PROPOSAL TO
TAIWAN NAVY

ACCEPTANCE TEST PLAN

M-CORE **FEBRURARY 07, 20**

TABLE OF CONTENTS

This page intentionally left blank.

ACCEPTANCE TEST PLAN

Taiwan Navy

M-Core

In-Plant Final

www.motorolasolutions.com/services/government

Steven Chiang
System Engineer
+886 2 7750 0388

Deo Hsu
System Engineer
+886 2 7750 0385

3.1 WIDE AREA TRUNKING FDMA/TDMA MIXED SITES

3.1.1 Talkgroup Call

1. DESCRIPTION

The Talkgroup is the primary level of organization for communications on a trunked radio system. Radios with Talkgroup call capability will be able to communicate with other members of the same Talkgroup. This provides the effect of a private channel down to the Talkgroup level.
This test will demonstrate that a Talkgroup transmission initiated by a radio user will only be heard by system users, which have, the same Talkgroup selected. As with other types of calls, Talkgroup calls can take place from anywhere in the system.

SETUP

RADIO-1 - SITE 1 - TALKGROUP 1
RADIO-2 - SITE 2 - TALKGROUP 1
RADIO-3 - SITE 1 - TALKGROUP 2
RADIO-4 - SITE 2 - TALKGROUP 2

VERSION #1.040

2. TEST

Step 1. Initiate a Wide Area Call with RADIO-1 in TALKGROUP 1.

Step 2. Observe that only RADIO-2 will be able to monitor and respond to the call.

Step 3. Initiate a Wide Area Call with RADIO-3 in TALKGROUP 2.

Step 4. Observe that only RADIO-4 will be able to monitor and respond the call.

Pass____ Fail____

3.1.2 Continuous Assignment Updating

1. DESCRIPTION

When a talkgroup is assigned a voice channel, the site controller continues to transmit the channel assignment on the control channel for the duration of the talkgroup call. Radios coming into use on the system are automatically sent to voice channels with conversations in progress involving their selected talkgroups.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1
RADIO-3 - TALKGROUP 1

VERSION #1.010

2. TEST

Step 1. Turn OFF RADIO-1.

Step 2. Initiate a Talkgroup Call using RADIO-2 and verify RADIO-3 hears the audio.

Step 3. While the Talkgroup Call is in progress, turn ON RADIO-1.

Step 4. Observe RADIO-1, which was just brought back into service, joins the Talkgroup Call already in progress.

Step 5. End the talkgroup call.

Step 6. Switch RADIO-1 to another talkgroup.

Step 7. Initiate a Talkgroup Call from RADIO-2 to RADIO-3.

Step 8. While the Talkgroup Call is in progress, set RADIO-1 back to TALKGROUP 1.

Step 9. Observe that RADIO-1 joins the Talkgroup Call already in progress.

Pass____ Fail____

3.1.3 End-to-End Call

1. DESCRIPTION

End-to-End Call is a selective calling feature that allows a radio user to carry on one-to-one conversation that is only heard by the 2 parties involved. Subscriber units receiving a End-to-End call will sound an alert tone. As with other types of calls, End-to-End Calls can take place from anywhere in the system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1
RADIO-3 - TALKGROUP 1

VERSION #1.020

2. TEST

Step 1. Using RADIO-1, press the Call button.

Step 2. Enter the unit ID of RADIO-2 with the keypad, or scroll to the location where this ID is stored.

Step 3. Press the PTT to initiate the End-to-End Call.

Step 4. Verify that RADIO-2 hears tones and the display indicates that a End-to-End Call has been received, but RADIO-3 receives no indications.

Step 5. Answer the call at RADIO-2 by pressing the Call/Respond button. If RADIO-2 has a display, verify it shows the ID number or Alias of the calling unit.

Step 6. Press the PTT switch on RADIO-2 and respond to the End-to-End Call. Note that if you do not press the Call button before pressing PTT, your audio will be heard by all members of the talkgroup, and not just by the radio initiating the End-to-End Call.

Step 7. Verify that RADIO-2 can communicate with RADIO-1.

Step 8. Verify that RADIO-3 does not monitor the End-to-End Call.

Step 9. End the End-to-End Call by pressing the "home" key and return to normal talkgroup operation.

Pass____ Fail____

3.1.4 Secure Operation

1. DESCRIPTION

Digital encryption is used to scramble a transmission so only properly equipped and configured radios can monitor the conversation. A "Key" is used to encrypt the transmit audio. Only radios with the same "Key" can decrypt the audio and listen to it.

SETUP

RADIO-1 - TALKGROUP 1 (SECURE TX MODE)
RADIO-2 - TALKGROUP 1 (SECURE TX MODE)
RADIO-3 - TALKGROUP 1 (SECURE MODE and no, or incorrect key)
RADIO-4 - TALKGROUP 1 (Clear TX Mode)

Note: The identical secure mode must be programmed into RADIO-1, RADIO-2, RADIO-4 and that RADIO-3 has no secure code loaded or has a unique secure code from the other testing radios.

VERSION #1.020

2. TEST

Step 1. Initiate a secure wide area call with RADIO-1 on TALKGROUP 1. Keep this call in progress until instructed to end the call.

Step 2. Observe that RADIO-2 will be able to monitor the call.

Step 3. Observe that RADIO-3 does not receive the call.

Step 4. Observe that RADIO-4 will also receive the call even with the secure switch set to the non-secure mode of operation.

Step 5. End the call from RADIO-1.

Step 6. Respond with RADIO-2 and verify that RADIO-1 receives the response audio but RADIO-3 cannot.

Pass____ Fail____

3.1.5 Emergency Alarm and Call with Hot Mic

1. DESCRIPTION

Users in life threatening situations can use the Emergency button on the radio to immediately send a signal to the dispatcher and be assigned the next available voice channel. An Emergency Call can be set to either Top of Queue or Ruthless Preemption operation. During an emergency call the Emergency ID will appear on the display of the subscribers. To demonstrate this, an Emergency Alarm and Call will be initiated from a portable which will be received by a portable, on the same talkgroup, affiliated at any site of any zone in the system.
This test will demonstrate when the Hot Mic option is configured, the subscriber will send an emergency and after a voice channel is assigned, the subscriber will automatically transmit for a programmable period of time.
Emergency Alarm with Voice to Follow (Hot Mic) is an option in the portable and must be enabled via software. This test case works for all portable radios. For mobile radios, specific mobile microphone models are required.
NOTE: If the subscriber does not have a display, the Emergency ID will not be displayed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1
RADIO-3 - TALKGROUP 1

Emergency Alarm w/ Voice Following must be enabled in the subscriber.

VERSION #1.030

2. TEST

Step 1. Using RADIO-1 send an Emergency Alarm by pressing the emergency button.

Step 2. Observe the display on RADIO-2 and RADIO-3 denotes an emergency and the unit ID or alias of RADIO-1.

Step 3. Observe that RADIO-2 and RADIO-3 can hear any audio from RADIO-1 even though RADIO-1 does not have its PTT switch pressed.

Step 4. Observe that RADIO-1 PTT times out and the radio dekeys.

Step 5. End the Emergency Call by holding down the Emergency button.

Pass____ Fail____

3.1.6 Dynamic FDMA/TDMA Emergency Alarm and Call with Top of Queue - FDMA call in queue

1. DESCRIPTION

Users in life threatening situations can use the Emergency button on the radio to immediately send a signal to the dispatcher and be assigned the next available voice channel if the FDMA/TDMA mode of the call can be supported by the available resource. Otherwise, the first call in the queue that can use the available resource gets assigned. An Emergency Call can be set to either Top of Queue or Ruthless Preemption operation. To accomplish this, an Emergency Alarm and Call will be initiated from a subscriber which will be received by a subscriber affiliated at any site of any zone in the system. In this case, the first available resource CANNOT support the emergency call mode.

NOTE: If the subscriber does not have the Display option, the Emergency ID will not be displayed. All radios and talkgroups should start with default priorities. Default is 10. SITE 1 must be TDMA capable.

SETUP

RADIO-1 (TDMA) - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 (TDMA) - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 (TDMA) - TALKGROUP 3
RADIO-3 - SITE - SITE 1
RADIO-4 (TDMA) - TALKGROUP 4
RADIO-4 SITE - SITE 1
RADIO-8 (FDMA-only) - TALKGROUP 1
RADIO-8 - SITE - SITE 1
Note: TALKGROUP 1, TALKGROUP 2, TALKGROUP 3 and TALKGROUP 4 are programmed for "Dynamic".

VERSION #1.010

2. TEST

Step 1. Verify the emergency type for TALKGROUP 1's template must be set up as Top of Queue.

Step 2. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.

Step 3. Initiate a call with both RADIO-2 and RADIO-4 and hold the PTT switches until instructed to release.

Step 4. Key RADIO-3 and verify the radio receives a busy tone. Release the PTT switch on RADIO-3.

Step 5. Using RADIO-1 send an Emergency Call by pressing the emergency switch and then the PTT switch. Observe that RADIO-1 cannot transmit due to the voice channel being busy.

Step 6. Release the PTT switch on RADIO-2. Observe that RADIO-3 receives the call back before RADIO-1 and is able to proceed with the call because the available channel resource is already busy with one TDMA call and can only support another TDMA call.

Step 7. Dekey RADIO-4 and RADIO-3.

Step 8. Observe that RADIO-1 receives the callback and is able to proceed with the call.

Step 9. Observe that the display on RADIO-8 denotes an emergency and the unit ID of RADIO-1.

Step 10. Dekey RADIO-1 and exit the Emergency mode by holding down the Emergency button on RADIO-1 until an alert tone sounds. Verify RADIO-1 returns to normal operation.

Pass____ Fail____

3.1.7 Dynamic FDMA/TDMA Emergency Alarm and Call with Ruthless Preemption - FDMA call over-rides

1. DESCRIPTION

Users in life threatening situations can use the Emergency button on the radio to immediately send a signal to the dispatcher and be assigned the next available voice channel. An Emergency Call can be set to either Top of Queue or Ruthless Preemption operation. To accomplish this, an Emergency Alarm and Call will be initiated from a subscriber which will be received by a subscriber affiliated at any site of any zone in the system. In this test case, the emergency call will cause 2 TDMA calls to be pre-empted.

NOTE: If the subscriber does not have the Display option, the Emergency ID will not be displayed. This test is not recommended for single site systems as RF contention will occur. SITE 1 must be TDMA capable.

SETUP

RADIO-1 (TDMA) - TALKGROUP 5
RADIO-1 - SITE - SITE 1
RADIO-3 (TDMA) - TALKGROUP 2
RADIO-3 - SITE - SITE 1
RADIO-4 (TDMA) - TALKGROUP 3
RADIO-4 - SITE - SITE 1
RADIO-8 (FDMA-only) - TALKGROUP 5
RADIO-8 - SITE - SITE 1
Note: TALKGROUP 5, TALKGROUP 2 and TALKGROUP 3 are programmed for "Dynamic".

VERSION #1.020

2. TEST

Step 1. The emergency type for TALKGROUP 5's template must be configured as Ruthless Preemption.

Step 2. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.

Step 3. Initiate a call with both RADIO-3 and RADIO-4 and hold the PTT switches until instructed to release. Both calls are assigned in the TDMA mode to the single voice channel.

Step 4. Key RADIO-1 and verify the radio receives a busy tone.

Step 5. Using RADIO-1 send an Emergency Call by pressing the emergency switch and then the PTT switch.

Step 6. Observe that RADIO-1 is granted the channel immediately and the Talkgroup Calls are dropped for RADIO-3 and for RADIO-4.

Step 7. Observe that the display on RADIO-8 denotes an emergency and the unit ID of RADIO-1. Also observe that the channel is assigned in the FDMA mode.

Step 8. Dekey RADIO-3 and RADIO-4.

Step 9. Exit the Emergency mode by holding down the Emergency button on RADIO-1 until an alert tone sounds. Verify RADIO-1 returns to normal operation.

Pass____ Fail____

3.1.8 Dynamic FDMA/TDMA Busy Queuing and Callback with Ten Talkgroup Priority Levels

1. DESCRIPTION

If no voice channel resources are available, radios requesting channels for new conversations are placed in a queue. Users of the same priority will move through the queue in a first in, first out sequence; however, users of higher priority will be inserted ahead of lower priority users in queue. When a voice channel becomes available, the radio at the top of the busy queue gets a channel assignment and generates a callback tone if the FDMA/TDMA mode of the call can be supported by the available resource. Otherwise, the first call in the queue that can use the available resource gets assigned. The callback tone alerts the user that a channel assignment was made and transmitting is now possible on the selected talkgroup. In this test case, the available resource can NOT support the FDMA call mode.

NOTE: An Emergency Call has the highest priority at level 1. The highest assignable priority is 2 and 10 is the lowest. All radios and talkgroups should start with default priorities. The default is 10. SITE 1 must be TDMA capable.

SETUP

RADIO-1 (TDMA) - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 (TDMA) - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-4 (TDMA) - TALKGROUP 4
RADIO-4 - SITE - SITE 1
RADIO-8 (FDMA-only) - TALKGROUP 6
RADIO-8 - SITE - SITE 1
Note: TALKGROUP 1, TALKGROUP 2 and TALKGROUP 6 are programmed for "Dynamic".

VERSION #1.020

2. TEST

Step 1. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.

Step 2. Verify the priority level for TALKGROUP 6's template is configured as priority 9.

Step 3. Initiate Talkgroup Calls with RADIO-1 and with RADIO-2. Keep these calls in progress until instructed to end them. Both calls are assigned in the TDMA mode to the single voice channel.

Step 4. Key RADIO-8 and observe that the radio receives a busy.

Step 5. Key RADIO-4 and observe that the radio receives a busy.

Step 6. End the call on RADIO-1.

Step 7. Observe RADIO-4 receives the first callback and can now make a call because the available resource can not support an FDMA call.

Step 8. End the calls on RADIO-2 and RADIO-4.

Step 9. Observe RADIO-8 now receives a callback and can make a call upon receipt of the callback indication since there is now a FDMA channel available.

Pass____ Fail____

3.1.9 Auto Site Affiliation

1. DESCRIPTION

A Radio affiliation is a function that links a unique radio ID and unique talkgroup to a specific site. This information is stored in a affiliation table in the zone database.
Before resources are assigned, the affiliation table is accessed to know which sites need to be assigned to support the call. Only the sites that need to be assigned that have associated talkgroups will be assigned. If the site does not have that talkgroup affiliated to it will not be assigned. This allows for more calls to be processed with fewer resources.

SETUP

RADIO-1 - TG1
RADIO-1 - SITE - SITE1
RADIO-2 - TG1
RADIO-2 - SITE - SITE1
RADIO-3 - TG2
RADIO-3 - SITE - SITE2
RADIO-4 - TG2
RADIO-4 - SITE - SITE2
This test requires the ZoneWatch feature.

Note: There are system settings which could affect the assignment of resources, such as required site.

VERSION #1.020

2. TEST

Step 1. Turn RADIO-1 off and on.

Step 2. Verify via ZoneWatch that RADIO-1 sends in its affiliation.

Step 3. Initiate a call using RADIO-1 on TG1.

