

Internet Draft  
PSTN and Internet Internetworking Working Group  
Expire in six months

M. Krishnaswamy  
Bell Laboratories,  
Lucent Technologies  
November 1997

## PSTN-Internet Internetworking - An Architecture Overview

[<draft-ietf-pint-inweb-00.txt>](#)

### Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

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

### Abstract

This memo is submitted as input to the draft PINT (PSTN and Internet Internetworking) Informational RFC. This document describes an internetworking architecture of the Public Switched Telephone Network (PSTN) and the Internet based on the Lucent prototype. This architecture enables access to PSTN services from the Internet. The four basic PSTN services that could be made available to an Internet User are described. We have used the World Wide Web as an example to show how these PSTN services can be seamlessly integrated into the Internet. Next a Service Support Transport Protocol for reliable transfer of service request from the Internet to the PSTN network is described. A simple Management Information Base (MIB) that is used for uploading information and performing authentication checks is

then described.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Service Description . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Overall Interconnection Architecture . . . . .	<a href="#">4</a>
<a href="#">4.</a>	Interfaces Relevant to the Work . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Role of the Web server and IN entities . . . . .	<a href="#">6</a>
<a href="#">6.</a>	A Click-to-Dial-Back Service Scenario . . . . .	<a href="#">7</a>
<a href="#">7.</a>	SSTP Information Exchange . . . . .	<a href="#">7</a>
<a href="#">8.</a>	Web server - SMS Interface and SNMP MIB . . . . .	<a href="#">10</a>
<a href="#">9.</a>	Security Considerations . . . . .	<a href="#">11</a>
<a href="#">10.</a>	References . . . . .	<a href="#">12</a>
<a href="#">11.</a>	Authors' Address . . . . .	<a href="#">12</a>
<a href="#">12.</a>	<a href="#">Appendix A</a> . . . . .	<a href="#">14</a>

## [1.](#) Introduction

Interconnection of the Internet and Public Switched Telephone Networks would provide more effective media to a user than either network type can do presently. Interworking of the Internet and PSTNs, based on open well-defined interfaces, will promote interoperability of both the networks and systems built by different vendors.

Based on the prototype developed in Bell Laboratories, this document describes a specific example of basic PSTN services that could be accessed from World Wide Web, the most popular Internet application/service. The Service Support Transport Protocol used to transfer the PSTN service requests from the Web server to the PSTN network is based on TCP so as to provide reliable communication between the two network entities.

On the PSTN side we have considered only one architecture, IN (Intelligent Network) in our case. IN has been standardized internationally by the International Telecommunications Union Telecommunications Standardization Sector (ITU-T) and is being widely implemented in the telecommunications networks around the world. Again within the IN, our document describes the interconnection to the two specific IN entities, Service Node (SN) and the Service Management System (SMS). A brief introduction to the Intelligent

Network architecture is provided in [Appendix A](#) for those not familiar with the IN.

A specific example of a World Wide Web User browsing the Web pages and clicking on a hyper-text link in a content provider's page to

place a PSTN service call is used throughout this document.

A Management Information Base for uploading Web content provider profiles to the SMS and providing service authentication and verification is next described.

Finally we briefly mention about some of the security issues involved in the internetworking of the PSTN and Internet.

## [2.](#) Service Description

The common denominator of the services introduced in this section is bringing telephone services (provided by PSTNs) to Internet users. Successful interworking of the Internet and Public Switched Telephone Network (PSTN) should enable integration of PSTN services (e.g., a telephone call) with those offered by the Internet through the World-Wide Web. Examples of such services are Click-to-Dial-Back, Click-to-Fax, Click-to-Fax-Back, and Voice-Access-to-Content, and they can be briefly described as follows:

With the Click-to-Dial-Back service, a Web user can initiate a PSTN call by clicking a button during a Web session. Such a call can be either incoming or outgoing. (An example of the former is when a user, while browsing through a catalogue, clicks the button inviting a sales representative to call him or her.)

