



# Cisco ITP MAP Gateway for Public WLAN SIM Authentication and Authorization

## Executive Overview

An increasing number of Global System for Mobile Communications (GSM) operators are recognizing the need for high-speed wireless data services. Such operators have decided to roll out wireless LAN (WLAN) technologies within their service and access portfolios as a complement to existing 2.5G and future third-generation cellular (3G) access and services.

Because proper user authentication has been and will continue to be a key success factor for access to its services, Cisco Systems has embarked on an effort to enable authentication of WLAN subscribers using the existing and well-proven GSM-based user authentication and existing GSM provisioning facilities.

The authentication process is very important to any user transaction. Whereas WLAN early market entry systems have based their authentication process upon username and password, initially using credential entry via a Secure Hypertext Transfer Protocol (HTTPS) Web page, these will evolve toward Extensible Authentication Protocol (EAP [RFC 2284])—or 802.1X-based solutions. EAP or 802.1X adoption will facilitate the migration to authentication schemes that support higher-entropy shared secrets and encryption key exchange, for example, comparable to those techniques currently used within the GSM networks.

Recognizing the need to bridge the native WLAN authentication and authorization mechanisms with the existing proven GSM-based authentication and provisioning model, Cisco Systems has introduced the Cisco IP Transfer Point (ITP) Mobile Application Part (MAP) Gateway function. The Cisco ITP MAP Gateway function enables existing GSM service providers to fully integrate 802.11 technology into their existing GSM network using subscriber-identity-mobile (SIM) cards. In this capacity, the Cisco ITP MAP Gateway is part of the Cisco Public WLAN solution architecture.

In addition to the Cisco ITP MAP Gateway functionality for WLAN SIM authentication and authorization, additional MAP-based features such as “SMS routing” are available. Details regarding this product, the ITP Multi-layer Router (MLR), are covered in a separate whitepaper.

## Overview of the Cisco ITP MAP Gateway Solution

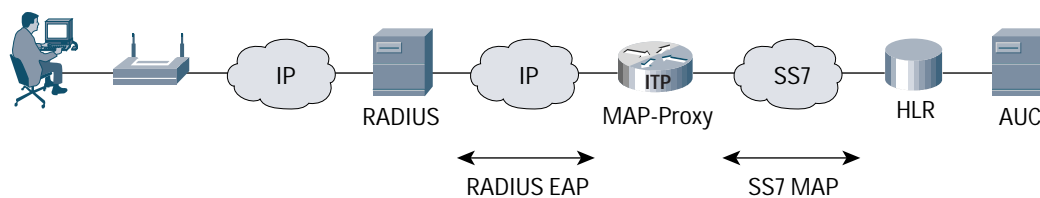
The Cisco MAP Gateway merges both WLAN EAP or 802.1X and GSM SIM authentication mechanisms transparently, so that the mobile node performs SIM authentication to the GSM Authentication Center (AUC) through a standard EAP Remote Access Dial-In User Service (RADIUS)-based authentication. The benefit is that the GSM operator, when implementing WLAN hot spots into the network, can keep the same subscriber provisioning, authentication, and service authorization that are already in place for GSM services.

Given that the WLAN client is equipped with a SIM card and the appropriate SIM card reader, the Cisco ITP MAP Gateway establishes a bridge between the RADIUS-based authentication used in WLAN networks and the SIM-based authentication used in GSM networks, in a fully transparent manner as shown in Figure 1:

- From the standpoint of the GSM Home Location Register (HLR), the Cisco ITP behaves just like another node in the Signaling System 7 (SS7) network (typically corresponding to a home public land mobile network [HPLMN]-based Visitor Location Register [VLR], as explained later in this document).
- From the RADIUS server standpoint, the Cisco ITP behaves like another RADIUS server.

Figure 1

The Cisco ITP MAP Gateway merges the WLAN and the GSM authentication together.



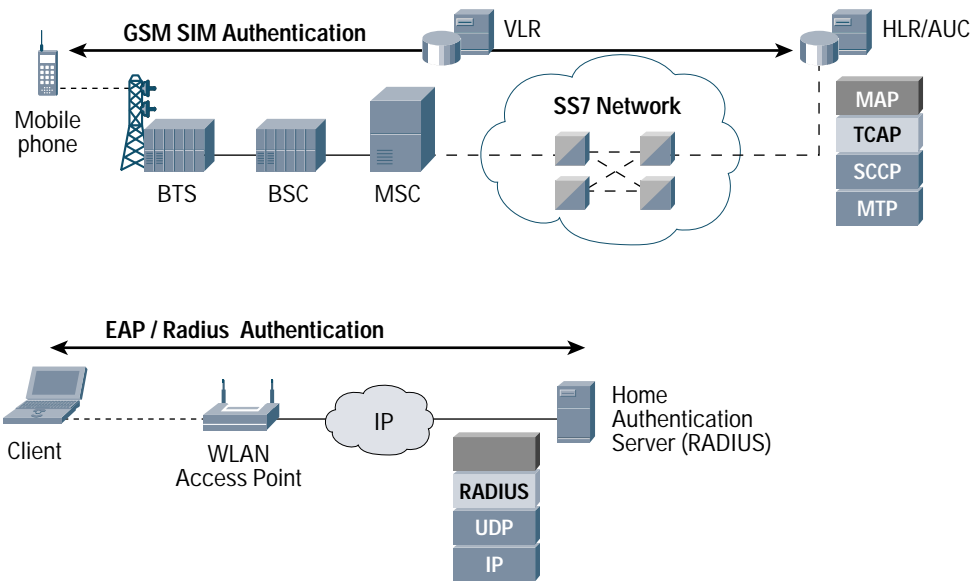
## Benefits of the Cisco ITP MAP Gateway

Assume a concurrent deployment of GSM and WLAN technologies within the same service provider's network, but in complementary geographical areas.

