How Packet Radio REALLY Works... the AX.25 Link Layer Protocol

How does packet get your information from point A to point B — error-free? And what are those funny letters and numbers at the top of packet frames all about?

Computers, like people, need a common language to communicate. People break up their messages into chunks we call "words," but computers—which send each other streams of "1"s and "0"s—need a different way to tell each other that one chunk of data has ended and another is about to begin. One method of doing this is known as the *link layer packet protocol*, and all computers in a data chain must be using the same one.

The link layer protocol used by amateurs for packet radio is called AX.25. Let's take a look at what an AX.25 packet looks like and how the different parts are used to ensure error-free data transfer.

Parts of a Packet

All HDLC (High-level Data Link Control) packets (more properly called "frames"), including those of AX.25, are similar and consist of six unique "fields," as shown in Figure 1.

Flag: Flag fields are put at the beginning and end of each frame (packet) to indicate the boundaries of the frame. A unique bit sequence is used (01111110) so other parts of the frame won't be mistaken for a Flag.

Address: This field normally specifies the destination of the frame. This is the actual callsign of the source, destination, and any digipeaters.

Control: This identifies the frame type, as described below, and carries other control information, such as frame number.

PID: The first byte of the Data field (see below) is the Protocol IDentification, specifying the type of protocol in use.

Data: This field contains the actual data to be transferred. Many frames do not have a data field.

FCS (Frame Check Sequence): This is how errors are detected in a frame. Using a special mathematical formula, the PAD (Packet Assembler/Disassembler) or TNC creates a number based on the rest of the fields. The other PAD/TNC does the same and, if the numbers match, the frame has no errors and is accepted.

Uncovering Hidden Info

If you set your TNC parameters properly, you can see most of the "hidden" information within each frame. Not all TNCs use the same commands to display the details. Your TNC's operating manual will explain how to monitor all frame types, including control frames, while connected. The example below is from an AEA PK-232 with **Monitor** set to level 6.

A typical packet frame, when viewed on a computer, might look like this (note, though, that this is usually on one line, but the magazine format forces it onto multiple lines):

KD6TH-4>N2DSY-2>N2IRZ [I;3,1]:0042z, 838 msgs, #40407 last @KD6TH-4 Mailbox>*

The first section (*KD6TH-4>N2DSY-2*>N2IRZ*) is the address field. The second section (*[I;3,1]*) is the control field, and the last section (*0042z, 838 msgs, #40407 last @KD6TH-4 Mailbox>*) is the data field. (The colon between the control and data fields is put there by the TNC). Note that you do not see the Flag, PID, or FCS fields.

AX.25 Frame Types

C	Connect frame. Also known as a "SABM" frame (Set Asynchronous Balanced Mode).
D	Disconnect frame.
DM	Disconnect Mode frame.
I	Information frame.
UA	Unnumbered Acknowledgement frame.
UI	Unnumbered Information frame.
RR	Receive Ready command and response.
RJ	ReJect frame.
RNR	Receive Not Ready command and response.
FRMR	FRaMe Reject response.
DM	Disconnected Mode response.

What Does It Mean?

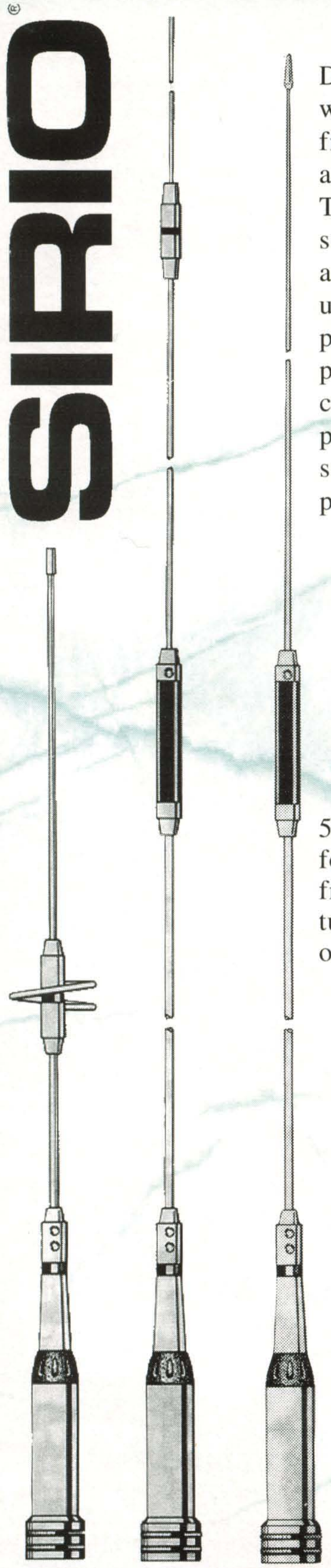
The examples below will explain the function of each frame type.

