

Appendix - 1xEV-DO

1. Overview - cdma2000 1xEV-DO

cdma2000 1xEV-DO (hereinafter referred to as EVDO) wireless protocol is a 3G wireless mobile broadband technology that provides data transmission capability and is available from multiple service providers. EVDO stands for Evolution Data Only/Evolution Data Optimized. EVDO provides mobile stations with connectivity to the Internet and push-to-talk (PTT) voice over IP (VoIP).

The DRT system can intercept Forward/Return Link channels using *cdma2000 1xEV-DO Release 0 and Revision A*.

1.1. Hardware Requirements

The DRT system must be a DRT1301C, DRT1183C, DRT120xC or DRT121xC system.

1.1.1. Required Keys

This capability requires the DRT system key to include the 1xEV-DO key and the Packet Data Recorder key.

1.1.2. Number of Base Stations

The table below shows the maximum number of Base Stations each module or unit (in the case of DRT1301C) can monitor. DSP resources used to follow calls for a 1xEVDO service are available to all monitored Base Stations for that service.

EVDO: Number of Base Stations/Calls Monitored

Type of DSP	Maximum Number of Base Stations/Calls Monitored
DRT1301C (3xDSP)	Forward Only = 6 Base Stations and 12 half duplex calls Forward and Reverse = 2 Base Stations and 4 full duplex calls
WPM3 (2xDSP)	Forward Only = 4 Base Stations and 8 half duplex calls Forward and Reverse = 2 Base Stations and 4 full duplex calls per WPM3

1.2. Site Survey

Site Survey may be used to identify the EVDO control channels in the area. For Site Survey, the Resource Usage bar on the **Configuration Wizard Service Settings** page does not identify the Base Station number (as it does when the selected service is EVDO). Instead, for Site Survey, the bar identifies the number of receiver channel resources. For the DRT1301C, you must select a minimum of 32 receivers on this bar in order to detect an EVDO Base Station because for Site Survey a DSP is equivalent to 16 receivers.

1.3. System ID vs. Sector ID

In some places, *Alaska* reports the Sector ID as the System ID. The Sector ID and System ID are the same within *Alaska*.

1.4. Logging

Activity/Event Logs and Chronologs may be created.

1.5. Privacy Profile

This format is affected by the Privacy Profile selected in *Alaska*.

1.6. User Interfaces

1.6.1. Alaska - Primary User Interface

The main configuration and monitoring interface is *Alaska*. *Alaska* is a user interface that is typically loaded onto a PC connected to the DRT system.

1.6.2. Hawaii - Provided for Evaluation

With *DRT1000 System Software R6.4.0*, DRT is including a new web browser user interface (UI) for evaluation.

Instructions for installing and initially opening *Hawaii* are described in the Cellular Appendix to the [DRT1000 Receive Software Manual](#) and also included in HELP for both *Alaska* and *Hawaii*. Then see the [Hawaii section](#).

When configuring the mission resources for EVDO, consider the information supplied in the [Receiver Resources](#) table.

Targeting is similar to how it is done with the mission is configured with *Alaska*, but *Hawaii* has its own Target Lists. Alternatively, *Hawaii* may utilize a *Crosshair* Targeting Database. See the [Targeting section](#) for details.

2. Alaska - EVDO

2.1. Configure Mission - 1xEV-DO

Open the **Configuration Wizard** normally and proceed to the **Service Settings** page.

- Select **1xEV-DO** as the **Service Type**.
- In the **Frequency Plan** field, select the frequency band to be covered.
- The **Monitor reverse frequency bands** box is checked by default. This selection allows you to monitor both Forward and Return channels. To monitor only Forward channels, uncheck the box.
- The Resource Usage bar displays the number of DSPs assigned to this service and whether they are assigned to monitor Forward or Reverse channels. The number of Base Stations that the DRT system can monitor with the assigned number of DSPs appears beneath the Resource Usage bar. Refer to the [Number of Base Stations/Calls Monitored table](#) for information on what your system is capable of. Also refer to the notes in the [PCAP File Data](#) section.
- Click **Next**.

Service Settings

Service Type: 1xEV-DO

Frequency Plan: 1xEV-DO Cellular 800 MHz

☒ Monitor reverse frequency bands

Service Name (CaseV): 1xEV-DO Cellular 800 MHz

Comment: Covers the 800 MHz Cellular band

Resource Usage

Total DSPs: 8 (Forward: 4, Reverse: 4)

8 base stations, 16 full duplex calls can be monitored.

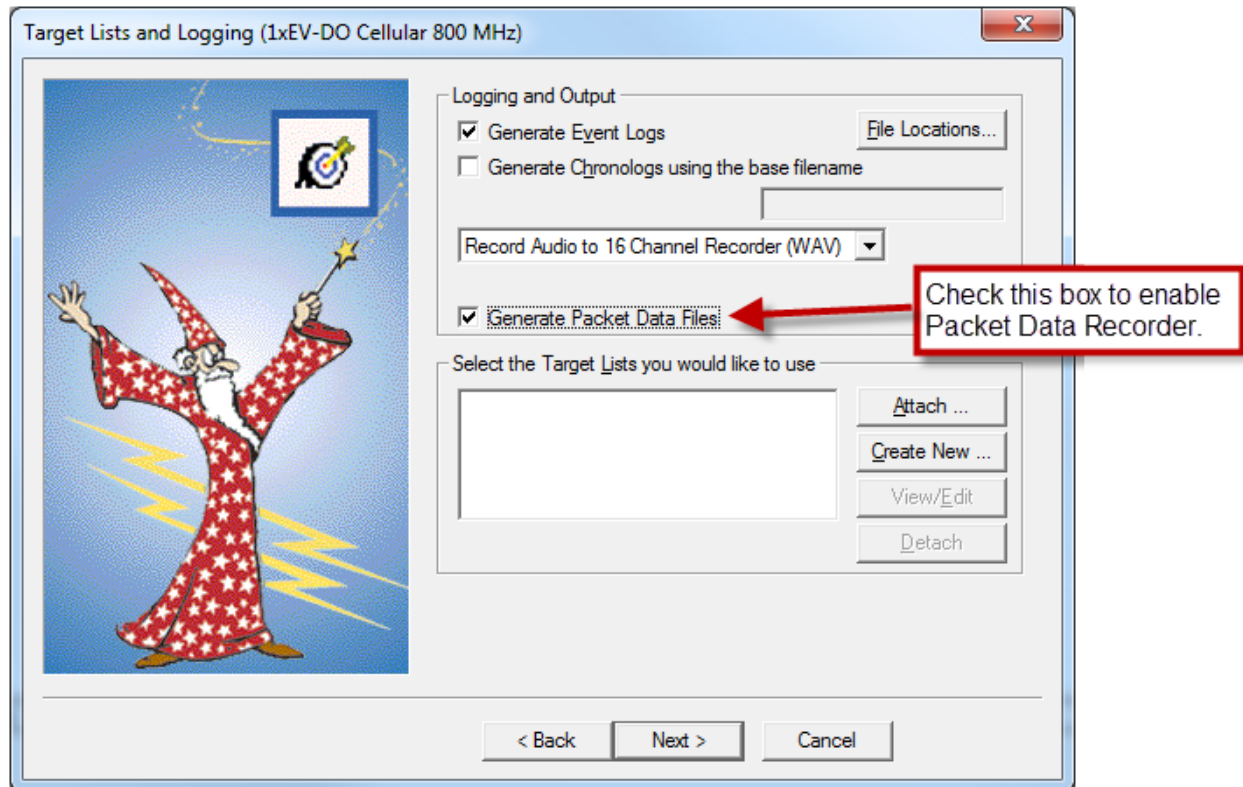
Make sure 4 full duplex calls can be monitored.

< Back Next > Cancel

The Monitor reverse frequency bands box is checked by default. Uncheck it to monitor Forward channels only.

On the **Target Lists and Logging** page:

- To capture the Packet Data (enable packet data recording) check the **Generate Packet Data Files** box .



- Attach a Target List. See the [Target section](#) for information on EVDO target types. Ensure that the *Target Match Actions* **Monitor** and **Output** are selected.
- Logging is available (both Event Logs and Chronologs).
- Proceed through the rest of the wizard normally.

Two antennas are required for Antenna Diversity. See the [Antenna Diversity section](#) for information on enabling Antenna Diversity.

