Alcatel·Lucent

TECHNOLOGY WHITE PAPER

IMS Interconnect: Peering, Roaming and Security – Part One

IMS interconnection promises to enable greater reach and richer offerings for the providers that establish successful peering arrangements.

This paper provides an introduction to IMS interconnection and identifies security considerations that carriers must address in order to achieve the proper balance of providing access while maintaining security.

The paper is organized into two parts – Part One introduces key concepts and definitions related to network interconnections and interconnect models, while Part Two addresses the security mechanisms within the IMS standards and identifies potential security threats that face IMS carriers looking to interconnect their networks.

Introduction

While service providers are rushing to bring their initial IMS service offerings into commercial service, a number of them are also beginning to look beyond their basic IMS architectures to explore the potential for connecting to other carrier's networks. By interconnecting their networks, carriers are looking to extend their reach and to leverage opportunities to explore new business models with partner providers.

These types of provider-to-provider connections are not a new phenomena, there are examples of interconnected carriers in the PSTN world, the mobile telephone environment, and in the IP service provider industry. The Internet is a perfect example of a fully interconnected network – subscribers can interact with other subscribers and services, regardless of which service provider they belong to.

The advantages of creating interconnected IMS networks include:

- Carriers can provide services to their IMS subscribers while those subscribers visit geographies, regions, or networks where that carrier does not have a physical presence.
- For voice traffic, carriers can bypass potentially costly network handoffs for calls to subscribers on other IMS networks by utilizing an IP network connection between the IMS networks to carry the traffic. One example of this is the peering agreements that some VoIP providers currently have, where a subscriber from one provider can call a subscriber of another provider over the IP network, totally bypassing the PSTN.
- Carriers can utilize the transport and access networks of their business partners to offer seamless access to their subscribers, such as in a scenario where a wireless provider might team with a DSL carrier to enable their customers to utilize IMS services both in the home (via the DSL connection) and while they are traveling (via a 3G data connection)
- Carriers can partner with multiple IMS applications/services providers to enhance the portfolio of applications and services they offer to their customers.

The purpose of this white paper is to provide an introduction to IMS interconnection and to identify some of the security considerations that carriers will need to address in order to achieve the proper balance of providing access while maintaining security.

The paper is organized into two parts – Part One will introduce key concepts and definitions related to network interconnections and interconnect models, while Part Two will address the security mechanisms within the IMS standards and will identify potential security threats that face IMS carriers looking to interconnect their networks.

Note: This paper is based upon the IMS concepts and standards defined by the 3GPP and by ETSI, but the behaviors for the selected elements are consistent in the other IMS standards – any exceptions will be noted appropriately.

Table of Contents

IMS Key Concepts & Definitions

There are a number of concepts that are central to the discussion of a multi-carrier environment. Within this document, the scenarios described will be based upon the following definitions

Interconnect and Peering

Interconnect refers to the connections between services providers/carriers for the purpose of carrying network traffic (phone calls, IP data, SIP sessions, etc) from subscribers on one carrier's network to subscribers on another carrier's network. Interconnect agreements have been in existence for some time now in the voice telecommunications industry. Typically, service providers that wanted to interconnect their voice networks would develop an agreement on the types of services to be provided over the interconnection, and then they would develop a variety of business and technical agreements on issues such as how to bill for the traffic, what levels of service must be provided, how best to route network traffic, and how to identify and resolve problems as they occur.

In the early years of IP networking, Internet Service Providers (ISPs) began to follow a model similar to the telecom interconnect model so they could extend the reach of their IP networks and thereby provide access between their subscribers and the rest of the Internet community. Network Access Points (NAPs) were established to provide facilities for the interconnection of these networks. The physical connections, along with the business agreements that were established to govern the passing of traffic between the providers were addressed within peering agreements drafted by the ISPs. The connectivity between large ISPs became known as *peering*.

With the introduction of IP-based protocols such as SIP, there was a need to distinguish between the various levels of peering that are possible between carriers. The two most relevant types of peering in the IMS environment are IP-protocol level (Layer 3) peering and SIP-level (Layer 5) peering. Layer 3 peering agreements address the routing of all types of IP-based data packets, while Layer 5 agreements are focused on the routing of SIP traffic (most typically session signaling) between carriers and customers on those carrier's networks. This creates some interesting possibilities for traffic flows. In an IMS network, the signaling traffic and the bearer traffic are handled separately, so it is conceivable that the routing of signaling traffic governed by a Layer 5 peering agreement may take a different path and be covered by a different peering agreement than the bearer traffic as it traveled over the most efficient Layer 3 route to its destination.

IMS and IMS-like environments contain a number of potential interconnect points, including connections to the PSTN, connections to various access networks (GSM/UMTS, wireline, cable), connections to other application-level services (SMS, MMS) and connections to other IMS providers. For the purposes of this paper, the term *peering* will be used exclusively to refer to Layer 5 (SIP) connection agreements with other IMS providers, while *interconnection* will refer to connectivity to other non-IMS networks.

In order for carriers to establish an IMS peering arrangement, they must first agree upon a range of technical and business agreements that will govern the types of IMS sessions that will be supported, how these sessions will be billed, how the sessions and user data will be secured, and what mechanisms the carriers will utilize to measure and charge for traffic as part of the settlement process. These agreements will normally take the form of formal contracts and technical policy documents.

Roaming, Home Networks, and Visited Networks

The notion of *roaming* (the act of a subscriber gaining access to their mobile network while traveling in another city or country) gained popularity with the growth of mobile phone networks. By establishing roaming agreements with other mobile carriers, a provider could offer seamless call origination and completion to their customers, regardless of the geographic location of the subscriber. Roaming agreements address a specific type of interconnection, one in which a subscriber looks to access a certain type of service (in the mobile world, it may be a voice call or GPRS data session) from a *visited network* while they are traveling outside of their *home network*.

In the mobile communications world, roaming agreements define which carriers' subscribers are permitted to make and receive calls and access services within a visited network, as well as identifying the types of payment that a provider would expect to receive from the other provider for carrying the voice traffic.

The IMS standards address scenarios in which an IMS user might travel outside of the reach of their IMS provider in a manner similar to the mobility model by defining the notion of a *home IMS network* and a *visited IMS network*. When an IMS subscriber wants to access IMS services while they are on a visited IMS network (a network served by the P-CSCF of an another IMS provider), they are considered to be *roaming*.

Specific roaming scenarios will be covered in greater detail later this document.

Service location process

In order to differentiate between how an IMS subscriber device (UE) behaves in a roaming scenario versus how it behaves in a non-roaming scenario, it is important to clarify the mechanisms and configuration details that control the process for how the UE locates, and connects to, the IMS.