As shown in Figure 2, without a MAP gateway solution, the service provider with both WLAN and GSM networks deployed has to keep the two authentication signaling processes totally separated, leading to separate provisioning expenses, and providing a non-homogeneous quality of service throughout the two authentication services. GSM users still authenticate to the MAP SS7-based HLR and AUC, whereas WLAN users (who are likely to be the same as the GSM users, but roaming into a different coverage area) authenticate through a combined mechanism, likely to be 802.1X or EAP and RADIUS based.

Figure 2

WLAN and GSM authentication signaling processes are natively separated.

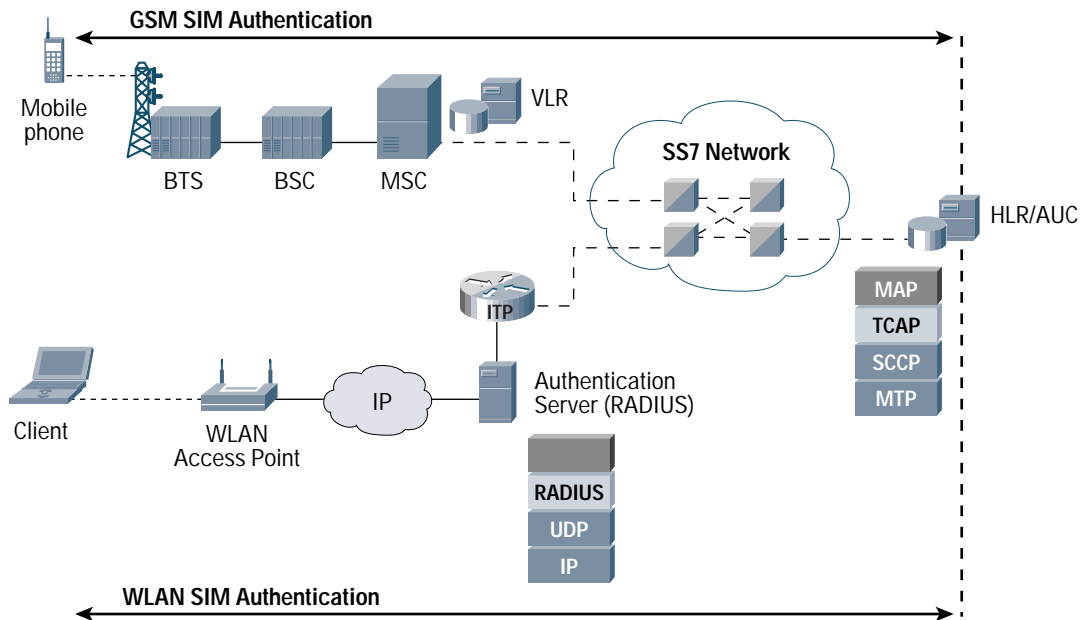


The introduction of a MAP gateway function in the cellular network (refer to Figure 3) enables the service provider to integrate the WLAN and GSM technologies into the same security mechanism. Benefits are numerous:

- *A homogeneous and more secure authentication*—The Cisco ITP MAP Gateway function enables a WLAN authentication based on the SIM card, where the subscriber identity and high entropy secret is stored in a tamper-resistant memory. SIM-based authentication is more robust to hacking than the typical username-and-password authentication used in traditional WLAN networks. SIM authentication has a very low risk of fraud and cloning because it is the most used mechanism for authentication currently in place in cellular networks.
- *The reuse of the existing provisioning system already available in the GSM network*—By using a MAP gateway, the operator can take advantage of its existing GSM HLR AUC for service provisioning and authorizing access, and thus reuse the existing process already in place for access to GSM-based services. Without a SIM-based authentication process enabled by the Cisco MAP Gateway, the right of access to WLAN service would necessitate a new and independent process, forcing the operator to implement, provision, and maintain a dedicated database—in addition to the existing HLR and AUC.

Figure 3

The Cisco ITP MAP Gateway enables the operator to merge both WLAN and GSM access security together.



In order to fully understand the function provided by the Cisco ITP MAP Gateway, it is useful to have a clear understanding of the distinct security mechanisms used respectively for WLAN and GSM authentications. Hereafter are described in more details the current authentication features respectively in place in WLAN- and GSM-based networks, and how the MAP gateway allows both features to merge into a common optimal feature set for both WLAN and GSM networks.