When you type a connect command into your TNC, the TNC generates a frame like: *N2IRZ*>KD6TH-4 [C,P]*

This means that N2IRZ is trying to establish a connection to KD6TH-4 (my local BBS). The asterisk (*) shows who is transmitting. The next symbol (>) shows the direction the frame is going (to KD6TH-4). The "C" indicates that it is a Connect frame, and the "P" means that the "Poll" bit is set. When the Poll bit is set, it means the originating station is *polling* for the destination station and

By Don Rotolo, N2IRZ

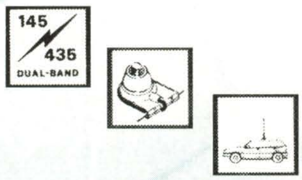
SIRIO®



HP 2070 • HP 2070 H • HP 2070 R

HP 2070 • HP 2070 H • HP 2070 R

Dual vehicular antennas working on the radio amateur frequencies of 2m70cm, tuning adjustments are not required. The whips, made of 17/7PH stainless steel, are very flexible and can be tilted to 90° without using keys or tools. Also a particular attention has been paid to the UHF-male antenna connector with a gold-plated pin, a "Teflon" insulator and a silicon rubber gasket for a perfect waterproofing.



TECHNICAL DATA

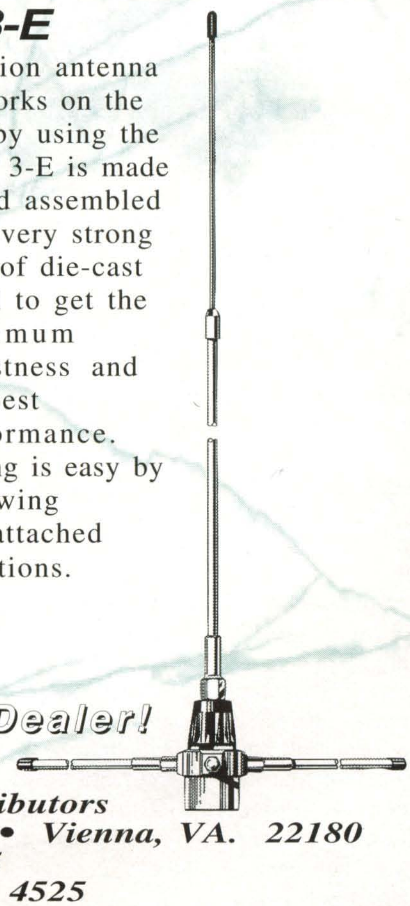
Type:	
HP 2070:	VHF 1/4 λ - UHF 5/8 λ Whip
HP 2070 H/R:	VHF 1/2 λ - UHF 2 x 5/8 λ Whip
Impedance:	50 Ω
Frequency range:	
HP 2070:	VHF 140-150 MHz/UHF 430-440 MHz
HP 2070 H/R:	VHF 142-148 MHz/UHF 430-440 MHz
Polarization:	vertical
V.S.W.R.: at freq. res.:	≤ 1.2:1
Bandwidth: at VSWR 2:1:	
HP 2070:	VHF/UHF 10 MHz
HP 2070 H/R:	VHF 4 MHz/UHF 6 MHz
Gain:	
HP 2070:	VHF 0 dBd - 2.15 dBi
	UHF 3.2 dBd, 5.35 dBi
HP 2070 H/R:	VHF 3 dBd - 5.15 dBi
	UHF 6 dBd, 8.15 dBi
Max Power:	VHF 150 Watts /UHF 100 Watts
Connection:	"UHF" Female
	gold plated center conductor
Length (approx.):	
HP 2070:	445mm
HP 2070 H:	1050 mm
HP 2070 R:	980 mm
Weight (approx.):	
HP 2070:	270 gr
HP 2070 H:	330 gr
HP 2070 R:	300 gr

GP 3-E

5/8 wave Ground Plane base station antenna for land and marine service. It works on the frequency range of 144-175MHz by using the tuning diagram enclosed. The GP 3-E is made of a non-corrosive aluminum and assembled on a very strong base of die-cast metal to get the maximum robustness and the best performance. Tuning is easy by following the attached directions.

