ETSI TR 170 012 V3.1.1 (2006-01)

Technical Report

Project MESA;
Technical Specification Group - System;
System Overview

Reference
DTR/MESA-SYS0070012v311

Keywords
broadband, digital, emergency, protection, radio, safety, SAR, satellite, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by Public Safety Partnership Project (MESA).

The contents of the present document are subject to continuing work within the Specification Group (SG) and may change following formal SG approval. Should the SG modify the contents of the present document, it will be re-released by the SG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to SG for information;

2 presented to SG for approval;

3 or greater indicates SG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines a system architecture that is capable of meeting the requirements of next-generation public service and public safety agencies. The present document articulates requirements that are detailed in the Project MESA Statement of Requirements document and captures other elements that encompass the overall user communication landscape.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] ETSI TS 170 001: "Project MESA; Service Specification Group - Services and Applications; Statement of Requirements (MESA 70.001)".

[2] ETSI TR 170 002: "Project MESA; Service Specification Group - Services and Applications; Definitions, symbols and abbreviations (MESA 70.002)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

connection: entilly formed when two devices communicate

NOTE: A connection between two devices includes the interfaces used and the link that is formed between them. A connection can also describe the upper layer elements within the context of overall connectivity to a mission's application needs.

device: is a type of communication component differentiated from other components by its stand-alone accessibility and functionality

NOTE: It is physically interactive, such that an input results in an action taking place within the device, as opposed to a component which may only be accessible through the network. Devices are generally more portable than other components and may possess capabilities to access or communicate with other devices and/or networks.

interface: physical or logical link between two entities

NOTE: In the present document it is used to refer to the physical interface that network components use to communicate with each other. This interface may be either wired, wireless or utilize other emerging techniques. All software interfaces will be specifically referred to as software interfaces.

When two or more interfaces communicate they form a **link**. This link may be wired, wireless or utilize other techniques, depending on the interfaces forming the link. The interfaces forming the link also determine the protocol of the link. Note that components or devices (i.e. NGN, converged) may be enabled to utilize and access multiple interface and link possibilities.

network component or simply a **component:** represents a physical piece of the network

NOTE: This component may serve in creating the network, facilitating the network or to access the network.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 170 002 [2] and the following apply:

AFIS	Automated Fingerprint Information System
ATF	U.S. Department of Treasury's Bureau of Alcohol, Tobacco, and Firearms
ATL	Attempt To Locate
CDMV	Canadian Department of Motor Vehicles
COMPUSEC	Computer Security
COMSEC	Communications Security
DHS	Department of Homeland Security (US)
DMAT	Disaster Medical Assistance Team
DMV	Department of Motor Vehicles (US)
DOD	Department of Defense (US)
DOT	Department of Transportation (US)
EAN	Extended Area Network
ECG	Electrocardiogram
EMS	Emergency Medical Services
ETS	Emergency Telecommunication Service
FBI	Federal Bureau of Investigation (US)
FCC	Federal Communications Commission (US)
FD	Fire Department
FIFO	First-in, first-out
FMC	Fixed/Mobile Convergence
GIS	Geographic Information System
GLS	Global Location System
HAZMAT	Hazardous Materials
HF	High Frequency
IAFIS	Integrated Automated Fingerprint Identification System
IDWCS	Integrated Digital Wireless Communications System
IETF	Internet Engineering Task Force
INFOSEC	Information Systems Security
IST	Incident Support Team
ISTEA	Intermodal Surface Transportation Efficiency Act (US)
ITS	Intelligent Transportation System / Intelligent Transport System
ITU	International Telecommunications Union
JAN	Jurisdiction Area Network
LAN	Local Area Network
LMR	Land Mobile Radio
MESA	Mobility for Emergency & Safety Applications
MRI	Magnetic Resonance Imaging
NCIC	National Crime Information Center (US)
NGN	Next-Generation Network (relates to convergence and FMC; packet-data)
NLETS	National Law Enforcement Telecommunications System (US)
NTIA	National Telecommunications and Information Administration (US)
OSA	Open System Architecture
OTAR	Over-The-Air-Rekeying
P25	Project 25
P34	Project 34
PAN	Personal Area Network
PASS	Personal Alert Safety Systems
PD	Police Department
PPDR	Public Protection and Disaster Relief
PSAP	Public Safety Answering Point
PSCD	Public Safety Communication Device
PSPP	Public Safety Partnership Project
PSWAC	Public Safety Wireless Advisory Committee (US)
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
SaR	Search and Rescue

SC	Steering Committee
SCADA	Supervisory Control And Data Acquisition
SCBA	Self Contained Breathing Apparatus
SENTRY	Federal Bureau of Prisons' "SENTRY" database (US)
SoR	Statement of Requirements
SSG	Service Specification Group
TCP	Transmission Control Protocol
TDR	Telecommunication for Disaster Relief
TETRA	Terrestrial Trunked Radio
TRANSEC	Transmission Security
US&R	Urban Search and Rescue
USAR/TSAR	Urban Search and Rescue/Technical Search and Rescue
WAN	Wide Area Network
WLAN	Wireless Local Area Network

4 Overview

The Project MESA System Reference Architecture describes the communication components that will either be incorporated into a Project MESA system, or with which a Project MESA system will interact. The document describes a general public safety and emergency services sector communication architecture or structure, and the common components in that architecture. Actual implementations may differ but the overall hierarchy should be similar even if all the pieces are not included, thus allowing for maxim flexibility and discretion of system owners, operators and users. The flexibility of the architecture allows for a communication system that addresses many different scenarios and specialized agency or user needs.

In addition, the present document describes potential applications that may run over the architecture and the various classes of service provided by the network to support those applications. Each class of service has different network and application requirements and these are detailed within the pressent document.

4.1 System of Systems

The present document describes the overall communication architecture that a Project MESA system operates in. A Project MESA system integrates into this architecture, establishing some networks and tying others together to enable seamless, secure mobility across and throughout MESA-established systems and connectivity or bridging to other established systems and networks, as authorized.

A Project MESA-defined broadband data system can take the form of temporary ad-hoc or flexible elements or can take the form of an overall command and management system composed of other systems that may include MESA-capable components and networks or other elements needed to constitute a successful mission. Some of the systems or components that may make up the larger System, are formed or accessed using MESA-capable or applicable technology.

The Project MESA "System of Systems" approach allows developers and implementers the flexibility to customize networks to better meet the needs of users. (see note) Due to diversity of user needs and operational environments, it is impossible to create a single network configuration that will meet the needs of all of the Project MESA members and the public service or public safety sector element they may represent. Each deployment of a public safety communication network will need to address the unique needs of its users, and no single network configuration can efficiently do this for all service and user needs. Using the "System of Systems" approach gives the system designers a common framework for next-generation communication planning and the ability to tailor a solution, thus providing the components and architecture necessary to customize a communication solution that efficiently meets the needs of its users. The utilization of standardized components and a common architecture will allow for compatibility, inter-connectivity and interoperability across legacy and next-generation deployments of this critical sector.

NOTE: It can be noted that the Project MESA Technical Specification Group-Systems (TSG SYS) also utilizes the term "System of Systems" to express the need for consideration of technologies that may be applicable to MESA TSG SYS work and the overall communication architecture that exists or is emerging for the public safety and emergency services sector.

The "System of Systems" approach also allows for divergent networks to be formed into single system (i.e. management, command), creating a common networking platform across all MESA-capable systems and bridging to other existing systems. The common networked platform would tie-together and/or mask differences in the underlying network structures and systems that are established (i.e. multiple ad-hoc "hot-spots"). Such a common platform deployment would allow a user to seamlessly migrate from one system or hot-spot to another and still be under the umbrella of an overall command and management structure. As indicated before, the overall architecture is flexible to needs of agencies and users and deployments may focus, for example, on single reactionary forces that utilize a single and temporary ad-hoc network to a system of systems command and deployment scenario that coordinates many individualized mission hot-spots.

5 Framework description

5.1 Overview

The overall communication framework described in the present document provides a common set of components and a structured relationship between MESA-defined components and existing or emerging systems. The architecture generally describes the components and the network formed among them. This does not represent a complete framework, but instead provides a fundamental understanding and architecture that can be used in the development of a fuller framework for next-generation communication needs. It makes sense to work towards an agreed upon and coordinated framework as Project MESA system capabilities and related external technical activities progress.

