Mutualink System Description

September 29, 2017

Version 1.0

Presented by:

Mutualink, Inc.
1269 South Broad Street
Wallingford, CT 06492
www.mutualink.net

Joe Boucher
Chief Technical Officer
Phone: (978) 467-4717
JBoucher@Mutualink.Net

Contents

1. Background

1.1 What is Mutualink?

Mutualink is fundamentally a cross-agency collaboration/interoperability system. It allows sharing of *any* media within & between *any* agencies over *any* networks.

The Mutualink distributed architecture allows each agency to preserve full sovereignty by enabling agencies to maintain exclusive control over their shared resources at all times.

Full multimedia communication is enabled:

- Voice: Radios, phones, users, PTT systems, PAs, intercoms, etc.
- Video: Cameras, video management systems, smartphones, webcams, etc.
- Text messaging, chat rooms, File sharing
- Location & GIS data sharing
- Generalized device data/information sharing

Mutualink is a highly-secure system; all participating identities are mutually authenticated, and all media is fully encrypted.

1.2 The Multi-Agency Interoperability Problem

Every public safety agency has private communications systems, data systems, etc. These systems are administered within the agency for security purposes, i.e. limiting access to internal personnel. In addition, these systems are necessarily isolated from similar systems in other agencies due to the very real need for securely controlling access to the systems and the data within. These isolated systems are called silos in some contexts.

Although silos are necessary constructs for maintaining agency sovereignty and control, they have a significant disadvantage when multiple agencies need to work together at incidents or events. This mutual response requires agencies to share information and communications to be effective in working together. It is in these situations where silos present an obstacle to the required collaboration.

Therefore, silos are good for security domains, yet bad for inter-agency interoperability.

2. Solution Overview

2.1 Virtual PTT Talkgroups

Virtual talkgroups can span multiple agencies and multiple disparate systems. Members of a talkgroup may include:

- PTT and MC-PTT applications on mobile devices and PCs using LTE, Wi-Fi, wired, etc.
- Trunked and conventional LMR channels/talkgroups
- PSTN and VoLTE calls
- PA systems, intercoms, and any systems capable of transmitting and/or receiving audio
- Any IP voice system compliant with the Session Initiation Protocol (SIP), Bridging System Interface (BSI), or P25 ISSI/CSSI specifications

Talkgroups may be administratively defined for more static use cases, or may be created on-the-fly as needed, e.g. for an incident response. This is a very powerful capability of Mutualink - any user may create an ad-hoc talkgroup, invite other users to it, and even add any of the above member types to it as needed such as an LMR talkgroup or PSTN call, etc.

Talkgroups are a voice-only group type of the more general Multimedia Sharing Group, described below.

2.2 Multimedia Sharing Groups

A uniquely differentiating feature of Mutualink is that it enables virtual talkgroups to include and share not just voice, but also full multimedia and data between all its members. These groups then become more than just "talkgroups" and can therefore be thought of as more generalized multimedia sharing groups.

2.2.1 Video

Video sources in a sharing group may include:

- Video cameras (IP or analog)
- Video Management Systems (IP or analog)
- Built-in cameras in Smartphones, tablets, laptops, or webcams
- Screen-sharing and window-sharing applications

Any video sources in a group may be viewed by any member of the group by using the Mutualink application on mobile devices or PCs, as well as any video monitors, etc. that are a member of the group.

A screen and/or an application window may be shared with other group members; this is commonly used to share situational awareness applications and private data system views to the group.

2.2.2 Text Messaging

Text messaging/chat capability is also included in all sharing groups; this messaging may also be extended to text-capable LMR radios that are in the group. In addition, groups may be connected to third-party chat rooms/services to further extend this capability.

2.2.3 File Sharing

Group members may also share files with each other. This is useful for items such as documents, pictures, floor plans, screen-shots, etc.

2.2.4 Location and Geospatial Data

Members may share their current locations with each other as well as share any geospatial or georeferenced data that is relevant to the group's mission. Integrations to CAD and AVL systems allow group members to share incident location, vehicle/asset locations, etc. with the group. This information may be viewed on a shared group map to establish a common operating picture across the group.

2.2.5 Data and Application Sharing

Application-specific data may be shared to the group; this allows disparate systems that understand a common data format to exchange information with each other. For example, this may be used to exchange data between CAD systems from different agencies, or between installations of the same application in multiple agencies.

