Network Working Group
Request for Comments: 2995
Category: Informational

H. Lu, Editor
I. Faynberg
J. Voelker
M. Weissman
W. Zhang
Lucent Technologies
S. Rhim
J. Hwang
Korea Telecom
S. Ago
S. Moeenuddin
S. Hadvani
NEC
S. Nyckelgard
Telia
J. Yoakum
L. Robart
Nortel Networks

November 2000

Pre-SPIRITS Implementations of PSTN-initiated Services

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document contains information relevant to the work underway in The Services in the PSTN/IN Requesting InTernet Services (SPIRITS) Working Group. It describes four existing implementations of SPIRITS-like services from Korea Telecom, Lucent Technologies, NEC, and Telia in cooperation with Nortel Networks. SPIRITS-like services are those originating in the Public Switched Telephone Network (PSTN) and necessitating the interactions of the Internet and PSTN.

Surveying the implementations, we can make the following observations:

- The ICW service plays the role of a benchmark service. All four implementations can support ICW, with three specifically designed for it.

- Session Initiation Protocol (SIP) is used in most of the implementations as the base communications protocol between the PSTN and Internet. (NEC's implementation is the only exception that uses a proprietary protocol. Nevertheless, NEC has a plan to support SIP together with the extensions for SPIRITS services.)

- All implementations use IN-based solutions for the PSTN part.

It is clear that not all pre-SPIRITS implementations inter-operate with each other. It is also clear that not all SIP-based implementations inter-operate with each other given that they do not support the same version of SIP. It is a task of the SPIRITS Working Group to define the inter-networking interfaces that will support interoperation of the future implementations of SPIRITS services.

Table of Contents

1. Introduction

This document contains information relevant to the work underway in The Services in the PSTN/IN Requesting InTernet Services (SPIRITS) Working Group. It describes four existing implementations of SPIRITS-like services from Korea Telecom, Lucent Technologies, NEC, and Telia in cooperation with Nortel Networks. SPIRITS-like services are those originating in the Public Switched Telephone Network (PSTN) and necessitating the interactions of the Internet and PSTN.

Invariably supported by the implementations examined in this document is the Internet Call Waiting (ICW) service. With ICW, service subscribers, while using their telephone lines for Internet access, can be notified of incoming voice calls and specify how to handle the calls over the same telephone lines.

The document first gives a detailed description of the ICW service. Then it proceeds to discuss each of the four implementations. The final sections of the document contains security considerations, the conclusion and references.

It is important to note that even though the term "SPIRITS server" is used throughout the document, it has no universal meaning. Its connotation depends on the context and varies from implementation to implementation.

2. Service Description of Internet Call Waiting

Internet call waiting is the single service that is specifically supported by all the implementations in question. In a nutshell, the service enables a subscriber engaged in an Internet dial-up session to

- be notified of an incoming call to the very same telephone line that is being used for the Internet connection;
- specify the desirable treatment of the call; and
- have the call handled as specified.

The details of the ICW service lie in the ways that a waiting call can be treated, which vary from implementation to implementation. In this section, we describe the features that are supported by at least one of the implementations. They are as follows:

- Incoming Call Notification - The subscriber is notified of an incoming call over the Internet, without having any effect on the telephone line that is being used by the modem. When a call comes in, the subscriber is presented with a pop-up dialog box on the PC. The dialog box may display any combination of the calling party number, calling party name, and calling time. Note that the display of the calling party name (or number) requires the availability of the caller name (or number) delivery feature.
- Online Incoming Call Disposition - Once informed of the incoming call, the subscriber has various options (indicated in the pop-up window) for handling the call. Possible options are:
  + Accepting the call over the PSTN line, thus terminating the Internet (modem) connection
  + Accepting the call over the Internet using Voice over IP (VoIP)
  + Rejecting the call

  + Playing a pre-recorded message to the calling party and disconnecting the call

  + Forwarding the call to voice mail

  + Forwarding the call to another number

  + Rejecting (or Forwarding) on no Response - If the subscriber fails to respond within a certain period time after the dialog box has been displayed, the incoming call can be either rejected or handled based on the treatment pre-defined by the subscriber.

- Automatic Incoming Call Disposition - Incoming calls are automatically handled based on dispositions pre-defined by the subscriber without his or her real-time intervention. The subscriber can pre-define the default disposition (e.g., re-directed to voice mail) for general calls as well as customized dispositions for calls from specific numbers. In the latter case, the subscriber selects a particular disposition for each originating number and stores this information in a profile. When a call comes in, the subscriber won't be presented the call but can examine the treatment and outcome of the call from the caller log (as described in the call logging bullet). Naturally, this feature also allows the subscriber to specify the desired treatment for calls originating from private or unpublished numbers.

- Multiple Call Handling - Multiple calls can arrive during call disposition processing. With multiple call handling, the subscriber is notified of the multiple calls one by one.

- Call Logging - A detailed log of the incoming calls processed during the ICW service is kept. Typical information recorded in the log include the incoming call date and time, calling party number, calling party name, and call disposition.

3. Korea Telecom's ICW Implementation

3.1. Overview

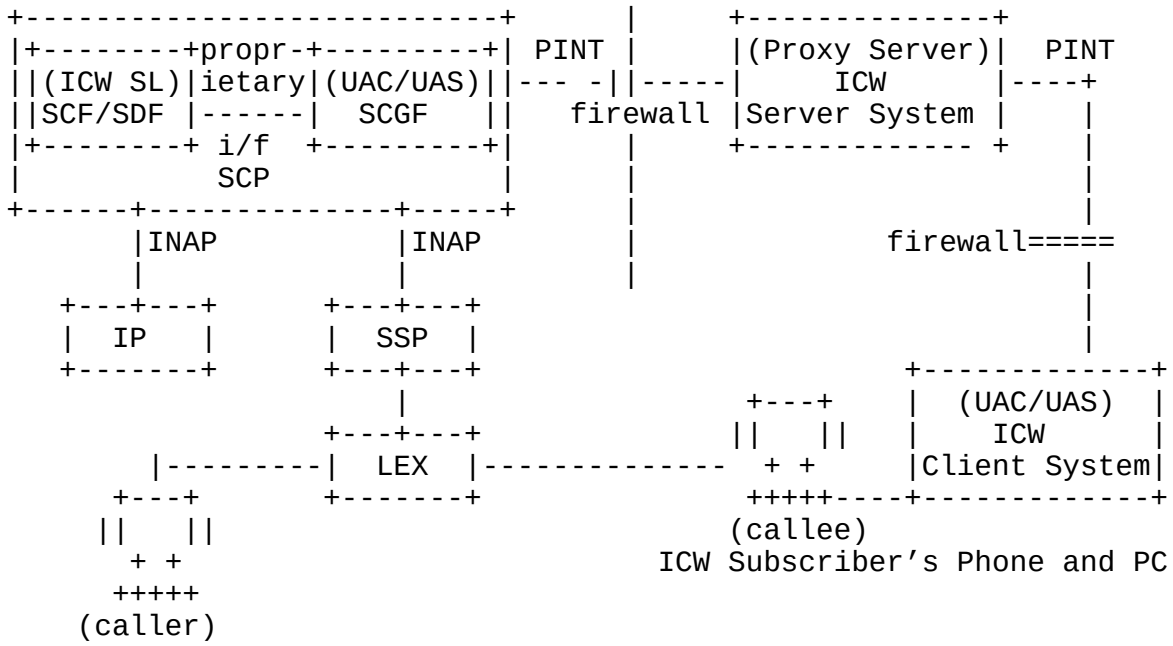
Korea Telecom's ICW implementation supports most of the features described in Section 2. (The major exception is the feature of receiving the incoming call over the Internet using voice over IP.) In addition, the Korea Telecom implementation supports flexible activation and de-activation of the ICW service:

- Automatic Activation/De-activation - When Internet dial-up connection is set up, the ICW service is activated or de-activated automatically.

- Manual Activation/De-activation - The subscriber can de-activate the ICW service manually when call notification is not desired during the Internet dial-up session and activate it when needed.

3.2. Network Architecture

Figure 1 depicts the network architecture of the Korea Telecom ICW service. The Service Switching Point (SSP), Service Control Point (SCP), and Intelligent Peripheral (IP) are legacy PSTN IN elements based on IN CS-1. In contrast, both the ICW Server System and the ICW Client System are new network elements that are installed in the Internet domain to support of the ICW service.



INAP : Intelligent Network Application Protocol
PINT : PSTN/Internet Interworking Protocol
SL : Service Logic
UAS : User Agent Server
UAC : User Agent Client

Figure 1: Network Architecture of the Korea Telecom ICW Service

3.3. Network Entities

3.3.1. SSP

The SSP performs the Service Switching Function (SSF) and Call Control Function (CCF). When detecting that the called party is busy (T_Busy), the SSP sends a query to the SCP and processes the call under the control of the SCP.

3.3.2. SCP

The SCP performs the Service Control Function (SCF) and Service Data Function (SDF). It, when queried, instructs the SSP to process the call based on the service logic. In the case of the ICW service, the service logic ultimately governs the notification of a waiting call to an online ICW subscriber and the disposition of the call. In addition, the SCP performs the Service Control Gateway Function (SCGF) for protocol inter-working between the PSTN/IN and Internet. It translates the SIP message from the ICW Server to the service control interface message and vise versa. The SCGF is an IP end point and behaves as a UAS (User Agent server) or UAC (User Agent client).

3.3.3. IP

The IP contains Service Resource Function (SRF). It, when necessary, plays announcements to the calling party during the ICW service before/after receiving the response from the ICW subscriber and records the calling party number or voice message from the calling party when the call is forwarded to the Voice Mail System (VMS).

3.3.4. ICW Server System

The ICW Server system serves as a SIP proxy or a redirect server for message routing between the ICW Client and SCGF. The ICW Server is also responsible for managing the ICW Clients that are connected to it. When an ICW Client (subscriber) sends a registration request for the ICW service, the ICW Server relays that request to the SCP, waits for the result of authorization from the SCP, and registers the authorized subscriber in its data base. In addition, the ICW Server monitors the connection status of the registered ICW Clients. As soon as a client deactivates the ICW service or terminates the Internet connection, the ICW Server detects the status change and deactivates the ICW service for the client. Finally, the ICW Server manages profiles for each ICW subscribers as well as logs all the call processing results.