Service location processes are similar between 3GPP IMS and TISPAN. Standards for both architectures assert that the UE will contain an ISIM (IMS Subscriber Identity Module), that retains IMS security-related data, including the home IMS network domain information. Initially, in 3GPP IMS implementations, the ISIM will reside on a UICC (essentially a SIM card), but there are provisions for future ISIM implementations that are not SIM-based. TISPAN includes provisions for the ISIM to exist either on the UE itself, or on a residential gateway that provides connectivity between existing PSTN handsets and the IMS. [1, 2]

When the UE establishes a connection to the IP network, it will first obtain an IP address (through DHCP or an address assignment mechanism unique to the access network type).[3]

Once the UE has received an IP address, it will utilize DHCP to request either the IP address or the DNS name of the local P-CSCF. If DHCP is not available, the UE can obtain the P-CSCF information through some other mechanism supported by the access network (in the case of GPRS, the P-CSCF information can be supplied during the establishment of the PDP context).

In the case of a 3GPP UE connecting via a wireless LAN, the UE will first request a local IP address for the wireless LAN via DHCP, and will then establish a tunneled connection (IKE security association and an IPSec ESP security association) with a packet data gateway (PDG). While the tunnel is established with the PDG, the UE will receive another IP address (associated with the tunnel) and will acquire the P-CSCF address from DHCP. [4]

DNS and ENUM

Another set of functional elements of the IMS infrastructure that are critical to peering and roaming scenarios are the DNS and ENUM functions.

There are a number of existing papers that cover the peering-support function of DNS and ENUM in greater detail, [5]. For the purposes of this paper, the following description will be sufficient.

DNS, the Domain Name Service, is the service responsible for providing a mapping between IP host DNS names (such as www.alcatel-lucent.com) and the IP address for that host (such as 192.168.1.1). When a host sends a request to the DNS server for a specific host name, the DNS server will respond with the IP address or other related information, depending upon the specific type of request it received.

The ENUM service, as defined in RFI 3761, [6] is responsible for mapping telephone type numbers (E.164 numbers) to Uniform Resource Identifiers (URIs) that point to specific application/address combinations, such as "sip:mostern@alcatel-lucent.com". When an IMS subscriber attempts to initiate a session with another IMS subscriber by dialing their E.164 number, the IMS session control layer will send a request to the ENUM service to resolve the E.164 number into a URI. The information contained within that URI may result in an additional DNS request to resolve the hostname in the address (in this example, "alcatel-lucent.com"). Within an IMS interconnect scenario, the returned address will point to the I-CSCF.

In order for most types of peering scenarios to work each of the IMS carriers in the peering relationship needs to be able to reliably route registrations and session requests to the appropriate destination IMS network. To do this, the originating IMS must be able to resolve the DNS and ENUM records for the subscribers in the destination IMS network.

Therefore, an IMS carrier involved in a peering relationship must share DNS and ENUM information with its peering partners through a shared DNS/ENUM infrastructure. The exact nature of how the DNS/ENUM infrastructure is shared is currently a topic for debate.

IMS Interconnect Models

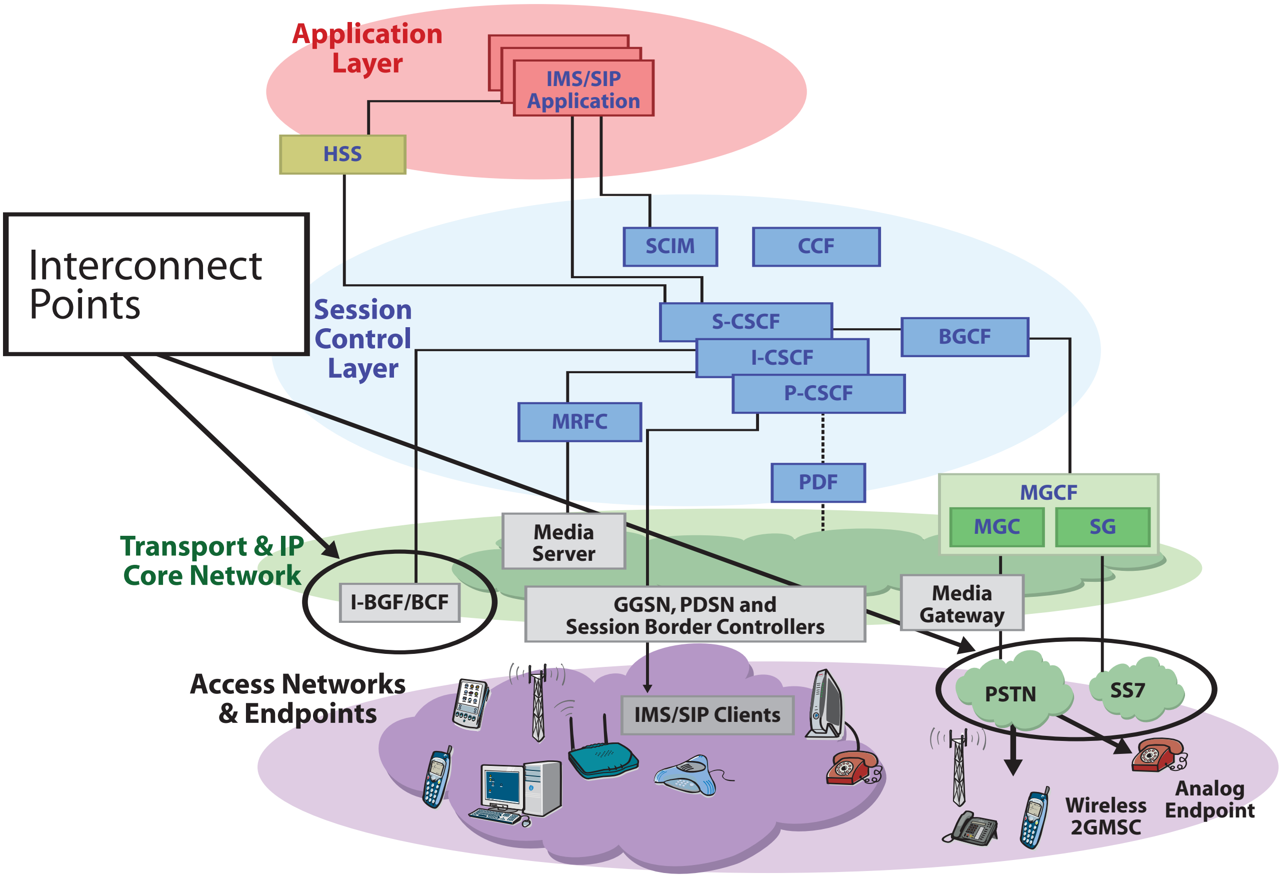
In order to illustrate how the security threats might impact IMS peering, it's helpful to identify the types of interconnect points and to define the possible peering models that can be created by looking at the various ways the interconnect points can be combined.

