Application Note

AEROFLEX
A passion for performance.

Using the 2975 to perform Control Channel Logging

This revised application note provides P25 test professionals with an overview of how the 2975 can be used in troubleshooting P25 protocol issues by using the P25 Control Channel Logging Option (Option 6).

Objective

The 2975 is a dynamic instrument that offers exciting new possibilities in the test and analysis of not only RF parameters, but also the ability to decode and analyze various aspects of signaling associated with P25 digital radio systems. The purpose of this application note is to provide P25 test professionals with an overview of how the 2975 can be used in troubleshooting P25 protocol issues by using the P25 Control Channel Logging Option (Option 6).

Understanding P25 Control Channel Operation

The P25 control channel feature for trunking is not specific to a P25 manufacturer or P25 RFSS (Radio Frequency Sub-System) configuration. All mobiles supporting P25 formats should be able to access a P25 trunking function as either standard configuration or as an option. In the P25 standard, the control channel maintains compatibility between conventional operation, in that the modulation format, the bit rate and many of the control messages are the same. In the case of P25, the control channel is a 9600-baud (data rate) channel using C4FM modulation to impart the digital 1's and 0's to the receiving radio.

The difference is that the trunked version uses packet access techniques and requires a request process to a resource controller which coordinates the user's access, while the conventional version permits users to control their own access by selecting a particular user channel. An example of how a control channel operates can be seen in figure 1.0.
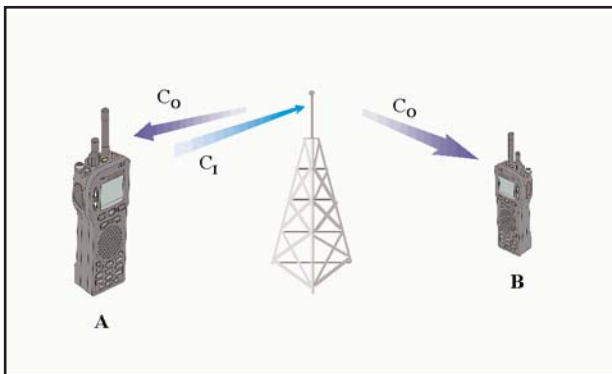

Figure 1.0 Control Channel Operation

As you can see, the repeater is putting out an outbound control channel, (Co) that both mobiles are monitoring. In P25 Trunking systems, the outbound control channel sends information in "packets" and those words are called Outbound Signaling Packets or OSPs.

Let's assume that mobile "A" wants to place a call to another user on the systems. Mobile A transmits a request to the repeater on an inbound control channel (CI). In P25 Trunking systems, the inbound control channel sends information words called Inbound Signaling Packets or ISPs. The repeater station and network process the request, and then send an alert on the outbound control channel that the designated user, mobile "B", recognizes as a call that is part of its group or that is designated specifically for itself.

As you can then see in figure 2.0, the calls are assigned to particular channels that operate on separate frequencies (f1, f2, f3, f4). These channels are called "traffic channels" in that they can carry both voice and data information. Besides voice and data information, this channel also carries associated control information in the form of LCO (Link Control Octets).

The transmit and receive frequencies for the mobiles are offset from each other (f1 and f2) (f3 and f4). This is called duplex offset. In the 800 MHz band, the offset is 45 MHz. Control of these resources is accomplished through the control channel that the mobile unit monitors continuously when not engaged in a communication session with another user or with the network.
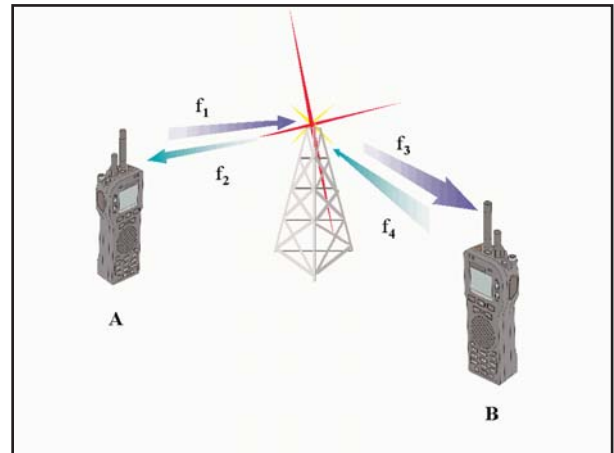

Figure 2.0 Two-way radio communications using trunked operation

How does "logging" a Control Channel Help Troubleshoot P25 Systems?