3.3.5. ICW Client System

The ICW Client System is an application program running on the subscriber's PC. Launched as soon as the subscriber powers on the PC, it monitors the Internet connection status of the PC (or subscriber). Upon the subscriber's connection to the Internet, the ICW Client sends a REGISTRATION request to the SCGF via the ICW Server and then eventually to the SCP. In this capacity, the ICW Client acts as a UAC to the SCGF, which acts as a UAS. Thereafter it notifies the ICW Server periodically of the connection status of the subscriber.

The ICW Client is also responsible for popping up a dialog box on the subscriber's PC to announce an incoming call. The dialog box displays the number and name of calling party, calling time, and the call processing options (including Accept, Reject, Forward to another number or VMS). After the subscriber selects the option, the ICW Client sends it to the SCP. In this capacity, the ICW Client acts as a UAS.

Depending on the pre-defined ICW Service Profile, the ICW Client may screen the incoming call before notifying the subscriber.

The ICW Client manages the ICW Service Profile, which contains the following fields:

- Subscriber Information (including, Name, Directory Number, Password)

- Service Status (Activation/De-activation)

- Automatic Call Processing Method

  + Call Processing Method on No Answer (Reject/Forward/VMS) - The call is automatically handled by the method if the subscriber doesn't respond after a pre-defined period of time.

  + Do Not Disturb Mode (On/Off) - When this is set on, the subscriber won't be notified of the incoming calls.

  + Call Processing Method on Do Not Disturb (Reject/Forward/VMS)

  + Call Processing List by Calling Party Numbers (Accept/Reject/Forward/VMS) - Calls originated from a number on the list are handled by the associated call processing method.

- The ICW Client records the call processing method and the result for each incoming call in a log file on the subscriber's PC. The

call record in the call log contains the following information:

- Calling Time
- Calling Party Number
- Calling Party Name (optional)
- Call Processing Method (Accept/Reject/Forward/Forward to VMS)
- Result (Success/Fail)

3.3.6. Firewall

Packet Filtering Firewall Systems are between the ICW server and clients as well as between the SCGF and ICW server for accessing the Korea Telecom IN Nodes.

3.4. Network Interfaces

- o The SCF-SDF, SCF-SSF, and SCF-SRF interfaces are the same as existing PSTN IN Interfaces based on the KT INAP CS-1.

- o The SCGF-SCF interface relays requests either from the IN or the Internet and is implemented based on the internal API of the SCP.

- o The SCGF-ICW Server and ICW Server-ICW Client interfaces are implemented based on the PINT Service Protocol V.1. We adopted UAS-Proxy-UAC relationships as shown in Figure 2.

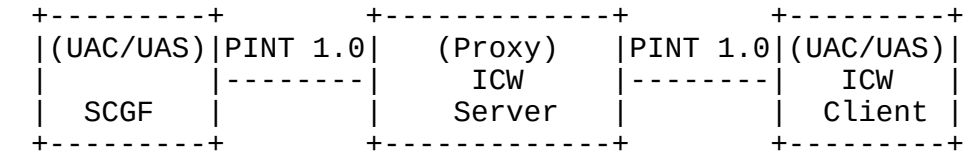


Figure 2: PINT Protocol Architecture

3.5. Protocols

3.5.1. Intelligent Network Application Part Protocol (INAP)

The SCP, SSP, and IP support the KT INAP V1.0, which is based on ITU-T INAP CS-1 with the incorporation of two INAP CS-2 messages [PRM (PromptAndReceiveMessage) and EM (EraseMessage)] for recording the voice message.

3.5.2. PINT Protocol

The ICW service uses the PINT Service Protocol 1.0 [1] for communications between the SCP and the ICW Server System, and between the ICW Server System and the ICW Client System. Developed in the

IETF PINT Working Group for invoking telephone services from an IP network, the PINT Service Protocol 1.0 specifies a set of enhancements to SIP 2.0 and SDP.

Summarized below are the elements of the PINT Service Protocol 1.0 relevant to the Korea Telecom ICW implementation:

- o REGISTER

  The REGISTER method is used to inform the SCP of the connection status of an ICW subscriber. With this method, the ICW Client sends to the ICW Server the IP address (of the PC) and phone number of the subscriber when the subscriber is first connected to the Internet. The ICW server relays the information to the SCP, which updates the data base (if the subscriber is authorized), and in the end sends a registration acknowledgment to the ICW Server and then the Client. After the subscriber is connected to the Internet, the ICW Client sends a REGISTER request to the ICW Server periodically at a pre-defined interval (e.g., 20 seconds) to indicate its connection status. The request is not relayed to the SCP. The ICW Server only checks if it is from the authorized subscriber. Finally, when the subscriber terminates the Internet connection, the Client sends the last REGISTER request to the SCP via the ICW Server. If the REGISTER request does not arrive during the pre-defined interval, the ICW Server can also detect the change of the connection status of the ICW Client.

- o INVITE

  The SCP uses the INVITE method to notify the ICW Client, via the ICW Server, of an incoming call.

- o ACK

  Both the SCP and the ICW Server use the ACK method to confirm the receipt of the final responses to their requests.

- o BYE

  The BYE method terminates a service session. In addition to this original usage, we use the value (success or failure) of the Subject header to indicate the result of the desired disposition of an incoming call in the PSTN.

o CANCEL

When the calling party releases the call before the called party responds, the SCP sends a CANCEL request to the ICW Client to cancel the INVITE request that it sent previously.

o OPTION

This method is not used in the KT implementation.

o Responses

The SCP responds to a REGISTER request with one of the status codes and associated comments below:

. 100 Trying: Trying
. 200 OK: Registered

The ICW Client responds to an INVITE request with one of the status codes and associated comments below:

. 100 Trying: Trying
. 200 OK: Accept the Call
. 303 see other: Forward the Call to Another Number
. 380 alternative service: Forward the Call to the VMS
. 603 decline: Reject the Call

3.6. Example Scenarios

3.6.1. ICW Service Subscription

Access to the Korea Telecom ICW service is by subscription. Here Korea Telecom serves as both the PSTN operator and IN-based ICW service provider. Note that the subscription data need to be loaded onto the relevant SSPs, including the local ones that may not be operated by Korea Telecom.

3.6.2. ICW Client Installation

An ICW subscriber should install the ICW Client program in his or her PC. The ICW Client is automatically activated to run as a daemon process when the subscriber’s PC is turned on. The Client monitors the Internet connection status of the subscriber.

3.6.3. ICW Service Activation

When the subscriber initiates the Internet connection or activates the ICW service manually, the ICW service is activated. That is done by sending a REGISTER request with the directory number and IP address from the ICW Client to the SCP through the ICW Server.

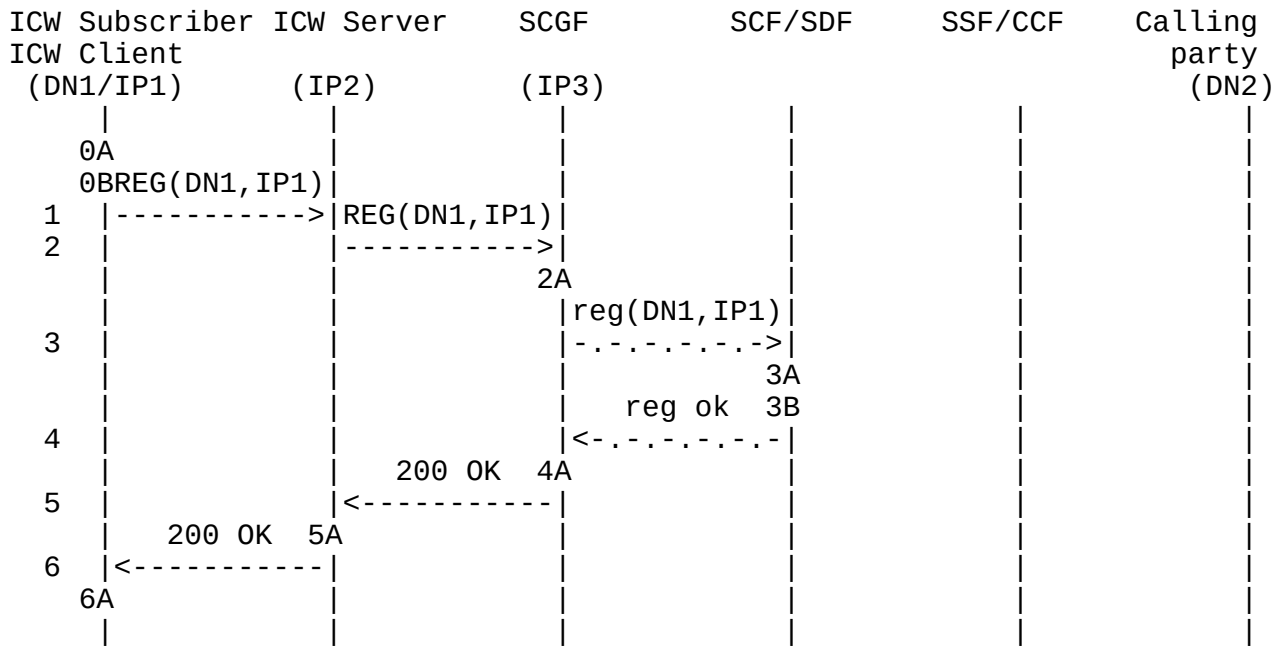


Figure 3: ICW Service Activation

As depicted in Figure 3, the relevant information flows are as follows:

(0A) The ICW subscriber dials the ISP access number and establishes a PPP connection.

(0B) The ICW Client detects the PPP connection.

1. The ICW Client sends a registration request to the ICW Server in order to register the IP address-DN relationship for the dial-up connection.

2. The ICW Server relays registration request to the SCGF.

2A. The SCGF translates the user registration information from the SIP message to the SCP internal API message.

3. The SCGF relays the user registration message to the SCF/SDF.

3A. The SCF/SDF authorizes the subscriber with the directory number based on the user registration information.

3B. The SCF/SDF stores the IP address of the ICW Client and sets the status to "Internet on-line."

