

Two-Way Communication Patching

Whitepaper

ISICSB Training & Outreach Committee
September 2024



**Iowa Statewide Interoperable
Communications System**
isicb.iowa.gov

Contents

Abstract.....	2
Introduction	3
Types of Patches.....	3
Soft Patches	3
Hard Patches	4
Patching	5
Resource Management with Patching	5
Resources and StatusBoard	5
Announcement of a Patch	5
Patching with Encryption	5
Local Policy and Procedure.....	5
Conclusion	6

Abstract

This whitepaper will discuss the process of two-way communications patching and how it works. On the Iowa Statewide Interoperable Communications System (ISICS), patches are used every day to ensure seamless true interoperable communications throughout the state of Iowa. Using patches ensures the safety of all first responders' safety on the front line.



Introduction

What is a Patch?

A patch is a group of one or more “linked” or “grouped” talkgroups that allows radio users to communicate with each other while on separate radio talkgroups and/or radio systems. While the patch is active, all talkgroups will act as one. Regardless of the talkgroup the user transmits from, the transmission will broadcast over the other talkgroups of the patch as well.

A communications patch is vital tool in ensuring effective and seamless radio communication between different users, agencies, and different radio systems. A patch allows users to bridge a gap between various radio networks, even if the other networks are using different protocols and technologies. Patches have been proven beneficial in high-scale emergency situations. A patch allows users to be interoperable with one another without any limitations of current system incapacibilities.

Types of Patches

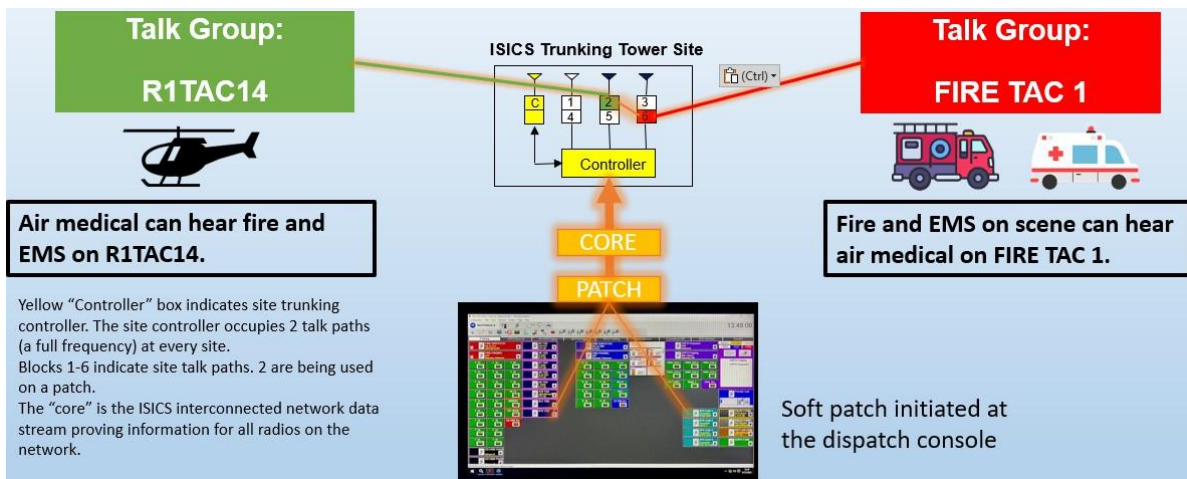
There are two primary types of two-way communication patches: console soft patches and hard patches.

Console soft patches are commonly established directly from the dispatch console with a few clicks on the radio dispatch screen. In contrast, hard patches involve physically connecting two or more subscriber radios through gateway equipment.

Soft Patches

Soft patches are the primary type of patch used on ISICS and are initiated at the dispatch console. This type of patch is used when utilizing resources within the same radio system. When a patch is created with one talkgroup to another on the same radio system, it requires no additional hardware. It is all handled within the trunked system core and site control channel. This requires no change in operation to units in the field and is done without any notice from the users.

Two-Way Communication Patching



(This diagram shows a soft patch that was initiated at a dispatch console. In the diagram, talkgroup on R1TAC14 (timeslot 2) and Fire TAC 1 (timeslot 6) are patched in together.)

Hard Patches

A hard patch is "hard-wired." This type of patch requires the use of physical gateway equipment with subscriber radios to complete a patch. These patches are used to patch between two different radio systems. These patches can also be used by a Communications Unit Technician (COMT) for emergency communications at the scene of an incident. The drawback of utilizing a hard patch is that the setup and configuration process can be time-consuming, requiring additional knowledge about the equipment involved.



(This diagram shows a hard patch that was initiated at a gateway. In the diagram, two portable radios are connected to the gateway through a wired connection to be able to talk to one another.)

Patching

Resource Management with Patching

A crucial consideration when using a patch is the number of resources required to facilitate a single conversation. Instead of using a single talkgroup, you are using two or more. This takes up an extra talk path(s) on the trunking site. Sites are limited to a certain number of talk paths.

Suggestion: possibility of patching between two system?

Resources and StatusBoard

Dispatch and credentialed COMU personnel have access to the ISICSB StatusBoard. This is a web-based communications tool that allows agencies to see what talkgroups are being used and which ones are available to be used at the regional and statewide interoperability talkgroup levels. It is very important to utilize the StatusBoard before placing a patch to ensure the talkgroup is open for use. ISICS StatusBoard training link [here](#).

Announcement of a Patch

It is considered best practice to always announce when a patch is created or taken down. This helps other users on the system know when a resource is being utilized and when it's available again for use.

Patching with Encryption

When patching an encrypted talkgroup, it's important to be mindful that there's a chance the encrypted talkgroup could lose its encryption, potentially allowing outsiders to listen in. If an agency operates with day-to-day encryption and patches to a statewide or regional interoperability talkgroup that is not encrypted, the audio will be broadcast unencrypted.

Local Policy and Procedure

Always make sure to refer to your agency's local operational policies and guidelines to ensure compliance. If you're unsure about anything, contact your immediate supervisor for clarification.

Conclusion

Effective communication is essential in public safety and emergency response, and the use of patches is a critical tool in achieving seamless interoperability across various radio systems and agencies. By understanding the different types of patches—soft and hard—and their respective applications, dispatchers and field personnel can ensure that communication remains clear and uninterrupted, even in complex and high-pressure situations.

Soft patches, managed directly from the dispatch console, provide a flexible and efficient way to link talkgroups within the same radio system without additional hardware. Hard patches, while requiring more setup and equipment, enable interoperability between different radio systems, making them invaluable in scenarios where multiple agencies need to coordinate efforts.

Resource management, the use of tools like the ISICSB StatusBoard, and adherence to best practices and local policies are all critical factors in successfully implementing and managing patches. Announcing the creation and removal of patches, monitoring the availability of talkgroups, and being mindful of encryption considerations are essential steps to maintaining the integrity and security of communications.

By leveraging the power of patches and adhering to these guidelines, agencies can enhance their communication capabilities, improve coordination, and ultimately ensure better outcomes in both routine operations and emergency situations.