The ability to capture and save over the air control channel messages (OSPs) provides very unique testing capabilities in P25 systems. This includes:

1. The ability to verify specific messages being generated correctly from the P25 RFSS infrastructure, and the mobile radio. System operators need to be 100% assured that the messaging for radios is exact and is being sent at the right time and in sequence. Improper timing or corrupt messages can effectively take an entire group of radios off the network. The ability to log not only OSP information, but also ISP and LCO (Traffic Channel) information greatly enhances the engineer's ability to isolate potential problems.

2. Verification of encryption. The P25 standard allows for the traffic channels (carrying voice or data) and the control channel to be encrypted. Logging the control channel can show the system operator whether the proper encryption algorithm identifier (ALGID) is being sent. In addition, the 2975 can optionally support AES as well as DES encryption and can be used to decrypt an encrypted control channel to verify that the encryption is not interfering with the messaging.

3. Field troubleshooting of radio "interoperability" problems. Since the P25 standard is an open standard, there are many potential suppliers of P25 equipment. Although the standards are well written and provide most of the information about implementing the proper protocol, sometimes interpretation variance of these standards can lead to radios that simply will not work on a given system. The 2975 allows the user to verify what the control channel is sending and then allows the system engineer or designer to verify radio interoperability with that control channel.

Understanding the different types of control channel formats used in P25 systems

The P25 control channel messages are provided in two formats, single and multi-block TSBK's or Trunking Signaling Blocks. Most of the control channel information is sent via the single TSBK, with the multi-block TSBKs reserved for messaging that requires more extensive information than can be carried in a single TSBK. See figure 3.0 for Single TSBK formats.
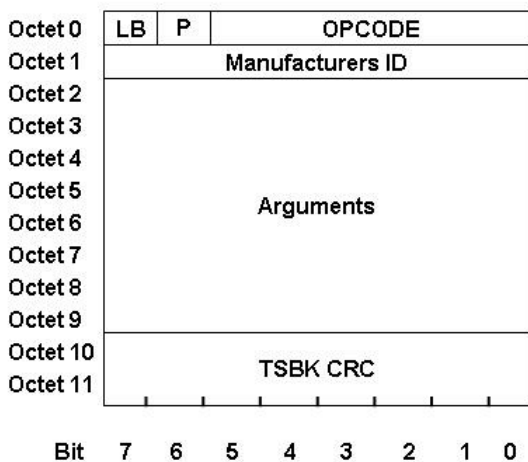
Figure 3.0 Single Block Packet Structure (Single Block TSBK) format

There are two different multiple block formats, one multiple block format uses the normal Unconfirmed Data Header format, with a special SAP identifier in the header that states it is to be processed as multiple block trunking information. The other type is very similar, except that the header contains additional information that includes embedded opcodes and trunking specific parameters for use in the multi-block TSBK. This is called the alternative MBT header. What determines the use of these two different types of message formats depends on the system implementation and the type of messages sent. See figure 4.0 for the multi-block TSBK formats.
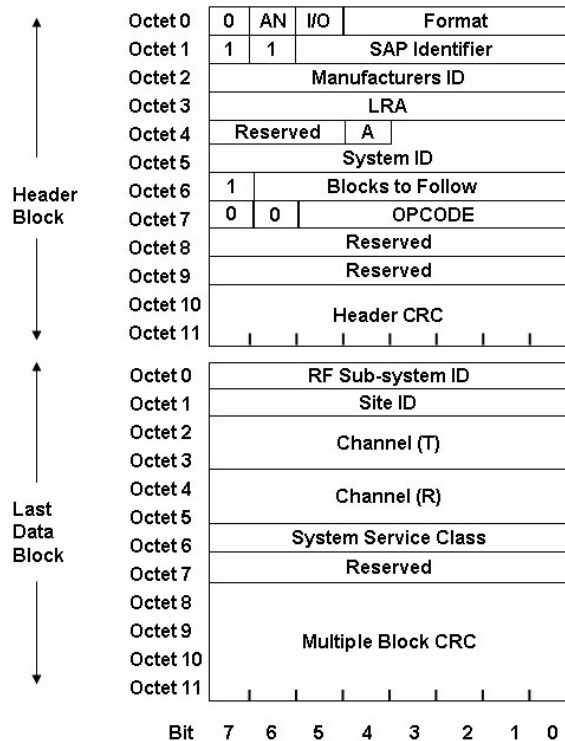
Figure 4.0 Multiple Block TSBK formats (RFSS Status Broadcast Message Shown)

Control channel messages that are logged

In review of the TIA/EIA-102 Standard, we see there are a number of control channel messages defined, both in the multi-block and single block formats. These can be broken down into three primary messaging groups, Voice Service, Data Service and Control and Status OSPs. The Voice Service OSPs deal with the transactions (messaging) sent between the control channel and the user to establish voice communications. Consequently, the data services act much in the same manner to support data service establishment. However, by far, the majority of the control channel signaling occurs for Control and Status Information. This information is critical to both the subscriber (user) and the RFSS (system

infrastructure) in that it sets up communication parameters before voice or data communication can occur.