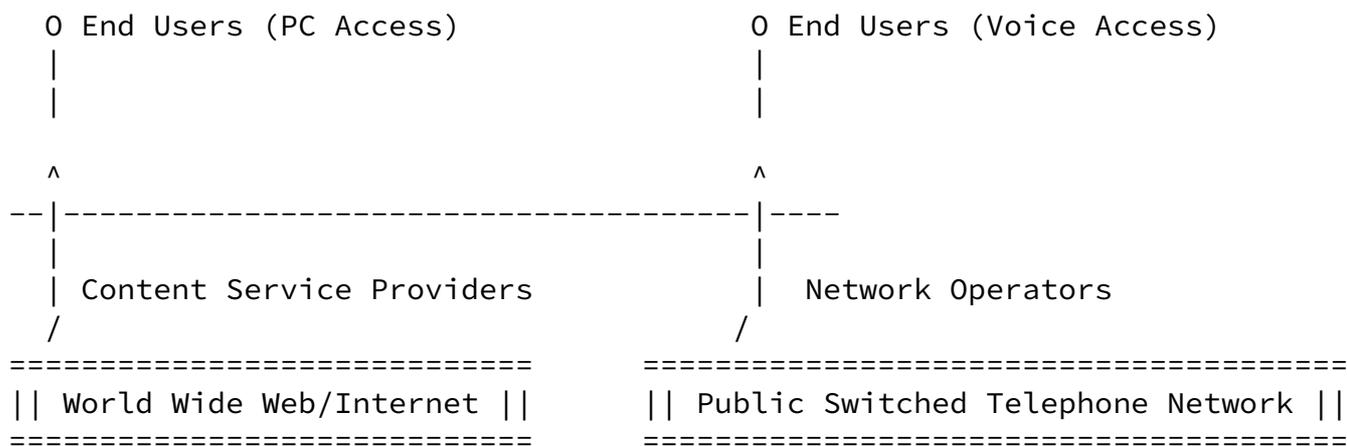
With the Click-to-Fax service, a Web user can send a fax by clicking a button during a Web session.

With the Click-to-Fax-Back service, a Web user can request (and subsequently receive) a fax by clicking a button during a Web session.

With the Voice-Access-to-Content service, a Web user can have access to the Web content by telephone. The content is converted to speech and transmitted to the user on a telephone line.

(In all of the above four cases the service request and the data thereof (for Click-to-Fax, Click-to-Fax-Back and Voice-Access-to-Content) are sent from the web server to the PSTN equipment).

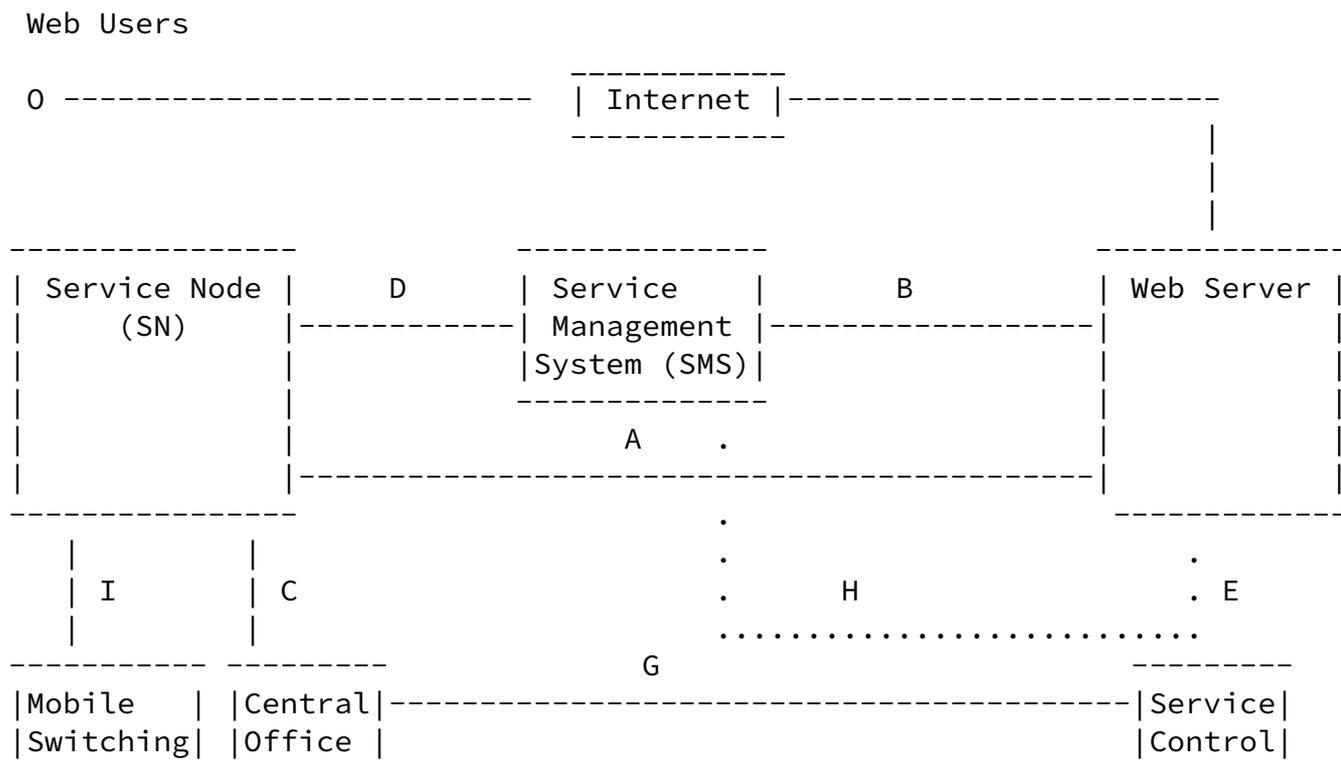
FIGURE 1:

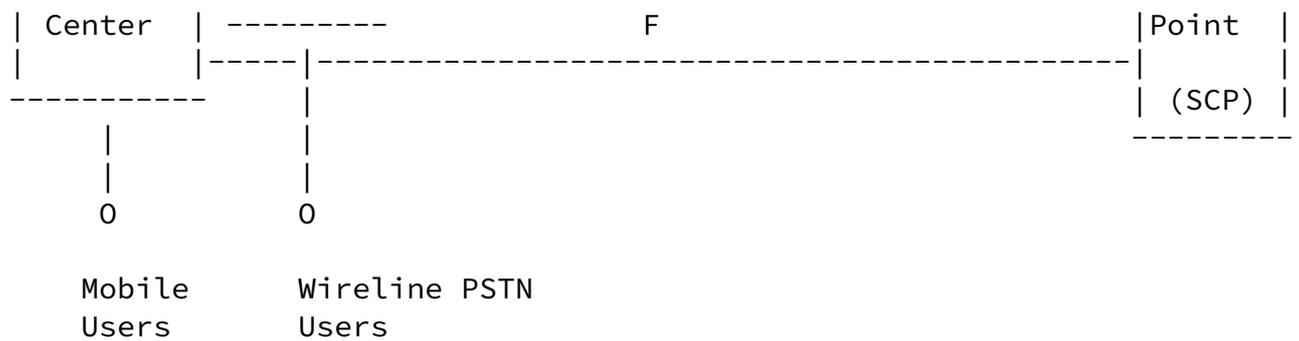


### 3. Overall Interconnection Architecture

A somewhat general view of the proposed project is presented in Figure 1. The figure distinguishes the two types of end-users: 1) the Web users, whose PCs (or other Internet access devices) are connected to the Internet, and 2) the telephone users, whose telephones or fax machines are connected to PSTNs. In this context, the proposed internetworking involves interconnection of Internet service providers and network operators (who own PSTNs).

Figure 2:





In Figure 2 we identify the scope of our work covered in this document in an overall PSTN/Internet interworking architecture.

The PSTN users are depicted connected to both the central office via wireline and mobile switching center via wireless communications. The IN entities that contain the Service Control Function (i.e., the SN and SCP) are shown with their respective interfaces to, first of all, the switches. Specifically, the ISDN-based interfaces from the SN to the MSC and center office are respectively marked I and C; the SS7-based interfaces from the SCP to the MSC and center office are respectively marked F and G. (The latter two interfaces are depicted with the dotted line because they are not within the scope of this work). Finally, the SMS is depicted together with its respective interfaces to the SN (D) and SCP (H). (Again, the interface H is

depicted with the dotted line because it is not within the scope of the work.)

On the Internet side, Figure 2 exhibits a Web user connected to the Web server. The server can have two interfaces: interface A to the SN and interface B to the SMS. (As before, a feasible, but not considered within the scope of this work, interface E to the SCP is depicted using the dotted line.)

#### 4. Interfaces Relevant to our work

Referring to Figure 2, the relevant interfaces are A, B, D, I, and C.

The interfaces between the SN and switches (interfaces I and C), as

well as the interface between the SN and SMS (interface D) have been studied in ITU-T Study Group 11;

In our work interface A is based on SSTP (Service Support Transport Protocol) carried on top of TCP/IP and the interface B is based on SNMP Ver 2.

