Chapter 10

TI Management

The TI is a technically complex C4 system. It is an important tool for the maneuver commander because it provides the transmission system and network services that carry the information he needs to operate within the planning cycle of his battlefield opponent. The information flowing within the TI must be treated as a force multiplier. Successful operation of the TI demands total coordination among all users. Network management ensures successful operation by implementing procedures that will provide the synergism needed to achieve network effectiveness. This chapter discusses ISYSCON (V)4 and the four major network management areas of the tactical network.

ISYSCON (V)4

10-1. ISYSCON (V)4 is the primary management tool used by the S6. It is responsible for network management of the communications systems of the TI LANs (primarily located in the TOCs). It is located in the G6/S6 vehicle that is operated by signal personnel.

10-2. The ISYSCON (V)4 will enhance warfighter operations by providing information management of an improved integrated data communications network linking mobile and static users across the battlespace. The TI will transport C2, SA, combat, CS, CSS, and BFA information, extending battlefield automated systems from the soldier/weapons platform horizontally and vertically across the battlefield for information exchange. The TI extends the ABCS and other automated systems to the soldier and weapons platforms. ISYSCON (V)4 will be able to establish and maintain direct automated interfaces and interoperability with all maneuver brigade communications systems.

10-3. The current concept of operations will require that the ISYSCON (V)4 engineer and plan the network configuration prior to initiation of operations based upon predeployment OPORDs and plans. However, on-the-fly operational requirements and FRAGOs will require that network reconfigurations and parameter changes be automated to the fullest extent possible and provide configurable network modeling tools.

OPERATIONAL AREAS

10-4. The paragraphs below discuss the five operational areas of ISYSCON (V)4 that allow it to plan and control connectivity, capacity, performance, and status of the tactical communications networks.

Configuration Management

10-5. Configuration management includes resource provisioning (timely deployment of resources to satisfy the expected service demand) and service provisioning (assigning services and features to end-users). It identifies exercises control over, collects data from, and provides data to the network. This capability is critical for preparing, initializing, starting, and providing for the operation and termination of services.

Performance Management

10-6. Performance management includes evaluating and reporting the behavior of network resources and ensures the peak performance and delivery of each voice, data, imagery, or video service.

Accounting Management

10-7. Accounting management includes gathering data about the utilization of network resources, setting usage quotas, and identifying user's usage of the network. The primary benefit of accounting management is that it enables the manager to measure and report accounting information based on individual and group users. This data can then be used to allocate resources and compute (by-user) the tactical cost (in terms of bandwidth, dollars) of transmitting data across the network. It also expands the manager's understanding of user utilization of network resources, which facilitates in the creation of a more productive network.

Security and COMSEC Management

10-8. Security and COMSEC management consists of security management and COMSEC management.

10-9. **Security Management**. This controls access and protects the network and network management systems against intentional or accidental abuse, unauthorized access, and communications loss. Flexibility is built into security mechanisms to accommodate ranges of control and inquiry privileges that result from the variety of access modes by operations systems, service provider groups, and customers whom need to be administratively independent. Security management controls access to resources and archives, retrieves security information, and manages the encryption process.

10-10. **COMSEC Management**. This utilizes the AKMS, which consists of the Automated COMSEC Engineering System and Local COMSEC Management System hardware and software.

10-11. COMSEC management automates crypto-net planning, management, and engineering to include COMSEC record keeping and audit trails. The AKMS interfaces with strategic and tactical electronically keyed systems. The planning/design process for crypto-nets/COMSEC keys initially compartmentalizes the network by major assemblage and subscriber devices (EPLRS, SINCGARS SIP/ASIP, and NTDR). COMSEC management includes the development of an operational plan, which consists of system initialization (cold start) planned keying, rekeying, movement/displacement (renetting), expiration of crypto period, and compromise.

Fault Management

10-12. Fault management includes trouble management, which–

- Relates alarms to the different services and resources.
- Initiates tests.
- Performs diagnostics to isolate faults to a replaceable component.
- Triggers service restoration/
- Performs activities necessary to repair the diagnosed fault.

10-13. Proactive maintenance responds to near-fault conditions that degrade system reliability and may result in an impact on services. Fault management performs routine maintenance activities on a scheduled basis, initiates tests to detect or correct problems before service troubles or outages are reported, and provide trouble-ticketing services.

RESPONSIBILITIES

10-14. Although the brigade and battalion S6 share responsibility in managing the TI, the brigade S6 has overall responsibility for the TI. The brigade and battalion S6s use the ISYSCON (V)4 to perform the network management mission of the TI. ISYSCON (V)4 allows the S6 to–

- Proactively optimize network performance with the capability to plan, configure/install, monitor, and maintain/troubleshoot the network.
- Operate as a control point for the logical configuration and efficient utilization of network assets, diagnose and isolate network faults, and correct problems before users of the network detect systems errors.
- Reduce network degradation and provide network users uninterrupted service in the case of network problems.
- Integrate all management subsystems.
- Identify potential network communications problems and recommend corrective actions related to the supported forces' planned movement.
- Defend against computer network attacks.
- Provide a clear picture of path availability and actual utilization of communications and automation resources that include the type of traffic that is flowing across the network and the security of the information on the network.
- Plan and engineer retransmission/relay requirements for tactical radios based on the units operational mission concept.

NETWORK PLANNING

10-15. The network planning process in the tactical environment is different than typical commercial network planning. In a commercial environment, the planning process can take several months and the base configuration does not constantly change. However, tactical networks are constantly changing and therefore must have a reduced planning cycle.

10-16. The flow of information is based on the OPORD. The division G3 provides the unit task organization (UTO) component to the OPORD. The division G6 creates and provides the Signal Annex to the OPORD. Similarly, the OPORD is passed to the maneuver brigades and battalions and used in the development of their OPORDs. In the case of the signal units, configuration data is generated from this OPORD. This configuration data is then passed up to higher echelons for verification and then disseminated to the proper units for implementation.

10-17. Many systems or software processes are involved in network planning. Some of the systems currently provide stand-alone planning functions and others provide input into the planning process. Table 10-1 lists some of the key top-level planning and management functions.

Table 10-1. Top-Level Planning and Management Functions

System	Functional Description
MCS	OPORD
ISYSCON (V)1	ACUS Planning, Data Input (IP, AS number)
NTDR network management tool (NMT)	NTDR Planning
Tactical Internet Configurer (TIC)/ Tactical Internet Designer (TID)	FBCB2 Planning
Satellite Communications (SATCOM) Planner (MCPTI)	Military Strategic and Tactical Relay (MILSTAR) Planning
Revised Battlefield Electronic CEOI System (RBECS)	Network Identification
NCS	EPLRS Planning
TOC Planner	Router and Switch Configurations
KG 175 Manager	KG 175 Planning

10-18. The following paragraphs discuss network planning for radios, network devices, and network services as they pertain to the TOC or the TI.

NOTE: Upper echelon Warfighter Information Network (WIN) components are planned and managed by the ISYSCON (V)1 at division and above and will not be specifically addressed in this manual.

NOTE: The ISYSCON (V)4 manages the TI and TOC LANs in the digitized division. The TOC LAN is not a part of the TI, but due to ISYSCON (V)4's dual responsibility of managing the TI and the TOC LANs, TOC LAN management is included in this manual.

SINCGARS SIP/ASIP

10-19. SINCGARS SIP/ASIP is capable of voice and data modes of operation. Radios placed in the voice mode of operation require:

- SOI – includes the call signs and other pertinent identifying information.
- Frequency hopset information – is used to uniquely identify the various networks and includes the net IDs.
- COMSEC key – provides the encryption necessary to secure the radio transmissions.

10-20. Radios placed in data mode require the frequency hopset information, COMSEC key, and INC management information base (MIB). Some data systems within the TI (AFATDS) use the tactical communications information module (TCIM) instead of the INC. Current planning for SINCGARS SIP/ASIP voice nets is done using RBECS to create the SOI and frequency hopset data. The ISYSCON (V)4 will use TIC/TID to create MIB load files.