The following is a list of control channel messages that can be logged by group:

Voice Service OSPs: **TIA Designation**

Group Voice Channel Grant	(GRP_V_CH_GRANT)
Group Voice Channel Grant Update	(GRP_V_CH_GRANT_UPDT)
Group Voice Channel Update-Explicit	(GRP_V_CH_GRANT_UPDT_EXP)
Unit to Unit Answer Request	(UU_ANS_REQ)
Unit to Unit Voice Service Channel Grant	(UU_V_CH_GRANT)
Telephone Interconnect Voice Channel Grant	(TELE_INT_CH_GRANT)
Telephone Interconnect Answer Request	(TELE_INT_ANS_REQ)
Unit to Unit Voice Channel Grant Update	(UU_V_CH_GRANT_UPDT)
Tel. Interconnect Channel Grant Update	(TELE_INT_CH_GRANT_UPDT)

Data Service OSPs

Individual Data Channel Grant	(IND_DATA_CH_GRANT)
Group Data Channel Grant	(GRP_DATA_CH_GRANT)
Group Data Channel Announcement	(GRP_DATA_CH_ANN)
Group Data Channel Announcement, Explicit	(GRP_DATA_CH_ANN_EXP)

Control and Status OSPs

Acknowledge Response - FNE	(ACK_RSP_FNE)
Adjacent Status Broadcast	(ADJ_STS_BCST)
Authentication Command	(AUTH_CMD)
Call Alert	(CALL_ALRT)
Deny Response	(DENY_RSP)
Extended Function Command	(EXT_FNCT_CMD)
Group Affiliation Query	(GRP_AFF_Q)
Group Affiliation Response	(GRP_AFF_RSP)
Identifier Update	(IDEN_UP)
Message Update	(MSG_UPDT)
Network Status Broadcast	(NET_STS_BCST)
Protection Parameter Broadcast	(P_PARM_BCST)
Protection Parameter Update	(P_PARM_UPDT)
Queued Response	(QUE_RSP)
RFSS Status Broadcast	(RFSS_STS_BCST)
Secondary Control Channel Broadcast	(SCCB)
Status Query	(STS_Q)
Status Update	(STS_UPDT)
System Service Broadcast	(SYS_SRV_BCST)
Unit Registration Command	(U_REG_CMD)
Unit Registration Response	(U_REG_RSP)
De-Registration Acknowledge	(U_DE_REG_ACK)
Location Registration Response	(LOC_REG_RSP)
Radio Unit Monitor Command	(RAD_MON_CMD)
Roaming Address Command	(ROAM_ADDR_CMD)
Roaming Address Update	(ROAM_ADDR_UPDT)

Voice Service ISPs: **TIA Designation**

Group Voice Service Request	(GRP_V_REQ)
Unit To Unit Voice Service Request	(UU_V_REQ)
Unit To Unit Voice Service Answer Response	(UU_ANS_RSP)
Telephone Interconnect Request-Explicit Dialing	(TELE_INT_DIAL_REQ)
Telephone Interconnect Request-Implicit Dialing	(TELE_INT_PSTN_REQ)
Telephone Interconnect Answer Response	(TELE_INT_ANS_RSP)

Data Service ISPs

Individual Data Service Request	(IND_DATA_REQ)
Group Data Service Request	(GRP_DATA_REQ)