4. The SCF/SDF sends the result of registration to the SCF/SCGF.

4A. The SCGF translates the user registration response of the SCP internal API message to the PINT message.

5. The SCGF relays the user registration response to the ICW Server.

5A. The ICW Server records the user registration information and the Internet on-line status for the subscriber in the data base.

6. The ICW Server sends the user registration response to the ICW Client.

6A. The ICW Client notifies the subscriber that the registration is completed successfully and the ICW service is in the active state.

3.5.4. Incoming Call Notification

When a calling party makes a call to the ICW subscriber, the SCP notifies the ICW Client of the incoming call and waits for the subscriber's response.

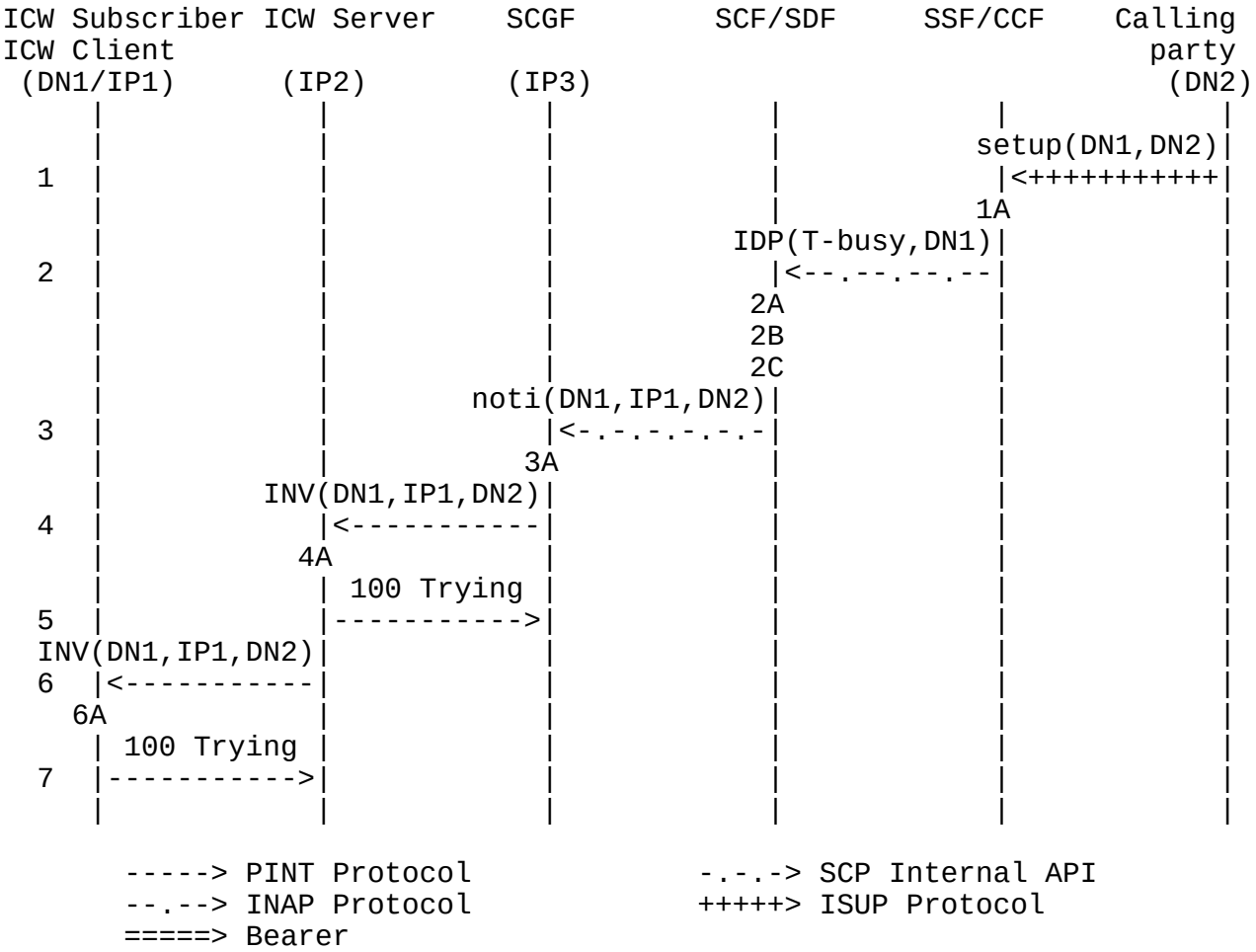


Figure 4: Incoming Call Notification

As depicted in Figure 4, the relevant information flows are as follows:

1. The calling party at DN2 (a telephone user) makes a call to the ICW subscriber (PC user) at DN1. The connection is set up using the existing ISDN signaling.

1A. The SSF/CCF detects that the callee (the ICW subscriber) is busy.

2. The SSF/CCF sends InitialDP (T_Busy) to the SCF/SDF.

2A. The SCF/SDF determines whether the user at DN1 is PSTN on-line or Internet on-line. (The SCF/SDF executes the KT Telephone Mail Service logic in the PSTN on-line case and the ICW service Logic in the Internet on-line case.)

2B. The SCF/SDF retrieves the IP address corresponding to DN1.

2C. The SCF/SDF may play an announcement to the calling party, while waiting for the response of the called party.

3. The SCF sends an incoming call notification to the SCGF.

3A. The SCGF translates the incoming call notification from the SCP internal format to the PINT format.

4. The SCGF relays the notification to the ICW Server.

4A. The ICW Server double-checks the subscriber’s status using the ICW subscribers profile in its own data base.

5. The ICW Server sends trying message to the SCGF.

6. The ICW Server relays the notification to the ICW Client.

6A. The ICW Client consults the ICW service profile to see if there is a pre-defined call disposition for the incoming call. If so, then the procedure for automatic call processing is performed.

6B. If there is no pre-defined call disposition for the incoming call, the subscriber is notified of the call via a pop-up dialog box.

7. The ICW Client sends trying message to the ICW Server.

3.6.5. Incoming Call Processing

The incoming call can be accepted, rejected, forwarded to another number, or forwarded to the VMS depending on the on-the-fly or pre-defined choice of the subscriber. This section describes the information flows for the cases of "Accept the call" and "Forward the call to another number."

3.5.5.1. Accept the Call

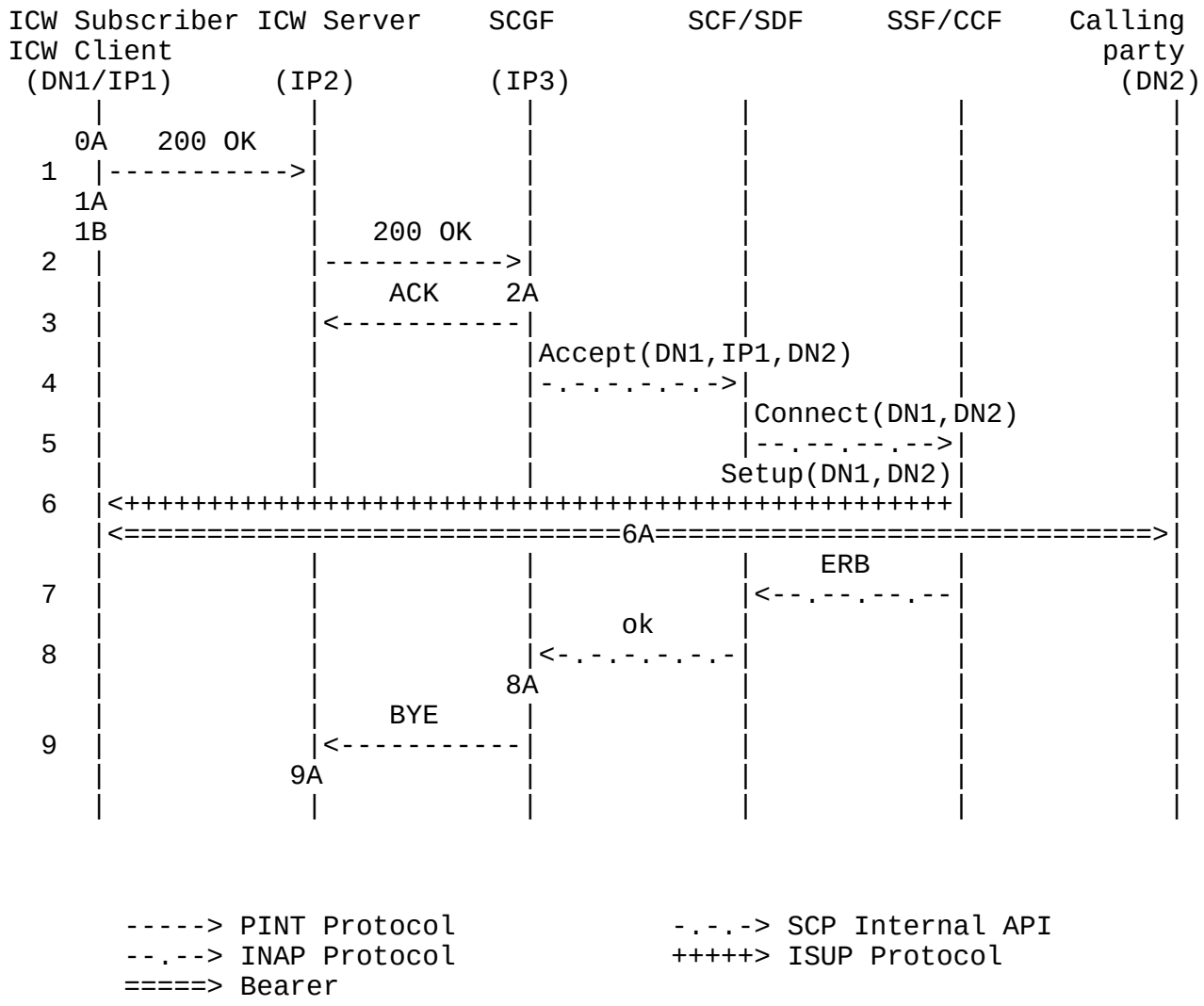


Figure 5: Incoming Call Processing - Accept the Call

As depicted in Figure 5, the relevant information flows are as follows:

0A. The ICW subscriber chooses to "Accept" the incoming call.