2.1.1. Enable Channel ID Log

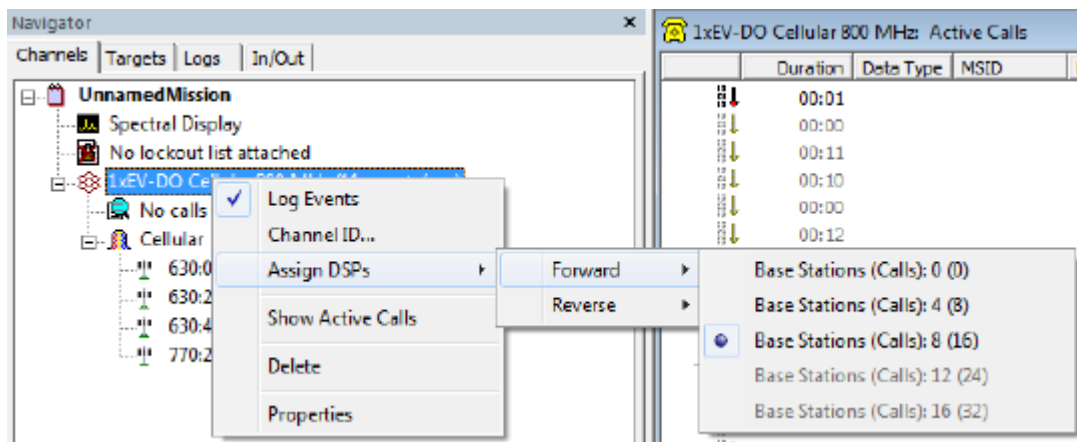
Overhead channel data is displayed and may be retained in the [Channel ID Log](#).

You may enable the Channel ID Logs after the wizard has finished. This is done normally through the Channel ID tool (opened through main menu>**Tools>Channel ID**, or clicking the Channel ID toolbar button). Note that you must run Channel ID again after Channel ID logging has been enabled. The log contents are described in the [Channel ID Log Fields](#) section.

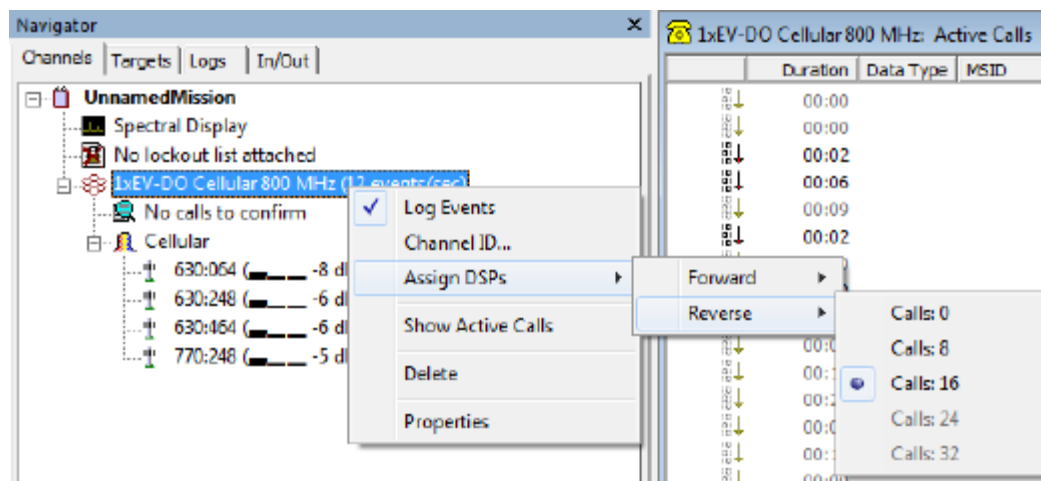
2.1.2. Change Receiver Assignments

The number of DSP receiver resources assigned to monitor the Forward and Return channels may be changed via the **Navigator's Channels** page > right-click the 1xEV-DO service > select **Assign DSPs**, then **Forward** (to monitor Forward channels), and select the number of Base Stations (Calls) to be monitored. Repeat the steps to monitor Return channels selecting **Reverse** and then the number of Base Stations (Calls).

Assign DSPs to Monitor Forward Channels

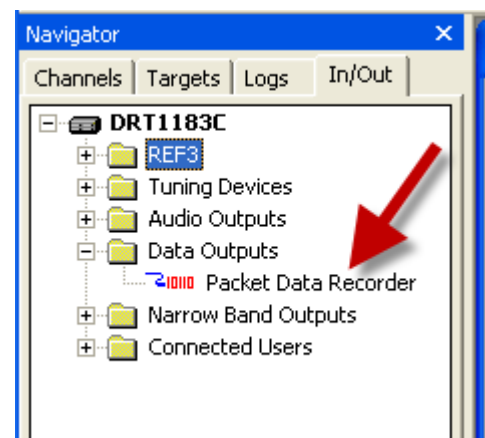


Assign DSPs to Monitor Return Channels



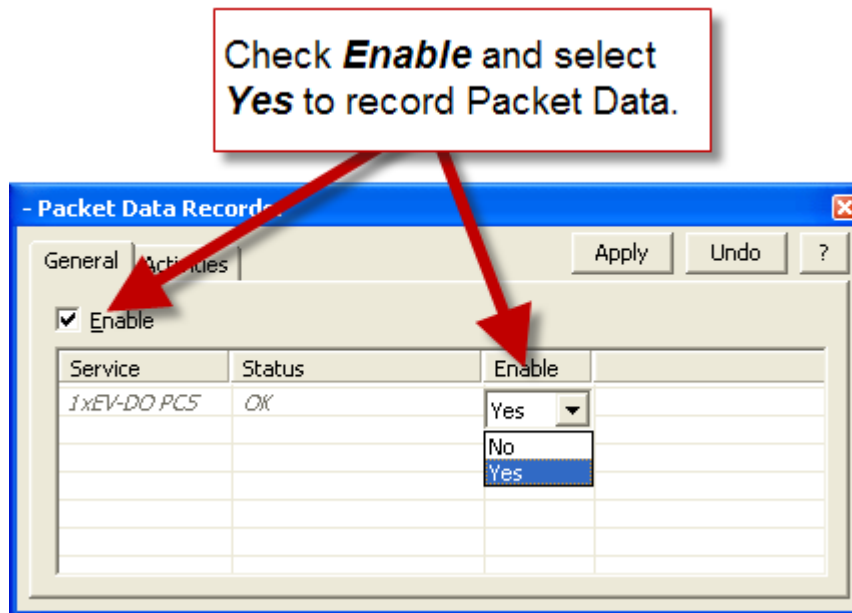
2.1.3. Manually Enable Packet Data Recording

If you did not enable the Packet Data Recorder as shown above in the wizard, you can do this later without going through the wizard again. Packet Data Recording must be enabled to save the intercepted data: after the wizard has finished, go to the **Navigator's In/Out** page and double-click the **Packet Data Recorder** line to open the **Packet Data Recorder Properties** sheet.



The **Packet Data Recorder Properties General** page displays a row for each configured service with the service name in the **Service** column.

- Check the **Enable** box to enable Packet Data Recording for ALL services.
- Then for an individual service, select **Yes** in the **Enable** column.



During the mission, the **Packet Data Recorder Activities** page will indicate when a data packet is currently being recorded including its filename.

General Activities						
Apply Close ?						
Service	Start Time	Target	Priority	Filename	File Size	
1xEV-DO Cellular 80...	2/25/2013 2:25:38 PM	Any Subnet	7	CE138DA773C2.pc...	2 KB	
1xEV-DO Cellular 80...	2/25/2013 2:25:51 PM	Any Subnet	7	CE138DA79C52.pc...	0 KB	
1xEV-DO Cellular 80...	2/25/2013 2:25:51 PM	Any Subnet	7	CE138DA79C12.pc...	0 KB	
1xEV-DO Cellular 80...	2/25/2013 2:25:50 PM	Any Subnet	7	CE138DA799C2.pc...	0 KB	
1xEV-DO Cellular 80...	2/25/2013 2:25:50 PM	Any Subnet	7	CE138DA798C2.pc...	135 KB	
1xEV-DO Cellular 80...	2/25/2013 2:25:50 PM	Any Subnet	7	CE138DA798A2.pc...	0 KB	
1xEV-DO Cellular 80...	2/25/2013 2:25:48 PM	Any Subnet	7	CE138DA79282.pcap	1 KB	
1xEV-DO Cellular 80...	2/25/2013 2:25:48 PM	Any Subnet	7	CE138DA79582.pcap	2 KB	

See the [PCAP Files section](#) for information on where the PCAP files are stored and how to change the storage location.

2.2. Antenna Diversity - EV-DO

Antenna Diversity is the use of two antennas to monitor a single band. This configuration can enhance system performance by resulting in a higher detected signal strength.

