

# Introduction to P25

TRG-00001-01-M · Issue 1 · October 2015

## **Contact Information**

### **Tait Communications Corporate Head Office**

Tait Limited  
P.O. Box 1645  
Christchurch  
New Zealand

For the address and telephone number of regional offices, refer to our website: [www.taitradio.com](http://www.taitradio.com)

## **Copyright and Trademarks**

All information contained in this document is the property of Tait Limited. All rights reserved.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, stored, or reduced to any electronic medium or machine-readable form, without prior written permission from Tait Limited.

The word TAIT and the TAIT logo are trademarks of Tait Limited.

All trade names referenced are the service mark, trademark or registered trademark of the respective manufacturers.

## **Disclaimer**

There are no warranties extended or granted by this document. Tait Limited accepts no responsibility for damage arising from use of the information contained in the document or of the equipment and software it describes. It is the responsibility of the user to ensure that use of such information, equipment and software complies with the laws, rules and regulations of the applicable jurisdictions.

## **Enquiries and Comments**

If you have any enquiries regarding this document, or any comments, suggestions and notifications of errors, please contact your regional Tait office.

## **Updates of Manual and Equipment**

In the interests of improving the performance, reliability or servicing of the equipment, Tait Limited reserves the right to update the equipment or this document or both without prior notice.

# Contents

---

<b>1</b>	<b>The P25 Standard</b>	<b>7</b>
1.1	What is APCO Project 25?	7
1.1.1	APCO Project 25	7
1.2	Benefits of P25	8
1.2.1	Open Standard	8
1.2.2	Interoperability and Migration Path	9
1.2.3	Levels of Interoperability in Radio Systems	10
1.2.4	Frequency Use	12
1.2.5	Digital Audio Quality	13
1.2.6	P25 Services	15
1.2.7	List of P25 Services	16
1.3	P25 Phase 2 Overview	17
1.3.1	P25 Phase 2 Additional Details	18
1.3.2	P25 Phase 2 Uses TDMA	20
1.4	Introduction to P25 Trunking	25
1.4.1	What is Trunking?	25
1.4.2	The Development of Trunking	25
1.4.3	Trunking Efficiency	29
1.4.4	Trunking Technologies	30
1.4.5	Advantages of a Trunked Radio System	30
1.4.6	P25 Standards	31
1.4.7	P25 Trunked System Identification	32
<b>2</b>	<b>P25 Network Architecture</b>	<b>35</b>
2.1	Network Overview	35
2.1.1	Standards and Open Interfaces	36
2.1.2	Conventional System Types	36
2.1.3	Trunked System Types	40
2.1.4	Conclusion	41
2.2	Linking	42
2.2.1	Linking Infrastructure	42
2.2.2	Linking - Monitoring and Management	43
2.2.3	Dedicated or Shared Network	43
2.2.4	Voice over IP	45
2.2.5	Trunking	47
2.3	Site Equipment	48
2.3.1	Introduction	48
2.3.2	Antenna System	48
2.3.3	Power Supply Equipment	48
2.3.4	Repeaters (Base Stations)	49
2.3.5	Networking Equipment	50
2.3.6	Linking Equipment	50
2.3.7	Trunked Site Control Equipment	50
2.3.8	Conventional Control Equipment	50

2.4	Central Site Equipment	51
2.4.1	Conventional	51
2.4.2	Trunking	52
2.4.3	Management	53
2.5	Gateways	54
2.5.1	Dispatch	54
2.5.2	Phone	55
2.5.3	Data	55
2.5.4	Analog Gateway	56
2.5.5	Alarms	57
2.5.6	Inter Sub System Interface	57
2.6	Network Management	58
2.6.1	Tactical Management	58
2.6.2	Technical Management	59
2.6.3	Network Monitoring	59
<b>3</b>	<b>Channel Operation and Configuration</b>	<b>61</b>
3.1	Physical and Logical Channels	61
3.1.1	Physical Radio Channel	61
3.1.2	What happens if there are not enough channels?	62
3.1.3	TDMA and Logical Channels	63
3.1.4	Summary:	63
3.2	P25 Channel Operation	64
3.2.1	FM Operation	64
3.2.2	P25 Phase 1 Operation	66
3.2.3	Trunked System	72
3.2.4	Traffic Channel Access Methods	74
3.3	Channel Configuration	78
3.3.1	Unit Numbering	78
3.3.2	Group Addressing Scheme	79
3.3.3	Trunked P25 System Numbering	79
3.3.4	Network Access Code (NAC)	80
3.3.5	Channel Addressing	81
<b>4</b>	<b>Call Types and Features</b>	<b>85</b>
4.1	Voice Calls	85
4.1.1	Talkgroup Call	85
4.1.2	Announcement Group Call	86
4.1.3	System Call	86
4.1.4	Unit to Unit Call	86
4.1.5	Emergency Call	86
4.1.6	Telephone-to-Radio Call	87
4.1.7	Radio-to-Telephone Call	87
4.2	Data Calls	88
4.2.1	Status Messages	88
4.2.2	Packet Data	88
4.2.3	Radio Check	89
4.2.4	Call Alert	89

4.2.5	Radio Inhibit / Uninhibit .....	89
4.3	Introduction to P25 Encryption .....	91
4.3.1	What is Encryption? .....	91
4.3.2	Levels of Encryption .....	91
4.3.3	A Secure Radio System .....	93
4.3.4	Keyfilling Methods .....	95
4.3.5	Encryption Keys .....	96
4.3.6	Key Types .....	97
4.3.7	Referencing the Key .....	98
4.3.8	Encryption Process .....	100
4.3.9	Subscriber Units and Encryption.....	103



# 1 The P25 Standard

---

## 1.1 What is APCO Project 25?

### 1.1.1 APCO Project 25

In 1989, the Association of Public Safety Communications Officials International (APCO), together with other US governmental organizations, set up the steering committee “Project 25” and gave it the task of selecting appropriate standards for digital public safety mobile radio communications.

This steering committee had the following objectives for its work:

- Provide enhanced functionality with equipment and capabilities focused on public safety needs
- Improve radio spectrum efficiency
- Ensure competition in system life cycle procurement
- Allow effective, efficient and reliable intra-agency and interagency communications

#### APCO Project 25 Standards

The result of the steering committee’s work is a set of standards known as APCO Project 25 (alternatively APCO 25 or P25).

The detailed work of producing standards documents was delegated to the Telecommunications Industry Association (TIA). The result to date is a set of over 30 documents, beginning with a System and Standards Definition (TIA TSB102-A) that was released in November 1995.

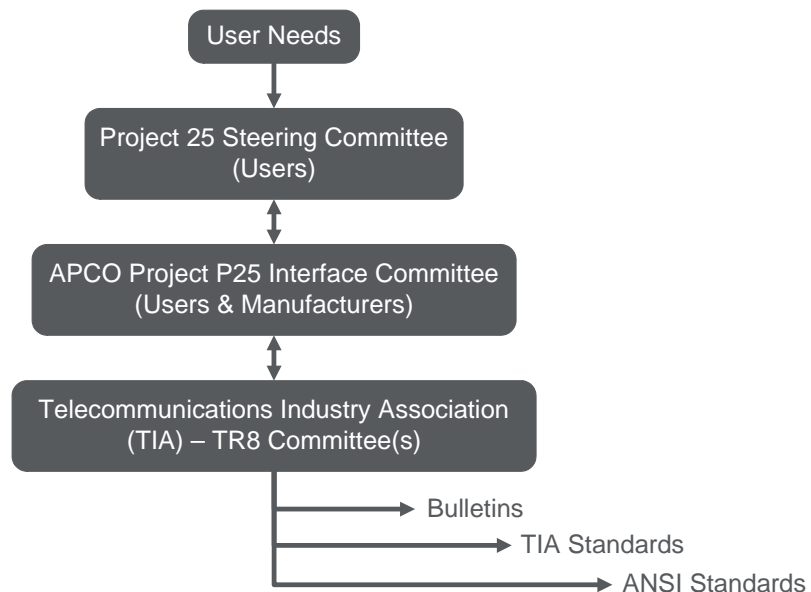


Figure 1.1 Committee structure

## 1.2 Benefits of P25

### Benefits of Project 25

P25 has a user focus and a clear statement of goals. The result is that P25 compliant equipment demonstrates it is able to meet a set of minimum requirements to fit the needs of public safety organizations.

The benefits P25 brings to the key areas listed below are described in the following sections:

- Open Standard (non-proprietary)
- Interoperability
- Migration Path
- Frequency Use
- Audio Quality
- Encryption
- Digital Services



### 1.2.1 Open Standard

P25 is an “open” standard and is not proprietary to a single manufacturer. This means that competition is possible between manufacturers not only when a new system is purchased, but over the life time of the system (e.g. each time new SUs are purchased).

The P25 standards define conventional, trunked and simulcast systems.

### Mandatory Requirements

There is clear definition on P25 functionality, and in order for a manufacturer to claim P25 compatibility, they must meet certain minimum functional criteria. At a minimum, to ensure interoperability between different manufacturers’ equipment, a P25 radio must meet two mandatory P25 standard interface components:

- The Common Air Interface (CAI)
- The Improved Multi-Band Excitation (IMBE) vocoder




**Standard Options** There is also a range of defined “Standard Options”, which a manufacturer may choose to add to their product. However, if included, the option must operate as defined by the P25 standards. This ensures interoperability between different manufacturers who choose to include these features.

For example, the various data services and encryption are standard features; equipment is not required to support them, but if it does, the implementation must follow the standard.

**Manufacturers’ Options** Beyond what is mandated and the range of standard options, there is a third category of features, which may be unique or proprietary to a manufacturer. These are known as manufacturers’ options.

This means that although many manufacturers make P25-compliant equipment, not all P25 systems are created equal. Individual manufacturers are free to incorporate additional features and functionality into their products.

 Many of the technologies used in Project 25 are proprietary, but the steering committee decided that it would only include a technology if the owners of intellectual property rights agreed to license it to other participating manufacturers at no cost (for mandatory features) or under “fair, reasonable and non-discriminatory terms.”

## 1.2.2 Interoperability and Migration Path

Interoperability is one of the major objectives of Project 25. Interoperability is “the ability of public safety personnel to communicate by radio with users from other agencies or departments.”

Interoperability with analog radio equipment also provides a migration path to digital.

### 1.2.3 Levels of Interoperability in Radio Systems

Radio systems offer different levels of interoperability. Task forces need a high level, while a lower level suffices for routine public safety operations. SAFECOM, a US federal organization concerned with interoperability issues for radio communications systems, has defined the “Interoperability Continuum”, which identifies five elements to be addressed when designing a system for interoperability. Those elements are described in the SAFECOM table below.

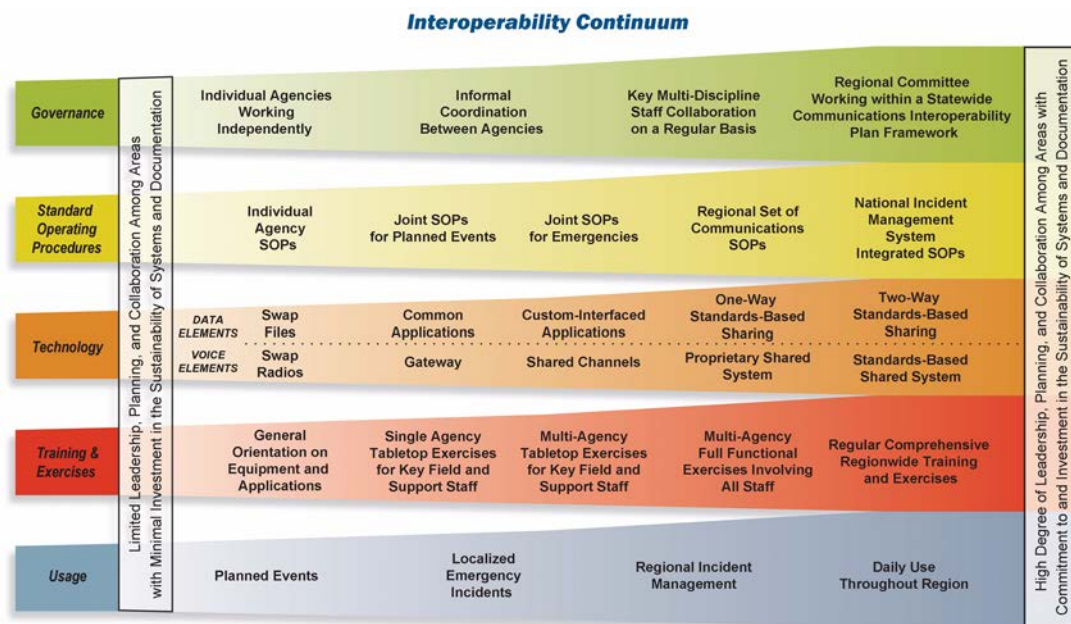


Figure 1.2 SAFECOM interoperability

#### Examples of Interoperability

Public safety agencies need to inter-operate in the following ways:

#### Gradual Migration to Digital

It is not always possible (financially or logistically) to upgrade an entire radio fleet at one time. It is often necessary for the new radios being installed to operate with the radios that are being replaced for a period of time. Only when all the radios have been installed and / or issued can the transition to P25 be completed.

#### Day-to-Day Interoperability

Involves coordination during routine public safety operations, for example:

- Firefighters from various departments join forces to battle a fire
- Neighboring law enforcement agencies must work together during a vehicular pursuit

## Mutual-Aid Interoperability

Involves a joint and immediate response to a catastrophic accident or natural disaster and requires tactical communications among numerous groups of public safety personnel. For example:

- Airplane crashes
- Bombings
- Forest fires
- Earthquakes

## Task Force Interoperability

Involves local, state, and federal agencies coming together for an extended period of time to address an ongoing public safety concern. Task forces lead the extended recovery operations for major disasters, provide security for major events, and conduct operations in prolonged criminal investigations.



**Figure 1.3 Interoperability**

### P25 Migration to Digital

A basic requirement for Phase 1 P25 digital radio equipment is backwards compatibility with standard analog FM radios. This supports an orderly migration into mixed analog and digital systems, enabling users to gradually trade out radios and infrastructure equipment.



Agencies can invest in the latest P25 technology and operate it initially in analog mode with the assurance that there is a clear migration path to the future.

### P25 Common Air Interface (CAI)

Some of the earliest TIA decisions related to the Common Air Interface (CAI) standard.

This interface standard specifies the type and content of signals transmitted by P25 compliant radios. A P25 radio using the CAI should be able to communicate with any other P25 radio using the CAI, regardless of manufacturer. Specifically it prescribes:

- Channel bandwidth

- Channel bit rate
- Modulation
- Frame formats including error detection, correction and encryption
- Voice frame information

The CAI also defines the “to” and “from” addresses, encryption, trunking and conventional control messages.

#### System-Level Interoperability

To meet the goal of Level 6 interoperability, the P25 standards are being expanded to include a standard for interconnecting different radio systems. The Inter RF Sub-System Interface (ISSI) can tie together radio systems from different manufacturers.

### 1.2.4 Frequency Use

P25 can be used on a wide range of VHF, UHF and 700/800 MHz frequencies, allowing existing analog channels to be upgraded to P25 digital channels. A new block of spectrum does not need to be purchased.

P25 channels are designed to be more spectrally efficient than traditional analog wideband channels. In a crowded RF environment, converting to P25 will allow more radio channels to operate in the same amount of RF spectrum. Enhancements to spectrum efficiency are being deployed in two phases.

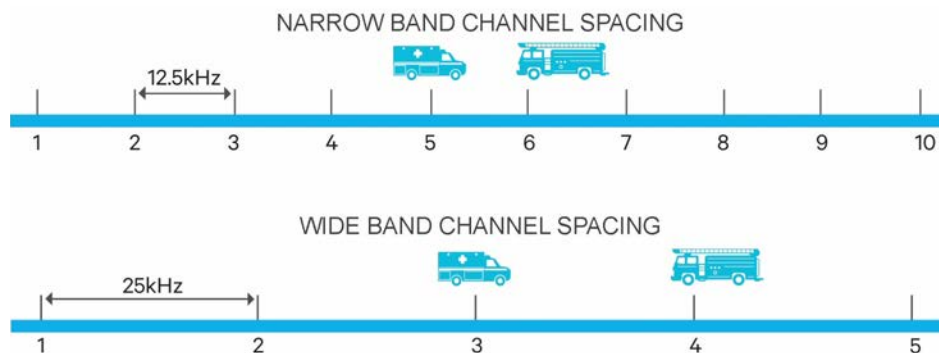


Figure 1.4 Channel spacing

#### P25 Phase 1

12.5 kHz channel spacing: This is twice as efficient as traditional analog wideband channels, which generally use 25 kHz.

C4FM (compatible 4-level FM) modulation: This enables 9600 bits per second to be transmitted on the 12.5 kHz channel.

IMBE (improved multi-band excitation) vocoding: This enables speech to be represented digitally using a bandwidth of only 4.4 kbps.

Phase 1 P25-compliant systems are backwards compatible and interoperable with legacy systems.

## P25 Phase 2

Phase 2 is a TDMA standard that will achieve one voice channel per 6.25 kHz bandwidth efficiency.

Phase 2 P25-compliant systems are backwards compatible and interoperable with P25 Phase 1 systems.

Phase 2 is an option for traffic channels on trunked P25 systems.

### 1.2.5 Digital Audio Quality

For the end user, one of the key benefits of a change from analog to P25 digital radio technology is the improvement in audio quality.

#### Analog Signal

An analog signal will gradually weaken and become harder to use as the distance from the site is increased. The user will experience increased amounts of “hiss and crackle” until finally the received audio is completely lost in noise.

#### Digital Signal

Digital P25 systems use a device called the IMBE™ vocoder to convert voice information into digital data. During the digitization process, the background noise, typically present in analog systems, is reduced. The data is then protected using error correction codes before being transmitted over the air. The receiver uses the error correction codes to correct for small errors (noise and “lost” portions of the transmission) in the received signal. The result is that full audio quality is maintained by the built-in error correction right to the edge of the coverage area. Fringe areas that were difficult to operate in under the analog system will become loud and clear under a P25 system.

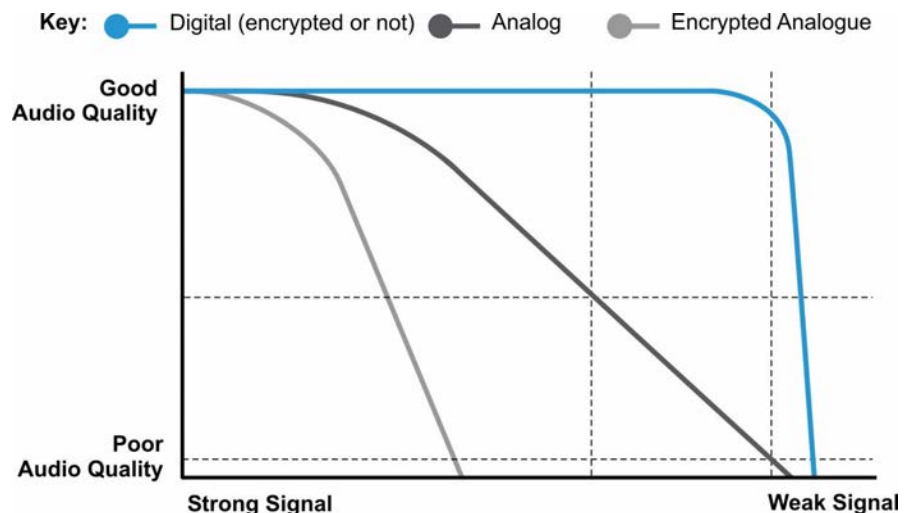


Figure 1.5 P25 coverage vs analog coverage

**Analog Encryption** There are various methods of encrypting an analog signal. However, in general for analog encryption, the more secure the encryption - the more rapidly the coverage will deteriorate.

**P25 Encryption** P25 transmissions may be protected by digital encryption. Because the vocoder produces a digital bit stream, it is relatively easy to encrypt. One major benefit of this type of encryption is that it does not affect speech intelligibility nor does it affect the system's usable range. Both of these advantages are major improvements over encryption that was used in analog systems.

The P25 standards specify the use of the Data Encryption Standard (DES) algorithm which has a 56 bit key and the Advanced Encryption Standard (AES) algorithm which has a 256 bit key.

To start the process, both the transmitting and the receiving devices must have an encryption key inserted. This is done using a key loader. Essentially, the key is the specific pattern that the encryption and decryption will follow. Most P25 SU equipment is optionally available with multiple keys. That is, a SU could use one key for one group of users and a separate key for another group of users.

P25 also includes a standardized Over The Air Rekeying (OTAR) function. OTAR is a way to greatly increase the utility of encryption systems by allowing transfer of encryption keys via radio. This remote rekey ability means that SUs no longer have to be physically touched in order to install a new or replacement key. OTAR can be done from a Key Management Facility, or KMF.



**Figure 1.6** Key loading

## 1.2.6 P25 Services

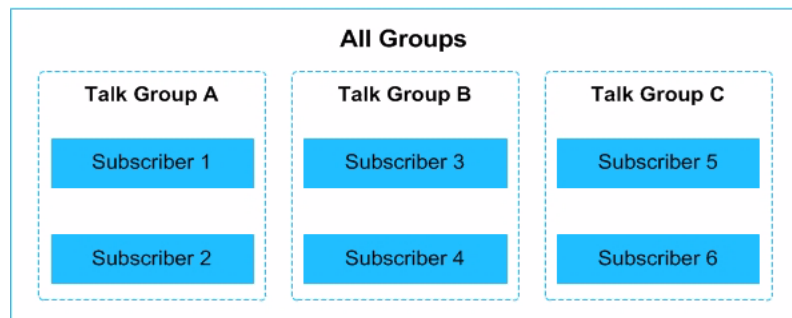
Because P25 transmissions are digital, it is easy to add extra information such as the destination ID (individual or talkgroup) and the caller ID. The P25 CAI defines signaling information that is sent over the air along with voice. This information allows a wide range of services to be offered.

### Identifying Users and Groups

Every SU on a P25 system has a Unit ID. Individual SU are typically numbered in the range 1 to 9,999,999. The Unit IDs should be programmed into the SUs using a national, corporate or agency wide unit identification scheme.

In addition to individual Unit IDs, P25 systems also use Talkgroups. A talk group is a group of radios that are required to operate together.

In a trunked system when a subscriber makes a call on a talk group the system automatically allocates a channel for the call. Therefore rather than selecting a channel to talk on the subscriber simply selects the group they wish to communicate with.



**Figure 1.7 Simple talkgroup operation**

In a conventional P25 system subscribers selected radio channel to talk on. In addition P25 talk groups can be used to share that one channel with multiple groups. However only one group can use the channel at a time.

- All SUs are operating on the same channel.
- SUs 1 and 2 communicate privately together by transmitting the Talkgroup A address.
- SUs 3 and 4 communicate privately together by transmitting the Talkgroup B address.
- SUs 5 and 6 communicate privately together by transmitting the Talkgroup C address.
- A message to all radios on the channel can be sent to a special All Groups address.

## 1.2.7 List of P25 Services

The CAI defines a number of “P25 Services”. These services are features that were previously provided by trunking or advanced Selcall. However, because individual radios can be identified on a P25 system and because the CAI specifies a method of transmitting additional information along with the voice, these services are available in P25 conventional mode. There are several other services specific to trunked P25 systems. These are outside the scope of this document.

<b>Unaddressed Voice Call</b>	A call to all users with in the coverage area of a conventional network.
<b>Group calls</b>	A call to a selected group of users on the network.
<b>Individual calls</b>	A call to an individual user on the network.
<b>Emergency Call</b>	A SU can make an emergency call. This has a higher priority than a normal call and the receiving SUs can identify that the call is an emergency call and indicate this to the user.
<b>Talking party identification</b>	The SU displays the ID number or name of the caller.
<b>Radio Check</b>	This is used by a dispatcher to check that a SU is available on the network. No action required by the user of the SU.
<b>Radio Unit Monitoring</b>	Radio unit monitoring is a feature by which a dispatcher may remotely cause a selected subscriber to transmit without the subscriber operator's intervention, and without causing an audible or visual indication at the SU that it is transmitting.
<b>Radio Inhibit / Uninhibit</b>	Tait has previously referred to this as “Stun” and “Revive”. Conventional P25 radios can initiate the “Inhibit” and “Uninhibit” commands. For security, Tait SUs are able to be programmed so that only a restricted number of IDs can initiate the “Inhibit / Uninhibit” function. An “Inhibited” SU will appear as if it is turned off. Power cycling the SU has no effect. A “Inhibited” SU has the following attributes: <ul style="list-style-type: none"> <li>■ There is No feedback on the User Interface (UI)</li> <li>■ It is NOT able to receive or make calls</li> <li>■ It will respond to a “Radio Check”, “Uninhibit” and “GPS request” commands</li> </ul>
<b>Call Alert</b>	The calling SU leaves its identity on the called SU, so that it can be called back.
<b>Messages</b>	Allows a short 12 character message to be left on another SU. The sending SU will automatically resend the message until it is acknowledged (limited number of retries).
<b>Status Query</b>	Allows a SU to request the status of another SU. There are 16 status labels. Each label can be up to 12 characters in length.
<b>Status Update</b>	A SU is able to send a status label to another SU. There are 16 status labels of up to 12 characters in length.



## 1.3 P25 Phase 2 Overview

P25 channels are designed to be more spectrally efficient than traditional analog wideband channels. In a crowded RF environment, converting to P25 will allow more radio channels to operate in the same amount of RF spectrum. Enhancements to spectrum efficiency are being deployed in two phases.

### P25 Phase 1

- 12.5 kHz channel spacing:
- This is twice as efficient as traditional analog wideband channels, which generally use 25 kHz.

### P25 Phase 2

- 12.5 kHz channels with TDMA (Time Division Multiple Access) to achieve two logical channels per physical channel.
- Thus, 6.25 kHz equivalence is achieved this is twice as efficient as P25 Phase 1.

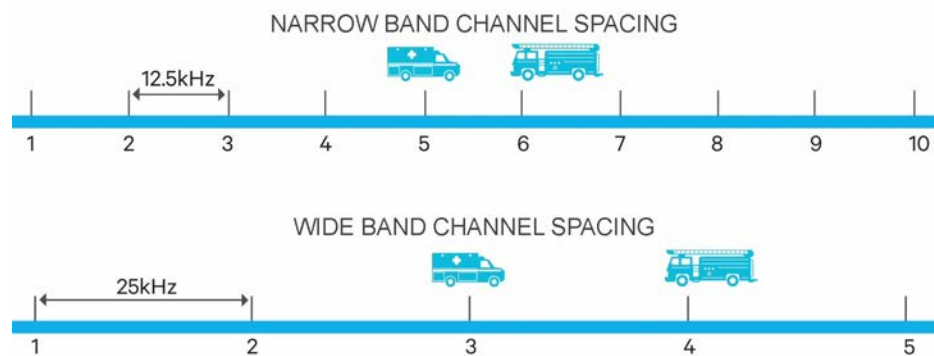


Figure 1.8 Channel spacing

### Key Points

- Phase 2 is more spectrally efficient than Phase 1, providing two effective channels per 12.5 kHz channel (6.25 each).
- Each base station channel can provide two effective voice traffic channels.
- Longer battery shift life in portables (only Transmit half the time).
- Phase 2 is available for trunking only.
- Additional software feature licenses are required in the infrastructure and SUs.
- Phase 2 was designed for Phase 1 backwards compatibility, so agencies with Phase 1 radios could use a Phase 2 - capable system.