1. The ICW Client sends the "Accept" indication to the ICW Server.

1A. The ICW Client records the subscriber’s selection for the incoming call in the call log.

1B. The ICW Client terminates the subscriber’s Internet connection.

2. The ICW Server sends an "Accept" message to the SCGF.

2A. The SCGF translates the "Accept" message to an SCP internal API message.

3. The SCGF sends an "ACK" message to the ICW Server.

4. The SCGF sends the "Accept" message to the SCF.

5. The SCF instructs the SSF/CCF to route the call to DN1.

6. The SSF/CCF initiates the connection setup to DN1.

6A. The bearer connection between the calling party (DN2) and the ICW subscriber(DN1) is set up.

7. The connection result is returned to the SCF through ERB.

8. The SCF sends a call completion message to the SCGF.

8A. The SCGF translates the call completion message to a PINT message.

9. The SCGF sends a "BYE" message to the ICW Server.

9A. The ICW Server records the call completion result in the log file.

3.5.5.2. Forward the Call to Another Number

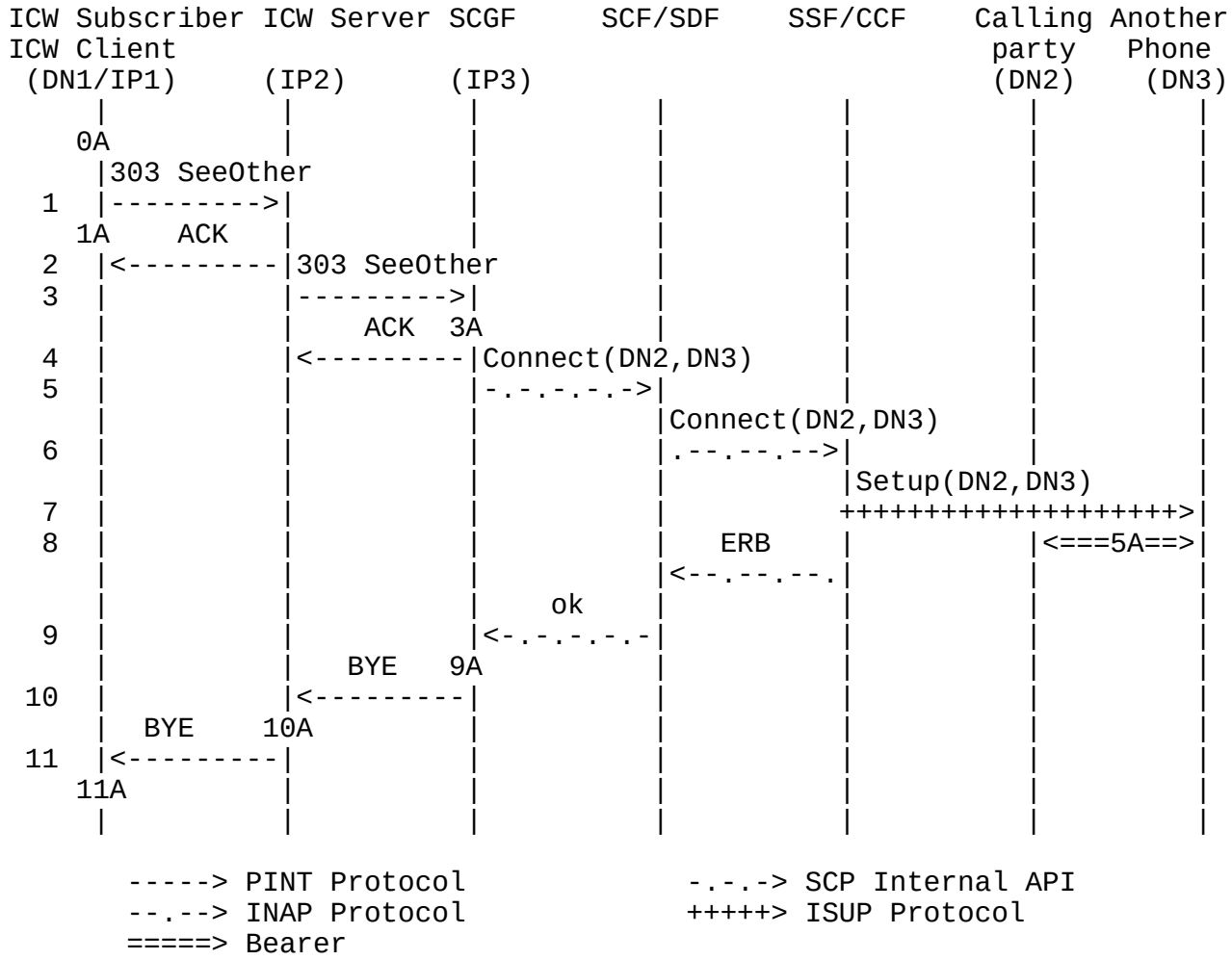


Figure 6: Incoming Call Processing - Forward the Call to Another

As depicted in Figure 6, the relevant information flows are as follows:

0A. The ICW subscriber chooses to "Forward to another number (DN3)" for the incoming call.

1. The ICW Client sends the "Forward to another number" indication to the ICW Server.

1A. The ICW Client records the subscriber’s selection for the incoming call in the call log.

2. The ICW Server sends an "ACK" message to the ICW Client.

3. The ICW Server relays the "Forward to another number" message to the SCGF.

3A. The SCGF translates the "Forward to another number" message to an SCP internal API message.

4. The SCGF sends an "ACK" message to the ICW Server.

5. The SCGF sends the "Forward to another number" message to the SCF.

6. The SCF instructs the SSF/CCF to route the call to DN3.

7. The SSF/CCF initiates the connection setup to DN3.

7A. The bearer connection between the calling party (DN2) and the new termination number (DN3) is set up.

8. The connection result is returned to the SCF through ERB.

9. The SCF sends a call completion message to the SCGF.

9A. The SCGF translates the call completion message to a PINT message.

10. The SCGF sends the call completion message to the ICW Server.

10A. The ICW Server records the call completion result in the log file.

11. The ICW Server sends the success of "Forwarding to another number" to the ICW Client.

11A. The ICW Client records the call completion result in the log file.

3.6.6. ICW service De-activation

The SCP de-activates the ICW service for a subscriber either upon the termination of the subscriber's Internet connection or upon the subscriber's manual request. In this section, we illustrate the former scenario.

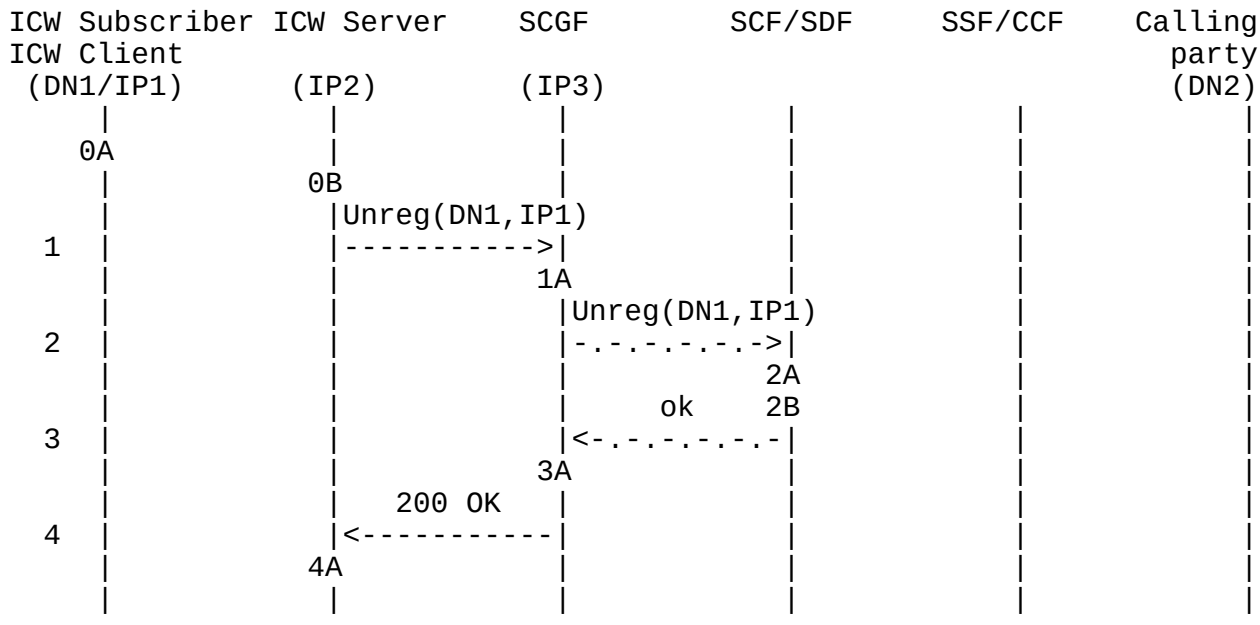


Figure 7: ICW Service De-activation

As depicted in Figure 7, the relevant information flows are as follows:

0A. The ICW subscriber terminates the Internet connection.

0B. The ICW Server determines that the Internet connection has been terminated when it does not receive the periodic on-line notification from the ICW Client.

1. The ICW Server sends an un-register message to the SCGF.

1A. The SCGF translates the un-register message to an SCP internal API message.

2. The SCGF sends the un-register message to the SCF.

2A. The SCF/SDF authorizes the subscriber with the directory number based on the un-registration information.

2B. The SCF/SDF records the Internet off-line status for that ICW Client.

3. The SCF/SDF sends a user un-registration response to the SCF/SCGF.

3B. The SCGF translates the user un-registration response to a PINT message.

4. The SCGF relays the user un-registration response to the ICW Server.

4A. The ICW Server records the Internet off-line status for the ICW Client (subscriber) in the data base.

4. The Lucent Technologies Online Communications Center

4.1 Overview

The Lucent Technologies Online Communications Center (OCC) is an Intelligent Network (IN)-based platform that supports the Internet call waiting service. Its basic components are the OCC Server and OCC Client, which are described in detail in the Architecture section. The OCC Server interacts with the PSTN entities over the secure intranet via plain-text Session Initiation Protocol (SIP) messages [2]. With the PC Client, the OCC Server interacts via encrypted SIP messages.

The OCC Server run-time environment effectively consists of two multi-threaded processes responsible for Call Registration and Call Notification services, respectively.

