocol that requires database replication may use the cache synchronization services provided by SCSP.

2.2.1 SCSP Phases

The SCSP protocol performs three phases:

Hello phase. The LS and its DCSs exchange Hello messages in order to establish a bi-directional peer-to-peer connection. Afterwards, Hello messages are periodically sent to ensure that connection is alive. If one node becomes inoperable, its peers will not receive Hello messages and the connection is closed, then it will try to establish a new one.

Cache Alignment phase. The connection reaches the bi-directional state, and the peer servers exchange the contents of their caches to synchronize them. Every server sends a summary of the entire database entries (Cache State Advertisement Summary records, CSAS) to its peers for comparing it with their own databases. After the CSAS comparison, a server decides what information should be requested from each peer. Database entries are exchanged as Cache State Advertisement records (CSA records). After the requested data is exchanged, all the caches within the SG are synchronized.

Cache Update phase. This phase is responsible for the propagation of updates to keep the caches synchronised whenever any change occurs. When a server sends an update to a peer, it always waits for the acknowledgment to ensure that the update was properly received and processed. Figure 2, shows all the phases in the SCSP protocol.

Figure 2. SCSP phases

2.3 TRIP Architecture

TRIP uses the LS to exchange routing information between different ITADs. All the LSs within the same domain are driven by the same policy and they have the same routing information database. The ITADs may be divided in smaller areas. Then, the LS are grouped into SGs that are used to synchronise all the databases of the LSs belonging to the same area. The information exchange between areas takes place by inter-area connections, which have at least one representative (LS) from each area involved in the agreement. These connected LSs are called external peers as they exchange inter-domain data. One LS from each participating ITAD can be present in the inter-domain SGs. The inter-domain SGs exchange routing information between different ITADs. The overall architecture is illustrated in figure 3.

Figure 3. TRIP architecture with inter-domain Administrative Domains

2.4 Configuration Mechanism

The TRIP/SCSP specifications do not mention from where the node gets all peers and the SG information. Each TRIP/SCSP node can load its SCSP configuration parameters from a static file. This means that every single change introduced in the topology of the network must be handled manually by the network administrator.

SCSP places no topological constraints on a SG, and this feature represents an important advantage over similar protocols. BGP, the current exterior routing protocol used for the global Internet, requires fully meshed topologies to interconnect all the members within the same Autonomous System (AS). The addition of a new member to a domain should be notified to all the existing nodes, which means a serious scaling problem.

SCSP allows database synchronization among nodes interconnected with an arbitrary topology. This feature provides a great deal of flexibility as well as simplicity in the configuration files of the nodes.

Even though this SCSP feature improves scalability, it is always better to automatically deal with topology changes. Therefore, an auto-configuration mechanism that improves the scalability of the system is proposed. Manual intervention is no longer required, since all the changes in topology are performed automatically. It prevents the network from accidental misconfiguration errors due to any manual intervention when modifying the configuration files of the servers. This improves the reliability and

availability of the system, where servers do not need to be restarted when there is a change in topology.

2.5 Security Mechanism

When designing the TCP/IP protocols the security issues were not a primary concern. Therefore, to have a completely effective dynamic configuration mechanism, it must be enhanced with some security procedures. The main vulnerability in the TRIP/SCSP architecture is IP spoofing, where the intruder pretends to be sending data from a fake IP address. This allows intruders to capture and modify routing information that is being exchanged between two LSs.

TRIP speakers should have the means to ensure that the information was truly generated by the sender, and not modified during the transmission. In case a third party has access to messages in transit, the sensitive information must remain inaccessible to guarantee the routing information integrity over different TRIP hops. Otherwise, the routing traffic could be vulnerable to several attacks that would lead to an incorrect operation of the protocol. TRIP packets could be intercepted and modified during transmission between peer nodes. The final consequence is an undesired operation of the whole IP Telephony architecture. The SCSP protocol has been extended with new headers to verify the identity of its peers before setting up the SCSP connections. The LS is able to verify that a received message comes from a real TRIP speaker that is authorized to act on behalf of its ITAD. The update message may traverse several ITADs and will be processed by several LSs during the propagation. The receivers need some mechanism to check the integrity of TRIP route attributes and verify the identity of the LSs that legitimately modified them.

Therefore, the auto-configuration mechanisms should verify the identity of other peer nodes that want to dynamically join the architecture (Figure 4).

3. AUTO-CONFIGURATION MODULE

The main purpose of the SCSP auto-configuration module is to address the static configuration problem. This mechanism must be able to handle dynamic changes in both intra and inter domain topologies when needed. Therefore, new servers can be added to existing SGs or new SGs can be created on-demand without any manual intervention.