2.2.1. Antenna Diversity Hardware Configuration

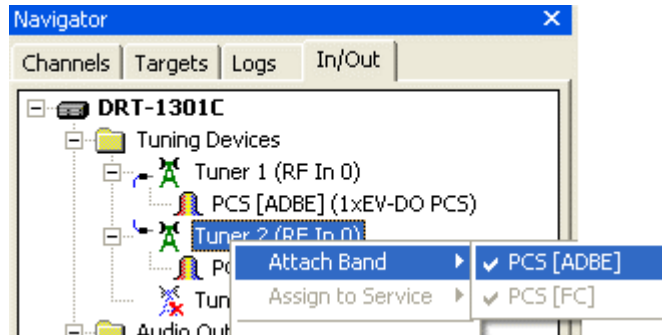
Instead of connecting one antenna to the lead tuner, connect two receive antennas to the **RF IN** connectors on two different tuners.

- For the DRT1301C, when the environmental front panel is attached, you will need a cable that has more than one RF IN connector. Cable 428-02129-001 is an example of such a cable. Contact DRT for more information.

2.2.2. Antenna Diversity Software Configuration

Use the **Configuration Wizard** to create the mission normally.

- After the wizard has finished, go to the **Navigator's In/Out** page.
- Identify a tuner that has an antenna connected but does not have a band attached. If the wizard has attached bands to both of the tuners that have antennas connected to them, identify the tuner with the band that you do NOT want to monitor, right-click it and select **Detach Band** to remove that band.
- Right-click the tuner with no band attached (but has an antenna connected) > select **Attach Band** and then select the same band that is attached to the other tuner (that has an antenna connected). The end result should be two tuners, each physically connected to its own antenna, now have the same band attached. A maximum of two tuners may be attached to a single band.
- Monitor the service in the normal way.



2.3. Channel ID - 1xEV-DO

The 1xEV-DO service provides dedicated search receivers that allow Channel ID to take place during intercept without deleting base stations. If the system reports that not enough resources are available to run Channel ID, drop all calls and run Channel ID again.

NOTE: In some cases, during Channel ID, control channels may be identified and associated with an incorrect band. This may happen when two bands overlap and a channel number in one band corresponds and lines up with the frequency of a channel of another band. For example, EV-DO channel 175:306 in the AWS band is also channel 175:306 in the 2 GHz band. Thus, if the EV-DO service ran Channel ID to scan the 2 GHz band, Channel 175:306 would be detected. Likewise, Channel 175:306 would be detected if Channel ID was also run against the AWS band. Because 175:306 was detected in both bands, the channel would be associated with both bands, duplicating the same channel.

Currently if the system knows that the channel is not really in the band in which *Alaska* displays it, the **Channel Properties Details** page displays a WARNING that the channel is not really in Band X but in Band Y. The base station reports the band (so 175:306 might report its band as AWS) allowing *Alaska* to display a warning in **Channel Properties** immediately, indicating that the band reported by the base station does not match the associated band.

2.3.1. Signal Quality

For a complete description of how to use the Channel ID tool, see the [Cellular Appendix](#) in the *Alaska* HELP files..

When running Channel ID for EVDO, you can specify a minimum Energy per Chip-to-Noise Ratio (Ec/No) and Signal Strength (RSSI) value to use as search criteria for channels within bands. This results in the DRT unit returning only signals with good quality. Specifying the lowest limit of the signal quality that you want lets you search for only signals with higher Ec/No ratio measurements and Signal Strength. Signal Quality bars in the Ec/No column indicate: 1 bar=POOR, 2 bars=FAIR, 3 bars=GOOD.

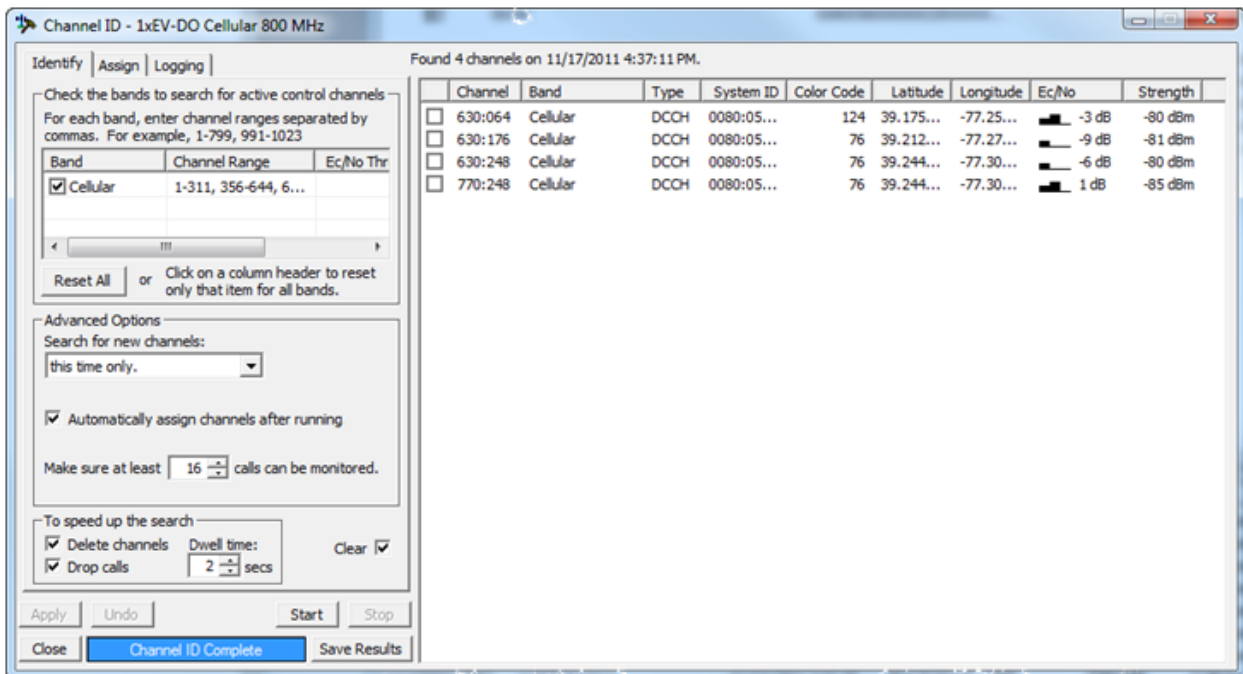
If channels are automatically assigned, signals with the best Ec/No values will be selected. If two signals are selected that have the same Ec/No values, the system selects the signal with the higher Strength (RSSI) to report. If system resources are low, signals with the best quality are reported that have the highest Ec/No and Signal Strength values.

Once Channel ID is run, the threshold values appear in the **Found Channels** window that fall within the threshold limits that you specified. Values in the columns can be sorted.

2.3.1.1. Specify Ec/No Threshold Value for Channel ID

- Open the Channel ID tool (**Main Menu>Tools>Channel ID**).
- Mark the check box for Bands to search and double-click the **Channel Range** field to add a range of channels to search.
- Click the **Ec/No Threshold** field and enter a value between -30 and 30 dB, with a signal quality resolution of 1 dB.
- Click the **Strength Threshold** (RSSI) field and enter a value between -30 and -120 dBm.
- Finish entering channel ranges to search for and click **Start**. When the system finishes identifying control channels, it brings up the **Assign** page for you to manually edit which control channel to monitor and how to allocate receivers, unless you have chosen to **Automatically Assign Channels** on the **Identify** page.
- Sort the **Ec/No** and **Strength** columns to view reported Ec/No and Signal Strength values.

The assigned channels also appear in the **Navigator**. For a description of the **Navigator** and channel monitoring, see [Monitor 1xEV-DO Mission](#).



2.3.2. Channel ID Log Fields - 1xEV-DO

For a complete description of how to configure Channel ID logging, see the [Cellular Appendix](#) of the *Alaska HELP* files. The Channel ID log file fields specific to EVDO are listed in the following table.