### 1.3.1 P25 Phase 2 Additional Details

The P25 standards documents for Phase 2 TDMA were published between 2009 and 2012. The core definition documents include the TDMA Overview (TSB-102.BBAA), the TDMA Physical Layer (TIA-102.BBAB), and the TDMA CAI MAC Layer (TIA-102.BBAC and BBAC-1), among others. The test documents include the TDMA CAI Conformance Tests (TIA-102.BCAD), TDMA Messages and Procedures Conformance Tests (TIA-102.BCAE), Recommended Compliance Assessment Tests for Phase 2 (TSB-102.CBBL), among others.

P25 Phase 2 is defined for trunking operation only. At this point, it appears unlikely that there will be a version of P25 Phase 2 for conventional operation.

P25 Phase 2 uses 12.5 kHz channels with TDMA (Time Division Multiple Access) to achieve two logical channels per physical channel. Thus, 6.25 kHz equivalence is achieved.

Phase 2 was designed for Phase 1 backwards compatibility, so agencies with Phase 1 radios could use a Phase 2 capable system. More detail is given later in this manual.

#### Backwards Compatibility

- Phase 2 capable radios are required to have Phase 1 functionality.
- The control channel on a Phase 2 system always operates in Phase 1 mode.
- Traffic channels can be dynamically allocated as Phase 1 or Phase 2 depending on the radios involved in the call.
- Migration to Phase 2 can be done in stages.
- Data is done in Phase 1 mode (OTAR, AVL, etc.)
- Simplex mode (SU-to-SU) is Phase 1.
- Failsoft is Phase 1.

#### Phase 1 vs. Phase 2

Phase 1 can be used in trunked or conventional configurations.	Phase 2 is currently available in trunking only.
Phase 2 requires additional coverage design considerations, especially for simulcast systems.	The sites may have to be spaced closer than for Phase 1 sites.
Phase 1 equipment has been undergoing compliance testing sanctioned by the Federal Government Compliance Assessment Program (CAP), sanctioned by the Department of Homeland Security.	No such program exists yet for Phase 2.
Phase 2 is capable of interactive power output control and can interrupt on-going transmission from subscriber units.	No such functions in Phase 1.

<http://www.p25bestpractice.com/>

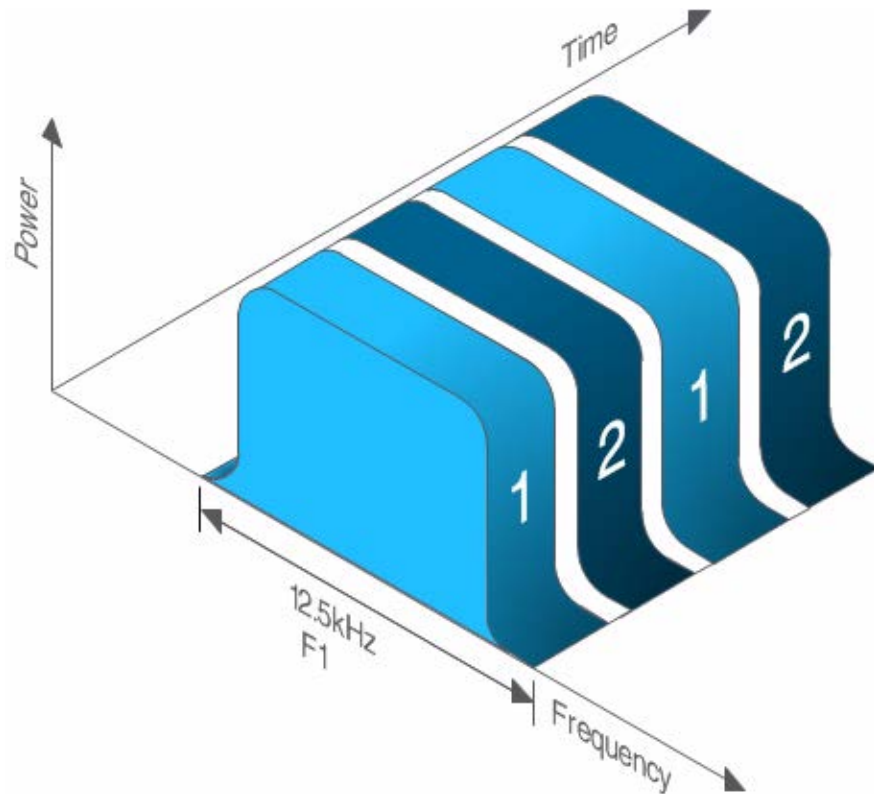
## Phase 2 Myths and Misconceptions

Phase 2 is necessary for FCC Narrowbanding	False	In the U.S., in the 700 MHz band, 6.25e is required from 1/1/2017. Besides that, it is not required.
There are no drawbacks to using Phase 2	False	Significant drawbacks are: coverage design considerations, lack of compliance testing, limited vendor competition
Everyone should upgrade to or install Phase 2	Absolutely false!	Significant expense and effort is required to upgrade from Phase 1 to Phase 2.
Phase 1 is an obsolete standard and being replaced by Phase 2	False	Phase 2 augments Phase 1, to address the infrequent situations where increased traffic capacity is needed, but does not replace Phase 1.
Phase 2 has to use 700/800 MHz spectrum	False	Phase 2 can be offered in any frequency band

<http://www.p25bestpractice.com/specifying/phase-1-or-phase-2/>

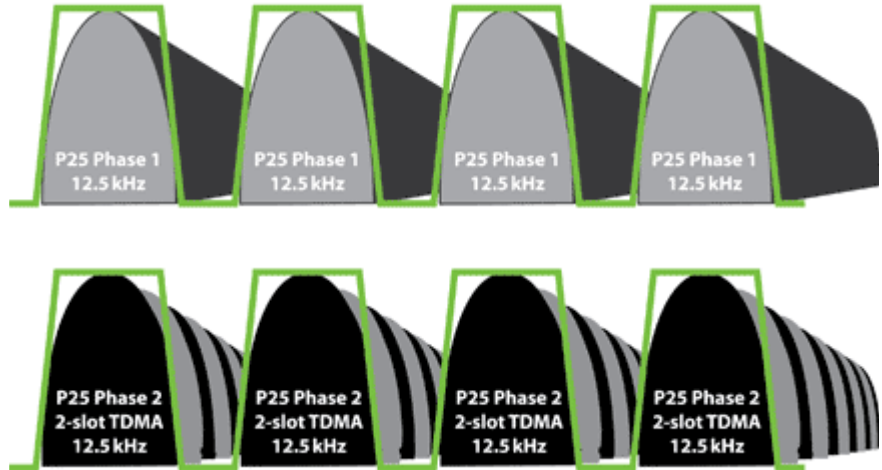
### 1.3.2 P25 Phase 2 Uses TDMA

Phase 2 uses TDMA (Time Division Multiple Access) to provide two logical channels on the same physical 12.5 kHz RF channel. The channel is divided into timeslots assigned alternately to each logical channel. Each timeslot has a duration of 30 ms.



#### P25 Phase 2 Infrastructure Considerations

- Standards currently defined for trunking only.
- Control channel is still Phase 1.
- Traffic channels can dynamically be Phase 2 or Phase 1, depending on the radios in that Talkgroup.
- Two-slot TDMA in 12.5kHz channel resulting in 6.25kHz equivalency.



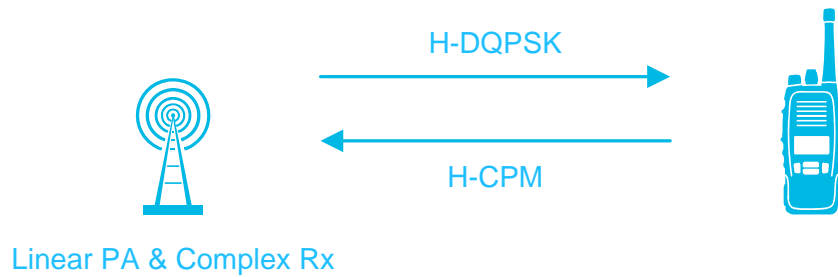
Source: National Institute of Justice web page, “Understanding FCC Narrowbanding Requirements”

**P25 Phase 2 Modulation**

Downlink: H-DQPSK (Harmonized Differential Quadrature Phase Shift Keying) used in the base station fixed-site equipment and requires linear transmit amplifiers.

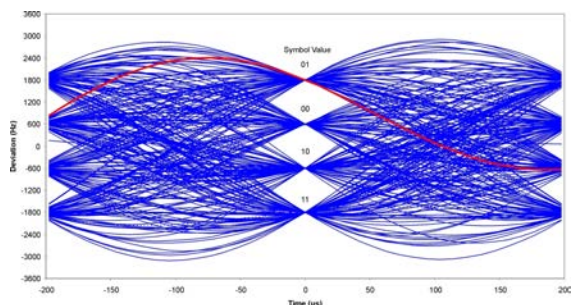
Uplink: H-CPM (Harmonized Continuous Phase Modulation) used in SUs “to enable use of the same non-linear amplifiers currently employed in P25 Phase 1 FDMA units.”

This requires a more complex receiver in the base station, where the complexity is concentrated, rather than the SUs.



## Phase 1 Uplink/Downlink: C4FM

P25 Phase 1 operates with a modulation scheme known as C4FM (Continuous 4-level Frequency Modulation). Each symbol transmits one dibit<sup>1</sup>, and one dibit is sent every 208 microseconds, for an effective data rate of 9600 bps. The PA transmits with constant power, and thus the constellation is circular.

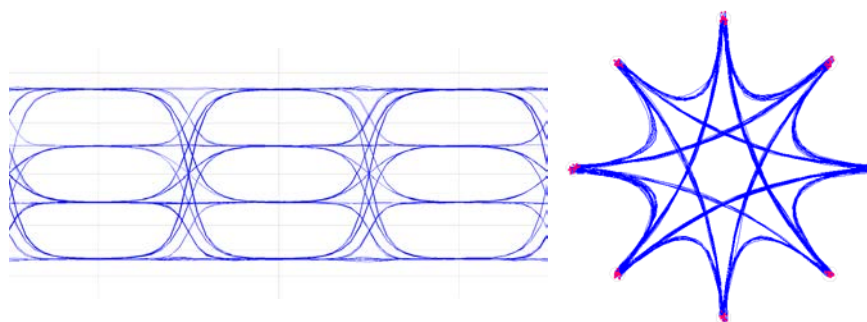


## Phase 2 Downlink: H-DQPSK

Phase 2 uses different modulation schemes. Outbound signals from the base station use H-DQPSK (Harmonized Differential Quadrature Phase Shift Keying), which requires linear transmitters. Inbound signals from the radios use H-CPM (Harmonized Continuous Phase Modulation) which requires a more complex receiver to detect and correct for errors. Thus, the complexity is concentrated within the base station.

The base station transmitter is continuously adjusting the output magnitude and phase, and thus the constellation is not circular as it is with Phase 1. Also, this mandates use of a linear PA.

Data is sent at the rate of one symbol every 166.67 microseconds, which corresponds to a data rate of 12,000 bps.

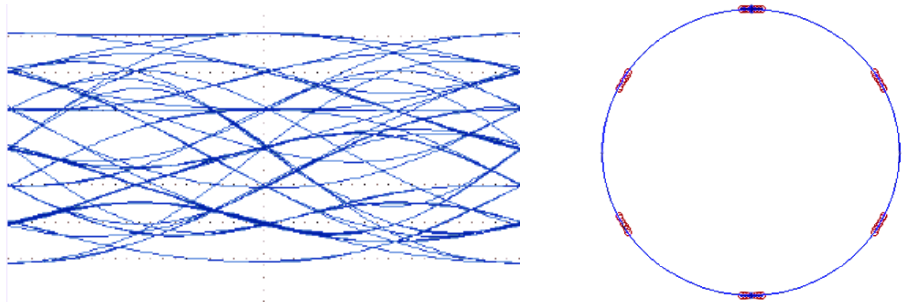


## Phase 2 Uplink: H-CPM

Inbound signals from the radios use H-CPM (Harmonized Continuous Phase Modulation) which requires a more complex receiver to detect and

- 
1. Dibit: Any one of four patterns from two consecutive bits: 00, 01, 10 and 11. Using phase modulation, a dibit can be modulated onto a carrier as a different shift in the phase of the wave.

correct for errors. H-CPM is constant-envelope, which means that the transmitter doesn't change power during the transmission (thus, the constellation appears as a circle). Like with C4FM, the transmitter moves the carrier smoothly between symbols, and thus the eyes are not open as much as with H-DQPSK. Although like C4FM, H-CPM sends a dibit per symbol, H-CPM has an equivalent of 7 states, not 4 as in C4FM. The reason for this is that the H-CPM transmitter always shifts the phase depending on the symbols that were sent previously.



**Phase 2 Coverage Considerations**

Usually, coverage is defined in terms of Delivered Audio Quality (DAQ), and a DAQ of 3.4 is commonly used for Public Safety systems. In P25 Phase 1, a DAQ of 3.4 corresponds to 2% BER.

In P25 Phase 2, a DAQ of 3.4 corresponds to:

- 2.4% BER on the downlink
- 2.6% BER on the uplink

On the uplink, H-CPM is more complex than C4FM, which means that it is “harder” to receive than C4FM. However, there is a lot of computational power in the base station, and through a lot of processing, the uplink coverage works out to be about the same as C4FM.

Therefore, the uplink coverage will be about the same, comparing a P25 Phase 1 system to a Phase 2 system.

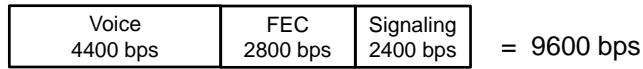
**Common Air Interface (CAI)**

P25 Phase 1 uses a full-rate vocoder, which operates at 7200 bps (4400 bps for voice and 2800 bps for Forward Error Correction). Add 2400 bps for signaling, and that works out to an overall data rate of 9600 bps.

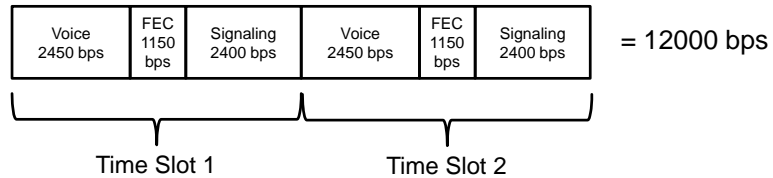
P25 Phase 2 uses a half-rate vocoder, which operates at 3600 bps (2450 bps for voice and 1150 bps for Forward Error Correction). Add 2400 bps for

signaling, and that works out to 6000 bps per timeslot. There are two timeslots in one 12.5 kHz channel, so the total bandwidth is 12,000 bps.

P25 Phase 1: Full-rate vocoder (7200 bps)



P25 Phase 2: Half-rate vocoder (3600 bps)



**SACCH (Slow Associated Control Channel)**

With the SACCH, for a brief period once every 1.44 seconds, the user's radio ceases to transmit and tunes its receiver to the transmit frequency to listen for signaling from the base station. If there is an emergency call or the dispatcher wants to pre-empt the call, the signaling tells the radio whether it should be transmitting. The user can then stop transmitting and release the channel at that site. (In Phase 1, the call can continue after the emergency call ends, with the talker still unaware of the emergency call.)



## 1.4 Introduction to P25 Trunking

### 1.4.1 What is Trunking?

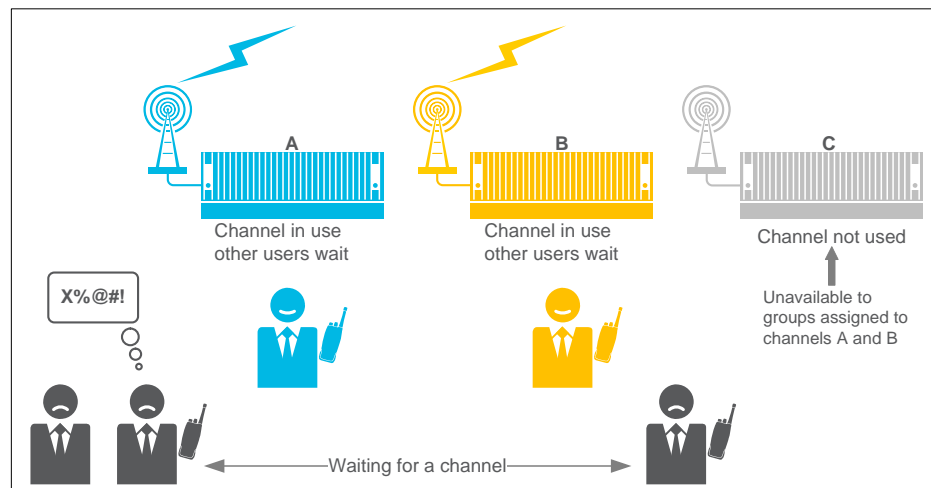
Trunking describes the process of selecting one clear communications path from many possibilities. Trunking is based on the premise that if 100 users are sharing a certain communications network, only around 10 users will actually use the network at any one time.

In radio communications, trunking is the dynamic and automatic allocation of repeater channels to radio users. Trunking has the added benefit of providing the ability to free up resources for a radio user in the event of an emergency.

### 1.4.2 The Development of Trunking

The diminishing availability of radio spectrum began to cause concern in the early 1980's, and it became obvious that more efficient management of the frequency spectrum was necessary.

Historically, organizations with a significant number of mobile staff had to rely on multi-channel communications networks or smaller systems restricted to a single frequency. The result was that some channels were overcrowded while other channels were unused. These problems were compounded for customers requiring communications coverage over extended areas.



An analogy could be made to walking into a bank to make a withdrawal and finding you had to wait in a long queue in front of the one teller who processes withdrawals, while another teller who processes only deposits had no one waiting. A much better system would be to allow the bank tellers to process any type of transaction, then you could simply go to the next one that is available.

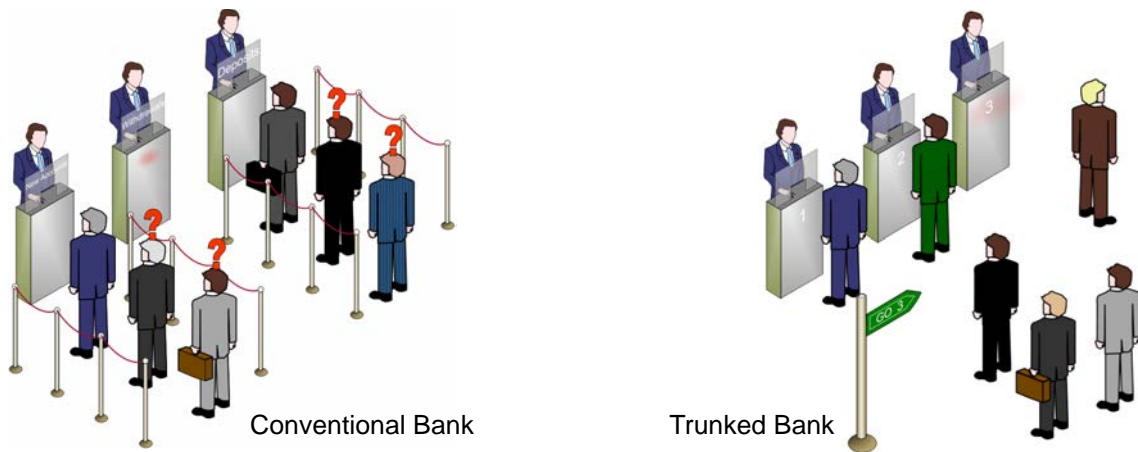


Figure 1.9 Without trunking - queues become longer

### Trunked Phone Lines

The name “trunk” comes from the telephone industry. Trunk lines are the telephone lines that run between telephone exchanges and are different from the line that runs to your house. If you call from your telephone exchange to another telephone exchange, the switching equipment at your exchange assigns your call a trunk line that runs to the other exchange. In effect, you “borrow” a trunk line for as long as you are connected.

When you hang up, your exchange recovers the trunk line you were using and makes it available for assignment to another caller. Therefore, it is not necessary to install 100 trunk lines to serve 100 telephone customers; only 10 lines will be sufficient to provide a high level of service.

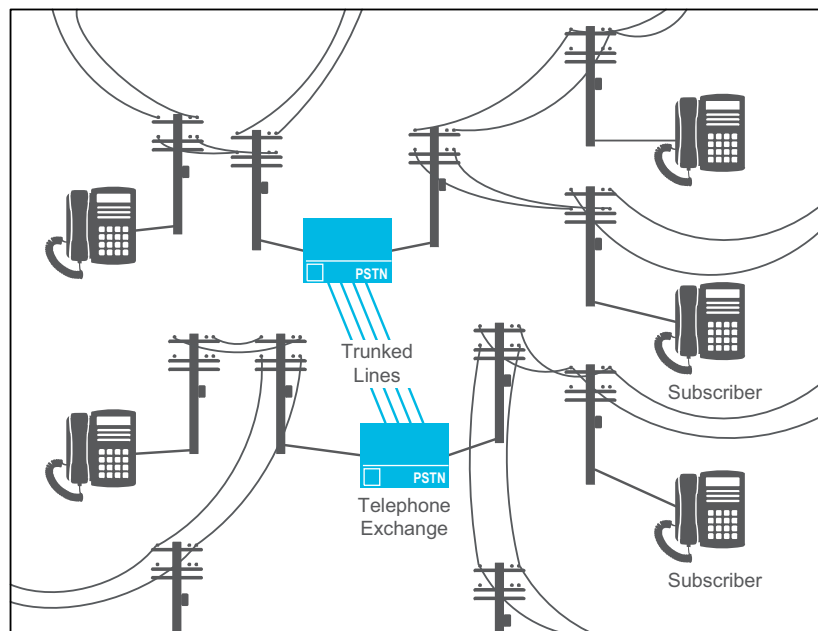


Figure 1.10 Trunked telephone concept

## Trunked Radio

Advances in technology provided a break-through in the form of low cost single chip microprocessors. This allowed the concept of trunking to be applied to mobile radio systems. A better name for trunked radio would be “computer aided radio” as it is the application of microprocessors and synthesizers that enables Trunked Radio Systems to share a pool of radio channels between many groups of users.

A trunked radio system has:

- A Control Channel that is used to send messages between the trunked system and the SUs.
- A number of Traffic Channels used for the voice calls.

Each group of users gets the exclusive use of a Traffic Channel for the duration of their call. No other groups are using the channel at the same time. A call has different meanings depending of the type of trunking:

- In Transmission Trunking, a call is a single over (press of the PTT).
- Quasi-Transmission Trunking uses a “Hang Time”. A reply within the hang time is part of the same call and uses the same traffic channel.
- In Message Trunking, a call may consist of several overs (a conversation) and continues until one of the users presses a button to end the call. It is typically used for individual calls.

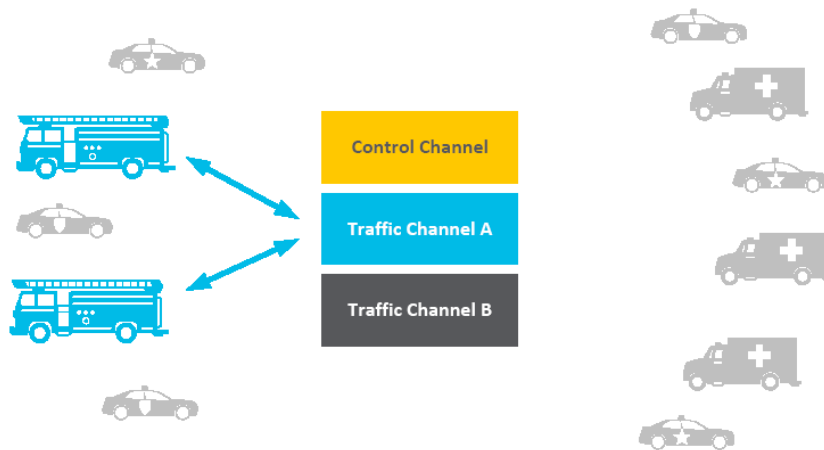
To set up a voice call on a trunking system:

- A subscriber presses the PTT, and the SU transmits a call request to the system via the control channel.
- The system sends, via the control channel, a Channel Grant message to the calling SU and the SU (or group of SUs) that they called.
- All the SUs involved in the call then tune to the designated traffic channel, and the call takes place.

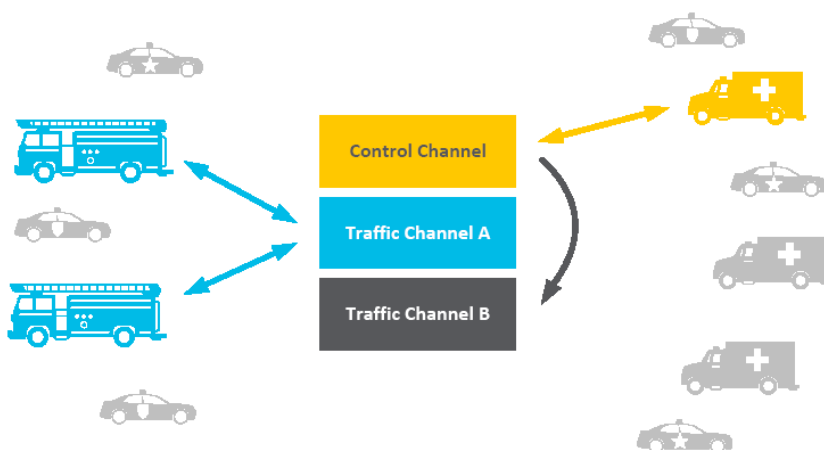
## Trunked Radio Example

A trunked site has a control channel and a number of traffic channels. The number of traffic channels required depends on the number of groups using the system and the number of calls taking place. Normally there would be at least four traffic channels, but in this simple example there are only two traffic channels. There may be hundreds of subscribers on a trunked system, but for simplicity this example shows just 11 subscribers. The subscribers consist of different groups or teams; in this example there are fire trucks, ambulances, police cars and highway patrol cars.