The proposed auto-configuration service do not rely on the presence of central servers to obtain the topology information. Instead, the mechanism is decentralized and all the required information is distributed on other existing

SCSP servers. This approach improves the scalability of all the architectures that are using SCSP as the underlying replication service.

The proposed auto-configuration module comprises two basic services: intra-SG and inter-SG. The former is aimed to facilitate the on-demand addition of servers to an existing SG, so its scope is limited to a single replication group.

The inter-SG mechanism, however, addresses a more specific problem closely related to the TRIP/SCSP architecture. Every ITAD makes use of at least one internal SG to perform the intra-domain synchronization. All SCSP nodes taking part in the ITAD must belong to the intra-domain SG. An operator may decide to further divide its ITAD into areas. In this case, there is a separate SG to perform the synchronization within each area, and additional SGs, called inter-area SGs, are set up to distribute the routing information between two or more areas. Inter-domain agreements between different operators also use additional SGs, known as inter-domain SGs, whose members are representatives of the ITADs involved in the agreement. The main goal of the inter-SG mechanism is to accommodate on-demand creation of inter-area and inter-domain relationships. This task involves the dynamic establishment of SGs.

3.1 Intra-SG Auto-configuration Service

The new server must be able to select a set of DCSs to connect to within an existing SG. The number of connection links in the group determines both the amount of traffic exchanged and the reliability of the communications. By minimizing the number of links we can reduce the amount of messages needed to propagate updates, but the reliability of the group is negatively affected. Weakly connected groups are more vulnerable to node failures since they can easily lead to the disconnection of the group because not alternative paths can be found. The internal topology of a SG can be represented as an undirected graph, which is a simple diagram consisting of points (vertices = SCSP servers) connected by lines (edges = connection between peers). To ensure the replication of information, it must be guaranteed that the graph is connected with at least one path between every pair of vertices. The topology, i.e. number of elements and how are they connected, affects replication performance and consistency determining the information flow within the group. Every topology can be considered as a composition of two basic models: star and inline. The star topology performs well for low update rates, since messages have to traverse fewer hops to reach their destinations. Inline topology is more suitable for systems with heavier update rates.

3.1.1 Neighbour Discovery Phase

The intra-SG auto-configuration procedure begins with an un-configured SCSP server with transport level connectivity but without any configuration information. In the Neighbour Discovery phase, the node starts sending Neighbour Discovery messages encapsulated in transport level multicast packets to the SCSP auto-configuration multicast address. All those servers that belong to the SG that the un-configured server wants to join must reply with a Neighbour Response message. This message contains the configuration information of the corresponding remote server. Upon receiving those packets from every node in the SG, the un-configured server can gather enough information to run the decision process and choose a set of servers to connect. The un-configured node receives both the identities of the servers in the SG and the relationships between them. Therefore, the Neighbour Response message provides an open way to exchange information about the SG members and the SG topology. It provides to the new server a "picture" of the SG topology. Afterwards, the criteria to select the peers during the decision process are system-dependent based on the architecture requirements. The proposed configurable mechanism can be easily adapted to the system requirements. The Neighbour Response message can be customised to carry different information about the remote servers. The decision function utilises the information received in the Neighbour Response messages to calculate a priority for every remote server present in the SG. The operations used to process the received parameters depend on the function itself, which is also system dependent providing great flexibility to the configuration module.

3.1.2 SG connectivity Calculation

In the decision process the un-configured server assigns a priority to every remote server and calculates the number of DCSs to connect based on the SG connectivity. The SG had k -connected before adding the new server to the SG, so it must be ensured that at least the same connectivity value remains after including the new node to the SG. It has been developed a function that calculates the SG connectivity using graph theory algorithms using the topological information received in the Neighbour Response messages. For k -connected SG, the un-configured server must establish connections with at least k neighbours to maintain the same reliability. The selection of those k servers is based on the priorities assigned by the decision function. Figure 4 shows the auto-configuration procedure.

Figure 4. Neighbour Discovery process with SCSP Hello Messages including authentication

3.2 Inter-SG Auto-configuration Service

This service automatically creates new SGs to interconnect existing SGs. It can be used in two different contexts: inter-area and inter-domain. In the former, an operator owns an ITAD, which is divided into different areas and the information exchange between areas requires the establishment of inter-area SGs. In inter-domain case, there are two or more ITADs belonging to different operators and the information exchange between operators is done by means of inter-domain SGs.

3.2.1 Gateway Discovery Phase

The SCSP server that triggers the inter-SG procedure acts as a master server, and is responsible for finding the remote servers belonging to the SGs that will participate in the new SG. Those servers will act as "gateways" between different SGs. The master server sends Gateway Discovery messages to SCSP multicast address. These messages contain the identifiers of the SGs involved in the procedure. The remote servers belonging to any of the SG identifiers carried by the GW Discovery message must process the message and send back responses that are collected by the master server.