EVDO Specific Channel ID Log Fields

Field	Description
Frequency	Frequency in Hz
Channel Number	Channel number
System ID	Sector ID
Description	Band Description
Channel Type	2 = DCCH
Unit ID	Name of the DRT unit which detected this channel
UTCDate	This is the GPS date if the unit is attached to a GPS receiver. If there is no GPS receiver attached this will be zero (1/1/1970).
UTCTime	This is the GPS time if the unit is attached to a GPS receiver. If there is no GPS receiver attached this will be zero (00:00:00).
SystemDate	This is the date according to the unit, as set on the DRT unit's embedded controller, when the log file began. This should match the UTC Date if automatic GPS time synchronization is enabled and the attached GPS receiver is locked.
SystemTime	This is the time according to the unit, as set on the DRT unit's embedded controller, when the log file began. Formatted as HH:MM:SS. This should match the UTC Time if automatic GPS time synchronization is enabled and the attached GPS receiver is locked.
GPS State	GPS lock condition: 0 = unlocked; 1 = locked
LAT	This is the latitude reported by a GPS receiver attached to the DRT system (if enabled), or the manually set coordinates. This is not the latitude reported by the Base Station. It is in the following format: XXdXXmXX.XXXS. For instance Latitude 6°52'10.33" would be represented as: 6d52m10.33s + indicates North; - indicates South
LON	This is the longitude reported by a GPS receiver attached to the DRT system (if enabled), or the manually set coordinates. This is not the longitude reported by the

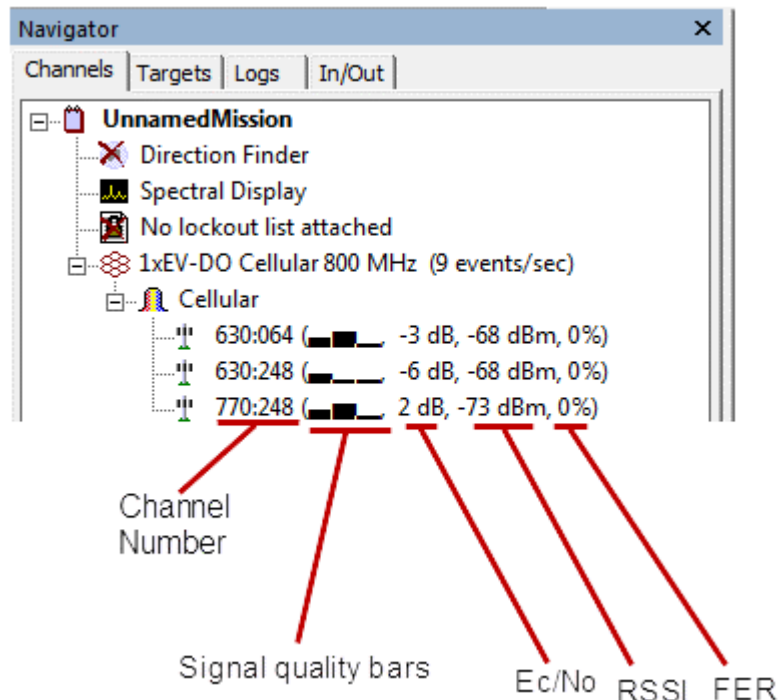
Field	Description
	Base Station. It is in the following format: XXXdXXmXX.XXXs. For instance Longitude 7°48'32.85" would be represented as: 7d48m32.85s + indicates East; - indicates West
Pilot PN Offset	Pilot PseudoNoise (PN) Offset. A method for assigning an offset to a base station that transmits a common pilot signal with respect to other base stations in a mobile telecommunications system. The common pilot signal is used to direct communications between mobiles and base stations. The Pilot Channel's PN offset. The PN offset defines a cell. The PN offset indicates the timing of the cell's short codes relative to system time (PN sequence offset in units of 64 PN chips).
Signal Strength	Relative Signal Strength Indicator (RSSI) in dBm of all Base Stations in the frequency.
Ec/No	Energy per Chip-to-Noise Ratio of the Base Station Pilot Channel
Sector LAT	This is the latitude as reported by the EV-DO Base Station . It is in the following form: XXdXXmXX.XXXs. For instance Latitude 6°52'10.33" would be represented as: 6d52m10.33s + indicates North; - indicates South
Sector LON	This is the longitude as reported by the EV-DO Base Station . It is in the following form: XXXdXXmXX.XXXs. For instance Longitude 7°48'32.85" would be represented as: 7d48m32.85s + indicates East; - indicates West

2.4. Monitor Mission Alaska - EV-DO

2.4.1. Navigator Channels Page

Once the **Configuration Wizard** has finished, Channel ID is run, and the **Navigator** pane opens.

Next to the service name there is an indicator in parenthesis that shows an events-per-second rate. This rate represents the number of events per second that the DRT1000 system has attempted to target on, averaged over the last five seconds.



DRT Company Confidential and Proprietary
USML XI(d)

The monitored Control Channels are displayed on the **Navigator's Channels** page. The channel number is identified as two numbers separated by a colon, such as 630:064. The first part of this sample number, 630, is the RF channel number. The second number, 064, is the Pilot PN Offset.

Signal quality values show a one-, two-, or three-bar graphic representation of signal quality ( ,  , ) that indicates varying degrees of signal strength and quality:

- If only 1 bar appears, the signal strength is POOR.
- If 2 bars appear, the signal strength is FAIR.
- If 3 bars appear, the signal strength is GOOD.

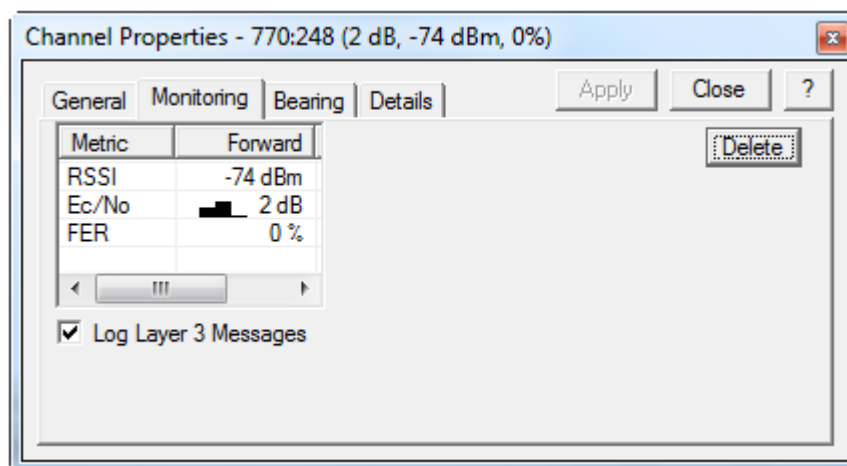
Other channel metrics are also displayed: the received signal strength (RSSI), the Ec/No (Energy per Chip to Noise Ratio of the Base Station Pilot Channel), and the Frame Error Rate (percentage). Note that the FER will always be 0 for this service.

This channel information is also shown on **Channel Properties**.

2.4.2. Channel Properties

Information about the detected forward control channels is displayed on the **Navigator**, on **Channel Properties**, on the Channel ID tool and, if enabled, is retained in a Channel ID log.

Open the **Channel Properties** sheet by double-clicking the channel shown on the **Navigator**. The channel information on the **Navigator Channels** page is shown on the **General** and **Monitoring** pages.



The information on the **Details** page is displayed in the normal way (click the **Refresh** button) and may be saved in the normal way (click the **Save** button). The latitude and longitude are that of the Base Station (self-reported) not the DRT system's GPS.



DRT Company Confidential and Proprietary
USML XI(d)

2.4.3. Channel ID Tool

The Channel ID tool displays some of the same information included in the Channel ID log file. An additional field reported here is the channel's **Color Code**. The channel's Color Code is NOT reported in the Channel ID log at this time.

Found 2 channels on 4/27/2010 1:46:45 PM.

	Channel	Band	Type	System ID	Ec/No	Color Code	Latitude	Longitude	Signal
<input type="checkbox"/>	630:064	Cellular	DCCH	0080:0580:0000:0025:100A:CE07:2400:EE01	-3 dB	19	39.175902...	-77.25...	-74 dBm
<input type="checkbox"/>	770:032	Cellular	DCCH	0080:0580:0000:0025:0C0A:CC23:8501:2A01	-9 dB	18	39.142569...	-77.41...	-100 dBm

2.4.4. Latitude and Longitude

Alaska and various log files report latitude and longitude; however, the source of the locating data may vary. For EVDO, the source may be the Base Station or a GPS receiver connected to the DRT receiver. The table below shows the source of the Lat/Lon data in the various windows and logs.








Sources of Lat/Lon Data in Alaska and Service Log Files

Alaska Window/Dialog or Log File	GPS Data Source
Channel ID Page	EVDO Base Station
Channel ID Log file	DRT System's GPS* and EVDO Base Station (Sector Lat/Lon)
Channel Properties Details page	EVDO Base Station (Sector Parameters)
Call Properties History Strength page	DRT System's GPS*
Activity Event Log	DRT System's GPS*
Chronolog	DRT System's GPS*

*System must be GPS capable (have GPS receiver attached/installed & GPS antenna connected), and GPS must be enabled in *Alaska*

2.4.5. Active Calls Window

Detected EVDO activity is monitored in the **Active Calls** window in the normal way. The table below describes the icons that are available for this service. The second table below describes the available **Active Calls** window fields.