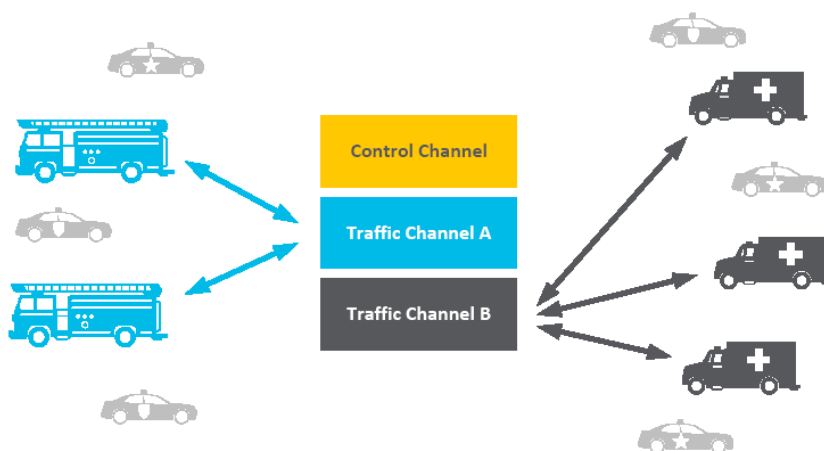
Trunking allows all these different user groups to share the same two traffic channels. In the picture below, a call is in progress between the two fire trucks, and the system has assigned Channel A for this call.



If one of the ambulances wanted to talk to the other ambulances, then when they make their call, the SU would use the control channel to send a request for a traffic channel to the system. The system would send a message back, which automatically directs all the ambulances to the available traffic channel; in this case Channel B.



The subscribers would use this channel for their call.



When either of these calls finish, that traffic channel is available to any subscriber for another call. The subscribers talking on the radio do not need to know what channel they have been allocated for the call; that all happens automatically in the SUs.

### 1.4.3 Trunking Efficiency

The key reason for adopting trunking technology is that it significantly increases the productivity and usefulness of a multi-channel mobile radio system.

In fact, the inherent efficiency of trunked radio is such that more than 50 radios can potentially be handled per channel. Several hundred radios may be able to share a multi-channel system without chaos during heavy traffic periods.

The way this is made possible is found in the interrelationship of three factors:

- Organization
- Queuing
- Call timing

#### **Organization**

Trunked radio systems are complex, so good organization is vital. A trunked radio system may support a number of different organizations, each with several talk groups, and many individual SUs.

#### **Queuing**

Queuing is a feature that becomes active when there are more people wishing to communicate than there are repeater channels available.

When this occurs, the SU requesting the call will display “System Queued” and the call request is placed in a list. When a channel is available, the SU will display a “Busy channel now free” message.

The occurrence of queuing on a correctly designed system is rare and queue times are short.

#### **Call Timing**

There are a number of timers included in the trunking system. The purpose of the timers is to improve the operational effectiveness of the trunking system.

## 1.4.4 Trunking Technologies

### P25

Quasi-transmission group calls

- Typical hang time: 2-5 seconds

P25	Message trunking		Transmission trunking		Quasi-transmission trunking	
	Individual	Group	Individual	Group	Individual	Group
Option 1	●			●		
Option 2	●					●

### MPT

Message trunking

- Typical call timeout: 30 seconds – 1 minute

MPT	Message trunking		Transmission trunking		Quasi-transmission trunking	
	Individual	Group	Individual	Group	Individual	Group
Option 1	●	●				
Option 2	●					Not recommended

### DMR

Mixed trunking call types

- Typical call timeout: 30 seconds – 1 minute

DMR	Message trunking		Transmission trunking		Quasi-transmission trunking	
	Individual	Group	Individual	Group	Individual	Group
Option 1	●	●				
Option 2	●			●		
Option 3	●					●

## 1.4.5 Advantages of a Trunked Radio System

A trunked radio system has several important advantages over a conventional radio system:

- It uses the available channels more efficiently. If a channel is free, then it will be allocated to a call, whereas it might be left unused in a conventional system.
- Because channels are used more efficiently, people don't have to wait as long for a free channel.

- Because channels are used more efficiently, fewer channels can be used for the same number of users.
- Because fewer channels are needed, the hardware cost per user is lower.
- Trunking makes it easy to share system with different agencies (cost sharing).
- Trunking makes it easy to expand and add capacity to the network without having to reprogram the SUs. If new channels are added to a site the control channel will simply direct radios to start using the new channel.
- Calls are more private, because the channel is allocated exclusively for a single call, and only the units in the call know which channel was allocated for the call.
- The dynamic allocation of channels and queuing features of trunking means if a channel fails at a site radio users may not experience any loss of communication. If the system is busy some additional queuing may occur.
- Trunking makes it easy to configure new talk groups and add new teams to the network.
- Trunked radios can still support conventional channels (e.g tactical, interoperability or fire ground channels).

#### 1.4.6 P25 Standards

There are a number of standards defining the operation of a P25 trunked radio system which define the features available and how they operate. These standards are published by the TIA. Some examples are listed below.

Document Title	Document Number
Common Air Interface	TIA-102.BAAA
Trunking Overview	TIA-102.AABA
Trunking Control Channel Formats	TIA-102.AABB
Trunking Control Channel Messages	TIA-102.AABC
Trunking Procedures	TIA-102.AABD
Link Control Words	TIA-102.AABF
Inter-RF Subsystem Interface Overview	TSB-102.BACC
Console Subsystem Interface Overview	TSB-102.BAGA

#### Open Interfaces

The primary drive behind these standards is to define a system that has an open architecture, so that the users of a system can purchase hardware from different manufacturers and know that it will operate.

There are continuous efforts within the TIA to define open IP-based system interface and RF interface standards. Some key examples are listed below:

- The P25 Console Sub-System Interface (CSSI) allows integration of best-in-class consoles and recording devices from different vendors.
- The P25 Inter RF Sub System Interface (ISSI) provides communications and subscriber mobility between RF sub-systems of different vendors. This allows multi-vendor system infrastructure implementation, thus reducing single source dependency of large system users.
- The P25 Common Air Interface (CAI) provides the user choice of SUs portable and mobile radios.
- Other P25 open interfaces ease implementation of data applications in offering a standardized connectivity. (Encryption, data base query, etc.).

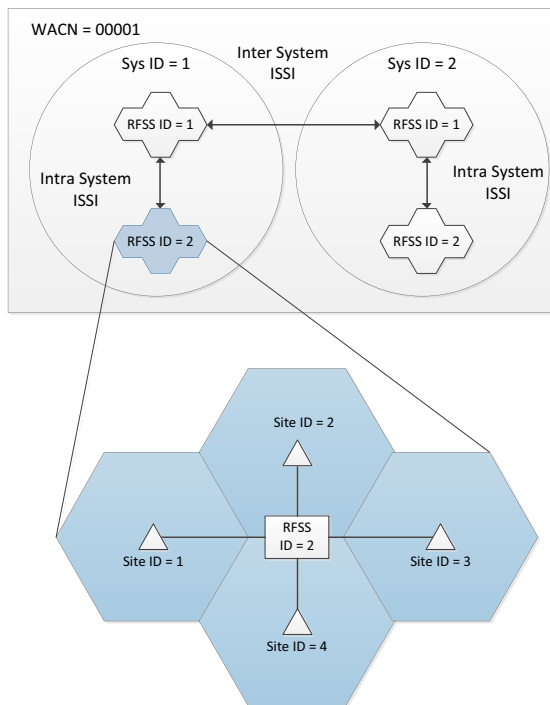
Work continues by the TIA to refine and publish standards for new features.

#### **1.4.7 P25 Trunked System Identification**

A P25 trunked Radio Frequency Sub System (RFSS) could have many sites and each site will have a control channel. It is also possible for more than one organization to install a P25 trunked RFSS in the same area. Therefore, it is important that the SUs can identify which system a control channel belongs to. To allow this to occur, the control channel is constantly sending messages that identify the site and the system. The SUs use these messages to identify a system, find new sites as the subscriber moves around, and to synchronize with the control channel when they move to a new site.

P25 systems and sites within that system are identified using four parameters defined below. The TIA states that a Land Mobile Radio (LMR) system is uniquely identified by its WACN and system ID. There is a document on the TIA web site “WACNguide010406.doc” that provides non-binding guidelines for the assignment of WACN and system identities.





**Figure 1.11 System identification**

1. Wide Area Communication Network address
  - (WACN) 20 bits
  - \$00001 to \$FFFFE
  - 1 to 1,048,574 Networks
2. System Identity
  - 12 bits
  - \$001 to \$FFE
  - 1 to 4094 Systems
3. RFSS Identity
  - 8 bits
  - \$00 to \$FE or
  - 1 to 254 RFSS
4. Site Identity
  - 8 bits
  - \$00 to \$FE
  - 1 to 254 Sites

**Acquiring a Network**

Before a SU can operate it must find the control channel. It must then get permission from the system to operate. This takes place in four stages:

- Hunting
- Acquisition
- Registration
- Group affiliation

**Hunting**

When a trunked SU is turned on it starts the process of finding a trunking system. The first step in the process is called “Hunting”. The purpose of the hunt is to locate a control channel.

**Acquisition**

The SU does not make any transmissions on a control channel until it is validated. It validates a control channel by listening to the messages from the system for the WACN and System ID. The SU may be in an area that has coverage from two or more sites and more than one control channel may be found during the hunt. The SU uses RSSI to rank channel quality and begins by validating the strongest signal. Once the best control channel has been acquired, the SU attempts to register with the network.

**Registration**

Full Registration takes place after hunting and acquisition. The SU sends a registration request. System checks validation and allocates the SU a Working Unit Identity (WUID).

**Group Affiliation** SU is registered on system but is not yet a member of a talk group. The SU Requests affiliation with a Talk Group. System checks validation and allocates the SU a Work Group Identity (WGID). If changing talk groups a new Group Affiliation request is sent.

**Voice Call Types** Now that the SU is registered and affiliated with the trunked network it can make calls. Typical voice call types include:

- Talkgroup call
- Announcement group call
- System call
- Unit to unit call
- Emergency call

These call types are described in later sections.

## 2 P25 Network Architecture

### 2.1 Network Overview

In any radio system coverage and capacity need to be considered.

Coverage is the area over which people need to communicate. A radio system is designed to deliver a minimum audio quality to the subscribers over a defined operating area. This may be achieved by a single repeater or by having overlapping coverage from more than one repeater, each repeating the same message.

Capacity is the number of simultaneous calls the system can handle. In other words the number of independent teams that can be talking at the same time. This is achieved by having a sufficient number of channels at each site.

Then there is the services the network will support (voice, data, encryption etc).

P25 networks can be designed to meet a wide range of requirements.

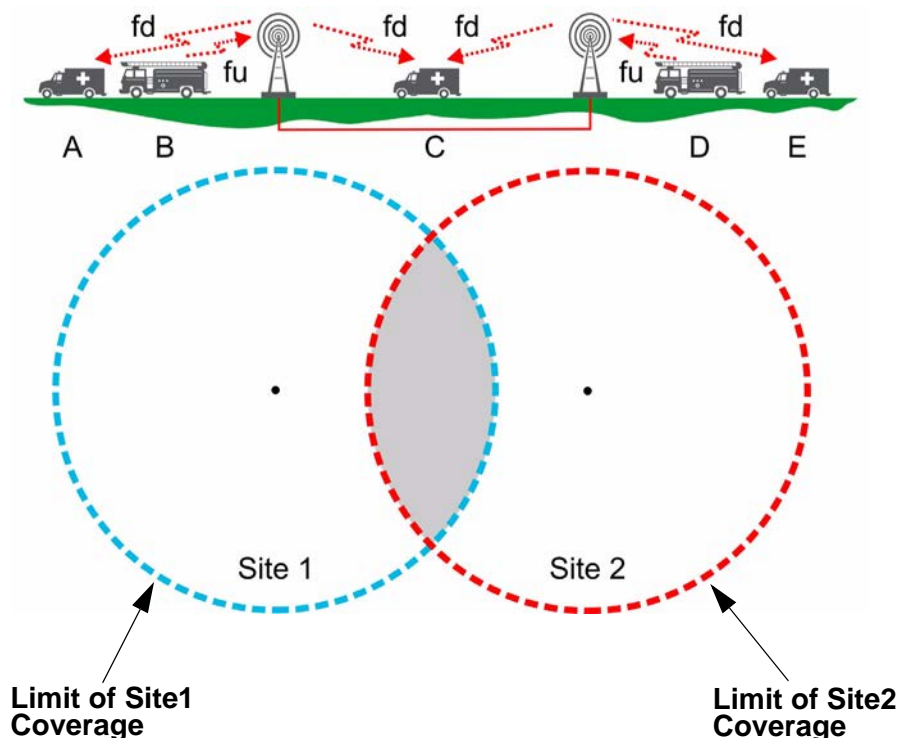


Figure 2.12 System coverage

## 2.1.1 Standards and Open Interfaces

There are a number of standards defining the operation of a P25 radio system which define the features available and how they operate. These standards are published by the TIA. The primary drive behind these standards is to define a system that has an open architecture, so that the users of a system can purchase hardware from different manufacturers and know that it will operate.

There are continuous efforts within the TIA to define open IP-based system interface and RF interface standards. Some key examples are listed below:

- The P25 Common Air Interface (CAI) provides the user choice of SUs portable and mobile radios and repeaters.
- There are a number of standards that define different aspects of trunking operation including:
  - Trunking Overview
  - Trunking Control Channel Formats
  - Trunking Control Channel Messages
  - Trunking Procedures
  - Link Control Words
- The P25 Console Sub-System Interface (CSSI) allows integration of best-in-class consoles and recording devices from different vendors to trunked P25 networks.
- The P25 Digital Fixed Station Interface (DFSI) allows integration of best-in-class consoles and recording devices from different vendors to trunked P25 conventional networks.
- The P25 Inter RF Sub System Interface (ISSI) provides communications and subscriber mobility between RF sub-systems of different vendors. This allows multi-vendor system infrastructure implementation, thus reducing single source dependency of large system users.
- Other P25 open interfaces ease implementation of data applications in offering a standardized connectivity. (Encryption, data base query, etc.).

Work continues by the TIA to refine and publish standards for new features.

## 2.1.2 Conventional System Types

In a conventional system, subscribers select a channel to communicate on. Tait offers a range of conventional system types, from a single repeater to wide-area simulcast or multicast networks in analog or digital mode.

### Simplex

Basic radio-to-radio communication in analog FM or digital P25 mode with no infrastructure. Typically used for on site or car-to-car communication.

## Repeater and Base Stations

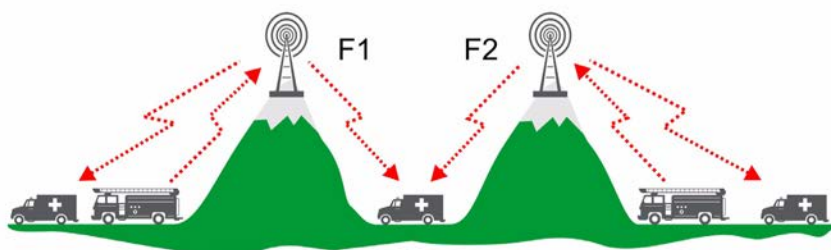
Increased range can be achieved if a repeater (transportable or permanent) is used. Signaling is often used to restrict access to the repeater and prevent interference. Analog or digital dispatch equipment may also be connected to the repeater and operate it as a base station.

## Scanning

If a user has to operate on a number of different repeaters, scanning means they do not have to manually change channel when they enter a new area. Alternatively, scanning allows a user to monitor other channels in addition to the one they are using for communication. When scanning, all channels in the scan group are sampled sequentially and continuously until one is found to contain valid traffic, that channel is then captured and the audio is heard. That channel is held until the conditions are satisfied for scanning to resume. The radio could be configured to allow a PTT to occur on the captured channel or to return to a default channel for transmissions.

Priority Scanning allows up to two priority channels to be checked more frequently by scanning them out of sequence on a timed basis. While the scanning has captured a non-priority channel, the priority channels are still regularly tested for activity to ensure that no vital information is lost.

Scan Group Editing allows the user to edit the members of the scan group from the radio front panel. This is a non-volatile action, and the changes will be saved.



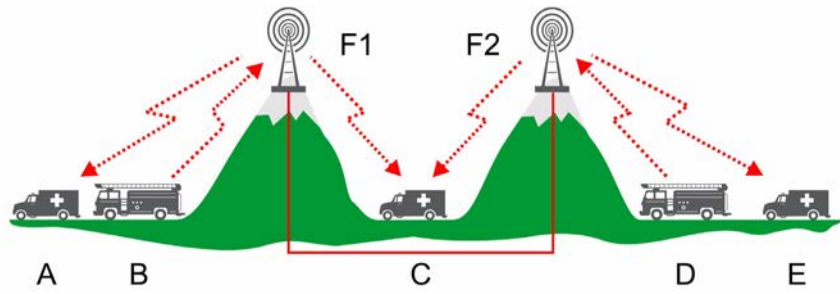
## Voting

Voting is used where a number of different repeaters all carry the same audio. A SU near one repeater site moving towards a second site will eventually receive a better signal from the second site than from the first site.

Voting in the SU allows the radio to automatically select from a group of channels the channel that has the best quality audio at any moment so the user will always hear the best signal. In the SUs, voting has 3 phases:

- Searching for activity (similar to scanning)
- Measuring the signal strength of all the channels
- Go to the channel with the best signal strength and unmute.

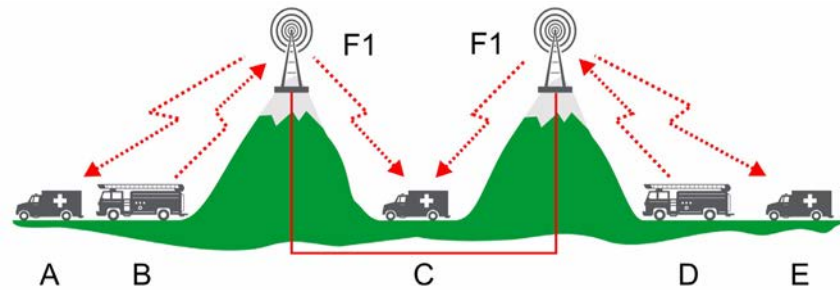
Voting also takes place in the network. Typically in a voted network, all the repeaters receive on the same frequency. When a SU transmits, voting takes place in the network to choose the receiver that received the best audio and this is retransmitted from all sites.



ⓘ The repeaters transmit on different frequencies.

**Simulcast**

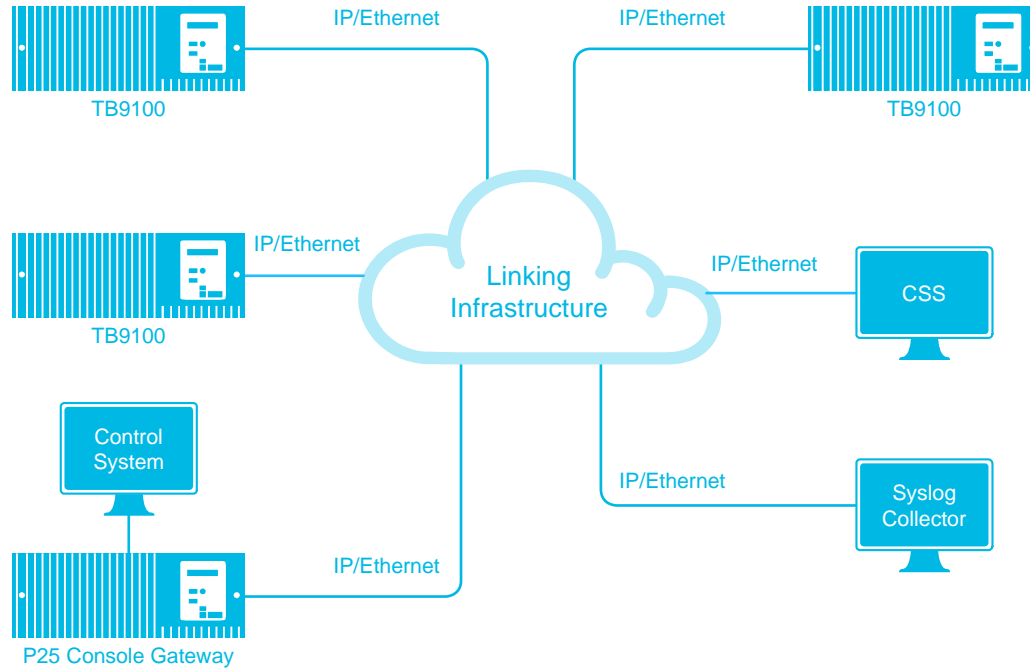
A simulcast network has several base stations transmitting on the same frequency with overlapping coverage areas. A simulcast network is designed so that the base stations time synchronize their transmissions making them all appear like one base station with a large coverage area. Simulcast is an effective way to cover a large area with only one frequency. Tait SUs have been designed to operate on simulcast infrastructure and can be configured to receive several non-standard modulation schemes often used on simulcast networks.



ⓘ The repeaters transmit on the same frequency.

**Tait Conventional Networks**

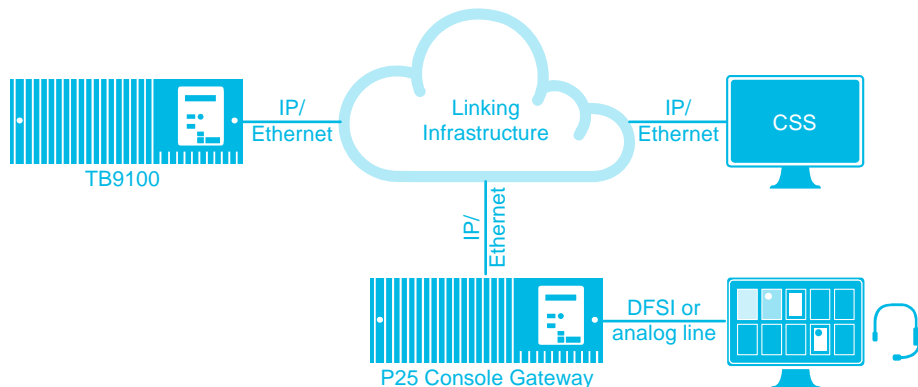
A TaitNet P25 network is a set of interconnected TB9100 base station transceivers. Each TB9100 can receive from and transmit to mobile and portable radios, just like any base station/repeater. However, TB9100s also have built-in networking and voting capabilities that enable them to combine together to form one or more logical channel groups with wide area coverage. Simulcast operation is also supported.



**Conventional Dispatch Console Support**

Dispatch equipment can be line-connected to a single TB9100 base station or to a whole channel group. If there are multiple dispatcher positions, the dispatch equipment usually has some kind of console switch to enable the dispatcher to select the channel to talk on.

Often, dispatch equipment is connected to the TaitNet P25 network via a P25 Console Gateway. The P25 Console Gateway provides an analog line if the dispatch equipment is analog, or a DFSI interface if the equipment is digital. Alternatively, dispatch equipment can be connected directly to a base station in the channel group. With the appropriate feature licenses, any TB9100 can provide an analog line interface or a DFSI interface.



### 2.1.3 Trunked System Types

Trunking is an efficient way for a large number of subscribers to share a limited number of channels. Intelligent controllers are added to the system. Instead of selecting a channel, a subscriber simply selects a group (or individual) they wish to communicate with, and the system automatically assigns them to a free channel for each call. Each network has a system key which prevents people from programming radios to work on the network without authorization from the network operator.

#### Single Site Trunking

A trunked site has a control channel and a number of traffic channels. When a subscriber makes a call, the control channel is used by the network to automatically send the caller and the called radio (or group of radios) to a traffic channel. The traffic channel is used for the call. At the end of the call, the SUs return to the control channel, and the traffic channel is available for others to use.

#### Multi-Site Trunking

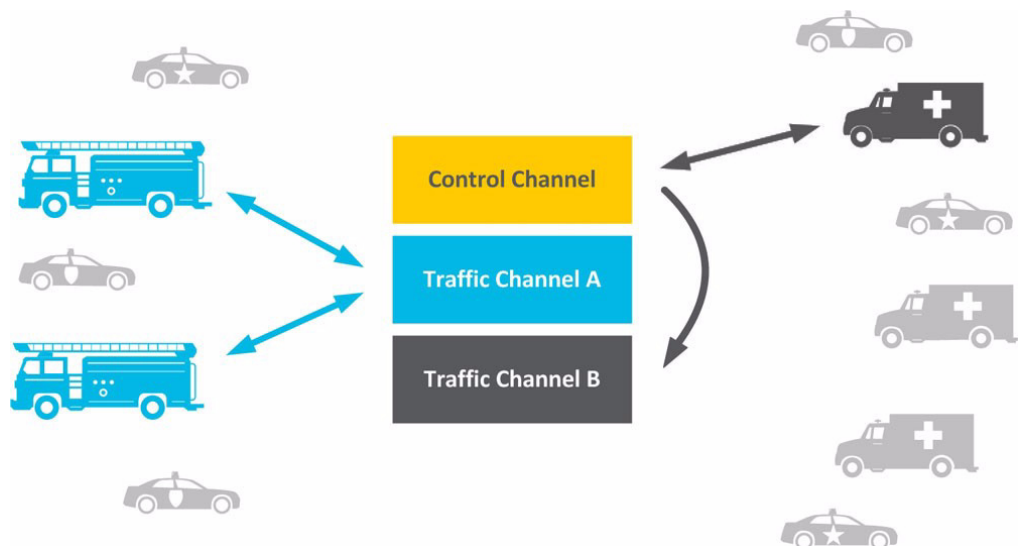
A trunked system with more than one site. As a SU moves around the coverage area, it automatically roams from one site to another so it is always listening to the best control channel. If a call involves SUs at different sites, a traffic channel is allocated at each site.

#### Receiver-Voted System

When portables and mobiles are used on the same system, sometimes the mobiles can make calls where the portables cannot because they transmit with more power. A receiver voted system has extra sites with receivers only (lower cost) to balance the coverage between portables and mobiles.