### Conventional EAP over 802.11 and RADIUS-Based Authentication

IEEE 802.1x is a standard for port-based network access control. It ensures that only authenticated users are allowed access to the network through the WLAN access point. The IEEE 802.1X standard was initially designed to enable authenticated access to IEEE 802 media, including Ethernet, Token Ring, and 802.11 WLANs. The 802.1X standard provides an authentication framework for WLANs, allowing a user to be authenticated by a central authority, for example, a HPLMN. The specific algorithm that is used to determine whether or not a user is authenticated is left open, and multiple options are possible.

Notably, 802.1X supports the EAP, a general protocol for authentication that supports multiple authentication mechanisms. EAP works on Ethernet, Token Ring, or WLANs. In a WLAN with 802.1X, a user (known as the supplicant) requests access to an access point (known as the authenticator).

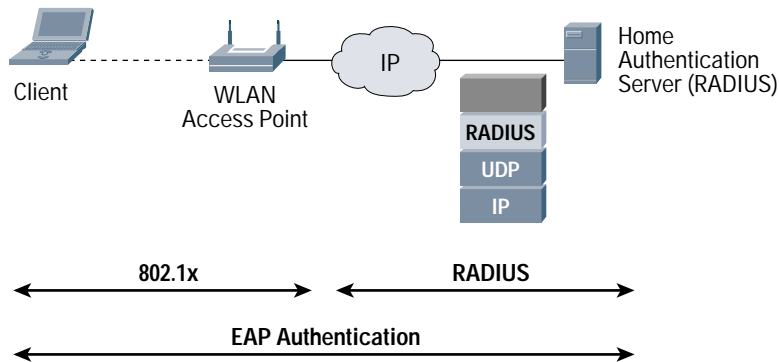
The authentication server is likely to use the RADIUS protocol between the server and the authentication peer on the access point. In this case, EAP messages are encapsulated using the RADIUS protocol to allow communication between the EAP supplicant and the back-end authentication server.

As Figure 4 shows, three components are involved in this combined EAP authentication process:

1. The *client device* that requests access to the WLAN service—It must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system.
2. The *RADIUS authentication server* that performs the actual authentication of the client—The authentication server validates the identity of the client and notifies the access point whether or not the client is authorized to access WLAN services. Because the access point acts as the proxy, the authentication service is transparent to the client.

- The *access point* that controls the physical access to the network based on the authentication status of the client—It acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The access point includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

Figure 4  
Combined 802.1x and RADIUS Authentication with EAP



### Limitations of EAP and Other Non SIM-Based Authentication Mechanisms

For WLAN access, a variety of different authentication applications have already been developed and are currently available in the industry. Generally, experts relate the level of security to the nature and the place of storage of the long-term secret key used for authentication between the client and the server. Three kinds of methods are available today:

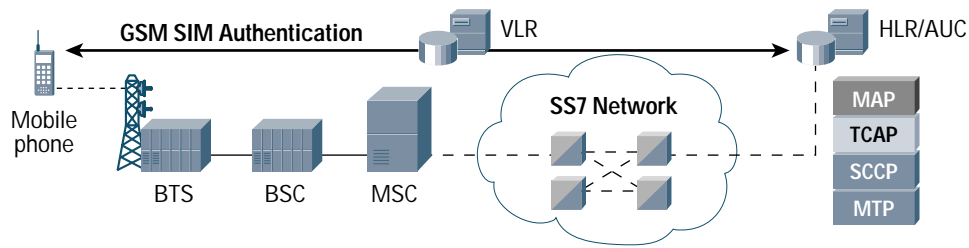
- The long-term secret key can be an alphanumeric password exchanged between the client and the user. This method is the lowest entropy, meaning it is the most easily attacked, for example, via a dictionary attack.
- The long-term secret key can be a more complex structure, stored in the hard drive of the user's device, whether this device is a PC or a personal digital assistant (PDA), for example. Whatever mechanism is used for actual authentication (EAP or non-EAP), the long-term key is still easily retrievable, because the operating system of the device itself is not tamper proof and allows ways to access information on the hard disk.
- The most secure and robust mechanism consists of keeping the long-term secret key in a closed environment such as a Smartcard. Most banking and commercial organizations are pushing today for the implementation of such mechanisms into their users devices, because this method is tamper resistant and provides application level security. The Smartcard provides a safe place to store valuable information such as private keys, passwords, or personal information such as health maintenance data. It is also a secure place to perform secure processes such as performing a public key or private key encryption.

### SIM-Based Authentication in GSM Networks

GSM networks use a Smartcard-based method for user authentication and data encryption. The SIM card is a Smartcard inserted in the user's handset, defining uniquely the user through an identity number named the international mobile subscriber identity (IMSI).

The SIM authentication is an end-to-end mechanism between the user and the AUC, located inside the user's database, named HLR, as shown in Figure 5.

Figure 5  
GSM SIM Authentication Architecture.



Three components are involved in the GSM authentication process:

1. *Mobile station*—The Mobile Station has a SIM card that contains an IMSI and a secret key ( $K_i$ ) shared with the AUC and authentication and key exchange algorithms, A3 and A8, respectively.
2. *Mobile Switching Center (MSC) and VLR*—These two components could be different, but they are shown as one for simplification.
3. *HLR and AUC*—These two components could be different, but they are shown as one for simplification.