Control and Status ISPs

Acknowledge Response - Unit	(ACK_RSP_U)
Authentication Query	(AUTH_Q)
Authentication Response	(AUTH_RSP)
Call Alert Request	(CALL_ALRT_REQ)
Cancel Service Request	(CAN_SRV_REQ)
Emergency Alarm Request	(EMRG_ALRM_REQ)
Extended Function Response	(EXT_FNCT_RSP)
Group Affiliation Query Response	(GRP_AFF_Q_RSP)
Group Affiliation Request	(GRP_AFF_REQ)
Identifier Update Request	(IDEN_UP_REQ)
Message Update Request	(MSG_UPDT_REQ)
Protection Parameter Request	(P_PARM_REQ)
Status Query Request	(STS_Q_REQ)
Status Query Response	(STS_Q_RSP)
Status Update Request	(STS_UPDT_REQ)
Unit Registration Request	(U_REG_REQ)
De-Registration Request	(U_DE_REG_REQ)
Location Registration Request	(LOC_REG_REQ)
Radio Unit Monitor Request	(RAD_MON_REQ)
Roaming Address Request	(ROAM_ADDR_REQ)
Roaming Address Response	(ROAM_ADDR_RSP)

LC Messages

Group Voice Channel User
Group Voice Channel Update
Unit to Unit Voice Channel User
Group Voice Channel Update - Explicit
Unit to Unit Answer Request
Telephone Interconnect Voice Channel User
Telephone Interconnect Answer Request
Call Termination/Cancellation
Group Affiliation Query
Unit Registration Command
Unit Authentication Command
Status Query
System Service Broadcast
Secondary Control Channel Broadcast
Adjacent Site Status Broadcast
RFSS Status Broadcast
Network Status Broadcast
Status Update
Message Update
Call Alert
Extended Function Command
Channel Identifier Update
Protection Parameter Broadcast

Configuring the 2975 to Decode Control Channel Messages

Setting up the 2975 to monitor and log control channel OSPs, ISPs or LC Messages, simply requires that Option 2975OPT6 is enabled.

Using the 2975 to Decode Control Channel Messages

Once the 2975 has been enabled with 2975OPT6, using the 2975 to log the control channel is very easy. By simply tuning to the appropriate trunking OSP control channel, mobile ISP channel or traffic channel, the user can decode a variety of control channel messages associated with each channel.

The quickest way to set up a system is to enable the duplex or receiver mode which will enable the user to tune the receiver to a desired frequency to "listen" to the appropriate inbound, outbound or traffic channel. Figure 5.0 shows how to setup a 2975 with the receiver mode, spectrum analyzer and control channel logger tile enabled.

Figure 5.0 Selecting Duplex Mode with Control Channel Logger and Spectrum Analyzer

As can be seen, with the 2975, users can log the channel message in three different modes, the symbols, the octets and the actual messages. This allows for great flexibility in logging the channel for short or long term analysis of the channel condition.

Logging of the base-band "Raw Symbols". This logs the digitized symbols from the base-band RF. This will allow engineers to obtain control channel symbols before the de-interleaving and error correction process to test demodulator design. See figure 6.0 for an example of this type of decoding.
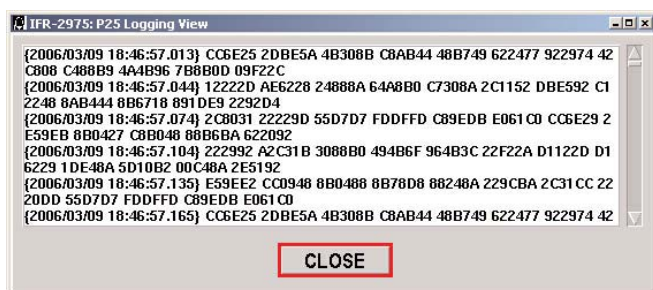

Figure 6.0 Logging Raw Symbols

Logging of the "Octets". This is done after the interleaving and error correction processes and provides the decoded Octets from either the OSP, ISP or LC Messages. See figure 7.0 for an example of the logged "Octets".
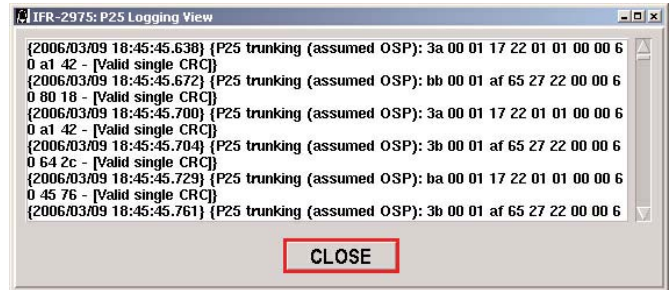