Step 4. Verify RADIO-2 can receive and respond to the call. Using ZoneWatch verify that no resources are assigned at SITE2 as there are no subscribers affiliated to TG1 at SITE2.

Step 5. Initiate a call on TG2 using RADIO-3.

Step 6. Verify that RADIO-4 can receive and respond to the call. Using ZoneWatch verify that no resources are assigned at SITE1 as there are no subscribers affiliated to TG2 at SITE1.

Pass____ Fail____

3.1.10 System Wide Call – Active Emergency Call Interaction – FDMA/TDMA Mixed Sites

1. DESCRIPTION

Active emergency talkgroup call is not impacted by a console system wide call.

SETUP

RADIO-1 - SITE 1 - TALKGROUP 1
RADIO-2 - SITE 2 - TALKGROUP 1

Configure an MCC 7500 console position for System Wide Call operation.

SITE 1 and SITE 2 have both TDMA and FDMA capable channels.

VERSION #1.020

2. TEST

Step 1. RADIO-1 initiates an emergency call by depressing the emergency switch and then the PTT switch.

Step 2. Observe that RADIO-2 can hear the emergency audio of RADIO-1.

Step 3. Unlock the system wide transmit capability by pressing the safety switch (scissor icon).

Step 4. Within 5 seconds, press the system wide instant transmit button on the system wide talkgroup window.

Step 5. Observe that RADIO-2 can hear the emergency audio of RADIO-1.

Step 6. Release the PTT switch on RADIO-1 and end the emergency call by holding down the emergency button.

Step 7. When emergency call is ended, observe that audio from the console transmit is heard at RADIO-1 and RADIO-2.

Pass____ Fail____

3.1.11 System Wide Call – FDMA/TDMA Mixed Sites

1. DESCRIPTION

Active talkgroup call transmissions initiated by radio users will be terminated by a console system wide call. Radios will hear audio from console system wide call.

SETUP

RADIO-1 - SITE 1 - TALKGROUP 1
RADIO-2 - SITE 2 - TALKGROUP 1
RADIO-3 - SITE 1 - TALKGROUP 2
RADIO-4 - SITE 2 - TALKGROUP 2

Configure an MCC 7500 console position for System Wide Call operation.

TALKGROUP 1 should be configured as TDMA only.

TALKGROUP 2 should be configured as FDMA only.

SITE 1 and SITE 2 have both TDMA and FDMA capable channels.

VERSION #1.020

2. TEST

Step 1. Initiate a Wide Area Call with RADIO-1 in TALKGROUP 1.

Step 2. Initiate a Wide Area Call with RADIO-4 in TALKGROUP 2.

Step 3. Observe that RADIO-2 will be able to hear the audio of RADIO-1 and that RADIO-3 will be able to hear the audio of RADIO-4.

Step 4. Unlock the system wide transmit capability by pressing the safety switch (scissor icon).

Step 5. Within 5 seconds, press the system wide instant transmit button on the system wide talkgroup window.

Step 6. Observe that the audio from the console transmit is now heard at RADIO-1, RADIO-2, RADIO-3.

Step 7. Dekey RADIO-4.

Pass____ Fail____

3.1.12 Prioirty Monitor/Priority Scan

1. DESCRIPTION

A subscriber unit can scan a pre-programmed list (in the radio) to find any Priority and Non-priority Talkgroups with assigned voice channels at that site. To demonstrate this, a call will be initiated from a portable at a remote site on a talkgroup monitored by a portable at the same site as the scanning radio. The scanning radio will scan from its selected talkgroup to the active talkgroup. The test will be repeated with an additional radio transmitting on the Priority Talkgroup while the scanning radio is scanning. This third radio will be on a remote site with a fourth radio on the Priority Talkgroup at the same site as the scanning radio.

SETUP

RADIO-1 - TG1 (SCANNING)
RADIO-1 - SITE - SITE1
RADIO-2 - TG1
RADIO-2 - SITE - SITE1
RADIO-3 - TG1
RADIO-3 - SITE - SITE2
RADIO-4 - TG2
RADIO-4 - SITE - SITE2
RADIO-5 - TG2
RADIO-5 - SITE - SITE1

VERSION #1.020

2. TEST

Step 1. Verify that RADIO-1 is set to TG1 and in the scan mode of operation and programmed to scan TG1 and TG2 with TG1 as its Priority Monitor Talkgroup.

Step 2. Verify Priority Monitor and the Valid Site setting is set to yes for SITE2.

Step 3. Initiate a Talkgroup Call with RADIO-4 to RADIO-5 and observe that RADIO-1 scans to the talkgroup and receives the call. Keep the call in progress until the completion of the following step.

Step 4. Initiate a Talkgroup Call with RADIO-3 and observe that RADIO-1 reverts to the TG1 and receives the call.

Pass____ Fail____

3.2 SITE TRUNKING FDMA/TDMA MIXED SITES

3.2.1 Site Trunking Indication

1. DESCRIPTION

When a remote site loses its link or does not have a link to the Zone Controller, the affected site will enter "Site Trunking" mode of operation. Radios locked onto this site will be serviced locally within this site's coverage area.

NOTE: If the subscriber does not have the Display option, the "Site Trunking" indication will not be displayed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
Lock the subscribers to SITE 1 if more than one site exists on the system.

VERSION #1.010

2. TEST

Step 1. Place SITE 1 into the Site Trunking mode.

Step 2. Verify that RADIO-1 and RADIO-2 are displaying the "Site Trunking" indication.

Step 3. Return the site to Wide Area Trunking unless the next test requires Site Trunking.

Pass____ Fail____

3.2.2 Talkgroup Call

1. DESCRIPTION

When a site goes into Site Trunking, radios with Talkgroup Call capability will be able to communicate with other members of the same talkgroup at that same site. Members of the same talkgroup at other sites will not be able to monitor those conversations.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 1
RADIO-4 - SITE - SITE 2

Note: All Radios should be "Site Locked"

VERSION #1.010

2. TEST

Step 1. Place SITE 1 into the Site Trunking mode.

Step 2. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1 at SITE 1.

Step 3. Observe that only RADIO-2 will be able to monitor and respond to the call. Note that RADIO-3 and RADIO-4 are not able this monitor the call since the site is not in wide area operation.

Step 4. Initiate a Talkgroup Call with RADIO-3 on TALKGROUP 1 at SITE 2.

Step 5. Observe that only RADIO-4 will be able to monitor and respond to the call.

Pass____ Fail____

3.2.3 Continuous Assignment Updating

1. DESCRIPTION

When a talkgroup is assigned a voice channel, the site controller continues to transmit the channel assignment on the control channel for the duration of the Talkgroup Call. Radios coming into use on the system are automatically sent to voice channels with conversations in progress involving their selected talkgroups.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 1

Note: All Radios should be "Site Locked"

VERSION #1.010

2. TEST

Step 1. Place SITE 1 into the Site Trunking mode.

Step 2. Turn OFF RADIO-1.

Step 3. Initiate a Talkgroup Call using RADIO-2.

Step 4. While the Talkgroup Call is in progress, turn on RADIO-1.

Step 5. Observe that RADIO-1, which was just brought back into service, joins the Talkgroup Call already in progress.

Step 6. Release the PTT of RADIO-2. Switch RADIO-1 to TALKGROUP 2.

Step 7. Initiate a Talkgroup Call using RADIO-2.

Step 8. While the Talkgroup Call is in progress, turn RADIO-1 back to TALKGROUP 1.

Step 9. Observe that RADIO-1, which was just set back to TALKGROUP 1, joins the Talkgroup Call already in progress.

Step 10. Return the site to Wide Area Trunking unless the next test requires Site Trunking.

Pass____ Fail____

3.2.4 End-to-End Call

1. DESCRIPTION

End-to-End Call is a selective calling feature that allows a dispatcher or radio user to carry on one-to-one conversation that is only heard by the 2 parties involved. When a site is in Site Trunking, Radios at the site will only be able to End-to-End Call other radios at the same site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 1

Note: All Radios should be "Site Locked"

VERSION #1.020

2. TEST

Step 1. Place SITE 1 into the Site Trunking mode.

Step 2. Using RADIO-1, press the Call button.

Step 3. Enter the Unit ID of RADIO-2 with the keypad, or scroll to the location where this ID is stored.

Step 4. Press the PTT to initiate the call.

Step 5. Verify that at RADIO-2 only tones are heard and the display indicates that a call has been received.

Step 6. Answer the call at RADIO-2 by pressing the Call/Respond button. Verify its display shows the ID number or alias of the calling unit.

Step 7. Press the PTT switch on RADIO-2 and respond to the call. Note that if you do not press the Call button before pressing PTT, your audio will be heard by all members of the talkgroup, and not by the radio initiating the End-to-End Call.

Step 8. Verify only RADIO-1 hears the audio from RADIO-2.

Step 9. End the End-to-End Call. Return the site to Wide Area Trunking unless the next test requires Site Trunking.

Pass____ Fail____

3.2.5 Dynamic FDMA/TDMA Emergency Alarm and Call

1. DESCRIPTION

Users in life threatening situations can use the Emergency button on the radio to immediately send a signal to the dispatcher and be assigned the next available voice channel if the FDMA/TDMA mode of the call can be supported by the available resource. Otherwise, the first call in the queue that can be supported by the available resources is assigned. To demonstrate this, an Emergency Alarm and Call will be initiated from a subscriber which will be received by a subscriber affiliated at any site of any zone in the system. In this case, the first available resource CANNOT support the FDMA call mode.

Note: In Site Trunking, the mode of all calls is dynamically determined by the Site Controller and Emergency Call operation is always Top of Queue. If the subscriber does not have the Display option, the Emergency ID will not be displayed.

SETUP

RADIO-1 (TDMA) - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-3 (TDMA) - TALKGROUP 2
RADIO-3 - SITE - SITE 1
RADIO-4 (TDMA) - TALKGROUP 3
RADIO-4 - SITE - SITE 1
RADIO-5 (TDMA) - TALKGROUP 4
RADIO-5 SITE - SITE 1
RADIO-8 (FMDA-only) - TALKGROUP 1
RADIO-8 - SITE - SITE 1

Note: All Radios should be "Site Locked"

VERSION #1.010

2. TEST

Step 1. Place SITE 1 into the Site Trunking mode. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.

Step 2. Initiate calls with both RADIO-3 and RADIO-5 and keep these calls in progress until instructed to release.

Step 3. Key RADIO-4 and verify the radio receives a busy tone.

Step 4. Using RADIO-1 send an Emergency Call by pressing the emergency switch and then the PTT switch.

Step 5. Observe that RADIO-1 cannot transmit due to the voice channel being busy. End the call on RADIO-3.

Step 6. Observe that RADIO-4 receives the call back before RADIO-1 and is able to proceed with the call because the available channel resource can only support a TDMA call.

Step 7. Dekey RADIO-5 and RADIO-4. Observe that RADIO-1 receives the callback and is able to proceed with the call.

Step 8. Observe that the display on RADIO-8 denotes an emergency and the unit ID or alias of RADIO-1.

Step 9. Dekey RADIO-1 and end the Emergency Call by holding down the Emergency button on RADIO-1 until an alert tone sounds. Verify RADIO-1 returns to normal operation.

Step 10. Return the site to Wide Area Trunking unless the next test requires Site Trunking.

Pass____ Fail____

3.2.6 Wide Area Recovery

1. DESCRIPTION

A site in Site Trunking will transition to Wide Area Trunking when all failures have been cleared. All subscribers should transition from Site Trunking to Wide Area Trunking and continue to process calls.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 1
RADIO-4 - SITE - SITE 2
CONSOLE-1 - TALKGROUP 1

Note: All Radios should be "Site Locked"

VERSION #1.020

2. TEST

Step 1. Set the status of SITE 1 to Wide Area and clear any system errors that may have placed SITE 1 into Site Trunking.

Step 2. Verify that the status of SITE 1 has transitioned into Wide Area Trunking.

Step 3. Verify that RADIO-1 and RADIO-2 no longer display Site Trunking.

Step 4. Verify Wide Area communications between RADIO-1, RADIO-2, RADIO-3, RADIO-4 and CONSOLE-1.

Pass____ Fail____

3.2.7 Site Trunking Roaming to Wide Area Sites

1. DESCRIPTION

Radios at a site that goes into Site Trunking will attempt to roam to a site in Wide Area Trunking so it is not stranded at a site with limited system resources available. The parameter used by the subcribers to to set a random timer which delays subscribers from flooding an adjacent site with registration requests is the Failure Random Holdoff Time (FRHOT). This is the maximum time the radio may wait before attempting to location register to a new site if the radio switches sites because of a site failure.
NOTE: This feature only works on a multi-site system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

Note: All sites should be in Wide Area at the start of this test. All radios should NOT be "Site Locked". The subscribers should not be configured for "Always Preferred" for this site which would prevent the radios from roaming under site trunking conditions.

VERSION #1.010

2. TEST

Step 1. Set the Failure Random Holdoff Time (FRHOT) setting for SITE 1 to 1 minute. (This can be found in the Unified Network Configurator Wizard.)

Step 2. Initiate a Talkgroup Call between RADIO-1 and RADIO-2.

Step 3. Note the site that the radios are affiliated to.

Step 4. Place the site the radios are affiliated to into Site Trunking.

Step 5. Once RADIO-1 and RADIO-2 have roamed to a wide area site, initiate a Talkgroup Call between RADIO-1 and RADIO-2.

Step 6. Return the FRHOT timer to the original setting.

Step 7. Return the site to Wide Area Trunking unless the next test requires Site Trunking.

Pass____ Fail____

3.3 SYSTEM MANAGEMENT TESTS

3.3.1 Configuration Management - Talkgroup Capabilities

1. DESCRIPTION

The Provision Manager (PM) controls the parameters for all radio users and dispatchers on the system.

Within the Subscriber section, the Talkgroup Configuration Window enables the network manager to tailor SmartZone Talkgroup Capabilities. Emergency, Secure and Priority Monitor are some of the features that can be enabled or disabled. The features that could be unique to the particular user are configured directly in the Talkgroup Configuration Window. The features that could be configured the same for a group of users are placed into records called profiles. The network manager references the profile which contains the desired setup for these features from the Talkgroup Configuration Window.

NOTE: A profile must already exist to be referenced through the Talkgroup Configuration Window but can be modified later if needed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

* Set the "Talkgroup Enabled" flag to YES for TALKGROUP 1 in the PM.

VERSION #1.030

2. TEST

Step 1. Initiate a call from RADIO-1 on TALKGROUP 1. Verify that RADIO-2 hears the RADIO-1 audio.

Step 2. Change the Talkgroup Enabled flag to NO for TALKGROUP 1 via the PM.

Step 3. Initiate a call from RADIO-1 or RADIO-2 on TALKGROUP 1. Verify that neither radio can initiate a call because of the change in status of the Group Enabled Flag of TALKGROUP 1.

Step 4. Initiate an Emergency call from RADIO-1. Verify that both the console (if present) and RADIO-2 can hear the transmission.

Step 5. Dekey RADIO-1.

Step 6. Change the Talkgroup Enabled flag back to YES for TALKGROUP 1 via the PM.