IMS Interconnect Points

Consider a common IMS architecture model as shown in Figure 1, wherein the functions are organized into four layers – the application layer, the session control layer, the transport layer and the access network layer.

The two primary points of interconnection are through the PSTN interconnect points (the MGCF, signaling gateways, media gateways) and the through border elements – the I-CSCF with Topology Hiding (THIG) in 3GPP release 6, or through the border control function for SIP signaling (I-BCF) and through the border gateway function (I-BGF) for the bearer traffic in 3GPP Release 7 [7, 8]. Within the figures in this document, the primary interconnect point at the core network layer is represented as an Interconnect Session Border Controller (I-SBC). Session Border Controllers can perform activities such as topology hiding along with other security functions, and will be discussed in more detail in Part II of this paper.

Figure 1: The IMS Architecture and Interconnect Points



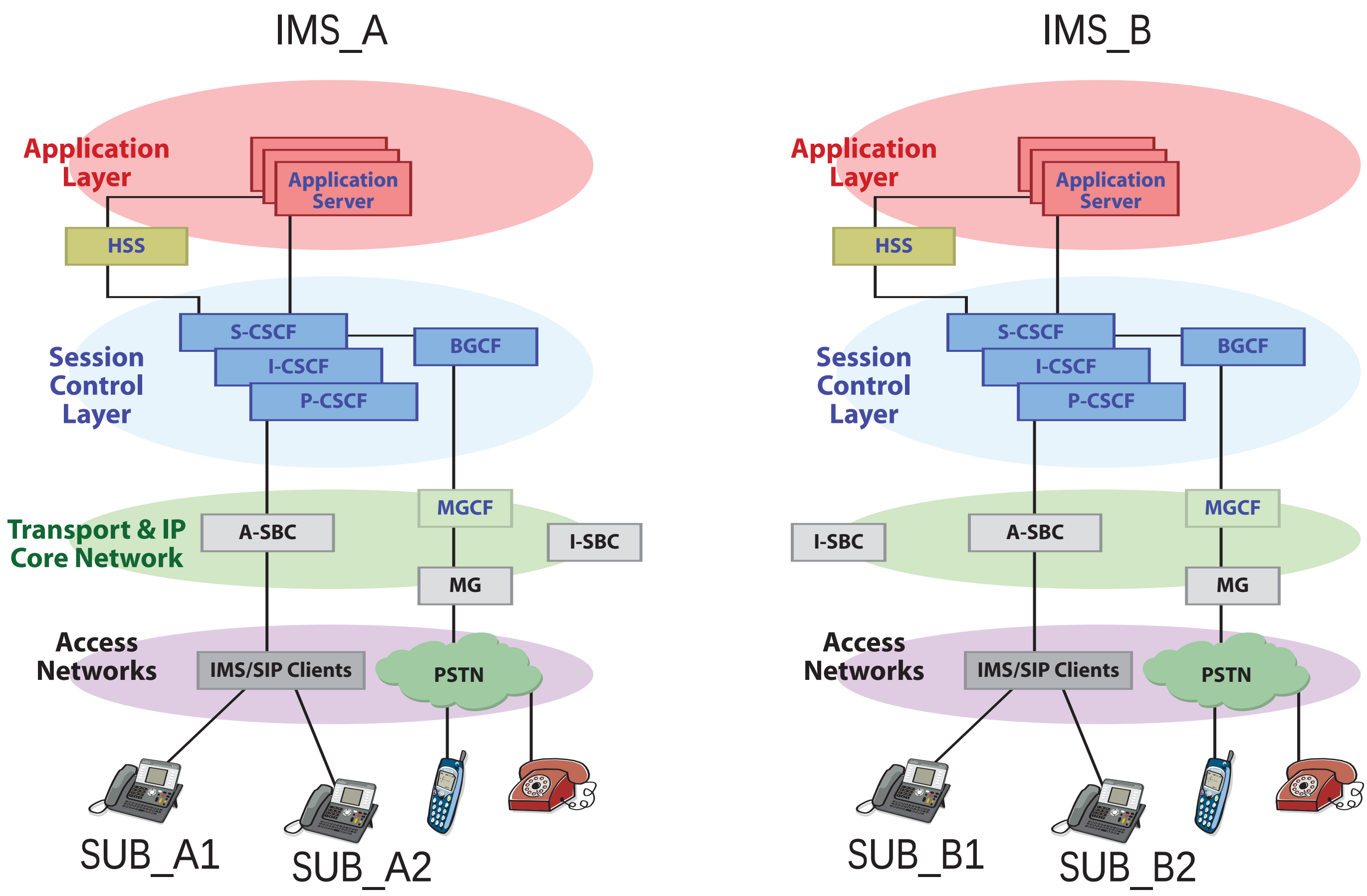
It follows that the types of possible interconnect models will be based on combinations of scenarios where an IMS is interconnected with the PSTN, or interconnected with one or more IMS networks (via IP connections), or it is interconnected both with the PSTN and other IMS networks, either directly or indirectly (via another connected network).

3.2 ETSI Interconnection Scenarios

Of the current IMS published standards, the ETSI TISPAN architecture places the most attention to the requirements for interconnecting multimedia networks. The scenarios described within this section are identified in Annex B of the *TISPAN IMS Functional Architecture* [9]

Throughout the description of these scenarios, we will use the following conventions to distinguish between the multiple IMS networks and connection types defined in the models — The IMS networks will be referred to as IMS_A, IMS_B, and IMS_C, while the subscribers for each of the respective networks will named accordingly – SUB_x#, where *x* represents the home network for the subscriber, and # is a number to distinguish between multiple users on the network. Following this convention, subscribers on IMS network A (IMS_A) would be SUB_A1, SUB_A2, SUB_A3, etc. See Figure 2 as an example.