Figure 7.0 Logging Octets

Logging of the actual "Messages". This allows the actual OSP, ISP of LCO messages to be decoded and the internal elements of the message displayed. See figure 8.0 for an example of a decoded control channel from a VHF system using multi-block messaging.
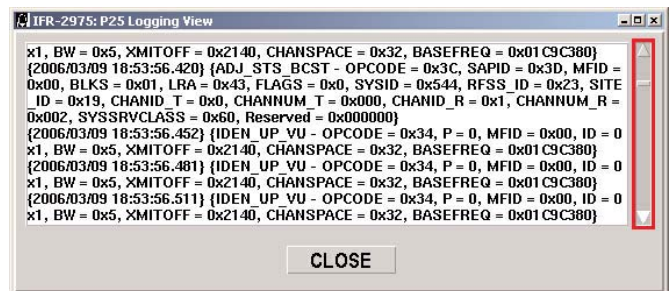

Figure 8.0 Logging the Decoded Control Channels

Understanding the Detailed Information

As we look at the detailed information about the control channel, we can see various bits of information coming across. What exactly does this mean? Looking at the decoded information in more detail allows us to understand how the 2975 logs the control channel information.

Raw Symbols

It is important to understand that the Raw Symbol mode of the logger provides access to the baseband RF symbols prior to the de-interleaving and error correction processes. When selecting this mode, we get information that looks like the following:

```
{2006/03/09 18:46:57.199} 12222D AE6228 24888A 64A8B0
C7308A 2C1152 DBE592 C12248 8AB444 8B6718 891DE9
2292D4
{2006/03/09 18:46:57.226} 2C8031 22229D 55D7D7 FDDFFD
C89EDB E061C0 CC6E29 2E59EB 8B0427 C8B048 88B6BA
622092
{2006/03/09 18:46:57.257} 222992 A2C31B 3088B0 494B6F
964B3C 22F22A D1122D D16229 1DE48A 5D10B2 00C48A
2E5192
{2006/03/09 18:46:57.287} E59EE2 CC0948 8B0488 8B78D8
88248A 229CBA 2C31CC 2220DD 55D7D7 FDDFFD C89EDB
E061C0
{2006/03/09 18:46:57.317} CC6E25 2DBE5A 4B308B C8AB44
48B749 622477 922974 42C808 C488B9 4A4B96 7B8B0D
09F22C
{2006/03/09 18:46:57.348} 12222D AE6228 24888A 64A8B0
C7308A 2C1152 DBE592 C12248 8AB444 8B6718 891DE9
2292D4
{2006/03/09 18:46:57.379} 2C8031 22229D 55D7D7 FDDFFD
C89EDB E061C0 CC6E29 2E59EB 8B0427 C8B048 88B6BA
622092
{2006/03/09 18:46:57.409} 222992 A2C31B 3088B0 494B6F
964B3C 22F22A D1122D D16229 1DE48A 5D10B2 00C48A
2E5192
{2006/03/09 18:46:57.439} E59EE2 CC0948 8B0488 8B78D8
88248A 229CBA 2C31CC 2220DD 55D7D7 FDDFFD C89EDB
E061C0
```

The first part of the information is the date. This is obtained from the 2975's internal date clock. The format is $yyyy/MM/DD$. Following the date information is the detailed time information. This information is displayed in either 12 or 24 hour formats. The detail of the time stamp goes down to 1/1000th of a second for appropriate resolution. Following the Date and Time stamp information, there are 12 groups of six hexadecimal characters that are the recovered symbols.

Raw P25 Trunking Octets

Following the "Raw Symbols", the 2975 goes on further to perform a decode to the Octet level of the data packets used in the OSP broadcast format. Below we can see the decoded Octets.

```
{2006/03/09 18:45:46.216} {P25 trunking (assumed OSP): 3b 00
01 af 65 27 22 00 00 60 64 2c - [Valid single CRC]}
{2006/03/09 18:45:46.245} {P25 trunking (assumed OSP): 3a 00
01 17 22 01 01 00 00 60 a1 42 - [Valid single CRC]}
{2006/03/09 18:45:46.276} {P25 trunking (assumed OSP): bb 00
01 af 65 27 22 00 00 60 80 18 - [Valid single CRC]}
{2006/03/09 18:45:46.306} {P25 trunking (assumed OSP): 3a 00
01 17 22 01 01 00 00 60 a1 42 - [Valid single CRC]}
{2006/03/09 18:45:46.312} {P25 trunking (assumed OSP): 3b 00
01 af 65 27 22 00 00 60 64 2c - [Valid single CRC]}
{2006/03/09 18:45:46.337} {P25 trunking (assumed OSP): ba 00
01 17 22 01 01 00 00 60 45 76 - [Valid single CRC]}
{2006/03/09 18:45:46.368} {P25 trunking (assumed OSP): 3b 00
01 af 65 27 22 00 00 60 64 2c - [Valid single CRC]}
```

These Octets are further defined in TIA/EIA-102.AABC. Since each of the trunking signaling blocks utilize 12 Octets (0 - 11), each line of the decoded control channel octets shows the full TSBK structure and validation of the CRC for each TSBK. See figure 3.0. again for the TSBK structure.