The GSM authentication is based on a challenge-response mechanism. The authentication algorithm that runs on the SIM is given a 128-bit random number (RAND) as a challenge. The SIM then runs an operator-specific confidential algorithm, A3, which takes the RAND and a secret key  $K_i$  stored on the SIM as input ( $K_i$  is allocated with IMSI at subscription time), and produces a 32-bit response secret response (SRES). Another algorithm, A8, is used to compute a 64-bit long key  $K_c$  with  $K_i$  and RAND. The  $K_c$  key is originally intended to be used as an encryption key over the air interface.

SRES values computed by SIM and AUC are compared by the AUC, and authentication is granted if those values match.

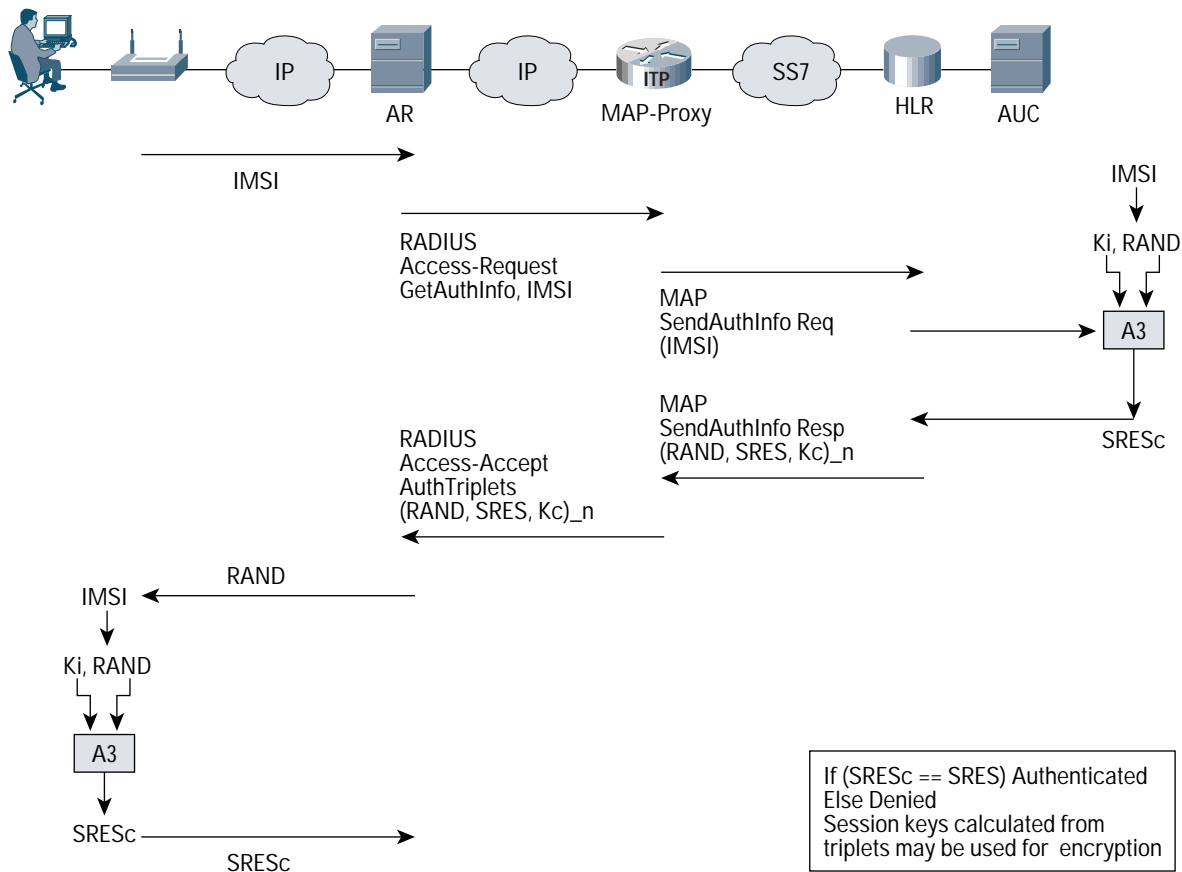
### Combined EAP SIM Authentication Through Cisco ITP

As described earlier in this document, the Cisco ITP MAP Gateway establishes a bridge between the RADIUS server and the HLR and AUC, such that the user establishes a SIM-like authentication to the GSM HLR and AUC:

- From the standpoint of the HLR, the Cisco ITP behaves like a VLR.
- From the standpoint of the RADIUS server, the Cisco ITP behaves like another RADIUS server.

Figure 6 shows the high-level data flow between the client, the RADIUS server (here, the Cisco Access Registrar), the Cisco ITP, and the HLR and AUC.

Figure 6  
High-Level Data Flow for EAP SIM Authentication Through Cisco ITP.



Note: This is a partial data flow that only shows the portion involving the IMSI.

### Differences with the GSM SIM Authentication

EAP and SIM are different from GSM, in the sense that several RAND challenges are used for generating several 64-bit Kc keys, which are combined to constitute a longer session key required for the specific 802.11 cipher suite.