EVDO Packet Data Recorder Icons:	
	Monitoring Forward only (simplex) data call. Additional icon  indicates when data is being recorded.
	Monitoring Forward and Return (duplex) data call.
	Grayed out version of icon indicates call no longer being monitored at all.
	Packet Data is being recorded.
	Packet Data could not be recorded.
	Packet Data is being recorded and logged.
Blank Line	Indicates data call has ended.

1xEV-DO Active Call Window Fields

Field Name	Column Header	Description
Unique ID	Unique ID	ID number that the DRT system gives to the call; all events related to the call will have the same Unique Connection (Call) ID
System ID	SID	Sector ID
Description	Description	From the Description field on the Target Properties sheet for the item that caused this number to be a hit.
Duration	Duration	Length of time call was received.
Start Time	Start Time	Time call started/began receiving
Stop Time	Stop Time	Time call stopped/was lost.
Last Event	Last Event	Last detected call or non-call event related to this call.
Event Count	#Es	Number of events related to this call.
Channel, Current	Chan	Current Traffic Channel Active Set: Channel:PN Offset, MAC Index. Multiple PN Offset/MAC Index pairs may be listed.
Channel, Control	Ctrl Chan	Control Channel that gives the mobile handset its Channel assignment.
Band, Current	Band	Description of the band; same as band name on Navigator .
Output Device, Fwd	Fwd Output Device	Not used yet.
Output Channel, Fwd	FOC	Not used yet.
Frequency, Current, Forward	Fwd Freq (MHz)	Displays the current forward frequency.
Caller ID	Caller ID	Not used yet.
MSID	MSID	Not used yet.
ESN	ESN	Not used yet.
Hit Number	Hit Number	Not used yet.
Target Number	Target Number	Number in the Target Properties sheet's Number field; may be a wildcard. See the Hit Number field for the actual number that fit the wildcard parameters.
Priority	Priority	The Target's priority (from the Target Properties sheet).
Target List	Target List	The Target List containing the target that generated this call as a hit.
Target Category (1-8)	Category 1...8	Categories on the Target Properties sheet (developed by operator to help with post-processing).
PSTN	PSTN	Public Switched Telephone Network (landline)10-digit telephone number used in the SIP URI for the Winphoria PTT protocol.
SIP URI	SIP URI	SIP URI - ASCII string value in the format <user>@<realm> used in SIP (Session Initiation Protocol).
Signal Strength, Rev.	RSS	Received signal strength of the reverse channel.
Reverse Ec/No	Rev Ec/No	Reverse channel Ec/No value.
Reverse Link Lock Status	R-Lock Status	Indicates the status of the receiver assigned to the reverse link signal. This field may say <i>Searching</i> , <i>Locked</i> or <i>Inactive</i> . <i>Searching</i> indicates that the receiver is attempting to acquire the reverse link signal. <i>Locked</i> indicates the reverse signal has been received. <i>Inactive</i> indicates receiver no longer searching for that call.
Data Session Type	Data Type	Indicates whether or not a Push-to-Talk (PTT) session is being monitored. If a PTT session is being monitored, the value in the Data Type column will be PTT. If no PTT session is being monitored, the value is BLANK.
UATI	UATI	UATI - 128-bit Unicast Access Terminal Identifier displayed as hexadecimal. The UATI is a unique temporary identifier that is assigned to a mobile when it enters a new subnet. The value is only displayed if the UATI assignment message is intercepted.

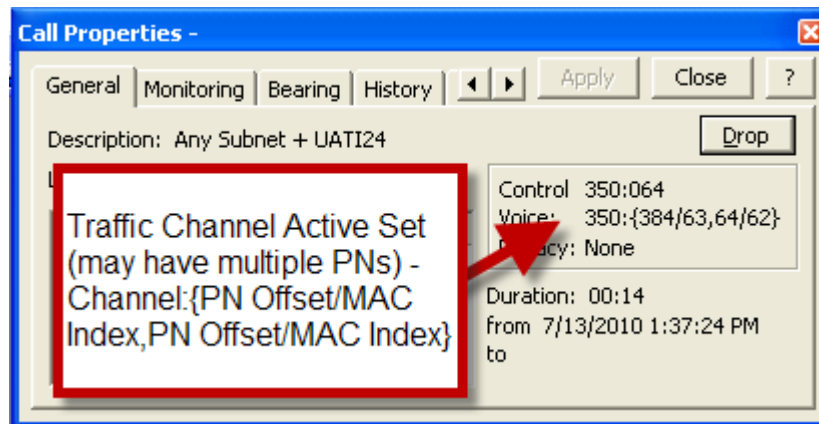
Field Name	Column Header	Description
Mobile IP NAI	NAI	NAI - Network Access Identifier ASCII string value in the format <user>@<realm> used in Mobile IP registration and authentication.

In the **Active Calls** upper pane, when the **Last Event** column reports a *Packet Data Out* event, that indicates that packet data files will be/are being transmitted and captured by the DRT system.

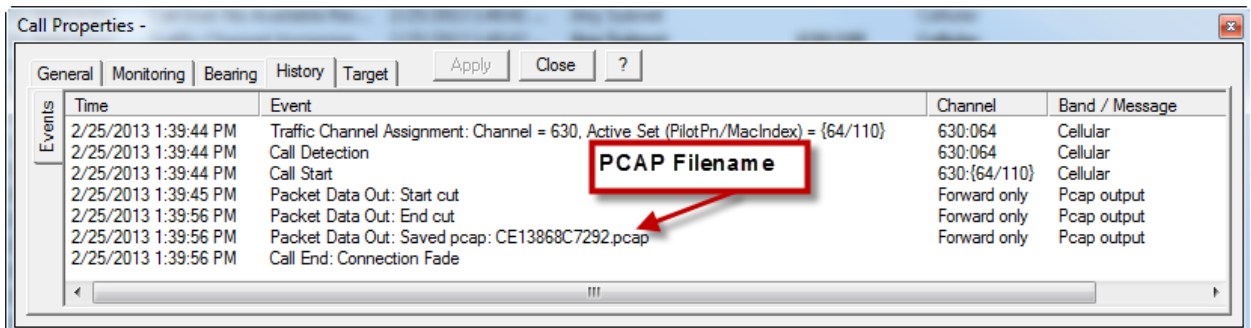
2.4.5.1. Call Properties

Within the **Active Calls** window, double-click a call (upper pane) or event (lower pane) to bring up **Call Properties** in the normal way for additional information.

The current Traffic Channel Active Set is displayed on the **General** page in the **Voice** field (as well as in the **Active Calls** window **Current Channel** field). The Traffic Channel Active Set may include multiple PN Offsets: Channel:{PN Offset,/MAC Index,PN Offset/MAC Index}.



The **Call Properties History Events** page displays the PCAP filename.



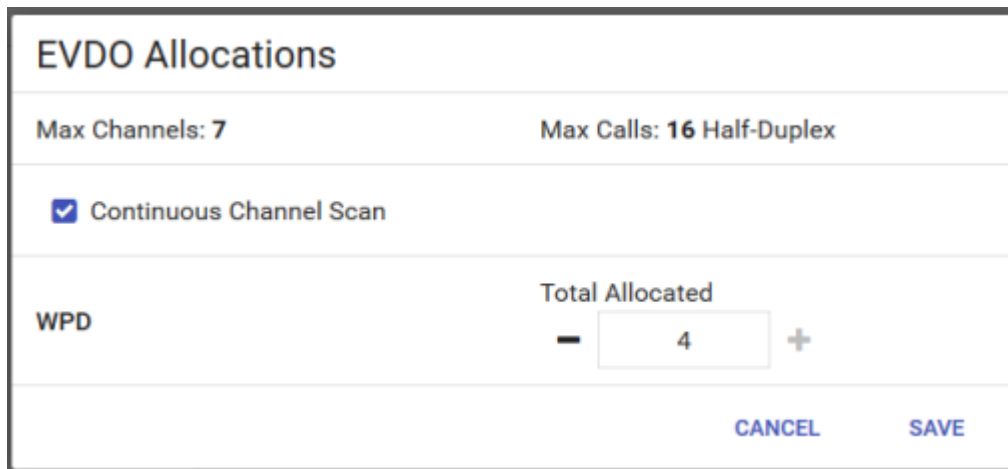
3. Hawaii - EVDO

Hawaii is the web browser user interface that may be used instead of *Alaska* to configure and monitor a mission. The Cellular Appendix provides instructions on how to use *Hawaii*. Note that other information specific to the service (for example, [targeting types](#) and [Chronolog definitions](#)) is described below.