Figure 2: Naming Conventions for Multiple IMS Architectures



SCENARIO 1: REGISTRATION FROM VISITED NETWORK (ROAMING)

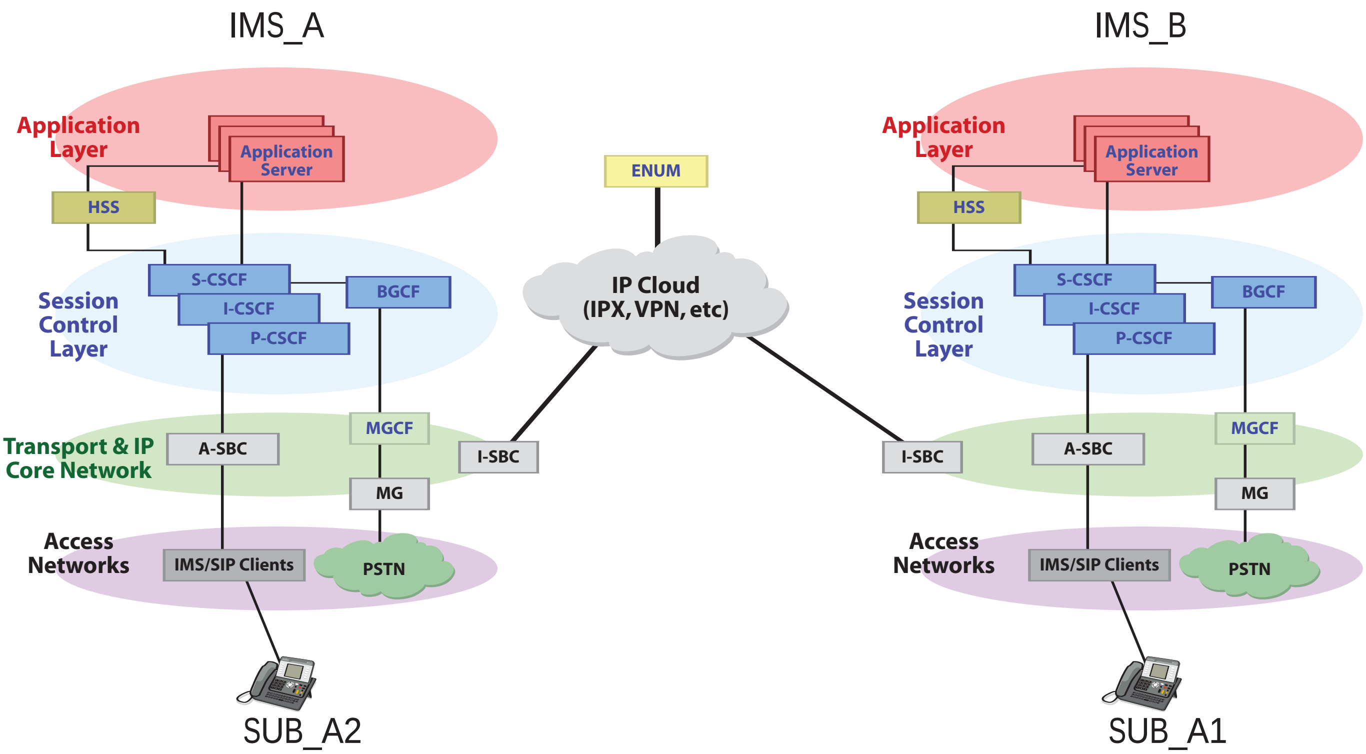
The first scenario would be considered a typical scenario for a roaming user. In this scenario, the SUB_A1 attempts to establish a connection while accessing an IP network connection that is served by IMS_B.

The UE for SUB_A1 will receive address information for IMS_B's P-CSCF via DHCP or other address assignment mechanism. SUB_A1 UE will then contact the P-CSCF for IMS_B and begin the authentication process. Once authentication is complete, SUB_A1 can access services and features provided by his home IMS network, IMS_A.

To illustrate this example, lets say SUB_A1 places a call to SUB_A2. The call request for SUB_A1 will initially be received by the IMS_B P-CSCF, which will forward the request through the IMS_B I-BCF, to the IMS_A I-BCF, then to the IMS_A I-CSCF and on to the IMS_A S-CSCF. Assuming that SUB_A1 is attempting to establish a call for which it has permissions, the call request will then go through to SUB_A1.

Figure 3 illustrates the roaming model described by scenario 1.

Figure 3: Scenario 1: IMS Roaming



SCENARIO 2: IMS SESSION BETWEEN TWO NETWORKS (PEERING)

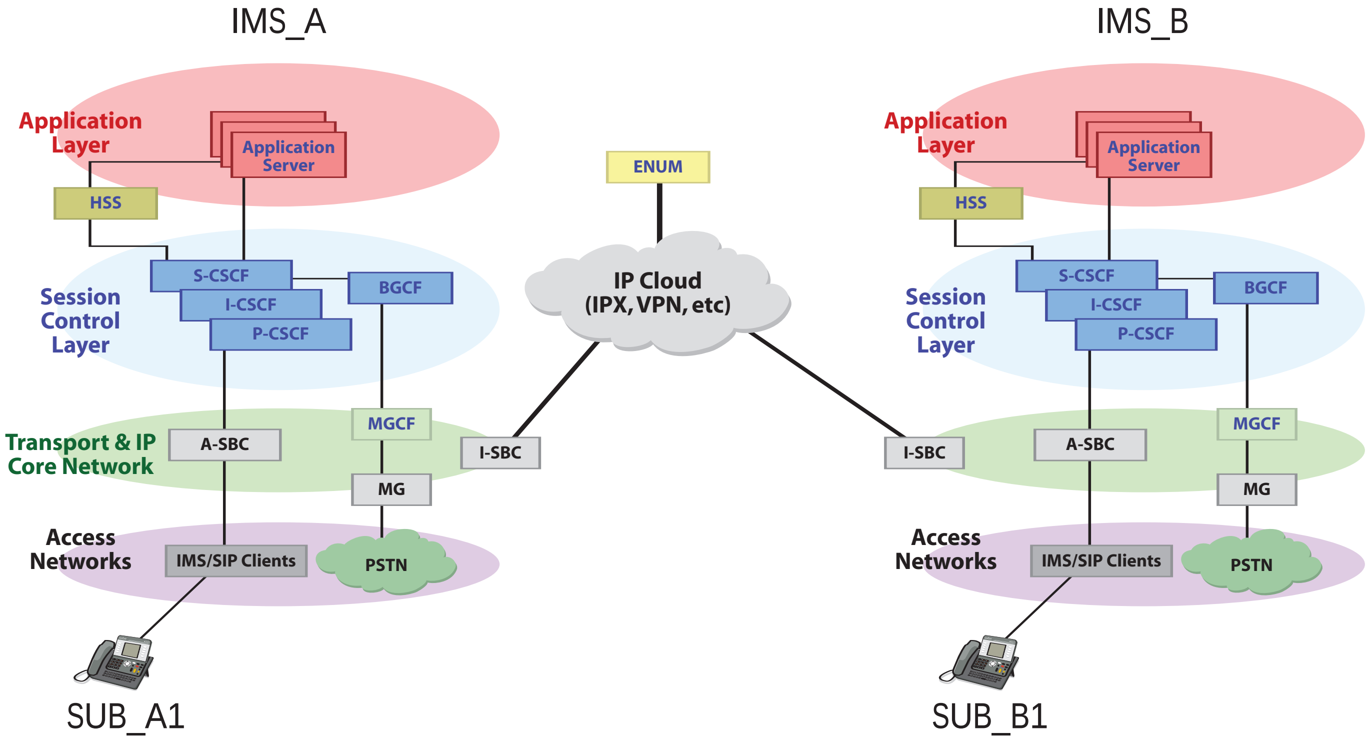
Scenario 2 follows the peering model. SUB_A1 initiates a session with SUB_B1. The CSCF within IMS_A recognizes that it does not serve the subscriber for the destination address, but that SUB_B1 is served by an IMS network with which it maintains a peering relationship.