2.2.6 Sensor Integration

Biometric, environmental, alarm, etc. sensors may provide information to the group or specific users using any of the media or data types described above. Such sensor data may also be used to trigger specific actions to occur in the system, for example to notify nearby and/or remote users that a particular event has occurred.

2.3 Users as Group Members

Users participate in sharing groups in one of two ways: 1) Using a Mutualink application on a supported device, or 2) Using another application or communication system that's connected to the group. The latter is accomplished using a Mutualink gateway as described in the next section; this section describes the Mutualink application.

The user application ("Collaboration GUI") is the primary user interface to the full suite of Mutualink capabilities. Users of this application may communicate/collaborate directly with each other using voice, video, text messaging, file sharing, location and geospatial data sharing, and screen sharing. In addition, users may direct the operation of Mutualink gateways that they are authorized to control.

2.4 Gateways as Group Members

Mutualink gateways enable external systems and devices to participate in a sharing group.

Gateways connect to an agency's existing communication or data system to enable media/data from that system to be selectively shared with and interoperate with other agencies via the Mutualink system.

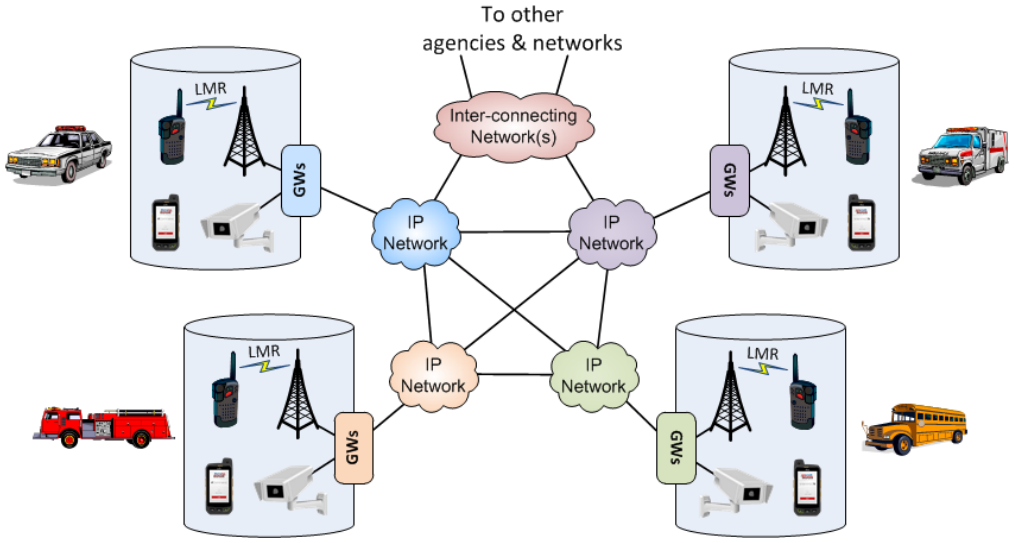
A gateway may be a physical device (e.g., when analog interfaces are required) or a logical software module (e.g. when only IP interfaces are required). Software gateway modules may reside on a small or large-scale server platform (either hosted or on premise) or co-exist with a Mutualink user application on a laptop/desktop platform, etc.

Types of gateways available include:

- **Radio Gateway**. Interface to analog or digital LMR systems, intercoms, PAs, etc.
- **Video Gateway**. Interface to analog or digital video feeds/cameras/systems/wearables.
- **Telephony Gateway**. Interface to analog or digital telephony systems, PBXs, PSTN, SIP systems.
- **System Gateway**. Interface to multimedia communication systems, PTT systems, group systems.
- **Data Gateway**. Interface to arbitrary data systems to provide application-specific or opaque data connections, e.g. CAD incident data, sensor/alarm data, or GIS and AVL systems for location and geospatial data.
- **Event/Alert Gateway**. Interface to alert/notification systems.

2.5 Enabling Multi-Agency Interoperability

Given the well-understood problem of siloed agency communication systems, the Mutualink solution selectively and securely bridges existing siloed systems together, as depicted in the following diagram.