Hawaii does not support:

- System ID Targeting

Start by configuring a mission that includes the EVDO protocol. *Hawaii* will assign receivers based on the receivers available in the system, the number of protocols configured, etc. If you want to review those assignments in detail for EVDO, on the **Resources** page, on the EVDO protocol line click **Settings** to bring up the **EVDO Allocations** view. Consult the [EVDO Number of Base Stations/Calls Monitored table](#) for information on how many Base Stations and Calls may be monitored by the DSP hardware in your system.



EVDO Allocations	
Max Channels: 7	Max Calls: 16 Half-Duplex
<input checked="" type="checkbox"/> Continuous Channel Scan	
WPD	Total Allocated - 4 +
CANCEL SAVE	

Continue on to the **Targeting Summary** page. This is where you add a Target List if using *Hawaii* Target List; if using *Crosshair*, continue on to the **Settings** page. See the [Targeting section](#) for details on targeting EVDO devices.

3.1. Enable Packet Data Recording

When you get to the Settings page, enable recording (capture) of the data packets. Under the EVDO protocol, find the **Packet Data Recorder** option and check to enable.

3.2. Other Settings

Other settings are made normally, including enabling *Crosshair*, logs, etc.

EVDO		
General		
Case Notation	2016-03-18 16-11-18_EVDO Service Mission name prefixed in system settings	SETTINGS
File Output		
Event Log	Enabled Roll over every 1 MB , new file every 30 minutes	SETTINGS
Call Log	Enabled Roll over every 1 MB , new file every 30 minutes	SETTINGS
Packet Data Recorder	Enabled If enabled, PCAP data will be recorded	<input checked="" type="checkbox"/>
Timers & Resources		
Continuous Channel Scan	Enabled Uses a channel resource to scan for new channels in the background while the mission is running.	<input checked="" type="checkbox"/>
Call Time Limit	No Minimum , No Maximum Specifies the minimum and maximum duration for each call	SETTINGS
Call Fade	Timer: 2 seconds Fade Reverse: false, Fade Unrouted Calls : false	SETTINGS
Confirmation Receiver	Priority: 9, Dwell Time: 3 seconds Unknown calls to confirm	SETTINGS
Targeting		
Crosshair Targeting	Disabled Server Address: 127.0.0.1:56011	SETTINGS

To capture the packets, enable the **Packet Data Recorder**

If desired, enable **Crosshair**

4. Targeting

4.1. Crosshair vs. Target Lists

You may use either a *Crosshair* Target Database or a flat file Target List created in the user interface (*Alaska* or *Hawaii*) to target specific devices.

4.1.1. Crosshair

Crosshair is the DRT targeting database that is supplied with the *DRT1000 System Software*. The database may run on the DRT system or a separate server. Instructions on installing *Crosshair* are supplied in the *DRT1000 System Software Release Notes*. *Crosshair* provides user-centric targeting; that is, multiple devices can be associated with a single targeted person (subject), and multiple target types pertaining to a single device can be contained within one entry. Additionally, *Crosshair* will add additional information to the database on a targeted device (e.g., NAIs) as it is discovered. For general instructions on how to use *Crosshair*, see the [Crosshair Manual](#) or *Crosshair* HELP files. Details specific to targeting this protocol are described below.

4.1.2. Target Lists

Target Lists may be created using either *Alaska* or *Hawaii*; however, *Alaska* and *Hawaii* Target Lists are NOT interchangeable. Both in *Alaska* and *Hawaii*, each Target List is specific to one protocol and there is a target item for each device/type. For example, if you are targeting a device by its IMSI, you will create a target item for that IMSI, and if you are also targeting that device by its IMEI, you will create another target item for the IMEI. Refer to the Cellular Appendix in either the online HELP or the manual PDF for general instructions on creating a Target List in whichever user interface you are using (*Alaska* or *Hawaii*). Details specific to targeting this protocol are described below.

4.2. Common Terms and References

The EVDO target types use the following common terms:

- NAI: Network Access Identifier value that identifies a mobile Device. The NAI is used to perform mobile registration.
- AT: Access Terminal value for the targeted Device.
- ATI: Access Terminal Identifier for the targeted Device within the network.
- UATI: Unicast Access Terminal Identifier which uniquely identifies the targeted Device within the network when the Device initially registers with the network. *Crosshair* does not report UATI values.
- OMA: Open Mobile Alliance protocol.
- PTT: The Push-to-Talk value identifies a PTT-specific Access Terminal (mobile Device) using the *Winphoria* PTT protocol.
- SIP URI: Session Initiation Protocol Uniform Resource Identifier. The SIP is used as a control protocol for PTT Devices that use the OMA PTT protocol. The IP URI is the unique user identifier used in SIP messaging.
- Subnet/Subnet Mask: The length of the Subnet ID is equal to the number of 1s in the most significant bits of the Subnet Mask can be variable lengths, which is a variable length but is a maximum of 128 bits long. The Subnet Mask is sent over the forward channels Sector Parameters Broadcast message. The Subnet Mask is reported on *Alaska*'s **Channel Properties Details** page. If the Subnet Mask has N 1s, the most significant N bits of the Sector ID and the UATI are identical to the Subnet ID.

4.3. Target Types

The table below describes the targeting types available in *Alaska* and *Crosshair*.

DRT Company Confidential and Proprietary
USML XI(d)

Target Identification Fields Table

Target Type	Description	Max Length/Format	Wildcard Use	Avail. in <i>Alaska</i>	Avail. in <i>Hawaii</i>	Avail. in <i>Crosshair</i>
NAI	This value identifies an AT (mobile device). The NAI is used to perform Mobile IP registration. During Mobile IP registration, the AT is authenticated and an IP address is assigned to the device. This registration typically only occurs when the phone first connects to a particular network and is updated periodically at a network-specified rate. This form of targeting only works if the data traffic belonging to the AT is captured during Mobile IP registration.	ASCII String: 254 characters on either side of @ sign Format: <user>@<domain> used in Mobile IP registration and authentication. e.g., CPannuli@EC.com	<i>Alaska</i> and <i>Crosshair</i> X, Y wildcards allowed anywhere except when Specific is selected. See additional info in next column. <i>Hawaii</i> Enter an e-mail address. Y wildcard allowed for either user, domain or both: Y@domain user@Y or just Y	YES In the Account field, use the drop-down to select Any , style="font-weight: bold;"> Any Any User, Any Domain or Specific and then enter an e-mail address with wildcards as noted below: <ul style="list-style-type: none">• Any (Y): targets Any User and Any Domain using the Y wildcard.• Any User: target any User (Y wildcard) in a specified Domain. The Y wildcard appears before the @ sign, e.g., Y@Sprint.com.• Any Domain: target a specified User in any Domain (Y wildcard). Type the User Name before the @ sign, e.g., Xavier@Y.• Specific: target a specified User in a specified Domain. Type the specific User before the @ sign and the Domain name after the @ sign, e.g., Xavier@Sprint.com.	YES Enter target in this format: user@domain	YES The NAI field consists of a drop-down that lets you target devices using the selections as described below. The adjacent fields are divided by the @ sign. Enter User and Domain criteria. <ul style="list-style-type: none">• Any (Y): target Any User and Any Domain using the Y wildcard.• Any User: target Any User (Y wildcard) in a specified Domain. The Y wildcard appears before the @ sign, e.g., Y@Sprint.com.• Any Domain: target a specified User in any Domain (Y wildcard). Type the User Name before the @ sign, e.g., Xavier@Y.• Specific: target a specific User in a specific Domain. Type the specific User before the @ sign and the Domain name after the @ sign, e.g., Xavier@Sprint.com.