6 Architecture

6.1 Overview

The overall public safety communication system architecture provides a description of the identified systems" components, including the components" structure and the connections formed among them. The architecture also explains the design principles behind the components and their connections. The chart below also implies a potential access or architectural relationship (interoperability, accessibility) between network types and or components.

6.2 Networks

Type	Scope	Capabilities	Bandwidth Required
Personal Area Network (PAN)	Single subject or object	Limited applications and location	Only enough for pre-designated and localized applications
Incident Area Network (IAN)	An incident or specific event. Examples include a MESA-capable ad-hoc "hot-spot" or other temporary network	Application varied and flexible network establishment, but location limited	Enough to support the incident or specific mission, including ad-hoc capabilities across environmentally challenging scenarios
Jurisdiction Area Network (JAN)	An entire jurisdiction. Examples include a traditional land mobile system or an incident-oriented MESA jurisdictional system of systems	Varied applications and locations, robust, well managed	Able to provide high bandwidth throughout the coverage area; extensive planning and engineering
Extended Area Network (EAN)	Unlimited, as technically feasible	Varied applications and locations as technically feasible; could include national or territorial service, database access, enhanced access capabilities and alternate communication channels	Unlimited, as technically feasible

6.2.1 PAN

6.2.1.1 Overview

The Personal Area Network is used to transfer information over a very limited physical space. The network is made up of multiple devices that are dedicated to a specific task. The scope of the network is generally limited to a minimal subject or object interaction, which involves another device, a person, vehicle, building, etc. Generally the devices on the PAN are sensors, or input devices; however, output devices can also be incorporated into overall capabilities. Examples could include terminal interaction or data acquiring activities between devices or sensing units, an information display/collection board in a building, or a "wired" personnel outfitting.

Since a PAN is designed with a specific scope in mind, it can be tailored to best meet that required capability. The PAN formed for a first responder needs to primarily function over a short distance, with potential capability to interact with or access another network type. This limited area flexibility allows for utilization of technologies and individualized capabilities that would be impractical in PANs with a larger and more complex scope, such as those found in buildings. It is also often known, during the design phase, which devices or applications will be utilized in the PAN, thus allowing for further optimization of the network. The specialized and individualized nature of the PAN sets it apart from more general communication networks like the IAN and JAN. These more generalized networks are designed for added complexity and a wider area of coverage than a PAN can employ.

6.2.1.2 Characteristics

- Network is dedicated to a single or minimal amount of tasks or application sets, within the scope of a minimal subject or object area.
- Devices transmitting data across the PAN are generally designed for specific tasks and interactions, not general communication needs. However, a PAN device could also access an existing EAN as applicable.

6.2.1.3 Relations

Devices on the PAN need to interface with other devices on the defined PAN. The devices need to connect to other networks and interfaces if they wish to interact with outside networks, terminals and databases. This requires a communication link that is capable of interfacing PAN elements with variant or external network elements and devices. Such a link, which could be internal or external to the device, facilitates inter-network communication (or intra-network in case of MESA System of Systems deployment) and can collect communication from affected networks, delivering the payload along to other designated recipients or network elements.

While a device on the PAN can do this inter-networking, the PAN devices generally do not have extensive resource capabilities due to their localized nature. Devices designed to communicate on either an IAN or a JAN generally have more resource capability or capacity and may be designed for networks and tasks that are more demanding. In most cases the subject of the PAN, (person, vehicle, building, etc.), connects to larger networks through a communication link enabled device. When possible, the PAN will communicate through this device to the established IAN and JAN, if necessary (i.e. automatic status or data updating across command structure, "always on" capabilities).

For PAN devices worn on or carried by a person, the internetworking is done by the person's communication device, including any internal communication link. Additionally, vehicle-based PAN devices can utilize the vehicle's existing or augmented communication link and or device to interface with other networks or augment application capabilities. Such a deployment could also infer limited mobility, depending on capability and needs. Building-based PANs can have the most flexibility in terms of computing and networking capabilities, due to potentially fewer form factor and power or backbone connectivity constraints. This may involve a number of different options, including wireless or satellite links, hard-wired or other access means to connect and interface with other PAN devices and networks (including extensions of ones own network).

6.2.2 IAN

6.2.2.1 Overview

The Incident Area Network (IAN) is dedicated to a single incident or event. The IAN can be pre-deployed for a planned event, such as a sporting or "nationally significant" event, or it could be dynamically deployed for an unplanned event or incident (all-hazards). Possible unplanned events range from a local law enforcement situation to relief efforts in a natural disaster area. Depending on the affected situational area and agencies engaged, interoperability, inter-connection and resource management become more critical. Note that an unplanned incident can involve fluid and challenging geographic and infrastructure scenarios that can affect initial staging operations and overall communication capabilities (i.e. terrorist attack or major hurricane/tsunami). The IAN can be deployed, for example, in situations were existing private and/or public communication infrastructure is diminished or non-existent. The IAN can involve MESA-capable or other components.

From a networking perspective an IAN is comparable to a mobile Ad-Hoc network, in terms of flexible establishment and connectivity options. The IAN is essentially a specialized Ad-Hoc network designed specifically to meet user and application requirements within a defined context. It is similarly dynamic and flexible, but has more constraints than a typical Ad-Hoc network in order to provide the required level of service to this user class. Depending on the requirements, constraints may be put in place on the role a device can play in the network and the priority of access each device receives. From a user perspective an IAN will be able to provide similar operation as "talk groups" found in current land mobile radios. It will provide localized and topic specific communication to a subset of the overall group, as applicable. However, traditional Ad-Hoc capabilities and variant forms of access to the IAN, other networks and the public Internet (as appropriate and secure) may also be utilized, depending on scenario, to augment capability needs in order to fulfil the required mission. Next-generation "aware" components, cognitive or software related radio and other technologies can enhance flexibility/agility and the user's capabilities; given the fluid nature of this network deployment and the potential scenarios it may entail.

If an IAN (or multiple MESA IANs) that is part of a MESA System can bridge to other networks, it will try to coordinate with them to improve communications. The coordination would not only reduce interference between adjoining networks, but it would improve security and mobility across the MESA System of Systems deployment. The coordination and unifying of networks is an essential part of the MESA System. The details of how this coordination occurs will be examined further in appropriate technical documents.

While an IAN can be pre-deployed for a planned event, it is designed to be quickly and easily deployed. The next-generation IAN is seen as self-configuring, where the best network connection possible is automatically established between available devices and network elements, and self-healing to provide the user with consistent communication. The IAN makes use of available devices and resources. Where there are a limited number of devices or limited access capabilities, communication coverage and external network access maybe unstable. To improve coverage, devices can be repositioned or more devices can be brought online. The ability to dynamically create a network is one of the strengths of the IAN, however it can sometimes result in having an incomplete coverage area (in a geographical sense). A MESA cell is the aggregate coverage provided by the components of a single IAN.

The IAN is capable of supporting a wide variety of applications. They range from challenging broadband applications such as mission critical voice/video communications that have demanding requirements, to less demanding or critical data transactions which may only require negligible resources or priority from the network. The possible applications require different classes of service or network priority. A higher class of service allows for more demanding applications to receive preferential treatment from the network. The MESA IAN is intelligent enough to reconfigure and allocate resources in order to deliver the level of service needed by a certain application.

Since an IAN is only available within a localized area, the network resources are shared by a relatively small number of devices. The result is that each device may be able to use a larger portion of available network resources, depending on scenario and scope of event or incident. This potential resource flexibility may make it easier for the network to accommodate applications that utilize large amounts of the network's resources. The IAN may also include a Peer-to-Peer or sub-grouping mode that would allow two or more devices to communicate directly and independent of established network channels. This mode would limit the impact of the communication on the IAN, however, it would probably involve an un-managed sub-IAN and thus applicable to individual or command agency or system owner policies. Additionally, any spectrum allocation, interference and capacity concerns would need to be addressed that involve resources requiring such attention.