#### Trunked Simulcast System

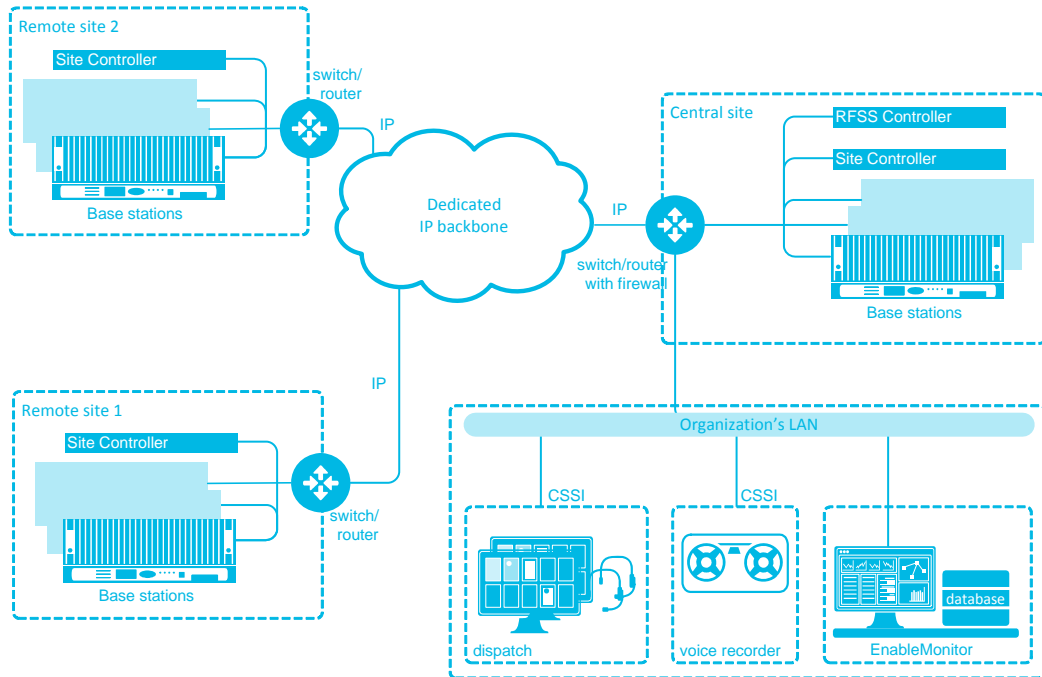
Where frequencies are scarce, trunking and simulcast can be combined to create trunked sites that cover wide areas by using multiple transmitters on the same frequency in different locations.





## Tait Trunked Networks

The Tait P25 trunked solution is an IP-based, digital trunked infrastructure specifically designed to provide mission critical voice and data communications over wide geographic areas. The scalability and flexibility of the Tait solution allows for the deployment of a cost-effective infrastructure which meets the mobile communication needs of Public Safety and Public Service users across multiple jurisdictions.



## Trunked Dispatch Console Support

In a trunked system, digital (IP) dispatch equipment can be connected to the network using the P25 Console Sub System Interface (CSSI) protocol.

Analog dispatch equipment can be connected to the TaitNet P25 trunked network via a Trunked Analog Gateway. The Trunked Analog Gateway is IP connected to the network and configured to be a member of a trunked Talk Group. It provides an analog line connection for the dispatch equipment allowing the dispatcher to communicate with the trunked Talk Group.

### 2.1.4 Conclusion

Versatile P25 compliant equipment can be configured to meet a wide variety of different system requirements. P25 compliant equipment is also able to overcome many of the technical barriers to interoperability, so customers can secure value in a multi-vendor environment.

## 2.2 Linking

### 2.2.1 Linking Infrastructure

The linking infrastructure is what interconnects the P25 repeaters, controllers and dispatch equipment to form a P25 network.

In recent years, we have seen increasing momentum for the transport of voice and data applications within the same network, and the progressive replacement of TDM networks by IP networks.

The initial motivation for this convergence was the reduction in communication costs and replacement of TDM switches by new generations of controllers and base stations equipped with an Ethernet interface. The level of cost reduction can be significant, as a unified packet network can:

- Reduce bandwidth consumption by using high-performance compression algorithms
- Lower line costs, fully redundant ring architecture can be used versus a hub and spoke plan
- Lower maintenance costs, as only one infrastructure for data and voice needs to be maintained

These technologies bring the following advantages for the design of mission critical systems:

- It takes advantage of IP multicast addressing for group and individual communications strengthening communications reliability and service availability in case of network failures.
- It provides the openness and interoperability means which mission critical systems desperately need:
  - Use of standard Internet Engineering Task Force (IETF) protocols
  - Use of web enabled applications and interfaces (such as SNMP) for network management, and open interface with external applications
  - Support for a native implementation of IP-based P25 system interfaces
  - Use off-the-shelf hardware for network controllers and networking equipment.
- It provides a future-proof multimedia LMR core system platform that:
  - Breaks away from proprietary hardware and software implementations.
  - Is ready to support emerging data applications.

## 2.2.2 Linking - Monitoring and Management

P25 linking is typically IP-based and consists of Local Area Network (LAN) equipment at each site and a bearer network of links that interconnect the sites to form a Wide Area Network (WAN). Often the LAN equipment belongs to the TaitNet P25 radio network, while the bearer network may be shared with other data services.

The linking infrastructure can be integrated with an organization's LAN. This makes it possible for PCs running suitable software to connect from anywhere in the organization and monitor and manage the radio network.

Due to the use of IP networking for the radio network, in larger organizations, the team that manage the computer network may take on the responsibility for the radio network linking. This can work very well but will require the networking team to understand the requirements for real time voice networking and the importance of certain links for voice communication. Also where the radio equipment and linking equipment are managed by different teams. A broader notification group for change management and fault reporting may be required.

## 2.2.3 Dedicated or Shared Network

Standard IP protocols mean there are many ways to engineer the linking. The network could be dedicated to the radio system or shared with other data systems.

IP linking provides an efficient means for multiplexing voice and data traffic over private wide area networks. Sharing voice and data on the same network does come with some risks. Real time voice applications have strict quality of service requirements on bandwidth, delay and jitter. This becomes more important if the P25 network shares the same linking as other data traffic between key locations. This can be effectively managed with QoS and Security protocols and capacity planning.

## Routed Network

In routed networks, each site has its own LAN segment. Routers are the interface between the LAN segments and the bearer network. They convert the data between Ethernet and other protocols such as T1 (for feeding to the bearer network) and vice versa.

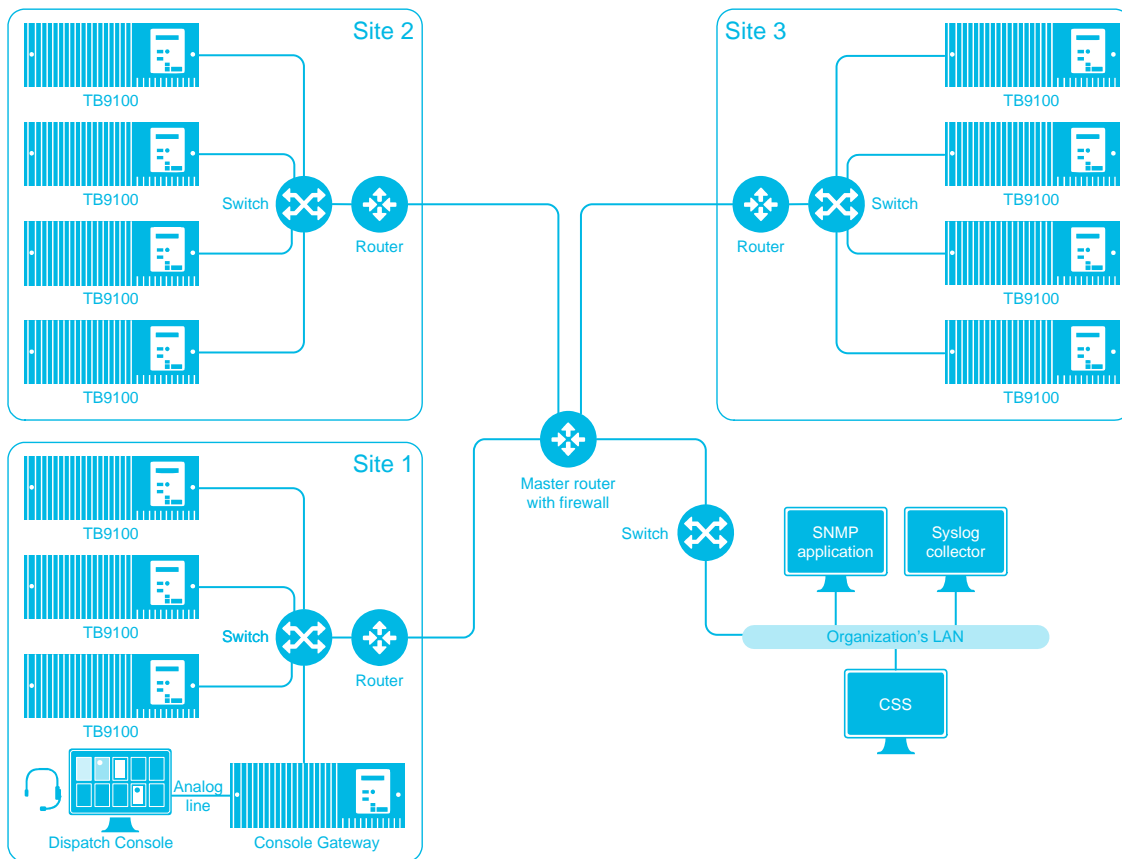


Figure 2.13 Routed network

This example uses a star topology, which limits the number of router hops to two even with a larger number of sites. Only Tait-approved routers can be used and they must be configured for particular requirements such as IP multicast and Quality of Service (to give the voice stream priority over other data). The bandwidth requirements can be reduced by the use of compressed RTP.

A CSS and a syslog collector can connect to any LAN segment. Communications to and from the CSS will be rapid with base stations on this LAN, but can be quite slow over the bearer network to base stations on other LAN segments, as its bandwidth is generally much smaller and voice traffic takes priority.

## Switched Networks

In switched networks, switches are used instead of routers to link sites. The whole TaitNet P25 network is essentially a single LAN. This is achievable if the remote links between sites have a sufficient bandwidth. The TaitNet P25 network can be integrated with the organization's LAN by configuring each as a separate VLAN (virtual LAN). Then a router is needed to route data between VLANs, in this case to enable the CSS and the syslog collector to operate from within the organization's LAN.

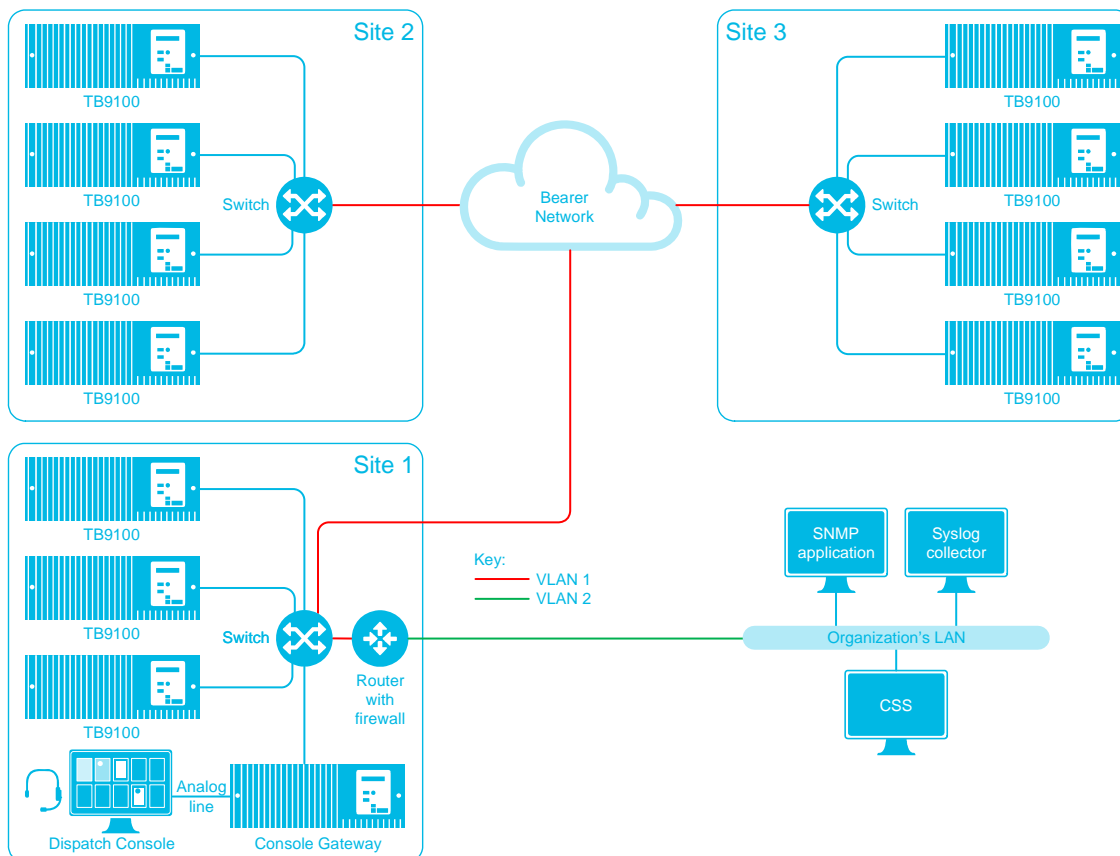


Figure 2.14 Switched network

The links between switches need to have sufficient bandwidth to ensure minimal jitter. Switches are not normally able to prioritize voice over IP packets. Link terminals on the other hand are often able to do this.

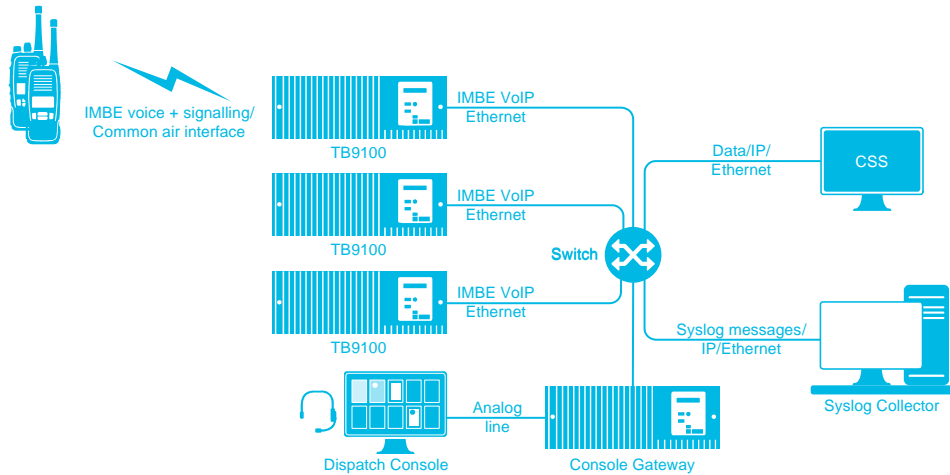
## 2.2.4 Voice over IP

The repeaters (or base stations) receive calls from SUs how is the voice sent over the IP network?

In digital P25 mode, these communications are already in digital IMBE format, with forward error correction added. The base stations correct any errors and remove the forward error correction bits. They put the result on the network as 'voice over IP' using RTP (the Internet real-time protocol). Switches pass the RTP packets to the router, and then over the bearer network to other network elements.

Modern dispatch equipment is IP connected to the same network. When interfacing to older analog dispatch equipment P25 Console Gateways convert these IP communications to suitable protocols and pass them to the dispatch console equipment.

Analog FM calls can also be networked. The received voice is converted into digital G.711 format by the base stations and sent out using RTP. G.711 needs more bandwidth than IMBE.



**Figure 2.15 Network signal paths with Tait TB9100 repeaters**

In addition to this voice traffic, the linking infrastructure carries alarm messages and Customer Service Software (CSS) communications. A PC running the CSS can communicate with any base station on the network, monitoring it, changing its configuration, or carrying out diagnostic tests. Alarms and other status indications can be sent to a syslog collector or SNMP manager.

## 2.2.5 Trunking

The network diagrams in the previous sections showed only the repeaters and networking equipment. In a trunked system there are also the site controllers and RFSS.

These devices are IP connected so can be placed anywhere on the IP network. However the choice is often dictated by the bandwidth requirements and the impact of fault conditions such as a link failure.

Typically the site controller is placed locally at the radio site and the RFSS controller and other gateways are located at a central site (such as the dispatch center) that may or may not have any radio equipment.

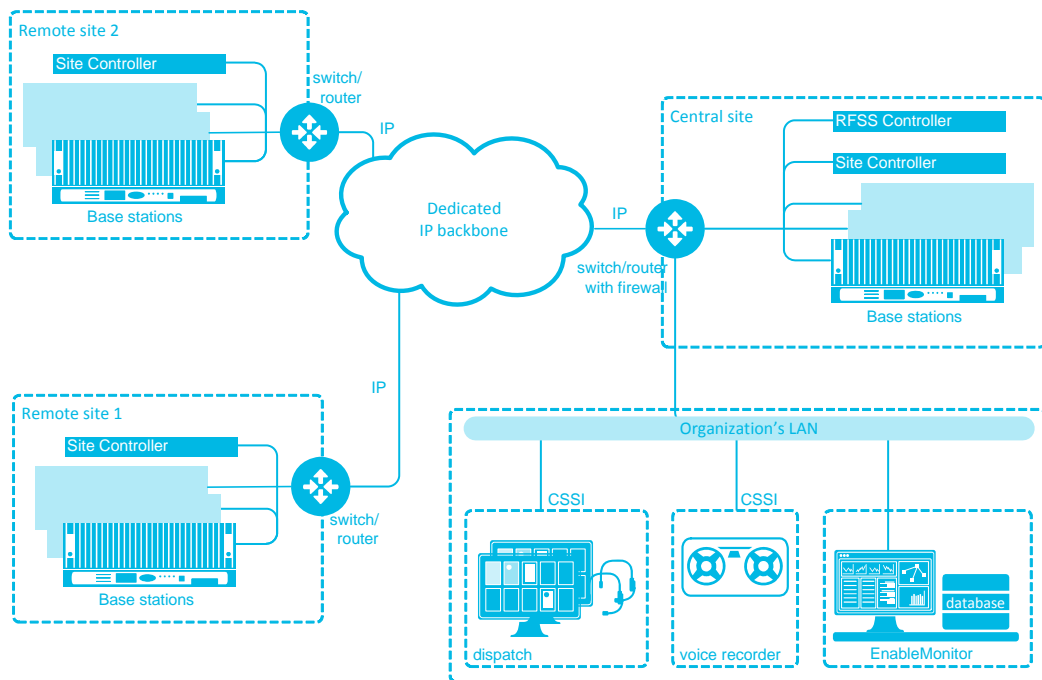
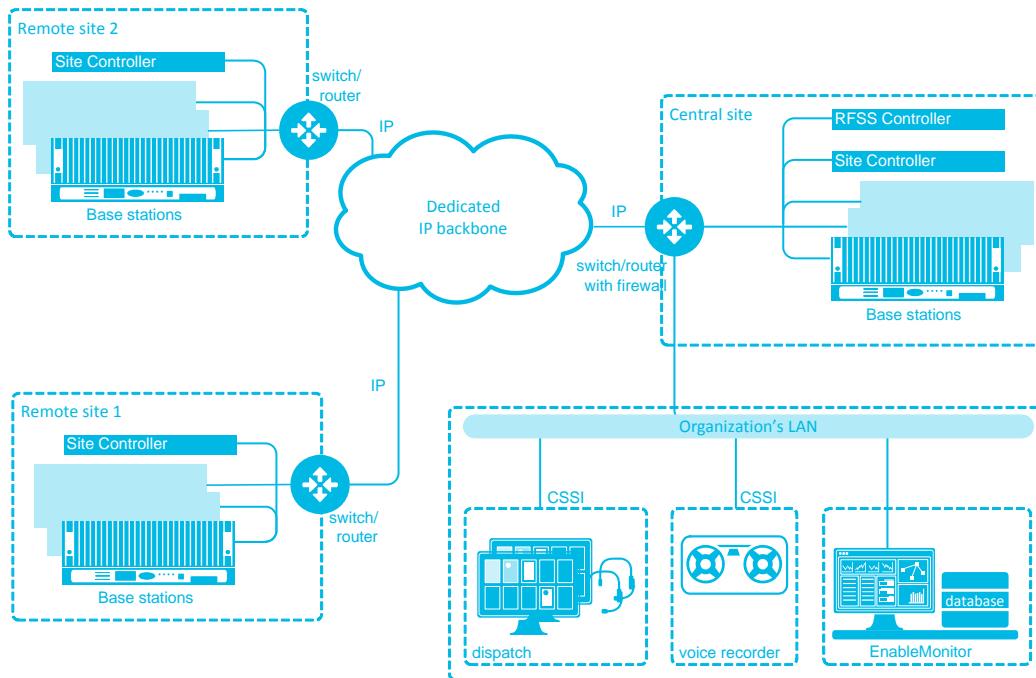


Figure 2.16 Trunked network example

## 2.3 Site Equipment

### 2.3.1 Introduction

The site equipment at a P25 radio site is very similar to the site equipment at an analog radio site. Remember a benefit of P25 was the ability to remove an analog channel and install a P25 channel on the same frequency. Also although a P25 network can be conventional or trunked in each case much of the site equipment is very similar. In this section I will simply give a general overview of a P25 radio site and try to highlight some key points.



### 2.3.2 Antenna System

A radio site will have an antenna system. This will be the same for a P25 or an analog radio site. There will be tower or mast with either omnidirectional or directional antennas (depending on the type of coverage footprint needed). Combining and filtering equipment can allow multiple repeaters to share the same antenna.

### 2.3.3 Power Supply Equipment

There is a range of power supply options available for P25 radio equipment. The site may run on AC mains power or be DC powered (often 12, 24 or 48v). Often there is backup power such as batteries and generators and power supply monitoring equipment.



### 2.3.4 Repeaters (Base Stations)

A repeater or base station is a radio receiver and transmitter that is located in a specific place (at a site). It is programmed with the receive and transmit frequency for a radio channel and enables mobile and portable radios to communicate with a dispatcher or over a larger range than via direct radio to radio communication.

They are often called Base Stations or Fixed Stations as they are physically installed at one location or Repeaters as they receive then retransmit the radio calls they receive.

A P25 repeater typically has a modular design and is made up a subrack containing some or all of the following modules depending on the configuration:

- Power supply unit to match the supply available at the site.
- Power amplifier of a suitable output power (50W and 100W are typical).
- Receiver and transmitter (sometimes in the same physical module).
- IP Network interface typically integrated into the repeater but it may be a separate module (in addition to IP an analog audio interface is often available).
- Front panel with indicators and controls and fans for cooling.



Figure 2.17 TB9400 P25 digital repeater

#### Channel Types

Typically the same repeater hardware can be configured for operation in a conventional or trunked Project 25 radio network.

- In a trunked system one of the repeaters acts as a control channel. This is not used to carry voice or data calls. Instead it is used by the system to communicate with the mobile and portable radios allowing them to request and be allocated a traffic channel from the pool for a call
- In trunked systems there is a pool of repeaters for voice and data calls these are called Traffic channels. The use of these channels is controlled by the site controller.
- In conventional systems all the repeaters are used for voice or data calls (or traffic). The mobile and portable radios are manually switched to the correct channel.

### **2.3.5 Networking Equipment**

A P25 site is typically IP connected this may be for voice, data and remote management. Therefore IP networking equipment is required on site. A IP switch connects all the repeater (and control equipment) together. This forms a local area network at the site. There may also be a router that connects to the linking to other sites.

### **2.3.6 Linking Equipment**

In addition to the Networking equipment there is likely to be linking equipment. This may be part of the radio network. Or provided by a 3rd party who can provide the required grade of service. Typical links are microwave or fiber. However other emerging technologies such as Mimo Max or legacy PDH systems may be used.

### **2.3.7 Trunked Site Control Equipment**

In a trunked system there is likely to be a device called a Site Controller located at the radio site. This is typically a server running a software application that controls the repeaters but may be custom hardware.

In many cases the Site Controller is located at the site but because P25 is typically IP connected the Site Controller could be installed off site and controls the repeaters over the link.

### **2.3.8 Conventional Control Equipment**

A conventional network may not have any control equipment the site may just have repeaters.

A large conventional systems that connect multiple sites together may have control equipment at the site to vote on the best signal being received from multiple sites. However often this function is now built into the repeaters themselves rather than being external equipment.

## 2.4 Central Site Equipment

In large radio networks there is often a central or master site. This controls all the individual sites and may or may not have its own radio equipment.

### 2.4.1 Conventional

A small conventional system may have no central site equipment.

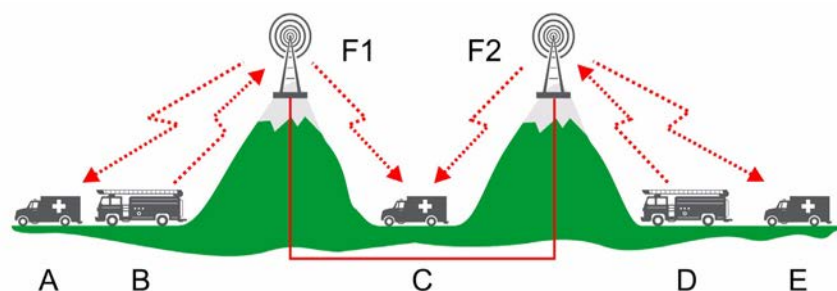
However in a large conventional system (voted or simulcast) where multiple sites broadcast the same call to provide increased coverage there is typically a master site that controls the audio that is rebroadcast from all the individual sites.

In a voted network, all the repeaters receive on the same frequency. When a SU transmits they are received by multiple sites. All the received audio is routed to the central site which chooses the receiver that received the best audio and this audio is retransmitted from all sites. Sometimes the voting is carried out by additional hardware at the central site. Sometimes there is no additional hardware it may be a software feature in the repeater.

A dispatch system will typically connect to this central site. To the dispatcher and radio users this group of repeaters acts like a single repeater with a large coverage area.

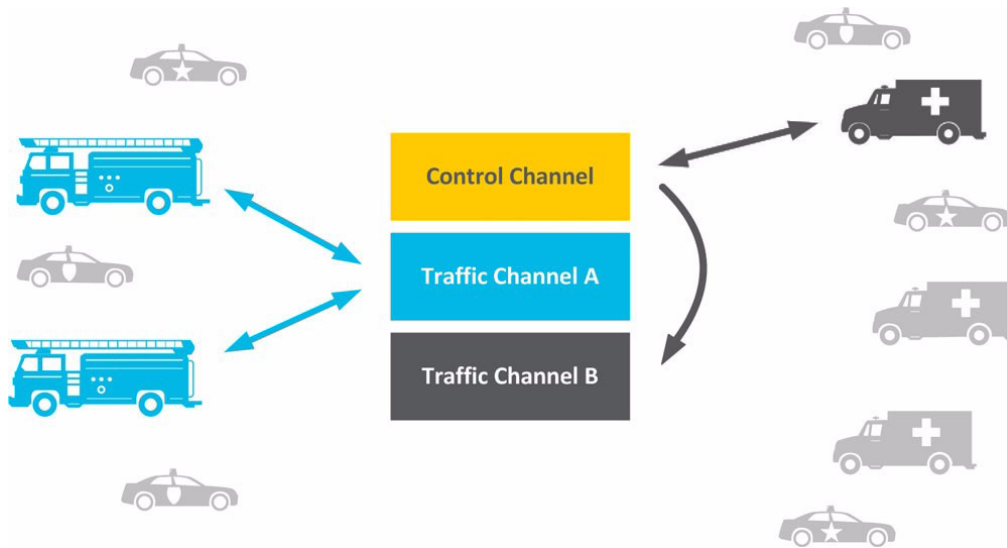
To increase coverage area additional sites can be added to the voted network.