OCC call registration services are initiated from an end-user’s PC (or Internet appliance). With those, a subscriber registers his or her end-points and activates the notification services. (The registration services are not, strictly speaking, SPIRITS services but rather have a flavor of PINT services.)

All OCC call notification services are PSTN-initiated. One common feature of these services is that of informing the user of the incoming telephone call via the Internet, without having any effect on the line already used by the modem. (A typical call waiting tone would interrupt the Internet connection, and it is a standard practice to disable the "old" PSTN call waiting service for the

duration of the call in support of the Internet connection between the end-user and the ISP.)

When a call comes in, the user is presented with a pop-up dialog box, which displays the caller's number (if available), name (again, if available), as well as the time of the call. If the called party does not initiate an action within a specified period of time the call is rejected.

As far as the disposition of the call is concerned, OCC supports all the features described in Section 2.

4.2. Architecture

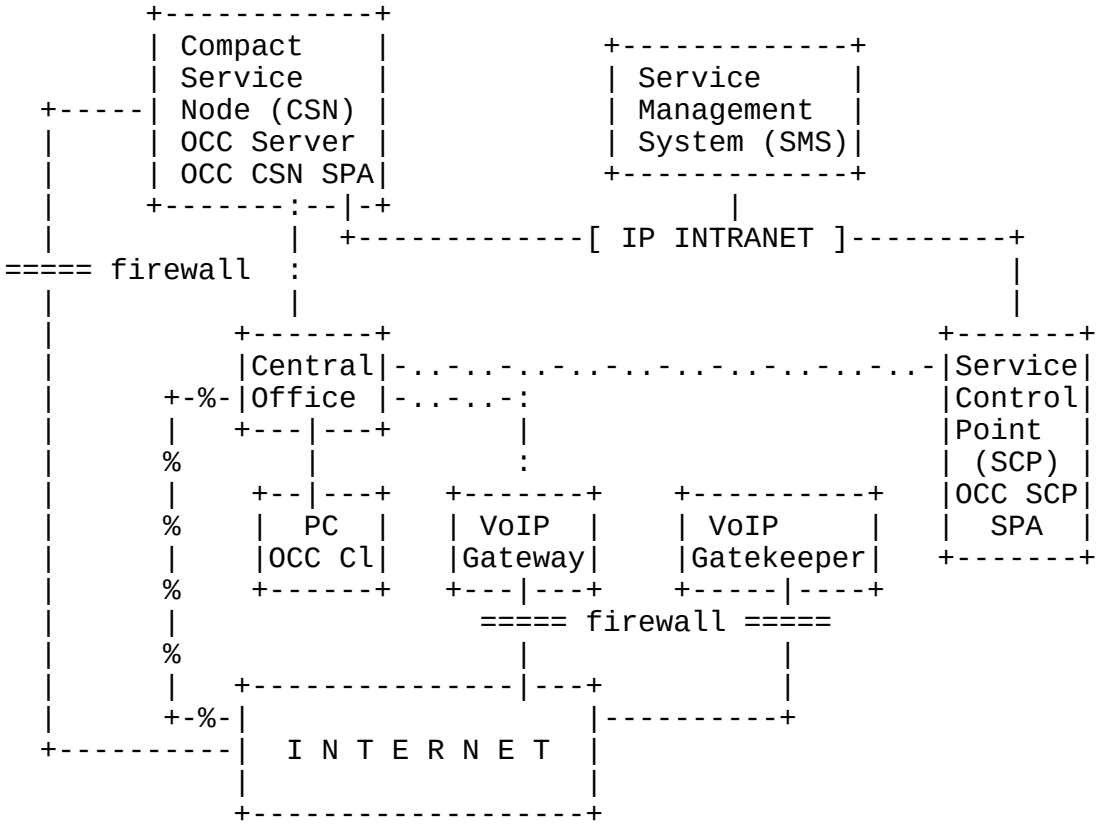
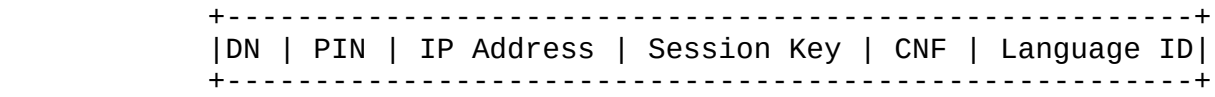


Figure 8: The Lucent OCC Physical Architecture

Figure 8 depicts the joint PSTN/Internet physical architecture relevant to the OCC operation. The Compact Service Node (CSN) and SCP are Lucent's implementations of the ITU-T IN Recommendations (in particular, the Recommendation Q.1205 where these entities are defined) augmented by the requirements of Bellcore's Advanced

Intelligent Network (AIN) Release 1.0) and equipped with other features. The Central Office (CO) may be any switch supporting the Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) and the call forwarding feature that would allow it to interwork with the CSN. Alternatively, in order to interwork with the SCP, it needs to be an IN Service Switching Point (SSP). In the latter case, the central office is connected to the SCP via the signaling system No. 7 (SS7) and INAP at the application layer.

The Service Management System (SMS) is responsible for provisioning of the SCPs, CSNs, and central offices. In particular, for IN support of the Internet Call Waiting, it must provision the Central Office to direct a terminating attempt query to the subsystem number corresponding to the OCC SCP SPA based on the Termination Attempt Trigger (TAT). In addition, the Subscriber Directory Number (DN), Personal Identification Number (PIN) and Language ID are provisioned for each subscriber into the OCC Subscriber entry of the SCP Real Time Data Base (RTDB). Figure 9 shows the structure of an RTDB entry.



Field Descriptions:

(DN) Directory Number - the subscriber’s telephone number

(PIN) Personal Identification Number - the subscriber’s password

IP Address - Internet Protocol Address of the subscriber

(CNF) Call Notification In Progress Flag (boolean) - the flag indicating if an attempt to notify the subscriber of a call is currently in progress

Session Key - unique identifier for the current registration session of the subscriber

Language ID - language identifier for the subscriber

Figure 9: Structure of the RTDB Subscriber Record

The Central Office, SMS, CSN, and SCP are the only PSTN elements of the architecture. The other elements are VoIP Gateway and Gatekeeper defined in the ITU-T Recommendation H.323, whose roles are to establish and provide the part of the voice path over IP. The Central Office is explicitly connected to the VoIP Gateway via the

ISDN PRI connection. In this architecture, CSN, VoIP Gateway, and VoIP Gatekeeper are the only entities connected to the Internet, with each respective connection protected by a firewall. The CSN and SCP are interconnected via a secure IP Intranet. There may be more than one CSN or SCP (or both) (and the SCPs come in mated pairs interconnected by X.25, anyway) in a network, but these details are not essential to the level of description chosen for this document. However, we note that load balancing and adaptation to failures by the use of alternative nodes is incorporated into the architecture.

When someone attempts to call the subscriber, the central office serving that subscriber interrupts normal termination processing and notifies the SCP which, in turn, can check whether that subscriber has registered that he (or she) is logged onto the Internet. Exploiting the standardized layering of service logic that characterizes the intelligent network, the central office will do this without requiring the installation or development of any central office software specific to OCC. The central office is simply provisioned to query the SCP when there is a termination attempt (i.e., TAT) directed to the subscriber’s directory number. (Note that the Central Office has no bearer circuit connection to the SCP, only a signaling one over SS7).

TCP/IP communication between the SCP and CSN utilizes a secure intranet. The subscriber, of course, is assumed to have access only to the Internet.

The intelligent network entities, the SCP and CSN, do have OCC related software. The OCC server is implemented on the CSN. In addition, one service package application (SPA) is installed on the SCP. Another SPA is located in the CSN and is needed only when the subscriber elects to accept an incoming call using voice over IP.

The OCC Server is a collection of Java servers on the CSN whose responsibilities include:

- Listening for incoming Call Notification (TCP/IP) messages from the SCP SPA.
- De-multiplexing/multiplexing incoming Call Notification messages sent from the SCP SPA.
- Relaying messages between the OCC Client and the SCP SPA.
- Listening for and authentication of OCC Client requests for service registration.

- Handling encryption/decryption of messages exchanged with the OCC Client, and generating session-specific encryption/decryption keys.

The OCC Client is a collection of software components that run on the Subscriber's PC. Its components include the SIP User Agent Server (which handles the exchange of SIP messages with the OCC Server and invokes the Call Notification pop-up window) and a daemon process that monitors the Point-to-Point Protocol (PPP) actions and is responsible for starting and stopping the SIP User Agent Server.

4.3. Protocol and Operations Considerations

The OCC Server uses distinct TCP/IP ports configured on the CSN to

- Listen for incoming SIP REGISTER messages (in support of registration service) sent from the OCC Client.

- Listen for incoming SIP INVITE messages (in support of call notification service) sent from the SCP.

During call notification, the SCP SPA is the client and thus is started after the OCC Server has been started. The SCP SPA and OCC Server exchange SIP messages over TCP/IP (via the Secure Intranet) using a "nailed-up" connection which is initiated by the SCP SPA. This connection is initiated at the time the SCP SPA receives the very first SIP REGISTER request from the OCC Server, and must prevail for as long as the SPA is in the in-service state. The SCP SPA also supports restarting the connection after any failure condition.

The OCC Server supports multithreading. For each Call Notification/Call Disposition event, a separate thread is used to handle the call. This model supports multi-threading on a "per message" basis where every start message (SIP INVITE) received from the SCP SPA uses a separate thread of control to handle the call. Subsequent messages containing the same session Call-ID (which includes the SPA's instance known as "call_index" and the SCP hostname) as the original start message is routed to the same thread that previously handled the respective initiating message.

The OCC Server dynamically opens a new TCP/IP socket with the OCC Client for each Call Notification/Call Disposition session. This socket connection uses the IP address and a pre-configured port on the PC running the OCC Client software.

For session registration, the OCC Server dynamically opens TCP/IP sessions with the SCP SPA. The SCP SPA listens at a pre-configured port to incoming SIP REGISTER messages sent by OCC Clients via the

OCC Server. To exchange SIP messages with the OCC Server, the OCC Client dynamically opens a TCP/IP socket connection with the OCC Server using a pre-configured port number on the CSN and the CSN's IP address.