Step 7. Initiate a call from RADIO-1 on TALKGROUP 1. Verify that both the console (if present) and RADIO-2 hear RADIO-1.

Pass____ Fail____

3.3.2 Configuration Management - Subscriber Capabilities

1. DESCRIPTION

The Provisioning Manager (PM) controls the parameters for all radio users and dispatchers on the system. Within the Subscriber section, the Radio User Configuration Window enables the network manager to tailor SmartZone subscribers' capabilities. Multigroup, Secure, Call Alert, End-to-End Call, and Telephone Interconnect are some of the features that can be enabled or disabled. The features that could be unique to the particular user are configured directly in the Radio User Configuration Window. The features that could be configured the same for a group of users are placed into records called profiles. The network manager references the profile which contains the desired setup for these features from the Radio User Configuration Window.

Note - A profile must already exist to be referenced through the Radio Configuration Window but can be modified later if needed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

* Flag both radios to be capable of Call Alert, Private Call, and Dispatch Calls.

* Set the "User Enabled" flag to YES for both RADIO-1 and RADIO-2.

VERSION #1.010

2. TEST

Step 1. Initiate a Call Alert (PAGE) from RADIO-1 to RADIO-2. Verify that RADIO-2 receives the Call Alert.

Step 2. Change the Call Alert Enabled flag to NO for RADIO-1 via the PM.

Step 3. Initiate a Call Alert from RADIO-2 to RADIO-1. Verify that RADIO-2 receives a reject when attempting to Call Alert RADIO-1.

Step 4. Change the Call Alert Enabled flag back to YES for RADIO-1 via the PM.

Step 5. Initiate a Call Alert from RADIO-2 to RADIO-1. Verify that RADIO-1 now receives the Call Alert.

Step 6. Initiate a End-to-End Call (CALL) from RADIO-1 to RADIO-2. Verify that RADIO-2 receives the End-to-End Call.

Step 7. Change the End-to-End Call Enabled flag to NO for RADIO-1 via the PM.

Step 8. Initiate a End-to-End Call from RADIO-2 to RADIO-1. Verify that RADIO-2 receives a reject when attempting to End-to-End Call RADIO-1.

Step 9. Change the End-to-End Call Enabled flag back to YES for RADIO-1 via the PM.

Step 10. Initiate a End-to-End Call from RADIO-2 to RADIO-1. Verify that RADIO-1 now receives the End-to-End Call.

Pass____ Fail____

3.3.3 Configuration Management - Access Permissions

1. DESCRIPTION

In ASTRO releases the Radio System Infrastructure management is done in the Unified Network Configurator (UNC) application. The Unified Network Configurator Wizard (UNCW) also helps to configure the system by having a User interface into the system configuration. Configuration parameters such as Individual and Talkgroup Default Access Permission, and Site Access Denial Type can be manipulated from these applications.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.030

2. TEST

Step 1. Delete the database record for RADIO-1 from the Provisioning Manager so that the system does not have any knowledge of RADIO-1. And distribute the configuration from the Provisioning Manager (i.e. invoke Distribute Configuration Changes operation).

Step 2. Verify the "Individual Default Access Permission" flag is set to "NO". If changes are made, approve the job in Voyence, then Publish Infrastructure Data from the Unified Network Configuration Wizard (UNCW).

Step 3. Initiate a call from RADIO-1 on TALKGROUP 1. Verify that the Radio System rejects the RADIO-1 call request because RADIO-1 has not been defined in the Radio User database.

Step 4. Change the Individual Default Access Permission flag to YES. After approving the job in Voyence, Publish Infrastructure Data from the UNCW.

Step 5. Initiate a call from RADIO-1. Verify that the system permits the RADIO-1 call request because the system grants radio access using default settings.

Step 6. From the Provisioning Manager, configure the RADIO-1 records that was automatically created as a result of the radio's PTT. And distribute the configuration from the Provisioning Manager (i.e. invoke Distribute Configuration Changes operation).

Step 7. Reset the "Individual Default Access Permission" flag to NO. After approving the job in Voyence, Publish Infrastructure Data from the UNCW.

Step 8. Initiate a call from RADIO-1. Verify that the Radio System permits the RADIO-1 call request because RADIO-1 is now a valid user.

Pass____ Fail____

3.3.4 ZoneWatch

1. DESCRIPTION

ZoneWatch is an administration tool for monitoring radio traffic on a system. A system manager can use ZoneWatch to analyze traffic patterns for load distribution and troubleshoot radio and site problems. ZoneWatch is used to view current radio traffic activity for the system. This activity is displayed in graphical format, color-coded for easy identification of the type of activity occurring on the system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 3
RADIO-4 - TALKGROUP 1
RADIO-4 - SITE - SITE 4

VERSION #1.010

2. TEST

Step 1. Verify that ZoneWatch has been configured for the Grid and Multi Site Scroll windows to display system activity.

Step 2. From the PC Application Launcher, select a zone folder.

Step 3. From within that zone, select ZoneWatch.

Step 4. Select the appropriate profile to be able to view the channel usage on the system.

Step 5. Initiate several calls with the radios and observe that the appropriate channel usage information is displayed.

Pass____ Fail____

3.3.5 Affiliation Display

1. DESCRIPTION

Affiliation Display is a Private Radio Network Management (PRNM)application that monitors the mobility of radios for a particular zone. Mobility describes how radio users travel between different sites in a zone and how they communicate with other members of their assigned talkgroup or even with members outside of their talkgroup. A radio can be viewed in more than one zone. As a radio roams from one site to another or changes talkgroups, Affiliation Display updates and displays the affiliation and de-affiliation information for a monitored radio. This information can be useful for the troubleshooting and tracking of radios in the system and for monitoring the movement of traffic within a zone.
The Affiliation Display is divided into three sections: Site Viewer, Talkgroup Viewer, and Radio Viewer.
- The Site Viewer displays the number of talkgroups and number of radios affiliated to that site.
- The Talkgroup Viewer displays how many radios are affiliated to that talkgroup and the number of sites at which the talkgroup has radios affiliated.
- The Radio Viewer window displays affiliation information for a custom list of radios.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2

VERSION #1.010

2. TEST

Step 1. Add RADIO-1,RADIO-2,RADIO-3, and RADIO-4 to the Affiliation Display.

Step 2. Verify that RADIO-1 and RADIO-2 show they are affiliated to SITE 1 and TALKGROUP 1.

Step 3. Verify that RADIO-3 and RADIO-4 show they are affiliated to SITE 2 and TALKGROUP 2.

Step 4. Change the talkgroup of RADIO-1 and RADIO-2 to TALKGROUP 2.

Step 5. Verify that RADIO-1 and RADIO-2's affiliated talkgroup changes to TALKGROUP 2 on the Affiliation Display.

Step 6. Change the site of RADIO-3 and RADIO-4 to SITE 1.

Step 7. Verify that RADIO-3 and RADIO-4's affiliated site changes to SITE 1 on the Affiliation Display.

Pass____ Fail____

3.3.6 Configuration Management - General Timeout Parameters

1. DESCRIPTION

System and call timeout parameters such as Private Call Ring, Group Call Service Timeout, Private Call Hang Time, Emergency Call Hang time, Maximum Group Call Duration and Maximum Private Call Duration can also be manipulated from the Unified Network Configurator (UNC) Wizard.

For this test the Private Call Duration will be limited to one minute. The call will change to transmission trunked after the one minute timer expires at which time the hang timers will come into play. Once the users have discontinued using the system for the Private Call long enough for the hang timers to expire the system will end the call.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.010

2. TEST

Step 1. Initiate a TALKGROUP 1 call from RADIO-1. Verify that the Radio System permits the RADIO-1 call request.

Step 2. In the manager, configure the "Maximum Private Call Duration" to 1 minute and apply.

Step 3. Initiate a End-to-End Call from RADIO-1 to RADIO-2. Continue to converse back and forth using RADIO-1 and RADIO-2,

Step 4. Verify that after one minute elapses, the system will transmission trunk the End-to-End Call because the maximum call duration has been exceeded. Once the hang time timer has expired the call will be terminated.

Step 5. Reset the Private Call Maximum Call Duration setting to be 10 minutes (default).

Pass____ Fail____

3.3.7 Site Wide Area Trunking to Site Trunking State using the Unified Event Manager

1. DESCRIPTION

Through the Unified Event Manager (UEM), the system user can run diagnostics that change the "Trunking State" of a site. The effect of the diagnostic is displayed on the UEM.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1 (Site Locked)
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 1 (Site Locked)

NMclient01 - UEM session up and running in the alarms view.

VERSION #1.030

2. TEST

Step 1. Initiate a Wide Area Call with RADIO-1 in TALKGROUP 1. Verify RADIO-2 and RADIO-3 will be able to monitor and respond to the call.

Step 2. Select SITE 1 in the Network Database > Sites option in the tree view. Right click and select "Issue Command". Select "Site Trunking" and apply to put the site in Site Trunking mode.

Step 3. Observe that the UEM alarms view shows that the site is now in Site Trunking and is User Requested.

Step 4. Verify ZoneWatch (if applicable) no longer shows the SITE 1 trunking activity. Also verify that RADIO-1 can no longer communicate with RADIO-2 but can still communicate with RADIO-3.

Step 5. Place the site back into Wide Area Trunking using the "Issue command" feature from UEM. Verify that the site returns to Wide Area mode using the UEM.

Step 6. Verify communications between RADIO-1, RADIO-2 and RADIO-3.

Pass____ Fail____

3.3.8 Unified Event Manager - Diagnostics - ASTRO Repeater Site

1. DESCRIPTION

The purpose of this test is to demonstrate diagnostic commands can be sent to a Radio Frequency (RF) site and the proper status is reported at the Unified Event Manager (UEM).

All commands are initiated from the UEM.

Standalone and MultiSite configurations are tested.

SETUP

NMclient01 - UEM session up and running in the Network Database view.

VERSION #1.030

2. TEST

Step 1. From the UEM, right click on an ASTRO Repeater Site managed resource and select the Command option.

Step 2. The command window opens for the ASTRO repeater Site managed resource with the following commands available: Site Trunking, Site Off, Wide Trunking, and Site Failsoft.

Step 3. Select Site Trunking and click the Apply button.

Step 4. The command execution status is displayed in the command window. After the command is executed, the site enters site trunking mode. The event is displayed in the Network Events Browser. An alarm is displayed in the Alarms Browser.

Step 5. Select Site Off and click the Apply button.

Step 6. The command execution status is displayed in the command window. After the command is executed, the site enters site off mode. The event is displayed in the Network Events Browser. An alarm is displayed in the Alarms Browser.

Step 7. Select Wide Trunking and click the Apply button.

Step 8. The command execution status is displayed in the command window. After the command is executed, the site enters wide trunking mode. The event is displayed in the Network Events Browser.

Pass____ Fail____

3.3.9 Unified Network Configurator Device Management - Site Parameter

1. DESCRIPTION

The Unified Network Configurator (UNC) allows users to perform various functions to managed devices on the system. This test will cover the modification of a parameter at a site.

For this test, the Site Alias parameter will be modified on all radio system devices at the site.

SETUP

If the UNC is not open, double-click the UNC shortcut (UNC) on the desktop, and a Smart Assurance Network Configuration Manager client session will launch. When prompted, use the Login dialog box to login to the UNC using the appropriate username and password.
If the UNC Wizard is not open, double-click the UNC Wizard (UNCW) shortcut on the desktop, and a UNC Wizard client session will launch. When prompted, use the Login dialog box to login to the UNC Wizard using the appropriate username and password.

VERSION #1.030

2. TEST

Step 1. Using the UNC Wizard, select a RF Repeater site or Simulcast Subsite to update. (Note: Changing an entire Simulcast Cell may take a considerable amount of time.)

Step 2. Change the Site Alias parameter to a new value and click the Submit button.

Step 3. From the tools menu of the UNC client session, open the Schedule Manager. Configuration remedy jobs are immediately added to the Schedule Manager with a status of Pending for all affected target devices.

Step 4. Highlight the pending Remedy jobs and approve them in the Schedule Manager. The remedy jobs are approved and indicate a status of running in the Schedule Manager.

Step 5. Refresh the Schedule Manager view until the jobs are completed.

Step 6. View the current configuration information for the devices at the site, and verify that the Site Alias has been updated in the devices current configuration.

Step 7. Return the site alias to the correct value.

Pass____ Fail____

3.3.10 License Manager – Session Force Release

1. DESCRIPTION

Under certain scenarios, active sessions may need to be released. If this need occurs, the sessions can be released from the License Manager through use of the Force Release functionality.

In addition to releasing the sessions from the Session tab in the License Manager, the licenses can be managed by left clicking on a license with active sessions under the Licenses tab.

Note: Once a user session is released, and if there are additional licenses available, the session for the license that was released can be renewed and will remain active. In addition, the releasing of licenses is only permitted for users belonging to the licadmin group.

SETUP

A user session that can be terminated is needed to run this test.

VERSION #1.010

2. TEST

Step 1. Start the License Manager application in the zone that is applicable for the target session.

Step 2. Under <Sessions> on the top bar on the License Manager application, you can view the sessions that are currently active in the system.

Step 3. Choose one of the active sessions to release.

Step 4. For the session to be released, select <Release> on the right side of the screen.

Step 5. When the Force Release window appears, select <Yes>.

Step 6. After the Force Release window disappears, refresh the screen.

Step 7. Demonstrate that the released license is no longer listed as an active session under the License Manager.

Pass____ Fail____

3.3.11 License Manager – View and Export Licenses

1. DESCRIPTION

The License Manager is used to manage Capacity, Feature, Session, and Trial licenses in the system. The License Manager provides a consolidated view of software licenses in the system.

The License Manager runs on a Zone basis. The system level licenses are contained in the License Manager in the zone that is colocated with the system servers (Eg. UCS) (typically zone 1).

SETUP

No specific setup is required for this test.

VERSION #1.020

2. TEST

Step 1. Start the License Manager application

Step 2. Under <Capacity Licenses>, you can view the capacity usage in the system (ex: Trunked Radio User). Note the Purchased Quantity and Used Quantity.

Step 3. Under <Feature Licenses>, you can view which features have been purchased on the system (ex: Provisioning Manager Interface).

Step 4. Under <Session Licenses>, you can view the session licenses in the system (ex: Zone Watch). Note the Purchased Quantity and Used Quantity.

Step 5. Under <Licenses> on the top bar on the License Manager application, you can view the licenses applicable for this system.

Step 6. Select <Export> in the upper right hand corner of the License Manager application.

Step 7. When the selector window appears, select <Save> to save the exported file.

Step 8. Once the file is saved, it can be opened and viewed (ex: Excel) and verify that the exported license file matches the licenses as specified in the License Manager.

Pass____ Fail____

3.4 FAULT MANAGEMENT

3.4.1 Unified Event Manager - Base Views

1. DESCRIPTION

The Unified Event Manager (UEM) in its base configuration provides a number of views. The purpose of this test is to demonstrate the key views available from the UEM.

The Physical Summary and Detail View (Physical Map) and Service Summary and Detail View (Service Map) in previous releases are deprecated and are replaced by the Zone Map. Custom views can be saved and retrieved by other NM Client users.