10-21. In the digitized division, the FBCB2 TIC/TID system will work in conjunction with the RBECS to plan all SINCGARS SIP/ASIP voice and INC-based data networks. TCIM-based data networks will continue to be planned using both the RBECS and manual methods. FBCB2 TIC/TID will run on the ISYSCON (V)4 platform at division, brigade, and battalion echelons.

10-22. Figure 10-1 shows the SINCGARS SIP/ASIP network planning data flow between the different devices used in the process. The FBCB2 TIC/TID includes the doctrinal voice network structure for a notional division. The operator (S6 personnel) has the ability to make modifications to the doctrinal net table to accommodate changes to support the current organizational structure.

10-23. The G6/S6 provides the RBECS operator with a list of SINCGARS SIP/ASIP nets for development of the master net list. An RBECS to FBCB2 translator process is created and integrated into the ISYSCON (V)4 to convert the FTP format into a JVMF format for use in the TIC/TID.

10-24. The RBECS assigns the net IDs, including frequency hopsets and COMSEC fill, and loads them into data transfer devices (DTDs). The net IDs are then passed back to the TIC for use in planning the TI.

10-25. The TIC uses the net IDs to develop the SINCGARS SIP/ASIP-related portion of the INC MIB. This information is delivered to the hosts.

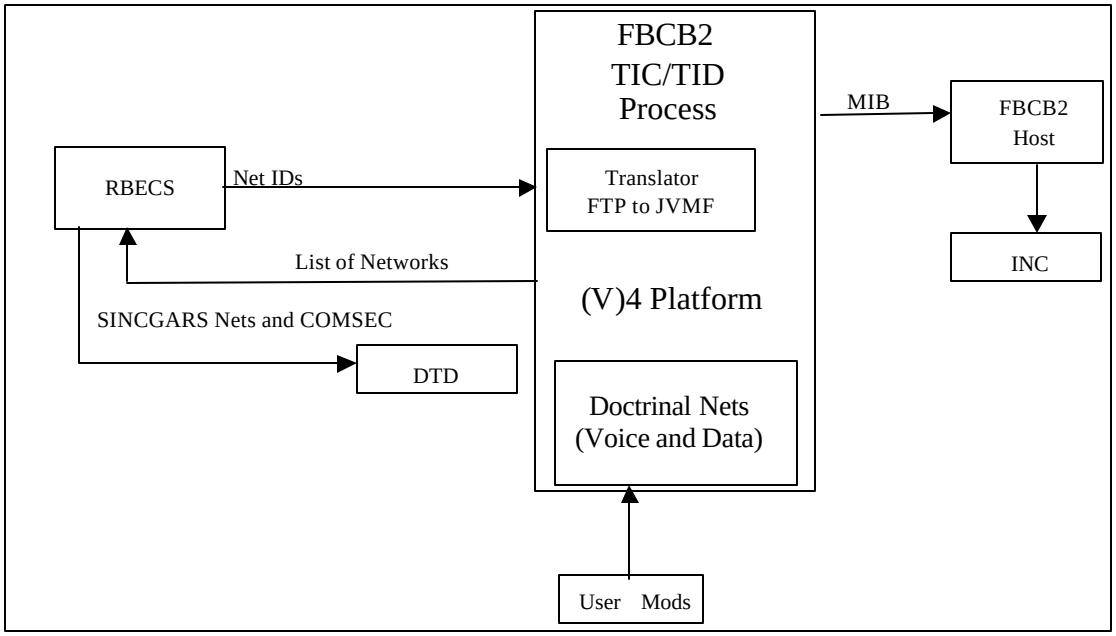

Figure 10-1. SINCGARS SIP/ASIP Network Planning Data Flow

EPLRS

10-26. ISYSCON (V)4 is required to participate in the planning of EPLRS net structures and virtual circuits. The ISYSCON (V)4 will exchange information with the NCS. This supports the C2 and SA requirements of the FBCB2.

10-27. EPLRS is a radio system with data transfer capabilities only (no voice). Network planning and control is performed using an interconnected system of NCSs. NCSs are division assets that are deployed based on geography and coverage areas.

10-28. The current EPLRS planning processes utilize some NCS tools, but mostly manual spreadsheet tools are used in the planning of EPLRS needline libraries. The needline libraries require various logical channels and contain the configuration (logical channel participants) for each RS in the network. Additional functionality in the NCS allows RS keying and rekeying using either a DTD (first initialization) or over the air rekeying (OTAR) (subsequent key periods).

10-29. The introduction of the ISYSCON (V)4 (FBCB2 TIC/TID tools) necessitates a new planning and initialization process for EPLRS. New IP-based functionality in EPLRS RSs provides the tool set required to make these changes.

10-30. Figure 10-2 shows the EPLRS planning data flow.

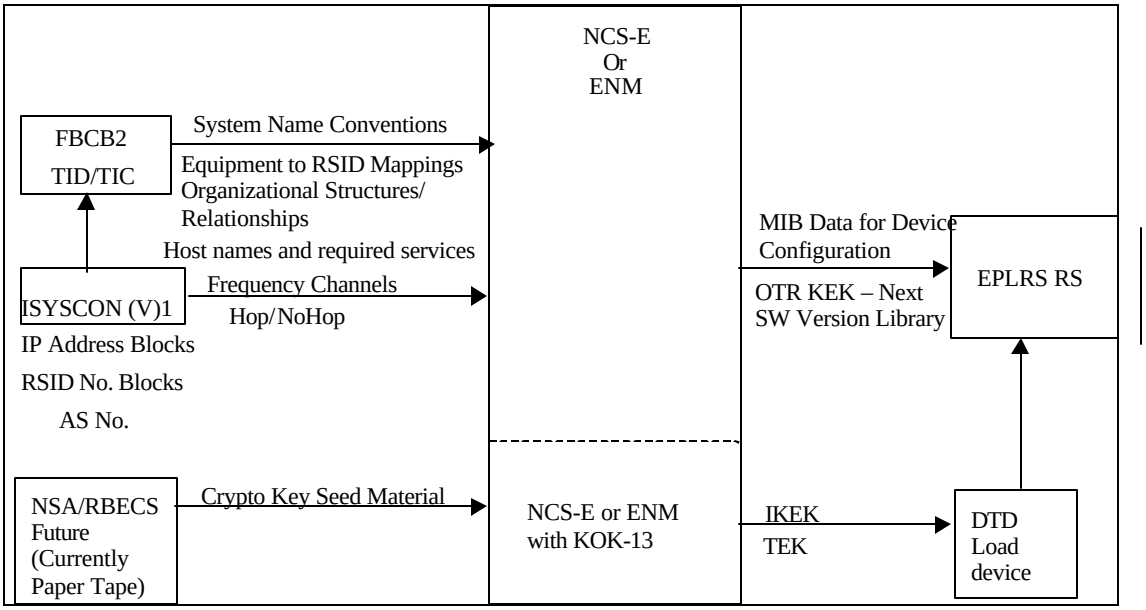

Figure 10-2. EPLRS Planning Data Flow

10-31. The ENM, a more distributed local EPLRS planning, initialization, and management system, is under development. The ENM will eventually eliminate the NCS-E hardware and replace it with the NCS-E software functionality running on the ISYSCON (V)4 platform at division, brigade, and battalion. In the digitized division, the ENM will be capable of all NCS functions except POS/NAV. The ENM will be able to run jointly with NCS-Es without interference. In addition, an ENM can create EPLRS simple network management protocol (SNMP) configuration information so EPLRS radios can be managed using COTS packages. The EPLRS in the digitized division will be able to function with or without these SNMP configurations.

SATCOM

10-32. SATCOM planning for the Spitfire; single-channel, anti-jam, manportable terminal (SCAMP); and secure, mobile, anti-jam, reliable tactical terminal (SMART-T) is performed for all resources at the division level. Initially, a PC-based interim-planning tool will be used to plan the MILSTAR network. In the digitized force, the MILSTAR communications planning tool integrated (MCPTI), which will reside on the ISYSCON (V)1 workstation at division, will plan the MILSTAR network.