For the VoIP Scenario, the CSN SPA, acting as a client, dynamically opens TCP/IP sessions with the SCP that handled the initial TAT query. As soon as the CSN SPA has successfully made the correlation and connected the two incoming call legs pertaining to a VoIP call back, the SIP 180 RINGING message will be sent back to the SCP SPA running on the actual SCP that instructed the SSP to forward the Caller to the CSN. This SIP message, which contains the VoIP Call Back DN dialed by one of the bridged call legs, is an indication to the SCP SPA that the VoIP Call Back DN is freed up.

A typical subscription scenario works like as follows:

1. Each VoIP Gateway is provisioned with a list of authorized VoIP Call Back DNs, each terminating on a particular CSN. These special DNs are used when an on-line subscriber elects to receive an incoming call via VoIP. In particular, they assist in routing an outgoing call from the subscriber's NetMeeting to the particular CSN to which the SCP is (roughly concurrently) forwarding the incoming call. (These two calls are joined in the CSN to connect the incoming call to the subscriber's Netmeeting client.) Furthermore, these special DNs permits that CSN to associate, and hence bridge, the correct pair of call legs to join the party calling the subscriber to the call from the subscriber's NetMeeting client.

2. The subscriber calls a PSTN service provider and signs up for the service.

3. An active Terminating Attempt Trigger (TAT) is assigned to the subscriber's DN at the subscriber's central office.

4. The PSTN service provider uses the SMS to create a record for the subscriber and provision the Subscriber DN and PIN in the OCC RTDB table in the SCP.

5. The subscriber is provided with the OCC Client software, a PIN and a file containing the OCC Server IP Addresses.

Finally, we describe the particular scenario of the OCC Call Disposition that involves voice over IP, which proceeds as follows:

1. The OCC subscriber clicks on "Accept VoIP".

2. The OCC Client sends a "SIP 380 Alternative Service" message to the OCC Server. This message includes a reference to the Call Back DN which will ultimately be used by the CSN to associate the call leg (soon to be initiated by the subscriber's NetMeeting) connecting to the subscriber (via the VoIP gateway) with the PSTN call leg connecting to the calling party.

3. The OCC Server closes the TCP/IP session with the OCC Client and sends to the SCP SPA the "SIP 380 Alternative Service" message which includes the Call Back DN.

4. The SCP SPA instructs the Central Office to forward the call incoming to the subscriber to the CSN. This instruction includes the Call Back DN.

5. The SSP forwards the Caller to the CSN referencing the Call Back DN. Note that the Call Back DN, originally assigned to the OCC client by the SCP when the subscriber was alerted to the presence of an incoming call attempt, flowed next to the OCC server when the client elected to receive the call via VoIP, then to the SCP, then to the central office in association with a SCP command to forward the incoming call to the CSN, then to the OCC server on the CSN in association with that forwarded call.

6. Meanwhile, the OCC Client extracts 1) the VoIP Call Back DN from the SIP INVITE message received during Call Notification and 2) the H323UID and H323PIN values from its properties file and updates the 'netmtg.cnf' file.

7. The NetMeeting application is launched and sets up a connection with the VoIP Gateway.

8. Once a connection is established between NetMeeting and the VoIP Gateway, NetMeeting initiates a phone call - passing to the VoIP Gateway the Call Back DN as the destination DN.

9. The VoIP Gateway consults the VoIP Gatekeeper and authenticates the NetMeeting call by verifying the H323UID and H323PIN values, and by ensuring the called DN (i.e., Call Back DN) is authorized for use.

10. After passing the authentication step, the VoIP Gateway dials (via PSTN) the Call Back DN and gets connected to the CSN. The CSN notes that it was reached by the particular Call Back DN.

11. The CSN bridges the Calling and Called parties together by matching on the basis of the Call Back DN.

12. The CSN notifies the SCP (SIP 180 Ringing) of status and references the Call Back DN so that the SCP can reuse it for other calls.

13. If the central office supports that two B-channel transfer (Lucent, Nortel, and perhaps other central office vender's do), an optimization is possible. The CSN can have the central office rearrange the topology of the newly connected call in such a way that it flows only through the central office and no longer through the CSN.

5. NEC's Implementation

5.1. Overview

The NEC implementation of the ICW service is based on IN. Via a SPIRITS server and an ICW client, incoming calls will be presented to the user via a pop-up screen dialogue box. This dialogue box informs the user of the call arrival time and the calling party's number and name (if available). The arrival of the call is also indicated with an accompanied audible indication.

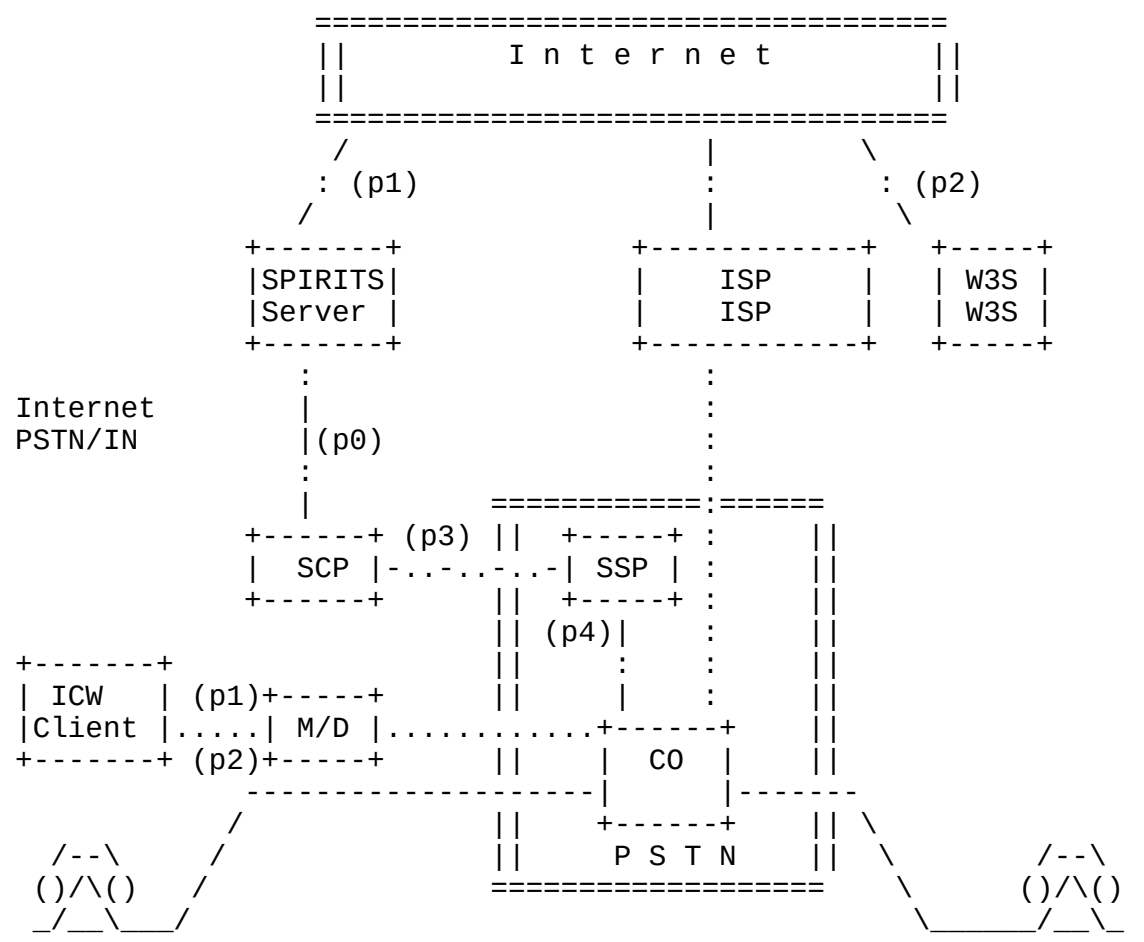
The pop-up dialogue box offers the user various call management options. Selecting a call management option allows the user to answer the call, forward it to another destination or to voice mail, or ignore it.

The user will be able to customize their service through various service set-up options. All calls presented to the user during an Internet session will be recorded in a call log.

Other features include Multiple call arrival management with which each new call arrival will generate its own pop-up dialogue box and audible indication.

5.2. Architecture and Overall Call Flow

Figure 10 depicts the NEC ICW system.



ICW Subscriber Calling Party

Legend:

ISP : Internet Service Provider
W3S : WWW Server
SCP : Service Control Point(acts as SPIRITS Client)
SSP : Service Switching Point
CO : Central Office
M/D : Modem

Traffic:

--- : PSTN Voice Traffic
... : PPP(IP traffic)
-..-: Signaling Traffic

Interfaces:

p0 : SPIRITS Server-SCP(SPIRITS Client) interface
p1 : SPIRITS Server-ICW Client interface
p2 : ICW Client-W3S interface
(Web access through HTTP)
p3 : SCP-SSP interface(INAP)
p4 : SSP-CO interface(ISUP)

Figure 10: the NEC ICW system

The description below provides the necessary steps to initiate the ICW service on a CO line, and how the ICW service is applied to an incoming call based on the above architecture:

1. The CO line is primed for the ICW service when the customer connects to their ISP by inserting a special activation code (e.g., *54) prefix in front of the ISP Directory Number.

2. The ICW service is activated when the user opens a secured session from an ICW client to the SPIRITS server. Once a session is open, the SPIRITS server will know the relationship between the line and the PC (i.e., it will know the Directory Number of the user's Internet line and the user's IP Address).

3. When a call arrives at a busy Internet line, the SSP will trigger the ICW service. The SCP which acts as the SPIRITS client will inform the SPIRITS server that a call is terminating to a busy Internet line. The message will include the Caller ID and Calling Line Identify Restriction (CLIR) Status of the calling party, and DN of the busy line.

4. The SPIRITS server will verify that if an ICW session has been established for the busy line. If so, the SPIRITS server will communicate with the user's ICW client application. The user will receive a real-time pop-up dialogue box including the Calling Name and Number of the Calling Party if available. The user will then select one of the following call management options:

   - Answer the call (the Internet connection will be automatically dropped and the phone will ring)
   - Send the call to Voice Mail
   - Forward the call to another destination
   - Ignore the call

5. When the Internet user has made a selection, the ICW client application will transmit this to the SPIRITS server. The SPIRITS server will instruct the PSTN via the SCP how to handle the call.

