EXHIBIT 5

Force XXI Battle Command Brigade-and-Below

Contract No. DAAB07-95-D-E604

CDRL G014

Summary Tactical Internet System Design Document (TISDD) (Version 3 - DRAFT)

23 September 1998

Prepared for:
Commander
U.S. Army CECOM
Attn: SFAE-C3S-FB
Ft. Monmouth, NJ 07703-5009

Prepared by:
TRW Tactical Systems
Systems & Information Technology Group
1800 Glenn Curtiss Street
Carson, CA 90746

host's queue waiting for the first unicast message to be delivered to its destination.

3. Prior to sending a unicast message to the attached router, the local host sets up a TCP connection with the destination host. To set up the TCP connection, the following happens:

   a. The local host sends a TCP SYN message to the attached router. The router routes the TCP SYN message to the exit gateway IP address.

   b. At this point, the setup of the EPLRS point-to-point circuit is the same as described above, except that a SINCGARS stub net gateway router will proxy-ARP for the destination host based on its client list. Multiple gateway routers could not respond to the ARP, but the hardware address in the first response will be used.

   c. The destination exit gateway router will read the source IP address of the IP header on the TCP SYN message and add a return route to the source IP address into the routing table. The gateway router sends a RFC 1256 advertisement onto the local SINCGARS net advertising the indicated source IP address.

   d. The destination gateway router then routes the TCP SYN message via the stub net to the router attached to the destination host.

   e. The destination router should install a route for the originator's source IP address via the gateway router that has sent the RFC 1256 advertisement referenced in paragraph c.

   f. At this point, the originating and destination hosts have a TCP connection setup and start transmitting the message data.

4. The termination of the TCP connection and EPLRS point-to-point circuit is the same described in Section 3.5.1.2.1, paragraph A6.

3.5.2 Internal Threads

3.5.2.1 SA Server Selection

The following description provides an example of the dynamic server selection and client registration process. Refer to Figure 3.5-5.

A. Upon initialization, each platform transmits a CRM on the local-area SA net. Based on the received CRMs, the platform with the highest server eligibility ranking (i.e., PL) is elected as the local-area SA server for the net.

B. Once elected, the local-area SA server transmits a server coordination message intended as a registration acknowledgment to FBCB2 platforms, which are clients of the local-area SA server.

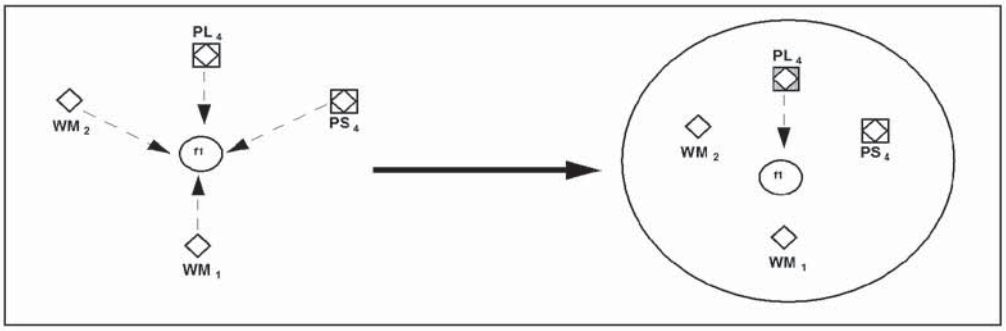

Figure 3.5-5 Dynamic Server Selection and Client Registration

3.5.2.2 SA Self-Server Selection

The following description provides an example of the self-server election process.

A. Upon initialization, the platform transmits CRMs on the local-area SA net.

B. Based on not receiving any CRMs or server coordination messages, the platform will designate itself as a self-server and disseminate its SA data directly onto the EPLRS SA CSMA needline.

3.5.2.3 SA Server Selection (Fractured Net)

The following description provides an example of the dynamic server selection process when the local-area SA net fractures (i.e., Platoon net). Refer to Figure 3.5-6.

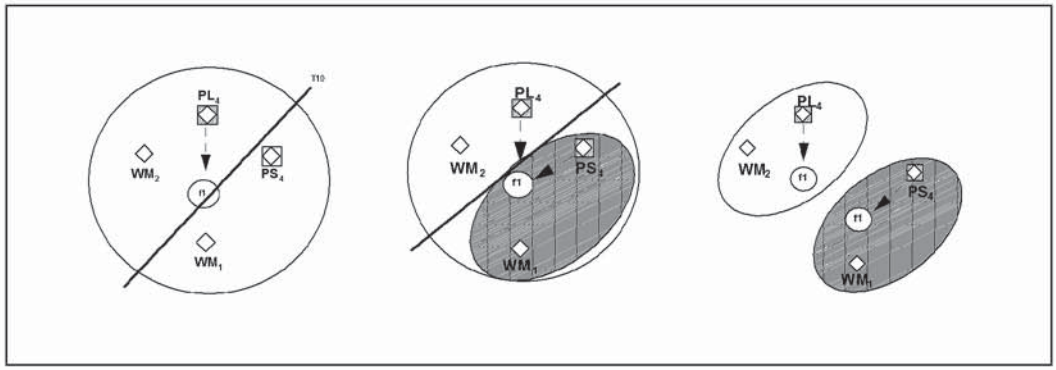

Figure 3.5-6 Dynamic Server Selection – Fractured Net

A. The PL is elected as the local position server. Once elected, the server periodically transmits a server coordination message on the local-area SA net.

B. After two minutes, PS and WM1 consider themselves de-registered from the PL.

C. PS and WM1 broadcast CRMs

D. on the local-area SA net. After which, the PS designates itself as the local position server, then transmits a server coordination message.

E. The PL and PS each periodically broadcast server coordination messages on the local-area SA net. After the PL hasn't heard from both the PS and WM1 for a period of 20 minutes, the PL will drop the PS and WM1 from its active client list and transmit a server coordination reflecting the change.

3.6 NETWORK MANAGEMENT

Network management consists of planning, changing monitoring, and corrective action.

3.6.1 Initial Planning

TBS

3.6.2 Configuration Changes

TBS

3.6.3 Network Monitoring

3.6.3.1 EPLRS Network Monitoring

TBS

3.6.3.2 SINCGARS Network Monitoring

TBS

3.6.3.3 FBCB2 Network Monitoring

FBCB2 will use a bottom-up, hierarchical approach to network monitoring.

Every FBCB2 platform monitors its local router and radios via SNMP queries and traps for status / malfunctions and provides this information to the host in the form of COMM status. Additionally, SA client / server status and SA statistics are available to infer the health of the SA network. The host has the responsibility to monitor, fault isolate and repair (or call for repair of) the equipment associated with the platform.