As we saw with the decoded "Raw Symbols", the Octets are time stamped. Each of the Octets contain two hexadecimal elements over 12 octets.

Decoded Control Trunking

The final level of decoding offered by the 2975 is the actual decoding of the OSP message field elements. An example is as follows:

```
{2006/03/09 18:53:55.766} {IDEN_UP_VU - OPCODE = 0x34, P =
0, MFID = 0x00, ID = 0x1, BW = 0x5, XMITOFF = 0x2140, CHAN-
SPACE = 0x32, BASEFREQ = 0x01C9C380}

{2006/03/09 18:53:55.811} {NET_STS_BCST - OPCODE = 0x3B,
SAPID = 0x3D, MFID = 0x00, BLKS = 0x01, LRA = 0x01, Reserved
= 0x1, SYSID = 0x722, Reserved = 0x0000, WACNID = 0xAF652,
Reserved = 0x0, CHANID_T = 0x1, CHANNUM_T = 0x000,
CHANID_R = 0x1, CHANNUM_R = 0x00A, SYSSRVCLASS = 0x60}

{2006/03/09 18:53:56.360} {IDEN_UP_VU - OPCODE = 0x34, P =
0, MFID = 0x00, ID = 0x1, BW = 0x5, XMITOFF = 0x2140, CHAN-
SPACE = 0x32, BASEFREQ = 0x01C9C380}

{2006/03/09 18:53:56.420} {ADJ_STS_BCST - OPCODE = 0x3C,
SAPID = 0x3D, MFID = 0x00, BLKS = 0x01, LRA = 0x43, FLAGS =
0x0, SYSID = 0x544, RFSS_ID = 0x23, SITE_ID = 0x19, CHANID_T
= 0x0, CHANNUM_T = 0x000, CHANID_R = 0x1, CHANNUM_R =
0x002, SYSSRVCLASS = 0x60, Reserved = 0x000000}

{2006/03/09 18:53:56.452} {IDEN_UP_VU - OPCODE = 0x34, P =
0, MFID = 0x00, ID = 0x1, BW = 0x5, XMITOFF = 0x2140, CHAN-
SPACE = 0x32, BASEFREQ = 0x01C9C380}
```

Here we see the actual data and time stamped message, with the decoded message opcode showing the first message to be an NET_STS_BCST, as shown by the Opcode 34. We then find additional information throughout the message as shown in TIA/EIA-102.AABC and AABC-1. (Note: This message comes from a VHF/UHF OSP control channel format using multi-block messaging).

Retrieving Log Files From the 2975

The 2975 provides for users to easily retrieve information from their unit. Since the 2975 logs files to its internal hard-drive and supports Ethernet connection to the system, the files can be obtained by following these easy steps:

1. Connect an Ethernet cable to the 2975 if you are on a LAN. You will need a cross over cable if you are connecting directly to a computer.

2. Enable a valid IP address on the 2975. This is done by selecting Mode, then the number 7, then 1 for the configuration screen. The 2975 supports DHCP and Fixed IP addressing, use DHCP if you are on a LAN or fixed if you are connected to a computer. If you are connected directly, use an IP address similar to the PC.

3. Verify that the 2975 can be accessed through your network. This can be done by "pinging" the unit's IP address.

4. FTP to the unit by a host program. Use Filezilla or WS-FTP Pro as examples.

5. The log files reside in /usr/p25_log/ directory.

6. Move the file to your computer.

7. You can now analyze the data.

Conclusion

By utilizing the power of this instrument, engineers and technicians can quickly ascertain interoperability problems and other problems associated with control channel implementations. The 2975 provides the various decoded formats for a variety of engineers in design, production and field test environments. For more information on the 2975, go to www.p25.com.

w w w . a e r o f l e x . c o m

i n f o - t e s t @ a e r o f l e x . c o m

AEROFLEX
A passion for performance.

Our passion for performance is defined by three
attributes represented by these three icons:
solution-minded, performance-driven and customer-focused.

Part No. 46891/917, Issue2, 06/06