10-33. The planning process includes a request of resources, TRANSEC keys, ephemeris data (principally the yaw and beam parameters–satellite location), and link planning information. This request generates a communications plan. The original planning process includes, but is not limited to, the amount of satellite resources required, number of terminals available, maximum number of links needed, and original key assignments. SATCOM systems configurations are then loaded into a DTD at division.

NOTE: GBS network planning is required for IP address assignment only.

10-34. Figure 10-3 shows an example of the SATCOM planning data flow.

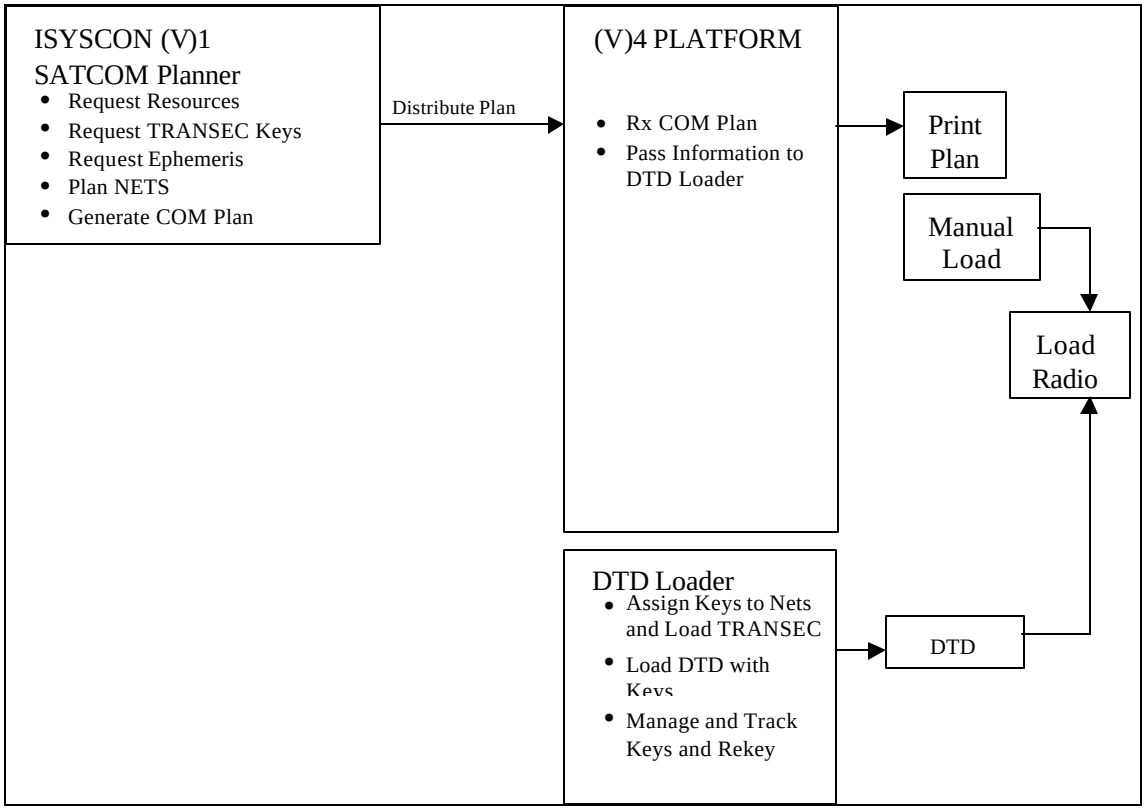

Figure 10-3. SATCOM Planning Data Flow

10-35. All SATCOM planning should be based on a 30-day window. Thus, there will be no dynamic reconfiguration of the SATCOM assets. The UHF demand assigned multiple access (DAMA) tactical satellite systems should be used for the single-channel devices (such as Spitfire) to optimize the available SATCOM resources. Therefore, the ISYSCON (V)4 will not be required to plan for SATCOM resources other than those previously identified.

TOC

10-36. The ISYSCON (V)4 will control the TOC LAN planning process. To control the network, the ISYSCON (V)4 requires information from several sources in both the maneuver and signal communities. Information process flow is required to plan each system that is connected to LANs. Data planning flows from the division to the brigade and then to the battalion. At each echelon in the flow, detailed planning creates configurations for the elements within that echelon's area of responsibility (AOR).

10-37. The TOC LAN planning process is summarized below.

- The MCS creates an OPORD, including a UTO.
- The ISYSCON (V)4 queries the C2 registry (C2R) for any units in the UTO for which it doesn't have data (Modification Table of Organization and Equipment [MTOE], symbology, unit identification code, user reference number [URN], and host name).
- ISYSCON (V)1 (at division) provides a block of IP addresses; a block of EPLRS RSIDs, and AS numbers to allocate to TOC elements.
- Through the TOC LAN planning process, the ISYSCON (V)4 assigns IP addresses and determines the role (host-name) to IP address mapping for the TOC servers and joint variable message format (JVMF) forwarder. This information is then provided to the FBCB2 TIC via JVMF message.
- The ISYSCON (V)4 platform runs through the TOC planner process to generate the TOC network plan. The TOC planner process includes, but is not limited to, the following:
  - IP addresses for network devices requiring stable addresses in the TOC, such as the GBS and battlefield video teleconferencing (BVTC) workstations.
  - Configuration information for the TOC routers, Ethernet switches, wireless LANs, EPLRS, and inline network encryption (INE) devices.
  - Configuration information for the Dynamic Host Communications Protocol (DHCP) server in the TOC. Additional information may need to be passed to the associated small extension node (SEN) system to correctly configure redundancy between the WIN DHCP and TOC services.
  - Initial DNS configuration information. Again, coordination with the NCS/DNS may be required. Run a server location protocol (SLP) to eliminate some of the DNS data replication complexity.

10-38. TOC planning includes subnetting and IP address assignment and router and switch configurations. Subnetting and IP address assignment are two of the most critical and most widespread requirements for the ISYSCON (V)4 platform. For each of the other planning processes to be successful, the network must be correctly subnetted and IP addresses assigned.

Subnets and IP Address Assignment

10-39. The ISYSCON (V)1 at division will assign a block of IP addresses for the WIN-Terrestrial (WIN-T) assets including the NC, large extension node (LEN), and SEN, as required. The ISYSCON (V)1 then divides the subnets and remaining addresses into logical blocks based on a notional requirement (a brigade typically requires 230 subnets). Using a subnet mask is part of the subnet process.

10-40. The Class B address has been further refined into a notional Class C structure by using the 255.255.255.0 subnet mask . Table 10–3 lists the conventional subnets for Class B addresses. Figure 10-4 shows a notional subnetting structure.

NOTE: that more refined subnet masks may be required in order to meet the subnetting requirement.

Table 10-3. Conventional Class B Subnets

Subnet Mask	Number of Subnets	Number of Hosts
255.255.192.0	2	16,382
255.255.224.0	6	8,190
255.255.240.0	14	4,094
255.255.248.0	30	2,046
255.255.252.0	62	1,022
255.255.254.0	126	510
255.255.255.0	254	254
255.255.255.128	510	126
255.255.255.192	1,022	62
255.255.255.224	2,046	30
255.255.255.240	4,094	14
255.255.255.248	8,190	6
255.255.255.252	16,382	2

10-41. Once the IP address blocks have been assigned, the next step is to assign IP addresses to specific devices. Once assigned, IP addresses will be included in the planning process. It has not been determined if the EPLRS LAN ports will be provided a separate subnet or be included in a TOC LAN subnet. The IP address space is a serious concern associated with digitization. Anything but maximum address space efficiency may load the IP block to exhaustion.