A simplified call flow for this model would be as follows: The call request from Sub_A1 will go first to the IMS_A CSCFs (P-CSCF and then S-CSCF). The IMS_A CSCFs will pass the session request through the IMS_A I-BCF, which will send through the I-BCF of IMS_B. The IMS_B I-BCF will forward the request through the IMS_B CSCFs (I-CSCF and S-CSCF), which will then pass the request to SUB_B1.

Assuming that a two-way peering agreement exists between IMS_A and IMS_B, the session will be allowed, and users from either IMS network will be able to establish sessions with each another.

Figure 4 illustrates the peering model described by scenario 2.

Figure 4: Scenario 2: IMS Peering

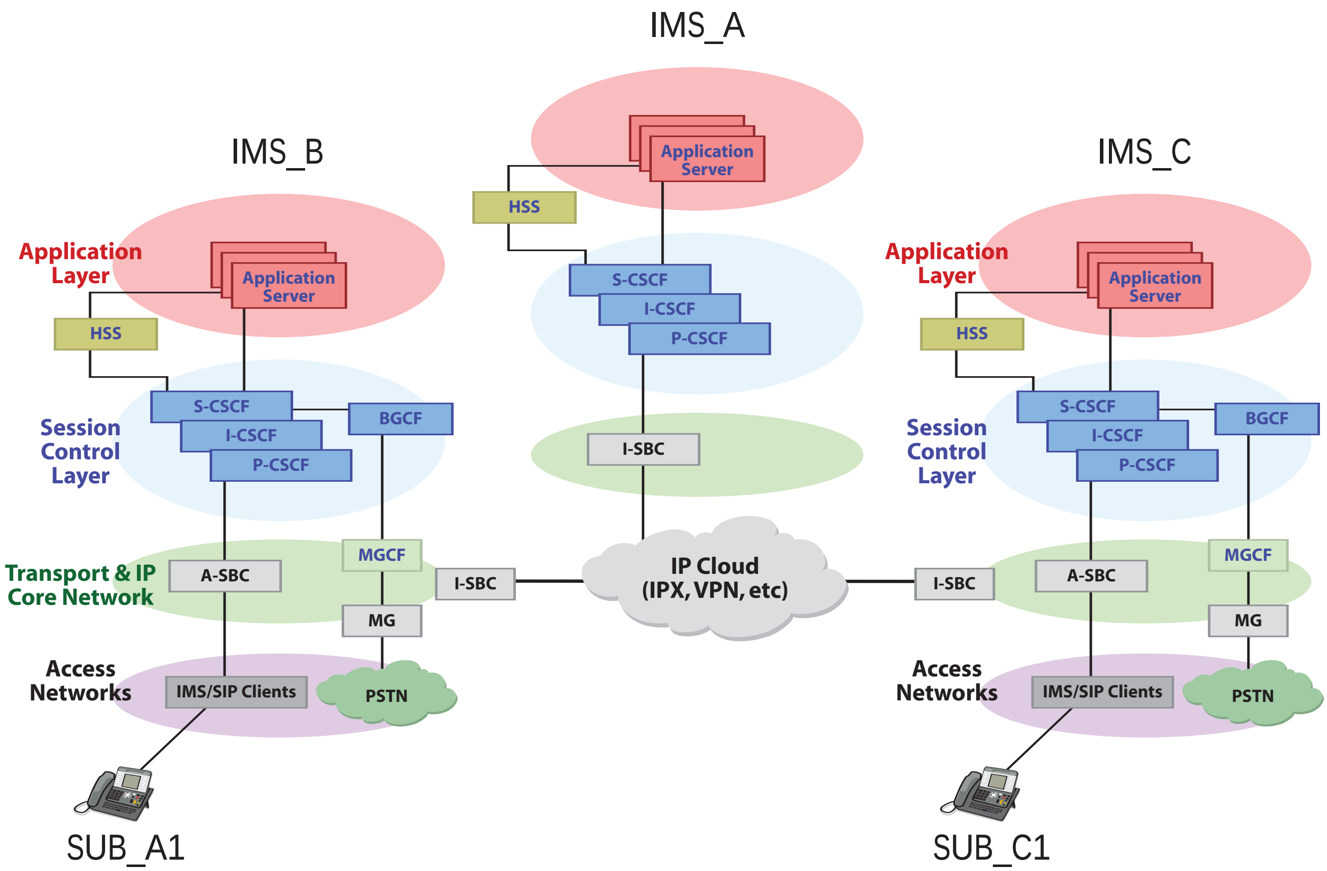


SCENARIO 3: ROAMING AND PEERING

Scenario 3 combines the scenarios 1 and 2. In this model, SUB_A1 establishes an IP network connection while visiting a network served by IMS_B. SUB_A1 then attempts to call SUB_C1 on IMS network C (IMS_C). In this model, a roaming agreement is required between IMS_A and IMS_B. IMS_A must also have a peering agreement with IMS_C.

Figure 5 illustrates the model described by scenario 3.