## 5. Role of the Web server and IN entities

### Web Server

The web server stores the profiles of content providers. The profile should include information such as content provider ID, telephone number and fax number. It may also include service logic that specifies, for example, the telephone (or fax) number to be reached based on time of the day, day of the week, or geographical location of the user, and the conditions to accept the charge of the calls.

The web server may also store the profiles of users who are pre-registered. Similar to the content provider profile, the user profile include information such as user name, password, telephone number, and fax number. The last two pieces of information can also be linked with time of the day and day of the week so the user can be reached at the appropriate telephone (or fax) number accordingly.

### Service Node

Situated in the PSTN, the SN, like the SCP, performs the service control function [1] [2]. It executes service logic and instructs switches on how to complete a call. Unlike the SCP, the SN also performs certain switching functions (like bridging of calls) as well

as a set of specialized functions (like playing announcements, voice recognition and text-to-speech conversion).

Another distinction between the SN and SCP is that the former is connected to switches via the Integrated Services Digital Network (ISDN) Primary or Basic Rate Interfaces (PRI or BRI) while the latter is connected to switches via the Signaling System 7 (SS7) network. As such, there are fewer security concerns connecting the SN than SCP to

the web server.

## Service Management System

The SMS performs administration and management of service logic and customer-related data on the SN. It is responsible for the replication of content provider profiles and provision of these data on the SN. These functions are not performed in real time.

### 6. A Click-to-Dial-Back Service Scenario

A Web user, who has simultaneous access to the Web and telephone services (this can be achieved, for example, by having an ISDN connection), is browsing through a sales catalogue and deciding to speak to a sales representative.

When the Web user clicks a button inviting a telephone call from the sales office, the Web server sends a message to the SN over the A interface, thus crossing the Internet-to-PSTN boundary. By matching the information received from the Web server with the content provider profile that had been previously loaded and activated by the SMS over the D interface, the SN recognizes the signal.

At this point, the SN calls the Web user. The user answers the call, hears an announcement (e.g., "Please wait, while we are connecting you to the sale agent") and is waiting to be connected to the sale agent. Then the SN invokes service logic as indicated in the profile. The execution of this logic selects an appropriate sales agent to call based on the time of the day. It is 8 P.M. in New York where the Web user is located, and the New York sales office has closed. But the San Francisco office is still open, and so the SN selects an appropriate central office, establishes the connection (the interface C) to this central office, verifies that there is at least one sales agent line that is free and instructs the switch to call the agent. Finally, the SN bridges the two calls and establishes a two-party call between the sales agent and the Web user.

### 7. SSTP Information Exchange

server. It is of a request/response type running on top of a reliable transport layer, such as TCP. The web server sends a request to the SN to invoke a service and the SN responds with a message indicating either success or failure. Note that the protocol effectively engages the service control function [1] [2] that is common to both the SN and SCP; for simplicity only the SN is mentioned.

#### A. Web Server to Service Node

In this direction, three kinds of messages may be sent: the Transaction Initiator message, the Data Message, and the End of Data message.

The latter two messages are needed if the service to be invoked involves data (e.g., click-to-fax, click-to-fax-back and voice-access-to-content). This is so designed to handle the varying size of data and to ensure that the size of each stream is within the allowable size of the underlying transport packet data unit (imposed by some implementations of TCP/IP).

##### a. Transaction Initiator

This message provides all the necessary information but data for invoking a service. It includes the following information elements:

- + Transaction ID, which uniquely specifies a service request. The same transaction ID should be used for all the accompanying data-related messages, if the service request involves data. One way for generating unique transaction IDs is to concatenate the information: date, time, web server ID (uniquely assigned for each one connected to the SN), and transaction sequence number (a cyclic counter incremented for each service request).
- + Service ID, which specifies the service to be invoked. The service may be click-to-dial, click-to-fax, click-to-fax-back or voice-access-to-content.
- + Content Provider ID, which uniquely represents the content provider. This information is the key to accessing the content provider's service logic and data on the SN.
- + Content Provider Directory Number, which is the telephone or fax number of the content provider to be called through the PSTN.
- + User Directory Number, which is the telephone or fax number of the user requesting the service.

---

- + Billed Party, which specifies the party (either the user or content provider), to be billed.

In addition, optional parameters may be sent from the web server to the SN. For example, a retry parameter may be sent to specify the number of times the SN will attempt to complete a service request upon failure before the transport connection times out.