10-42. The ISYSCON (V)4 platform also manages Class D (multicast) addresses. The Class D address space allocation is similar to that of the Class B. The addresses will be passed from the ISYSCON (V)1 to the appropriate ISYSCON (V)4. The ISYSCON (V)4 will assign a block for the FBCB2 multicast groups that are principally based on the doctrinal network structure. Another block will be assigned for the TOCs for ABCS multicasting. The general rule for inter-TOC multicast address assignment is that the address will be assigned by the higher echelon and passed down to the appropriate echelons.

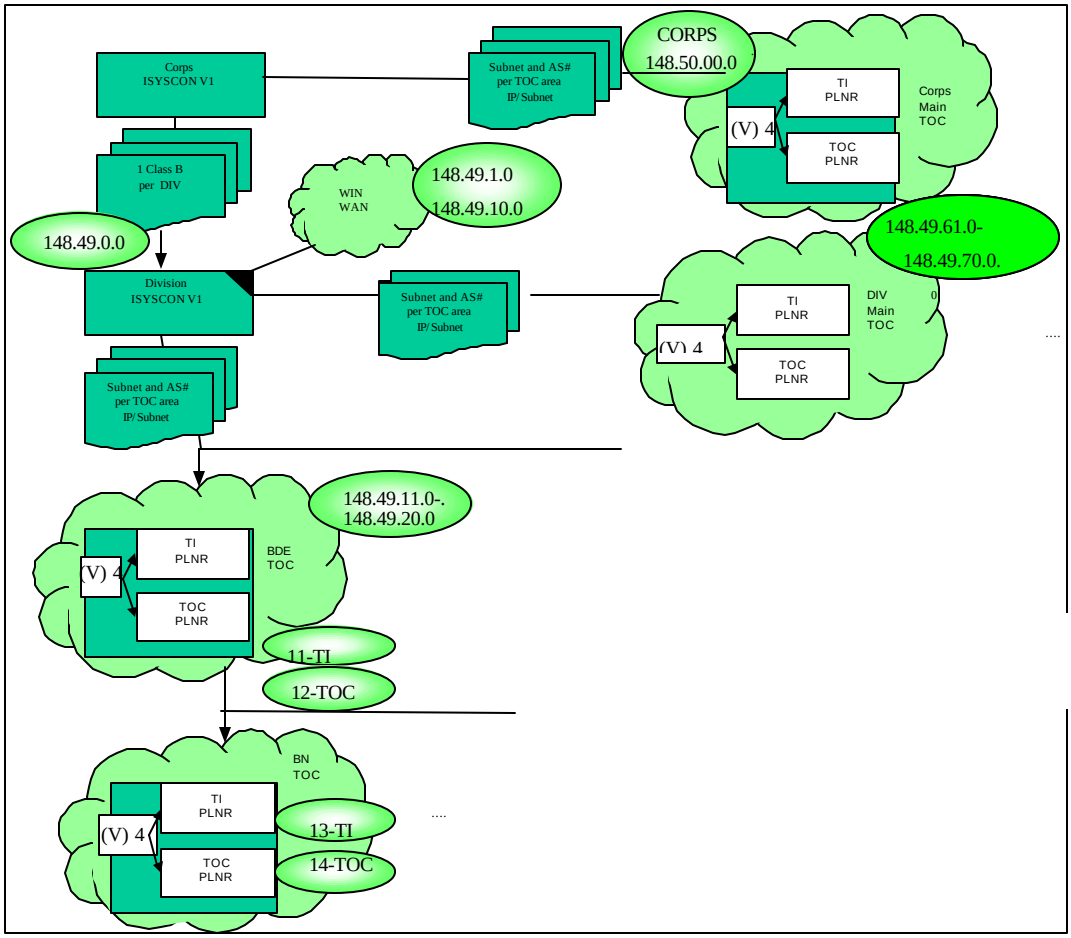

Figure 10-4 Notional Subnetting Architecture

Router Configuration

10-43. The router configuration process requires detailed planning by the signal personnel using the ISYSCON (V)4 platform. The paragraphs below discuss areas of the router configuration process. Figure 10-5 identifies the input and output flow diagram for each area of consideration in the router configuration process.

10-44. Router configurations have been identified and added to the router configuration tables. The modeling process is used to verify that the router configurations agree with the information entered into the individual network devices such as the NTDR, wireless LAN, and Ethernet switch.

10-45. The network configuration information is passed to the ISYSCON (V) 1, where all the router configurations can be run through the verification process. The goal is to identify any anomalies with the router/switch architecture such as routing loops and duplicate IP addresses for the entire division.

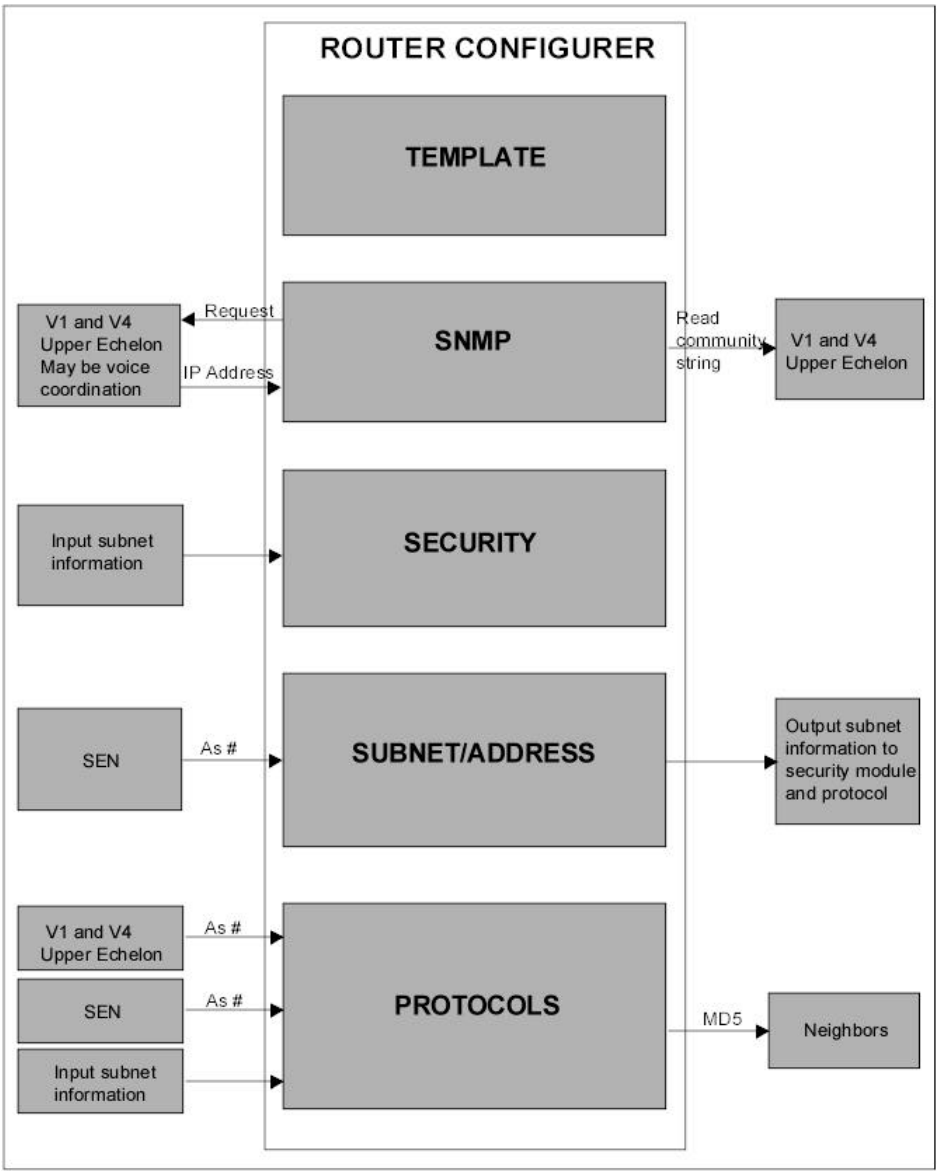

Figure 10-5. Router Configuration Data Flow

10-46. **Templates**. Institute the physical TOC as templates based on MTOE data that is previously known, entered/modified by the manager, or received from the C2R. The operators will layout the main TOC and split TOC configurations with a graphical tool that shows the higher-level vehicle configurations, lower-level components, and ports within each component. This tool will be written as part of the TOC planner process running on the ISYSCON (V)4. It will create subnets and host address space requirements. The last known configuration will be used as a deviation point.