3.2.2 Decision Process and SG Identifier Selection

The inter-SG auto-configuration service can be customised to match the requirements of different architectures. The Gateway Response open message is used to inform the master server about gateway features.

Afterwards, the master server runs its decision function in order to compute a priority for every remote gateway. This function use the information received in the Gateway Response messages and it is completely system-dependent, meaning that must be configured considering the system requirements. The master server calculates the priorities for the remote gateways, decides which servers will take part in the new SG and establishes new connections with them. In this process the master server has to select a SG identifier for the new SG. SCSP reserves 16 bits to store SG identifiers bringing up to a maximum of 65.536 different SGs in a system. The SG identifiers can not be reused thus the master server should select a free one for the new SG. The proposed solution is to divide the total range of identifiers into two groups. The first one encompasses identifiers 0-59.999 that are reserved for conventional SGs. The second group will use identifiers 60.000-65.535 that are reserved for inter-area and inter-domain SGs.

3.3 Definition of Profiles for the Auto-configuration Module

The proposed auto-configuration module provides SCSP based architectures with an open and customisable auto-configuration mechanism. Nevertheless, the module has to be completed with an auto-configuration profile that indicates how to define the priorities calculated, and how those values are processed by the decision functions. Thus, every SCSP based system has to define its own profile considering the requirements of the architecture and the nature of the replicated information. This nature determines the update rates that will be sent to the SCSP layer.

3.4 Auto-recovery Service for Network Load Optimisation

This section presents an enhancement to the proposed auto-configuration mechanism for SCSP based systems focusing in load optimisation. The described intra-SG and inter-SG services consider the use of the k-connectivity factor of the SG to guarantee the graph connectivity. This approach introduces certain redundancy because of the multiple paths between servers within the SG. The k-connectivity tolerates failures without any dynamic topology reconfiguration, but it means that the same information is sent through different paths producing extra network load.

Therefore, a system with 1-connected graph is the optimum in terms of network load. The drawback is that these kinds of graphs can be disconnected with a single node failure. Thus, it is necessary to provide an auto-recovery mechanism to ensure that replication within the SG keeps working. The auto-recovery procedure detects the failure of a node and

automatically reconfigures the SG topology to ensure that the corresponding graph remains connected. This is achieved by establishing new temporary connections between servers. Once the server that failed is recovered, the temporary relationships are removed and the topology of the SG returns to its original state. The auto-recovery procedure involves three tasks.

The Failure detection performed by the Hello Finite State Machine (HFSM) of the SCSP that is monitoring the state of the connection between the LS and the DCS. **The auto-recovery function** is run when the server detects a failure in the SG. The set of actions to be taken depends on the base topology being used (inline or star) and the position occupied by the server that breaks down. **The Maintenance of up-to-date topology** performed by every server located within the SG. The distribution of reliable topology information in the system is crucial for the correct operation of the auto-recovery procedure. The actions taken by servers when a failure occurs will be based on this information, so it must be accurate and consistent.

4. CONCLUSIONS

This paper presents the suitable architecture to achieve a fully IP-switched networks converge for providing IP Telephony service. A TRIP and SCSP prototype was implemented for deploying a test bed. The initial prototype [7] has been enhanced with security and auto-configuration modules and the design and test results of those modules are evaluated. Therefore, we can point out that the TRIP specifications can easily be extended with security and auto-configuration modules to achieve an optimal and scalable architecture.

REFERENCES

- [1] 3rd Generation Partnership Project, 3GPP. www.3gpp.org.
- [2] M. Handley, H. Schulzrinne, E. Schroeder, J. Rosenberg. "Session Initiation Protocol", RFC 2543, IETF.
- [3] Rosenberg, J., Salama, H. and Squire, M. "Telephony Routing over IP (TRIP)". Internet draft, IETF, August 2001.
- [4] Rosenberg, J., Schulzrinne, H. "A Framework for Telephony Routing over IP". RFC 2871, IETF, June 2000.
- [5] Costa-Requena J., Kantola R., Beijar N. "A Common Numbering Infrastructure for IN and IP Telephony", presented at IN2000, Cape Town, South Africa, May 2000.
- [6] Luciani, J., Armitage, G., Halpern, J., Doraswamy, N. "Server Cache Synchronization Protocol (SCSP)". RFC 2334, IETF, April 1998.
- [7] Kantola R., Costa-Requena J., Beijar N. "An Architecture for an SCN/IP Telephony Routing Testbed". The first IP. Telephony Workshop, Berlin, Germany, April 2000.
- [8] Gonzalez Olias, I. " Security and auto-configuration of Location Servers for IP Telephony". Helsinki University of Technology, Networking Laboratory, 2002.