If additional capacity is needed another set of repeaters may be installed at each site. This can provide communication to a separate group and be independent of the first channel. However the same linking and networking equipment may be used.



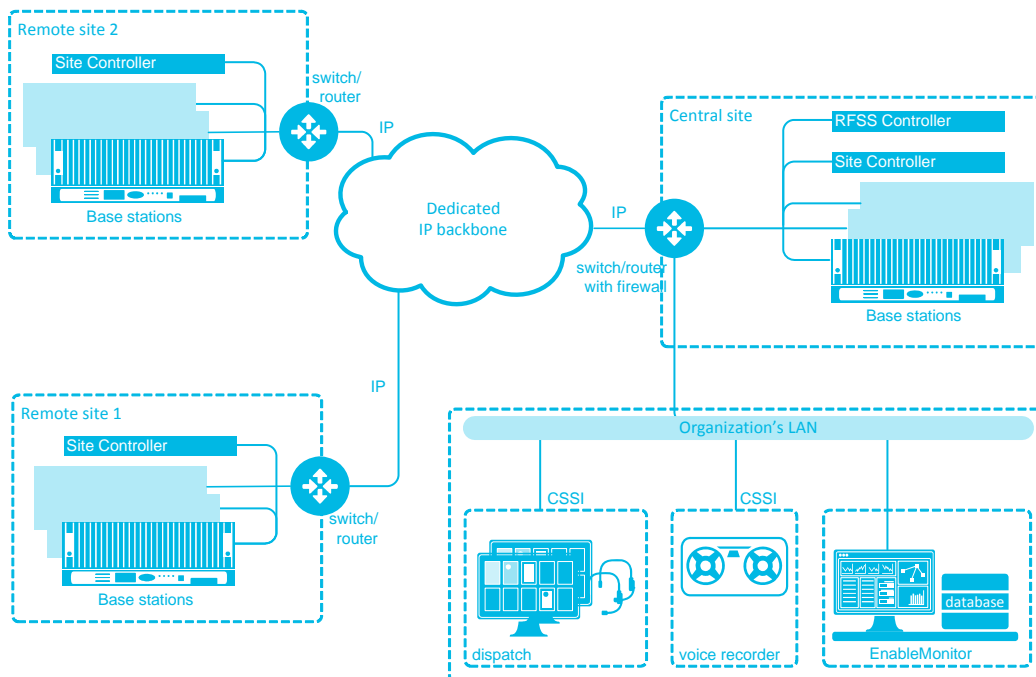
## 2.4.2 Trunking

A trunked system has a controller at each site controlling the channels.



However a trunked system may be made up multiple sites. This collection of sites is controlled by a Radio Frequency Sub-System Controller. Note that even on a single site trunked system there is a RFSS.

The RFSS controls which radios are permitted to access the system and what sites they can use. The RFSS also controls which groups are valid on the system and what sites they can use. It is often involved in the routing of audio between sites (although this task may be handled by the site controllers). Dispatch equipment will also connect to the RFSS. Larger networks can be made by joining multiple RFSS together



### **2.4.3 Management**

Because P25 networks (Conventional or Trunked) are IP connected there is often a monitoring and management system. This collects and logs call records from the system. It also monitors and displays performance and fault information. Fault management often uses the industry standard SNMP protocol. This allows the radio network and linking network to be monitored in one place.

## 2.5 Gateways

P25 networks have standard interfaces defined. These allow different subsystems to connect. They are effectively gateways to other systems.

### 2.5.1 Dispatch

One of the key benefits of the P25 system infrastructure is the possibility for users to select the most suitable dispatch consoles, accommodating their operational needs and budgetary constraints.

In addition to voice calls consoles provide advanced features to operator position such as, but not limited to:

- Console priority
- Patching channels together
- Status messaging
- Emergency calls
- Automatic Number Identification (ANI) of callers
- Instant recall recording
- Console phone interface
- and many other features

The P25 system is capable of supporting different dispatch console manufacturers as they implement the IP-based P25 CSSI or DFSI standards.

The CSSI protocol is an IP-based interface from a P25 trunked network to a dispatch console system. These consoles can be designed to virtually any size or configuration depending upon the specific needs. The system grants specific privileges to the dispatch operator. For example, a dispatch position operator has the ability to override an active call from a SU. Voice recorders often interface to the system using the CSSI protocol

The DFSI protocol is an IP-based interface from a P25 conventional repeater or network of repeaters to a dispatch console system. It includes channel control commands and the ability to operate in analog or digital mode.

However, many agencies have existing analog console systems that they wish to interface to a P25 network. This can be achieved by using an Analog Gateway.

## 2.5.2 Phone

The P25 protocol allows phone calls. Many systems have a gateway that allows a radio user to make a PSTN or PABX calls.

Telephone calls are an option feature of P25 trunked networks. In many public safety networks this feature is required as the dispatcher can patch a phone call through when needed.

In commercial systems such as petro-chemical dialling phone numbers may be required and for safety reasons cellular phones may not be permitted on site. Therefore some networks allow radio subscribers to dial phone numbers from their radio.

The P25 standard includes a protocol to transport the dialled digits to a telephone gateway. This gateway then validates if that number is permitted to be dialled. If so it sets up the call and transcodes the audio between analog on the telephone network and P25 digital on the radio network.

## 2.5.3 Data

P25 systems can support IP packet data. This means each radio can be allocated an IP address and data applications can talk to subscribers via its IP address.

There are several standardized data services provided by P25. These include:

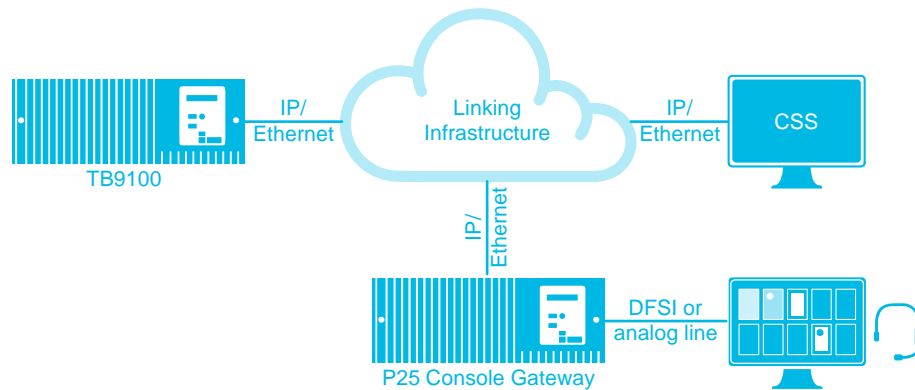
- GPS or location information.
- Over The Air Rekeying (remote change of encryption keys)
- Over The Air Reprogramming (radio configuration changes over the air)

However IP Packet Data P25 allows P25 to support a large range of data applications. However because the transport mechanism is standard the data application's themselves can be proprietary and custom made

## 2.5.4 Analog Gateway

In some cases a new digital radio network needs to be connected to an existing analog console system (or analog radio channel). Some vendors provide gateways between the digital network and an analog console. Tait has two such gateways a Console Gateway for conventional systems (although if there is a local repeater at the dispatch center this can be configured to act as the gateway) and a Trunked Analog Gateway (TAG) for trunked networks.

The Analog Gateways has been developed to allow older dispatch consoles that use a 4 wire analog interface that supports either E&M or tone remote operation to interface to the network. The gateway can also translate between P25 signaling and MDC1200 signaling. MDC1200 signaling can be used for ANI, for calling an announcement group, for providing the number of an individual call, and for supplementary services. The gateway also serves as an encryption/decryption point for encrypted calls, and therefore supports key management activities such as loading and updating key material.





## 2.5.5 Alarms

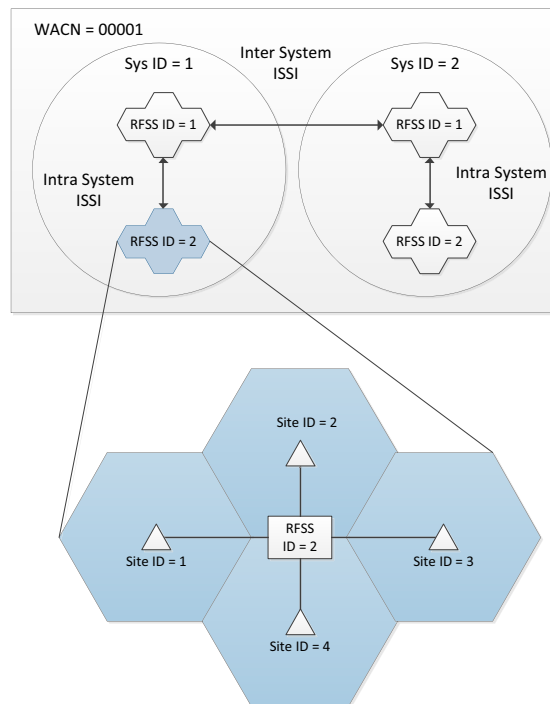
Because P25 systems are typically IP connected standard IP protocols for fault management are typically used. Many P25 systems can interface to SNMP management systems.

## 2.5.6 Inter Sub System Interface

The term “RFSS” is used to describe a completed, autonomous trunked radio sub-system managed by the RFSS Controller. The RFSS Controller controls a number of RF sites, dispatch sites, external interfaces, and provides the full set of services to its “home” subscribers.

A user at any location within the RFSS coverage area can, with the proper authorization, press the SU’s Push-To-Talk (PTT) button to make a call to any valid talk group or individual located anywhere else in the coverage area.

The ISSI standard protocol allows RFSSs provided by different vendors to be joined together to form one wide area communication network.



## 2.6 Network Management

In this chapter I am going to look at three aspects of network management:

- Tactical Management - The management of subscribers and groups using the network
- Technical Management - The configuration of network hardware
- Network Monitoring - Fault and Performance information

These tasks may be carried out by the same person or different teams so we will look at each in turn.

The terminology I am using comes from a Cassidian P25 Trunked Network manager but the same concepts will apply to any trunked radio system.

### 2.6.1 Tactical Management

This is the management of subscribers and groups on the network.

In order for a SU to gain service on the network it must be declared to the trunked Radio Frequency Sub System Controller (RFSS) as a valid unit. The Talk Groups for the various teams that use the network and the sites they are permitted to use must also be declared to the system.

When a network is first designed it will be designed to provide coverage over a specified area and to be able to handle a certain number of calls. During the deployment of the network the initial fleet of SUs and groups is declared to the system.

Over time units and groups may be added or deleted as more subscribers join the network or if units are lost or damaged. Units may also be temporary removed for maintenance.

On many P25 networks this type of tactical management can be carried out from a web browser connected to the RFSS. On networks shared by many agencies it is often possible to restrict the tactical management login to a subset of units and groups on the system. On large state-wide networks individual agencies may not carry out Tactical Management on the network directly. They may submit a request for more unit IDs to the body that manages the network for a number of agencies. That agency will then ensure there is enough capacity for all users and validate the new units. The requesting agencies can then configure and issue the SUs.

## 2.6.2 Technical Management

Technical Management relates to the network infrastructure itself.

The configuration of sites, channels and any gateways to dispatch systems or telephone networks. Once the system is designed and deployed there may be very little Technical Management required. However over time additional capacity or coverage may be required and new sites or channels may be added to the network.

On many P25 networks this type of tactical management can be carried out from a web browser connected to the RFSS.

The access to the Technical Management features of the network is typically restricted to a different login than tactical management. However proprietary software tools for configuring specific network elements such as repeaters is not uncommon.

## 2.6.3 Network Monitoring

In addition to the initial configuration of the network it is important to monitor the network to ensure it is operating correctly. This includes:

- Monitoring for faults and alarms from network elements (such as repeaters, controllers and linking equipment).
- Performance monitoring - is there sufficient capacity in the network to handle the volume of calls being made.

As most P25 networks are IP connected fault management is often carried out using standard IP techniques such as SNMP. Any alarms or faults are sent to a central server and alarms can be generated at network management centre or via SMS or email if a fault occurs.

Performance management typically means reviewing logs or utilization records to identify if there is any queuing or waiting to access channels occurring. This information can help target future investment in network to the specific areas (i.e sites) that are handling the most calls.



# 3 Channel Operation and Configuration

## 3.1 Physical and Logical Channels

One topic that often causes confusion in digital radio networks is the difference between physical and logical channels.

### 3.1.1 Physical Radio Channel

A physical radio channel is a radio frequency or pair of frequencies that is allocated by the regulatory body to an agency for communication.

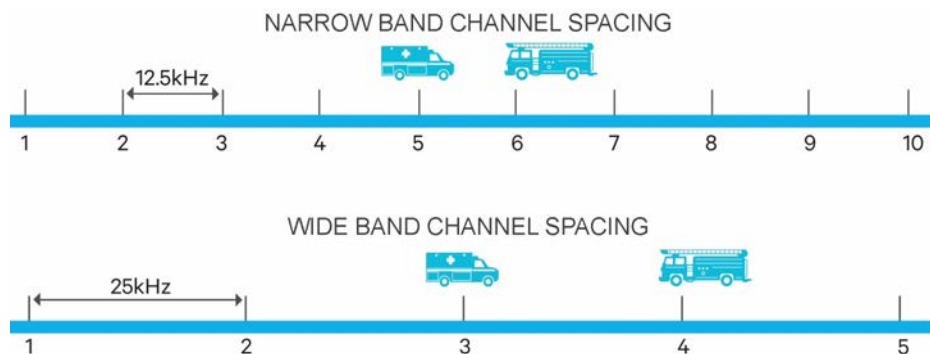


Figure 3.18 Radio channel

In simplex (direct radio to radio communication) the same frequency may be used for reception and transmission. Where repeaters are used a pair of frequencies may make up the radio channel, one frequency for transmitting into the repeater and another frequency for receiving from the repeater. This pair of frequencies is still one radio channel.

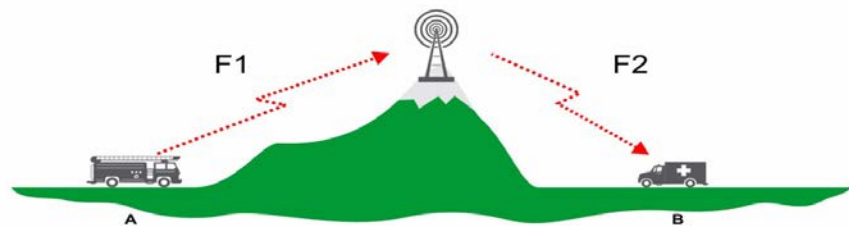


Figure 3.19 Repeaters use a pair of frequencies

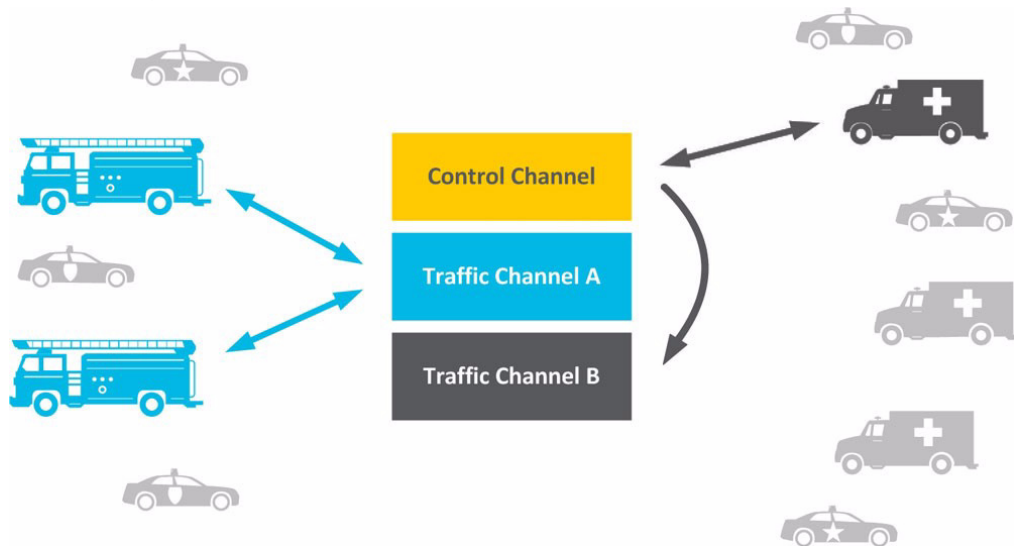
Traditionally a radio channel could carry one voice call - one person talking. This is also true for Phase 1 P25 digital radio. The voice from the talker is converted to digital data and constantly streamed on the channel as a digital data stream. If the system had to have the capacity to allow two different teams to talk at the same time a second physical channel would be required.

### 3.1.2 What happens if there are not enough channels?

A trunked system only allocates a channel when a call is in progress. This means more groups can be allocated to the radio network than there are channels the system. The pool of available channels is shared by the groups on the network.

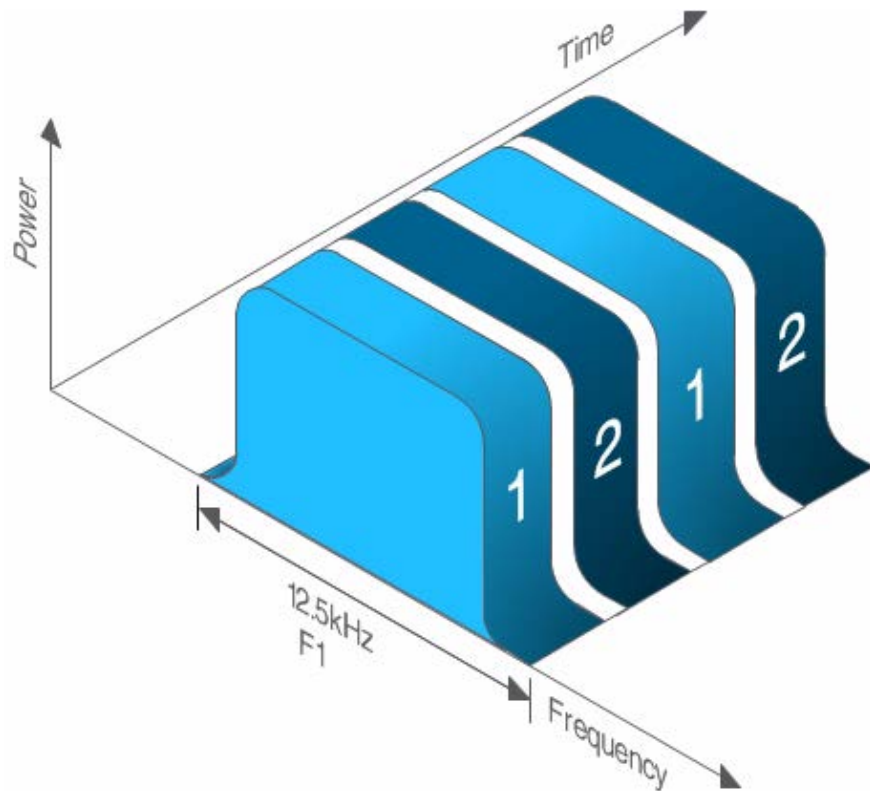
This works well up to a point. However when the system gets busy and many groups are making calls there may be times when there are not enough channels available to handle all the calls. Some groups will need to wait for a channel to become free before they can access the system. This is known as queuing on the trunked system.

On busy trunked system where there are many different groups sharing the same network a site is designed to have enough capacity for all the critical groups to be able to use the system at the same time. There must be enough channels on the site that queuing should be a vary rare event. This can quickly use up all the available physical radio channels in that area and limit the number of groups that can use the network (with out the risk of queueing). A method was needed to allow the system to handle more calls.



### 3.1.3 TDMA and Logical Channels

Many digital radio standards use a technique called Time Division Multiple Access (TDMA) to allow a radio channel to carry more than one call at the same time.



The physical channel is divided up into two or more logical channels using time slots. P25 phase 2 uses two time slots. The voice from one talker is converted to digital but the data is transmitted in only one of the time slots. At the receiving end the data is received in that time slot and the original voice is recreated. The other time slot (or logical channel) is still free to carry a different conversation. A call from another team can be allocated to the same physical channel but use the second time slot. The ability of each physical channel to be split into two logical channels doubles the capacity of the radio system to handle calls. Allowing a greater number of groups to share the radio network and all talk at the same time

### 3.1.4 Summary:

- A physical channel is a radio frequency allocated by the regulatory body.
- In P25 phase one a physical channel and a logical channel are the same.
- In P25 phase two a physical channel is divided into two time slots or logical channels.
- Each time slot can carry an independent call.
- This increases the capacity of the radio network.

## 3.2 P25 Channel Operation

This chapter is going to look at a number of aspects of P25 channel operation.

1. First we will review how a Analog FM radio channel works.
2. Then we will look at how a P25 Digital radio channel carries voice.
3. Finally we will look at how channel is allocated in a P25 trunked radio system.

### 3.2.1 FM Operation

Before explaining the operation of a P25 transmitter, this section provides a brief review of the operation of an FM radio system.

#### Block Diagram FM Transmitter

1. The user's speech and any background noise is picked up by the microphone.
2. It is amplified and filtered to pass only frequencies in the range 300Hz to 3kHz. This audioband contains all the frequencies required to understand human voice. The audio may also be pre-emphasized, which allows some of the noise picked up during transmission to be reduced by the receiver. Analog signaling, if used, is also added.
3. It is encoded onto an RF carrier. The encoding device is a voltage controlled oscillator and produces Frequency Modulation (FM). In FM, the carrier is deviated in relationship to the amplitude of the audio. The rate of deviation matches the frequency of the audio. A constant amplitude constant frequency audio signal (e.g. a whistle) will produce a waveform like the one shown below.
4. The frequency modulated signal is then amplified and transmitted.

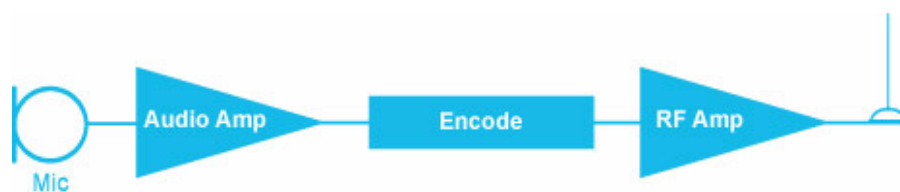
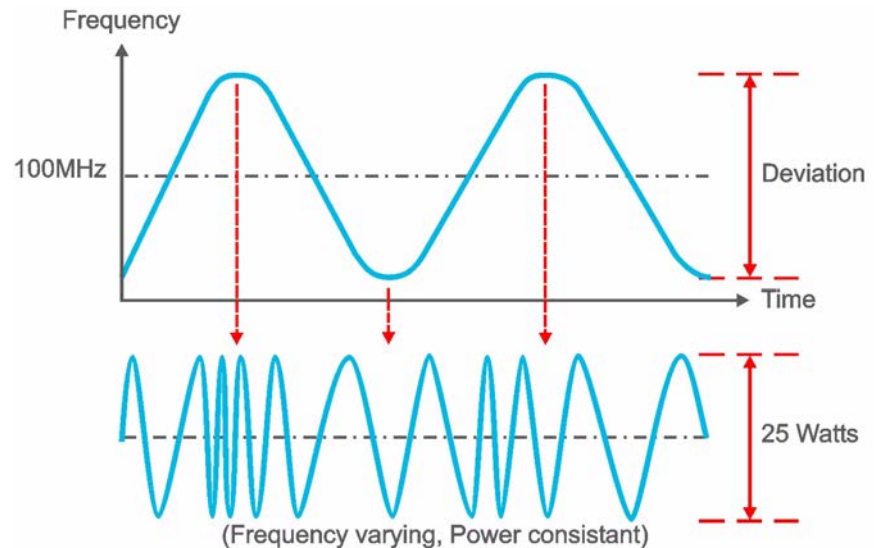


Figure 3.20 Simple FM transmitter





**Figure 3.21 FM modulation**

**Analog Signaling**

Analog conventional radios can send subaudible signaling to enable radio and base station receivers to discriminate between incoming calls. A receiver only unmutes to the calls intended for it.

This signaling can be sent as continuous sub-audible tones (CTCSS/PL) or as a constant stream of low speed data that is modulated onto the carrier using frequencies below the speech band (DCS/DPL). The tone/data is recognized by the radio equipment but filtered out before the audio is output via the speaker.

Signaling can also be used to identify radio users on the system. This signaling is typically sent as a burst of in-band tones (DTMF) or a burst of data (MDC1200) at the start or end of a transmission.

**Receiver Operation**

In an FM receiver, the FM signal that was transmitted (plus any noise picked up along the way) is converted back into analog audio and output via a speaker. De-emphasis can reduce some of the noise picked up during transmission but cannot remove it altogether.

If signaling is used, the radio receiver can be programmed to operate in different modes; the mode selection controls the operation of the receiver gate.

Monitor Mode:

- The receiver will unmute on any recognized signal.

Normal Squelch:

- The receiver unmutes only when the correct signaling is received.

These settings are preset in the radio, however typically the monitor function can be assigned to a function key on the radio.

### 3.2.2 P25 Phase 1 Operation

All P25 radios transmit and receive using the Common Air Interface (CAI). The CAI is a standard protocol for transmission and reception that ensures P25 radio equipment from different manufacturers will interoperate.

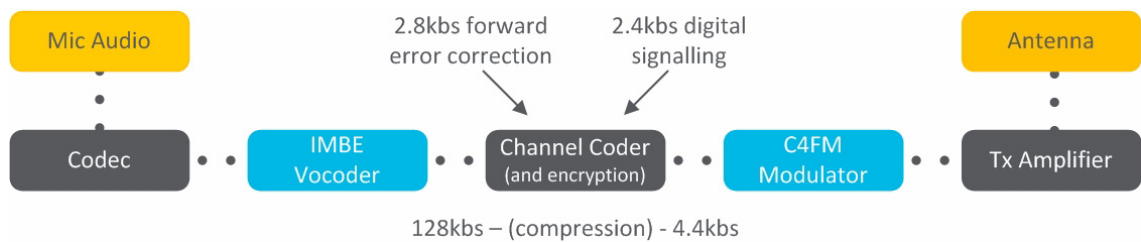
P25 radios will also operate in conventional analog mode, making them backwards compatible with existing analog radio systems. In analog mode, the P25 radio will operate exactly the same as an FM radio, with the capability for CTCSS (PL), DCS (DPL), pre-emphasis and de-emphasis, and wideband or narrowband operation. Many P25 radios offer many other advanced features in analog mode such as MDC1200 or DTMF ANI signaling.