SETUP

NMclient01 - UEM session up and running.

VERSION #1.010

2. TEST

Step 1. Alarms View: In the navigation pane expand Fault Management and select Alarms. The view displays active alarms for managed resources, displaying impacted managed resources and specific objects on the managed resource along with selected alarm properties.

Step 2. Alarm View Search: Customize the Active Alarms display by selecting the View option from the menu bar, then select Search. Perform a Managed Resource search for channels, site controllers and routers by entering "Contains" and ch, sc, and z00 respectively in the search fields to perform the three separate searches. For each of the three searches a filtered alarm view is displayed that contains alarms for the appropriate device in the search.

Step 3. Network Events View: In the navigation pane expand Fault Management and select Network Events. The view displays recent events reported for managed resources, displaying impacted managed resources and specific object on the managed resource along with selected event properties. Alarming events are base for creating alarm objects.

Step 4. Physical Summary View: In the navigation pane expand Zone Views and Physical, then select Physical Summary View. The Physical Summary View provides an aggregated alarm severity status of the devices located at all subnets in the Zone.

Step 5. Service Summary View: In the navigation pane expand Zone Views and Service, then select Service Summary View. The Service Summary View provides a quick summary of the service status of sites in a Zone, including access to Channel status.

Step 6. Zone Map: In the navigation pane, expand Zone Views and select Zone Map. The Zone Map view provides an aggregated alarm severity status of the devices located at discovered sites in the Zone.

Step 7. Network Database: In the navigation pane select Network Database. The Network Database displays a list of all discovered Managed Resources and Sites. The display includes properties of each

resource as well as overall severity of all objects and/or sub resources

Pass____ Fail____

3.5 RADIO CONTROL MANAGER (RCM) FEATURES

3.5.1 Dynamic Regrouping

1. DESCRIPTION

Dynamic Regrouping allows the Radio Control Manager (RCM) to assign individual radios operating in different talkgroups to a temporary talkgroup via the Regroup command. Network managers or supervisors can override individual radio talkgroup selections by steering regrouped subscribers to a new talkgroup containing users which need to communicate on a temporary basis. After receiving a Regroup command, a radio will ignore the current setting of the talkgroup selector and move to the target talkgroup specified in the Regroup command. Unless the supervisor issues a LOCK command, the radio user can deselect the target talkgroup by selecting another talkgroup using the radio selector. A unique location on the radio selector is reserved for the target talkgroup following a Regroup command.

Dynamic Regrouping assignments can be initiated rapidly, but not instantaneously. Regrouping is best suited for planned activities or occasional changes from normal routines. It is not intended for immediate responses such as high speed chases or for a rapid deployment on a per incident basis.

Regrouped radios receiving a second Regroup command will move to the new target talkgroup specified in the second command. When a regrouped radio receives a Regroup command, all information pertaining to the previous Regroup command is lost. A Cancel Regroup command or a Revert returns an individual radio to its normal operation.

Note - RCM user must be attached to primary and target talkgroup.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1
RADIO-3 - TALKGROUP 2
RADIO-4 - TALKGROUP 2

2. TEST

Step 1. With the RCM open from the main Command tab click on the “+” button . Choose Regroup.

Step 2. Enter TALKGROUP 3 in the target field.

Step 3. Enter the IDs or aliases of RADIO-1, RADIO-2, RADIO-3 and RADIO-4.

Step 4. Once all desired radio information is entered and appears in the command window click the submit to initiate the command.

Step 5. Observe all radios are regrouped and are able to communicate on TALKGROUP 3.

Step 6. Switch the Subscriber to the Dynamic Regroup channel.

Step 7. Observe that the radios are able to select different talkgroups and are not locked onto the regrouped mode. Note: The Talkgroup selector knob has to be set to the dynamic regroup position before switching to any other talkgroup.

Step 8. Observe that the Regroup task appears in the Command tab.

Step 9. Issue a Selector Lock command all four radios and verify their selectors have been locked.

Step 10. Revert both commands and verify the radios have returned to normal operation.

Pass____ Fail____

VERSION #1.030

3.5.2 Selective Radio Inhibit

1. DESCRIPTION

The INHIBIT command issued by the Radio Control Manager (RCM) disables a radio, preventing it from transmitting or receiving any audio. All of the radio's functionality ceases while a radio is inhibited by the RCM. Once inhibited, the radio cannot be used to monitor voice channels or for any other radio user initiated activity. Note that an inhibited radio still monitors the control channel so that it can be re-enabled with the Cancel Inhibit command. Upon receiving the Cancel Inhibit command from the RCM, the radio returns to its normal operation.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

VERSION #1.030

2. TEST

Step 1. With the RCM open from the main Command tab click on the “+” button .

Step 2. Enter the IDs or aliases of RADIO-1.

Step 3. Select "Selective Inhibit" button.

Step 4. Once all desired radio information is entered and appears in the command window click the submit to initiate the command.

Step 5. Observe RADIO-1 is inhibited and appears to be dead.

Step 6. Observe that the Inhibit task appears in the Command tab.

Step 7. Cancel the Inhibit by selecting the task in the Command tab and clicking the Revert button to submit the task.

Step 8. Observe that the Cancel Inhibit task appears in the Command tab and that RADIO-1 is returned to normal operation.

Pass____ Fail____

3.6 INTEGRATED VOICE AND DATA (IV & D)

3.6.1 Outbound Data Transfer

1. DESCRIPTION

This test will demonstrate the transfer of a short message from the host computer on the Customer Enterprise Network (CEN) to a mobile user terminal.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
Host computer - Connected
MDT-1 - Connected
Note: RADIO-1 must be affiliated to the system and have a mobile data terminal (MDT) connected.

VERSION #1.010

2. TEST

Step 1. From a Host computer on the Customer Enterprise Network (CEN), generate an outbound message to MDT-1, using the ping command from the MS-DOS prompt: ping -w 4000 <destination IP address>

Step 2. Verify that the Host computer receives a response from MDT-1.

Pass____ Fail____

3.7 LOCATION SERVICE

3.7.1 Location Information Received

1. DESCRIPTION

The Location system will receive information on the provisioned subscribers.

Note: Location requires reception of a clear GPS signal which may not always be possible in the CCSi environment. Location tests are not recommended for staging but rather for the final destination when it is possible to perform outdoor tests more easily.

SETUP

Location services installed and configured for 30 second updates

RADIO-1 - GPS-enabled and provisioned with Location Service

Note: It is possible that an external GPS antenna may be required if testing inside CCSi.

VERSION #1.040

2. TEST

Step 1. From the device list on the location client expand the device details for RADIO-1.

Step 2. Verify that the Latitude, Longitude and update time are shown for RADIO-1.

Step 3. Move the RADIO-1 location enough to cause the RADIO to report a new GPS location. Verify that the new location information is received.

Pass____ Fail____

3.7.2 Location Updates

1. DESCRIPTION

The Location Service send updates at configured time intervals. These intervals can be updated which will send a message to the subscriber updating the reporting parameters.

Note: Location requires reception of a clear GPS signal which may not always be possible in the CCSi environment. Location tests are not recommended for staging but rather for the final destination when it is possible to perform outdoor tests more easily.

SETUP

RADIO-1 - GPS enabled and provisioned on the Location Service

Note: It is possible that an external GPS antenna may be required if testing inside CCSi.

VERSION #1.040

2. TEST

Step 1. From the device list, expand the device details for RADIO-1. This will display the Latitude, Longitude and the update time.

Step 2. In the UNS Configuration Manager, set the Device Interval for RADIO-1 and update the parameter to 30 seconds.

Step 3. Verify that RADIO-1 is updating every 30 seconds by looking at the device list.

Pass____ Fail____

3.8 TELEPHONE INTERCONNECT

3.8.1 Landline Telephone To Subscriber Interconnect over VoIP Interface

1. DESCRIPTION

This test verifies the capability to receive phone calls from a landline telephone on a radio, where a landline telephone is connected to the interconnect system via a VoIP interface. Note the VoIP phone is not connected to the IP-PBX that is part of the Interconnect subsystem, rather the VoIP phone is connected to a second IP-PBX that is usually owned by customer. The dialing method in this test is overdial, i.e. a landline telephone user calls a central telephone number first, then when prompted, enters a subscriber extension number to complete the call.

Some radios feature phone list capability with programmable alias names which may be assigned. Radios with keypad operation may also be programmed for unlimited dialing capability.

Since the telephone interconnect functionality depends upon the Private Branch Exchange (PBX) unit, sites must be Wide Area Trunking in order to support this telephone interconnect function. In addition, radios cannot be site-locked to a specific site before initiating a telephone interconnect call.

Note : A radio can be setup to use either the Private Branch Exchange (PBX) in the zone it is affiliated with or a PBX in a default zone.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1

IP-Analog Media Gateway connects a landline telephone to the IP-PBX
Telephony firewall is setup between ASTRO system (including 3rd party IP-PBX) and outside IP world

VERSION #1.010

2. TEST

Step 1. From the test telephone line, dial the telephone number of a phone line connected to the IP-PBX.

Step 2. Confirm that an automated voice is heard in the telephone prompting the landline caller to enter the eight-digit unit ID of the target radio.

Step 3. Enter the eight-digit radio ID of RADIO-1.

Step 4. Confirm that ringing is heard on RADIO-1 only and that the display indicates a phone call is being received.

Step 5. Press the Telephone Interconnect button on RADIO-1 to answer the landline-to-subscriber interconnect call.

Step 6. Verify that the landline-to-subscriber call can be completed, and the radio and landline users can communicate.

Step 7. Confirm that RADIO-2 does not listen to the call.

Step 8. Hang up the interconnect call.

Pass____ Fail____

3.8.2 Subscriber To Landline Telephone Interconnect over VoIP Interface

1. DESCRIPTION

This test verifies the capability to make phone calls to a landline telephone from a radio, where landline telephone is connected to the interconnect system via a VoIP interface. Note the VoIP phone is not connected to the IP-PBX that is part of the Interconnect subsystem, rather the VoIP phone is connected to a second IP-PBX that is usually owned by customer. The dialing method in this test is direct dial, i.e. no DTMF overdialing is involved.

Some radios feature phone list capability with programmable alias names which may be assigned. Radios with keypad operation may also be programmed for unlimited dialing capability.

Since the telephone interconnect functionality depends upon the Private Branch Exchange (PBX) unit, sites must be Wide Area Trunking in order to support this telephone interconnect function. In addition, radios cannot be site-locked to a specific site before initiating a telephone interconnect call.

Note : A radio can be setup to use either the Private Branch Exchange (PBX) in the zone it is affiliated with or a PBX in a default zone.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1

IP-Analog Media Gateway connects a landline telephone to the IP-PBX
Telephony firewall is setup between ASTRO system (including 3rd party IP-PBX) and outside IP world

No specific site affiliation is required to begin this test.

VERSION #1.010

2. TEST

Step 1. Using RADIO-1, initiate a telephone call to a test telephone phone number.

Step 2. Verify the telephone rings.

Step 3. Pickup the phone and confirm that RADIO-1 and the landline user can communicate.

Step 4. Confirm that the landline user hears a tone after each radio transmission signifying the half-duplex nature of the interconnect call.

Step 5. Confirm that RADIO-2 does not listen to the call.

Step 6. Hang up the interconnect call.

Pass____ Fail____

3.9 MCC 7100/7500 TRUNKED RESOURCES

3.9.1 Talkgroup Selection and Call

1. DESCRIPTION

The Talkgroup Call is the primary level of organization for communications on a trunked radio system. Dispatchers with Talkgroup Call capability will be able to communicate with other members of the same talkgroup. This provides the effect of an assigned channel down to the talkgroup level. When a Talkgroup Call is initiated from a subscriber unit, the call is indicated on each dispatch operator position that has a channel control resource associated with the unit's channel/talkgroup.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 2
RADIO-3 - TALKGROUP 1
RADIO-4 - TALKGROUP 2
CONSOLE-1 - TALKGROUP 1
CONSOLE-2 - TALKGROUP 2

VERSION #1.010

2. TEST

Step 1. Initiate a wide area call from CONSOLE-1 on TALKGROUP 1.

Step 2. Observe that RADIO-1 and RADIO-3 will be able to monitor the call. Dekey the console and have either radio respond to the call.

Step 3. Observe that all consoles with TALKGROUP 1 can monitor both sides of the conversation.

Step 4. Initiate a wide area call from CONSOLE-2 on TALKGROUP 2.

Step 5. Observe that RADIO-2 and RADIO-4 will be able to monitor the call. Dekey the console and have either radio respond to the call.

Step 6. Observe that all consoles with TALKGROUP 2 can monitor both sides of the conversation.

Pass____ Fail____

3.9.2 PTT Unit ID/Alias Display

1. DESCRIPTION

Console operator positions contain various resources such as talkgroup, multigroup, End-to-End Call which enables the dispatcher to communicate with the subscriber units. If activity occurs on one of these operator position resources, the unit ID or associated alias of the initiating radio appears at the console resource.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1
CONSOLE-1 - TALKGROUP 1
CONSOLE-2 - TALKGROUP 1

VERSION #1.010

2. TEST

Step 1. Select the resource for TALKGROUP 1 on CONSOLE-1.

Step 2. Initiate a call on TALKGROUP 1 from RADIO-2 and observe that the alias is seen at CONSOLE-1 in the resource window as well as in the Activity Log window.

Step 3. Initiate a call from RADIO-1 and observe that the alias of RADIO-1 is seen at CONSOLE-1 in the resource window as well as in the Activity Log window.

Step 4. Modify RADIO-2's alias. Make sure to give enough time for the alias change to propagate to the Zone Controller.

Step 5. Initiate a call from RADIO-2 and observe the new alias of RADIO-2 is seen at CONSOLE-1 in the list in the resource window as well as in the Activity Log window.

Step 6. Return RADIO-2's alias to its original state.

Pass____ Fail____

3.9.3 Talkgroup Patch

1. DESCRIPTION

Talkgroup Patch allows a dispatcher to merge several talkgroups together on one voice channel to participate in a single conversation. This can be used for situations involving two or more talkgroups that need to communicate with each other.
Using the Patch feature, the console operator can talk and listen to all of the selected talkgroups grouped; in addition, the members of the individual talkgroups can also talk or listen to members of other talkgroups. Patched talkgroups can communicate with the console dispatcher and other members of different talkgroups because of the "supergroup" nature of the Patch feature.

NOTE : If "secure" and "clear" resources are patched together, one repeater for each mode may be assigned per site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 2
RADIO-3 - TALKGROUP 1
RADIO-4 - TALKGROUP 2
CONSOLE-1 - TALKGROUP 1 and TALKGROUP 2

Note: All 4 Radios must have the same home zone.

VERSION #1.010

2. TEST

Step 1. Using CONSOLE-1 create a patch between TALKGROUP 1 and TALKGROUP 2.

Step 2. Initiate a patch call from CONSOLE-1.

Step 3. Verify RADIO-1, RADIO-2, RADIO-3, and RADIO-4 can monitor the call.

Step 4. Initiate several calls between the radios and verify successful communication.