Important aspects of this solution:

1. In each silo, gateways ("GWs") are connected to the communication and data systems that the owning agency wishes to share with other agencies
2. These gateways are then connected to one or more IP networks that allow the gateways to communicate with each other.
3. The gateways may be controlled by authorized users whether they are within the owning silo or remote within the inter-connecting networks. These users direct what information from the gatewayed systems should be shared to which sharing groups.

This is a distributed system in which the gateways and users may communicate directly with each other. No central servers are required to enable this interoperability; such central control points could introduce undesired third-party control and therefore loss of sovereignty by the various agencies.

2.6 Group Behavior

Talkgroups and Multimedia Sharing Groups in the Mutualink system may be either static or dynamic:

- Static groups are typically created by administrators, typically for teams that frequently work together.
- Dynamic groups can be created by any authorized user. They can then invite other users and gateways into the group; users can accept or reject that invitation.

Groups can span agencies as well as multiple local and remote networks.

Each member can push any form of media/data to the group, each member then decides which media/data they wish to consume.

All media/data in the group is highly encrypted with a dynamic per-group encryption key.

2.7 System Security

A Mutualink system consists of at least one security domain. The foundation of every security domain is a Public Key Infrastructure (PKI) that is managed by the domain administrators.

Identity Validation

All users and gateways in a domain are authenticated by the domain administrators and are issued a signed X.509 certificate from one of the PKI's Certificate Authorities (CAs).

Users and gateways mutually validate each other's identities with asymmetric encryption and signatures using public key cryptography based on these certificates.

Group Encryption

When a sharing group is created, a new symmetric encryption key is dynamically generated. When another user or gateway is invited to the group, the asymmetric key is passed securely from the inviter to the invitee.

All group media and data is encrypted and decrypted with the symmetric key.

3. System Components

The Mutualink system is very modular; any number of the following components may be mixed and matched in a deployment as needs dictate.

3.1 Mutualink User Applications

There are two types of Mutualink user applications available:

1) Standalone IWS applications (a.k.a. thick clients). These applications run on Windows and Linux and do not require a server to function; they may communicate directly to each other and other Mutualink components over supported IP networks.
2) Edge IWS clients (a.k.a. thin clients). These applications run on iOS, Android, Windows, Mac, and Linux and must connect to a Mutualink Edge server to function.

The standalone IWS application is also available on a dedicated Windows or Linux appliance.

The IWS applications include the ability to:

- Create groups, invite other users to groups, accept or decline invitations from others

- Add authorized gateways to groups, choose channels/feeds/users/groups from external systems to share/connect to a group
- PTT voice transmit and receive
- Share video from local cameras, share screens or windows, view video & screens from others
- Send & receive text messages, send & receive files
- Share their location, view group members on a map, invite others to groups from the map
- Overlay traffic, weather, etc. on group maps

3.2 Mutualink Edge (ME) Server

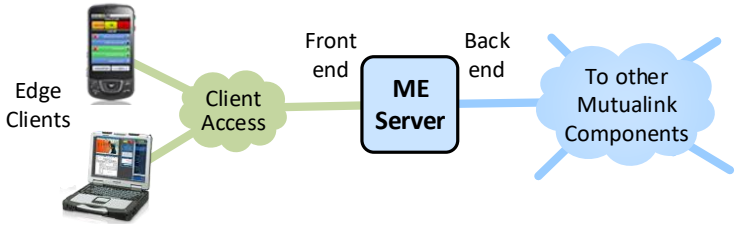
The Mutualink Edge (ME) server allows multiple Edge IWS clients to connect and participate in sharing groups. These servers are available for on-premise or tactical deployments as either software modules or hardware appliances in capacities ranging from 5 to 100 concurrent users. For additional resiliency for these deployments, redundant servers are available as on optional capability.

The ME server is also available as a cloud-hosted service for an unlimited number of concurrent users.

The ME has two logical IP networking interfaces:

- The back-end, which is the interface that it uses to connect to other Mutualink components
- The front-end, which is the interface for incoming Edge client connections. This interface is typically connected to the Enterprise LAN for on-premise deployments, or the Internet for public/cloud deployments, etc.

A single network interface could be used for both functions, but it's frequently desirable to keep the client ("public") traffic segregated from the interoperability ("private") traffic.



The ME has a web-based management portal that allows administrators to configure users, configure static groups, assign permissions to users, etc.

