Mobile Wireless

Internet Forum

Layered Functional Architecture

Draft Technical Report MTR-003

Version 1.0

Contribution Reference Number: MWIF 2000.138.9

Mobile Wireless Internet Forum

Contribution Reference Number:	MWIF 2000.1389
Last Saved:	2nd August 2000
Working Group:	Architecture
Title:	MWIF Layered Functional Architecture
Source:	MWIF ARCHITECTURE WORKING GROUP
Editor	Mary Barnes

Status: [To be added by Secretariat to reflect development status of the document]

Abstract: This document describes the MWIF Layered Functional Architecture. A diagram of the architecture is provided as well as definitions and descriptions of the functional elements in the layers.

For addition information contact:

Mobile Wireless Internet Forum

39355 California Street, Suite 307, Fremont, CA 94538

+1 (510) 608-3994

+1 (510) 608-5917 (fax)

info@mwif.org

www.mwif.org

Table of Contents

1 Introduction

This document defines the MWIF Layered Functional Architecture. A diagram of the Layered Functional Architecture accompanied by basic definitions of the Functional Elements is first presented. Detailed definitions and functionality provided by each of the elements in the architecture, with the exception of the Access Network elements, are then provided. The RAN elements will be described in detail in MTR-007 (MWIF IP Radio Control / Bearer in the RAN).

1.1 Objectives of the MWIF Technical Report

The objective of this document is to capture the MWIF Layered Functional Architecture and to serve as the basis for development of the MWIF Network Reference Architecture (MTR-004).

1.2 Definitions

This document employs the following terminology:

- Must, Shall, or Mandatory — the item is an absolute requirement of the Technical Report (TR).
- Should — the item is highly desirable.
- May or Optional — the item is not compulsory, and may be followed or ignored according to the needs of the implementers.

1.3 Overview of the Technical Report

This document describes the MWIF Layered Functional Architecture. A diagram of the architecture is provided as well as definitions and descriptions of the functional elements in the layers.

1.4 Release plan

It is the objective of the MWIF to provide timely industry direction for mobile wireless internet. In order to accomplish this, the MWIF will periodically release Technical Reports. The period in which Technical Reports will be released will be frequent enough to meet the objective of timely industry direction.

This Technical Report is the third in a series intended to specify the MWIF architecture. At the time of release of this report, the following MWIF Technical Reports are scheduled:

MTR-001 MWIF Architectural Principles

MTR-002 MWIF Architecture Requirements

MTR-003 MWIF Layered Functional Architecture

MTR-004 MWIF Network Reference Architecture

MTR-005 MWIF Gap Analysis

MTR-006 MWIF IP Transport in the RAN

MTR-007 MWIF IP Radio Control / Bearer in the RAN

2 References

1 mwif2000.082; Functional Definitions/Benchmark Workbook

2 mwif2000.129; Osaka Architecture WG meeting summary (includes LFA diagram)

3 RFC 2753; Framework for Policy-based Admission Control

4 draft-ietf-enum-e164-dns-00.txt

5 ITU-T Recommendation E.164 (05/97), "The international public telecommunication numbering plan".

6 mwif2000.116; All IP Network Architecture: Conceptual Framework and Functional Model

7 draft-ietf-aaa-na-reqts-05.txt; Criteria for Evaluating AAA Protocols for Network Access

8 draft-ietf-aaa-proto-eval-00.txt; AAA: Protocol Evaluation

3 Abbreviations

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
API	Applications Programming Interface
CSM	Communication Session Manager
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FAN	Fixed Access Network
GNS	Global Name Server
IETF	Internet Engineering Task Force
IN	Intelligent Network
IP	Internet Protocol
ISP	Internet Service Provider
MGC	Media Gateway Controller
MM	Mobility Manager
OAM & P	Operations, Administration, Management and Provisioning
PSTN	Pubic Switched Telephone Network
QoS	Quality of Service
RAN	Radio Access Network
SNMP	Simple Network Management Protocol
SS7	Signalling System Number 7
UMTS	Universal Mobile Telecommunications System

URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTRAN	UMTS Terrestrial Radio Access Network
VPN	Virtual Private Network

4 MWIF Layered Functional Architecture

The following diagram is the MWIF layered functional architecture:

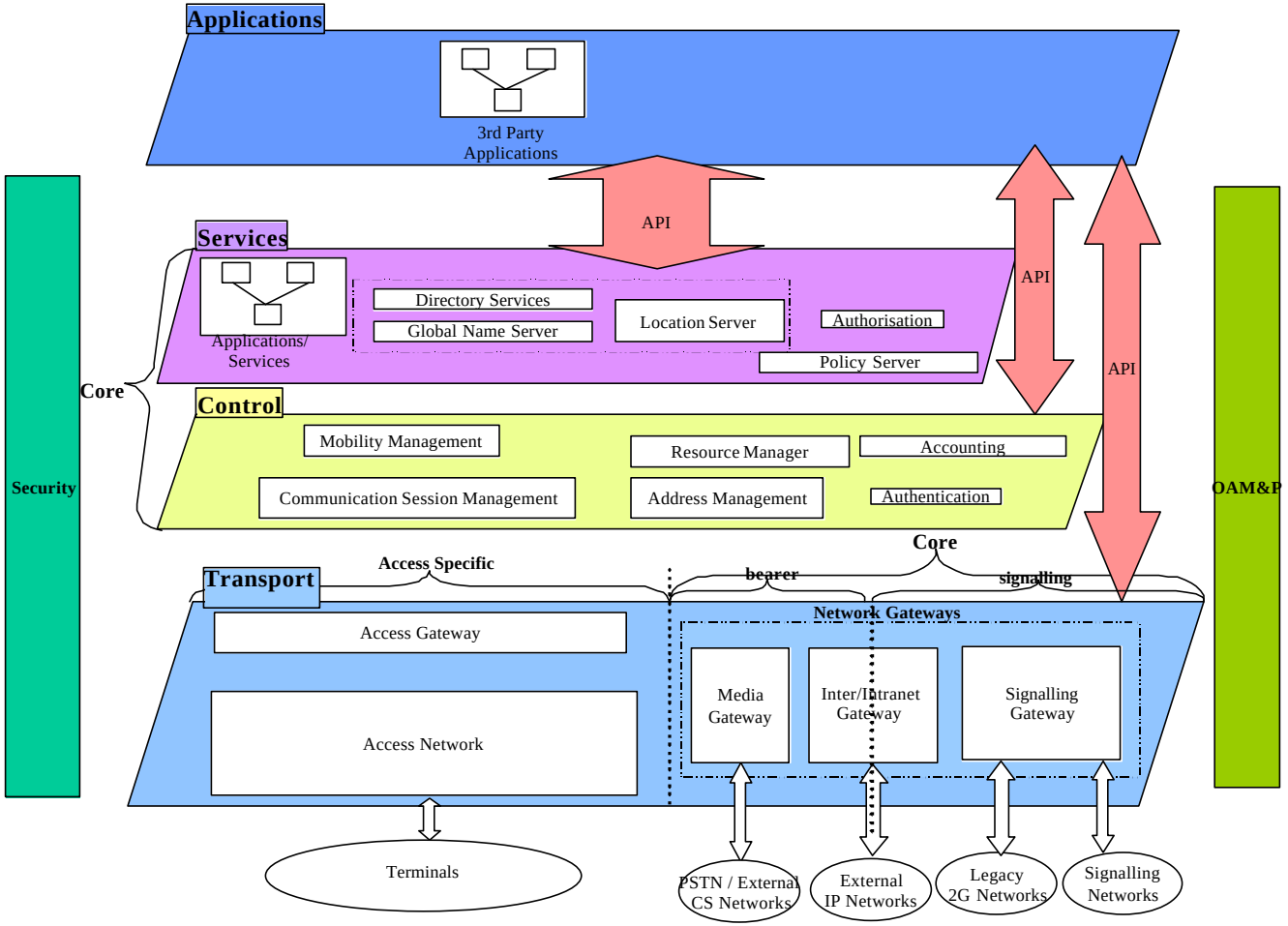

Figure 1: MWIF layered functional Architecture

5 Definitions Of Functional Elements

This section provides the definitions and basic functionality of the elements depicted in the Layered Functional Architecture. The subsequent sections provide a more detailed explanation of the overall functionality provided by each layer and the functional elements within each layer.

Services/Applications: an operator (network, virtual, ISP, etc.) provided function whereby service logic for features and services reside, and which supports a service creation environment, and provides management of services.