EAP and SIM also enhance the basic GSM authentication mechanism with network authentication. When GSM authentication was defined, the rogue base transceiver station (BTS) was perceived not to be a security threat. Hence, EAP SIM defines a client challenge of the network, whereby the RAND challenge is accompanied with a message authentication code in order to provide mutual authentication.

### EAP SIM Process: A Mutual Authentication

#### Network Authentication

In the first step, the client responds to the EAP or SIM or Start request by transmitting a 16-byte (128-bit) random number generated by the supplicant called Nonce. The RADIUS server uses that random number, together with user's IMSI, Ki, and two or three GSM random numbers RAND[n], to calculate the 20-byte Media Access Control (MAC) of the SIM or EAP challenge packet, MAC\_RAND, returned to the client in the second step. The challenge packet also includes the two or three random numbers RAND[n] used for generating the session keys. The client first authenticates the challenge (and, therefore, the network) by calculating a MAC\_RAND of its own and comparing it to the one sent by the network. If there is a match, the client knows that it is communicating with an authentication server that has connectivity to the user's AUC, implicitly indicating that there is an established trust relationship between the user's HPLMN and the WLAN access point operator.

## Client Authentication

Then, the client uses RAND[n] and the GSM A3 and A8 algorithms to calculate the matching SRES[i] and Kc[n], respectively. IMSI, Ki, and SRES[n] are used to calculate a new MAC, MAC\_SRES, which is returned as the response. The network uses MAC\_SRES to authenticate the client; note that SRES[n] is never directly returned over the air, and consequently an eavesdropper is unable to use RAND or SRES pairs to attack the secret key, Ki.

### Benefits: A More Secured Authentication Mechanism

Overall, the Cisco ITP MAP Gateway enables the network to provide the same level of protection as in the GSM and Universal Telecommunications System (UMTS) cellular networks. The data encryption keys Kc[n], that are used in the calculations for MAC\_RANDOM or MAC\_SRES, are never sent over the air. Kc[n], as well as IMSI, Nonce and the version information, are used by the network and the client to independently calculate the cipher key, Kc, which will be used for encrypting data on the air link. SRES is not carried over the air either. There is no known way to obtain complete GSM triplets by mounting an attack against EAP or SIM.

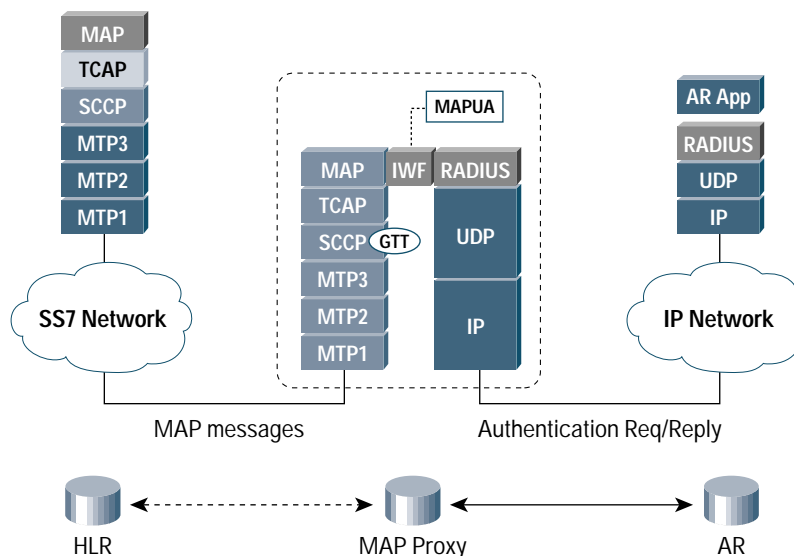
### Cisco ITP MAP Gateway Protocol Compliance and Interoperability

#### Compliance with Existing Standards

Figure 7 provides a closer look to the interfaces between the Cisco ITP MAP Gateway, a RADIUS server, and a traditional time-division multiplexing (TDM)-based SS7 HLR. The Cisco MAP Gateway has successfully interoperated in mobile operator networks with the industry-leading HLR and Signaling Transfer Point (STP) suppliers. Interoperability with the RADIUS Cisco Access Registrar has also been successfully achieved.

Figure 7

Cisco ITP MAP Gateway Interfacing a Cisco RADIUS Server and a Traditional SS7 HLR.