3.3 Mutualink Gateways

There are many different types of Mutualink gateways, but they all have a common purpose: To enable media/data from non-Mutualink systems/devices to be selectively shared with and interoperate with other agencies via the Mutualink system.

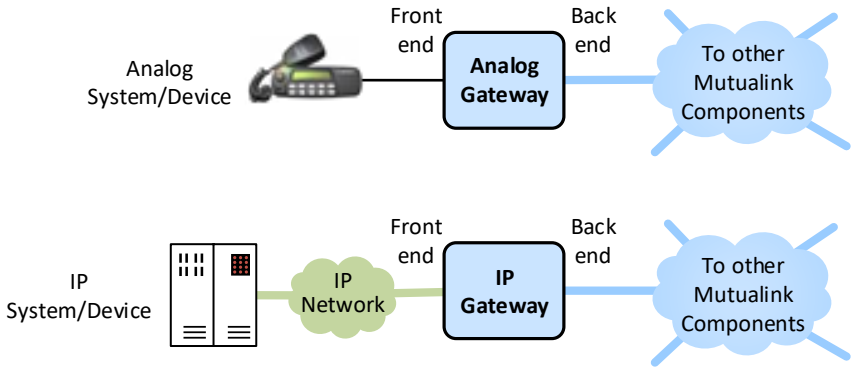
If an analog interface is required to integrate to an external system/device, then a physical gateway appliance is typically required. This is most common for analog radio, telephony, or video interfaces. If the interface to an external system/device can be accomplished using an IP network connection, then the "IP gateway" can be realized as a software module running on an approved platform.

Multiple gateway functions can reside on the same physical host. The maximum number of analog gateways in one host depends on how many analog interfaces can physically fit in the chassis, whereas the maximum number of IP gateways in one host depends primarily on the CPU and memory capacity of that host. When mixing both analog and IP gateways on one host, both limits come into play.

Like ME servers, gateways also have two logical interfaces:

- The back-end, which is the IP network interface that it uses to connect to other Mutualink components
- The front-end, which is the interface that connects to the external system or device. For analog gateways this will be an analog interface; for IP gateways this will be an IP network interface.

For IP gateways, a single network interface could be used for both the back-end and front-end functions, but it's frequently desirable to insulate external devices/systems from the interoperability traffic.



3.3.1 Land Mobile Radio (LMR) Gateways

Mutualink LMR/radio gateways may be either analog gateways or IP gateways depending on the capabilities of the radio system requiring integration.

Analog Radio Gateways

These gateways provide the following capabilities when connected to an analog radio interface:

- Analog Rx & Tx voice: Balanced/unbalanced, 2-wire/4-wire, various terminations
- Tone Remote Control (TRC): Channel select, monitor
- Control I/O: E&M, PTT/COR, Monitor, TxGrant, Channel select
- Serial and USB control: Channel select, PTT-ID, Monitor, Text Messaging

Supported analog interfaces include: Portable radios, mobile radios, base stations, console systems, intercoms, PA systems, any 2-wire/4-wire voice interface.

Analog radio gateways are available in 1-, 2-, and 4-channel capacities, and in standalone, rack-mount, and rugged tactical chassis.

Additionally, analog radio gateways can perform any function that an IP radio gateway can since the analog gateway is essentially an IP gateway with analog interfaces added.

IP Radio Gateways

These gateways provide the following capabilities over an IP radio interface:

- Radio-over-IP (RoIP): SIP or RTP; unicast or multicast; G.711, G.729, and linear-16 codecs
- P25: ISSI or CSSI
- DMR: AIS
- Bridging System Interface (BSI): SIP + RTP
- Various proprietary radio vendor interfaces
- Coming soon: Mission Critical Push-to-Talk (MC-PTT)

For larger-capacity IP radio gateways (i.e. P25, DMR, BSI, and MC-PTT) redundant gateways may be deployed for additional resiliency. It is recommended that these gateways be deployed in different locations for enhanced geo-redundancy.

3.3.2 Video Gateways

Mutualink video gateways may be either analog gateways or IP gateways depending on the video system/device requiring integration. Furthermore, video gateways may be configured to operate in one of two modes:

- **Input Mode**: Input video gateways receive video feeds from external sources and send those feeds to Mutualink sharing groups.
- **Output Mode**: Output video gateways receive video feeds from Mutualink sharing groups and send those feeds to external video systems/displays.