TECHNICAL DATA

Type:	5/8 λ Ground Plane
Impedance:	50 Ω
Frequency range:	144-175 MHz
	tunable by diagram
Polarization:	vertical
V.S.W.R.: at freq. res.:	≤ 1.2:1
Bandwidth: at VSWR 2:1	7 MHz
Gain:	3 dBd - 5.15 dBi
Max Power:	300 Watts
Connection:	UHF Female
Wind resistance:	40m/second
Length (approx.):	1300 mm
Weight (approx.):	850 gr
Mounting mast:	ø 30 mm



Call your favorite Dealer!

EDCO
Electronic Distributors
325 Mill Street • Vienna, VA. 22180
(703) 938 8105
FAX: 703 938 4525

"If you set your TNC parameters properly, you can see most of the 'hidden' information within each frame."

expects an immediate response (sort of asking "are you there?"). If the destination station was to respond, it would send an "F," or *Final*, bit in response ("yep, I'm here"). Other than when there is a loss of communication, missed packets, or no activity on the link for a while, the Poll and Final bits will rarely be used again.

*** Connected

KD6TH-4 hears the packet, decodes it properly, and is able to establish a connection with N2IRZ, so it sends: *KD6TH-4*>N2IRZ [UA,F]*

This *Unnumbered Acknowledgement* frame means that KD6TH-4 has acknowledged receiving N2IRZ's Connect request and confirms the connection. Your TNC generates the familiar "*** *Connected to...*" message for you. KD6TH-4 now sends some data, a greeting (the "Connect Text"): *KD6TH-4*> N2IRZ [I,P;0,0]:Hi Don, Welcome to KD6TH-4 BBS !*

The "I" tells us that this is an *information* frame. The information ("Hi Don...") can be any text or other data. "P" is for *Polling*—KD6TH-4 must make sure N2IRZ is still there because this is the first data exchange of the connected session. What is interesting here are the numbers in the "*[I,P;0,0]:*" part. The first number is the next frame number that KD6TH-4 expects from N2IRZ, and the second number is the number of the frame that is being sent. The order of the numbers switches when N2IRZ is sending. The frame numbers count up from 0 to 6, and then restart at 0. This means that a maximum of seven frames may be sent at once—if eight were to be sent, the other TNC would receive two frames with the same frame number and wouldn't know where they belonged.

Many types of data corruption, including out-of-sequence frames, are guarded against by the AX.25 protocol. Anyway, upon receiving this frame without errors, N2IRZ sends: *N2IRZ*>KD6TH-4 [RR,F;1]*, telling KD6TH-4 that N2IRZ got frame 0 correctly and is ready to receive frame 1. KD6TH-4 sends two more info frames to N2IRZ:

KD6TH-4>N2IRZ [I;0,1]:*** You have Unread Mail !!!*

KD6TH-4>N2IRZ [I;0,2]:0045z, 745 msgs, #40498 last @KD6TH-4 Mailbox>*

Got It!

If both frames were received correctly, N2IRZ would acknowledge receiving them by acknowledging only the last frame received, frame 2, with an *RR*

FLAG	ADDRESS	CONTROL	PID & DATA	FCS	FLAG

A typical packet (HDLC) frame. See text for an explanation of each field within the frame.

"Many types of data corruption, including out-of-sequence frames, are guarded against by the AX.25 protocol."

frame. The BBS would then wait for my next data frame, telling it what to do (such as LM to list my messages). However, N2IRZ didn't get the first packet without errors, but did get the second, so it sends: *N2IRZ*>KD6TH-4 [RJ;1].*

This tells KD6TH-4 that it is rejecting the received packet (packet number 2)—N2IRZ still wants packet number 1. As previously mentioned, if both packets were received correctly, N2IRZ would have simply sent *[RR;3]* and the process would continue.