#### b. Data Message

This message provides the (encapsulated) user data part of a service request. For example, in the case of click-to-fax-back such data are the content to be faxed to the user. Each message is composed of the transaction ID and a data segment. The transaction ID must be the same as that of the transaction initiator part first invoking the service.

#### c. End of Data Message

This message contains the transaction ID and the end of data delimiter. The transaction ID is the same as that of the relevant transaction initiator message.

### B. Service Node to Web Server

The SN must respond to a service request from the web server. The response message consists of the information elements:

transaction ID, service type, result, time, and error code.

- + Transaction ID, which is the same as that of the original service request.

- + Service Type, which is the same as that of the original service request.

- + Result, which is either success or failure.

- + Time, which indicates the time of the day completing the request.

- + Error Code, which gives the reason for failure. Possible reasons for failure are content provider telephone (or fax) busy, content provider telephone (or fax) no answer, user telephone busy, user refusal to complete, user no answer, nuisance control limit reached,

and content provider telephone (or fax) not in the SN database.

## 8. Web Server - SMS Interface and SNMP MIB

This interface is needed to upload the content provider profile from the web server to the SMS and manage the information against any possible corruption. The SN verifies the Content Provider ID and the Content Provider Directory Number sent by the Web Server with the content provider profile preloaded from the SMS.

The content provider profile is based on ASN.1 structure and we use SNMP to set/get the object identifiers in the SMS database. [3] [4]

Following is an example of the simple MIB available on the SMS.

```
inwebContProviderTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF InwebContProviderEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        " A table containing Content Provider profiles "
    ::= { inweb 1}

inwebContProviderEntry OBJECT-TYPE
    SYNTAX          InwebContProviderEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        " A conceptual row of the inweb. Each row
          contains profile of one Content Provider"
    INDEX          { inwebSmsNumber }
    ::= { inwebContProviderTable 1 }

InwebContProviderEntry ::= SEQUENCE {
    inwebSmsNumber          Integer32,
    inwebContentProviderId Integer32,
    inwebContentProviderPhoneNumber Integer32,
    inwebContentProviderFaxNumber Integer32
}
```

inwebSmsNumber OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

" Serial number of the SMS - used for SNMP indexing "  
 ::= { inwebContProviderEntry 1 }

inwebContentProviderId OBJECT-TYPE

M. Krishnaswamy

[Page 10]

---

PSTN-Internet Internetworking Architecture

November 1997

SYNTAX Integer32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

" A number that uniquely identifies each Content Provider "  
 ::= { inwebContProviderEntry 2 }

inwebContentProviderPhoneNumber OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

" Content Provider's Phone Number "  
 ::= { inwebContProviderEntry 3 }

inwebContentProviderFaxNumber OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

" Content Provider's Fax Number "  
 ::= { inwebContProviderEntry 4 }

## 9. Security Considerations

We only address the security issues concerning the interface between the Web server and the SN (or SCP). Those concerning the interface between the user and the Web server are not specific to this proposal and won't be discussed. The interface between the Web server and SMS is based on SNMP and will rely on its own security features.

#### + Secure Communication Links

If the Network Operator (PSTN provider) is also Web Service provider, the Web Server and SN/SMS will be over a corporate intranet. This network is almost always protected by the corporation's firewall and so can be deemed secure.

Nevertheless, if the Network Operator and the Web Service provider are different corporations, then it is likely that there may not exist a dedicated secure communication link between the Web Server and SN/SMS. The communications may be required to be carried over Internet. This raises serious security considerations. One possible solution is to use Virtual Private Networks (VPN). VPNs features support authentication of the calling and called parties and encryption of the messages sent over unsecure links (Internet).

M. Krishnaswamy

[Page 11]

---

PSTN-Internet Internetworking Architecture

November 1997

#### + Non-Repudiation

All transactions will be logged on both the Web server and the service node to account for all operations in case of doubt or dispute. The log information on the SN can also be used to generate bills.

#### + Malicious Requests of Users

A user may make repeated requests to a content provider directory number maliciously. This can be handled by setting a Nuisance Control Limit (NCL) on either the SN or the Web server or both. The NCL may be based on requests from the same user within a, for example, 15 minute period.

A user may also attempt to request a call from a directory number other than that of a content provider. Such an attempt can be handled by verifying the directory number (and the content provider ID) against the database on the SN containing all the content provider information. If the directory number (or the content provider ID) is not in the database, the request will be rejected.