5.3. Interfaces and Protocols

5.3.1. SCP (SPIRITS Client)-SPIRITS Server Interface

5.3.1.1. Connecting to SPIRITS Services

The physical connection between the SCP and the SPIRITS server will be via a LAN/WAN. The logical connection will use the UDP/IP communications as defined in RFC 768 and RFC 1122.

If a socket connection is not currently established, the SCP will periodically try to open a connection. The SCP routing tables will be configured so that all available connections to a SPIRITS server are used.

5.3.1.2. Message Types

Two different types of message are used between the SCP and the SPIRITS server: "Connection Management Message Type" and the "Data Message Type". These messages will carry the remote operation messages which are based on ITU-T Q.1228 SCF-SCF interface with some NEC proprietary extensions.

NEC also has a plan to support SIP/SDP-based protocols for the SPIR-ITS client-server interface in the near future.

5.3.1.2.1 Connection Management Message Type

Connection management messages are to support functions related to the opening and closing of connections and monitoring connections to ensure reliable communications are maintained between the SCP and a SPIRITS server. The SCP is responsible for establishing a connection to a SPIRITS server. A connection can be closed by either the SCP or the SPIRITS server.

The "Connection Management Message Type" includes the following operations:

- scfBind - scfUnbind - activitytest

Opening a Connection

If a connection is not open to an SPIRITS server, the SCP will periodically try to open a connection until it is opened. If after a pre-determined number of attempts the connection is not opened, the socket connection will be released and then re-established and then the attempt to open the connection will be repeated.

The sequence for opening a connection is:

1. SCP will transmit a scfBind invokation message to the SPIRITS server. This message also carries the version information and activity test interval.

2. The SPIRITS server, upon receiving an invokation of the scfBind from a particular SCP, will reset all the data concerning the connection and then responds with either a return result containing the Web Server Identification number or a return error with a reason.

3. When the SCP receives a return result, if the ID number does not match the number configured in the SCP, then a scfUnbind will be sent indicating the wrong ID number. If the SCP receives nothing or a return error is received, then the scfBind will be retried after a pre-determined period of time.

4. Once the SCP has received a return result, the SCP will send Handling Information Request or Activity Test.

Upon receiving an invokation of activityTest, the SPIRITS server should reply with a return result of activityTest. If the SPIRITS server does not receive any invokation messages of Handling Information Request or Activity Test from the SCP for four times the Activity Test Interval value in milliseconds, the SPIRITS server should then close the connection.

To close a connection an invokation of the scfUnbind is sent by either the SCP or SPIRITS server to the remote end. When an invokation message of the scfUnbind is received, the receiving end should terminate the connection.

scfBind

The scfBind operation is used to open the connection between the SCP and the SPIRITS server. The SCP will send the SPIRITS server an invokation of the scfBind to establish an association. If the SPIRITS server is ready to handle the request then it should respond with a return result.

The return result of scfBind contains the identifier of the SPIRITS server. If the SCP receives the return result where the identification of the SPIRITS server does not match that registered against the SPIRITS server, then the SCP will send an invokation of the scfUnbind indicating an incorrect identifier was received.

If the SPIRITS server is not ready to handle the request or cannot handle the version, then it should respond with a return error.

scfUnbind

The scfUnbind operation is used to close the connection between the SCP and the SPIRITS server. Either the SCP or the SPIRITS server can invoke this operation.

Upon receiving an invokation message the receiving end should terminate the connection.

activityTest

If the SCP has not sent a Data Message for the time period specified by the "Activity Test Interval", it will send an invokation message of activityTest. When the SPIRITS server receives such an invokation, it will reply with a return result message of activityTest.

Its contents should be retained by the SPIRITS server. They are to be echoed back in the return result so that the message reply time can be calculated.

5.3.1.2.2. Data Message Type

SCPs use the following operations, which are sent to the SPIRITS server via a Data-Message-Type message, to request execution of some service procedure or notification of an event that takes place at the SCPs:

o handlingInformationRequest

  The handlingInformationRequest message will request a SPIRITS server the execution of some service procedure.

o handlingInformationResult

  The handlingInformationResult message will show the SCP the result of the execution, which was carried out by the SPIRITS server.

o confirmedNotificationProvided

  The confirmedNotificationProvided message will indicate to the SPIRITS server of an event, which takes place at the SCP. If the confirmedNotificationProvided indicating 'caller abandon' is received, the SPIRITS server will inform the client of the caller abandon and send the SCP a return result for the confirmedNotificationProvided.

The invoked operation has always a response which is either a return result of the operation or an invokation of another operation.

If a Data Message is not replied to within a pre-determined time out period then the message will be resent a number of specified times. Once the number of times has been exceeded, if another node exists, the message will be sent to another node if it is available. If all available SPIRITS servers have been queried then Message Time out will be returned to the calling process.

If an invokation of the handlingInformationResult is received with the cause=63 (Service not available), the handlingInformationRequest will be sent to another node if it is available. If all available SPIRITS severs have been queried then cause=63 will be returned to the calling process.

5.3.2. SPIRITS Server-ICW Client Application Interface

The following is a list of the application messages that are sent via the secure protocol (refer to section 5.3.3):

- VersionInfo (ICW client -> SPIRITS server)

  Indicate the current version of ICW client software. The SPIRITS server uses this information to determine if the client software is out of date.

- VersionInfoAck (SPIRITS server -> ICW client)

  If the VersionInfo message from an ICW client indicates to a SPIRITS server that it is an out of date version, the URL information is returned within the VersionInfoAck message for use in downloading the newer version. If the client software is up to date, the message simply indicates so and does not include any URL information.

- CallArrival (SPIRITS server -> ICW client)

  Sent by the server to tell the client someone has called the DN.

- CallID

  An identifier for this call. Unique in the domain of this client/server session.

- o CallingNumber

- o CallingName

  The name of the calling party is sent to the Client Application from the SPIRITS server. When available, the name is sent as a 15-character string. If the name is unavailable it is sent as "Name Unavailable". If the calling party has CLIR set, it is sent as empty (" ").

- o CallConnect (ICW client -> SPIRITS server)

  If a corresponding CallConnect is not received within a certain period after sending a CallArrival, the SPIRITS server will behave as though a CallConnect, Handling=Ignore had been received.

- o CallLost (SPIRITS server -> ICW client)

  Sent by server to cancel a CallArrival before a CallConnect is received by the server.

5.3.3. Secure Reliable Hybrid Datagram Session Protocol (SRHDSP) for Use Between ICW Client Application and SPIRITS Server

5.3.3.1. Overview

In principle the solution involves session initiation over SSL (meeting requirements for standards based security) after which the SSL session is closed, thereby reducing the number of simultaneous TCP/IP sessions. The rest of the session is communicated over UDP/IP, secured using keys and other parameters exchanged securely during the SSL session.

5.3.3.2. Session Initiation

The ICW client initiates an SRHDSP session, by reserving a UDP/IP port, and opening an SSL session with the service (e.g., ICW) on the service's well known SSL/TCP port. After establishing the SSL Session, the ICW client sends the server its IP address, the reserved UDP port number, and the set of supported symmetric key algorithms.

The server responds with a symmetric key algorithm chosen from the set, the server's UDP port for further communication, heartbeat period, and the value to use for the sequencing window.

The client then generates a symmetric key using the selected algorithm and transmits this to the server. The SSL session is then closed and the SRHDSP session is considered open.

5.3.3.3. Secure Reliable Datagram Transport

Application, and subsequent session management messages use symmetric signaling. That is, the signaling is the same whether the client is sending a message or the server is sending a message.

The message packets are transmitted securely. The protocol corrects for lost, duplicated and out of sequence packets.

5.3.3.4. Session closure

The client or server may close the session.

A session is closed using a Close message including the next sequence number, and encrypted with the agreed key.

The receiver, on processing (as opposed to receiving) a Close message, should set a timer, when the timer expires all details of the session should be forgotten. The timer is to allow for retransmission of the close if the Ack gets lost, we still need to be able to decrypt the subsequent retransmission and re-acknowledgment.

If any message other than a close is received after a close is processed, it is ignored.

6. Telia/Nortel's Implementation

6.1. Overview

The system implemented by Telia in cooperation with Nortel Networks is designed to support services that execute before the end-to-end media sessions are established. These services include, for example:

- call transfer and number portability for redirecting calls
- call waiting and call offering for announcing a pending call
- call screening and don't disturb for filtering incoming calls
- automatic call distribution and 800-services for selecting termination point

The Telia/Nortel system aims to allow service providers to develop the services mentioned above. Presently, prototypes for online incoming call disposition and automatic incoming call disposition (described in Section 2) have been developed to prove the concept.

In the Telia/Nortel architecture, services run on top of SIP Redirect Servers. The distributed nature of SIP enables these servers to be hosted, for example, by an enterprise server, a Service Provider's server cluster, a user's desktop PC, or even by a hand-held cordless device.

The SIP Redirect Server receives a SIP INVITE message for each call regardless of which network the call is being set up in. The server MAY apply any kind of service logic in order to decide on how to respond to the invitation. Service logic may interact with the user to allow the user to specify how to handle a call such as described in Section 2. This, however, is not the focus of the Telia/Nortel system.

6.2. Architecture and Protocols

The general idea behind the architecture is to create services as if all communication was based on IP and all clients and servers were SIP enabled. This of cause is not true in existing telecommunications networks. Hence, a new type of network element, the Service Control Gateways (SCG) hides the true situation from the services.

SCGs convert network-specific call control signaling to SIP messages and vice versa. A SCG behaves as a regular SIP User Agent (UA) towards the services and as a network-specific service control node in the network where the call is being set up. For example, when connecting to a GSM network, the SCG can play the role of an SCP or a MAP or an ISUP proxy. The specific role depends on what service triggers are being used in the GSM network.

SCGs handle protocol conversions but not address translation, such as telephone number to SIP URL, which is handled by a regular SIP Server to keep the SCG as simple as possible.