Step 5. Dissolve the patch created in step 1.

Pass____ Fail____

3.9.4 Console Initiated End-to-End Call to Subscriber

1. DESCRIPTION

End-to-End Conversation is a selective calling feature which allows a dispatcher or radio user to carry on one-to-one conversation that is heard only by the two parties involved. Subscriber units receiving a End-to-End call will sound an alert tone. As with other call types, End-to-End Calls operate across sites as well as within the same site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1
CONSOLE-1 - TALKGROUP 1

VERSION #1.020

2. TEST

Step 1. Using CONSOLE-1, select the "PRIVATE-CALL" tile and click the Call function.

Step 2. Select the unit to be End-to-End Called, in this case RADIO-1. (or select the numeric keypad and enter the Unit ID to be End-to-End Called.)

Step 3. Click the Send button.

Step 4. Answer the End-to-End Call with RADIO-1 and respond to the console.

Step 5. Verify RADIO-2 does not hear the End-to-End conversation.

Step 6. After completing the End-to-End Call, return to the normal talkgroup mode.

Pass____ Fail____

3.9.5 Multigroup Call

1. DESCRIPTION

This trunking feature allows an equipped console operator position to transmit an announcement to several different talkgroups simultaneously. As with Talkgroup Calls, multigroup calls operate across sites as well as within the same site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 2
RADIO-3 - RANDOM
CONSOLE-1 - ATG 1

Note: TALKGROUP 1 and TALKGROUP 2 are members of ATG 1. RANDOM is any talkgroup not a member of ATG 1.

VERSION #1.010

2. TEST

Step 1. Using CONSOLE-1, select the ATG 1 resource.

Step 2. Initiate the Multigroup Call from CONSOLE-1.

Step 3. Observe that RADIO-1 and RADIO-2 receive the Multigroup Call.

Step 4. Verify that RADIO-3 does not receive the Multigroup Call because it is not a member of ATG 1.

Step 5. Answer the Multigroup Call using RADIO-1 and observe CONSOLE-1 receives the response.

Step 6. Verify that if the call is answered within the repeater hang time, the console will receive the call on the ATG 1 resource tile, otherwise the console will receive the call on the TALKGROUP 1 tile.

Step 7. Verify that if the call is answered within the repeater hang time, RADIO-2 will monitor the call.

Pass____ Fail____

3.9.6 Emergency Alarm and Call Display Description

1. DESCRIPTION

Users in life threatening situations can use the emergency button on the radio to send an audible alarm and a visual alarm signal to a console operator in order to request immediate system access to a voice channel for an emergency call. An emergency alarm begins after the radio user presses the radio's emergency button. Pressing the emergency button places the radio in "emergency mode". To begin an emergency call, the radio user must press the radio's PTT button while in "emergency mode." The assigned voice channel will be dedicated to the emergency caller's talkgroup for an extended period of time, equal to the Message Hang Time plus the Emergency Hang Time. As with other call types, emergency calls can operate across sites as well as within the same site.

SETUP

RADIO-1 - TALKGROUP 1
CONSOLE-1 - TALKGROUP 1
CONSOLE-2 - TALKGROUP 1

VERSION #1.020

2. TEST

Step 1. Initiate an Emergency Alarm from RADIO-1.

Step 2. Observe the Emergency from RADIO-1 is received at CONSOLE-1 for TALKGROUP 1 and the text in the talkgroup resource indicates the trigger condition for the emergency when applicable (mandown condition, vehicle crash or vest pierce).

Step 3. Acknowledge the Emergency at the operator position. Verify CONSOLE-2 receives notification that the call has been acknowledged.

Step 4. Initiate a call with RADIO-1 to initiate an Emergency call.

Step 5. Observe CONSOLE-1 and CONSOLE-2 can monitor RADIO-1

Step 6. Clear the Emergency from CONSOLE-1 on TALKGROUP 1.

Step 7. End the Emergency Alarm from RADIO-1.

Pass____ Fail____

3.9.7 Talkgroup Selection and Call – Secure

1. DESCRIPTION

The Talkgroup Call is the primary level of organization for communications on a trunked radio system. Dispatchers with Talkgroup Call capability will be able to communicate with other members of the same talkgroup. This provides the effect of an assigned channel down to the talkgroup level. When a Talkgroup Call is initiated from a subscriber unit, the call is indicated on each dispatch operator position that has a channel control resource associated with the unit's channel/talkgroup.
Digital encryption is used so only properly equipped and configured subscribers can monitor the conversation. A "Key" is used to encrypt the transmit audio. Only radios and Consoles with the same "Key" can decrypt the audio and listen to it.

SETUP

RADIO-1 - TG1 (Secure TX Mode)
RADIO-2 - TG2 (Secure TX Mode)
RADIO-3 - TG2 (No Keys)
RADIO-4 - TG1 (Clear TX Mode with Keys loaded)
CONSOLE-1 - TG1 and TG2 (Secure TX Mode)

VERSION #1.020

2. TEST

Step 1. Initiate a wide area secure call from CONSOLE-1 on TG1.

Step 2. Verify RADIO-1 can monitor and respond to the secure call.

Step 3. Verify RADIO-4 can monitor and respond to the secure call because even though it is in clear mode the correct encryption keys are loaded for the secure call.

Step 4. Initiate a wide area secure call from CONSOLE-1 on TG2.

Step 5. Verify that RADIO-2 can monitor and respond to the secure call. Note that RADIO-3 cannot monitor the call.

Pass____ Fail____

3.10 SYSTEM RELIABILITY FEATURES

3.10.1 Redundant Zone Controller Switching – Manual Switchover

1. DESCRIPTION

In a non-Dynamic System Resilience (DSR) configuration the Zone Controller subsystem uses two Zone Controllers in a redundant configuration. The standby Zone Controller is made active either upon the loss of the active Zone Controller or upon a user command from the Unified Network Configurator. In a DSR configuration there are 4 Zone Controllers in a redundant configuration. Any one of the 4 could be active to keep the Zone Sites in Wide Area Trunking. If using DSR configuration the Unified Event Manager (UEM) will report the Zone Controller switchover in both UEMs.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 3 (In another Zone if available, otherwise set to a random site in the same Zone.)

VERSION #1.010

2. TEST

Step 1. Verify the state of the current Zone Controllers is Active or Standby in the Unified Network Configurator (UNC). (There will be 2 Zone Controllers in single Zone or 4 in the case of DSR configured zones.)

Step 2. Using the Unified Network Configurator, switch the Standby Zone Controller to the Active state.

Step 3. Verify using UNC, UEM and ZoneWatch (if applicable) that the standby Zone Controller becomes active and brings all sites back wide. Wait for the Radios to settle out the site affiliations.

Step 4. Key RADIO-1 and verify that RADIO-2 and RADIO-3 hear the audio.

Step 5. End the call from RADIO-1.

Step 6. Verify that Zone Controller that was previously “Active” comes back up to an “Enabled” and “Standby” state.

Pass____ Fail____

3.10.2 Redundant Zone Controller Switching/Automatic Switchover

1. DESCRIPTION

In a non-DSR configuration the Zone Controller subsystem uses two Zone Controllers in a redundant configuration. The backup Zone Controller is made active either upon the loss of the active ZC or upon a user command from the Unified Network Configurator (UNC). In a DSR configuration there are 4 Zone Controllers in a redundant configuration. Any one of the 4 could be active to keep the Zone Sites in Wide Area Trunking. If using the Dynamic Resilience Zone configuration the Unified Event Manager will report the Zone Controller switchover in both Unified Event Managers (UEM).

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - Site3 (Site3 should be in another Zone if applicable.)

* The Zone Controllers should be successfully synchronized before performing this procedure.

VERSION #1.030

2. TEST

Step 1. Verify the state of the current Zone Controllers is Active or Standby in the Unified Network Configurator (UNC). (There will be 2 Zone Controllers in single Zone or 4 in the case of DSR zones.)

Step 2. Reset the active Zone Controller application via the Unified Event Manager (UEM) diagnostic.

Step 3. Verify using UNC, UEM and ZoneWatch (if applicable) that the standby Zone Controller becomes active and brings all sites back wide. Wait for the Radios to settle out the site affiliations.

Step 4. Key RADIO-1 and verify that RADIO-2 and RADIO-3 hear the audio.

Step 5. End the call from RADIO-1.

Step 6. Verify that Zone Controller that was reset comes back up to a “Standby” state.

Pass____ Fail____

3.10.3 Redundant Site Controller Switching - User initiated

1. DESCRIPTION

The Site Controller subsystem uses two Site Controllers in a redundant configuration. The backup Site Controller is made active either upon the loss of the active Site Controller or upon a user initiated command from the Unified Event Manager (UEM).

SETUP

RADIO-1 - TG1
RADIO-1 - SITE - SITE1 (Site Locked)
RADIO-2 - TG1
RADIO-2 - SITE - SITE1 (Site Locked)
RADIO-3 - TG1
RADIO-3 - SITE - SITE1 (Site Locked)

All Radios should be "Site Locked".

VERSION #1.030

2. TEST

Step 1. Initiate a call using RADIO-1. Verify RADIO-2 and RADIO-3 can communicate with RADIO-1.

Step 2. Verify both Site Controllers are enabled by viewing the site status in the UEM. Both Site Controllers should have a green, normal indication.

Step 3. Initiate a user disabled on the active Site Controller using the UEM.

Step 4. Verify that the backup Site Controller becomes active by viewing the status LED on the front panel of the Site Controller and the UEM.

Step 5. Key RADIO-1 and verify that RADIO-2 and RADIO-3 hear the audio.

Step 6. End the call from RADIO-1.

Step 7. Enable the user disabled Site Controller and verify both are in Normal state.

Pass____ Fail____

3.10.4 Multiple Control Channels

1. DESCRIPTION

A maximum of four channels are eligible for assignment as control channel at each site. In the event that the assigned control channel fails at any remote site, the Zone Controller automatically selects one of the other control capable channels as the active control channel for that site. A Control Channel Preference Level can be used to rank the control capable channels where 1 is the highest ranking and 4 the lowest.

SETUP

RADIO-1 - TG1
RADIO-1 - SITE - SITE1
RADIO-2 - TG1
RADIO-2 - SITE - SITE1
RADIO-3 - TG2
RADIO-3 - SITE - SITE1
RADIO-4 - TG2
RADIO-4 - SITE - SITE1

VERSION #1.030

2. TEST

Step 1. Initiate a Talkgroup Call with RADIO-1 on TG1.

Step 2. Observe that only RADIO-2 will be able to monitor and respond to the call.

Step 3. Initiate a Talkgroup Call with RADIO-3 on TG2.

Step 4. Observe that only RADIO-4 will be able to monitor and respond to the call.

Step 5. Power off the control channel at SITE1.

Step 6. Observe that the control channel rotates to the next available channel capable of acting as a control channel.

Step 7. Initiate a Talkgroup Call with RADIO-1 on TG1.

Step 8. Observe that only RADIO-2 will be able to monitor and respond to the call.

Step 9. Initiate a Talkgroup Call with RADIO-3 on TG2.

Step 10. Observe that only RADIO-4 will be able to monitor and respond to the call. Power up the channel previously powered off to return the system to normal operation.

Pass____ Fail____

3.10.5 Site Failsoft

1. DESCRIPTION

Failure of all control channels, failure of all voice channels, or failure of the site controller will cause a site (RF Subsystem) to enter failsoft operation. Subscribers can be programmed to operate in failsoft by talkgroup; to search its list of control channel frequencies in failsoft; or to disable failsoft altogether. When a site enters failsoft, a radio programmed for failsoft by talkgroup will first look for a specific failsoft channel dictated by the selected talkgroup. Since many systems have different frequencies across sites, if the radio is unable to find the talkgroup's failsoft channel the radio will instead operate in the control channel search failsoft mode. A radio programmed or needing to search control channels for failsoft frequencies will lock onto the first control channel in its control channel list.

Note: Radios should not be site locked when in failsoft mode. The radio will not check the full list of 64 control channels programmed into the radio's code plug. All radios should be programmed to have the same sequence of control channel frequencies.
Note: The subscribers MUST be SmartZone capable.

SETUP

RADIO-1 - TG1
RADIO-1 - SITE - SITE1
RADIO-2 - TG1
RADIO-2 - SITE - SITE1
RADIO-3 - TG2
RADIO-3 - SITE - SITE1
RADIO-4 - TG2
RADIO-4 - SITE - SITE1
* Program the Radios for failsoft operation by talkgroup. TG1 should use a different channel for failsoft than TG2 and neither should be a control channel.
* In order to prevent roaming turn off all sites except the site under test.

VERSION #1.030

2. TEST

Step 1. Using the Unified Event Manager (UEM), place the subsystem into failsoft mode.

Step 2. Verify that the Radios emits a failsoft tone approximately once every ten seconds.

Step 3. Initiate a Talkgroup Call from RADIO-1 while in failsoft mode.

Step 4. Verify that only RADIO-2 can hear RADIO-1.

Step 5. Dekey RADIO-1 and power down the failsoft channel associated with TG1.

Step 6. Key RADIO-1 and verify RADIO-2 can still monitor the call but the other radios cannot.

Step 7. Dekey RADIO-1 and initiate a Talkgroup Call from RADIO-3.

Step 8. Verify that only RADIO-4 can hear RADIO-3.

Pass____ Fail____

3.11 OVER THE AIR REKEYING (OTAR)

3.11.1 Encrypted Hello

1. DESCRIPTION

The KMF operator can send an encrypted message to any radio to confirm that radio is on the system and that its encryption services are functioning.

Note: The devices under test must have a valid air address registered with the KMF and must be accessible on the data system.

SETUP

RADIO-1 - TALKGROUP 1
Note: The radio must be current in the KMF

VERSION #1.020

2. TEST

Step 1. Go to the Radio Management page of the KMF

Step 2. Select RADIO-1 from the list.

Step 3. Initiate an Encrypted Hello operation

Step 4. Go to the Operation Status page of KMF, verify that RADIO-1's Encrypted Hello operation is shown. The operation is complete when the Operation Status is completed.

Pass____ Fail____

3.11.2 Full Update to Subscriber

1. DESCRIPTION

The entire set of encryption keys (in addition to other state parameters) are sent to a radio using the Full Unit Update command.

Note: The devices under test must have a valid air address registered with the KMF and must be accessible on the data system.

SETUP

RADIO-1 - TALKGROUP 1 (Secure Mode)
RADIO-2 - TALKGROUP 1 (Secure Mode)
RADIO-2 will be a reference radio.

Note: It is assumed that both radios under test are current with the KMF.

VERSION #1.030

2. TEST

Step 1. Delete both TEKs from the CKR assigned to the talkgroup under test, from RADIO-1.

Step 2. Using RADIO-1, verify when the subscriber is set to secure mode, the radio indicates a key fail.

Step 3. Go to the Radio Management page of the KMF.

Step 4. Select RADIO-1 from the list.

Step 5. Initiate an Full Update operation.

Step 6. Go to the Operation Status page of KMF, verify that RADIO-1's Full Update operation is shown. The operation is complete when the Operation Status is "Completed." Note that a warmstart operation will occur if the TEK selected for the OTAR session is one of the TEKs assigned to CKR.