Target Type	Description	Max Length/Format	Wildcard Use	Avail. in Alaska	Avail. in Hawaii	Avail. in Crosshair
SIP URI	This value uniquely identifies a Push-to-Talk AT (mobile Device) which employs the OMA PTT protocol. SIP is used as a control protocol for Push-to-Talk devices using the OMA PTT protocol. The SIP URI is the unique user identifier used in SIP messaging.	ASCII String: 254 characters on either side of @ sign Format: <user>@<domain> used in SIP. e.g., CPannuli@EC.com	<i>Alaska and Crosshair X, Y wildcards allowed anywhere except when Specific is selected. See additional info in next column.</i> <i>Hawaii Y wildcard allowed for either user, domain or both: Y@domain user@Y or just Y</i>	YES Enter data the same as noted above for the NAI target type.	YES Enter target in this format: user@domain	YES Enter data the same as noted above for the NAI target type.
Subnet	This value identifies a group of related base stations and is a section of a Provider's network in a specific geographic location: The Subnet field is a value between 1 and 104 bits. It is entered into 7 subfields. Six of these fields have 4 characters and the last has 2. NOTE: The length of the Subnet ID is equal to the number of 1s in the most significant bits of the Subnet Mask, which is 128 bits long and which is sent over the forward channel's Sector Parameters Broadcast message. The Subnet mask is reported on <i>Alaska's Channel Properties Details</i> page. If the Subnet mask has N 1s, the most significant N bits of the Sector ID and the UATI are identical to the Subnet ID.	<i>Alaska</i> 7 subfields: 1. 4 Hex char 2. 4 Hex char 3. 4 Hex char 4. 4 Hex char 5. 4 Hex char 6. 4 Hex char 7. 2 hex char <i>Crosshair and Hawaii</i> 26 Hex char	X and Y wildcards are allowed in all parts.	YES	YES	YES

Target Type	Description	Max Length/Format	Wildcard Use	Avail. in Alaska	Avail. in Hawaii	Avail. in Crosshair
ATI	<p>The network uses a 128-bit identifier known as the Universal Access Terminal Identifier (UATI) to identify the phone's current session. ATI is a 32-bit value. The top 8 bits of the ATI are the color code. The lower 24 bits of the ATI are transmitted in the lower 24 bits of the UATI Assignment messages. The UATI is a temporary identifier which can be re-used and re-assigned at any time. Typically the entire UATI cannot be reconstructed from control channel signaling messages.</p> <p>This field contains a box that when checked allows targeting with both the Subnet and ATI. By default this box is NOT checked. When unchecked, Subnet and ATI are not included in the targeting.</p> <p>NOTE: Because the UATI is a temporary identifier which can be re-used and re-assigned at any time, targeting that includes both the Subnet and ATI might return data that is not associated with the targeted Device.</p>	ATI: 8 Hexadecimal	No wildcards are allowed.	NO	NO	YES
IP Address	The Home IP Address value is taken from the Mobile IP Registration Reply Message.	IP Address: 15 Decimal (Dotted Quad)	No wildcards are allowed.	NO	NO	YES

Target Type	Description	Max Length/Format	Wildcard Use	Avail. in <i>Alaska</i>	Avail. in <i>Hawaii</i>	Avail. in <i>Crosshair</i>
System ID*	The System Sector ID is a 128-bit value written in IPv6 format, where each Hex character represents 4 bits. With the Sector ID, a CDMA channel pair uniquely identifies an EVDO sector. This value is sent over the forward channel's Sector Parameters Broadcast message.	8 subfields: 1. 4 Hex char 2. 4 Hex char 3. 4 Hex char 4. 4 Hex char 5. 4 Hex char 6. 4 Hex char 7. 4 Hex char 8. 4 Hex char	X and Y wildcards are allowed.	YES	NO	NO
PSTN (Alaska) PTT (Crosshair)	This value uniquely identifies a PTT-specific AT (mobile device) which uses the Winphoria PTT protocol. SIP is used as a control protocol for PTT devices using the Winphoria PTT protocol. Winphoria uses the AT's PSTN as the unique User ID used in IP messaging.	<i>Alaska</i> 10-digit telephone number used in the SIP URI for the Winphoria PTT protocol. <i>Crosshair</i> and <i>Hawaii</i> 32 Decimal digits	<i>Alaska</i> X, Y, and partial wildcards allowed.	YES	YES	YES

*NOTE: This target type is only used when the DRT unit is conducting Channel ID. Entering a System ID target will limit the DRT unit to targeting mobiles within that system. To find IDs operating in an area run Channel ID for the service without any System ID targets. Once a control channel is identified and listed on the **Navigator's Channels** page, its System ID is reported on that channel's **Properties General** page. To focus on that system, create a System ID target for that system and run Channel ID again.

5. Captured Data, EVDO

5.1. PCAP File Data

An EVDO mobile device can receive data from multiple base stations during a single session. The DRT system will capture and combine all session data into a single PCAP file for that session. To maximize the likelihood of capturing all data for a session, DRT recommends that you monitor as many EVDO base station signals as possible.

5.2. Logs

Packet Data events may be recorded in the **Activity/Event Log** and in the Chronolog.

If logging is enabled, successfully targeted packet data call events are logged in the **Activity/Event Log** regardless of whether the packet data recorder is enabled. If the packet data recorder is enabled, then the packet data file start and stop cuts are also recorded in the **Activity/Event Log**. The logged data will include the names and locations of the output PCAP file and the output XML file.

5.3. Recorded Packet Data Files

5.3.1. PCAP File Location

Two types of files can be created for each intercepted packet data call: the Packet Capture (.PCAP) file containing the recorded packet data and the XML file containing the SRI data. By default, the PCAP and sri.xml files are stored on the DRT system in the \\DrtUnitName\FtpShare\PacketDataFiles directory. The filename is created by the DRT system.

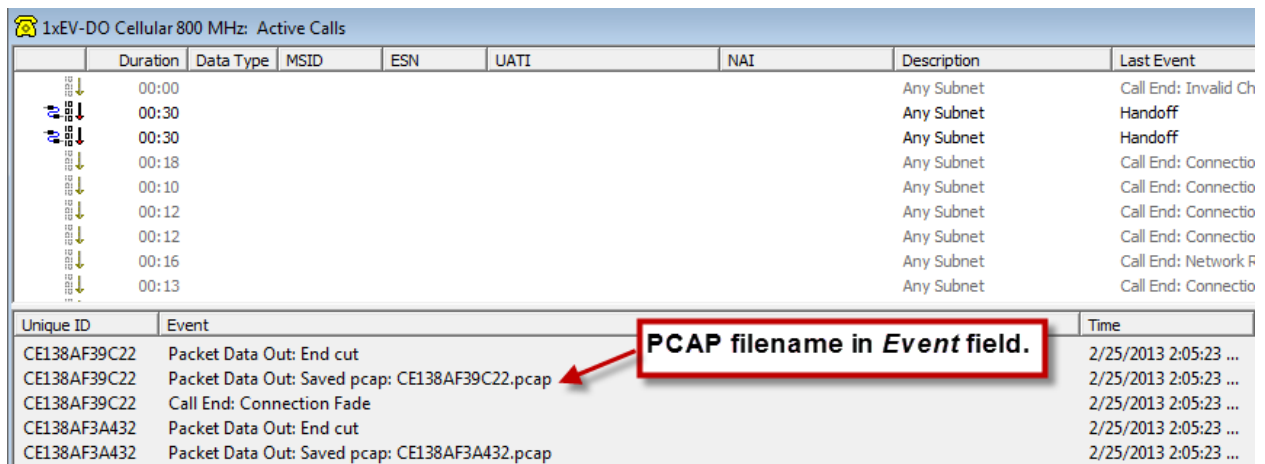
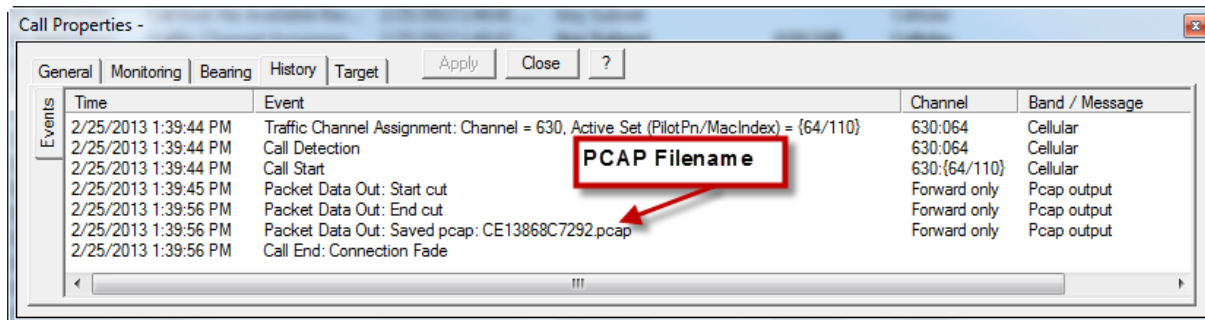
Depending on the environment, the space on the DRT system may fill up quickly with PCAP files. You can change the location for these files using *Alaska's* **File Location** tool:

- From the main menu:
 - Select **Tools > File Location** to bring up the **Data Storage Configuration** sheet.
 - In the left pane, select **Recorded Packet Data Files**, then check the **Network Directory** option. In the **Path** field, enter or browse to the network path.
 - Click **OK**

5.3.1.1. PCAP Filenames

The PCAP filename is the Unique ID.