10-47. Generic device templates are used to make up the default configuration information for specific types of network elements such as routers. The template contains default format information. Since a router script file is format-dependent, the order of lines in a script affects the routing functions. The template is required to maintain the desired structure of the router configurations such that the individual statements are in the proper location of the router configuration.

10-48. **SNMP**. Specific information in the managed objects must be included to allow the exchange of SNMP traffic between the ISYSCON (V)4 and the managed element. Two of the data sets are the network management station(s) IP addresses and the read and write community string (SNMP read and write password that is unencrypted – droarp in this example).

10-49. Several network managers may be assigned to a router. The local TOC ISYSCON (V)4 will have read access into the SEN's router to obtain status information on the edge device connecting the TOC to the WAN. ISYSCON (V)4 could give enhanced switch operating procedures (ESOPs) equivalent read access to the TOC routers. Therefore, specific SNMP server information must be exchanged between the ISYSCON (V)4 and SEN operators.

10-50. To establish SNMP information with the SEN, the local net manager sends the IP address and read community string of the ISYSCON (V)4 to the ESOP operator in the SEN, who places this information in his router configuration. The SEN operator then responds with the IP address and read community string for his router. The OPCON of the ESOP router will be under the control of the SEN operator; however, the ISYSCON (V)4 will have insight (operational status), via SNMP, into the edge router of the colocated SEN. The remaining devices within the TOC will direct SNMP traps only to the ISYSCON (V)4 platform within that TOC.

10-51. **Security**. ACLs limit the types of data that can be sent over a particular port. It can allow access to particular users for a particular type of network traffic. One of the key uses for access control within a TOC is to deny high bandwidth traffic from access to low bandwidth communications medium.

10-52. Integers 1 to 99 represent a standard ACL that permits or denies traffic based on a source node or network address. Integers ranging from 100 to 199 represent extended access control lists. The extended control list is much more sophisticated than the regular access control list. It restricts traffic based on protocol, source, and destination. Without specific guidance or ACL templates/algorithms, ACLs can be very large and complex to manage. A preconfigured group of ACL templates will be loaded into each ISYSCON (V) 4. It will be automatically inserted into each router configuration file as the ISYSCON (V)4 TOC planner process generates the template. The operator will have to override the list if changes are to be made.

10-53. **Subnets and IP addressing**. Each brigade and battalion TOC will have a predefined number of generic subnets that must be allocated. Based on the block of IP addresses that were received from the ISYSCON (V)1 or a higher echelon ISYSCON (V)4, the actual numbered subnets will be

generated. Also, subnet masks will be included to minimize the IP address space that must be advertised. Each port on a router/switch should advertise a single subnet.

10-54. Each network device on an Ethernet non-point-to-point link must assign an IP address to each port. Additionally, loopback addresses need to be assigned to network devices, where applicable, so the network manager can send an SNMP query to the device as opposed to a port, which may or may not be operational on the device.

10-55. **Protocols**. Protocols used in the digitized division are discussed below.

- **Open Shortest Path First (OSPF**). Assign OSPF area numbers to network devices and integrate with templates. Within the TOCs, several OSPF dynamic RAs must be linked together. Figure 10-6 shows BGP-4 ASs and OSPF RAs. The actual OSPF RAs are subject to change as the architecture evolves. The NTDR has been identified as the backbone RA (Area 0). This assignment is critical because all traffic between OSPF areas must traverse through OSPF Area 0. OSPF does not require static addresses be assigned and is therefore more dynamic than BGP-4.
- **Border Gateway Protocol-4 (BGP-4).** Determine BGP-4 neighbors and integrate with templates. BGP-4 data must be entered into the router configuration for traffic that must transverse ASs. Neighbor addresses and AS numbers are hard-coded into the router configuration for BGP-4. The WIN backbone neighbor information comes from either the ISYSCON (V)1 or from the SEN operator who is controlling a WIN edge router that is actually a physical neighbor of the TOC router being configured.
- **Multicast**. Multicast protocols that will likely be implemented in the router configuration include–
  - Internet group management protocol (IGMP).
  - Proxy IGMP for INC and NTDR.
  - Protocol independent multicasts (PIMs) sparse-mode completed from template.
  - PIM dense-mode completed from template protocols.

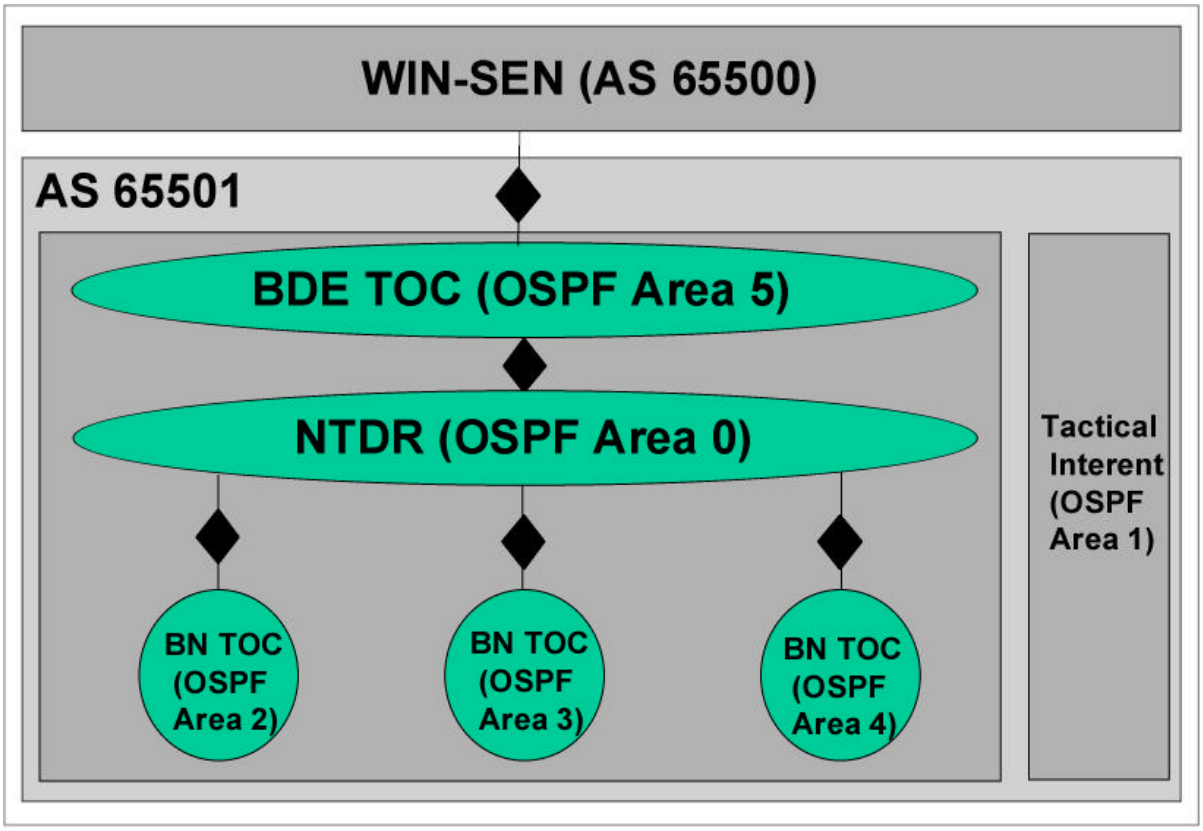

Figure 10-6. BGP-4 ASs and OSPF RAs

10-56. **Switch Configuration**. The switch configuration is less detailed than the router configuration. Virtual local area networks (VLANs) are the most complex part of configuring the switch. If VLANs are required, they will follow the same paradigm as the router configuration through templates and simplified configuration data such as default spanning tree data. Figure 10-7 shows a typical switch configuration. Currently, VLANs within a tactical environment is questionable because of the additional configuration required.