6.2.2.2 Characteristics

- An IAN is agile, dynamic and flexible with regard to network and geographic implementation needs; the activated network can involve locations were supporting infrastructure may or may not be prevalent or available.
- Capable components or members of an IAN can dynamically form the network and its routing path. Additionally, a master node (command and control unit) may also be employed (including satellite backhaul and wireline/other tie-ins), that additional components would link to and thus expand network functionality (size and scope).
- The dynamic nature can also signify that there may be challenges related to providing complete geographic coverage and access to external elements. A MESA System of Systems deployment can facilitate overall resource management and situational command. Additional challenges may involve the prioritization of traffic.
- An IAN is capable of handling many different types of traffic and components, assuming common linkable elements.

6.2.2.3 Relations

Most devices that use the MESA IAN are also capable of communicating on the larger MESA JAN or communicate with a traditional JAN, given proper authorization. The JAN is engineered (i.e. infrastructure, spectrum, etc.) to reliably provide consistent coverage and QoS to a wide area that is usually defined by some authoritative jurisdiction (i.e. city, county, some countries, incident area). MESA devices may also be able to communicate on the JAN, when IAN coverage is not established or authorized. Many IAN devices are also capable of connecting to various PANs and even EANs, depending on an entity's planned or deployed architecture.

Communication in the IAN is very flexible by nature and can be coordinated by allowing devices to route communication between each other. This also allows incident specific information to stay localized. If certain communications are intended for a device not in the IAN, it will be routed through the IAN's connection to the JAN or other appropriate network, as exists or is authorized. When a device is in motion, its connection to the IAN adapts to ensure that connectivity is maintained. Other roaming capabilities are also envisioned (i.e. leave IAN jurisdiction and enter an established JAN).

6.2.2.4 Simplified schematic example of potential MESA IAN Ad-Hoc Network

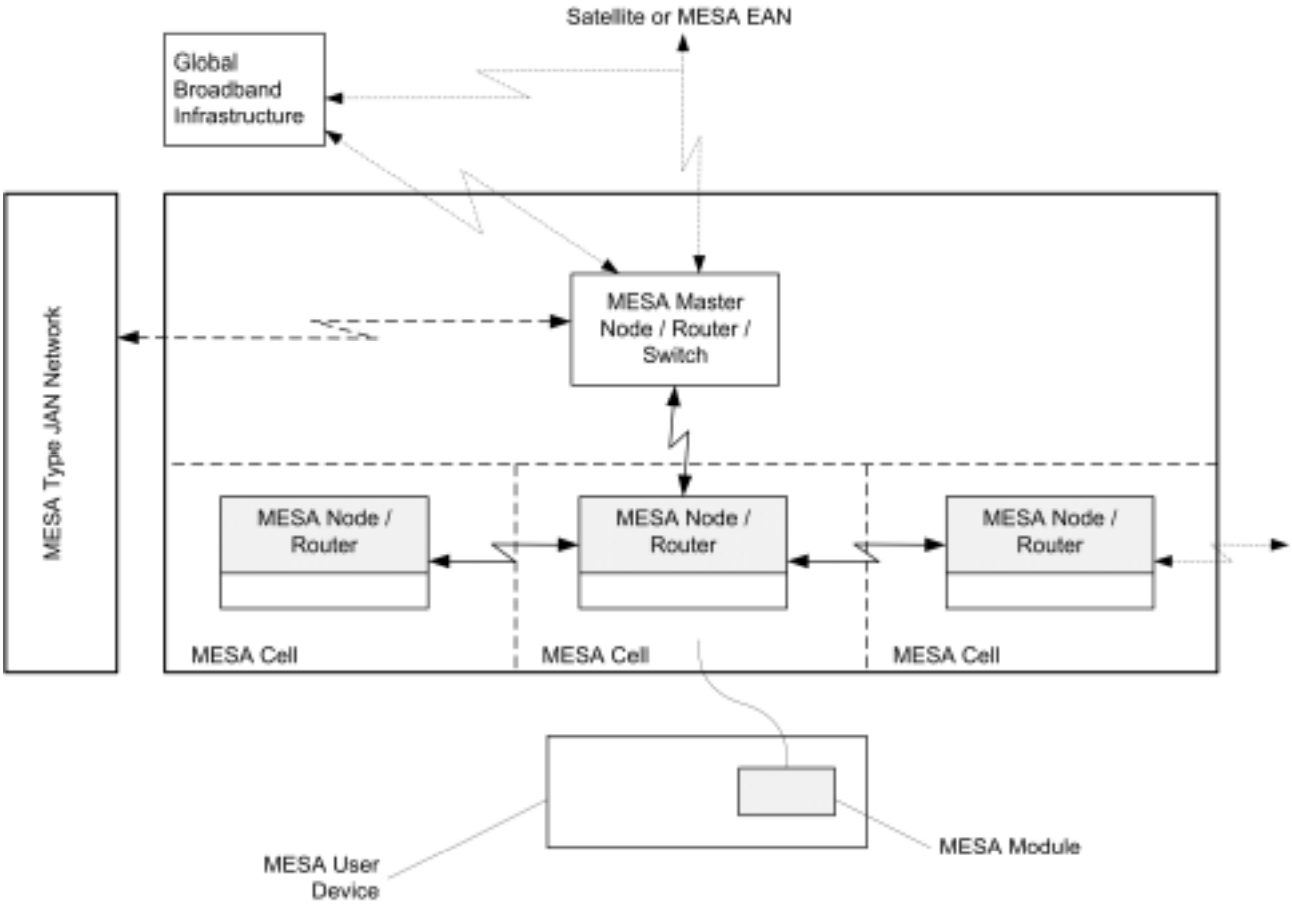

Figure 1

Figure 1 is a simplified example of a MESA Ad-Hoc network configuration.

6.2.3 JAN

6.2.3.1 Overview

The Jurisdiction Area Network (JAN) is designed to provide specific agency or shared access coverage over a wide area that may include such geographic boundaries as a city, county or country. The design and deployed placement of JAN infrastructure elements are well planned to ensure complete coverage and sufficient bandwidth, a high QoS level and reliability factor that corresponds to the nature of this mission-critical user group. The JAN's infrastructure utilizes powerful communication towers and other two-way broadcast infrastructure elements to provide for the capabilities mentioned above. These towers or communication link points can vary in both shape and size, depending on planning and coverage needs. Some are designed for placement on hill tops while other are much smaller and are designed for use inside buildings and tunnels. Note that a JAN may be synonymous with an EAN, depending on a jurisdiction's planned or deployed architecture. This clause mainly relates to more tradition JANs, however, a MESA System of Systems [JAN] deployment can also be considered a form of temporary or dynamically deployed JAN that connects and manages multiple IANs, PANs, etc.

Although a JAN is normally a static or predominantly pre-configured network, it allows for some dynamic reconfiguration. This may especially be the case with emerging or next-generation capabilities. If a particular jurisdiction needs supplementary resources, it is possible to allocate additional network resources to the affected area. For example, it is possible to augment the network with mobile transmission towers that can be repositioned in areas requiring additional or augmented resources. Additionally, it is possible to augment network resources and or enhance user capabilities through other available or Ad-Hoc infrastructure components; realizing that "mission-critical" quality levels expected in a planned JAN may be transformed while accessing such augmented resources. Even with these abilities the JAN is not as dynamic as an IAN. The JAN is dedicated to providing complete and consistent coverage over a specified jurisdiction. Therefore, the established JAN cannot radically shift resources as demands change because the JAN still needs to provide consistent availability across the entire coverage area.

JANs include traditional Land Mobile Radio (LMR) networks, with the infrastructure of the JAN providing network access and coordination over a large area. Such a JAN uses a topology were devices normally communicate through towers instead of talking directly to each other. Fixed infrastructures such as towers enable the JAN to provide a predetermined level of coverage for a specified area. The fixed topology of the JAN makes it possible to guarantee minimum performance and coverage levels. In some case this may allow the JAN to provide a higher level of coverage and mission-critical reliability than the IAN. Devices should be able to reliably connect to the JAN anywhere within the area of coverage. Connectivity handoff, with regard to device or terminal mobility, between the different JAN communication towers and associated infrastructure, should be seamless and invisible to the user. Additionally, the ability for peer-to-peer communications, to augment user capabilities, is recognised and desirable for next-generation designs. Next-generation capabilities may also include other flexibility options that are not tied only to the network.