In digital mode, the Common Air Interface offers a number of features that are direct replacements of features offered by analog FM radios. However, the CAI provides these features in a very different way. There are also a number of features specific to P25 operation.

This section will introduce the CAI and the basic operating blocks of P25 Phase 1 radio equipment and their functions. P25 Phase 2 is covered in other chapters.

#### Block Diagram of a P25 Transmitter

1. The microphone converts speech into an analog electrical signal.
2. The codec samples that signal and produces a stream of digital information. This information is coded at 128 kbits/s.
3. P25 uses a specific method of digitized voice (speech coding) called Improved Multi-Band Excitation (IMBE™). The IMBE™ voice encoder/decoder (vocoder) removes much of the background noise by encoding only characteristics that represent the sound of the human voice. This reduces the bit rate to 4.4 kbits/s.
4. To protect the voice signal from errors caused by fading and interference, 2.8 kbits/s of forward error correction (FEC) is added.
5. Signaling information is interwoven with the voice signal, adding a further 2.4 kbits/s.
6. The output of the vocoder may be encrypted. Then the signaling, voice and error correction is formatted into P25 Speech Frames.
7. A P25 modem modulates the carrier with this digital data, using the C4FM modulation scheme.



**Figure 3.22 P25 Phase 1 Transmitter block diagram**

**The Vocoder**

The vocoder is a device that compresses the digital information from the codec using mathematical algorithms. The P25 Phase 1 vocoder is the Improved Multi-Band Excitation (IMBE) vocoder that was developed by Digital Voice Systems, Inc. (DVSI). It reduces the bit rate of the voice information from 128 kbits/s to 4.4 kbits/s. The IMBE product is a model-based vocoder. This vocoder does not allow all input signals to be digitized to its output. Music will not be transmitted at all clearly and a steady state tone will warble and be unclear. The IMBE vocoder only digitizes the input sounds which it “thinks” are speech, thereby effectively filtering out other unwanted background sounds. This particular unit is used in all P25 transmitters and has been selected from competing products and after tests with different voices and background noises – e.g. sirens, gunshots, and traffic noise.

The P25 Phase 2 vocoder is the Advance Multi-Band Excitation (AMBE) vocoder and was also developed by DVSI. This Dual-Rate Vocoder retains the existing 7200 bps Full-Rate capability while adding a new 3600 bps Half-Rate capability. This provides essentially the same voice quality as Full-Rate while using only half the bit rate - facilitating a substantial increase in spectral efficiency.

- The vocoder reduces the bit rate of the voice information
- The vocoder removes much of the background noise

**Forward Error Correction**

To protect the voice signal from errors caused by fading and interference, forward error correction (FEC) is used.

FEC is additional data added to the transmission which enables the receiving radio to not only detect but correct for errors. This enables the audio quality to be maintained over the usable range of the system. Over 1/4 of the data transmitted by a P25 radio is for error correction.

However, there is a point at which the signal is so badly corrupted that the receiving radio is unable to correct for errors. This is typically when the error rate reaches 5 percent. Once the limit of error correction is reached, the quality of the audio signal degrades very rapidly and is quickly lost altogether.

**Digital Signaling**

The P25 CAI defines signaling information that is sent over the air along with voice. Because transmissions are digital, it is easy to add extra information such as the destination talkgroup, caller ID and Network Access Code (NAC). This signaling doesn't just appear at the beginning of

## Digital Signaling

The P25 CAI defines signaling information that is sent over the air along with voice. Because transmissions are digital, it is easy to add extra information such as the destination talkgroup, caller ID and Network Access Code (NAC). This signaling doesn't just appear at the beginning of the voice stream; it is interwoven with it, so that users can still join a call, even if they missed the beginning.

### Aggregate Data Rate

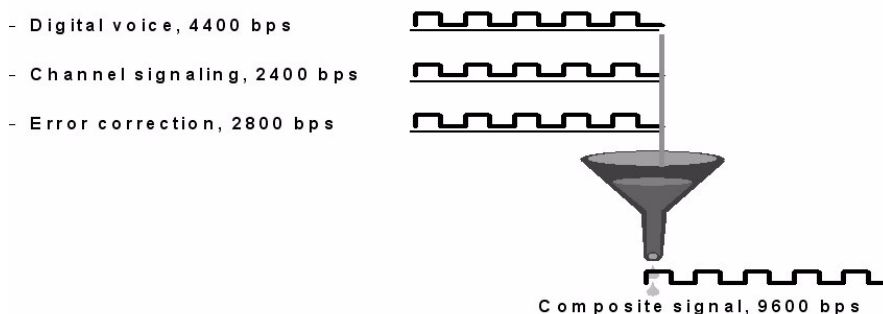


Figure 3.23 P25 composite signal

### Network Access Code

The Network Access Code (NAC) is a 12 bit number that ranges from hexadecimal \$000 to \$FFF and contains 4096 addresses.

A NAC is the digital equivalent to CTCSS (PL) or DCS (DPL).

It can be used as a means of selectively accessing the base station infrastructure. A NAC can specify a particular base station/repeater or a particular network. It then functions as a base station or network address. If the network is a TaitNet digital network, the NAC can specify a channel group within the network. When the NAC is used in this way, radios and the base station are all programmed with the same receive and transmit NAC. This prevents receivers unmuting to signals from other sources.

Alternatively, the NAC can be used to distinguish particular groups of users. It then functions as a talkgroup ID. Each group of radios is given a particular NAC (generally the same one for transmitting and receiving). The base station infrastructure is configured so that it receives any NAC and retransmits the NAC that it received.

There are two special NAC codes:

- \$F7E - tells the base station receiver to unmute when a digital signal with any NAC is detected.
- \$F7F - does the same, but also tells the base station to use the NAC of the received signal when re-transmitting (rather than the preprogrammed transmit NAC code for the channel).

## Individual ID

Every SU on a P25 system has a Unit ID.

The Unit ID is a 24 bit address (hexadecimal \$000000 to \$FFFFFF) allowing up to 16,777,216 individual IDs. However, some of the IDs are reserved for special functions. Typically, individual radios are numbered from Unit 1 to Unit 9,999,999.

This is transmitted when a call is made and can be used by the receiving radio to show the caller ID.

An individual call to another radio unit is made by including that radio's individual ID as the destination ID.

## Talk Group ID

A talk group is a group of radios that are required to operate together. Talk group numbers have a 16 bit number that ranges from hexadecimal \$0000 to \$FFFF and contains 65,536 addresses.

A talkgroup ID can be sent in place of an individual address.

## All Inform ID

It is possible to operate a P25 system without talk groups and allow everyone to hear all the calls. However, if talk groups are used and a message must be sent to all the talk groups, a special talk group ID \$FFFF (65535) can be used. This is a call to everyone on the system and its use is often restricted to dispatchers.

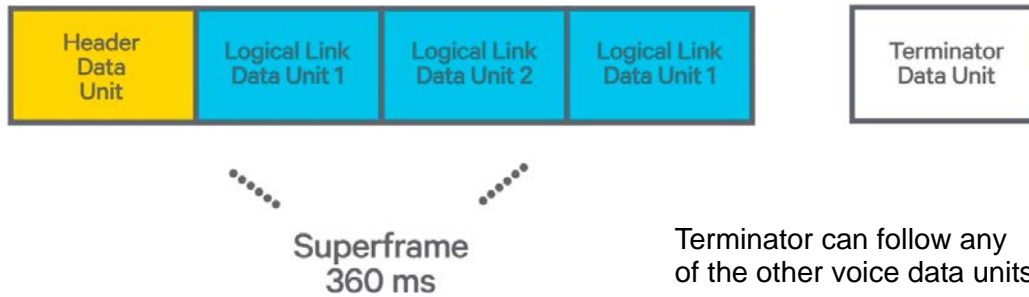
## Other Signaling Information

The CAI specifies a wide range of other signaling information that can be sent along with the voice. Some examples include:

- Emergency Indicator
- Encryption Sync
- Manufacturer ID
- Status Messages
- Status Symbols

### Structure of P25 Speech Frames

An over (part of a conversation that begins when the user presses PTT and ends when he/she releases it) starts with a header data unit, continues with a series of "logical link data units" (LDU) that carry the digital speech, and ends with a Terminator Data Unit.



**Figure 3.24 CAI packet configuration**

There are two types of LDU: LDU1 and LDU2. The two together are referred to as a superframe.

The header data unit contains:

- Frame synchronization information
- Network Identifier (NID), containing the Network Access Code and the Data Unit Identifier (indicates what type of data follows)
- The ID of the talk group that the caller belongs to
- Encryption information
- Manufacturer's ID, which enables systems to implement special features specific to one manufacturer

LDUs (both LDU1s and LDU2s) contain:

- Frame synchronization
- NID
- 9 voice codewords (IMBE frames)
- Status symbols, which indicate whether the channel is busy, idle, or unknown

The terminator data unit contains frame synchronization and the Network ID. It signifies the end of the message.

**C4FM Modulation**

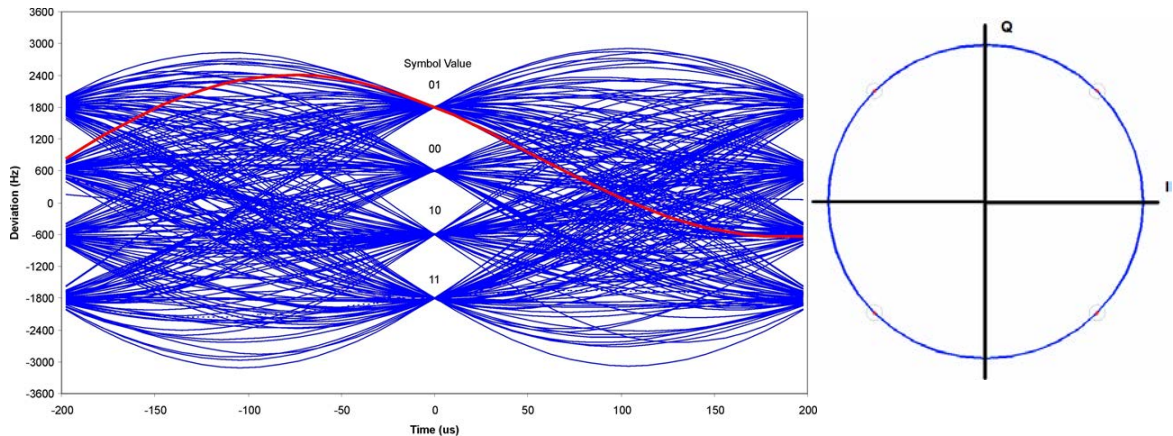
The APCO P25 Phase 1 standard mandates the C4FM modulation scheme. In the C4FM modulation scheme, each set of two bits (dibit) is represented as a fixed deviation from the transmit frequency.

Information	Frequency deviation
01	+1.8 kHz
00	+0.6 kHz
10	-0.6 kHz
11	-1.8 kHz

The APCO P25 Phase 1 standard mandates the transmission of the data at 9.6 kbs. There are 2 bits per baud (or symbol) this means the symbol rate is 4800 symbols per second and that the receiver must be able to detect a symbol every 208 microseconds. A synchronization sequence built into P25 transmissions allow the receiver and transmitter to synchronize. Every

208us a the deviation from the P25 transmitter must be at the correct deviation level to represent a dibit of data to the receiver. The transmitter then has 200us to change the deviation to represent next dibit before the receiver decodes the next symbol.

One way to represent this is with an Eye Diagram. By repeatedly plotting the changes in deviation over time it can be seen that every 208us the repeated traces pass through the same four positions, representing the different dibits. This results in an eye-shaped hole among the various traces.:



**Figure 3.25 C4FM eye diagram and constellation diagram**

The RF output of digital C4FM, like that of analog FM, has a constant amplitude. This can be represented by a Constellation Diagram. The red dots represent the 4 symbol positions. Since the amplitude does not change during the transitions the constellation diagram looks like a circle.

A Nyquist filter is used to minimize interference between symbols and the shaping filter helps to make the signal immune to noise on the channel (to improve performance, like the pre-and de-emphasis on analog FM).

### **P25 Reception**

Receiving a P25 signal is the reverse of the transmit procedure. The radio demodulates the signal, corrects any errors, and extracts the signaling. The vocoder and the codec then reconstruct the analog voice signal from the digital data.

The radio receiver can be programmed to operate in different modes; the mode selection controls the operation of the receiver gate.

Monitor:

- The receiver will unmute on any recognized voice signal.

Normal Squelch:

- The receiver unmutes only when the correct NAC is received.

Selective squelch:

- Requires that the destination address and the NAC are correct before the receiver will unmute.

These settings are preset in the radio, however the monitor function can be assigned to a function key on the radio.

#### Voice Delay

Encoding analog voice into digital and back to analog again does introduce a delay. Limits for end-to-end delays are recommended in the P25 Standard:

- Direct simplex delay = 250ms (mic-speaker)
- Via repeater = 350ms
- Via network = 500ms

### 3.2.3 Trunked System

Both the examples above looked at how an over (part of a conversation that begins when the user presses PTT and ends when he/she releases it) occurs on a conventional channel. On a trunked system there are a number of additional steps before an over can take place.

#### The Control Channel

A trunked radio system has a number of traffic channels, used for voice communication, and a control channel. The control channel is used to send messages between the Fixed Network Equipment (FNE) and the SUs. In P25, these messages are called Trunked Signaling Blocks (TSBKs).

There are two types of TSBK:

- An Inbound Signaling Packet (ISP) is sent from the SU to the system.
- An Outbound Signaling Packet (OSP) is sent from the system to the SU.

The control channel at each site is constantly active sending out OSPs. When not setting up calls, these OSPs identify the system to allow network Acquisition and roaming to take place.

#### Network Acquisition

Before a SU can operate, it must find the control channel and get permission from the system to operate. This takes place in four stages:

- Hunting
- Acquisition
- Registration
- Group affiliation

#### Hunting

When an SU is turned on, after completing its power-on self test, the SU then starts the process of finding a trunking system. The first step in the process is called “Hunting”. The purpose of the hunt is to locate a control channel.



To decrease the hunting time, the SU is programmed with a list of possible control channels. When the SU is turned on, if the SU has used the network before, the SU will first check the last control channel it was on. If that channel is not found or the first time a SU is used, it will go through a full hunt (all programmed control channel frequencies) looking for a local control channel.

Hunting is also used once the SU has successfully acquired the trunking system. The SU continues to hunt for better sites as the subscriber roams around the network. This is covered in the roaming section.

## **Acquisition**

The SU does not make any transmissions on a control channel until it is validated. It validates a control channel by listening to the messages from the system for the WACN and System ID.

The SU may be in an area that has coverage from two or more sites and more than one control channel may be found during the hunt. The SU uses RSSI to rank channel quality and begins by validating the strongest signal. Once the best control channel has been acquired, the SU attempts to register with the network.

## **Registration**

After successful completion of the hunting and acquisition (validation) process, the SU now has to apply for registration.

When the SU sends a Unit Registration Request to the site, it is applying for permission to operate. This request is processed by the Site Controller and the RFSS controller.

- If the radio is validated on the trunking system, the SU will receive an Accepted Unit Registration Response message and its Working Unit IDentity (WUID). The SU can now proceed with the Group Affiliation process.
- If the SU is not validated on the trunking system, a deny message is sent back and the SU continues to hunt.

The process described above is a Full Registration used during network acquisition. The Roaming section describes a location registration (or location update) that occurs whenever an SU wants to move onto another site within an RFSS.

## **Group Affiliation**

The SU is now registered with the trunked network but is not yet part of a talkgroup with other subscribers. The SU may be programmed to start-up on a default group, the last used group or the group that indicated by a selector switch on the radio. However, the SU has to inform the trunked system which group has been selected.

During this process, the SU sends a Group Affiliation Request to the site. This request is processed by the Site Controller and the RFSS controller.

- If the affiliation request is successful, the SU will receive its Working Group IDentity (WGID) and Announcement Group ID (AGID) and can now make and receive calls. Depending on the SU configuration, the display may show the group name and / or number and the site information.
- If affiliation is unsuccessful (perhaps the group is not permitted to be used in that location), the radio will not be able to operate on the selected talkgroup in that location. Typical SU behavior is to display a message such as “No Service” and begin hunting again.

The Group Affiliation message is used to update the RFSS database, meaning that the site which the SU has registered on must now be included whenever a call is made to that group even if the call begins on another site in the network.

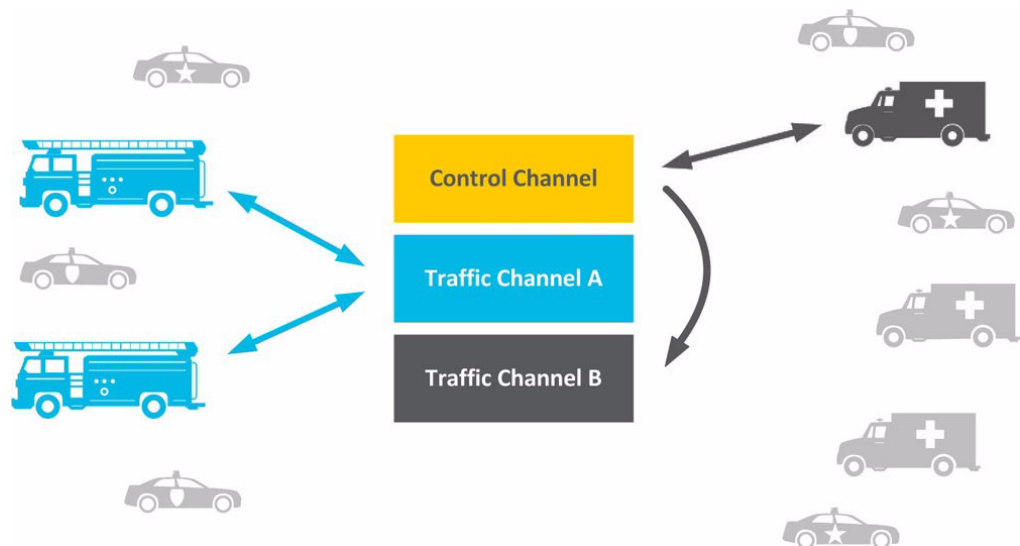
The user interface on the SU can be used to select a different talkgroup. Every time this is done, a new group affiliation request is sent to the site.

### **3.2.4 Traffic Channel Access Methods**

When you press your microphone PTT (Press To Talk) button, your SU sends an ISP (Inbound Signaling Packet) message to the trunking system’s control channel at the site. The Site Controller locates an idle Traffic Channel within its pool of channels and transmits an OSP (Outbound Signaling Packet) via the control channel that directs your SU and any other SU associated with your talkgroup to change to the selected available idle traffic channel.

The details of the channel access procedure differ for different call types and different system configurations.

- Transmission Trunking
- Message Trunking



**Figure 3.26 Traffic channel access**

**Transmission Trunking**

In Transmission Trunking, a channel is allocated for each PTT press. At the end of the PTT, the call is finished, and the traffic channel goes back into the pool.

The benefit of this system is that the channel is immediately available for another call. The disadvantage is that on a very busy system, there may be a queue of people waiting for channels. A subscriber who has an important reply to the transmission will be placed at the end of the queue and could have a long delay before a channel is available for their reply.

**Message Trunking**

In message trunking, a traffic channel is allocated for the entire conversation, even if there are multiple transmissions. To do this, message trunking uses a hang timer to reserve the traffic channel to ensure it is available for a reply. For group calls, the hang time is typically 2 or 5 seconds. After the initial transmission, all the members of a group remain on the traffic channel until the hang timer expires. If no one replies, the hang timer will expire and the traffic channel goes back into the pool. However, if, before the hang time expires, someone wishes to reply, then the channel will be available. For individual calls, the hang time is typically much longer, and calls are ended by pressing a call clear button, but an inactivity timer will also clear down the call if no further transmissions are made in a preset time.

**Call Continuation**

There are two methods of call continuation that can be used within the hang time for message trunking. The method used depends on the SU.

**Control Channel Method**

A reply is not immediately made on the traffic channel, instead the SU first sends a new request to the control channel and waits to be sent back to the same traffic channel. The benefit of this is:

- Each SU is validated before activity occurs on the traffic channel.
- Call records identify each SU involved in the conversation.
- In a multi-site system, if multiple radios attempt to reply, there is

a clean mechanism to establish who will transmit. Normally, the first SU will get the channel unless the other unit has a higher priority.

**Direct Method**

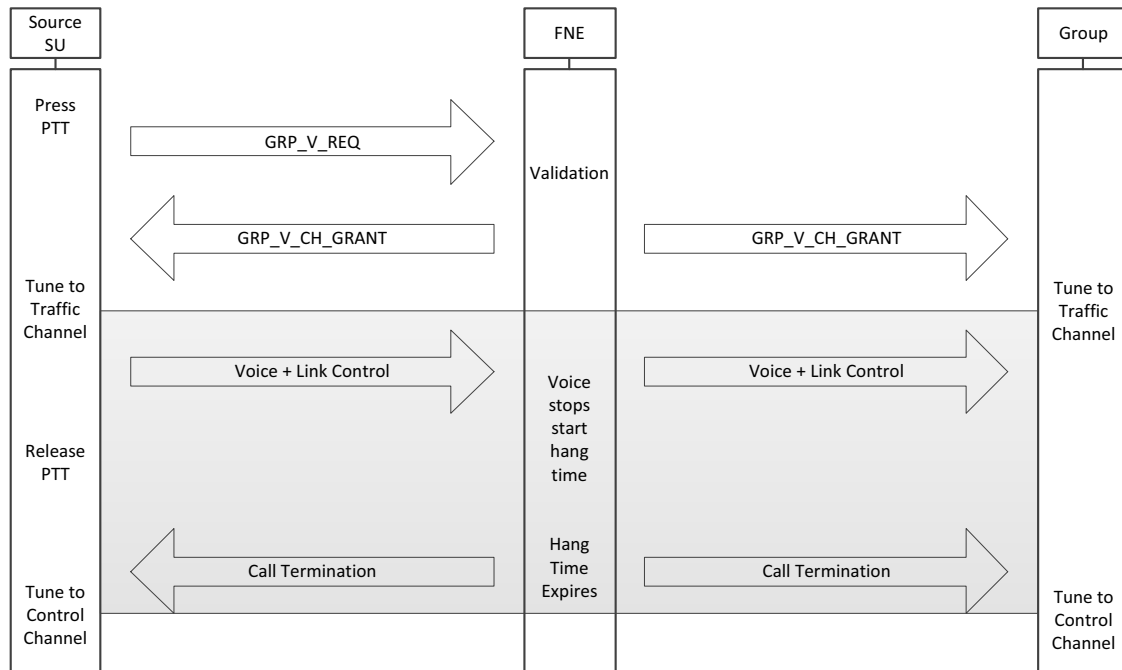
The SUs do not need to return to the control channel between each transmission on the traffic channel.

**Unit to Group Voice Call Example**

This example shows a group call using message trunking with a hang time and the control channel access method.

**How it works**

- The Source SU requests a call to the Destination talk group via the Control Channel.
- The Control Channel passes the request via the Site Controller to the RFSS for call validation. The call Validation includes:
  - SU Validation
  - Talkgroup Validation
  - Coverage Validation
- If the validation is successful, a traffic channel is allocated to the call and a Channel Grant message is sent out to the group.
- At the end of the first over, the hang time starts.
- Every time any SU wants to talk, the radio sends a “Group Voice Request” to the control channel. The control channel passes the request to the Site Controller to the RFSS to validate the calling SU.
- If there is no SU currently transmitting, the SU receives a Group Voice Channel Grant message, the SU then tunes back to the traffic and transmits.
- When no further “Group Voice Request” messages are received, the hang time times out and the call is cleared down.



**Figure 3.27 Group call sequence diagram**

## Unit to Unit Voice Call Example

This example shows a unit to unit call using message trunking with a hang time and direct access method.

The process for initiating an individual call from the SU user interface depends on how the radio is programmed. The information describes how the channel is allocated after the subscriber requests an individual call.

### How it works

- The source SU1 requests a call to the destination SU2 via the Control Channel.
- The Control Channel passes the request via the Site Controller to the RFSS for call validation. The call validation includes:
  - Source SU validation
  - Destination SU validation
- If the validation is successful, the destination SU is contacted and the SU rings.
- The destination subscriber then must accept the call.
- Once the call is accepted, a traffic channel is allocated to the call.
- The subscribers can make multiple transmissions on the traffic channel without going back to the control channel.
- Once the entire conversation is complete, the channel is cleared down. This can be initiated in two ways:
  - By one of the subscribers pressing a call-end button, or
  - Waiting for the inactivity timer to expire.

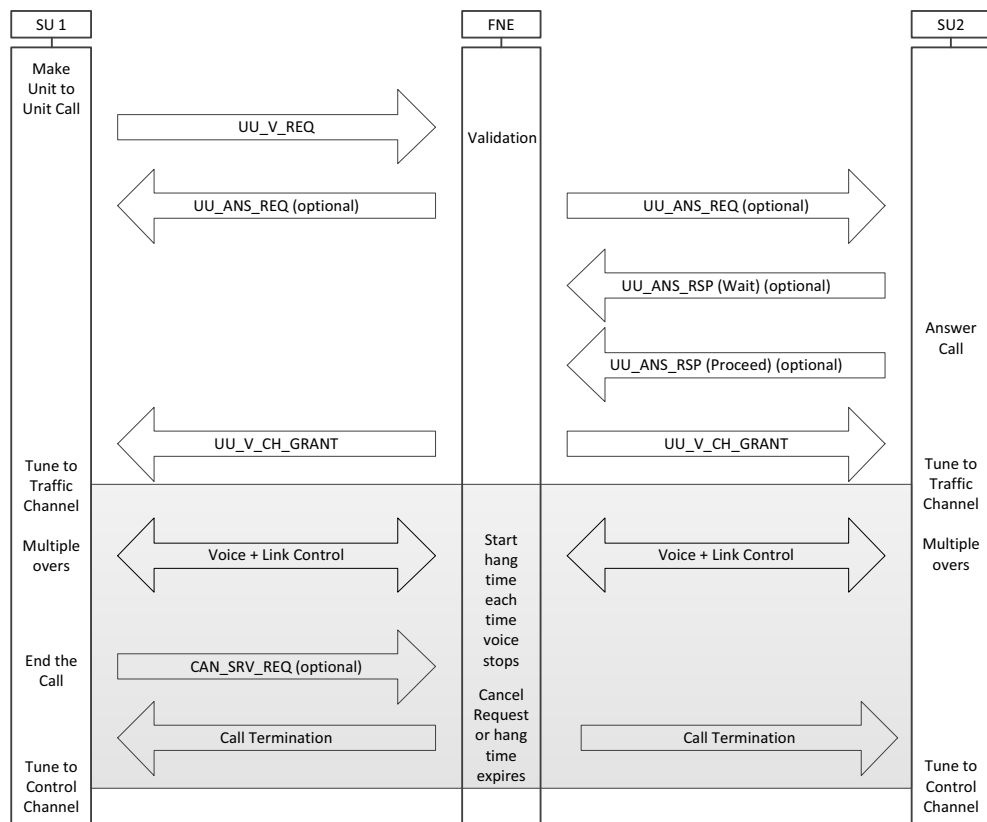


Figure 3.28 Unit to unit call sequence diagram

## 3.3 Channel Configuration

This chapter looks at how units and groups are numbered in a P25 radio system (conventional or trunked). Then reviews how a P25 trunked network is identified and how radio channels are addressed on a trunked system.