Step 7. Now that RADIO-1 contains the keys in the CKR, verify secure communications between RADIO-1 and RADIO-2.

Pass____ Fail____

3.11.3 Keyset Changeover

1. DESCRIPTION

The Changeover procedure is initiated by the KMF and is used to direct a radio or a group of radios to perform a keyset changeover. This procedure is used to direct radios and managed devices, system wide, to changeover from using one keyset to another keyset.

Note: The devices under test must have a valid air address registered with the KMF and must be accessible on the data system.

SETUP

RADIO-1 - TALKGROUP 1 (Secure Mode)
RADIO-2 - TALKGROUP 1 (Secure Mode)
RADIO-3 - TALKGROUP 1 (Secure Mode)

Make a note of the active keyset.

Any devices managed by the KMF that are not currently communicable by the KMF will appear as failures and/or retry opportunities (ROPs) throughout portions of this test.

VERSION #1.020

2. TEST

Step 1. Go to the Keyset Management page of the KMF.

Step 2. Set the inactive keyset to be the active keyset.

Step 3. A dialog box will apper asking if you want to “Set the active keyset only” or “Set active keyset and perform Changeover”

Step 4. Select the option to “Set active keyset and perform Changeover.”

Step 5. Depending on the size of the KMF database, the keyset changeover may take some time to complete. After the keyset changeover is complete, using RADIO-1's on screen menu or a KVL, verify that the keyset that was set to active is now the active keyset in the radio.

Step 6. Verify communications between RADIO-1, RADIO-2 and RADIO-3 on TALKGROUP 1.

Pass____ Fail____

3.11.4 Locked Out

1. DESCRIPTION

The KMF operator can designate a radio as "Locked Out." When a radio has been locked out at the KMF, any rekey request from the radio user is denied and results in a "No Service" message from the KMF.

Note: The devices under test must have a valid air address registered with the KMF and must be accessible on the data system.

SETUP

RADIO-1 - TALKGROUP 1

Radio under test must have the Rekey Request option available and configured via CPS.

VERSION #1.020

2. TEST

Step 1. Go to the Radio Management page of the KMF.

Step 2. Edit RADIO-1 to change its Locked Out state to “yes.”

Step 3. Initiate a Rekey Request from RADIO-1.

Step 4. Go to the Operation Status page of KMF, verify that RADIO-1’s Rekey Request operation is shown. The operation is complete when the Operation Status is “Completed.”

Step 5. Open up the operation’s details and Verify that the Rekey Request from the radio user is denied and "No Service" is displayed. Note that this will not impact normal voice operations, unless the radio does not have the correct TEKs. 'Locked out' denies the radio OTAR.

Step 6. Return RADIO-1 to normal service by Editing it to change its Locked Out state to “no.”

Pass____ Fail____

3.11.5 Radio Enable

1. DESCRIPTION

A Key Management Facility (KMF) operator can select the previously inhibited radio and re-enable the voice communications and user ergonomics using the enable command.

Note: The devices under test must have a valid air address registered with the KMF and must be accessible on the data system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1

RADIO-1 is currently in the inhibited state.

Note: The radio must be current in the KMF

Note: RCM inhibits and OTAR inhibts work interchangeably. If the radio, that is properly programmed, has been inhibited with OTAR, it can be re-enabled with RCM.

VERSION #1.020

2. TEST

Step 1. Go to the Radio Management page of the KMF.

Step 2. Select RADIO-1 from the list.

Step 3. Initiate an Enable operation.

Step 4. Go to the Operation Status page of KMF, verify that RADIO-1's Enable operation is shown. The operation is complete when the Operation Status is "Completed."

Step 5. Verify that RADIO-1 can now communicate with RADIO-2.

Pass____ Fail____

3.11.6 Radio Inhibit

1. DESCRIPTION

A Key Management Facility (KMF) operator can select any radio and completely disable the voice communications and user ergonomics using the Inhibit command. The enable command reverses these states.

Note: The devices under test must have a valid air address registered with the KMF and must be accessible on the data system.

Note: Zeroizing an inhibited radio will deem it unusable and the radio will only be usable again if sent to a Motorola Solutions depot for service. The KMF will display a warning if an attempt is made to zerioze an inhibited radio.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1

Note: The radio must be current in the KMF

VERSION #1.020

2. TEST

Step 1. Verify communications between RADIO-1 and RADIO-2.

Step 2. Go to the Radio Management page of the KMF.

Step 3. Select RADIO-1 from the list.

Step 4. Initiate an Inhibit operation.

Step 5. Go to the Operation Status page of KMF, verify that RADIO-1's Inhibit operation is shown. The operation is complete when the Operation Status is "Completed."

Step 6. Verify that RADIO-1 is turned off and cannot communicate with RADIO-2.

Pass____ Fail____

3.11.7 Subscriber Zeroize

1. DESCRIPTION

The Key Management Facility (KMF) can select any radio and permanently erase all encryption keys using the Zeroize command. This command is not reversible without a physical connection between the subscriber and a KVL. A KMF Operator can send this message to a radio that needs to be excluded from all secured communications. When the radio receives this message, all encryption keys (TEKs, UKEKs, KLK) are deleted from the radio, and it is permanently disabled in the KMF database. The KMF will not perform any more key management services to this radio until it is re-initialized.

Note: The devices under test must have a valid air address registered with the KMF and must be accessible on the data system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1

Both radios should initially have Keys.

Note: When a radio is zeroized, the radio record in the KMF is permanently flagged to zeroize. If this field is not unchecked, the radio will continue zeroizing every time it is fully updated.

VERSION #1.030

2. TEST

Step 1. Verify secure communications between RADIO-1 and RADIO-2.

Step 2. Go to the Radio Management page of the KMF.

Step 3. Select RADIO-1 from the list and initiate a Zeroize operation.

Step 4. Go to the Operation Status page of KMF, verify that RADIO-1's Zeroize operation is shown. The operation is complete when the Operation Status is "Completed."

Step 5. RADIO-1 no longer has any keys. The radio will display "Key Fail" if set to secure mode.

Step 6. Initiate a talkgroup call from RADIO-2. Verify that RADIO-1 does not unsquelch since it does not have any keys to decrypt audio.

Step 7. Connect a KVL to RADIO-1 and verify the radio has no TEKs and no KEKs.

Step 8. Attempt to perform a Full Update from the KMF to RADIO-1. Go to the Operation Status page of KMF, verify that RADIO-1's Full Update operation is shown.The operation is complete when the Operation Status is "Completed" with 1 failue. The failure is an indication that the TEKs and UKEKs were deleted from RADIO-1; a UKEK is required to perform a Full Update.

Step 9. In order to re-initialize the radio in the KMF database, first configure the zeroized pending setting in the radio record to "no", then perform a Red or Auto store and forward from the KVL to the KMF server then to the radio and back to KMF server.

Step 10. Verify secure communications between RADIO-1 and RADIO-2.

Pass____ Fail____

3.12 OVER THE ETHERNET KEYING (OTEK)

3.12.1 Encrypted Hello using over the Ethernet Keying (OTEK)

1. DESCRIPTION

The KMF operator can send an encrypted message to any console to confirm that console is on the system and that its encryption services are functioning.

Note: If the console has just been powered up, make sure to let it stabilize and to login via the console user interface to make sure the console registers with the KMF. Verify KMF registration by observing the KMF's Operations Status page to see that the test console has registered.

SETUP

CONSOLE-1 - TALKGROUP 1

Note: The console must be current in the KMF.

VERSION #1.020

2. TEST

Step 1. Go to the Console Management page of the KMF.

Step 2. Select CONSOLE-1 from the list.

Step 3. Initiate a Encrypted Hello operation

Step 4. Go to the Operation Status page of KMF, verify that RADIO-1's Clear Hello operation is shown. The operation is complete when the Operation Status is "Completed."

Pass____ Fail____

3.12.2 Full Update to Console using Over The Ethernet Keying (OTEK)

1. DESCRIPTION

The entire set of encryption keys (in addition to other state parameters) are sent to a console using the Full Unit Update command.

Note: If the console has just been powered up, make sure to let it stabilize and to login via the console user interface to make sure the console registers with the KMF. Verify KMF registration by observing the KMF event viewer to see that the test console has registered.

SETUP

CONSOLE-1 - TALKGROUP 3 (Reference console)
CONSOLE-3 - TALKGROUP 3 (test console that will be used for OTEK operation)
It is assumed that CONSOLE-3 initially does not have any traffic keys but does have a UKEK.

Note: It is assumed that this test will occur after all OTEK configurations are completed.
Note: This can be done with a VPM based console or a secure card based console.

VERSION #1.020

2. TEST

Step 1. Initiate a secure call on TALKGROUP 3 from CONSOLE-1 to CONSOLE-3

Step 2. Verify that no audio is received on CONSOLE-3 because the console does not have a key or has the incorrect key.

Step 3. Go to the Console Management page of the KMF

Step 4. Select CONSOLE-3 from the list

Step 5. Initiate a Full Update operation.

Step 6. Go to the Operation Status page of KMF, verify that CONSOLE-3's Clear Hello operation is shown. The operation is complete when the Operation Status is "Completed."

Step 7. The console will now have the current keys. Go to the Console Management page of the KMF and verify that CONSOLE-3's currency state is marked as "Current."

Step 8. Now that CONSOLE-3 is current, verify secure communications between CONSOLE-1 and CONSOLE-3.

Pass____ Fail____

3.12.3 Keyset Changeover Using Over the Ethernet Keying

1. DESCRIPTION

The Changeover procedure is initiated by the Key Management Facility (KMF) and is used to direct a radio, console, or a group of radios and consoles to perform a keyset changeover. This procedure is used to direct the intended radios or consoles to changeover from using one keyset to another keyset.

SETUP

CONSOLE-1 - Secure Capable, registered and current with KMF
CONSOLE-2 - Secure Capable, registered and current with KMF

VERSION #1.020

2. TEST

Step 1. Verify that Keyset 001 is the active keyset.

Step 2. Go to the Keyset Management page of the KMF.

Step 3. Select Keyset 2 from the list by clicking 'Set Active Keyset'

Step 4. A dialog box will apper asking if you want to “Set the active keyset only” or “Set active keyset and perform Changeover.”

Step 5. Select “Set active keyset and perform Changeover.”

Step 6. Depending on the size of the KMF database, the keyset changeover may take some time to complete. After the keyset changeover is complete, using the GUI, verify that Keyset 002 is now the active keyset on CONSOLE-1, and CONSOLE-2.

Pass____ Fail____

3.13 RADIO AUTHENTICATION

3.13.1 Radio Fails Authentication

1. DESCRIPTION

This test verifies that a radio that fails authentication does not get access to system services. The authentication failure is notified to the user of the radio. Also, the authentication failure is notified to the infrastructure by alarm on Unified Event Manager (UEM) and zone watch shows the authentication failure. Additionally, historical reports capture that an authentication failure occurred.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1

An authentication key for RADIO-1 is in AuC
System wide Authentication is Enabled
RADIO-1 is configured to indicate authentication failure.

VERSION #1.010

2. TEST

Step 1. KVL load a randomly created authentication key into RADIO-1

Step 2. Cycle power on RADIO-1.

Step 3. Confirm authentication failure was indicated on RADIO-1, zone watch, and an alarm on UEM.

Step 4. Key RADIO-1.

Step 5. Confirm RADIO-1 cannot perform a Talkgroup call with RADIO-2.

Step 6. Check historical reports for occurrence of authentication failure.

Pass____ Fail____

3.13.2 Radio Successfully Authenticates

1. DESCRIPTION

This test verifies that the radio has performed and passed authentication. The user of the radio is not notified that authentication has been successful, but it is shown on the infrastructure with Zone Watch.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-2 - TALKGROUP 1

No authentication key for RADIO-1 in AuC.
System wide Authentication is Enabled

VERSION #1.010

2. TEST

Step 1. KVL load a randomly created authentication key into RADIO-1.

Step 2. Download this authentication key from the KVL to the AuC.

Step 3. Verify on AuC client that the authentication key was received.

Step 4. Cycle power on RADIO-1.

Step 5. Verify on Zone Watch that authentication was performed.

Step 6. Confirm RADIO-1 can perform a Talkgroup call with RADIO-2.

Pass____ Fail____

3.14 DYNAMIC SYSTEM RESILIENCE

3.14.1 Gateway GPRS Support Node 1 Failure

1. DESCRIPTION

This test will demonstrate that in the event of a failure of the Gateway General Packet Radio Services (GPRS) Support Node (GGSN) in the Primary Core, the Backup Core Packet Data Gateway becomes active. After the GGSN failure, the Primary Core Packet Data Gateway reports an inoperable state and data functionality will continue to be provided on the Backup Core Packet Data Gateway.
Note: This test case applies to the following data services - Trunking IV&D and Conventional IV&D data. The test case can be executed with any or all of the supported data services and should include the appropriate packet data gateways, sites and the radio personalities in the setup of the test case.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
Packet Data Gateway 1: Active
Packet Data Gateway 2: Standby

VERSION #1.030

2. TEST

Step 1. Send inbound data from RADIO-1, then send outbound data to RADIO-1.

Step 2. Pull the power cord to GGSN 1 in the Primary Core.

Step 3. Observe, in the Primary Core Unified Event Manager and Backup Core Unified Event Managers, the Packet Data Gateway 1's Application State transition to 'Inoperable'.

Step 4. Verify Packet Data Gateway 2's Redundancy state is 'Active' using the Unified Network Configurator (UNC) "Quick Commands" or the Unified Event Manager in the Primary and Backup Core.

Step 5. Observe, in both Unified Event Managers, the Link Status of the Packet Data Gateway's common managed links transition through various states to 'Up'.

Step 6. Verify that radios automatically context activate.

Step 7. Send inbound data from RADIO-1, then send outbound data to RADIO-1.

Step 8. Plug the power cord in to GGSN 1 in the Primary Core.

Pass____ Fail____

3.14.2 Packet Data Gateway 1 Failure

1. DESCRIPTION

In a system with Dynamic System Resilience (DSR), each zone has two Packet Data Gateways (PDG) for each Integrated Voice & Data (IV&D) and/or Conventional Integrated Voice & Data service; one PDG in the primary core, and one PDG in the backup core. The PDGs securely communicate to automatically select one active PDG. The selection algorithm is weighted to give preference to the PDG serving the most number of sites or the PDG in the primary core if the number of serving sites is equal. The standby PDG does not synchronize any context databases with the active PDG.

This test will demonstrate in the event of a Primary Core Packet Data Gateway failure, the Backup Core Packet Data Gateway becomes active. After the failure, data functionality will continue to be provided on the Backup Core Packet Data Gateway.

Note: This test case applies to both Trunking IV&D, Conventional IV&D.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
Packet Data Gateway 1: Active
Packet Data Gateway 2: Standby

VERSION #1.030

2. TEST

Step 1. Send inbound data from RADIO-1, then send outbound data to RADIO-1. Note down the CAI IP address on the Radio unit.

Step 2. Disconnect the Ethernet links on the Packet Data Router and Radio Network Gateway in the Primary Core.