The infrastructure of a JAN normally communicates with a Central Office. The Central Office can serve as a central location to manage communications across a jurisdiction. The actual operation of each Central Office will vary from jurisdiction to jurisdiction, but a central facility should exist for each jurisdiction. The management of operations within a jurisdiction may be co-located at a Central Office. However operations can also be handled at a separate, networked location. Allowing for management of operations to occur in the field, when needed, instead of a remote location, provides for increased and flexible situational awareness capabilities. The flexibility of the location of operational management makes this possible and takes into account the first responder "on-scene" command needs.

It is also important for the Central Office to have communication ties to other adjacent JANs, etc. and their respective command structure. Having a coordination of communication between neighbouring JANs is important to furthering the goals of Project MESA since events are generally confined to jurisdictional boundaries. This coordination needs to be at both the technical level and the procedural. The Extended Area Network, described in clause 6.2.3.2, describes a "bridging" capability for inter-JAN communication links. The EAN, in this case, would be the interconnecting link between JANs.

A MESA System of Systems-type JAN is similar in the sense of overall coordination and management, however, is more dynamic and temporary as it involves tying together other systems and components that a specific incident or event requires, across variant geographic scenarios. The MESA-type JAN is capable of supporting or coordinating a large number of applications and users, including all those supported by the IAN.

6.2.3.2 Characteristics

- Engineered to provide constant coverage and consistently reliable service over a wide area or jurisdiction.
- Utilization of a fixed topology that makes it possible to guarantee a certain level of coverage and resource allocation. A MESA System of System JAN is a variation on the "fixed" element, yet provides similar service as indicated.
- May allow for adjusting of network resources or augmenting of capabilities, but not as flexible as an IAN.

6.2.3.3 Relations

The infrastructure of the JAN provides access to the JAN and for connected devices as characterized in clause 6.3.2. In addition, some devices accessing the JAN may are also be able to access an EAN through the JAN. A device connected to the JAN may also have the capability to provide access to any networks it is connected to, depending on authorization. This allows for minimal devices on a PAN to be connected to the resources of the JAN (i.e. MESA-type JAN), if required. The ability to interconnect networks is one benefit of utilizing a system of systems approach that can utilize standardized solutions to provide interconnectivity. JANs can also be interconnected with each other through an EAN linkage or other means. This allows for interconnection, increased situational communications and potential component mobility from one JAN to another JAN (and its connected component or sub-network such as an IAN or PAN).

6.2.3.4 Simplified schematic example of MESA IAN and MESA JAN Integration

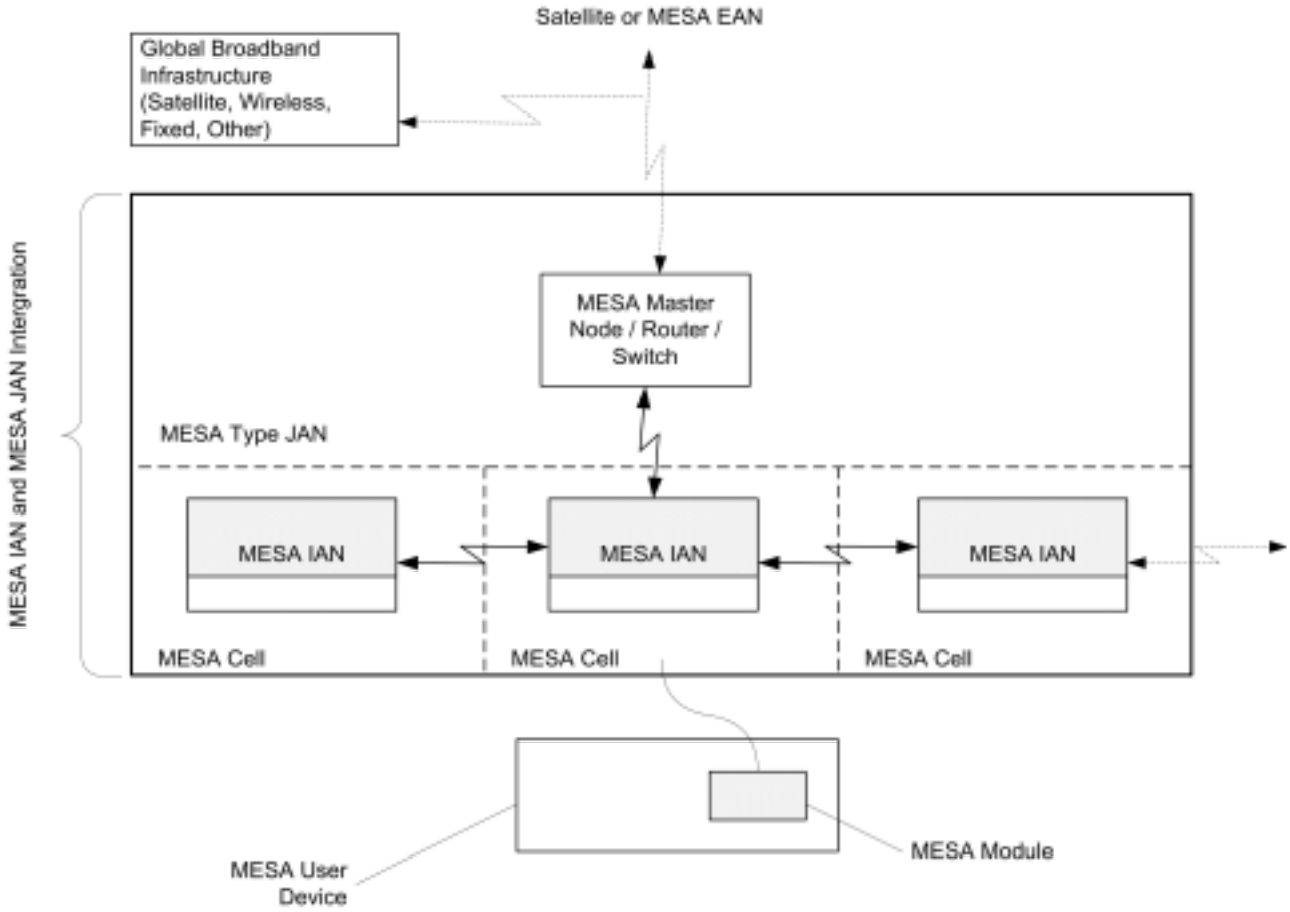

Figure 2

6.2.4 EAN

6.2.4.1 Overview

The Extended Area Network (EAN) can represent traditional backend networks used to access various databases and information sources. The EAN can also be designed to provide overlay services or access coverage over a very wide area and can be responsible for tying together various JANs. Note that JANs are frequently connected at the physical level and may also need to sustain or be required to provide end-to end security/authorization across such systems. The EAN can also provide for a bridging that allows for mobility and some form of access between JAN or other network access, and thus can provide for continuous basic access or seamless communication when travelling across or between jurisdictional boundaries or authorized networks. This also implies, for example, that a connection formed while in one IAN could be able to be carried over to another IAN or MESA JAN, via an EAN link, and that this authorized migration should happen automatically and with minimal user intervention.

The Central Office (i.e. Comm Centre, Dispatch Center) for each JAN should also manage the connection between that JAN and other JANs, through the EAN or other facilitating means. The Central Office already serves as a central coordination point for the JAN's entire communication infrastructure and also manages the communication within the JAN. This makes the Central Office a natural point from which to coordinate a connection to other JANs. Each JANs' Central Office should coordinate with each other to ensure that communication can migrate seamlessly between JANs.

NOTE: It is not always the case that the dispatch center is either a logical or physical connection point for inter-jurisdictional communications. An example includes the U.S. interagency messaging between mobile data systems (e.g. CapWin) and regular MDT/MCT traffic to motor vehicle systems, NCIC, NLETS, etc. This traffic does not generally get routed through dispatch. Most often, IT staff manages the connections between data systems. It is particularly true where cross-system credentials, as discussed in the previous clause, are of issue.

While the EAN plays an important role in the system of systems concept, it is not the focus of the present document. This is largely because the EAN is mainly a fixed resource and the interface between networks should be standardized by applicable standards bodies. Attention should be paid to the access and security procedures for the EAN to ensure compatibility across different implementations; however this is outside the scope of the present document.