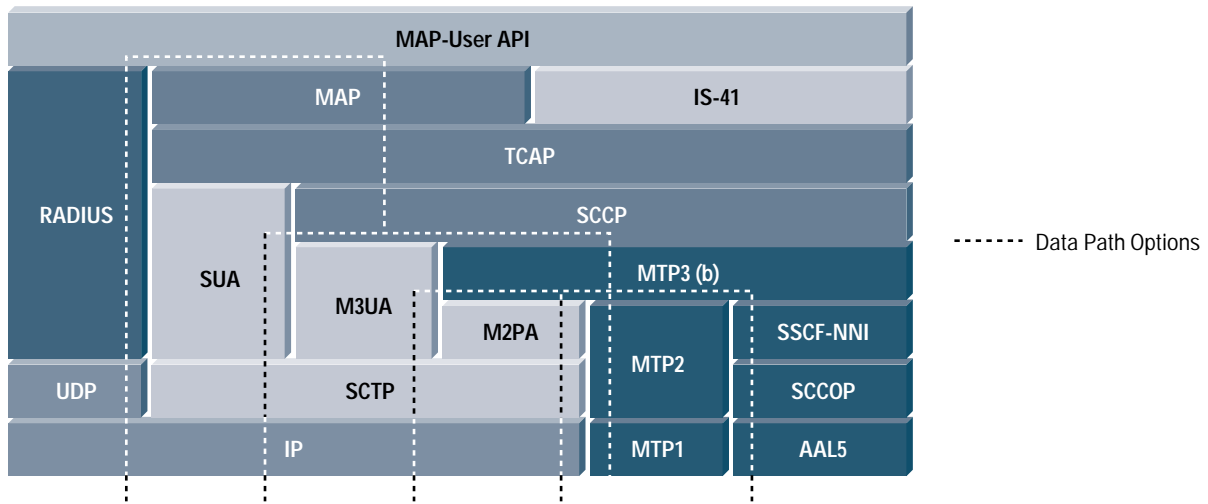


In addition, the Cisco MAP Gateway can also interoperate with nontraditional SS7 end nodes, such as Internet Engineering Task Force (IETF) Sigtran M3UA- and Sigtran SCCP User Adaption (SUA)-based HLRs. Sigtran is an IETF-based standard for SS7-over-IP (SS7oIP) applications, such as those designed for UMTS networks.

More specifically, as shown in Figure 8, the Cisco ITP can support a variety of implementations to interface the SS7 network:

- Traditional SS7 protocol links over ITU or ANSI message transfer part 1, part 2, and part 3.
- High-speed ATM-based links over ATM Adaption Layer 5 (AAL5), Service Specific Connection Oriented Protocol (SCCOP), and Service Specific Coordination Function (SSCF) Node-to-Network Interface (NNI) protocols
- IETF Sigtran M2PA Peer-to-Peer Protocol for MTP3 over IP
- IETF Sigtran Client Server M3UA for SCCP over IP and SUA for MAP over IP protocols, for IP native SS7 HLR applications

Figure 8  
Cisco ITP MAP Gateway Protocol Stack.



### Further Compliance with Standards

The Cisco solution complies with SIM EAP, which specifies an EAP mechanism for authentication and session key distribution using the GSM SIM. SIM EAP is on its way to becoming a full standard in IETF.

### Cisco ITP Configurable MAP Gateway Features

#### EAP SIM-Based Authentication

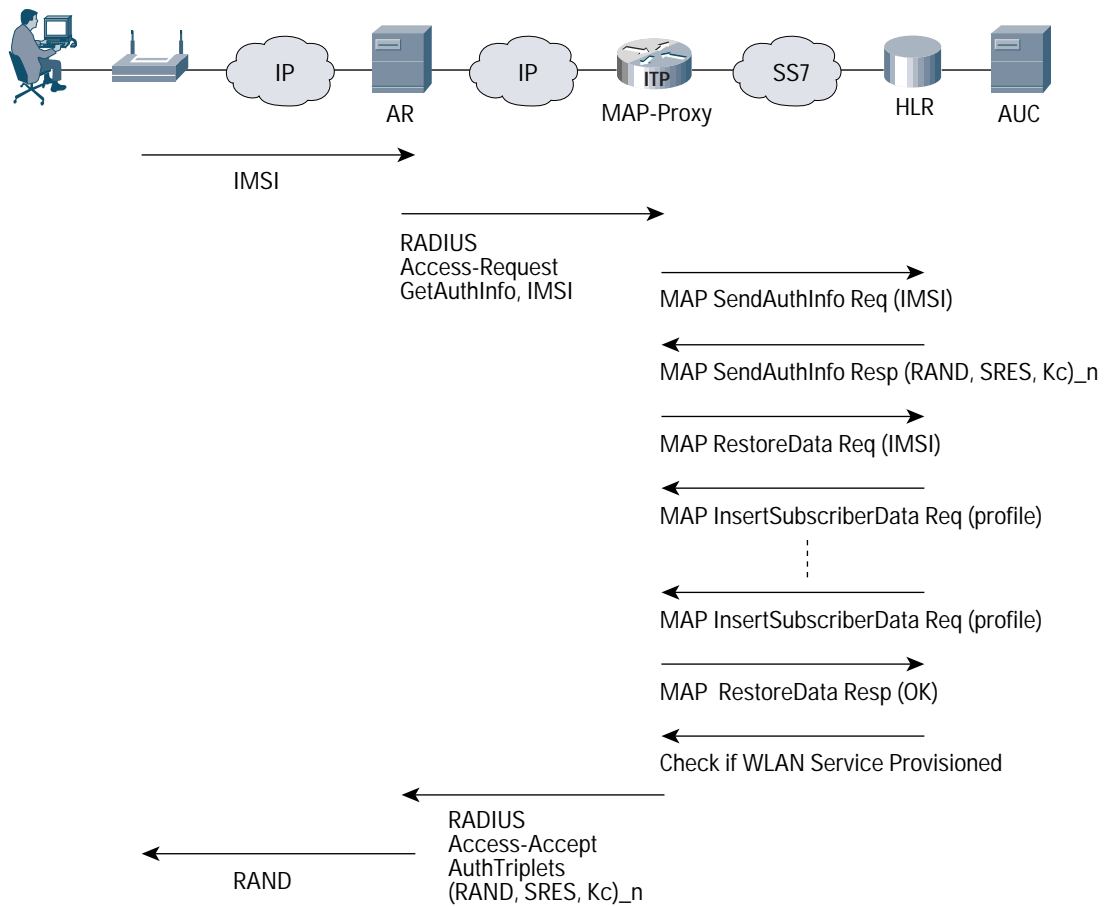
When an authentication request is sent to the RADIUS server, the RADIUS server forwards the authentication request to the Cisco ITP. The Cisco ITP sends a MAP Send-Authentication\_Info request to the AUC to retrieve authentication triplets, and then returns those triplets embedded with the authentication response to the RADIUS server. The RADIUS server then performs a standard authentication response to the client.