10-57. Based on the amount of configuration information that is required, every attempt should be made to simplify switch configurations. Generic templates must be developed for all echelons.

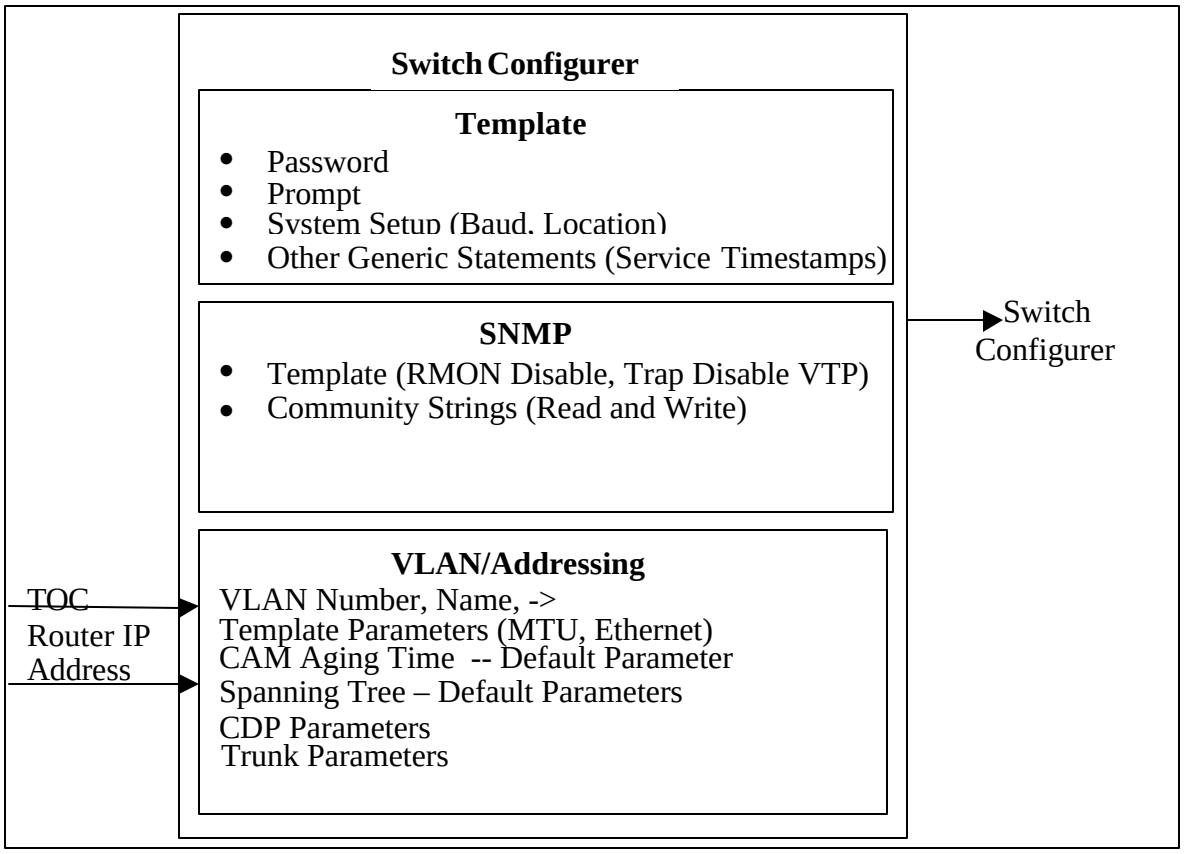

Figure 10-7 Switch Configuration Data Flow

NAME SERVICES

10-58. ISYSCON (V)4 develops both the DNS and DHCP initialization files to include the IP address pool, stable addresses for servers and EBC hosts, location of the DNSs, default gateway (router), FBCB2 addresses, and IP tuning parameters.

10-59. Figure 10-8 provides a notional data flow for DNS and DHCP services. Two different threads are identified. The right side of the figure shows the TOC process, while the left side shows the WIN-T (NCs and SENs) process. At each echelon from division down to battalion, the ISYSCON (V)1 or ISYSCON (V)4 passes down a block of IP addresses to the next lower echelon. The current process has the initial battalion configurations being developed at brigade and pushed down to the battalion. The WIN-T components use predefined file templates for the router and switch configurations. The DNS plus seed information and DHCP information will be made into a template.

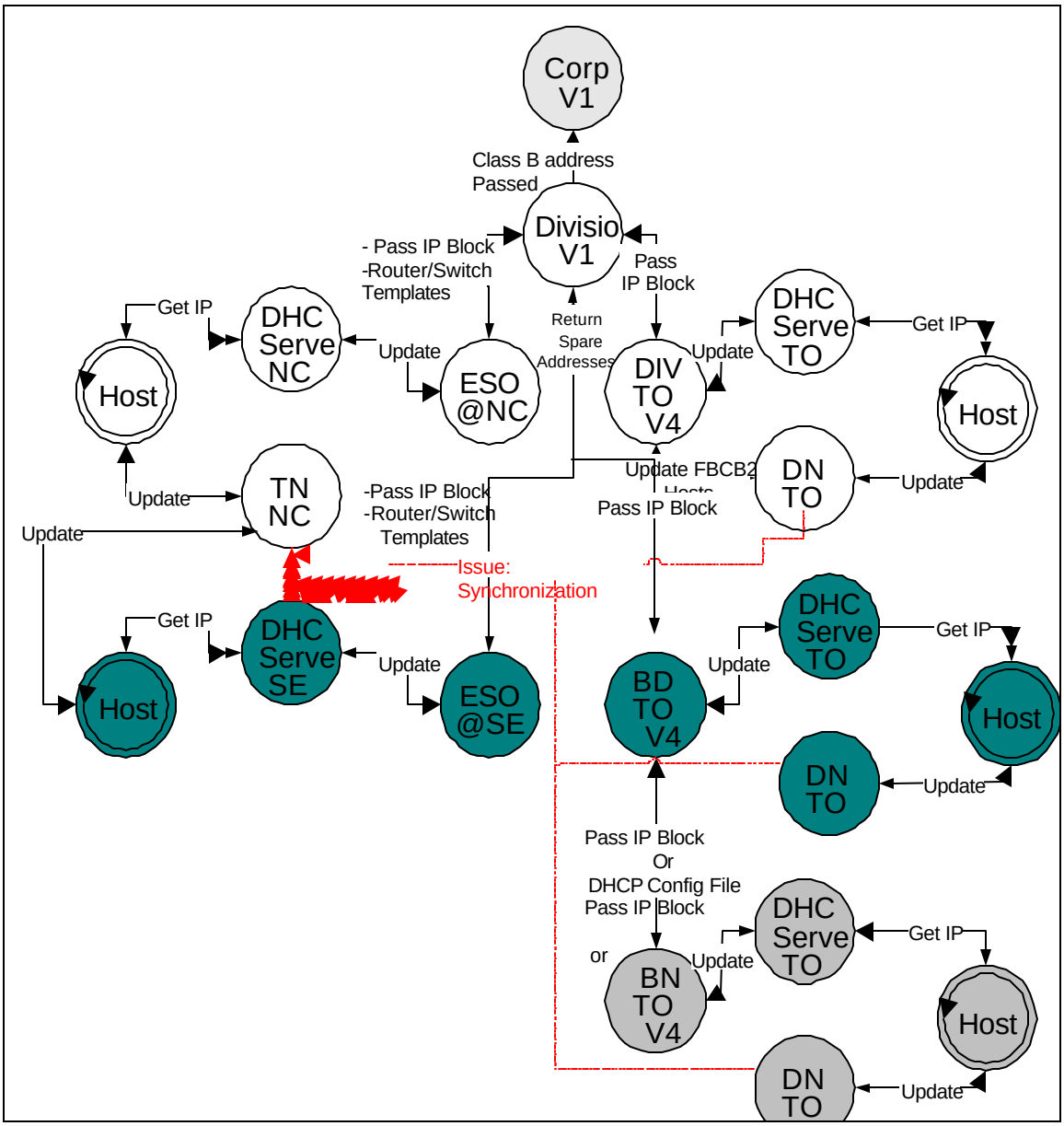

Figure 10-8. Notional DNS and DHCP Services Data Flow

10-60. The local ISYSCON (V)4 DHCP planner process identifies the subnets required for TOC operation, including split/jump TOC components. The subnets will be automatically generated once the manager provides one of the policies (one subnet per vehicle or one subnet for the area behind the router). A default policy will be in place rather than the network manager identifying the policy. However, division and brigade TOCs require one default subnet per area behind each router. Battalion TOCs will have a subnet per vehicle behind each router. However, if a vehicle moves between the main and the jump cell, a unique subnet per vehicle will be required. This