As indicated above, the EAN can also be utilized, in a jurisdictional sense, for backend or backhaul networks used to transmit data to other jurisdictions, access various databases and information sources. The EAN can also be designed to provide overlay services or access coverage over a very wide area or entire jurisdiction (localized or across entire nation-state). Such a deployment can provide enhanced or augmented capabilities to traditional JAN, IAN or even PAN users.

6.2.4.2 Characteristics

- Connects JANs together.
- Provides extended or enhanced capability and access to databases and informational resources from a PAN, IAN, or MESA-type JAN and related devices.

6.2.4.3 Relations

The EAN can connect JANs and networks administered by various public safety agencies provide access to divergent databases or networks and provide access to the public Internet (as applicable) or VPNs.

The JAN can provide access to an EAN or use the EAN link to bridge multiple JANs. MESA devices that are able to access the JAN should also be able to access any appropriate EANs, depending on deployment scenario. The EAN can resemble an intranet, allowing users to connect to (backend) databases and provide global network connectivity. The EAN may also serve as a bridge to traditional or emerging communication technologies and access platforms, such as PSTNs, mobile infrastructure and public Internet services. Next-generation devices should also be able to seamlessly move from one JAN or unconnected IAN to another using this connection.

6.3 Structure/Architectural Scenarios

This clause is intended to illustrate general network architecture scenarios presented in the present document. Actual implementations can utilize these models as a starting point in determining their own system needs. Through customization of the components in the system, it is possible to address many different scenarios and specialized agency or user needs. Component terms seen in figure 3 are described later in the present document.

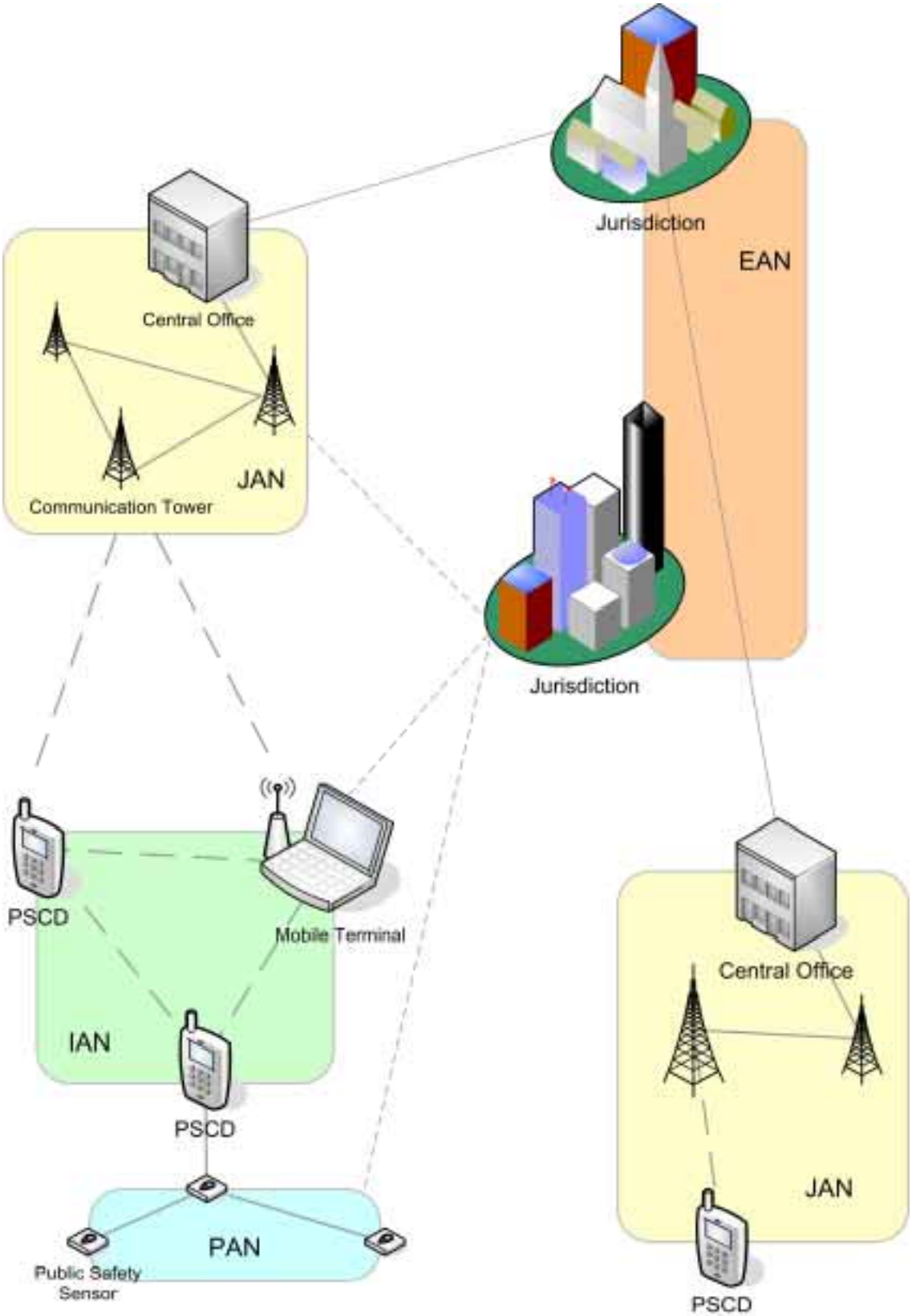

Figure 3

Figure 3 illustrates a variety of the connections and configurations possible in a MESA-capable system.

6.3.1 Overview

In order to get a better understanding of the Project MESA-defined system of system architecture, it is easiest to look at a typical configuration and the devices that access each network. There of course will be some exceptions to this configuration in complex or demanding scenarios. The descriptions below relate to the architectural scenario illustrations above.

6.3.2 Components

6.3.2.1 Public Safety Sensor and Networked Devices

The PAN is comprised of special purpose devices or components of limited scope and transmission radius. In many cases, devices on the PAN are sensors and these sensors are referred to as Public Safety Sensors. These sensors are generally limited to communicating with other devices on the PAN. An example can involve heart rate and ambient temperature monitors worn by first responders. Such a configuration involves three devices, including the two sensor devices and one device which aggregates the data and transmits it to the radio or terminal device utilized by the first responder or other public service/safety user. Data could also be transmitted from the third device to a command monitoring point. The first responder radio referred to is called the Public Safety Communication Device (PSCD) and explained in detail later. The third device's data-logger functionality is also capable of recognizing preset events, such as a spike in temperature, and pushing an alert to the associated PSCD. In addition the PSCD can poll the data-logger device for updated monitoring information.

It is important to emphasize that this is an envisioned configuration to illustrate the general architecture. It is plausible that different devices or terminal types are utilized, or that devices are focused on another subject type, such as a building. The PAN and the devices connected to it are specialized for a defined subject, such as a building, person or vehicle, and encompass a limited functional radius. Interconnection with other PANs or networks allows for increased communication reach, coordination and information flow.

6.3.2.2 Communication Devices

The Public Safety Communication Device (PSCD) and the Mobile Terminal are both general types of communication devices. The major differences between the device types relates to the portability and capability levels of the devices. A PSCD is generally a handheld or mobile device and may not include as many capabilities in the interest of conserving power and weight. A Mobile Terminal is usually vehicle based, allowing it a more dependable power supply, improved antenna placement or reach and improved transmit/receive functionality due to increased power levels. Note that the term "Mobile", in this specific context, does not translate to other uses of the term or the term mobility, as "Mobile" in this Public Safety context usually involves vehicles or other similar situations. The term "mobility" utilized in standards activities has more relation to a PSCD than a Mobile Terminal.

Both device types are capable of communicating over an establish IAN or a JAN. When the PSCD is in range of an IAN, all communication will be through the IAN. If an IAN is not reachable or one has not been established, communication will go through the JAN, as able or authorized. Depending on individualized structure, the communication devices are also capable of connecting to PANs, EANs or other networks, as capable and authorized. A PSCD or Mobile Terminal can also serve as the aggregate point for a PAN and monitor the values of connected devices and may be capable of forwarding information from the PAN onto the IAN or JAN if necessary. The devices on a PAN that a PSCD would connect to, for example, might include heart rate monitors, geo-location sensors, motion sensors and many more. A Mobile Terminal, for example, might connect to the existing JAN and to a PAN, including functionalities that could include the vehicles light bar and the various sensors, video units and other elements incorporated into the vehicle.