Consider a service example of number portability. A conventional number portability implementation in a mobile Circuit Switched Network (CSN) uses INAP messages to carry number queries to a network-internal data base application. Here, a SCG and a high-performance SIP Redirect Server, referred to as the Number Server (NS), have replaced the data base typically located in an SCP. (See Figure 11.)

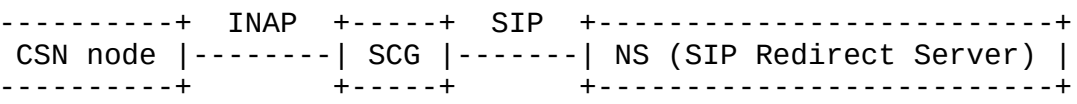


Figure 11: An Architecture for Number Portability

The INAP IDP message that carries the number query is converted to a SIP INVITE message by the SCG and is then forwarded to the NS (SIP Redirect Server).

If the called number is not registered, then the NS will return "404 Not Found". The SCG interprets this as "non ported number" and returns a CON message to the CSN network, making it connect the call to the called number.

If the number is ported and hence registered, then the NS will return "301 Moved Permanently" with a TEL URL (routing number) in the contact field. The SCG then returns a CON message to the CSN network, making it connect the call to the number that was conveyed in the contact field.

The solution above enables the same Number Server to provide Number Portability to multiple networks by means of using multiple SCGs.

If we make the SIP server in the number portability example operate in proxy mode for selected numbers, then it will become a kind of service router, able to relay number queries to any SIP-Redirect-Server-based service anywhere, provided there is an IP connection to the host in concern. Figure 12 shows the arrangement.

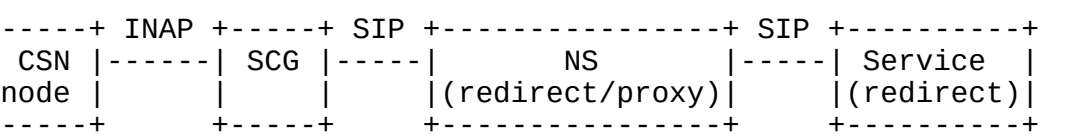


Figure 12: SIP-Based Service Router

Suppose that we connect a value-added service, such as a Personal Call Filtering service hosted by a user’s desktop PC, to a certain telephone number. The INAP IDP message is converted to a SIP INVITE message by the SCG and is then forwarded to the NS, just as in the previous example. However, in this case, the number is registered with a reference to a SIP URL. This makes the Number Server proxy the SIP INVITE message to the registered URL, which is the address of the service.

The service responds as a SIP Redirect Server and the Personal Call Filtering service logic determines the response. The NS sends the response back to the SCG which converts the response to an appropriate INAP message. The response from the service is typically "302 Moved Temporarily" with a telephone number in the Contact field.

If the response is 301 or 302, as the examples above suggest, then a telephone number is carried in the contact field. If the user can be reached via several different addresses, then all of them SHOULD be added to the response by means of multiple contact fields. The SCG then selects an address that is valid for the node or application that issued the number query.

As illustrated by the service examples, the Telia/Nortel system aims to allow the introduction of multi-network services without requiring multi-protocol support. The services hence operate in the same way regardless of in which network the call is made and common IP services can be shared across heterogeneous networks.

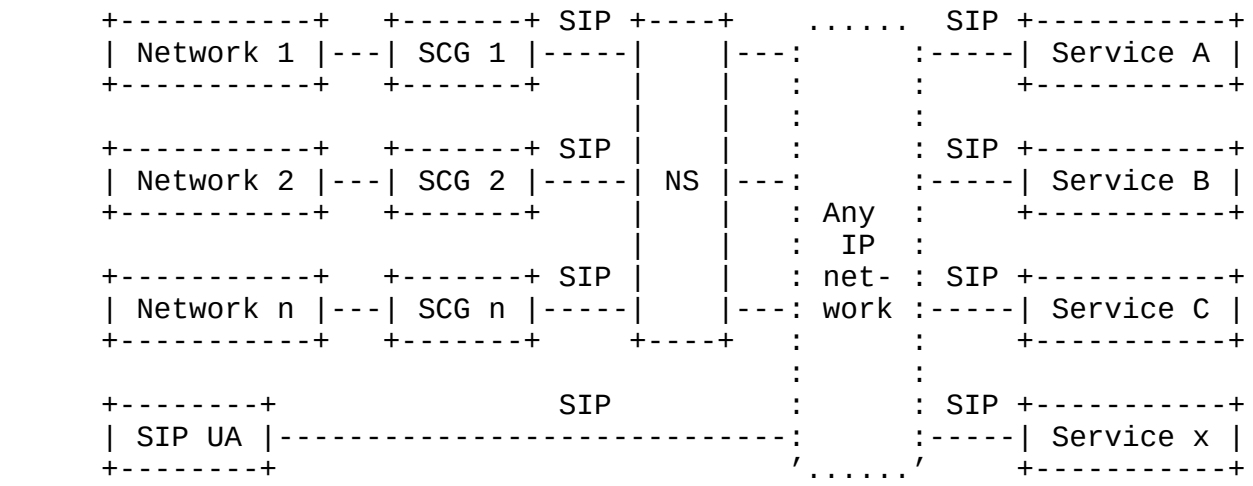


Figure 13: Interconnecting Heterogeneous Networks via SIP

6.3. Security

The Telia/Nortel architecture uses security mechanisms available to ordinary SIP services, implemented as they would be in a pure SIP network. The architecture described here does not impose any additional security considerations.

General security issues that must be considered include interconnection of two different networks. SCGs must therefore include mechanisms that prevent destructive service control signaling from one network to the other. For example, a firewall-type

mechanism that can block a denial-of- service attack from an Internet user toward the PSTN.

7. Security Considerations

Overall, the SPIRITS security requirements are essentially the same as those for PINT [3, 4], which include, for example:

+ Protection of the PSTN from attacks from the Internet.

+ Peer entity authentication to allow a communicating entity to prove its identity to another in the network.

+ Authorization and access control to verify if a network entity is allowed to use a network resource.

+ Confidentiality to avoid disclosure of information (e.g., the end user profile information and data) without the permission of its owner.

+ Non-repudiation to account for all operations in case of doubt or dispute.

As seen in the previous sections, most implementations examined in this document have employed means (e.g., firewalls and encryption) to meet these requirements. The means are, however, different from implementation to implementation.

8. Conclusion

This document has provided information relevant to the development of inter-networking interfaces between the PSTN and Internet for supporting SPIRITS services. Specifically, it described four existing implementations of SPIRITS-like services. Surveying these implementations, we can make the following observations:

- The ICW service plays the role of a benchmark service. All four implementations can support ICW, with three specifically designed for it.

- SIP is used in most of the implementations as the based communications protocol between the PSTN and Internet. (NEC's implementation is the only exception that uses a proprietary protocol. Nevertheless, NEC has a plan to support SIP together with the extensions for SPIRITS services.)

- All implementations use IN-based solutions for the PSTN part.

It is clear that not all pre-SPIRITS implementations inter-operate with each other. It is also clear that not all SIP-based implementations inter-operate with each other given that they do not support the same version of SIP. It is a task of the SPIRITS Working Group to define the inter-networking interfaces that will support inter-operation of the future implementations of SPIRITS services.

9. References

[1] Petrack, S. and L. Conroy, "The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services", RFC 2848, June 2000.

[2] Handley, H., Schulzrinne, H., Schooler, E. and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, March 1999.

[3] Lu, H. (Ed.), Krishnaswamy, M., Conroy, L., Bellovin, S., Burg, F., DeSimone, A., Tewani, F., Davidson, D., Schulzrinne, H. and K. Vishwanathan, "Toward the PSTN/Internet Inter-Networking--Pre-PINT Implementations", RFC 2458, November 1998.

10. Authors' Addresses

Igor Faynberg
Lucent Technologies
Room 4L-334
101 Crawfords Corner Road
Holmdel, NJ, USA 07733-3030

Phone: +1 732 949 0137
EMail: faynberg@lucent.com

Hui-Lan Lu
Lucent Technologies
Room 4L-317
101 Crawfords Corner Road
Holmdel, NJ, USA 07733-3030

Phone: +1 732 949 0321
EMail: huilanlu@lucent.com

John Voelker
Lucent Technologies
Room 1A-417
263 Shuman Blvd PO Box 3050
Naperville, IL, USA 60566-7050

Phone: +1 630 713 5538
EMail: jvoelker@lucent.com

Mark Weissman
Lucent Technologies
Room NE406B
200 Lucent Lane
Cary, NC, USA 27511-6035

Phone: +1 919 463 3258
EMail: maw1@lucent.com

Weizhong Zhang
Lucent Technologies
Room 01-A5-17
2000 Regency Parkway
Cary, NC, USA 27511-8506

Phone: +1 919 380-6638
EMail: wzz@lucent.com

Sung-Yurn Rhim
Korea Telecom
17 Woomyun-dong
Seocho-gu, Seoul, Korea

Phone: +82 2 526 6172
EMail: syrhim@kt.co.kr

Jinkyung Hwang
Korea Telecom
17 Woomyun-dong
Seocho-gu, Seoul, Korea

Phone: +82 2 526 6830
EMail: jkhwang@kt.co.kr

Shinji. Ago
NEC Corporation
1131, Hinode, Abiko,
Chiba, 270-1198, Japan

Phone: +81 471 85 7412
EMail: ago@ssf.abk.nec.co.jp

S. Moeenuddin
NEC America, Inc
1525 Walnut Hill Lane,
Irving, TX, USA 75038

Phone: +1 972 518 5102
EMail: moeen@asl.dl.nec.com

S. Hadvani
NEC America, Inc
1525 Walnut Hill Lane,
Irving, TX, USA 75038

Phone: +1 972 518 3628
EMail: hadvani@asl.dl.nec.com

Soren Nyckelgard
Telia Research
Chalmers Teknikpark
41288 Gothenburg
Sweden

EMail: soren.m.nyckelgard@telia.se

John Yoakum
Nortel Networks
507 Airport Blvd, Suite 115,
Morrisville, NC, USA 27560

EMail: yoakum@nortelnetworks.com

Lewis Robart
Nortel Networks
P.O. Box 402
Ogdensburg, NY, USA 13669

EMail: robart@nortelnetworks.com

11. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.