Figure 5: Scenario 3: IMS Roaming and Peering



A simplified call flow for this model would look like this:

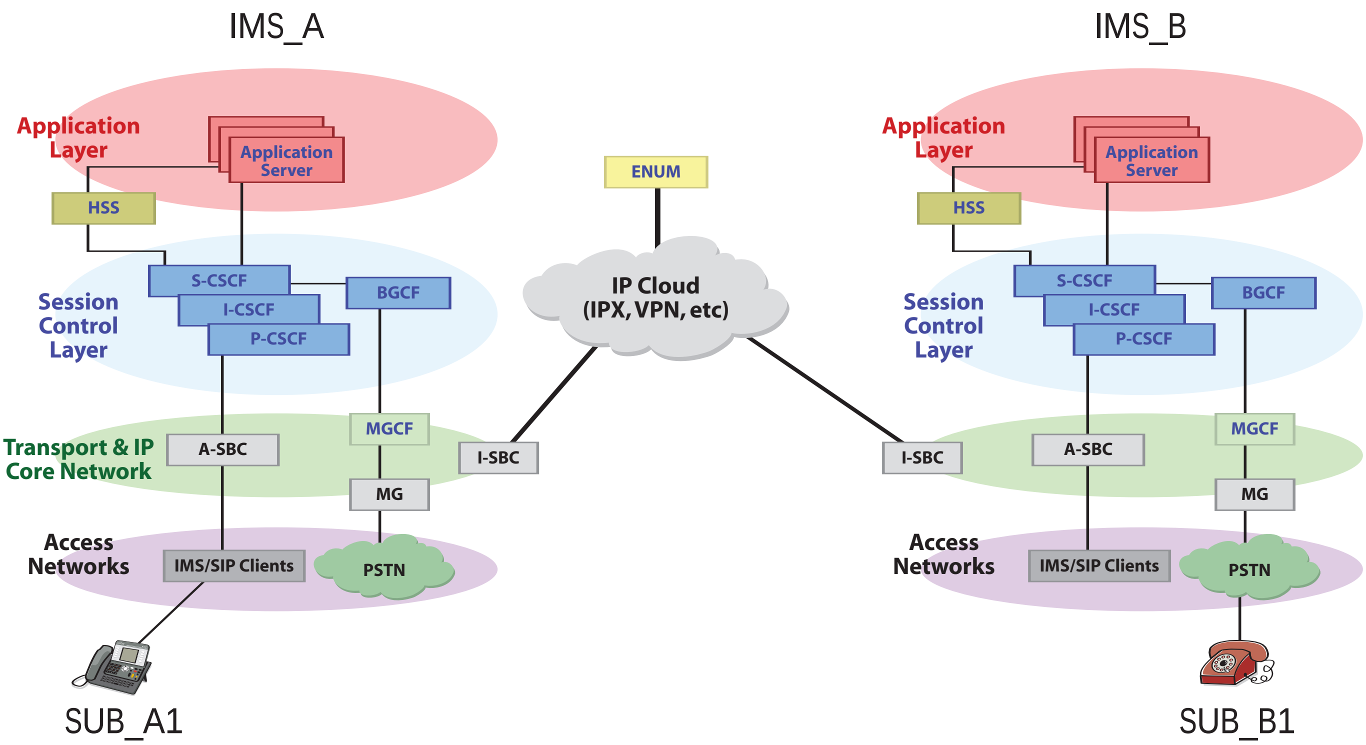
```
SUB_A1 sends call request to P-CSCF of IMS_B
P-CSCF sends request through I-BCF of IMS_B
I-BCF of IMS_B sends request to I-BCF of IMS_A
I-BCF of IMS_A sends request to CSCFs of IMS_A (first I-CSCF, then S-CSCF)
CSCFs of IMS_A send request to I-BCF of IMS_A
I-BCF of IMS_A sends request to I-BCF of IMS_C
I-BCF of IMS_C sends request to CSCFs of IMS_C (first I-CSCF, then S-CSCF)
CSCF of IMS_C sends request to SUB_C1
```

SCENARIO 4: PEERING + PSTN INTERCONNECT ORIGINATOR CONNECTS TO PSTN, PSTN BREAKOUT OCCURS IN A VISITED IMS (NOT THE ORIGINATOR'S HOME IMS)

Scenario 4 combines a peering scenario between IMS_A and IMS_B (scenario 2) with the breakout to the PSTN occurring in IMS_B. One example of this type of interconnection would be where the carrier/owner for IMS_B might have better local PSTN connectivity in a particular region than the owner of IMS_A. This scenario would enable a model in which an IMS carrier maintained no PSTN interconnects within its own network, but instead has established relationships with other IMS carriers for all call breakouts to the PSTN.

Figure 6 illustrates the peering model described by scenario 4.

Figure 6: Scenario 4: Peering and PSTN Interconnect



From a call flow perspective, this would look similar to scenario 2, except that the traffic would flow through the MGCF, SGW, MGW complex for the IMS_B network.

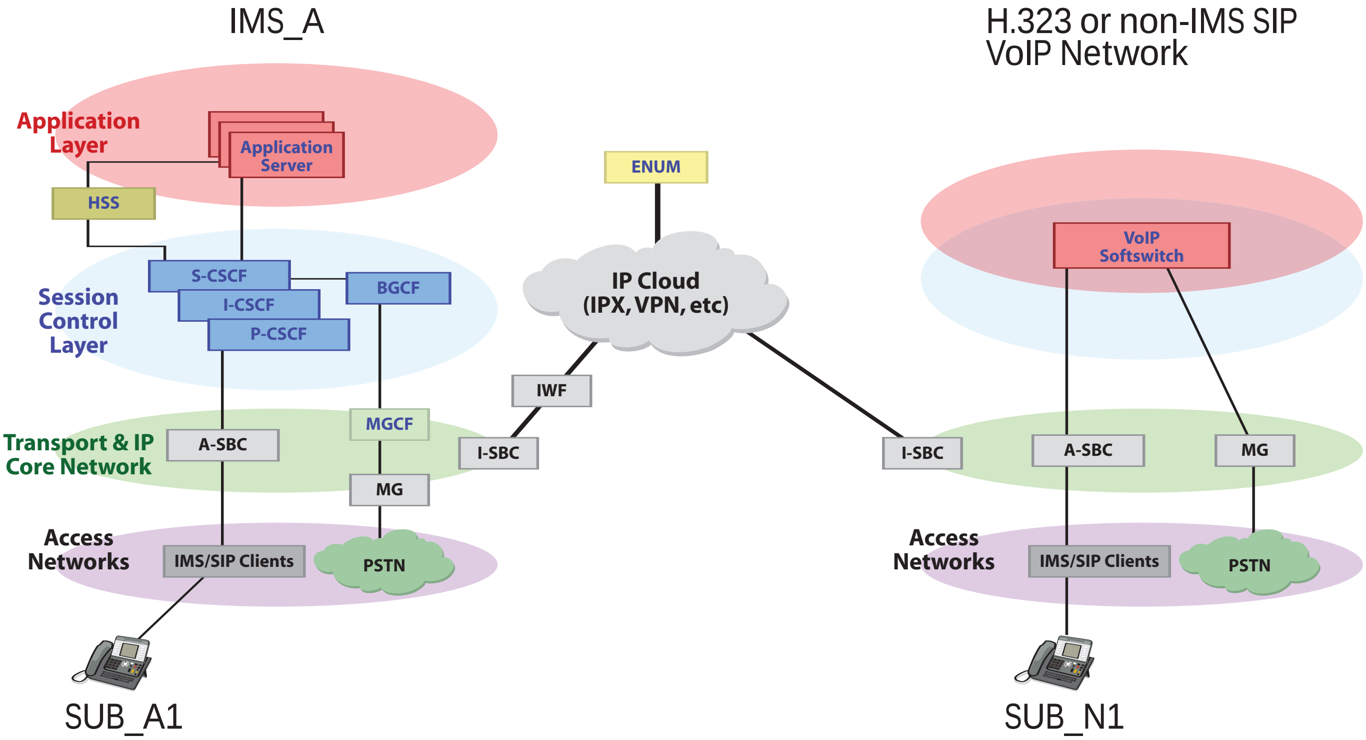
SCENARIO 5: PEERING WITH NON-IMS NETWORK

The scenario 5 model addresses network connections between an IMS network and a non-IMS network, such as an H.323 network or a non-IMS SIP network.