An IAN is dynamically formed between the enabled communication components or devices in given area. The most capable devices are responsible for determining the structure of the network (i.e. accessing and linking to a Master Node) and providing the network, as appropriate, a linkage to a MESA-type JAN or provide resources such as a bridge to external networks. The coordination of communication between all of the devices in an IAN could be handled by a specific or master device on the IAN or through a MESA-type JAN (i.e. System of Systems). In many cases, the vehicle-based Mobile Terminals could assume this role as they may offer a stable point from which to build a network around. A Mobile Terminal can also allow for a more stable connection due to better antenna location and length, increased signal strength dynamics and a dedicated power source. However, there are many cases when a Mobile Terminal is not practical or desired, and as such, an IAN could be formed by two or more mobile (untethered) PSCDs. The method used to form MESA IANs is adaptable enough to handle a wide variety of communication device deployments and also can involve variant architectures and networks. Other network types utilize communication devices and terminals as appropriate for their architecture and needs. MESA devices should also be inclined to self-heal and re-establish connections.

6.3.3 Connections

This clause illustrates potential connections relating to the overall communication architecture and as found in a MESA-capable system and includes communication scenarios between devices or other components that may or may not include MESA-capable devices. This information includes the relationship between network and device types, and both the components" interfaces and the links between them. Actual deployment structure and context depends on jurisdiction, capability needs and deployment options.

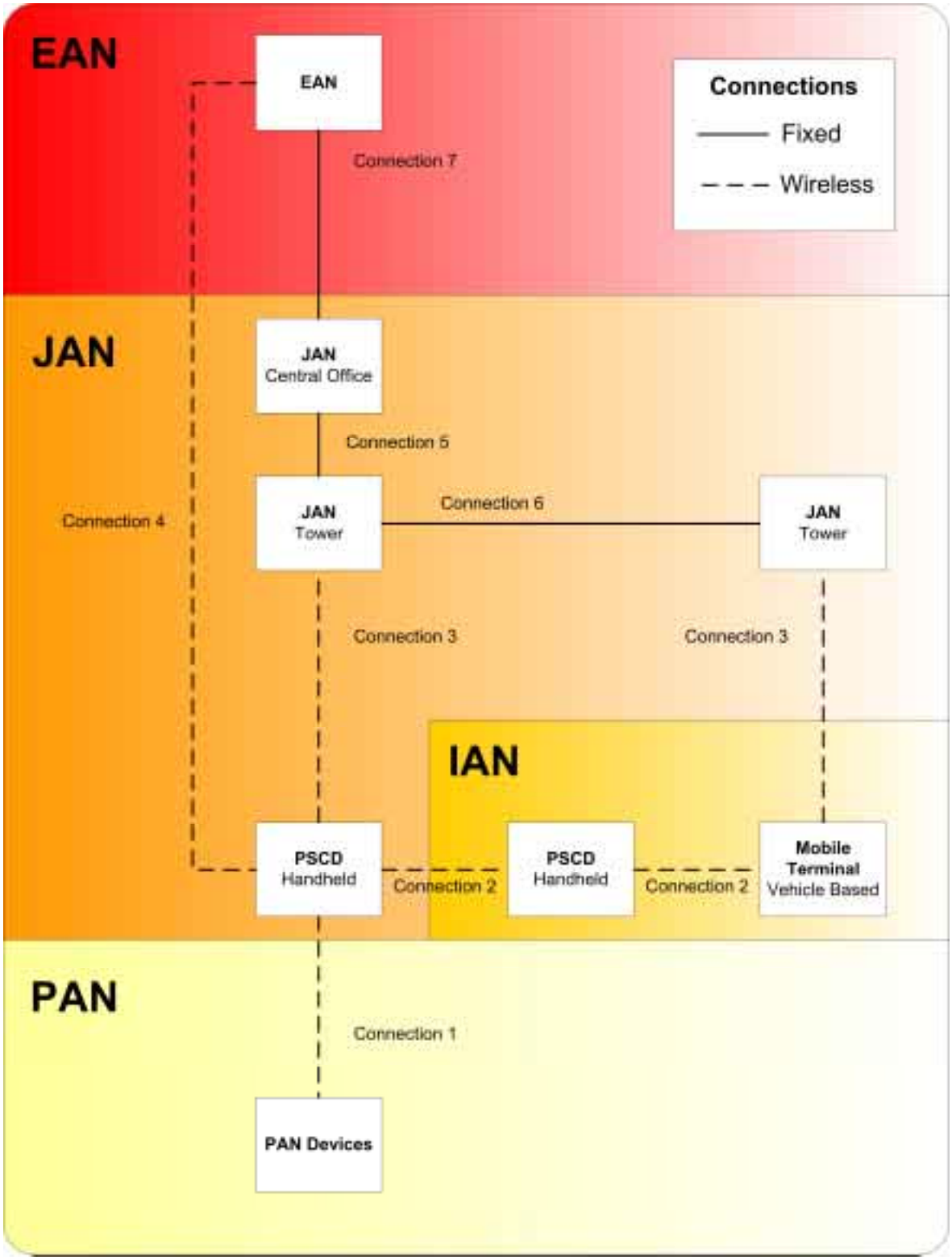

Figure 4

Figure 4 helps enumerate the possible connections in a MESA system.

6.3.3.1 Connection 1

Connection 1 is a connection between a Public Safety Sensor and a PSCD. There may be more than one sensor, and the data is either aggregated by a designated device and transmitted to the PSCD and other destinations or aggregated at the PSCD itself. The distance of this link is generally short. The interfaces utilized are generally wireless, but may be wired in some instances.

6.3.3.2 Connection 2

Connection 2 is a connection between Communication Devices. This connection creates an IAN. A Mobile Terminal or PSCD may also connect with other such devices through this link or interact with a "home" JAN.

6.3.3.3 Connection 3

Connection 3 is a connection between a Communication Device and a JAN communications tower (or related structure). This connection is used if the Communication cannot establish a connection to an IAN or if the JAN is the appropriate network connection.

6.3.3.4 Connection 4

Connection 4 is a connection between a Communication Device and the EAN. This connection utilizes overlay services or access coverage provided by cellular, satellite or another 3rd part service to connect with the EAN.

6.3.3.5 Connection 5

Connection 5 is a connection between a JAN communication tower (or related structure) and the JAN central office. The JAN central office contains the dispatch office for the jurisdiction. In addition the JAN central office handles interfacing between an established EAN and the JAN. Not all JAN communication towers are connected to the JAN central office. Some JAN communication towers may only be connected with another communication tower and route communication through that connection. Towers or other such structures can also be utilized purely to provide jurisdictional coverage such as a repeater.

6.3.3.6 Connection 6

Connection 6 is a connection between JAN communication towers (or related structure). Most communication going across this link will eventually go to the JAN central office. However this connection allows for towers, or designated communication points, to communicate directly. This connection could be used to forward communication from one area of the JAN to another.

6.3.3.7 Connection 7

Connection 7 is a connection between the JAN central office and an established EAN. This connection is used to allow different JANs to communicate and access off-site data sources.

7 Network Requirements

7.1 PAN

This clause describes the different classes of services and applications a PAN should support. Class 0 should receive the highest level of preference, followed by Class 1 and so on. The transmission, queuing and processing of communications should adhere to these Classes of Service.

7.1.1 Class 0

7.1.1.1 Characteristics

- Used for emergency alerts and related critical communications.
- Messages and other payloads MUST be delivered in the timeliest of manner. Techniques should be used to ensure this critical characteristic.
- Packets should be delivered with in a fixed amount of time and latency.
- Rate control should be practiced to prevent overloading the network.

7.1.1.2 Description

In the PAN, this class of service is used for critical emergency alerts. This type of communication is generally a short alert message, announcing that a certain event has occurred. It is important that this communication is successfully received in a minimal amount of time. Devices should be able to depend on the network delivering the message within a fixed amount of time.

7.1.1.3 Applications

Generally these transmissions are triggered by an abnormal event. The event could be a ballistics vest detecting impact or another sensor detecting a dangerous environment / condition. When such an event occurs, the application transmits a short message to describe the event. The message may also trigger an automated response, serve as an alert that the event occurred, or trigger augmented payload/data transmission to other internal and external elements.