#### SIM-Based Authorization

This feature allows the operator to authorize a subscriber only if that subscriber has subscribed to the WLAN service, assuming EAP SIM authentication is already successful (See Figure 9).

Allowed services are usually in the subscriber profile in the HLR. However, most HLRs do not have dedicated fields for WLAN service yet, because it was not part of the European Telecommunication Standards Institute (ETSI) recommendations. Standard bodies are currently working on implementing this feature, but meanwhile, WLAN can use some services fields that are little used. The two types of fields supported by the Cisco ITP are the bearer service (BS) and the teleservice (TS). Any BS or TS existing service in the HLR subscriber profile can be used, and is configurable (though operators are generally going with BS 31).

Figure 9  
Data Flow Overview for Authentication and Authorization Process.



### Caching of Triplets

The Cisco ITP MAP Gateway can cache a configurable number of triplets from the HLR and perform authentication locally if needed.

The Cisco ITP configuration can also allow the reuse of triplets for several occurrences of the same user’s authentication process, if the operator wants to implement such a policy.

In addition, the time period during which the triplets will be stored in the cache memory of the Cisco ITP MAP Gateway is configurable.

### Performances and Capacity

Table 1 shows a summary of Cisco IP Transfer Point key features.

Table 1 Cisco IP Transfer Point Features

Category	Available today
Dimensions for Cisco 7513 chassis (H x W x D)	33.75 x 17.5 x 22 in. - less than 3 feet tall (85.73 x 44.45 x 55.88 cm)
Dimensions for Cisco 7206VXR chassis (H x W x D)	5.25 x 16.8 x 17 in. (13.34 x 42.67 x 43.18 cm)

Table 1 Cisco IP Transfer Point Features

Category	Available today
Link capacity	Up to 720 SS7 links for Cisco 7513; up to 24 SS7 links for Cisco 7206VXR
Number of authentication(s)	Up to 1800/sec
Number of authentications and authorization(s)	Up to 400/sec

### Cisco ITP MAP Gateway Deployment Topologies

The actual topology is ultimately the choice of the network designer, and it depends highly on the network specifics. However, hereafter are discussed some examples of Cisco ITP-based topologies that enhance redundancy and cost savings by centralizing or decentralizing the Cisco ITP function:

- A decentralized topology means that the Cisco ITP MAP Gateway node resides next to the RADIUS server (collocated in the same data center) in each region. In that case, there are as many MAP gateway nodes as there are local RADIUS servers. All MAP gateways have an SS7 connection with the central HLR or AUC.
- In a centralized architecture, however, the MAP gateway node is unique and typically collocated with the HLR or AUC. It establishes several RADIUS connections with the local RADIUS servers. The long-distance links are IP based, a setup that can, depending on the topology, can take advantage of the existing IP network in place and save some transmission costs. Note that IP Security (IPSec) can be used on the IP links between the Cisco ITP and RADIUS server to protect the sensitive signaling traffic.
- Finally, another type of topology consists of taking advantage of the Sigtran IP-based M2PA backhaul capability of the Cisco ITP, by having both remote MAP gateways in each local data center and a centralized MAP gateway collocated with the HLR cluster. The central MAP gateway communicates with remote MAP gateways via an IETF standardized SS7oIP peer-to-peer protocol named Sigtran M2PA.

### Cisco ITP MAP Gateway Reliability and Redundancy

#### Node and Architecture Redundancy

The Cisco ITP MAP Gateway products are built on the proven Cisco 7500 or Cisco 7200VXR Series Router hardware platforms. Both Cisco 7500 and 7200VXR Series routers are widely deployed in industry segments that require high reliability and availability—telecommunications, health care, banking, brokerage, aviation, and military installations. The Cisco Customer Advocacy organization monitors mean time between failure (MTBF) and mean time to repair (MTTR) for Cisco 7500 series hardware and software. From customer results, single Cisco IP Transfer Point availability can achieve “six nines” or 99.9999 percent availability with a calculated downtime of approximately one second per year.