approach applies for brigade and above TOCs; the battalion TOCs are provided with a subnet per vehicle due to the router architecture. During this time, the routers are configured based on default template and algorithm and are automatically assigned IP addresses.

10-61. Once the subnets are identified, the network manager will identify, based on policy, those hosts that require a stable IP address. The number of hosts that require stable IP addresses is currently limited to the TOC server and BVTC hosts.

10-62. Similarly, a pool of IP addresses based on TOC size and spare addresses will be assigned for each subnet in the TOC. It is assumed that the main and the jump portion of the TOC operate autonomously even when they are connected. The only difference between jump and connected operations is that a LAN is used to connect the main and jump cells and the WAN is used for interconnection in the jump mode. The same principle applies with a task force, where a field artillery or military intelligence battalion may be brought in to support a TOC.

10-63. The router IP address (default gateway), subnets, and server IP addresses are defined because of the router configuration process. This information, in addition to predefined IP settings, is passed to the C2R/server boot process and loaded into the DHCP server(s). Even if there is redundancy in DHCP servers, all the information is loaded into each potential TOC DHCP server.

10-64. The TOC and NCS will use the same product so that data replication and DNST synchronization is automatic.

10-65. Two approaches can be taken regarding synchronization between the TOC and the network name services. First, data can not be exchanged between the SEN and the TOC DHCP servers that limit or deny a WAN user insight into the TOC DHCP address space and vice versa. When the primary DHCP and subsequent backups fail, the router requires reconfiguration to allow boot protocol traffic to exit the router. It also requires an update that includes subnet information to be sent to the DHCP server. Second, always exchange subnet information and use the other DHCP server in either the TOC or the SEN as a backup. The first option is currently where the design appears to be migrating.

10-66. The digitized division does not have dedicated TOC servers. Therefore, any ABCS host can take over TOC server responsibility. The TOC server consists of the JVMF forwarder, C2R, DNS/tactical name server (TNS), and DHCP servers. The goal is to run all of the TOC server services on a single ABCS host, where this network server has a well-known stable address. ABCS hosts acting as the server will have a single IP address for both the server and the host's role. The server address does not change regardless of which ABCS box the server functions reside on. However, at battalion echelons, each host is on a separate subnet. If a single server IP address was used, the routers would require reconfiguration to become the server. The best approach with the least risk is to have two dedicated servers located in the vehicles containing the NTDRs at each battalion.

10-67. The DHCP configuration requires subnet information for the TOC. This includes a subnet for each vehicle, a block of addresses in each subnet, a subnet mask, the address of the router, the address of servers, and static hosts as defined by the SOP or the operator. The output of the DHCP server is the IP addresses (from a pool or static), default route/gateway router, name server, C2R, and the network mask. Figure 10-9 shows the DHCP data flow. The ISYSCON (V)4 uses input that it has received from other ISYSCONs and develops a DHCP configuration file that is then loaded into the host via the C2R/ABCS server initialization process.

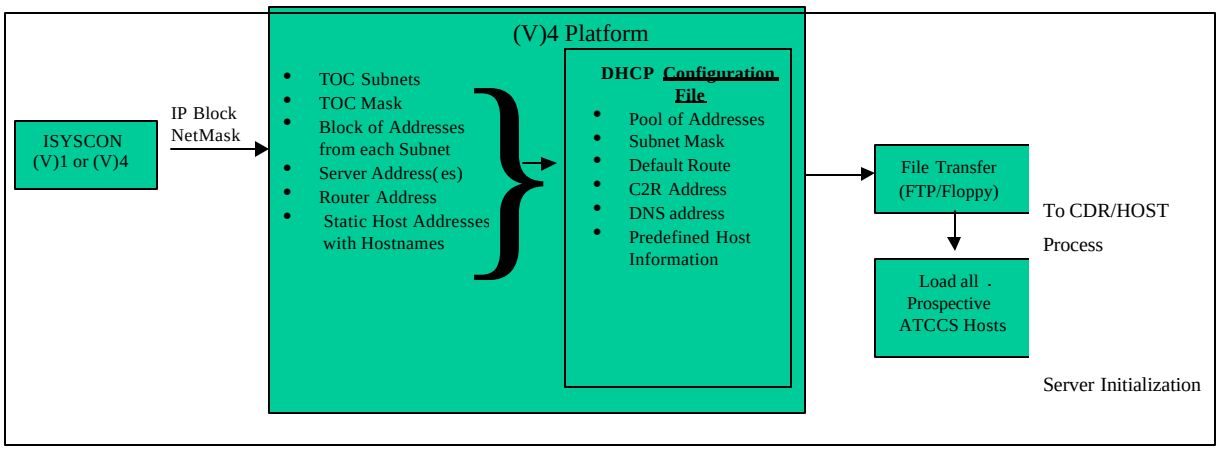

Figure 10-9. DHCP Data Flow

NTDR

10-68. The NTDR in the digitized division will function as a TOC-to-TOC WAN data transport system. Its function for division, brigade, and battalion level maneuver units is similar to that of the TPN or ATM-enhanced WINs for corps, division, and brigade echelons. The NTDR will provide data transport between TOCs and other participating assets at these echelons.

10-69. The NTDR can be configured to accommodate a variety of network architectures. Brigade-size elements will have an NTDR network consisting of 20-25 RSs (including 6 relays). Each brigade-size NTDR network will be within a brigade/task force AS. The transport (RF) side IP address for each brigade-size NTDR network will have a single IP subnet allocated to it. The digitized division will have several networks, including brigades, based on geographic relationships between division level units assigned their own autonomous areas. Routing within an autonomous area is via OSPF embedded in the NTDR RS routing card. BGP-4 is not implemented in the embedded routing card of the NTDR; therefore routing between autonomous areas is not possible without the addition of an external router capable of BGP-4 communications.

10-70. The NTDR NMT plans, initializes, monitors, and troubleshoots/reconfigures NTDR RSs and networks. One NTDR NMT is allocated per NTDR AS. The NTDR NMT is normally connected to a NTDR and works in conjunction with RBECS and a DTD to plan, initialize and monitor an NTDR network. The NTDR NMT will reside in the S6 vehicle with the ISYSCON (V)4.

10-71. The NTDR requires information from several sources to complete a plan. Figure 10-10 shows the NTDR data flow.