Step 3. Observe, in the Primary Core Unified Event Manager and Backup Core Unified Event Manager, the Packet Data Gateway 1's Redundancy State transition to 'Communication Failure'.

Step 4. Verify Packet Data Gateway 2's Redundancy state is 'Active' using the Unified Network Configurator (UNC) "Quick Commands" or the Unified Event Manager in the Primary and Backup Core.

Step 5. Observe, in both Unified Event Managers, the Link Status of the Packet Data Gateway's common managed links transition through various states to 'Up'.

Step 6. After a short period, verify that the radio context activation is unaffected and its CAI IP remains the same value as prior to the switchover.

Step 7. Send inbound data from RADIO-1, then send outbound data to RADIO-1.

Step 8. Restore the Packet Data Router and Radio Network Gateway links in the Primary Core.

Pass____ Fail____

3.14.3 Primary Core Failure - Switchover to Back-up Core (Voice and Data Services)

1. DESCRIPTION

Dynamic System Resilience (DSR) allows a system to continue to function with minimal loss of voice and/or Data communications due to the failure of any controlling master site.
This test will demonstrate in the event of a complete Primary Core failure, the Backup Core takes over in order to return the system back to wide area trunking. Some of the Backup Core equipment automatically takes over while the Network Management servers like the Provisioning Manager Server and Unified Network Configurator require manual switchover.
Note: This test case applies to the following data services - Trunking IV&D and Conventional IV&D data. The test case can be executed with any or all of the supported data services and should include the appropriate packet data gateways, sites and the radio personalities in the setup of the test case.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-5 - TALKGROUP 1
Mobile Data Terminal (MDT) connected to RADIO-5
UDP Tool installed on both the MDT and Host computers
Zone Controller 1: Active
Zone Controller 2: Standby
Zone Controller 3: Standby
Zone Controller 4: Standby
Packet Data Gateway 1: Active
Packet Data Gateway 2: Standby
Unified Network Configurator 1: Active
Unified Network Configurator 2: Standby
User Configuration Manager: Active
User Configuration Manager 2: Standby
System Statistics Server 1: Active
System Statistics Server 2: Active

VERSION #1.050

2. TEST

Step 1. Initiate a TALKGROUP 1 call from RADIO-1. Verify that RADIO-2 receives the audio.

Step 2. Using RADIO-5 MDT, configure the data application for periodic inbound data messages. (1 message every 30 seconds) Observe at the Host PC that data messages are received.

Step 3. Pull the power cords to the Primary Core LAN Switches 1 & 2. (Also the redundant power supply (RPS) if equipped.)

Step 4. In the Unified Network Configurator (UNC), select Zone Controllers 1 through 4 and check the redundancy state using the Quick Command feature. (Note: In a single Zone system or when the test is run on the Zone with the primary core system servers the backup UNC will need to be manually enabled to run the quick command.)

Step 5. Verify that Zone Controller (ZC) 3 is Active. (Note that the transition of ZC 3 to the "Active" state causes the currently active ZC to reset and the sites will temporarily lose Wide Area Trunking while the connection to ZC 3 is established.)

Step 6. In the Unified Network Configurator, select any of the Packet Data Gateways 1 and 2 and check the redundancy state using the Quick Command feature.

Step 7. Verify that Packet Data Gateway 2 is Active.

Step 8. Initiate a TALKGROUP 1 call from RADIO-1. Verify that RADIO-2 receives the audio.

Step 9. Observe at the Host PC that received data messages have continued.

Step 10. If the backup servers were enabled for the test, they should now be disabled. Return the system to normal by powering up the core switches. Verify once the Zone Controllers start to communicate only 1 Zone Controller will be active.

Pass____ Fail____

3.14.4 Single Ethernet Link RF Site Router Path Failure

1. DESCRIPTION

This test will demonstrate in the event of a failure of an RF Site Router's Ethernet link path to the Primary Core, in a single site router configuration, the RF Site Router routes packets through the Backup Core to the Primary Core. The Site Control Paths are unaffected by the failure.

NOTE: This test is not applicable in a system with combined Core/Exit Router/Gateways.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
Zone Controller 1: Active
Zone Controller 2: Standby (Does not apply for M1 DSR)
Zone Controller 3: Standby
Zone Controller 4: Standby (Does not apply for M1 DSR)

VERSION #1.030

2. TEST

Step 1. Initiate a Talkgroup call from RADIO-1 on TALKGROUP 1. Verify that RADIO-2 receives the audio.

Step 2. Pull the power cords to both the Core Routers in the Primary Core.
Note: For M1 this is only one Core Router in the primary and one Core Router in the backup core.

Step 3. Observe, in both Unified Event Managers, both the Core Routers in the Primary Core have failed.

Step 4. Verify, via the Unified Event Manager (e.g. in the Primary Core), that Zone Controllers 1 and 2, Packet Data Gateway1 and the RF sites are unaffected by the RF site link outage.

Step 5. Initiate a Talkgroup call from RADIO-1. Verify RADIO-2 receives the audio.

Step 6. Plug the power cords in to both the Core Routers in the Primary Core.
Note: For M1 this is only one Core Router in the primary and one Core Router in the backup core.

Pass____ Fail____

3.14.5 Primary Core Link Failure - Ethernet Console Site Link

1. DESCRIPTION

This test will demonstrate that in the event of a failure of a link to the Primary Core, the Console Site Router routes packets through the Backup Core to the Primary Core. The Site Control Paths are unaffected by the failure.

NOTE: This test is not applicable in a system with combined Core/Exit Router/Gateways.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
CONSOLE-1 - TALKGROUP 1
CONSOLE-1 - SITE - CONSITE 1
Zone Controller 1: Active
Zone Controller 2: Standby (Does not apply for M1 DSR)
Zone Controller 3: Standby
Zone Controller 4: Standby (Does not apply for M1 DSR)

VERSION #1.030

2. TEST

Step 1. Initiate a Talkgroup call from CONSOLE-1 on TALKGROUP 1. Verify that RADIO-1 and RADIO-2 receive audio.

Step 2. Pull the power cords to both the Core Routers in the Primary Core.

Step 3. Observe, in both Unified Event Managers, both the Core Routers in the Primary Core have failed.

Step 4. Verify, via the Unified Event Manager (e.g. in the Primary Core), that Zone Controllers 1 and 2, and the Consoles in the site are unaffected by the Console site link outage. The Zone Controller state can also be found using the UNC "Quick Command" feature.
Note: For M1 ZC2 is not present

Step 5. Initiate a Talkgroup call from CONSOLE-1 on TALKGROUP 1. Verify that RADIO-1 and RADIO-2 receive audio.

Step 6. Plug in the power cords to both the Core Routers in the Primary Core. Upon restoration of the link, the Console Site Router routes packets to the Primary Core.

Step 7. Initiate a Talkgroup call from CONSOLE-1 on TALKGROUP 1. Verify that RADIO-1 and RADIO-2 receive audio.

Pass____ Fail____

3.14.6 User Requested Active - Packet Data Gateway 2

1. DESCRIPTION

In a system with Dynamic System Resilience, each zone has three Packet Data Gateways (PDG) for each Integrated Voice & Data (IV&D), High Performance Data (HPD) data service and/or Conventional Integrated Voice & Data ; one PDG in the primary core, and one PDG in the backup core.
This test will demonstrate that a Backup Core Packet Data Gateway can be activated to take over wide area data services during an upgrade scenario where the Primary Core Packet Data Gateway is being upgraded.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
Mobile Data Terminal connected to RADIO-1
Packet Data Gateway 1: Active
Packet Data Gateway 2: Standby
UDP Tool installed on MDT and Host PC

VERSION #1.020

2. TEST

Step 1. Configure the UDP Tool for periodic inbound data messages. (1 message every 30 seconds) Observe at the Host PC that data messages are received.

Step 2. In the Unified Network Configurator, select Packet Data Gateways 1 and 2 and check the redundancy state using the Quick Command feature.

Step 3. Verify that Packet Data Gateway 1 is Active.

Step 4. Set Redundancy state of Packet Data Gateway 2 to ‘Active’, via the active Unified Network Configurator.

Step 5. In the Unified Network Configurator, select Packet Data Gateways 1 and 2 and check the redundancy state using the Quick Command feature.

Step 6. Verify that Packet data Gateway 2 is Active.

Step 7. Observe at the Host PC that received data messages have continued.

Pass____ Fail____

3.14.7 User Requested Active - Zone Controller 3

1. DESCRIPTION

For normal operation, only one of the Zone Controllers (ZCs) is in the Active state. Assuming no critical failures, the remaining ZCs are in either the Standby or User Requested Standby state. For instance, if ZC1 was the active ZC and it failed, the redundant ZC2 would take over. Standby ZC3 will take over and become active either when both ZC1 and ZC2 fail (for example, because of a master site destruction) or when the InterZone link is down.
This test will demonstrate that a Backup Core Zone Controller can be activated to take over wide area trunking services during an upgrade scenario where the Primary Core Zone Controllers are being upgraded.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 – TALKGROUP 1
RADIO-2 - SITE - SITE 2
Zone Controller 1: Active
Zone Controller 2: Standby (Does not apply for M1 DSR)
Zone Controller 3: Standby
Zone Controller 4: Standby (Does not apply for M1 DSR)

VERSION #1.020

2. TEST

Step 1. Initiate a Talkgroup call from RADIO-1 on TALKGROUP 1. Verify that RADIO-2 receives the audio.

Step 2. In the Unified Network Configurator, select Zone Controllers 1 through 4 and check the redundancy state using the Quick Command feature.

Note: For M1 ZC2 and ZC 4 are not present

Step 3. Set Redundancy state of Zone Controller 3 to ‘Active’, via the active Unified Network Configurator.

Step 4. Note that the transition of Zone Controller 3 to the "Active" state causes the currently active Zone Controller to reset and the sites will temporarily lose Wide Area Trunking while the connection to Zone Controller 3 is established.

Step 5. In the Unified Network Configurator, select Zone Controllers 1 through 4 and check the redundancy state using the Quick Command feature.

Note: For M1 ZC2 and ZC 4 are not present

Step 6. Verify that Zone Controller 3 is Active.

Step 7. Initiate a Talkgroup call from RADIO-1 on TALKGROUP 1. Verify that RADIO-2 receives the audio.

Pass____ Fail____

3.15 REPORT GENERATION TESTS

3.15.1 Historical Reports

1. DESCRIPTION

Performance reports can be created automatically for dynamic statistical information about the air traffic activity on the system. These reports provide assistance with system management, resource planning, usage allocation, and monitoring. All reports are preformatted and summarize air traffic activity for a configured time span.

Note: Depending on the time span selected smaller time intervals may not be available.

SETUP

No prior setup is required for this test.

VERSION #1.010

2. TEST

Step 1. From the PC Application Launcher, select a zone.

Step 2. From that zone's menu, choose Zone Historical Reports.

Step 3. From the Historical Reports Player window that opens, select a report.

Step 4. Using the left mouse button, click on the view button.

Step 5. Observe a window opens allowing a user to enter report parameters.

Step 6. Enter all desired data for the report and Generate Report.

Step 7. Observe a window appears showing the requested report.

Step 8. Close the report window.

Step 9. Run the following reports during testing: Talkgroup at Zone Summary; User at Zone Summary; Site Summary.

Pass____ Fail____

3.16 NETWORK SECURITY TESTS

3.16.1 Authentication, Authorization and Accounting

1. DESCRIPTION

System administrators and users have different roles in using and administrating the system. The level of user's authorization should fit their role. The system supports centralized definition of user's role, and enforces least privilege authorization

SETUP

A properly configured account for "John Smith" set up in Domain Controllers using a login of johnsmith.
(Make sure that the script to configure UNIX properties is run.)

Note: Creating the user account in any Domain Controller is possible, but time is needed for Active Directory data to synchronize across zones.

VERSION #1.020

2. TEST

Step 1. Login to the Domain Controller, with the Administrator account. Verify the account "John Smith" has been set up with the following attributes, "domuser" as the primary group and "zc-login" as secondary group.

Step 2. Login to Zone Controller as "johnsmith". At the command prompt type "admin_menu" to launch the administrative menu.

Step 3. Select "Services Administration" and then "Syslog Client".

Step 4. Verify that the "Display Centralized Logging Status" is presented with "*" and execution of the operation is not permitted.

Step 5. Attempt login to ZDS as "johnsmith". Verify that the user is not able to access ZDS,
since the user is not member of the "zds-login
group.

Step 6. Login to the Domain Controller again. Add "auditors" and "zds-login" as secondary groups.

Step 7. Login to Zone Controller as "johnsmith". Execute "Display Centralized Logging Status" to verify user now being authorized for
the operation.

Step 8. Login to ZDS as "johnsmith". Verify that now the user is able to access ZDS.

Pass____ Fail____

3.16.2 Centralized Logging - Log the Successful Login to NM Client

1. DESCRIPTION

The Centralized Logging Feature is an optional component . When installed, it collects the Operating System logs of network clients in the system. Events captured include: System Startup and Shutdown Events, Login Failures & Successes, Logouts, Elevation of privileges, Hardware Failures, Software Failures, and Resource Taxation.

SETUP

No prior setup is required for this test.

VERSION #1.030

2. TEST

Step 1. Log on to the NM client using your Active Directory account that is a member of the Installation Administrator or Platform Administrator group (instadm or netwadm).

Step 2. From the NM client, open the Internet Explorer.

Step 3. In the Internet Explorer, enter the following URL: https://loghost<XX>.zone<Z> where <XX> is the number of the Centralized Event Logging Server you are trying to access and <Z> is the number of the zone where the Centralized Event Logging server resides

Step 4. Log in to “Syslog Viewer” using the username and password for your Active Directory account that is a member of one of the following Active Directory groups:
- platadm
- auditor
- instadm

Step 5. Once you logged in Syslog Viewer. The latest logs appear. Verify the NMClient Login has been logged. Verify the messages can be searched by using the filter option.

Step 6. To close, “Syslog Viewer” application select “Logout” option from the File menu..

Pass____ Fail____

3.16.3 Centralized Logging - Voice Processor Module Events - Authentication Services Disabled

1. DESCRIPTION

The Centralized Logging Feature is an optional component. When installed, it collects the Operating System logs of network clients in the system. Events captured include: System Startup and Shutdown Events,
Login Failures & Successes, Logouts, Elevation of privileges, Hardware Failures, Software Failures, and Resource Taxation.

SETUP

VPM CONSOLE-1 Configured

VERSION #1.030

2. TEST

Step 1. Log on to the NM client using your Active Directory account that is a member of the Installation Administrator or Platform Administrator group (instadm or netwadm).

Step 2. From the NM client, open the Internet Explorer.

Step 3. In the Internet Explorer, enter the following URL: https://loghost<XX>.zone<Z> where <XX> is the number of the Centralized Event Logging Server you are trying to access and <Z> is the number of the zone where the Centralized Event Logging server resides.

Step 4. Log in to “Syslog Viewer” using the username and password for your Active Directory account that is a member of one of the following Active Directory groups:
• platadm
• auditor
• instadm

Step 5. Once you logged in Syslog Viewer. The latest logs appear.

