D-STAR Protocol Basics

Summary

This lesson examines how the D-STAR protocol functions and how D-STAR packets are constructed. The DV and DD modes of D-STAR are compared. The student will learn about how protocols may be encapsulated and how D-STAR performs error detection and correction.

D-STAR Packets

D-STAR is a packet-based protocol. As you learned in the previous lesson that means the data is assembled into a package containing the data itself plus other information about the data and how the communications system should handle it. Packets are transmitted in their entirety and the receiving system processes the packet as a group.

There are two types of packets in the D-STAR air link protocol; DV (data and voice) and DD (high-speed data). Figure 3-1 shows the basic structure of each type of packet. Before examining the details, observe the similarities between the two packets. The packets consist of a *header* segment and a *data* segment. (Data segments are sometimes referred to as *payloads*.)

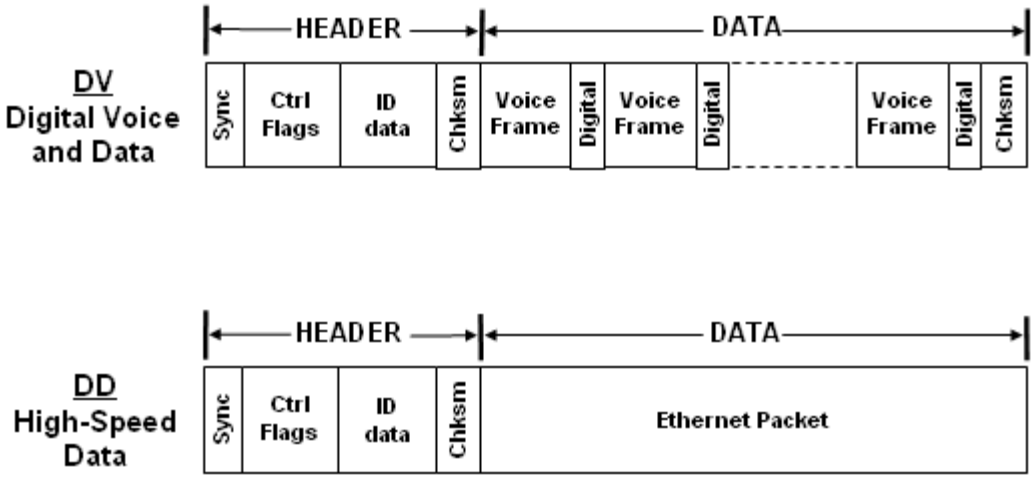

Figure 3-1

The header segment contains information about the packet; control **flags**, identification of the sender and destination, and D-STAR network routing directions. The header contains the information the receiving device needs to process the data, whether that means reading and acting on the data or just forwarding it on to another receiver elsewhere in the system.

The D-STAR backbone has its own protocol that carries the gateway-to-gateway information - the **Asynchronous Transfer Mode** (ATM) protocol. Because the method by which the gateways communicate is not public, the ATM protocol is not discussed in this course.

Overhead

The header and other information added to the original set of data creates a small amount of **packet overhead**. The additional information in the header is transmitted at the same

rate as the data, reducing the net data rate. It is a challenge for protocol designers to minimize overhead, while still providing enough information to make the protocol useful.

Table 3.1 shows the amount of overhead for the DV and DD packets. The DV packets are always the same size with 11 pairs of voice and data frames (see below for DV packet structure). There are two situations for the DD packets. The first is for a packet carrying the minimum amount of data. This is not common and minimizes efficiency. The second, a packet with the largest allowed data payload, is closer to actual practice. Clearly, it is best to send the maximum amount of data if efficiency is the most important concern.

Table 3.1 - D-STAR Protocol Overhead

Protocol	Header (bytes)[1]	Data (bytes)	Packet Size (bytes)	Overhead	
				Bytes	Pct (%)
DV	51	1056	1107	51	4.6
DD (min data)[2]	51	66	117	51	43.5
DD (max data)[2]	51	1520	1571	51	3.2

[1] - the header size is rounded up to the next full byte because of the 15-bit sync field

[2] - data size includes the terminating checksum (see error detection)

Protocol Overhead

An important difference between packet radio and D-STAR is that packet radio (AX.25) requires an acknowledgement and the receiver can request retransmission if the packet is received with errors. The time it takes for the packet's receiver to process and acknowledge the packet adds to the overall time to transfer data. This waiting time is called **protocol overhead**. D-STAR is a one-way protocol--no response is required from the receiver to acknowledge that a packet was received. As you will learn, D-STAR does not require acknowledgement because error detection and correction are built-in to the data.

Encapsulation

D-STAR also employs a common technique of using one protocol to send data formatted according to another protocol. In the DV packet, voice data is contained in short segments (called **frames**) formatted according to the AMBE protocol. In the DD packet, the data segment is formatted according to the Ethernet protocol. This process of putting data from one protocol "inside" another protocol is called **encapsulation**. The encapsulating protocol (D-STAR in this case) acts as a wrapper or envelope for the packets from the encapsulated protocol, just as a paper envelope carries documents or letters.