#### [10](#). References

[1] ITU-T Q.12xx Recommendation Series, Geneva, 1995.

[2] I. Faynberg, L. R. Gabuzda, M. P. Kaplan, and N. J. Shah, "The Intelligent Network Standards, their Application to Services". McGraw-Hill, 1996.

[3] Information processing systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), International Organization for Standardization. International Standard 8824, (December, 1987).

[4] McCloghrie, K., Editor, "Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1902](#), January 1996.

#### [11](#). Author' Address

Murali Krishnaswamy  
E-mail: murali@bell-labs.com  
Telephone: +1-732-949-3611  
Fax: +1-732-949-3210

M. Krishnaswamy

[Page 12]

---

PSTN-Internet Internetworking Architecture

November 1997

Bell Laboratories  
Room 2G-527A  
[101](#) Crawfords Corner Road  
Holmdel, NJ 07733-3030  
USA

[12. Appendix A](#) - Intelligent Network (IN)

IN ([1], [2]) is an architectural concept that provides for the real-time execution of network services and customer applications in a distributed environment consisting of interconnected computers and switching systems. Also included in the scope of IN are systems and technologies required for the creation and management of services in this distributed environment.

In PSTNs, user's telephone terminals and fax machines are connected to

telephone switches. The switches (which can be Central Offices--for wireline communications and Mobile Switching Centers (MSCs)--for wireless communications) are specialized computers engineered for provision of services to the users. The switches themselves are interconnected in two ways: 1) through trunks on which the voice is carried and 2) through a specialized fault-tolerant data communications network, which is (principally) used for call setup and maintenance. This network is called (after the ITU-T standard protocol suite that it uses) Signalling System No. 7 (SS7). In addition, the switches are connected to general purpose computers that support specialized applications (called Operations Systems) whose role includes network management, administrative functions (e.g., billing), maintenance, etc. Operation systems are not connected to the switches through the SS7 network, which is, again, engineered only for set-up and real time maintenance of calls. In most cases, X.25 protocol is used for communications between operations systems and switches.

Even a simple two-party call in most cases involves several switches, which may also be located in different PSTNs. To this end, the switches alone comprise a complex distributed processing environment. As far as the end users are concerned, the switches are ultimately responsible for delivering telecommunications services. Certain elementary services (such as provision of the dial tone, ringing the called line, and establishing a connection between two users) are called basic services, and all switches can presently cooperate in delivering them to end users.

In addition, a multitude of services (such as Freephone [a.k.a. 800 number in North America], Conference Calling, Call Forwarding, and many others) require much more than basic call processing. Such services are called Supplementary Services, and their implementation requires that specialized applications (called Service Logic) be developed. Developing switch-based service logic for each supplementary service would be an extremely expensive (if at all possible) task, which--in the presence of multiple switch vendors--would also require an extensive standardization effort.

The IN architecture is the alternative which, in a nutshell, postulates using a network-wide server (called Service Control Function [SCF]). The SCF executes service logic and instructs the switches on how to complete the call. A switch is involved only in executing the basic call process,

which is interrupted (at standardized breakpoints called triggers) when specialized service logic needs be executed. On encountering such a breakpoint, the switch issues a query to the SCF and waits for its instruction. In addition (and this is essential for supporting the services described in [section 2](#)), the SCF may initiate a call on its own by instructing switches to establish necessary connections among themselves and to the call parties.

Physically, the SCF may be located in either stand-alone general purpose computers called Service Control Points (SCPs) or specialized pieces of equipment called Service Nodes (SNs). In addition to executing service logic, a service node can perform certain switching functions (such as bridging of calls) as well as a set of specialized functions (such as playing announcements, voice recognition and text-to-speech conversion).

An important distinction between an SCP and SN is that the former is connected to switches via the SS7 network while the latter communicates with the switch via Integrated Services Digital Network (ISDN) Primary or Basic Rate Interfaces (PRI or BRI), which combine both the signaling and voice paths. With the present state of IN standardization, in principle, either an SCP or SN could be connected to an Internet server in order to support the services outlined in section two. To further narrow the scope of work so as to produce tangible results as soon as possible, the proposed project specifically addresses only interconnection between a server and SN.

Within the IN architecture, the relevant administration of the network entities (i.e., setting the triggers in the switches, transferring externally developed service logic to SCPs and SNs, and maintaining the network databases with the customer-related data) is performed by a specialized Operation System called Service Management System (SMS).