7.1.1.4 Network Requirements

At this level of service the PAN must support:

1. A bounded delivery time for messages. This provides a real-time communication environment. It limits how long it will take for another device to react to an event.

7.1.1.5 Application Requirements

On this network and at this level of service, applications must support:

1. A rate control mechanism that ensures each unique event is reported in a timely matter, but duplicate event messages get filtered out. The volume of messages should scale to ensure that a reliable communication channel exists.

7.1.2 Class 1

7.1.2.1 Characteristics

- Used for normal status updates and communication or alerting needs.
- A best effort should be made to deliver messages.
- Failed messages should not be retransmitted.
- Rate control should be practiced to prevent overloading the network.

7.1.2.2 Description

In the PAN, this class of service is used for normal or day-to-day communications. This class is generally used for transmission of data that is constantly being updated. Retransmission of a failed message is generally not needed since updated data will get transmitted periodically.

7.1.2.3 Applications

This class is used for normal communications between devices. This can include querying the status of a Self Contained Breathing Apparatus (SCBA), the heart rate of a first responder and other data communication needs. Applications should use this class for communication that is important but not unexpected. Since the messages are normally automated, rate control should be practiced in order to allow the network to scale.

7.1.2.4 Network Requirements

At this level of service the PAN should:

1. Make a best effort to deliver a message but should not guarantee message delivery.

7.1.2.5 Application Requirements

On this network and at this level of service, applications should:

1. Control their transmissions in order to prevent overloading the network.
2. Not retransmit failed messages. Instead, applications should wait until fresher data is available or a periodic transmission occurs.

7.2 IAN

This clause describes the different classes of services and applications an IAN should support. The dynamic and flexible nature of the IAN makes it a unique networking environment. Applications and networking techniques should take this into account and act accordingly.

Class 0 should receive the highest level of preference, followed by Class 1 and so on. The transmission, queuing and processing of communications should adhere to these Classes of Service.

7.2.1 Class 0

7.2.1.1 Characteristics

- Used for mission-critical voice and video conferencing, and other critical data communication needs.
- Messages or payloads must be delivered immediately.
- Extremely low and stable latency is required.
- Retransmission of messages is not allowed due to latency requirements.
- Messages must be able to be delivered to multiple recipients and or authorized groups.
- Multiple recipients must receive the messages at the same time to allow for real-time critical coordination and efficient communication.

7.2.1.2 Description

In the IAN, this class of service is used for mission-critical voice, video, and other data communication. This requires extremely low latency, little to no jitter, and negligible packet loss. Network performance in both directions needs to be similar to allow for full-duplex voice and video communications. Messages delivered to multiple recipients should arrive at similar times. These communications should be of the utmost priority for the network.

7.2.1.3 Applications

This class of service should be used by mission critical voice and video conferencing applications. The conferencing is used to deliver life-critical communication. Other critical data applications may also apply. In this class of service, network performance is not negotiable, and all resources can be devoted to ensure the required level of network performance is met.

The nature of the communications means that the entire message should be delivered quickly and completely to all designated recipients. All recipients should receive the message at the same time, since the communication is used for coordination.

7.2.1.4 Network Requirements

With this class of service the IAN should:

1. Deliver messages with a minimal amount of latency.
2. Involve latency that is similar for all recipients and in the reverse direction.

3. Minimize the amount of variability in latency (jitter).
4. Use techniques to minimize any chance of packet loss. Re-transmission of lost packets is not an option with this class of service.
5. Correctly deliver messages to recipients even if the topology of the network changes or is in a state of change or reconfiguration.
6. Be possible to designate multiple recipients for a message's destination.
7. Dynamically change or re-allocate network resources available to this class in accordance to need.

7.2.1.5 Application Requirements

On this network and with this class of service, applications should:

1. Identify all users currently participating in the conference or grouping.
2. Recognize that users should be able to dynamically join and leave groups.
3. Use techniques to prevent and correct errors in communication. This may include Forward Error Correction coding.
4. Make the user aware if errors in communication are occurring.

7.2.2 Class 1

7.2.2.1 Characteristics

- Used for non-mission-critical voice and video conferencing.
- Minimal amount of latency, jitter and packet loss.
- Designed for group communication at both the network and application level.
- Application should prevent and correct for errors.

7.2.2.2 Description

In the IAN, this class of service is used for non-mission-critical voice, video and other data communication. While this class of service has similar requirements as class 0, performance allowances can be made to give class 0 communications more resources or to allow for scalability. Low latency, low jitter and a negligible amount of packet loss are required at this level of service. Some communications may require improving one performance characteristic at the expense of another. It should be possible to designate this through a Quality of Service (QoS) function. The ability to communicate with a group is required with this form of communication and this should be supported at the network layer.

7.2.2.3 Applications

This class of service should be used for more conventional (based one's specific user scenarios) or applicable day-to-day voice and video applications to support emergency operations. This class is appropriate for communications that can be repeated or clarified if they become lost or corrupted. While the network will take steps to prevent the loss and corruption of communication, the application should also be able to correct for them if they occur. The conferencing application should allow for a group or groups of users to communicate with each other, and allow such users the ability to join and leave the group as desired and authorized.

7.2.2.4 Network Requirements

With this class of service the IAN should:

1. Deliver messages with a minimal amount of latency.
2. The latency should be similar for all recipients and in the reverse direction.
3. The amount of variability in the latency (jitter) should be minimal.
4. An effort should be made to minimize packet loss. The technique used should not compromise network performance or scalability.
5. Message should be correctly delivered to recipients even if the topology of the network changes or is in a state of change.
6. It should be possible to designate multiple recipients to a message.
7. The network should use rate control to allow for scaling and the dedication of service to class with a higher precedence.
8. A method for provision of QoS should be available to allow applications to give preference to a particular performance metric.

7.2.2.5 Application Requirements

On this network and with this class of service applications should:

1. Identify all users participating in the conference.
2. Users should be able to dynamically join and leave groups, as applicable.
3. Use techniques to prevent and correct errors in communication. This may include Forward Error Correction.
4. If there are errors in communication, the user should be made aware.

7.2.3 Class 2

7.2.3.1 Characteristics

- Used for signalling and control messages.
- Minimized latency and packet loss.
- Messages should be prioritized to facilitate rate control.

7.2.3.2 Description

In the IAN this class of service is used for signalling and control messaging for applications. Both latency and packet loss should be low for this class of service. The loss or delay of packets in this class of service may have an impact on the applications operating in class 0 and 1. Packets should make up a small amount of the overall network usage and should not be sacrificed to devote more resources to class 1. TCP or a similar protocol should be used to ensure packet delivery. Packets need to also be delivered in sequential order to the application.

7.2.3.3 Applications

This class of service is used by applications to send signalling and control messages. A conferencing application might use signalling messages to join a group or announce the presence of a user. A video surveillance application would use this class of service to send a message to control a remote camera. Other similar functions can be envisioned. Applications should actively work to ensure that they send out the minimal amount of messages necessary to the minimal amount of people. In addition, applications should prioritize their messages to allow for a reduction in the number of such messages if the network becomes overloaded.

7.2.3.4 Network Requirements

With this class of service the IAN should:

1. Minimize latency and packet loss.
2. Should follow the prioritization designated by the application when reducing the message volume.
3. TCP or a similar session protocol should be utilized and to ensure an "in order" or sequential packet delivery guarantee.

7.2.3.5 Application Requirements

On this network and with this class of service applications should:

1. Work to control the volume of messages they send out.
2. Messages should be prioritized in case some messages need to be dropped.
3. Applications should propagate only recent and relevant signalling messages.

7.2.4 Class 3

7.2.4.1 Characteristics

- Used for Instant Messaging and database queries.
- Packet loss should be prevented.
- Latency should be reasonable.

7.2.4.2 Description

In the IAN, this class of service is used for interactive low bandwidth communication. While this class of communication would benefit from low latency, it is not essential. A reasonable amount of latency is acceptable with this class. Like most forms of communication, packet loss is not acceptable. Since there are not tight latency requirements, it is possible to resend lost packets. Packet ordering should be maintained if possible. TCP or a similar protocol should be used to maintain ordering and prevent packet loss.