Directory Services/Global Name Server/Location Server: This functional element provides the network with directory information. This information may range from user service profiles, network polices, to configuration data for applications/services, hosts, and network elements. It also provides address translation between different addressing schemes of hosts and users. This functional element also provides the network entities with the current geographical location of a subscriber terminal.

Policy Server: Policy server comprises the network policy repository as well as policy editing and management tools for updating and management of network policies.

Security (including AAA): Security is the function that ensures authorized use of network resources and services by subscribers, equipment, agents, or other services, and the capability for confidentiality and non-repudiation for authorized use of network resources and services.

Mobility Management: In the Control layer, this represents the ability for an end user to move between IP subnets. Mobility management functionality in the control layer includes Inter-administrative Domain Terminal Mobility and Macro Terminal Mobility.

Communication Session Management: The CSM is a server that provides for the establishment, maintenance and release of multimedia sessions.

Resource Manager: The Resource Manager in the Control Layer manages Core Network bandwidth.

Address Management: Address Management in the Control layer is responsible for assignment and recovery of addresses within the address space of an administrative domain.

Access Gateway: An Access Gateway provides the interface between an Access Network and a Core Network.

Network Gateways (and their controllers): The Network Gateways functional element is a collection of gateways as required to interconnect the core to external networks consisting of the following:

- Inter/Intranet gateway
- Media gateway
- Signalling gateway

Individual gateways are typically divided between bearer and signalling gateways.

6 Layered Functional Architecture Detailed Descriptions

The architecture consists of four logical layers:

1. Applications
2. Services
3. Control
4. Transport (Access and Core)

As well, there are some functional elements spanning several layers (i.e. OAM&P and Security).

Also, note that the Layered Functional Architecture proposed in this document identifies necessary functions for supporting a wide range of voice, data, and multimedia services and applications in each plane. However, each application only utilizes the necessary subset of functional elements in each plane.

6.1 Applications Layer

The Applications Layer is comprised of 3rd party applications/services that are provided to end users. 3rd Party refers to applications provided by someone other than the owner of the Services layer, and are not under the direct administrative control of the network operator. Access from the Applications layer to the Services, Control and Transport layers is provided by Open APIs.

6.2 Services Layer

The Services Layer provides the end user service control and services essential to the effective operation of the Control and Transport layers.

The Services Layer is comprised of the following functional elements:

- Services/Applications
- Directory Services/Global Name Server/Location Server
- Policy Server
- Authorization

6.2.1 Services/Applications

Services/Applications is an operator (network, virtual, ISP, etc.) provided function whereby service logic for user features and services reside, and which supports service creation environment, and provides management of services.

It consists of a set of functions that provide the subscriber with useful applications that may or may not be related to a call/session. These functions include the detection of service requests, events and call/session states and the precedence ordered execution of specific actions that are triggered by these events.

As part of the service authorization process, the Authorization function may pass a descriptor to the CSM. This descriptor identifies the applications/services functions to be performed (whether in the CSM or Application /Service level). The descriptor could be in the form of a script or a pointer to a specific service application. These applications run independently and interface to other system

resources as required (e.g., databases, CSM, etc.). The interface to the system resources will be defined in an API specification.

The necessary functions for supporting complex features are performed in the service and/or application layers. This allows a service provider the flexibility to redefine existing features.

6.2.1.1 Service Logic

An operator provided set of functions and interfaces allowing:

- Standardized supplementary services (e.g., call waiting, call forwarding, three party, etc.),
- Additional non-standardized supplementary services,
- IN services: VPN, prepaid, free phone,
- Customized services by third party through specific APIs, including:
  - Enterprise level services,
  - Subscriber level services (may imply script downloading).

6.2.1.2 Service Creation Environment

APIs enabling development of services/applications by operator or third party:

- Script definition,
- Event and trigger on event definition.

6.2.1.3 Service Management

Service Management refers to the infrastructure in the Services Layer required to provide services to a subscriber independent of their network point of attachment and is comprised of the following elements:

- Security/authorisation for the Services is provided by the Security/AAA functional element described in another section
- Subscriber Service Mobility refers to the ability of the subscriber to obtain services in a transparent manner regardless of the serving network or device (subject to the limitations of the network and device). This mobility includes the ability of the home service provider to control the services it provides to the subscriber in a serving network.
- Subscriber Service Portability is for further study.