If N2IRZ hadn't received either packet, something interesting happens: no response is sent. KD6TH-4, after sending the last frame, starts its **FRAck** (FRame Acknowledgement) counter. If an acknowledgement or reject frame isn't received before the **FRAck** timer expires, KD6TH-4 would make sure N2IRZ was still there, by polling: *KD6TH-4*> N2IRZ [RR,P;0]*

KD6TH is telling N2IRZ that a session is established, and KD6TH expects packet number 0 from N2IRZ. Note that the polling bit is set. If N2IRZ hears that packet, he would reply: *N2IRZ*> KD6TH-4 [RR,F;1],* and KD6TH-4 would send the two packets again. This process will repeat until either N2IRZ acknowledges both packets or KD6TH has sent a certain number of polling frames (set by **RETry**). If the acknowledgement arrives, the packet QSO continues. If the **RETry** limit is reached, KD6TH-4 then tries to end the session by sending *Disconnect* frames until N2IRZ acknowledges the disconnection or the **RETry** limit is reached.

Data Exchange

Let's assume that all goes well. Information packets are traded between KD6TH-4 and N2IRZ for a few minutes while N2IRZ reads his mail and checks out a few bulletins. Eventually, N2IRZ is finished with the BBS, so he signs off: *N2IRZ*>KD6TH-4 [I;5,2]:Bye*

This is N2IRZ's frame 2 (perhaps the 80th time he has sent a frame numbered 2 in this session), and he expects frame 5 back. KD6TH-4 responds:

KD6TH-4>N2IRZ [RR;3]*
KD6TH-4>N2IRZ [D,P]*

First the "I" frame containing *"Bye"* is acknowledged, and then KD6TH-4 initiates a disconnect. N2IRZ responds: *N2IRZ*>KD6TH-4 [UI,F],* and they are disconnected. KD6TH-4 now sends out its *"MAIL_FOR:"* beacon: *KD6TH-4*> BBS [UI]: Mail_for: N2DSY KA2USU KB7UV KB2BAV WA2SPO*

"That covers the basics of the AX.25 packet protocol. If you'd like to learn more, you can buy a copy of the paper defining AX.25 from the ARRL, or download it on the Internet...."

This last frame is an *Unnumbered Information* frame. The place it is addressed to (in this case, "BBS") is specified by the **UNproto** command, which usually has the default of "CQ."

Other Messages

Now you have a good idea of what C, UA, I, RR, RJ, D and UI frames are like. A *DM* frame is sent when the other station is busy or its **CONOk** parameter is Off, causing your TNC to generate a message like: *"*** Disconnected - KD6TH-4 Busy"* while KD6TH-4's TNC generates a *"*** Connect Request: N2IRZ"* message, which, as an automated station, KD6TH-4 ignores.

The other frame types are somewhat rare: *RNR* is sent when one station polls another ("are you there?") but the other station isn't ready to process another packet yet. The RNR frame tells the other station to hold off for a while, similar to RS-232 flow control. *FRMR* is only sent when something really wrong occurs: the frame that was received has a good FCS, meaning there were no errors, but the frame type (I, UA, RR, etc) is either undefined or in violation of the protocol, in other words, an inappropriate reply.

Beyond the Basics

That covers the basics of the AX.25 packet protocol. If you'd like to learn more, you can buy a copy of the paper defining AX.25 from the ARRL, or download it on the Internet at <http:// www.rmsd.com/hamradio/ax25.std> (without the "<>" marks). For a wealth of information concerning radio equipment for 9,600 baud and above, check out N6GN's High Speed Packet Page at <ftp://col.hp.com/hamradio/packet/ n6gn/index.html>. For general information about packet radio, useful packet-related files, and interesting links to other packet-related web pages, visit the TAPR (Tucson Amateur Packet Radio) Home Page at <http:// www.tapr .org>.

"Pack"ing It In

Well, that's all the time we have this month. Next month, we'll look at packet networks and the basics of building a good one. After that, we'll get away from packet for a while to discuss other data modes you can try.

Till then, 73 and happy packeting! ■