The fully redundant Cisco ITP platform allows switchover mechanisms in case of link, port adapter, or central processor failure, so that the time of unavailability of service remains minimal. If traffic is interrupted during the time of the switchover, packets are lost, triggering resending by the RADIUS server. Upon reestablishment of the link, the packets from the HLR and the RADIUS server are processed again by the MAP gateway.

Finally, the architecture itself can also be redundant and involve several ITPs for load sharing and backup purposes. In particular, the Cisco Access Registrar allows the definition of multiple ITP MAP gateways. Therefore, in case of the failure of a MAP gateway, the traffic can be redirected to the backup ITP. The Cisco RADIUS Server can also be configured to round robin across the ITPs.

## Network Management

The Cisco ITP network management solution combines the Cisco Signaling Gateway Manager (SGM) with existing Cisco and third-party IP network management products. Cisco SGM, along with CiscoWorks, CiscoView, and ecosystem partner products such as Agilent acceSS7 and HP OpenView, can provide end-to-end management suites for the Cisco ITP SS7 network—enabling network administrators to discover, manage, and troubleshoot Cisco ITP networks. In conjunction with leading management vendors of off-the-shelf SS7 network management applications for end-to-end call trace, packet analysis, and long-term trending and analysis, this management solution enables quick integration with existing SS7 network management applications.

Cisco SGM is a software application that enables network administrators to manage the SS7oIP layer of Cisco ITP networks. Cisco SGM is a client /server architecture which supports Windows, Solaris, and Web-based clients Figure 10 illustrates the Cisco SGM topological display of a SS7oIP network.



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems Europe  
11 Rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9  
France  
www-europe.cisco.com  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

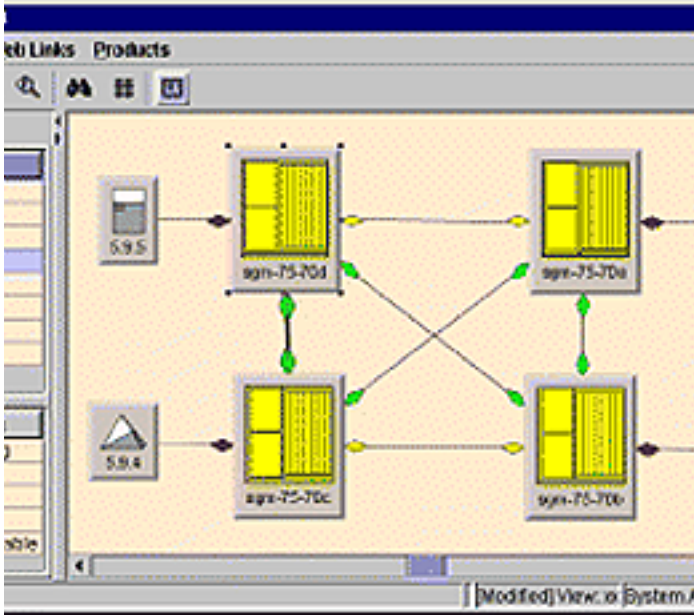
Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 317 7777  
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Figure 10  
Cisco SGM Topology Display



## Conclusion

By implementing the Cisco ITP MAP Gateway function into their network, mobile service providers will be able to achieve a smooth integration of WLAN technology into their existing GSM architectures, ensuring a high and homogeneous level of security and service access authorization. Various centralized or decentralized options allow a flexible implementation of the Cisco ITP MAP Gateway, whereas the support of a variety of ITU, ANSI, and IETF SS7overIP standards enable the Cisco ITP to interface the GSM operator's HLR in various ways.

Offered on both the Cisco 7200VXR Series and Cisco 7500 Series platforms, the Cisco ITP MAP Gateway offers much flexibility in choosing the link density, performance, and redundancy characteristics required for a given deployment. Deployed on the Cisco 7500 Series, the high processing capacity of the Cisco ITP MAP Gateway enables the network and the traffic to scale on the same platform. The Cisco ITP MAP Gateway opens the door today to new technology deployments for cellular operators.

## Abbreviations

AUC: GSM authentication center

AP: WLAN access point

CAR: Cisco CNS Access Registrar, Cisco implementation of the EAP capable RADIUS functionality.

EAP: Extensible Authentication Protocol (RFC 2284)

GSM: Global System for Mobile Communications, European Telecommunication Standards Institute (ETSI) standard for second-generation cellular (2G) networks

HLR: Home Location Register, subscriber database for GSM networks

IMSI: International mobile subscriber identity

HPLMN: Home public land mobile network

ITP: Cisco IP Transfer Point, signaling gateway for SS7 and IP networks

MAP: Mobile Application Part, ETSI GSM standard for mobility management signaling in cellular networks

MS: Mobile station, equivalent to a handset in GSM networks

RADIUS: Remote Access Dial-In User Service

SIM: Subscriber identity mobile, identifies uniquely a GSM subscriber

UMTS: Universal Telecommunications System, 3GPP standard for third generation of cellular systems

VLR: Visitor Location Register, a local GSM database that acts as a HLR proxy for the subscriber

WLAN: Wireless LAN, from IETF 802.11 standard