### 3.3.1 Unit Numbering

A SU may be either a radio (portable, mobile or fixed station) or a wireline dispatcher. Every SU on a P25 system (conventional or trunked) has a Unit ID. The Unit ID is a 24 bit address (hexadecimal \$000000 to \$FFFFFF) allowing up to 16,777,216 individual IDs. Some of the IDs are reserved for special functions - such as identifying the trunked system so typically individual radios are numbered from Unit 1 to Unit 9999999 (allowing up to 7 digit unit IDs to be allocated). This ID number is transmitted when a call is made and can be used by the receiving radio to show the caller ID. An individual call to another radio unit is made by including the called radio's individual ID as the destination ID.

Often the an agency will allocate blocks of IDs using a logical grouping. For example if 5 digit IDs are used all the first digit may identify the team of group. The second digit whether the ID is used by a mobile of portable and the last 3 digits are then used to identify individual units in that team.

On a trunked network each SU has a Subscriber Unit ID (SUID), that includes the Unit ID and the ID of the trunked system it is registered on. This allows for the calls to be made between trunked systems. The SUID is made up as follows:

Home System WACN ID (20bit) - Home System ID (12bit) - Unit ID (24 bit)

Within a Registration Area, a SU is allocated a unique abbreviated address known as the Working Unit ID (WUID). On the unit's home system, this is typically the Unit ID. If they are a guest on another RFSS, it may be an alias. The SU initiates and responds to messages addressed to its WUID.

The following WUIDs are defined:

- \$000000 No Unit
- \$000001 - \$FFFFFFB Assignable
- \$FFFFFFC Reserved for system operator functions
- \$FFFFFFD Reserved for the system call processing functions
- \$FFFFFFE Reserved for registration
- \$FFFFFFF All Units

### 3.3.2 Group Addressing Scheme

P25 allows for group calls to be made to a team of people. This is achieved by addressing the call to a talk group. Talk group numbers have a 16 bit number that ranges from hexadecimal \$0000 to \$FFFF and contains 65,535 addresses. The address FFFF (or 65535 in decimal) is a special all call address that will call all other groups. Trunked systems also allow announcement groups to be defined this is a group address that is made up of a number of smaller groups. Unlike some other radio standards the P25 unit and group number ranges are independent - you can have both a unit 1 and a group 1.

On a trunked network each group has a unique Subscriber Group ID (SGID) that includes the Group ID and the ID of the trunked system the group is declared on (the home system for that group). This allows for the calls to be made between trunked systems. The SGID is made up as follows:

Home System WACN ID (20bit) - Home System ID (12bit) - Group ID (16bit)

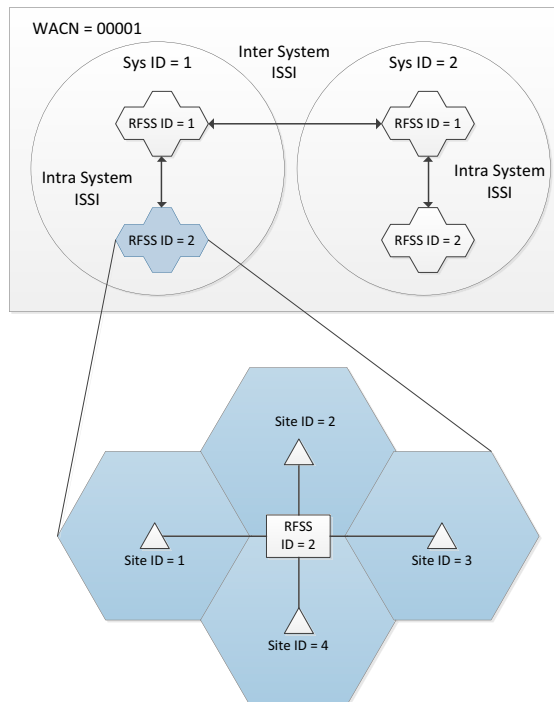
Within a system, an SGID is assigned a unique abbreviated address known as the Working Group ID (WGID). On the home system, this is typically the Group ID. If they are a guest on another RFSS, it may be an alias. The SU initiates and responds to messages addressed to its WGID.

The following WGID are defined:

- \$0000 Null Group
- \$0001 - \$FFFE Assignable Groups
- \$FFFF All Groups

### 3.3.3 Trunked P25 System Numbering

A P25 trunked Radio Frequency Sub System (RFSS) could have many sites. SUs can roam to different sites connected to a single RFSS; this ensures they always use the best site for communication. If necessary, Talkgroups can be restricted to specific sites to restrict the geographic coverage area of that group. RFSSs in different locations can be joined together using the Inter RF Sub System Interface (ISSI) to form wide area networks. It is also possible for more than one organization to install a P25 trunked RFSS in the same area. A SU may or may not be permitted to roam from one RFSS to another. Therefore, it is important that the SUs can identify which system a control channel belongs to. To allow this to occur, the control channel is constantly sending messages that identify the site and the system. The SUs use these messages to identify a system, find new sites as the subscriber moves around, and to synchronize with the control channel when they move to a new site. P25 systems and sites within that system are identified using four parameters defined below. The TIA states that a Land Mobile Radio (LMR) system is uniquely identified by its WACN and system ID. There is a document on the TIA web site "WACNguide010406.doc" that provides non-binding guidelines for the assignment of WACN and system identities.



**Figure 3.29 System identification**

1. Wide Area Communication Network address
  - (WACN) 20 bits
  - \$00001 to \$FFFFE
  - 1 to 1,048,574 Networks
2. System Identity
  - 12 bits
  - \$001 to \$FFE
  - 1 to 4094 Systems
3. RFSS Identity
  - 8 bits
  - \$00 to \$FE or
  - 1 to 254 RFSS
4. Site Identity
  - 8 bits
  - \$00 to \$FE
  - 1 to 254 Sites

**i** ISSI may be used between two RFSSs within an LMR system or between two LMR systems. Where a distinction has to be made, this document uses the term Intra-System to refer to RFSSs with the same system ID, and Inter-System to refer to RFSSs with a different System ID.

**Broadcast Messages**

There are several different types of TSBK messages that are transmitted from the Fixed Network Equipment (FNE) via the control channel to identify the system.

Network Status Broadcast (NET\_STS\_BCST) message

- The Network WACN ID + The System ID

RFSS Status Broadcast (RFSS\_STS\_BCST) message

- The System ID + RFSS ID + Site ID

**3.3.4 Network Access Code (NAC)**

The NAC code is used in both conventional and trunked systems. The Network Access Code (NAC) is a 12 bit number that ranges from hexadecimal \$000 to \$FFF and contains 4096 addresses.

**Conventional NAC Use**

In a conventional system it is programmed in both the mobile and portable radios and in the repeater and can be used as a means of selectively



accessing the base station infrastructure providing a function very much like the that provided by a Sub-audible Tone in analog systems. A typical use in a wide area conventional system is to provide increased protection from undesired co-channel interference. This can occur when there are a limited number of frequencies available and the same frequency is being used at two sites. This is acceptable providing there is enough separation between the sites that the coverage does not overlap. However because of terrain variation and the fact that mobile and portable radio users move around there is still a risk that at some point a mobile or portable radio intending to talk on one repeater is picked up by the other repeater. If a different NAC code is programmed into each repeater it prevents the repeater from keying up on transmissions that do not have the same NAC.

### **Trunked System NAC Use**

This same ability to provide increased protection from undesired co-channel interference also applies to trunked systems. The Network Access Code is used for both trunked traffic and control channels. The NAC field contains a 12 bit value but in trunking there is a relationship between the NAC and the System ID..

- Eight of these bits derive from the upper 8 bits of the trunked system ID and are common to all sites throughout the entire system. For example, if the System ID is 3B5 in hexadecimal, all the NACs at all sites will begin with 3B.
- The remaining four bits of the NAC (called the Access Code Index or ACI) are then configured on a per-site/per-simulcast-subsystem basis by the system installers to provide interference protection between sites.

### **3.3.5 Channel Addressing**

In a conventional radio system mobile and portable radios are pre-programmed with the channels they can use. The channel for communication is selected by the user of the radio. If a new channel is to be added to the network the mobile and portable radios must be reprogrammed with this channel so the radio users can access it.

In a trunked network a pool of channels is available at each site that the network can allocate for calls. The available channels can change over time as the system grows and expands. Rather than reprogram all the SUs each time a channel is added to the network the mobile and portable radios are simply programed with one or more channel plans from which the frequency all available and future channels can be calculated. When a trunked radio requests a call the system responds with the channel plan and channel number to use for the call and the SU then calculates the Tx and Rx frequencies to use.

#### **Trunked Channel Plan**

The RF spectrum is broken up into ranges or blocks. Each block is given an ID and defines set of continuous channels with common parameters.

This is called a Channel Identifier, or also commonly called a Frequency Plan. The parameters are named from the perspective of the SU. This means that the same names are used for the same parameters irrespective of whether they are being programmed into an SU or an RFSS controller. Up to 16 channel plans can be defined. Each channel plan can address 4000 unique channels. If a 12.5kHz channel spacing was used, one plan would cover a 50MHz span of frequencies.

A channel plan includes:

- ID: A unique identifier for the parameter set.
- Bandwidth: The bandwidth of the channel (normally 12.5 kHz).
- Transmit offset sign: Indicates whether the transmit (inbound) frequency is offset positively or negatively from the receive (outbound) frequency.
- Transmit offset: The size of the offset in MHz. The transmit offset is the amount that the SU's transmit frequency (base station's receive frequency) is offset from the SU's receive frequency (base station's transmit frequency).
- Channel spacing: The spacing in kHz between one channel and the next.
- Base frequency: The frequency channel 0 of this frequency plan. This is the SU receive frequency (the base station transmit frequency).

ID	Base	Bandwidth	Spacing	Sign	Offset
1	462.5MHz	12.5kHz	6.25kHz	+	5.1875MHz

Figure 3.30 Example channel plan

**Channel Identifier Update (IDEN\_UP)**

Channel Identifier information is programmed into the RFSS and into the SUs. In addition, the RFSS shall periodically generate IDEN\_UP or IDEN\_UP\_VU messages informing the SUs of the channel characteristics to associate with a specified channel identifier value. This means SUs can learn new channel plans even if they were not originally programmed with this information.

- The IDEN\_UP message are recommended for use in the 700 and 800 MHz bands (fixed Rx/Tx offset).
- The IDEN\_UP\_VU message is used for Base Frequencies in the VHF and UHF bands, 136 MHz to 172 MHz and 380 MHz to 512 MHz.

**Using a Channel Plan**

A trunked system may only use a small number of the channels that could be addressed by the channel plan, but all control and traffic channels in the P25 trunked system must be able to be addressed using a channel plan.

ID	Base	Bandwidth	Spacing	Sign	Offset
1	462.5MHz	12.5kHz	6.25kHz	+	5.1875MHz

Channel Number	SU Rx	SU Tx	Used Channels
0	462.50000	467.68750	
1	462.50625	467.69375	
2	462.51250	467.70000	
...	...	...	
77	462.98125	468.16875	
78	462.98750	468.17500	
79	462.99375	468.18125	CCH
80	463.00000	468.18750	
81	463.00625	468.19375	
...	...	...	
151	463.44375	468.63125	
152	463.45000	468.63750	
153	463.45625	468.64375	TCH1
154	463.46250	468.65000	
155	463.46875	468.65625	
...	...	...	
233	463.95625	469.14375	
234	463.96250	469.15000	
235	463.96875	469.15625	TCH2
236	463.97500	469.16250	
237	463.98125	469.16875	
...	...	...	
309	464.43125	469.61875	
310	464.43750	469.62500	
311	464.44375	469.63125	TCH3
312	464.45000	469.63750	
313	464.45625	469.64375	
...	...	...	

**Figure 3.31 Four channels addressed using the example channel plan**

The repeater equipment at the site is programmed with the correct frequency information based on the licensed frequencies allocated to the trunked system. The RFSS, site controllers and SUs are programmed with the channel plan and can refer to each RF channel simply by using the Channel Identifier and Channel Number. This makes over the air messaging more efficient. This also means a new channel or site can be added to the trunked network and SUs do not need to be reprogrammed.

**Implicit and Explicit Addressing**

When a subscriber pushes the Press To Talk button on their SU a group voice request is sent to the control channel at the site. The site then responds with the channel to use for the call from the channel plan. There are two ways traffic channel frequencies can be identified:

- Group Voice Channel Grant - Short Channel Form (Implicit) is the standard packet format used in a Channel Grant message for a voice call. A channel (receive and transmit) is addressed by referring to a Channel Identifier and a Channel Number.
- Group Voice Channel Grant - Explicit Channel Form is the packet format when an explicit designation for the transmit and receive frequency values is required (no fixed offset between transmit and receive). A channel (receive and transmit) is addressed by separately referring to a Channel Identifier and a Channel Number for Transmit and a Channel Identifier and a Channel Number for Receive.



# 4 Call Types and Features

## 4.1 Voice Calls

This section looks at the typical voice call types on a P25 network. Many call types apply to both conventional and trunked networks.

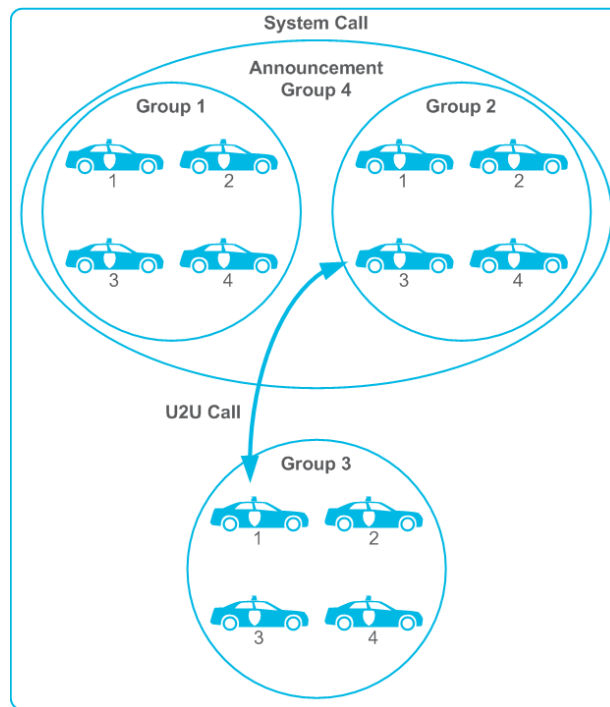


Figure 4.32 Voice calls

### 4.1.1 Talkgroup Call

In a P25 system, departments are able to form communication groups called “talkgroups”. The talkgroup call is the primary voice communication level in a P25 system, as the majority of conversations take place within a talkgroup. Only those SUs that are programmed to use a particular talkgroup can communicate with other members of the same talkgroup. SUs are capable of being programmed with multiple talkgroups.

In a trunked system talkgroup calls provide the effect of a “dedicated channel” for the duration of the SU call. Therefore, in a shared infrastructure environment, talkgroups enable users to maintain “partitioned” communications within their department talkgroup and still share the infrastructure with other departments and communicate with different teams by selecting different talkgroups.

Most conventional systems simply use a different channel for each group. However it is possible to configure multiple talk groups to share a single conventional channel.

#### **4.1.2 Announcement Group Call**

In a P25 trunked system, an announcement group call is a predefined amalgamation of different talkgroups into a single group call. This ability is controlled by the system manager.

This allows important messages to get out to multiple teams in one transmission rather than having to be repeated multiple times.

#### **4.1.3 System Call**

The system call is a call that reaches the broadest audience possible. When a system call is made, it will be received by all SUs and consoles registered on the system.

A use for this call may be an evacuation message for a work site in an emergency.

#### **4.1.4 Unit to Unit Call**

The unit to unit call or private call allows SUs to selectively call another individual user or the console (and vice versa) in the system and communicate “privately”. The user must switch the SU into Private Call mode and enter the ID of the unit being called to initiate this type of call. This feature is under the control of the system administrator, thereby limiting this feature to only those SUs they wish to have this capability.

#### **4.1.5 Emergency Call**


Emergency Call/Alarm provides users with the ability to inform dispatch personnel and other members of their group of a life-threatening situation. By depressing the SU’s Emergency Alarm button, an alarm is sent to the dispatcher and the voice call is flagged as an emergency call.

In a conventional system this can take place on the current channel that was being used for communication or the radio can be programmed to switch to a separate channel used for emergency calls.

In a trunked system the emergency alert is sent to the dispatcher via the control channel. The dispatcher can be immediately notified of the emergency status by an audible alert and visual display of the emergency caller’s ID at the console, or by a display of the unit alias. This sequence will take place even if all voice channels are temporarily busy, providing

immediate notification of the emergency situation at the dispatch center. Upon activation of the emergency SU's status, the emergency unit will be assigned the highest priority level for voice channel access regardless of how many units are already in queue. If all voice channels are occupied when an emergency call is made, then the unit initiating the emergency will be given priority access to the system. Some trunked systems allow this priority access to be configured in two ways:

- **Top of the Queue:** The SU that initiates an Emergency call will be placed at the top of the busy queue list, regardless of how many units are already in the queue and allowed access to the next available channel.
- **Pre-emption:** Instead of waiting for the next available channel, the system pre-empts the voice channel of the lowest priority call and assigns it immediately to the emergency call. Note: If all the channels are busy with ongoing uplink activity some trunked systems will place the call at the top of the queue until the unit that is transmitting de-keys before assigning the channel. This is in order to avoid conflict between two transmitting SUs on a pre-empted channel.

 In P25 Phase 2 the use of two time slots allows for a feature called Slow Associated Control Channel. This means if there is an emergency call or the dispatcher wants to pre-empt the call, the signaling can tell a radio that is not in emergency mode to stop transmitting to make the channel available for the emergency call.

#### 4.1.6 Telephone-to-Radio Call

In networks with a PSTN gateway, telephone users can call radios and talkgroups. The telephone user dials the telephone number of the gateway and then overdials the number of an individual SU or group. The PSTN gateway receives the overdialed string and then communicates with the RFSS controller to set up the call to that SU or group. The network administrator can specify whether an SU is permitted to receive telephone calls.

#### 4.1.7 Radio-to-Telephone Call

To call a telephone, the SU user simply selects telephone call from the menu and then dials the telephone number. If the PSTN gateway is connected to a PBX, that number can simply be the phone's extension number. SUs can be programmed with a list of numbers or names, so that the SU user can select one from the list.

When the RFSS controller receives the string, it communicates with the PSTN gateway to set up the call to that telephone number. If one line is busy, the FXO card in the router makes another available. The network administrator can specify whether an SU is permitted to make telephone calls.

## 4.2 Data Calls

In addition to voice calls the P25 network supports a wide range of data calls. This section lists just a few of the key data and other features supported by P25 in addition to voice calling. Many of these features are intended to replace existing features used by public safety on analog radio networks allowing an easy migration to P25. Other features are new enhancements that could be used to improve operations or management of the radio network.

### 4.2.1 Status Messages

Status messages have been used in radio communications for many years and P25 supports the use of status messages. A pre-programmed list of messages is configured in the radio units and the dispatch console. Rather than sending a voice call update the status of a job a message can quickly be sent. On a trunked system this takes place on the control channel and does not use any traffic channel resources.

Status messages work well for teams that have a standard set of situation updates that have to be reported. For example when a call out is made they may always have to update that they have left the station, and again once they are on site, and again when the job is complete. Or they can be used for features such as sending a call me back request to a dispatcher

The status message can be sent from the radio directly but in many cases the sending of status messages is integrated into a control console in the vehicle. The P25 standard also allows for a radio or dispatcher to query the status of another radio

### 4.2.2 Packet Data

P25 also supports Packet Data calls. Instead of the P25 radio channel carrying packets of digital voice it can carry packets of data from applications inside the radio or devices connected to the radio. A typical way of using this ability is IP packet data where the P25 radio is given an IP address just like a PC on a computer network. The dispatch or comms center can then have IP connected data applications that can send or receive data to unit in the field. There are a few standard applications defined that allow multiple radio manufacturers to support the same service. There is also scope to create a wide range of custom applications to meet the specific operational requirements of an organization.

#### GPS Location Updates

One of the standard applications for data is location updates using GPS.

Identifying where radio users are can be essential safety feature when working in life threatening situations. It can also be a valuable time and money saver in commercial applications.



Many P25 radios available today have GPS build in and enabling location updates may simply be a software feature. There is then a wide range of Automatic Vehicle Location (AVL) applications available. These can be chosen to suit the application whether that be sending updates to a central comms center or sending a location update as part of an emergency call to a command vehicle.

#### **Over The Air Rekeying (OTAR)**

Encryption is an important feature of P25. One of the problems with encryption is how to update the key in a fleet of radios. A small tactical team can come together at the start of an operation and load a key with a cable connected key loader but if a fleet of hundreds of radios is to be updated it can be very difficult to physically touch each radio with a keyloader. Over the Air Rekeying or OTAR provides a secure way of sending out new encryption keys over the air. This makes it easier to implement a key management plan that requires the updating of encryption keys on a regular basis or the rapid replacement of a key if a radio has been lost or stolen to be achieved.

#### **Over The Air Programming (OTAP)**

Another feature provided by some P25 radios using Packet Data is the ability to reprogram them over the air. Over The Air reprogramming (OTAP) is a powerful way to manage a large fleet of radios. If a new group, channel or feature is added to the network all the deployed radios can be reprogrammed remotely. Rather than having to bring all the radios in for programming or send someone out to reprogram all the portables or mobiles.

### **4.2.3 Radio Check**

This is used by a dispatcher to check that a SU is available on the network. No action required by the user of the SU. This can help identify if a called party is not responding because they are out of coverage or if the call is getting through but they are still not responding.

### **4.2.4 Call Alert**

This feature works similar to paging. Rather than voice calling a radio and asking if the person is available to take a call a call alert is made. The radio beeps and displays the ID of the caller and the person receiving the call alert can then call them back.

### **4.2.5 Radio Inhibit / Uninhibit**

Another powerful feature is the ability to inhibit and uninhibit a radio remotely. This can be essential if encryption is used. If a radio is lost or stolen and it has the encryption keys someone with that radio could listen to the secure calls. The ability to inhibit that radio and receive feedback that the command was successful provides confidence that the lost radio is disabled.

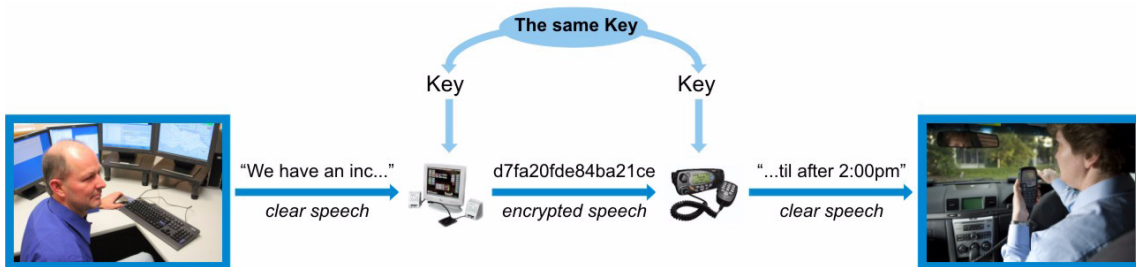
and can not be used to make or receive calls. If the radio is later recovered it can be uninhibited and returned to service.

This feature can also be useful for vehicle maintenance or transporting of radios from place to place. The radio can be configured and ready for use - but inhibited preventing any use of the radio until the authorized user has possession of the radio (or vehicle)

## 4.3 Introduction to P25 Encryption

### 4.3.1 What is Encryption?

Encryption in a P25 radio is a service provided to enable secure communication between parties. By loading the same key into all the radios in a group, all radios in that group can then talk among each other privately - and no outsiders can intercept the communications.



For this system to operate, we must have exactly the same key in both radios and each radio must use the same encryption algorithm. For P25 systems, we use Digital Encryption Standard (DES) and Advanced Encryption Standard (AES) algorithms. Whenever a user presses the PTT button, the radio periodically transmits the applied algorithm ID and Key ID (and a Message Indicator used for synchronization) with the encrypted speech. The receiving units then can determine which key and algorithm to use for decrypting.

The actual algorithms used for encryption are not secret. They are very widely available and under extreme public scrutiny at all times. The security in these systems is not in keeping the algorithm secret - it is all based on keeping the keys secret. This is not just P25 practice - this is the only correct way to manage any secure encryption system.

### 4.3.2 Levels of Encryption

There are two encryption algorithms in general use in P25 radio systems. These are DES and AES. DES is reasonably old now and so AES is becoming the normal choice for most organizations. The reasons to use DES nowadays are to maintain compatibility with older radios, to save cost, or to enable interoperability with other radio users on other radio networks. International export restrictions may also mandate use of an algorithm limited to 56-bit key lengths, thus restricting the P25 radio system to DES. The only significant difference between DES and AES are their levels of security. Although the two algorithms operate differently, the simplest way to think about this is that DES uses a 56 bit key whereas AES uses a 256 bit key. The difference is mathematically enormous. There are  $2^{56}$  keys available for DES and  $10^{77}$  keys (1 with 77 zeros following) keys for AES.

## **Digital Encryption Standard (DES)**

DES uses a 56 bit key (that is about 72,000,000,000,000,000 possible keys). The most successful way to crack a DES encryption system is by brute-force techniques. Machines have been developed to test every key until a message is decrypted. Some of these machines test >80 billion keys per second! These machines decrypt the same message over and over again with different keys, until the decrypted message decodes correctly. This is usually confirmed when the checksum for the message is correct. DES has been cracked in as little as 22 hours (a network of >10,000 PCs).