6.2.2 Directory Services/Global Name Server/Location Server

The Location Server, Directory Services and Global Name Server (GNS) functional elements are considered to be a single functional element from an architectural perspective. Note that this functional element also consists of the IP infrastructure functions such as DNS in the Services layer. This functional element is the repository of the objects (i.e. database entries) and corresponding access methods associated with the terminal, subscriber and service. The objects maintain the relationship between the subscriber, terminals and services. This functional element also maintains the relationship of naming/number/addressing to entities.

For the purpose of clarifying the functionality, the following definitions for “Location Server”, “Global Name Server” and “Directory Services” are provided:

6.2.2.1 Location Server

The location server stores all dynamic information associated with user, terminal, and service mobility. With the exception of terminal geographic location, updates for terminal, user, and service location information are provided from the mobility manager and are made available to all architectural elements via an open interface. This location information is stored both in the home network Location server and the visited network Location server (assuming the terminal is roaming).

6.2.2.1.1 User/Terminal Geographic Location

User/Terminal Geographic Location is the geographic location of the terminal (e.g., latitude, longitude, and altitude coordinates) provided or derived from information from the Access Gateway. The network element which initially writes and subsequently updates this information is described in further detail in the MWIF Network Reference Architecture (MTR-004). Expected update rates and accuracy are beyond the scope of this document.

6.2.2.1.2 User/Terminal Location

- User/Terminal Serving Administrative Domain Location is the identity of the serving network's operator (e.g., Operator1.net). This information is provided by the Mobility Manager.
- User/Terminal Home Administrative Domain Location is the identity of the home network's operator (e.g., Operator1.net). This information is provided by the Mobility Manager.
- User/Terminal Network Location identifies the presence of the user/terminal in the serving network (e.g., something like the Care of Address from Mobile IP). Presence constitutes network reachability for the respective terminal. This information is provided by the Mobility Manager.
- User IP address currently registered for the terminal. This information is provided by the Mobility Manager.

6.2.2.1.3 Service Location

Upon service registration, a service endpoint (e.g., home application server URL) is selected and stored in the home network location server. This information is used for service within the home network or outside the home network when service is proxied in the visited network.

6.2.2.2 Global Name Server

The Global Name Server (GNS) maps URI to subscriber. It also maps an E.164 number to an IP address.

6.2.2.3 Directory Services

Stores all statically provisioned user profile information including but not limited to level of service, calling features, roaming capabilities, subscriber profile, etc.

Additional terminal capabilities may be stored.

6.2.3 Policy Server

The Policy Server provides the policy rules for subscriber policy usage, expected QOS, valid times and routes. The Policy Server allows for separation of policy rules from policy enforcement (e.g., bandwidth management, jitter control, packet counting/queuing). The Policy Server is a policy repository and does not make policy decisions or provide policy enforcement. The Policy Server also provides policy rules for the applications serving a user.

6.2.4 Authorization

Authorization answers the question "what may you do?" Clearly, only authenticated individuals may be authorized to act (excluding consideration of emergency services to non-authenticated individuals), and what actions they have permission to perform may be related to who they are. However, these permissions may also relate to time of day, type of access, and the simultaneous activities of other entities. For instance, a user may normally be permitted to place a telephone call, but cannot when no resources are available. Profiles govern authorization. Profiles detail the network resources at particular times that each user may utilize. Profiles may detail charges for a particular network resource and the amount of permitted usage for a network resource that this user may consume.

Authorization is the act of certifying or providing permission for provision of one or more services to a subscriber. The Authorization Function retrieves the policy rules from the Policy Server and then retrieves other appropriate data necessary (from the Directory Services, Applications, etc.) to make a determination using the rules.

As part of the service authorization process, the Authorization function may pass a descriptor to the CSM. This descriptor identifies the applications/services functions to be performed or invoked (whether in the CSM or Application /Service level).

6.3 Control Layer

The Control Layer consists of functionality necessary for the control of the IP Transport.

The Control Layer consists of the following functional elements:

- Authentication
- Accounting
- Mobility Management
- Communication Session Management
- Resource Manager
- Address Management

6.3.1 Authentication

Authentication answers the question "prove that you are who you say you are?" An exchange happens between the entity to be authenticated and the Authentication Function, in which the entity offers proof of its identity, and the Authentication Function determines whether the authentication credentials are valid.

6.3.2 Accounting

Accounting answers the question "what did you do and when did you do it?". Accounting is the process of recording requested and actual network resource usage during a particular user activity. Data collection for purposes of real-time and non-real-time accounting occurs at all layers and needs to support per user resource and service usage. Consolidation of this data for forwarding to billing functions is located in the control layer.