Step 6. Connect to the VPM of a VPM based console serially via CSS; issue the command to reset the VPM.

Step 7. Once the VPM is online, observe that the Syslog Viewer shows the VPM device's startup event message. Verify that log messages are being received from the syslog clients [ie VPM clients] on the syslog server [ie loghost01].

Step 8. Observe that the Syslog Viewer shows up the VPM device's successful login event message.

Step 9. To close, “Syslog Viewer” application select ”Logout” option from the File menu.

Pass____ Fail____

3.16.4 Centralized Logging - Voice Processor Module Events - Authentication Services Enabled

1. DESCRIPTION

The Centralized Logging Feature is an optional component. When installed, it collects the Operating System logs of network clients in the system. Events captured include: System Startup and Shutdown Events, Login Failures & Successes, Logouts, Elevation of privileges, Hardware Failures, Software Failures, and Resource Taxation.

SETUP

VPM CONSOLE-1 Configured

VERSION #1.030

2. TEST

Step 1. Log on to the NM client using your Active Directory account that is a member of the Installation Administrator or Platform Administrator group (instadm or netwadm).

Step 2. In the Internet Explorer, enter the following URL: https://loghost<XX>.zone<Z> where <XX> is the number of the Centralized Event Logging Server you are trying to access and <Z> is the number of the zone where the Centralized Event Logging server resides.

Step 3. Log in to “Syslog Viewer” using the username and password for your Active Directory account that is a member of one of the following Active Directory groups:
• platadm
• auditor
• instadm

Step 4. Connect to the Voice Processing Module (VPM) of a VPM based console serially via CSS using the valid user name and password. Observe that the syslog server contains the VPM device’s successful login event message.

Step 5. Issue the command to reset the VPM.

Step 6. Once the VPM is online, observe that the “Syslog Viewer” shows up the VPM device’s startup event message. Verify that log messages are being received from the syslog clients [ie VPM clients] on the syslog server [ie loghost01].

Step 7. Close CSS application.

Step 8. Launch CSS application. Login to the VPM of a VPM based console serially via CSS with an invalid username and password..

Step 9. Observe that the “Syslog Viewer” shows up the VPM device’s unsuccessful login event message.

Step 10. To close, “Syslog Viewer” application select “Logout” option from the File menu.

Pass____ Fail____

3.16.5 Service Access Architecture - Site Lan Switch

1. DESCRIPTION

The Service Access Architecture feature provides secured communications access between the Radio Network Infrastructure (RNI) and service users. The feature can be viewed as four primary access scenarios as follows:
1. Access to the RNI from Motorola System Support Center via dedicated WAN connection
2. Access to the RNI via dial-up connection provided by modem located in the DMZ (The service user for this scenario may be Motorola service users or customer based service users)
3. Access to the RNI via dial-up connection provided by modem located at Simulcast Prime Site (The service user for this scenario may be Motorola service users or customer based service users)
4. Access to the RNI via LAN switch located at a remote site (The service user for this scenario may be Motorola service users or customer based service users)

The purpose of this test is to validate secure remote access from a remote site.

SETUP

This test requires NMclient01 to be installed at the master site.

If the remote site switch is MAC port lockdown enabled, the service PC user will require an account in the Authentication Access Architecture (AAA) server.
User to be authenticated must be entered into the Domain Controller.

VERSION #1.010

2. TEST

Step 1. Connect a service PC to a remote RF site LAN switch.

If MAC port lockdown is enabled, the service PC user will require 802.1x authentication.

Step 2. Start Windows remote desktop application from service PC.

Step 3. Connect to NMclient01 at the Master Site.

Step 4. Verify NM client applications can be accessed remotely from the service PC.

Pass____ Fail____

3.16.6 SNMPv3

1. DESCRIPTION

The SNMPv3 feature provides secured network management traffic between network managers (NM) and network elements (NE). When a system is installed or migrated, the SNMPv3 communications between above NMs and NEs are "clear" that is the system initial default mode, i.e. No Authentication and No Privacy. The system can be configured for Authentication w/o Privacy, or Authentication w/ Privacy.

This test demonstrates that the NMs and NEs cannot communicate unless both are configured properly.

UEM - Unified Event Manager
CSS- Configuration Service Software
UNC - Unified Network Configurator
VPM - Voice Processing Module
PCA – Provisioning and Configuration Agent

SETUP

Note: Not all systems will include all devices.

VERSION #1.050

2. TEST

Step 1. The initial v3 communication should be functioning as "Clear" mode when network managers (UEM, UNC, InfoVista, and MOSCAD permanent manager) and SNMPv3 devices (site elements, MNR Routers, HP LAN switch, VPM devices and MOSCAD RTU) are initially installed and configured.

Step 2. Choose an SNMPv3 device and change the MotoMaster v3 user credentials. Use CSS for G-Series site elements, and VPM devices use Router User Interface for router, use MOSCAD permanent manager for MOSCAD RTU, and use PCA for the DSC 8000.

Step 3. Verify that the UEM will raise a "Comm Loss" alarm when UEM detect it is unable to perform SNMPv3 operation to this SNMPv3 device. From UNC, use "Test Credentials" command to verify that the v3 communication to this device fails. From InfoVista, the statistic graph will not show collected data because of this v3 communication failure.

Step 4. Make the same MotoMaster v3 credentials change in UEM, UNC, and InfoVista.

Step 5. Verify that fault management, configuration management, and performance management functions from UEM, UNC, and InfoVista to this SNMPv3 device are become normal again. UEM will also clear the "Comm loss" alarm.

Pass____ Fail____

3.16.7 SSH - User Authentication and Encrypted Session - Communication to Zone Controller

1. DESCRIPTION

The primary goal of this feature is to provide a secure point to point connection between two different machines where the connection is encrypted and both ends have been authenticated. Securing these services is accomplished through the use of the Secure Shell (SSH) protocol. SSH is a network protocol that allows the transmission of data securely between two end points by using public-key encryption techniques, thus ensuring confidentiality and integrity of the data. SSH also supports authentication of a user who is attempting to remotely access the network as well as authentication of both network components involved in the communication.
The test addresses the following:

1. Illustrates that telnet is disabled at the server.
2. Illustrates user authentication.
3. Illustrates that SSH connection can be established.

SETUP

PuTTY application at NM Client should be pre-configured with the Zone Controller host key in the known host list.

An account capable of logging into Zone Controller has been created in Domain Controller.

VERSION #1.030

2. TEST

Step 1. Attempt to connect to the Zone Controller from the NM Client via telnet. Verify a failed connection attempt.

Step 2. Attempt to connect to the Zone Controller from the NM Client via PuTTY.

Step 3. Enter the wrong password and verify that access is denied.

Step 4. Enter the correct password and verify successful connection.

Pass____ Fail____

3.16.8 SSH - User Authentication and Encrypted Session - Voice Processing Module (VPM)

1. DESCRIPTION

The primary goal of this feature is to provide a secure point to point connection between two different machines where the connection is encrypted and both ends have been authenticated. Securing these services is accomplished through the use of the Secure Shell (SSH) protocol. SSH is a network protocol that allows the transmission of data securely between two end points by using public-key encryption techniques, thus ensuring confidentiality and integrity of the data. SSH also supports authentication of a user who is attempting to remotely access the network as well as authentication of both network components involved in the communication.
The test addresses the following:

1. Illustrates that telnet can be disabled at the server.
2. Illustrates user authentication.
3. Illustrates that SSH connection can be established.
4. Illustrates server authentication. User is prompted with warning message if the server key has changed.

SETUP

Setup the VPM with clear protocols enabled and secure protocols enabled. PuTTY application at NM Client should be pre-configured with the VPM public key in the known host list.

VERSION #1.010

2. TEST

Step 1. Verify that a telnet session can be established between the NM Client and the VPM.

Step 2. Disable clear protocol operation at the VPM

Step 3. Attempt to connect to the VPM from the NM Client via telnet. Verify a failed connection attempt.

Step 4. Attempt to connect to the VPM from the NM Client via PuTTY

Step 5. Enter the wrong password and verify that access is denied.

Step 6. Enter the correct password and verify successful connection.

Pass____ Fail____

3.16.9 Virus Protection (McAfee Antimalware)

1. DESCRIPTION

The network clients in the system are protected by anti-virus software. In this test, a mock virus will be introduced to the system. This test virus was developed by the European Institute for Computer Anti-Virus Research (EICAR) to provide an easy and safe way to test whether the anti-virus software is working, and see how it reacts when a virus is detected. This is a 70-byte file, which if executed, simply displays the message: "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!"

SETUP

Acquire the EICAR test virus file (http://www.eicar.org/anti_virus_test_file.htm), and place it on a removable media drive.

VERSION #1.040

2. TEST

Step 1. Log on to the NM client using your Active Directory account that is a member of the Installation Administrator or Platform Administrator group (instadm or netwadm).

Step 2. Insert removable media with the EICAR test virus on a NM client. Attempt to execute the EICAR test virus.

Step 3. McAfee Antimalware software on the NM client will Quarantine the EICAR virus upon execution and logs a Malware detection event to Windows event log. Verify the Error message ID “259”under Windows Application events. McAfee Antimalware software on the NM client will also notify the malware detection event to McAfee ePO Server (CSMS).

Step 4. Log on to CSMS using the Windows “administrator” account.

Step 5. Start the ePO Server console by double-clicking the Launch McAfee ePolicy Orchestrator Web Console icon on the CSMS Windows desktop that appears.

Step 6. Log on to ePO administrative console by using account that has administrative privilege to View threat events on forwarded by endpoint device (NM Client).

Step 7. From McAfee ePolicy Orchestrator Web Console Menu perform the following steps: Select Reporting, Select Queries & Reports. In the Quick Find field type MSI, click Apply. Locate query MSI: All Events and click Run (to the right of the query name)
Note: Depending on the number of systems and event it may take several minutes to display results.

Step 8. Review Threat Events or use custom filtering to create a smaller subset. When done click Close on (lower right of the screen)

Pass____ Fail____

3.17 BACKUP AND RECOVERY (BAR)

3.17.1 Data Backup for Zone Controller Using the Backup And Recovery Server

1. DESCRIPTION

The main features of Backup And Recovery (BAR) are the ability to centrally backup and restore certain network elements. The relevant data can be backed up without affecting system operation.

SETUP

No setup required.

VERSION #1.010

2. TEST

Step 1. Login to BAR Server with the appropriate account and password.

Step 2. Select the menu option that allows you to schedule a backup client.

Step 3. Follow the on screen instructions to schedule a one-time backup of the Zone Controller (ZC).

Step 4. Approximately one hour after the backup was scheduled to start, view the backup report on the BAR Server to verify the backup was successful.

Pass____ Fail____

3.18 ADVANCED MESSAGING SOLUTION (AMS)

3.18.1 Device ID Messaging (Radio to Smart Client)

1. DESCRIPTION

Messaging to a radio Device ID allows the sender of a message to address a message to a radio regardless of the user of the radio. When no user name is logged on a radio, the message is identified by the sending Device ID.
This test will demonstrate sending a message from a radio with no user name logged on to an AMS Smart Client (SC).

SETUP

PremierOne User Accounts
LoneDispatcher1 with Password 1

Logon "LoneDispatcher1 on AMS Smart Client SC-1 with password "Password1"

RADIO-1 Logged off but powered on

VERSION #1.040

2. TEST

Step 1. Compose a text message on RADIO-1 selecting "LoneDispatcher1" from the Data Users List as the address [TMS > COMP > NEW > type message > ADDR > LIST > select address].

Step 2. Send the text message from RADIO-1 to "LoneDispatcher1" [PTT].

Step 3. Verify Smart Client SC-1 receives the message.

Step 4. Verify that the message shows from RADIO-1's Device ID.

Pass____ Fail____

3.18.2 Device ID Messaging (Smart Client to Radio Device ID)

1. DESCRIPTION

Messaging to a radio Device ID allows the sender of a message to address a message to a radio regardless of the user of the radio. When no user name is logged on a radio, the message is identified by the sending Device ID.
This test will demonstrate sending a message from a SMART CLIENT to a radio Device ID.

SETUP

PremierOne User Accounts-
LoneDispatcher1 with password "Password1"

Logon "LoneDispatcher1" on AMS Smart Client SC-1 with password "Password1"

RADIO-1 Logged off but powered on

VERSION #1.040

2. TEST

Step 1. Compose a text message on Smart Client SC-1 selecting RADIO-1's Device ID from the address book as the address.

Step 2. Send the text message from Smart Client SC-1 to RADIO-1's Device ID.

Step 3. Verify RADIO-1 receives the message [HOME > TMS > INBX].

Pass____ **Fail**____

3.18.3 Group Messaging (Smart Client to Text Messaging Group)

1. DESCRIPTION

Group messaging allows the sender of a text message to address the message to multiple destinations using a single text message group address. The text messaging group address must be previously defined and its address members selected. This test will verify sending a message from an AMS Smart Client (SC) to a text messaging group address.

SETUP

PremierOne User Accounts-
LoneDispatcher1 with password Password1

Equipment setup
Logon "LoneDispatcher1 on AMS Smart Client SC-1 with password "Password1"

Power on RADIO-1, RADIO-2, and RADIO-3

"RadioGroup1" group address must be previously defined with RADIO-1, RADIO-2 and RADIO-3 defined as members of the group.

VERSION #1.020

2. TEST

Step 1. Compose a text message on Smart Client SC-1 selecting "RadioGroup1" from the address book as the address

Step 2. Send the text message from Smart Client SC-1 to "RadioGroup1"

Step 3. Verify RADIO-1, RADIO-2 and RADIO-3 receive the message [HOME > TMS > INBX]

Pass____ Fail____

3.18.4 Group Messaging (Radio to Text Messaging Group)

1. DESCRIPTION

Group messaging allows the sender of a text message to address the message to multiple destinations using a single text message group address. The text messaging group address must be previously defined and its address members selected. This test will verify sending a message from a radio to a text messaging group address

SETUP

Equipment setup
RADIO-1, RADIO-2 and RADIO-3 are powered on.

"RadioGroup2" group address must be previously defined with RADIO-1, RADIO-2 and RADIO-3 defined as members of the group.

VERSION #1.020

2. TEST

Step 1. Compose a text message on RADIO-1 selecting "RadioGroup2" from the Data Users List as the address [TMS > COMP > NEW > type message > ADDR > LIST > select address]

Step 2. Send the text message from RADIO-1 to "RadioGroup2" [PTT]

Step 3. Verify RADIO-1, RADIO-2 and RADIO-3 receive the message [HOME > TMS > INBX]

Pass____ Fail____

3.19 SIGNOFF CERTIFICATE

By their signatures below, the following witnesses certify they have observed the system Acceptance Test Procedures.

Signatures

TAIWAN NAVY
WITNESS: _____Date: _____

Please Print Name: _____ _____

Initials:

Please Print Title: _____

TAIWAN NCIST
WITNESS: _____Date: _____

Please Print Name: _____ _____

Initials:

Please Print Title: _____

V&V ITCL
WITNESS: _____Date: _____

Please Print Name: _____ _____

Initials:

Please Print Title: _____