You can see PCAP filenames throughout *Alaska*. While the call is going on, the name is displayed on the **Packet Data Recorder Activities** page. It is also displayed on the Events (lower pane) of the **Active Calls** window in the **Events** field and the **Call Properties History Events** page, which is available as long as the call is still displayed on the **Active Calls** window. Additionally, if Event logging is enabled, the PCAP filename is stored in the Activity/Event Log which may be viewed within *Alaska* or within the opened raw log file.



5.3.1.2. Open SRI Data Files

The SRI data is recorded to an XML file which can be opened with any text editor.

6. Open PCAP Files

You can select a default PCAP Processor for *Alaska* to use to open PCAP files. See the *Alaska* HELP files for details.

To open PCAP files in a human readable format, you will need a 3rd Party PCAP File Processor like *FASTRAK*.

7. EVDO Chronolog Definitions

Chronolog definitions may be copied without consulting DRT.

The following table describes changes between versions:

Version	Changes from previous version	First release that created this version
1	Initial release	Beta
2	Changed Traffic Channel Active Set History to print only unique active set entries and to be limited in the number of unique entries printed.	5.6
3	Adding NAI, called SIP URI, and calling SIP URI. Adding EVDO Rev. A Base Station Indicator	6.1

7.1. Format

All Chronolog data is ASCII text. A Chronolog contains two types of records, Header Records and Call Records. Each record is terminated with a CRLF (carriage return line feed pair).

7.2. Header Record

The first line of the file is a header record. The header record fields are the same for all formats. The header record fields are described in the HELP section *Receive: Basic Operations>Logs>Call Log/Chronolog>Chronolog Format* and the DRT1000 Receive Software Manual. The Wireless Format number for the EVDO format is 42, so Field 2 will be 42.

7.3. Mode of Connection

Each call record will contain a value representing the connection mode. The connection mode values are defined in this table:

Value	Description
0	Voice
1	Reserved
2	Data
3	Paging
4	Session Start (UATI assignment)
5	Session Close
6	Redirect

7.4. Reason for End of Call (EOC)

The following table describes the mapping between DRT's Reason for End of Call, and the REOC values from the *Signal Related Information ICD*, Version 5.0, dated 7 Oct 1997.

DRT EOC Reason	SRI EOC Value	SRI EOC Explanation
No Available Receiver	38	Non route (No demods)
User Request	07	Operator stopped copy
Call Pre-Empted for another call	09	Bumped by a higher priority
Release Received	04	Hang-up received
Fade Timer Expiry	05	Signal timed out
Invalid Channel	39	Frequency out of bounds
Unsupported Configuration	69	Inaccessible output
Internal Error	13	Selection system audio routing problems
Duplicate MSID	29	Undefined
Log closed before EOC	11	Missed hang-up
Call Pre-Empted for a confirmation receiver	09	Bumped by a higher priority
No target match	37	Non-hit MID
Audio not routed	07	Operator stopped copy

7.5. Call Record

Each call record (line) in a Chronolog contains the information for a single call, with the fields separated by a colon. Text strings are enclosed in double quotes (to allow a colon embedded in the text field). Double quote characters in text strings are converted to single quote characters (in SMS messages, for instance). The record is terminated with a CRLF (carriage return line feed).

EV-DO Call Record Fields

Field	Description	Length	Values	Format	Example
1	Date Up	8	Year, Month, Day digits	YYYYMMDD	19990630
2	Time Up	7	Hour, Minute, Second digits, plus time zone indicator (Z for Zulu)	HHMMSSZ	150923Z
3	Date Down	8	Year, Month, Day digits	YYYYMMDD	19990630
4	Time Down	7	Hour, Minute, Second digits, plus time zone indicator (Z for Zulu)	HHMMSSZ	151041Z
5	Unique Connection ID /Transaction ID	12	Hex characters	48 bit hex number	CD5E12F7E7C2
6	Unit Latitude	var	Decimal Degrees (current DRT unit location)	DD.DDDDDD	38.123456

Field	Description	Length	Values	Format	Example
7	Unit Longitude	var	Decimal Degrees (current DRT unit location)	DDD.DDDDDD	-79.123456
8	Originating Sector's System ID (aka Sector ID)	32	128 bit hexadecimal (NOT in IPV6 format)	DDDDDD...DDDD	0080058000000025080A F8CDC900EE01
9	Originating Sector's Color Code	var	Decimal Sector Color Code	DDD	149 or 17
10	Subnet Mask	32	128 bit hexadecimal (NOT in IPV6 format)	DDDDDDDDDDDDDDDD DDDDDDDDDDDDDDDD DD	FFFFFFFFFFFFFFFFF00 00000000000000
11	UATI	32	128 bit hexadecimal (NOT in IPV6 format)	DDDDDDDDDDDDDDDD DDDDDDDDDDDDDDDD DD	0080058000000025080A F8CDC900EE01
12	NAI	var	ASCII	"s@s"	user@realm
13	Home Address (HoA)	var	IP Address in decimal notation	DDD.DDD.DDD.DDD	192.168.2.1
14	Mobile Origination	1	0: Invalid / Unknown 1: Mobile Terminated 2: Mobile Originated	D	1
15	Reverse Received	1	0: Reverse Not Received 1: Reverse Received	D	0
16	Mode of Connection	1	See Mode of Connection table above	D	0
17	Reason for EOC	2	See Reason for EOC table above	DD	04
18	Target Identifiers	var	Target item description, as entered in Target List	"ssss..."	"Joe Schmoe"
19	Case Notation*	var	Case Notation, as entered for Service properties Appended with a '*' if audio routed	"ssss..."	"US14-14791242D"
20	Packet Data Routed	1	0: not routed 1: routed	D	1
21	Originating Sector	var	Decimal digits, '.' to indicate Pilot Pn Offset, followed by a C or P to indicate "Cellular band" or "PCS band". A "U" following the channel indicates the band is other than C or P.	DDDD.DDDC	384.064C
22	Traffic Channel Active Set History	var	List of active sets with '>' character to indicate a handoff. See below for further explanation.	DDD;DDD; DD.DDDD.DDD.DDD; DD.DDDD.DDD;> DD.DDDD.DDD; If handoff occurred: DDDD.DDD.DDDC;...> DDDD.DDD.DDDC;...	002;002;00.0384.064.02 7;00.0384.056.05; 00.0384.150.055;>00.03 92.052.012; 00.0392.056.051;00.392. 018.018;

Field	Description	Length	Values	Format	Example
23	ATI	8	32 bit ATI value, hexadecimal	DDDDDD...DDDD	
24	Mobile Latitude	var	Decimal Degrees (last known mobile location)	DD.DDDD	38.1234
25	Mobile Longitude	var	Decimal Degrees (last known mobile location)	DDD.DDDD	-79.1234
26	Originating Sector's Country Code	3	Decimal Digits	DDD	310
27	Stored Packet Data Path	var	Full	"sss...."	\\UnitName\FtpShare\PacketDataFiles\CD5E12F7E7C2.pcap
28	Num Packets Recovered	var	Decimal Digits	DDD	6
29	Target Selection Result	1	0: not targeted 1: targeted This field is used for determining if the call was background logged.	D	1
30	Target Rule	var	Target rule for target match	"sss..."	"XXX9165554"
31	Called Party Target Rule	var	Directory rule for target match (TELDRA) **	"sss..."	"XXX9165554"
32	Calling Party Target Rule	var	Directory rule for target match (TELDRO) **	"sss..."	"3019165554"
33	Hit List	var	Comma-separated prioritized list of target hit selectors.	"ssss,ssss,ssss..."	"NAI"
34	EVDO BS Rev A indicator	1	0: Rel 0 1: Rev A 2: Unknown	D	1
35	Audio Routed	1	0: not routed 1: routed	D	1
36	Called PSTN	var	PSTN number	DDDDD....	3019165554
37	Calling PSTN	var	PSTN number	DDDDD....	3019165554
38	Called SIP URI	var	ASCII	"s@s"	user@realm
39	Calling SIP URI	var	ASCII	"s@s"	user@realm

Notes:

* Currently, the case notation value is the service name.

** In EVDO, these fields are always blank. The notion of "called" or "calling" parties does not apply to data formats.

Traffic Channel Active Set History

This field contains the traffic channel history of the call. Channels are separated by a '>' character, indicating a call handoff.

Each member of the active set is followed by a ';' character. Each member of the active set contains the following fields: Band Class, EVDO Channel Number, Pilot Pn Offset, and Mac Index each separated with a '.' character. The first "DDD" in the field is the number of active sets intercepted. The second "DDD" in the field is the number of active sets recorded. Only the first 49 unique active set updates will be recorded followed by the last active set regardless of uniqueness.