In this scenario, it is likely that there will be a device fulfilling the Inter Working Function (IWF) that will provide translation/normalization services between the IMS and non-IMS networks.

Figure 7 illustrates the peering model described by scenario 5.

Figure 7: Scenario 5: Peering with a non-IMS network

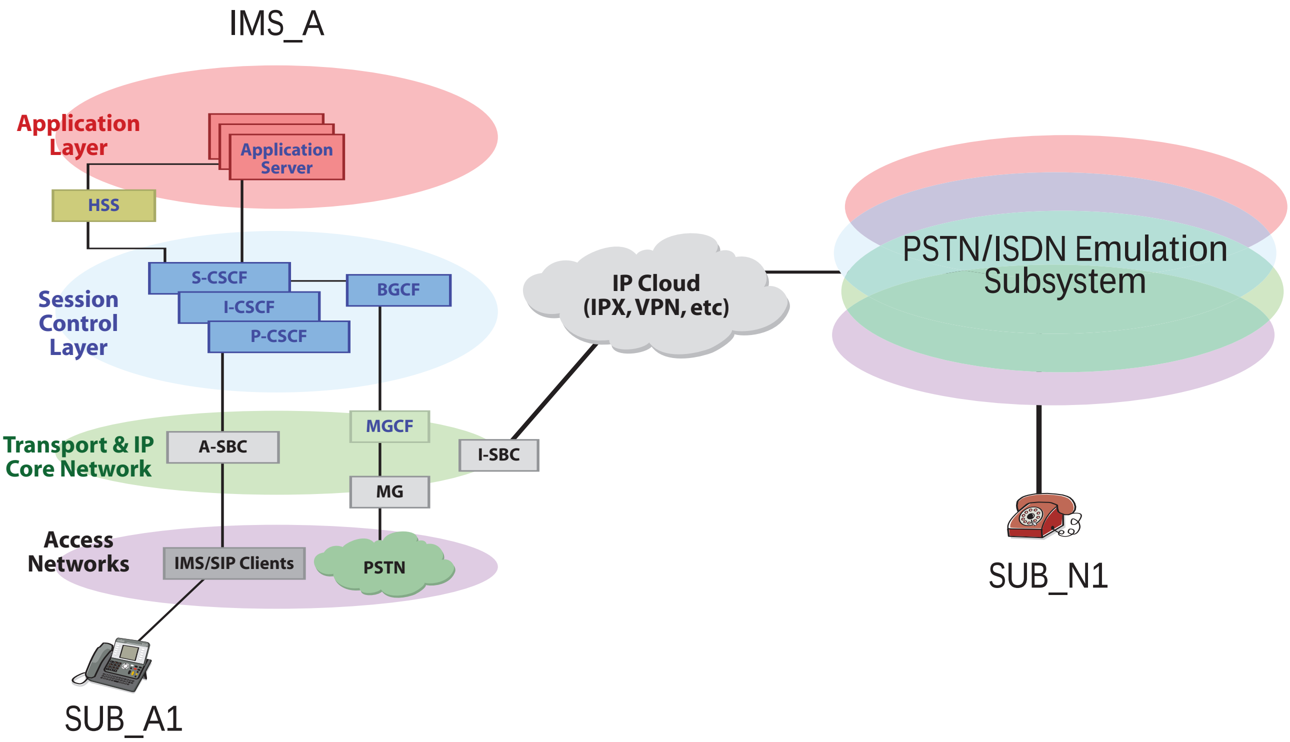


SCENARIO 6: PEERING WITH PES

In scenario 6, the IMS network (IMS_A) establishes a connection with a network that provides PSTN Emulation Services (PES — normally a network that provides H.248 signaling between the Access Gateway Control Function (AGCF) and the media gateways.) In this model, the subscribers within the PES will be utilizing normal PSTN handsets, utilizing an emulated PSTN line connected to a line access gateway (LAG).

Figure 8 illustrates the peering model described by scenario 6.