7.2.4.3 Applications

This class of service is used by applications to send Instant Messages and query databases. Other possible usages might include text-based alerts and automated messages triggered by an event. Applications should include the option of automated or pre-defined messages to allow for use on capability-limited devices.

7.2.4.4 Network Requirements

With this class of service the IAN should:

1. Efficiently distribute messages to multiple recipients.
2. Correct for packet loss if it does occur.
3. Accommodate multiple recipients.

7.2.4.5 Application Requirements

On this network and with this class of service, applications should:

1. Provide the option of automated or pre-defined inputs.
2. (optional) Provide automated text to speech converters to allow for easier field operation.

3. (optional) Provide automated or "opt-in" capabilities to allow for usage by persons with disabilities or impairments.

7.2.5 Class 4

7.2.5.1 Characteristics

- Used for the transfer of large amounts of data.
- Messages can be delayed as long as user response time is reasonable.
- Packet loss should be prevented but packet transmission may be deferred to other classes.

7.2.5.2 Description

In the IAN this class of service is used for high bandwidth communications that are not time dependant. The packets are time sensitive but they do not become less important if they are delivered slightly later. This allows the network to give preference to higher classes of service as long as it is still able to deliver the message or payload in a timely manner. Messages can be queued or delayed as long as user response time does not suffer.

The network also makes an effort to prevent the loss of packets. Since all communications in this class of service are bulk data, preventing the loss of packets prevents the eventual retransmission of the packet. However packets maybe dropped to give preference to other classes. It is beneficial to the network to prevent the loss of these packets since the network will try to resend them.

7.2.5.3 Applications

This class of service is used by many applications. It provides a level of service needed by many high performance data applications. These applications include voice messaging, GIS and mapping, high-resolution photo transfer and the streaming of near real-time video. This class of service is too general to specify all of the possible applications and their requirements. In general, applications using this class of service should allow for network delays and buffer accordingly. In addition applications should also allow the network enough time to correct for errors before resending packets or requesting the packet again.

7.2.5.4 Network Requirements

With this class of service the IAN should:

1. Limit preventable packet loss.
2. Deliver packets in a timely manner.

7.2.5.5 Application Requirements

On this network and with this class of service applications should:

1. Allow for network delays by buffering messages.
2. Allow the network a reasonable amount of time to correct for errors.

7.2.6 Class 5

7.2.6.1 Characteristics

- Used for general network applications.
- Messages may be dropped or queued to benefit other classes.

7.2.6.2 Description

In the IAN, this class of service is used for traditional network communication. This class of service is provided the least level of service guarantees and is suitable for traffic that can be preempted by more important classes of service. If a network has extra capacity it can increase the preference given to this class of service, however applications should not expect such treatment.

7.2.6.3 Applications

This class of service is used by general networking applications. The applications range from web browsing to E-mail. These applications should have very few expectations of the network other than normally expected. Applications running at this class will not receive any preferential treatment and will have to defer to applications running at other classes.

7.2.6.4 Network Requirements

With this class of service the IAN should:

1. Improve the level of service if extra capacity exists.

7.2.6.5 Application Requirements

On this network and with this class of service applications should:

1. Have no expectations of any level of service provided by the network.

7.3 JAN

The classes of service provided by the JAN are equal to those previously provided for the IAN (see clause 7.2) and the description of these service classes will not be repeated in this clause. The IAN classes of service should be referenced as needed. Additionally, the network considerations for the JAN are similar to those of the IAN. Both networks need to maintain connectivity and session information as nodes or devices shift from accessing one network component to another, and across variant jurisdictional locations. Unlike the topology of an IAN, the JAN's topology allows for established and centralized control, making session management easier across network components. The requirements for either network are similar, however the method used to reach these requirements may differ. JANs frequently have rigorous auditing requirements, including system and/or network transaction audit trails, the ability to provide statistical reports and agency-by-agency and site-by-site reports.

8 Device Requirements

8.1 Common Communication Device Requirements

There is a core set of features that are common among MESA-capable devices that will be utilized to provide next-generation public service and safety communications. Some of these features are required while others are optional. The optional features are included in some devices in order to allow them to meet the specific needs of a defined task or mission.

8.1.1 Required

These features are required in all common communication devices. They are necessary in order to provide the stated level of service. Some non-common devices and features utilized by a network user may be different as they enhance user capabilities and are not necessarily part of structured network. However, all communication devices utilized by users should strive to fulfil the requirements articulated in this clause, thus promoting functionality across the Public Safety communication sector.

1. All devices must include a built-in "help" system and allow for a training mode. The help system should provide contextual assistance and guide the user through specific tasks. The training mode should allow the user to practice tasks without affecting the networks operation.

2. All devices must capture operational data and make the data accessible to appropriate requesters. The captured data should be tamper resistant and authoritative.

3. All devices must be capable of locally storing data. The amount of storage required depends on the capabilities of the device and the features it provides.

4. All devices must be able to transmit to other authorized devices based upon their relative location. For instance, transmitting to all devices within a given radius.

5. All devices must support status queries from an authorized source. Devices should be able to have all of their relevant status information queried both locally and from a remote location.

6. All devices must support some degree of over the air re-programming or re-configuration. The re-programming should occur in a reasonable amount of time. Multiple devices should be able to be re-programmed at the same time. Actual degree of re-programming may be dependent on emerging technologies and needed user capabilities.

7. User profiles and customization should be transferable from one device to another. A user should be able to move from one device to another within an established network; having the existing profile cloned to the new device, resembling the original device. This allows devices to be used interchangeably and provides a consistent user experience.

8. All devices must support forms of hands-free operation. Applications supported in this way may vary due to specific needs, technological capability or ergonomic/form-factor issues relating to defined user needs.

9. All devices must support "plug and play" components. Add-on components should be able to be swapped from one device to another. Supports standardized, multi-vendor compatibility.

8.1.2 Optional

While these features make for a more capable device, they may not be necessary in all user scenarios and applications.

1. Devices may support advanced identification techniques including biometric identification. Techniques used should be compatible across devices supporting this feature.

2. Devices may support voice or keying commands, allowing a user to control the device through a pre-defined set of commands. This feature allows for a greater level of hand-free operation.

3. Devices may support a voice-based language translation feature. This feature would allow for spoken words to be translated into a different language. This feature should allow users to translate from their native language to a foreign language and back from the foreign language to the native language.

4. Devices may support communications capabilities and interfaces for the disabled or impaired, including telecommunications for the deaf (TTY/TDD) or emerging Braille applications.

5. Devices may support adaptive or cognitive transmission techniques. For example, by changing transmit power or coding scheme a device can adapt to a challenging RF environment.

6. Devices may support transmission techniques that have a low probability of detection. This feature is used to mask transmissions, something valuable in covert or other secure operations.

8.2 Mobile Terminal

Mobile Terminals are usually vehicle-based communication devices that public safety personnel utilize. The features found in these devices, as previously illustrated, do not extend beyond the general feature set described above.

8.3 Public Safety Communication Device

The PSCD is frequently carried by the first responder or other specialized communities, so there are some additional ergonomic features that are not part of the general requirement set.

8.3.1 Required

1. All devices have a maximum weight that they must be under, depending on mission. The maximum weight is determined by the device's usage.
2. All devices must have an acceptable shape or form-factor that is designed for the task in which they are being used.
3. All devices must have a minimum battery life. The required battery life is defined separately for each public service and safety discipline (i.e. first responders).
4. All devices must adhere to usability standards specified by service disciplines. The usability standard should include specifications on button size and placement.
5. All devices must not cause the user undue fatigue during continuous usage.
6. All devices must accommodate a wide range of users, from a user who is smaller than 95 percent of the population to a user who is larger than 95 percent of the population.

8.4 Public Safety Sensor

Many devices utilizing the PAN are sensors and other related elements. These devices vary in complexity from temperature sensors to remote controlled video surveillance cameras. They are designed to operate without user intervention and they alert users if certain events occur. A public safety sensor must support a set of core features.

8.4.1 Required

1. All devices must support queries over the network from other devices.
2. All devices are limited in transmission radius, similar to RFID capture/transmission functions but possibly more complex and varying radius parameters.

History

Document history		
V3.1.1	January 2006	Publication