6.3.3 Mobility Management

The Mobility Management functional entity in the Control layer consists of the following functions:

- Handover control

- Roaming

The levels of mobility supported in the Control Layer include Macro Terminal mobility and Inter-administrative Domain Terminal Mobility. The Control Layer mobility consists of the following functions:

- Updates user/terminal locations in the Location Server. Refer to section User/Terminal Location (section 6.2.2.1.2) for definitions of the locations maintained.
- Provides handover control for the Macro Terminal mobility and the Inter-administrative Domain Terminal Mobility.

6.3.4 Communication Session Manager

The Communication Session Manager (CSM) in the Control Layer provides the following functionality:

- Session/Call state management
- Manages application of tones and announcements to the user
- Interfaces with Service Plane functional entities
- Interfaces with other Control Plane entities as necessary.

The Communication Session Manager is responsible for control of IP multimedia sessions for a given subscriber. As the Communication Session Manager accomplishes its work, there may be a need for an interaction with the Authorisation Function to provide information to the services layer, to ask for a decision relative to a service invocation, etc. The Communications Session Manager is shielded from the organization of the services, from service interaction complexities, and from the creation/deletion of service logic.

As part of the service authorization process, the Authorization function may pass a descriptor to the CSM. This descriptor identifies the applications/services functions to be performed or invoked. The descriptor could be in the form of a script or a pointer to a specific service application. The CSM provides a basic set of intrinsic session processing features (e.g., call hold, call waiting tone, call release, etc.).

6.3.5 Resource Manager

The Resource Manager in the Control Layer manages Core Network bandwidth.

6.3.6 Address Management

Address Management provides the control of address assignment and recovery of addresses within the address space of an administrative domain. The address management involves allocation and deallocation of IP addresses. The DHCP protocol may be used to accomplish the address management task.

6.4 Transport Layer

The Transport Layer provides the IP bearer and signalling transport from the user to the core network (and on to external networks).

The Transport Layer is comprised of both access network specific functional elements and access independent Core Network elements. The only access network specific functional element addressed by this document is the Access Gateway. The RAN specific functional elements are to be addressed by a separate RAN architecture document (MTR-007).

The Core Network functional elements in the Transport Layer are the Network Gateways (and their controllers).

6.4.1 Access Gateway

An Access Gateway provides the interface between an Access Network and a Core Network. An Access Gateway is the point of demarcation between an Access Network and a Core Network. From the point of view of a Core Network, an Access Network is the set of functionality available at an Access Gateway.

An Access Gateway hides the specifics of an Access Network from the Core Network and provides edge routing functionality for the Core Network. An Access Gateway interfaces the Access Network and Core Network bearers and provides policy enforcement, as necessary.

An Access Gateway interacts with control plane management entities (e.g., Mobility Management, Resource Management, Accounting, etc.). An access gateway creates outbound and/or receives inbound flows in the gateway in response to control plane management entity requests.

6.4.2 Network Gateways (and their controllers)

The Network Gateways functional element is a collection of gateways as required to interconnect the core to external networks. Individual gateways are typically divided between bearer and signalling gateways.

Network gateways can provide the following functionality:

1. Enforce QoS policy.
2. Apply throughput control and firewall policies.
3. Generate statistics of resource usage (for O&M).
4. Perform protocol conversions as required.

The Network Gateway functional entity has been divided into the specific gateways as follows:

- Media gateway: terminates PSTN voice traffic and converts the traffic as required between IP and PSTN formats.
- Intra/Internet gateway: provides the interconnection point between carrier's Core IP networks and external networks. An Intra/Internet gateway provides firewall functionality and analysis of packets.
- Signalling gateway: converts legacy signalling (SS7, other out-band signalling) into appropriate IP signalling, and converts IP signalling into legacy signalling, and supports roaming to other networks.

6.5 Security

Security is the function that ensures authorised use of network resources and services by subscribers, equipment, agents, or other services, and the capability for confidentiality and non-repudiation for authorised use of network resources and services.

The IETF AAA function is considered a fundamental functional block of security within MWIF.