Figure 8: Scenario 6: Peering with a PSTN Emulation Service



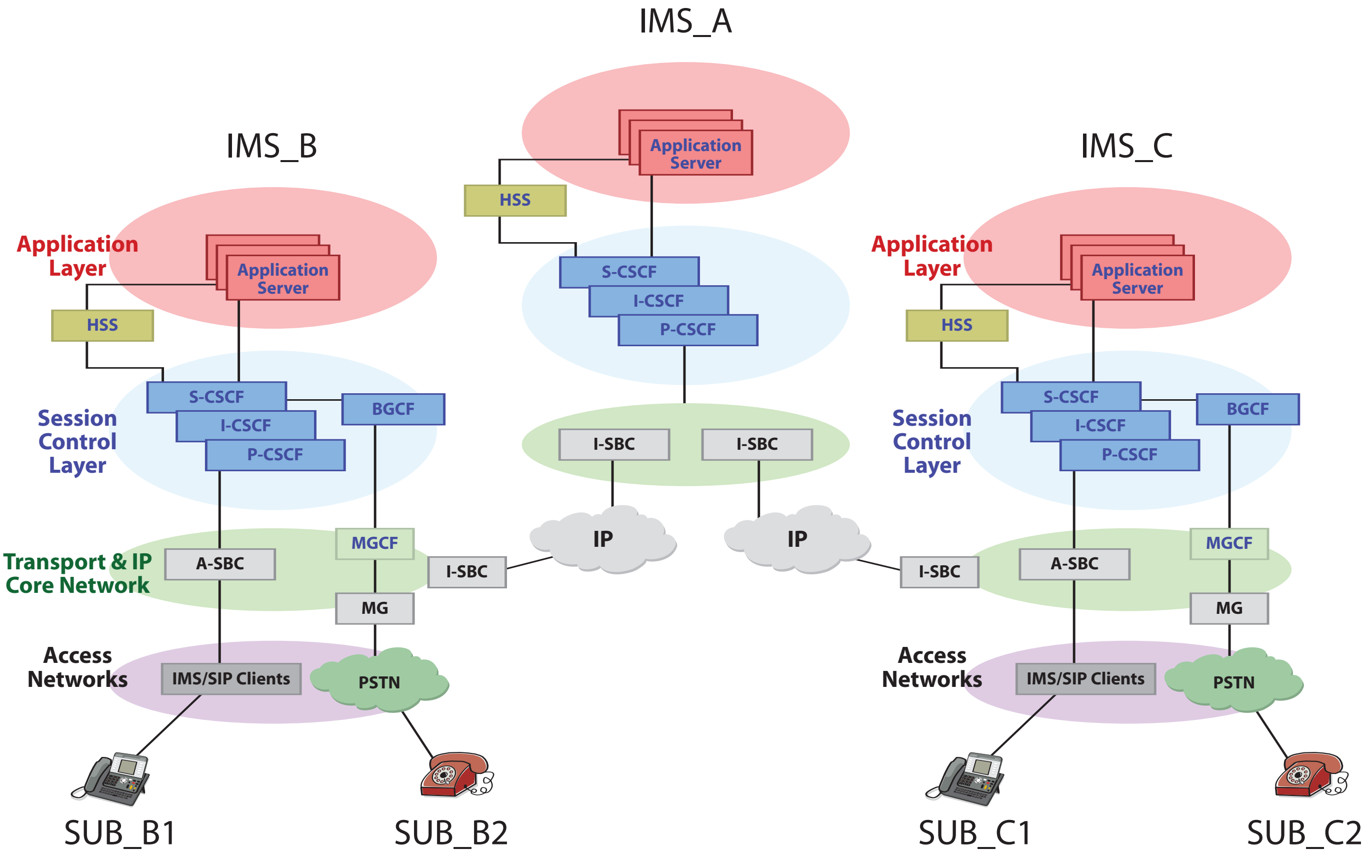
SCENARIO 7: IMS TRANSIT

In scenario 7, IMS_A provides connectivity services between one or more other IMS networks. In this model, IMS_A acts only as a transit network, where traffic originating in one IMS network (IMS_B) travels through a second network (IMS_A) only to be delivered through to a third network (IMS_C).

The IMS transit model enables an IMS carrier to act in the role of a traffic hub, whereby a carrier can establish a relationship with a single network owner (in this example, the owner of IMS_A) to gain reach to subscribers and network breakout points across a number of other IMS (and PSTN) networks.

Figure 9 illustrates the peering model described by scenario 7.

Figure 9: Scenario 7: IMS Transit



ADDITIONAL PEERING/INTERCONNECT MODELS

While the TISPAN interconnect scenarios accommodate a wide variety of peering models, the IMS architecture enables the potential for scenarios that go beyond the TISPAN models.

For example, the distributed nature of IMS lends itself to scenarios where service providers may choose to provide selected services in support of multiple IMS network providers. Consider a situation where a provider chooses to specialize in providing application services – it is conceivable that an application provider could serve subscribers from a number of other IMS networks.

Another example would be where an enterprise might choose to maintain control over selected IMS functions, (such as maintaining subscriber information), while contracting with a service provider to maintain shared session control access facilities, and application services.

While some of these models may require extensions to the existing standards, the groundwork for many of them has already been laid. These arrangements may introduce additional security considerations that will need to be carefully evaluated before the models can be implemented.

This concludes Part I of this white paper. Part II of the paper will address the security considerations related to IMS interconnection, peering and roaming models by describing the basic IMS security fundamentals, identifying security threats associated with IMS, and describing how those threats may apply to multi-IMS interconnect scenarios.

References

[1] 3rd Generation Partnership project. *Access Security for IP-Based Services*, 3GPP TS 33.203, October 2006

[2] European Telecommunications Standards Institute (ETSI). *Characteristics of the IP Multimedia Services Identity Module (ISIM) Application*, ETSI TS 131.103, December 2005

[3] 3rd Generation Partnership Project. IP Multimedia Call Control Protocol Based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3, 3GPP TS 24.229, October 2006

[4] 3rd Generation Partnership Project. *3GPP System to Wireless Local Area Network (WLAN) Interworking*, 3GPP TS 24.235, September 2006

[5] J.Deshpande, et. al., End-to-end VoIP and Real-Time Multimedia Peering across MSOs and Other Service Provider IP Networks, Bell Labs, Lucent Technologies, Internal Memorandum

[6] P. Faltstrom, M. Mealling. The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM), RFC 3761, Internet Engineering Task Force, April 2004

[7] 3rd Generation Partnership Project. *IP Multimedia Subsystem (IMS) Stage 2, Release 6*, TS 23.228 V6.14.0, June 2006

[8] 3rd Generation Partnership Project. *IP Multimedia Subsystem (IMS) Stage 2, Release 7*, TS 23.228 V7.5.0, October 2006

[9] European Telecommunications Standards Institute (ETSI). Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS) Functional Architecture, ETSI ES 282 007, June 2006

List of Acronyms

3GPP	3rd Generation Partnership Project
AGCF	Access Gateway Control Function
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
ENUM	tElephone NUmber Mapping
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
I-BCF	Interworking Border Control Function
I-BGF	Interworking Border Gateway Function
I-CSCF	Interrogating Call Session Control Function
IPSec IKE	IP Security Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
I-SBC	Interconnect Session Border Controller
ISIM	IMS Subscriber Identification Module
ISP	Internet Service Provider
IWF	Inter Working Function
LAG	Line Access Gateway
LAN	Local Area Network
MGCF	Media Gateway Control Function
MMS	Multimedia Message Service
NAP	Network Access Point
P-CSCF	Proxy Call Session Control Function
PDG	Packet Data Gateway
PES	PSTN Emulation System
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol
SMS	Short Message Service
SP	Service Provider
THIG	Topology Hiding Internetworking Gateway
TISPAN	Telecommunications and Internet Converged Services and Protocols for Advanced Networking
UE	User Equipment
URI	Uniform Resource Identifier
VoIP	Voice over IP
VPN	Virtual Private Network

About the Author

Morgan Stern
Principal Consultant, Global Convergence Center of Excellence
Alcatel-Lucent Services

Morgan Stern provides guidance to service providers in the development and implementation of network evolution initiatives. In his role, he draws upon experience gained during more than 15 years in the telecom and IT industries assisting clients in areas such as network optimization, VoIP migration, IMS architecture design, IT integration, and network convergence. He is the author of three books and a variety of articles and papers on IP network services, network security, and directory services.

www.alcatel-lucent.com

Alcatel·Lucent