Video gateways can also include bidirectional voice/audio capability as part of the integration if desired.

Analog Video Gateways

More properly called non-IP gateways, these gateways provide the following capabilities:

- Input: Composite, VGA, DVI, HDMI
- Output: VGA, DVI, HDMI

Additionally, analog video gateways can perform any function that an IP video gateway can since the analog gateway is essentially an IP gateway with analog interfaces added.

IP Video Gateways

These gateways provide the following capabilities:

- Input: MP2T or RTP, RTSP client, MPEG2, MPEG4, H.263, H.264, H.265, unicast or multicast
- Output: MP2T or RTP, RTSP server, H.264, unicast or multicast

3.3.3 Telephony Gateways

Mutualink telephony gateways may be either analog gateways or IP gateways depending on the telephony system/device requiring integration. These gateways may be used to make outgoing calls and accept incoming calls to/from the PSTN or a PBX.

For incoming calls, an optional PIN may be assigned to the line so that only authorized users may call in on the line. When an incoming call comes in to a telephony gateway, that call may be routed to a specific user, set of users, or a group depending on the configuration of the gateway.

Analog Telephony Gateways

This gateway includes an FXO port to connect an analog POTS line from the PSTBN or a PBX.

IP Telephony Gateways

The IP telephony gateway is really a subset of the IP radio gateway; it provides the following capabilities:

- Signaling: SIP (or none for just RTP)
- Voice: RTP unicast or multicast
- Codecs: G.711, G.729, and linear-16

3.3.4 System Gateways

System gateways are IP-only gateways that provide an interface to a variety of multimedia communications systems. This includes Unified Communication (UC) systems as well as other group PTT voice systems. For interfacing to specific channels or talkgroups on voice-only systems, an IP radio

gateway will usually suffice. For systems that include other media such as video, or require enhanced integration beyond specific channels or talkgroups (e.g. unit-to-unit calls), a System Gateway is used.

The capability provided by a System Gateway depends greatly on the capabilities of the external system under integration.

3.3.5 Data Gateways

Data gateways are a class of gateways that provide integration to various non-media systems, i.e. systems without voice or video capability. Some of these gateways are listed below for illustrative purposes.

- **GIS Gateways**. These gateways connect to enterprise GIS and AVL systems (including CAD systems) to share location and geospatial data within a sharing group.
- **Text/Chat Gateways**. These gateways connect to external text/chat systems to extend the text messaging capability in a sharing group to an external chat room, etc.
- **Application Data Gateways**. These gateways allow applications to share arbitrary data to a sharing group. Other applications connected to that sharing group that understand that data format may then consume that data, allowing multiple application instances to communicate with each other without being interpreted by the Mutualink system.

3.3.6 Event/Alert Gateways

These gateways typically integrate to event sources such as alert/panic-button systems, notification systems, etc. and initiate various actions with other Mutualink components when events occur. The event gateway therefore is a generic “trigger mechanism” for automated actions in the Mutualink system.

When the external system sends an event notification to the event gateway, there is typically additional information associated with the event that is also sent. For example, the location of the event (e.g. lat/lon or building ID), the type of event (e.g. police, fire, medical), and the priority (e.g. emergency, urgent, routine).

The event gateway includes a sophisticated rules engine that can trigger a complex sequence of actions. These actions may be any action that an IWS user can perform, and can be customized according to the event info for that specific event. Examples of actions the event gateway can perform:

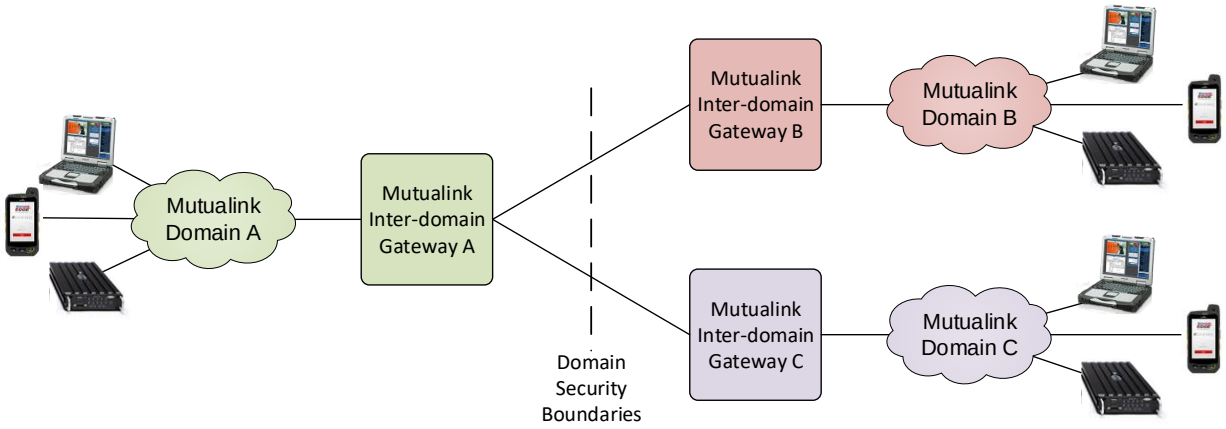
- Create a sharing group and invite all law enforcement users within a 1-mile radius
- When a panic button is pressed in a school, create a sharing group and invite the school security officers as well as the local PSAP. Automatically send them the video feed from the video camera closest to where the panic button was pressed.
- When a fire alarm activates, automatically send the alarm company the closest video feed and live audio.

3.4 Mutualink Inter-Domain Gateway (IDG)

The Inter-Domain Gateway (IDG) provides an administratively-controlled interface point for connecting multiple Mutualink systems/domains to each other, or for connecting a Mutualink system to non-Mutualink systems.

To establish communication with another system, the IDG administrator configures a "trust relationship" between the local IDG and a remote IDG. The trust relationship defines the functionality allowed between the local domain and the remote domain; these administrative controls include:

- Which local users and groups should be visible to the remote domain, and how local user identities should be mapped to the remote domain
- Which remote users and groups should be visible to which local users, and how remote user identities should be mapped to the local domain
- What media types are allowed between domains and what the bandwidth usage rules are
- What local information may be shared to the remote domain



IDGs may be deployed as single instances, or in redundant pairs (co-located or geo-dispersed) for additional resiliency.

3.5 Mutualink Application Programming Interface (API)

All the capabilities available to an Edge IWS user are also available for programmatic use via the Mutualink Edge API. This API provides the following capabilities:

- Create groups, invite other users to groups, accept or decline invitations from others
- Add authorized gateways to groups, choose channels/feeds/users/groups from external systems to share/connect to a group
- PTT voice transmit and receive
- Share video feeds to groups, extract video & screens from others
- Send & receive text messages, send & receive files
- Share locations to groups, read locations of group members

Development using this API is accomplished with a cross-platform SDK available through the Mutualink Partner Program.

4. Networking and Deployment

4.1 Connecting Mutualink Components

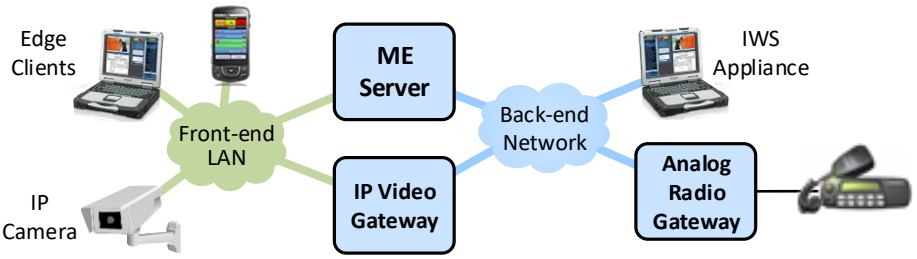
To allow multiple Mutualink components to work together as part of an overall system, the back-end network interfaces of the components must be networked together. Minimally, this means that they must be IPv4-routable to each other (i.e. can't pass through NATs). Additionally, to take full advantage of the distributed peer-to-peer capabilities, multicast should be enabled between the components.

For these reasons, the back-ends of components are typically inter-networking using LANs for local connectivity and VPNs for remote connectivity.