The following functions are elements of security, but may be performed at other areas in the network:

- Non-repudiation
- Authorization

- Authentication
- Confidentiality – encryption (link or end-to-end)
- Firewall
- VPN proxy
- Certificate server
- Separate access, transport, and application functions

6.5.1.1 AAA

In the IETF model, AAA is a framework to provide for Internet authentication, accounting and authorization. For roaming, the AAA framework comprises an AAA instance in the visited and home network, and optionally several AAA proxies and/or brokers in intermediate networks.

The AAA communicates with a Policy Server and provides implementation of service level agreements and business policy.

The Authentication and Accounting functionality are considered to be part of the Control Layer. The Authorization is considered to be part of the Service Layer. Further details on these functional entities are provided in these specific sections of the document.

6.6 Operation, Administration, Maintenance & Provisioning (OAM&P)

OAM&P comprises all necessary functions for provisioning, maintenance, operation and administration of a network. OAM&P is responsible for ensuring proper operation and maintenance of network transport, control, and service infrastructure during their lifespans.

Specifically OAM&P performs:

- Configuration Management
- Fault Management
- Performance Management
- Billing Management
- Security Management

6.6.1 Configuration Management

Configuration Management is responsible for network provisioning, subscriber profile management, and configuration of network elements (e.g., routers, network servers) as well as the relations among them.

6.6.2 Fault Management

Fault Management is responsible for detection, isolation and recovery of the network from failures. It also collects information about and manages the errors/faults occurred in and alarms raised by the network and/or its elements.

6.6.3 Performance Management

Performance Management is comprises of all functions (e.g., monitoring, etc.) necessary to ensure QoS and efficient use of resources in the network.

6.6.4 Billing Management

Billing Management is responsible for collection, storage, and processing of all necessary data for billing network services and applications according to the value chain.

6.6.5 Security Management

Security Management is responsible for maintaining the network security infrastructure (e.g., passwords, security credentials).

7 GLOSSARY

Inter-administrative Domain Terminal Mobility: This level of terminal mobility refers to the ability of the terminal to move across administrative domain boundaries. The terminal may be within any wireless or fixed network.

Macro Terminal Mobility: This level of terminal mobility refers to the ability of the terminal to move across subnet boundaries within the same administrative domain.

Micro Terminal Mobility: This level of terminal mobility refers to the ability of the terminal to move across internal boundaries of an access network.

Policy: The combination of rules and services where rules define the criteria for resource access and usage.

Subnet: A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

Document History

Date	Version	Comment
June 2, 2000	Version 0.1	Initial draft format for document, including definitions to date from mwif2000.082.4
June 6, 2000	Version 0.2	Updates based on June 2 conference call and email comments.
June 9, 2000	Version 0.3	Updates based on June 9 conference call and email input.
June 15, 2000	Version 0.4	Updates based on Call Flow Breakouts at Lockdown.
June 20, 2000	Version 0.5	Editorial conversion to MWIF draft format. Updates based on mailing list discussion/input between lockdown week 1 and week2.
July 9, 2000	Version 0.6	Updates based on resolution of issues and call flows at week 2 of the lockdown.
July 14,2000	Version 0.7	Updates based on mailing list proposals/discussions and July 14th conference call.
July 17, 2000	Version 0.8	Work group consensus version – based on additional input on Version 0.7 (mwif2000.138.6). This version goes to the TC for a 2 week comment period (prior to ballot).
August 1, 2000	Version 0.9	Updates following July 31st conference calls – comments incorporated based on those received during 2 week comment period. This version is available for 24 hour editorial review prior to submission of version 1.0, which is the ballot version.
August 2, 2000	Version 1.0	Version approved as basis for TC ballot.

Areas for Future Study

Date	Version	Issue
July 31, 2000	Identified in Version 1.0	The issue of Subscriber Service Portability needs to be better understood if it remai ns as a Requirement. There are at least 2 different interpretations within the group.
July 31, 2000	Identified in Version 1.0	Whereabouts in the MWIF Architecture does the network provide conference bridges? Proposal: Either add conference capability into the MWIF Layered Functional Architecture or add text into the document indication that this is a necessary function but that it is not shown on the diagram.
July 31, 2000	Identified in Version 1.0	Whereabouts in the MWIF Architecture does the network provide tones? It is stated in 6.3.4 that the CSM manages the application of tones, however there appears to be no functional

		entity that provides the tones. Proposal: Add tone capability into the MWIF Layered Functional Architecture or add text into the document indication that this is a necessary function but that it is not shown on the diagram.