The problem for P25 voice message cracking is that it is not easy to work out if the message has been decrypted. There is no checksum in the P25 speech data. If a machine tests 80 billion keys per second, then it must determine if the decoding is correct 80 billion times a second. This is not possible (as far as we know) with a P25 speech signal - virtually without reconstructing the audio and listening to it. If a key was tested once per second it would take a leisurely 22 billion years to check all keys. Let's assume you can somehow test 1000 keys per second, and only have to test half the keys before striking it lucky, you will only need 11 million years and so, even if these numbers are exaggerated a million times, it will still take 11 years to discover that the drugs bust is about to happen - which may be a little late!

The point is, by whatever the technology, key cracking is a major technical challenge. It is extraordinarily unlikely that anyone will crack a DES key on a P25 system.

## **Advanced Encryption Standard (AES)**

AES algorithms run with a 256 bit key. AES has never been cracked. With such a large key, the astronomical numbers make key cracking quite improbable: If keys were tested at 88 billion per second, then it would take 352 million years to test all the codes.

## **Algorithm Approvals**

The National Institute of Standards and Technology (NIST) issued the Federal Information Processing Standards (FIPS) 140 Publication Series to coordinate the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the United States federal government.

FIPS140-2 approval is required for many users, in particular U.S. federal users. FIPS-140 requires testing and verification of the crypto module boundaries and functionality by an external accredited crypto test lab. Having the crypto module certified by NIST to FIPS-140 is a very good quality reassurance for the radio's crypto module security.

AES has been adopted as the US Federal standard algorithm for encryption. The DES algorithm with only 56 bits can no longer be approved by NIST (USA) or CSA (Canada).

- ① For this reason, Tait uses a Triple DES algorithm, with a single 56 bit key used 3 times. This effectively encrypts exactly the same as single DES but the algorithm is able to be approved by NIST and Canadian Standards Association (CSA). By achieving this approval, we can be reassured that we have implemented the algorithm in the correct manner.

### 4.3.3 A Secure Radio System

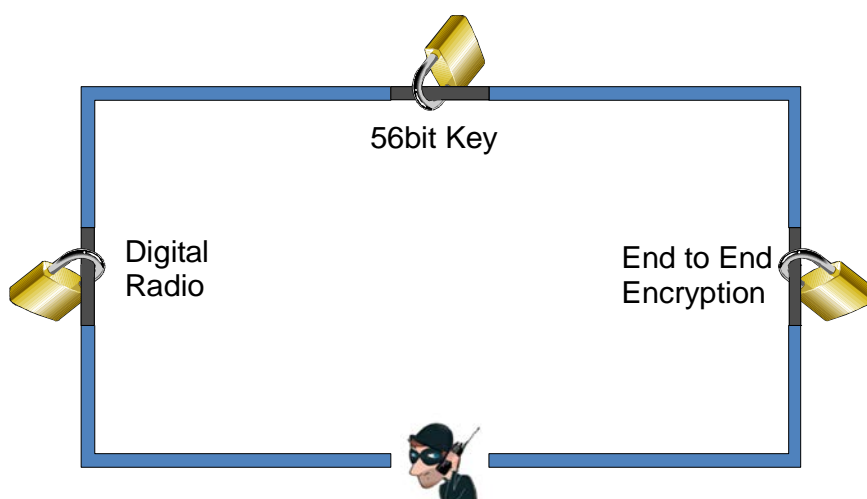
To correctly design a radio system, it is essential to understand the threats to the systems.

At first, many users believe that simply by deploying AES instead of DES, they assure themselves of complete security. This is not really the case.

The mathematical chance of finding a key by decryption technology for either AES or DES is beyond practicality - so decrypting an intercepted message is very unlikely.

Your threat is not someone guessing or calculating the key - it is in the key management and the radio management. For example, if a third party is able to get hold of just one encrypted radio, they could listen to encrypted communication on that radio, and you have conveniently saved them 352 million years of computing time.

The security of the system is reliant upon the security of the keys (both the variables and the devices that contain them) - and the organizational processes around them. This section introduces a few of the important points to consider, but does not attempt to document all aspects of key security.



#### Asset Management Procedures

Having encryption is of no value if there is poor management of the assets that contain the key. Once a key is loaded into a SU, the security of the system relies on being confident of where that SU is and that it has not been lost, stolen or gotten into the wrong hands by any other means. Even if the

asset is not lost, it may still be a security risk if it is in an uncontrolled location because the vehicle it is in is currently being repaired or serviced. Possible asset management risk areas include:

- Inability to identify SUs.
- Issuing of SUs is uncontrolled.
- Return of SUs is uncontrolled.

If there are procedures in place to identify if an asset has been lost, stolen, or is in an uncontrolled location, there must also be a method of ensuring communication on the remaining SUs is still secure.

This may include:

- The ability to Inhibit and Uninhibit SUs.
- The immediate loading of new keys into the remaining units.

### Key Storage and Loading Procedures

It is also often necessary to change the radio keys at regular intervals, so there must be strict security procedures to define how this rekeying is managed.

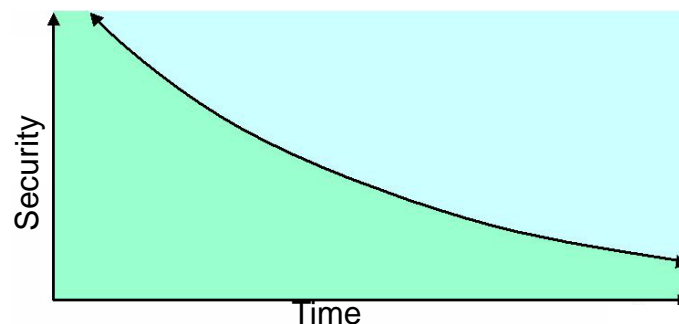
- Who are the Key Custodians?
- How often are the new keys generated?
- How are the keys stored?
- Who has access to the key loaders?
- How are the keys distributed and loaded in to the SUs?
- When are keys removed from SUs?

If there are no procedures in place to ensure that the keys remain secure, there can be no confidence that the communications will be secure.

### Key Life

Given enough time, it might be possible for a 3rd party to figure out what the encryption key is or obtain a SU with the key in it. For communications to remain secure, it is necessary to change the encryption key from time to time. How frequently the key is changed depends on the level of security required.

- For low-security communications with no threat to life, a key may be kept for a year or more.
- For critical tactical operation keys, new keys may be used for each operation.



### 4.3.4 Keyfilling Methods

There are two techniques for putting keys into radios:

- Cabled Key Filling
- Over The Air Rekeying

#### Cabled Key Filling Using a Key Fill Device (KFD)

This is the basic means of sending keys to a radio. A Key Fill Device (KFD) is pre-programmed with a number of keys, and the user can download these to a number of radios. Using a KFD requires physically connecting to each radio to load keys.

For small fleets, a Key Fill Device is probably sufficient. However, for large fleets, having to physically connect to each radio in order to change keys with a KFD makes changing keys a complex, time consuming process. Security of the KFD is paramount. You have a major problem if a KFD is misplaced!



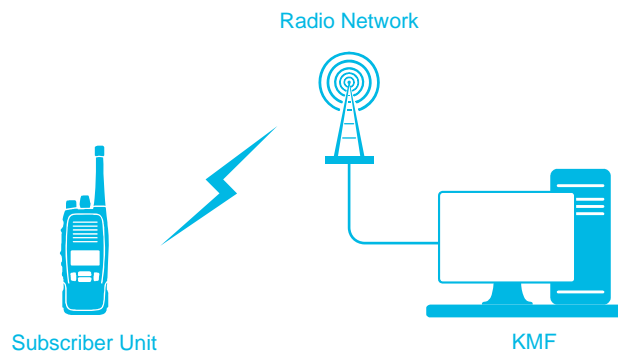
#### Over the Air Rekeying

Over the Air Rekeying (OTAR) allows new encryption keys to be sent out over the air to SUs without needing to physically handle each radio. OTAR requires a Key Management Facility (KMF). The KMF is programmed with all the keys in the system (typically it generates these), all the radios in the system, and the allocation of keys and radios to groups. The KMF will manage the keys that are in the radios on the system without the need to physically connect to the radios. Some KMFs will also manage radio Inhibit and Uninhibit.

- ⓘ The Tait KMF will work on both Trunked and Conventional radio systems. It will manage the radios, groups, and keys in a fleet. It will also allow for interactive radio diagnostics, key performance reporting, and fleet control. It will allow for variable crypto-periods across a fleet, thus making it possible to reliably manage both very secure teams and large fleets.

The KMF is usually a Client-Server type system accessed from a desktop PC. A KFD is initially used to program the radio with the UKEK (Unique Key Encryption Key). This allows secure communications to take place over the air with the KMF. The KMF can then send encryption keys and other messages over the air to the radios using standard Key Management Messages (KMM). Because standard messages are used over the air, a KMF can typically manage any OTAR-enabled P25 radios in a fleet.

Although a KMF sounds like the perfect solution to a management nightmare - it does not solve all problems. It still requires careful planning to design a fleet to optimize the workload of the KMF and to avoid compromising user security with over-zealous distribution of keys. KMFs also rely on having access to the radio fleet over the air. Depending on the fleet size, it will be necessary to take this into account when analyzing the capacity of the system.



### 4.3.5 Encryption Keys

An encryption key is a secret number stored in the SU and used to encrypt and decrypt the message. The Key Variable (the secret number) can be created by the Crypto Officer or randomly generated by a Key Management Facility (computer software that manages an encrypted radio network). Below are examples of a DES and AES key (keys are entered in hexadecimal notation).

DES Key Variable	0123456789ABCDEF
AES Key Variable	0123456789ABCDEF0C1C2C3C4C5C6C7D0D1D2D3D4D5D6D7E0E1E2E3E4E5E6E7

A Tait SU can store up to 34 different encryption keys. These keys can be DES keys, AES keys or a mixture of the two.

Depending on the system requirements:

- A key may be strapped to a particular channel, group or individual call. This ensures a known key is used whenever a call is made.
- Alternatively, the subscriber may be allowed to select the key to use when making a call. This allows different keys to be used depending on the situation.

For either of the above options, the subscriber may have the option of turning encryption on and off or encryption may be permanently enabled.



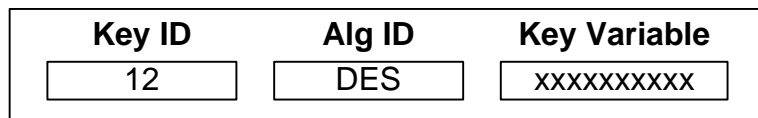
**Identifying the Key** The encryption key itself must remain secret, but since there may be more than one encryption key in a SU, there must be a way to identify which key to use when an encrypted transmission is received.

When a key is created, the following information is created and tagged to the key:

**Key Variable** The Key Variable is the actual 56bit DES or 256bit AES key. This is a secret number created by the Crypto Officer (or randomly generated) that is used to Encrypt and Decrypt the message. This number must be stored in each SU but also kept secret.

**Alg ID** When a key is created, it is given an Algorithm (Alg) ID that identifies whether the key is for AES or DES.

**Key ID** When a key is created, it is given a Key ID. This is a number between 1 and 65535 that uniquely identifies this key variable. All DES keys must have a unique Key ID and all AES keys must have a unique Key ID. However, a DES Key ID can be the same as an AES Key ID, as both the Alg ID and Key ID are used together to identify the key.



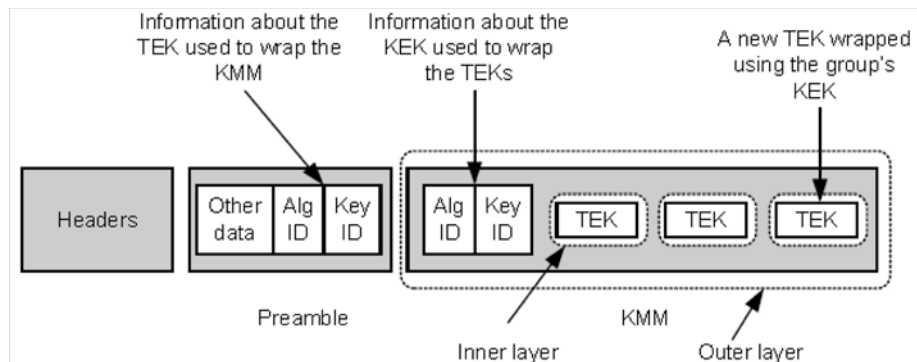
### 4.3.6 Key Types

There are two different types of keys, Traffic Encryption Keys (TEK) and Key Encryption Keys (KEK). Both types of keys are defined in exactly the same way with a Key ID, Alg ID, and a Key Variable, but TEKs and KEKs are used for different purposes:

**TEK** A Traffic Encryption Key is used to encrypt voice (or data) communications on a channel.

**KEK** A Key Encryption Key is used on an OTAR system to encrypt keys when they are sent out over the air.

The new keys (TEKs) are encrypted with a KEK before being sent out to the SU in a Key Management Message (KMM). The Key Management Message, including the new keys, is also encrypted using a Traffic Encryption Key. In effect, keys sent by OTAR are encrypted twice, as the key material will be encrypted with a KEK, and then the data message that carries the key material over the air will be encrypted with the TEK.

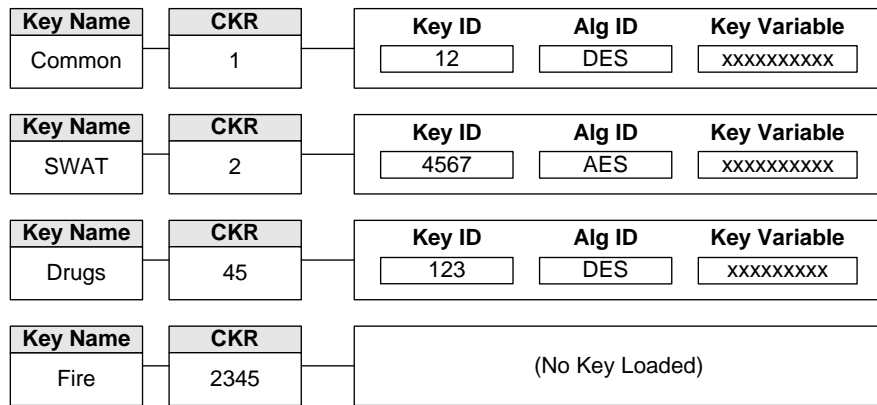


<b>UKEK</b>	A Unique Key Encryption Key (UKEK) is a KEK that must be loaded into a radio using a Key Fill Device before OTAR can be used to send keys over the air to that radio. It is called a UKEK as the KEK should be unique (different) in every radio. This means that when keys are sent out, they are encrypted differently for every radio. This prevents a stolen radio from being reprogrammed with a new valid radio ID and continuing to receiving the key updates.
<b>Provisioning Key</b>	The KMF must know which UKEK has been loaded into each radio. To simplify this process, often all radios are first programmed with the same UKEK in the radio workshop. This is called a Provisioning Key (or a Shop Key). The KMF can be configured to replace this Provisioning UKEK with a truly unique UKEK using OTAR. However, for convenience, some organizations simply leave the Provisioning UKEK in all radios.
<b>CKEK</b>	A Common Key Encryption Key (CKEK) is a KEK that is shared by a group of radios to allow key update messages to be broadcast to multiple radios at one time. However, CKEKs are rarely used, as broadcast messages cannot be used on trunked networks and are currently not supported on conventional networks.

#### 4.3.7 Referencing the Key

Up to 34 keys can be stored in the SU. Each key will have a specific purpose. Some may be used for low security general communication and others for high security tactical operations. If multiple keys are used, it would be very difficult to remember which Key ID to use for each call type, especially since the Key ID would change every time a new key is loaded into the SU. Therefore, a different method is used to reference the key that should encrypt a call.

<b>Common Key Reference</b>	A Common Key Reference (CKR) is a number between 1 and 65535 (typically 1-4095 used for TEKs and 61440-65535 used for KEKs). The CKR is like the address in the SU where a key can be stored. The Key Variable, Alg ID and Key ID are all stored in that location using a key loader or via OTAR. The SU is configured to use the key stored in a particular CKR location to encrypt the call. If a key is replaced, a new Key Variable, Alg ID and Key ID are stored in that location, but the same CKR number is used to identify the purpose of that key. When an encrypted call is received, the SU checks all the CKR locations to see if any contain the Key ID of the key that was used to encrypt the call.
<b>Key Name</b>	If multiple encryption keys are used, they are likely to be designated for different purposes. Each CKR location can be given a name (using the programming software), so the subscriber can easily identify the purpose of the key in that location. For example a police force may have one CKR called “Common” which stores the key used on the general dispatch channel by everybody, and another CKR called “SWAT” that stores a key which is used by only the SWAT team.



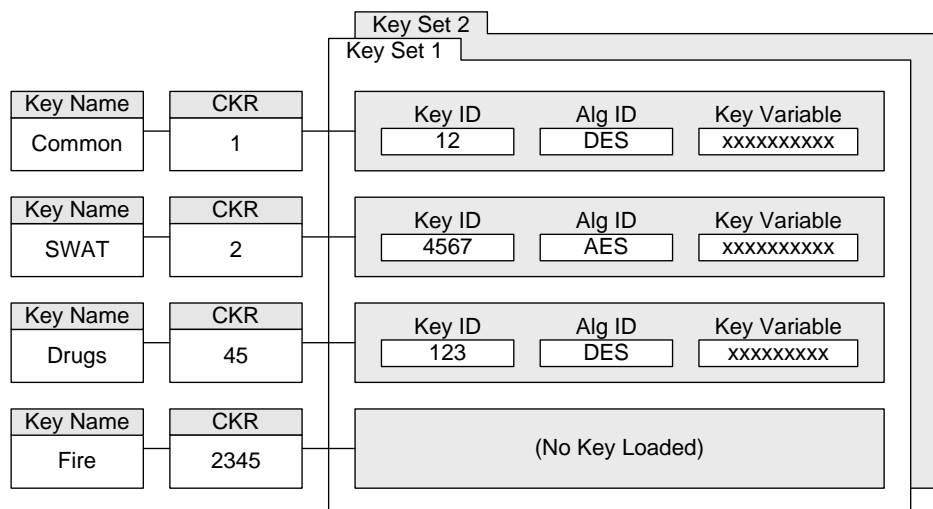
**i** Key Name used in this example is from the radio user’s perspective. Technically, it is the CKR name, but radio users often simply talk about the Key Name. From a Crypto Officer’s perspective, working with a KMF, there will be a Key Name that refers to the actual key in that CKR location. For example, the name of the CKR may be Common, and key in this location may be called Common.v1; next year it will be replaced with a key called Common.v2.

**Keysets**

When the time comes to replace an encryption key, it may not be possible to change the key in all the SUs at the same time. This would result in a situation where some of the fleet had the old key and some had the new key and communication could not be guaranteed.

The solution is to have two keysets. One keyset is the active keyset that is used by the SU to encrypt calls. The second keyset is inactive and keys stored here are not used to encrypt calls, but will still be used to decrypt calls if they are received encoded with that Key ID.

The key in the inactive keyset can be replaced with a new key without affecting communications. When all SUs have the new key, the inactive keyset can be made the active keyset. During the changeover period, if a subscriber has not yet changed over keysets, so long as the new key is in the inactive keyset, and a call is received, the SU will still decrypt and hear the call.



### 4.3.8 Encryption Process

SUs store the Key Variable, Alg ID and Key ID, of all the keys they can use to encrypt and decrypt calls. When a SU transmits an encrypted call, the message is encrypted using the currently selected Key Variable.

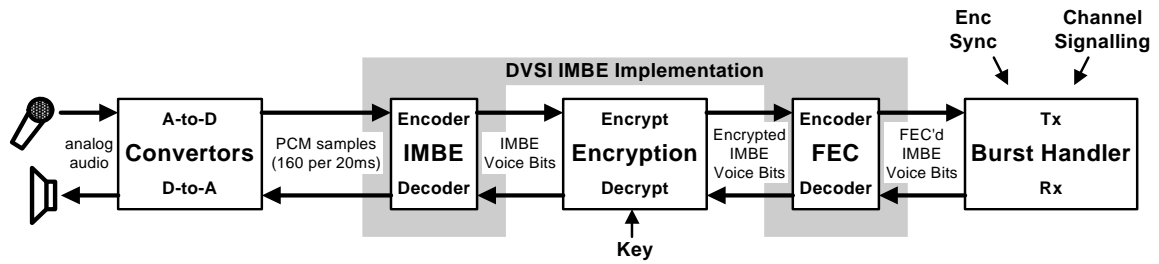
The receiving SU may also be programmed with more than one key, but must use the same key to decrypt the call that the transmitting SU used to encrypt the call.

For this reason, the transmitting SU also transmits the Alg ID and Key ID of the key variable that it used to encrypt a call. When a SU receives an encrypted transmission, it identifies the key and algorithm used to encrypt the call by looking at the Key ID and Alg ID that were transmitted with the message.

#### Encrypting the Voice

A P25 voice transmission is encrypted as follows:

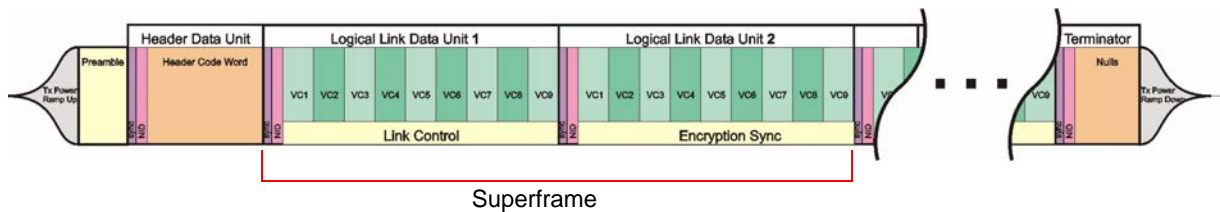
1. The subscriber speaks into the microphone.
2. The analog audio and any background noise picked up is converted into digital data in a device called a Codec.
3. The digital voice is compressed and background noise removed in a device called a Vocoder. This also breaks the speech up into 20ms blocks of data called voice codewords.
4. The voice codewords are encrypted using either a DES or AES algorithm (mathematical process) and the selected encryption key.
5. Forward Error Correction is added. This is additional data added to the transmission that allows the receiver to not only detect but also correct errors introduced when the message was transmitted.
6. The Burst Handler builds the P25 frame by adding the following:
  - Link Control signaling. This includes information like the Network Access Code, the ID of the SU sending the transmission, and the address of the SU or talkgroup the transmission is for.
  - Encryption Signaling. This includes information like the Alg ID and Key ID, which tell the receiver the key and algorithm used to encrypt the call, and the Message Indicator which tells the receiver a random start point in the algorithm that was used by the transmitter.
7. The P25 frame is then passed on to the C4FM modem to modulate onto the RF carrier.



### P25 Frame Structure

The P25 Common Air Interface mandates that the following frame structure be used to transmit a call:

1. A common practice, which is not part of the P25 standard, is to start with a Preamble. This allows scanning receivers time to identify that a transmission is about to begin.
2. A Header is sent that includes the Network Access Code and Address information, along with the encryption sync information required to decrypt the next 360ms of voice.
3. Logical Data Unit 1 (LDU1) is sent. This contains 9 voice codewords (180ms of voice) and also repeats the channel signalling.
4. Logical Data Unit 2 (LDU2) is sent. This contains the next 9 voice codewords (180ms of voice) and the encryption sync information. The Encryption Sync repeats the Key ID the Alg ID sent in the header and has a new Message Indicator used to decrypt the next 360ms of voice.
5. Together, LDU1 and LDU2 are known as a P25 Superframe. Superframes repeat for the duration of the transmission.
6. At the end of the transmission, a Terminator is sent.

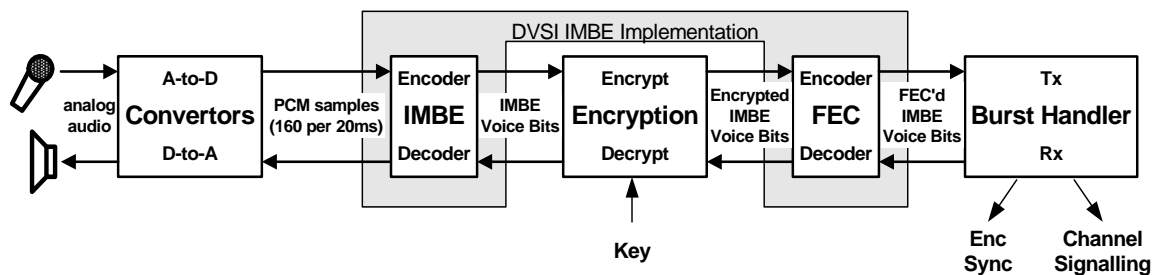


The Message Indicator (MI) is a number indicating the start point in the encryption algorithm; it is pseudo-randomly generated when the encryption process starts. The receiving SU must use the same number to decrypt the call, so the Message Indicator is transmitted over the air in the header. With every P25 superframe (360ms), a new Message Indicator is generated and used to decrypt the next superframe. However, since it is not truly a random number, as long as the receiving SU receives one Message Indicator, it can calculate what the Message Indicators should be for the remainder of the call.

## Decrypting the Voice

The decryption process is the reverse of the encryption process:

1. The Burst Handler breaks down the P25 Frame by separating:
  - P25 Voice Codewords
  - Link Control signaling
  - Encryption Signaling
2. Forward Error Correction is used to not only detect, but also correct any errors introduced when the message was transmitted.
3. The voice codewords are decrypted using the encryption key and algorithm specified in the transmission. If the SU does not have the specified key, the call can not be decrypted.
4. The decrypted digital voice is decompressed by the vocoder.
5. The digital voice is converted back into analog audio in the Codec.
6. The audio is amplified and the subscriber hears the audio from the speaker.



### 4.3.9 Subscriber Units and Encryption

Encryption is an optional feature, and not all models of SU support encryption.

- Some SU models do not support encryption and can not be upgraded to support encryption.
- Some SU models can support encryption, but must have the correct Software Features enabled.
- Some SU models require a hardware module to be fitted in order for the radio to support encryption.

Encryption can be used on both conventional and trunked systems. If OTAR is to be used, Packet Data must also be configured in the SU and supported by the network.

There are many settings that must be correctly configured for encryption and OTAR to operate correctly, only a few key parameters are described in this section. The remainder of this section uses the TP9100 portable and programming software as an example to describe how encryption could be configured in a SU. These features may not be available, or may be configured in a different way on other SUs.

#### Subscriber Unit Operation

The user controls related to encryption are configured when the SU is programmed. Operating the SU in encrypted mode can be made exactly the same as operating it in clear mode with no user control of encryption permitted. However, the SU may be configured to allow the subscriber to:

- Turn encryption on and off, or encryption may be permanently enabled for specific (or all) channels.
- Select the key used for a call or a particular key may be strapped (always used by) to that channel or group.
- Zeroize or delete all keys from the SU.
- Request that the KMF does a key update.