4.2 Single-site Networking

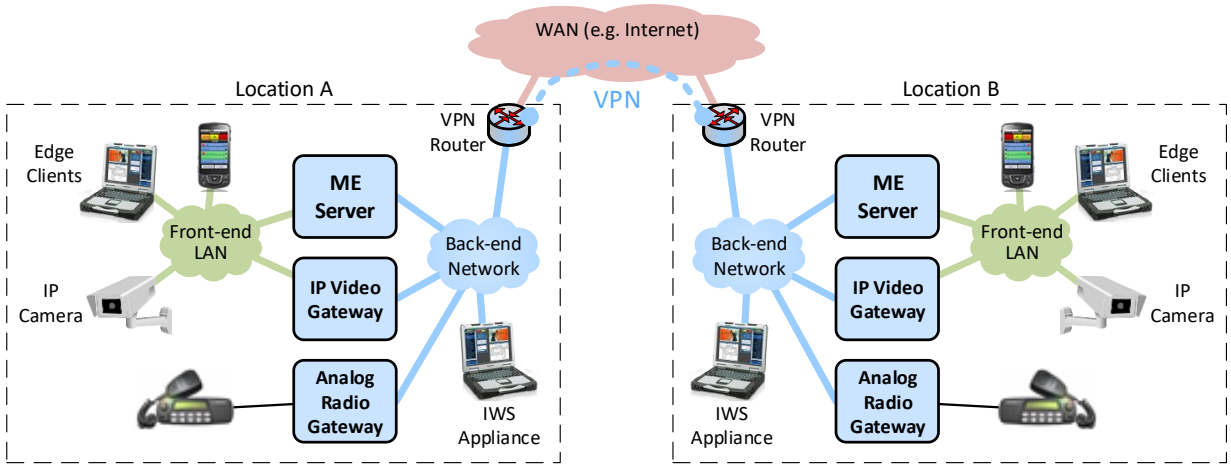
Here's a simple example of creating a system with a few components in a single location. Note that:

- The back-ends of all components are all connected so they can communicate with each other.
- The front-ends of the ME and IP video gateway are connected to a LAN so that the Edge clients can connect to the ME and the video gateway can access the IP camera.



4.3 Multi-site Networking

If two agencies wish to interoperate with each other ("bridge their silos"), it could look like the following. Note that the two back-end networks are networked using a VPN between the locations.

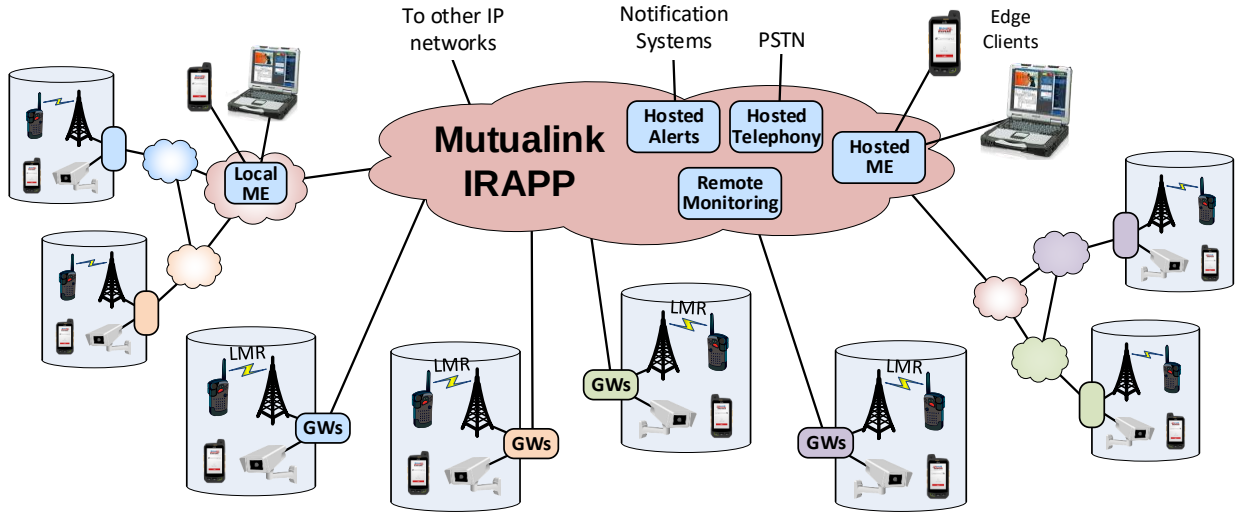


This connection is fine for two agencies, but what happens when each of those agencies wishes to interoperate with several other agencies? The point-to-point VPNs between many locations can quickly become unmanageable. This is where IRAPP comes in.