D-STAR Packet Structure

This section defines each element of the D-STAR packet header and data segments.

Header

The header segment is the same for both the DV and DD packets. Figure 3-2 shows the

structure of the D-STAR packet header.

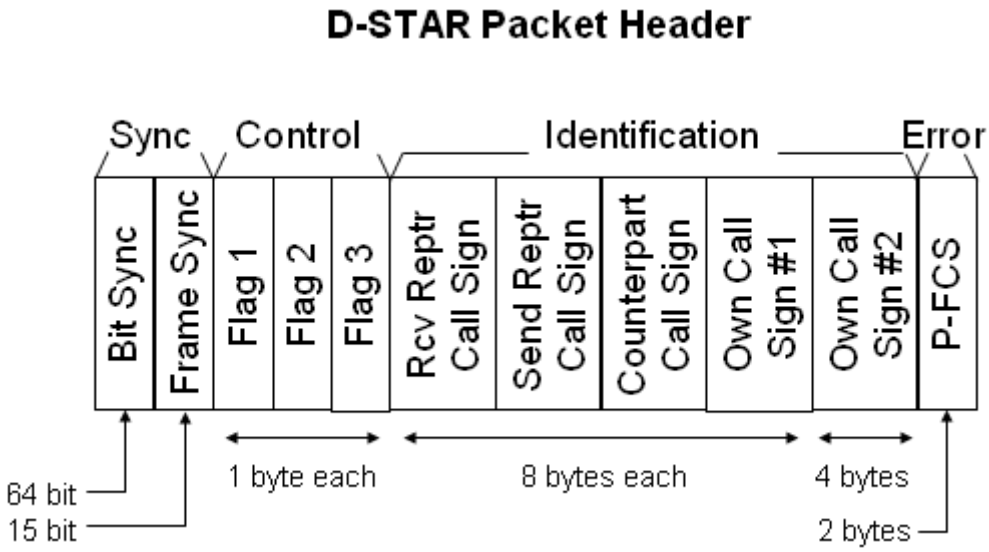

Figure 3-2

Sync Frames

Because a packet can start at any time, it takes the receiver some time to detect and synchronize with the incoming packet data. Sync frames are unique patterns of bits that the receiver can use to unambiguously determine that a packet is beginning. The receiver is then ready to process the data elements that follow. D-STAR uses two sync frames

- Bit Sync is a standard pattern for the GMSK 1010 modulation used by D-STAR
- Frame Sync is '111011001010000' - a unique bit pattern in D-STAR packets.

Control Flags

The bits in the control flag bytes are used to direct the processing of the packet. For a detailed description of the function of each bit, refer to the D-STAR protocol technical description document.

Flag 1

Flag 1 bits indicate whether the data is control data or user data, whether communications is simplex or repeater, set priority, etc.

Flag 2

Flag 2 is reserved for future use as identification data.

Flag 3

Flag 3 is reserved to indicate the version of the D-STAR protocol being used so that if new functions are added in the future, the receiver can apply them properly.

Identification Data

There are four **fields** of identification data. These carry information about the origin and destination of the packet.

Receive Repeater Call Sign

The call sign of the repeater that is to receive the packet

Send Repeater Call Sign

The call sign of the repeater that is sending the packet

Counterpart Call Sign

The call sign of the station that is to receive the data.

Own Call Sign #1 and Own Call Sign #2

The first field contains the call sign of the station that originated the data. The second field contains suffix information.

P-FCS Checksum

A **checksum** is used to detect errors as described below. The P-FCS checksum is computed from the Flag and ID data bytes. Any transmission errors in those bytes can be detected as a discrepancy in the P-FCS value.

D-STAR Error Detection and Correction

Transmission errors can occur in any digital data transmission, even those over wired networks. Somewhere along the way, a noise burst or a loose connection changes whatever represents a 0 bit to a 1 bit or vice versa. Depending on the bit's importance, the result can be insignificant or catastrophic.

How can D-STAR correct errors in digital voices? To combat transmission errors, D-STAR uses two techniques:

- *Error detection* codes are used to detect transmission errors. These only tell the receiver that the data is damaged, but not how. D-STAR checksums follow the CRC-CCITT standard.
- *Error correcting* codes contain information about the payload data. Because the codes are sent with the data to enable correction at the receiver, they are called *Forward Error Correcting* or FEC codes. FEC codes contain enough extra information for the receiver to repair most damage.

Both the DV and DD data packets in Figure 3-1 use the P_FCS checksum to protect the information in the header. The DD data packet also contains the Ethernet data packet checksum at the very end of the packet. It protects the Ethernet data payload.

In the DV packet data segment, each **AMBE 2020** digitized voice frame contains its own FEC code to allow the receiver to repair errors in that 20 msec of speech. DV digital data frames are not protected, relying on the transmitting and receiving applications to detect and correct errors.

Click the "Review" button to review the topics covered in this lesson. When you are ready, click "Next" to continue...