4.4 The Interoperable Response and Preparedness Platform (IRAPP)

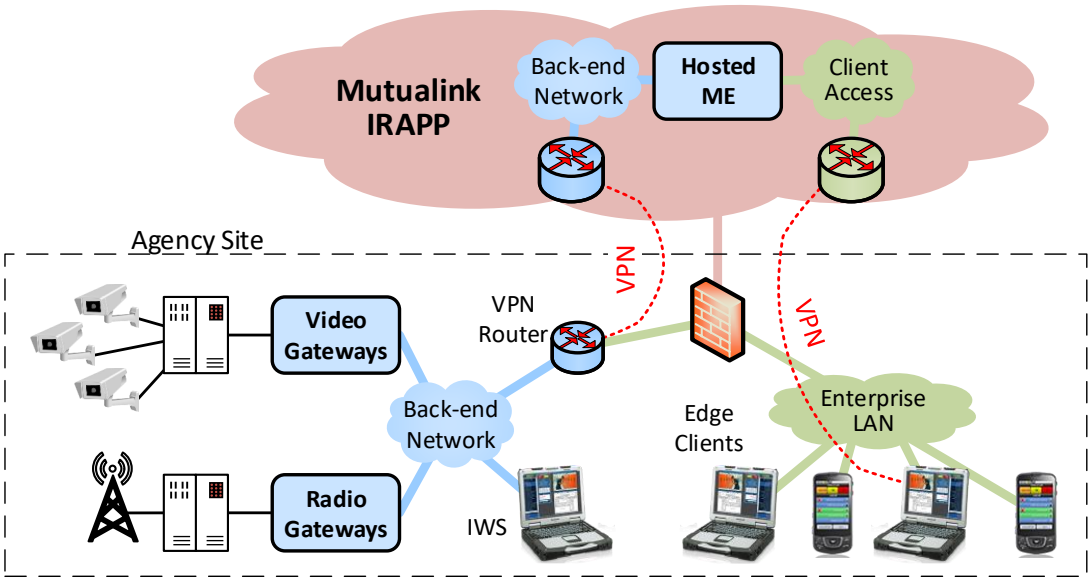
Mutualink operates a nationwide private secure network known as IRAPP. Access to this network is via secure VPN only (software or hardware) and is limited to authorized Mutualink customers. IRAPP provides the following value to our customers:

1) **Ubiquitous connectivity**. Secure networking connectivity between all IRAPP participants. Once an agency connects to IRAPP, they instantly have interoperability access to all other agencies on IRAPP. This solves the above problem of many point-to-point VPNs between agencies – connect once to IRAPP and you're connected to everyone.
2) **Hosted Edge Service**. If an agency does not wish to deploy their own ME server on-premise, Mutualink provides a hosted service that allows users to use their Edge IWS clients wherever there is Internet connectivity.
3) **Hosted Telephony Service**. Mutualink offers a PSTN telephony gateway service that allows agencies to dynamically connect outgoing and incoming PSTN calls to sharing groups.
4) **Hosted Alert Notification Service**. If an agency does not wish to deploy their own event/alert gateway on-premise, Mutualink offers a hosted service that provides the same functionality. This service receives events from an agency's alert/notification system and executes the sequence of actions defined by that agency's configured rules.
5) **Remote Monitoring and Support**. Mutualink Customer Support is able to monitor connected components for loss of connectivity or other issues and work with the agency to correct the problem before it leads to an outage. Additionally, they are able to perform patches and upgrades on an ongoing basis at the agency's discretion.



4.5 Hybrid Deployments

A common deployment scenario for an agency is to deploy some equipment on-premise (e.g. gateways to integrate to on-premise systems) and utilize the IRAPP Hosted ME service for other users.



Notes:

- The on-premise VPN router connects through the enterprise firewall to the hosted back-end network via secure hardware VPN.
- The Edge clients connect to the front-end client access network via secure software VPN.
- If an on-premise ME server is not deployed, a local IWS may be used to control the local gateways if connectivity to IRAPP is lost.

4.6 IRAPP-only Deployment

If agencies do not require gateway integrations to external systems or an on-premise ME at a particular location, then the deployment of Mutualink capability at that location can be as simple as installing the Edge IWS software on the desired client systems.