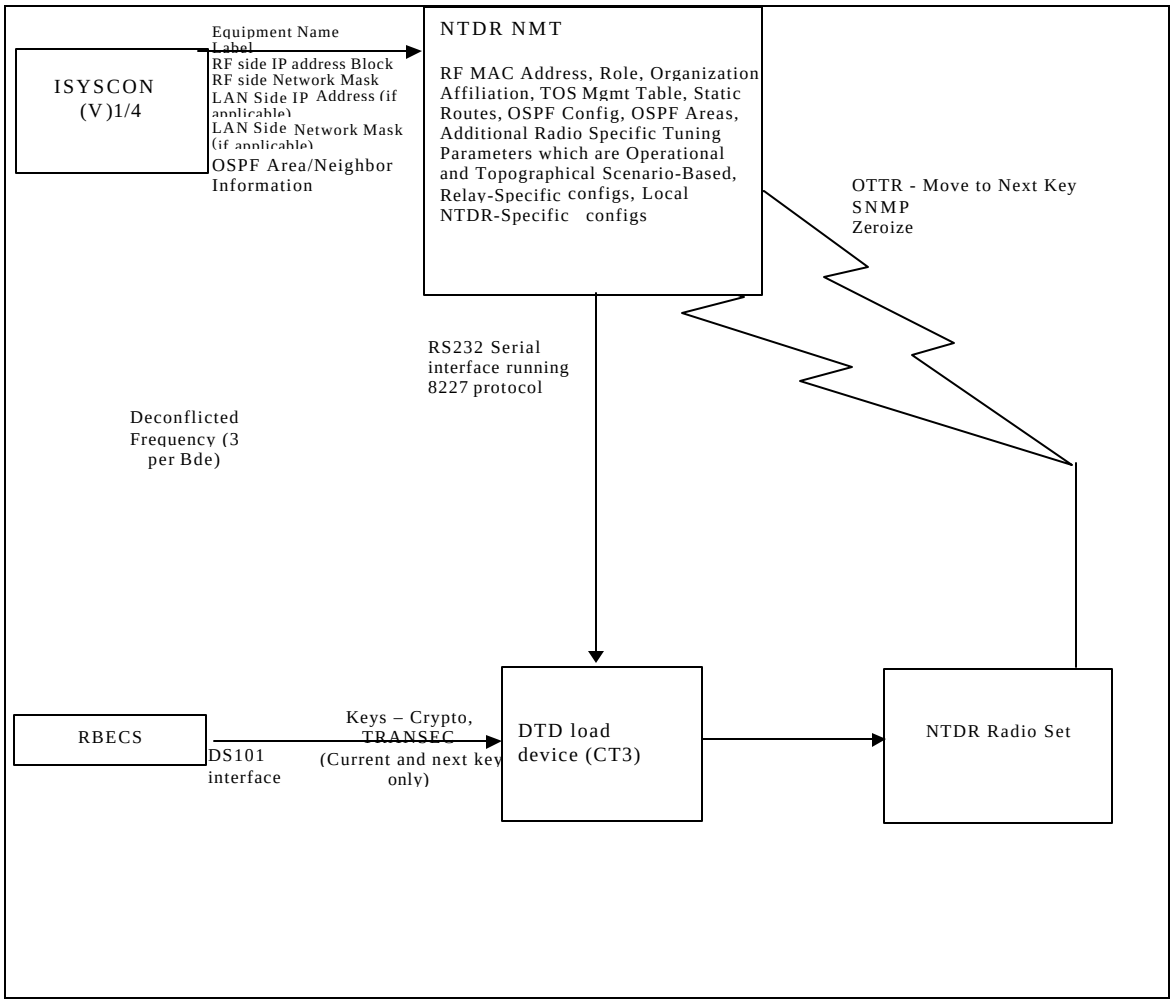

Figure 10-10. NTDR Data Flow

10-72. Two potential LAN configurations are available for TOC-based NTDRs. The first is to run Port 1 or Port 2 of the NTDR as an Ethernet port and assign an IP address and mask to the port. In current TOC architectures, this Ethernet segment would connect directly to a TOC router. The NTDR Ethernet address would be assigned an IP address and mask from the TOC subnet. The OSPF would be run between the TOC router and the NTDR port.

The NTDR router card would isolate the TOC subnet from the NTDR RF transport subnet.

10-73. In the second configuration, a port connected to the TOC router would run as an unnumbered serial interface. This precludes the need to assign an IP address to the NTDR port. No routing protocol would be run between the TOC router and the NTDR. The TOC router would make all traffic decisions and the NTDR would process all data sent via the serial link. This configuration is easier to plan and more efficient in the use of IP addresses. The limiting factor is the ability of the NTDR to implement this type of interface and the data rate supported by the serial interface.

10-74. Certain key NTDRs must be configured differently to operate and be manageable. The NTDR NMT radio and relays are the primary systems with special requirements. The NTDR associated (and normally co-located with) the NTDR NMT station must be a designated clusterhead to enable it to communicate with other clusterheads to send and receive SNMP information and perform OTAR functions.

10-75. Relays must also be clusterheads and must be located to ensure adequate LOS visibility and range connectivity to be successful in their requirements. This LOS planning indicates that a terrain profiling capability must be present at the echelon where relay deployment decisions will be made. The division level has the resources, both computing (ISYSCON) and manpower, to properly plan and implement relay requirements of maneuver elements.

SECURITY DEVICES

10-76. The KG 175 is the inline network encyrptor (INE) in the digitized division. The KG 175 operates with tactical IP and ATM networks and tunnels through the backbone network at different security levels. The KG 175 will be used to tunnel unclassified STAMIS data over the SECRET backbone network. Consequently, configuration and monitoring of the KG 175 device is via SNMP. However, the KG 175 has the TI system manager (TISM), a separate manager that provides–

- Security management — consists of access control services, tactical compromise and recovery, and audit data collection and recovery.
- Network management — consists of the configuration of network parameters and status collection.
- Key management — consists of key assignments, r-key of firefly key, and the compromised key list distribution.

10-77. Since there is a dedicated KG 175 management station, there will be swivel chair operation from the ISYSCON (V)4 to the TISM.

SENSITIVE BUT UNCLASSIFIED (SBU) USERS

10-78. SBU users require an additional workstation to support the SBU network because the ISYSCON (V)4 does not support multi-level security.

10-79. SBU engagement operations networks will consist of dedicated channels to provide the SOS requirement. A block of IP addresses will be provided for the SBU engagement operations networks. Eventually, the

ISYSCON (V)4 will provide some type of network planning for these networks. However, the ultimate goal is to provide IP packet precedence to meet the SBU engagement operations SOS requirements.

ABCS

10-80. The various host systems operating within a TOC LAN and across the TOC to the TOC WANs need application layer configuration information. Unlike the lower echelons, where the FBCB2 TIC/TID running on the ISYSCON (V)4 is responsible for both application layer and TI network layer planning, the ABCS application layer planning will be completed on a tool running on one or more ABCS host systems. A TOC planner process running on an ISYSCON (V)4 will plan the TOC LAN and TOC-to-TOC WAN systems.

10-81. Information exchange between the ABCS planner system and the TOC planner process on the ISYSCON (V)4 is via an FTP or disk transfer except in the area of SNMP configurations, which are performed using SNMP sets. The DHCP provides the remaining host configuration.

FBCB2

10-82. The network communications pipes and the client-server and host-to-host relationships must be properly planned and configured for FBCB2 applications to function. By necessity, some information is common to both areas; however, ensure maximum separation between network layer configurations and applications layer configurations so networks are not configured specific to any particular application, but rather generic for any application.

10-83. The FBCB2 TIC/TID process running on the ISYSCON (V)4 will be responsible for FBCB2 host configurations and TI network configurations.

10-84. The FBCB2 planning process will take place at the brigade TOC. Figure 10-11 shows the FBCB2 data flow.

NETWORK INITIALIZATION

10-85. Once the network planning cycle is complete, the configuration information must be loaded into each network device. Configuration data can be initialized through a DTD that contains particular configuration information including TRANSEC and COMSEC keys. It can also be initialized through a configuration file that is loaded into each device. Examples of these configuration files are the router/switch configurations, DHCP/DNS seed files, and the FBCB2 database/MIB configurations.

10-86. When initializing the network, it must be determined if the network has or has not been established and if configuration data exists. If the network is established and an existing configuration file is loaded and operating, the configuration file must be modified before initialization. If the network has not been established, the configuration file will be loaded during a cold start.

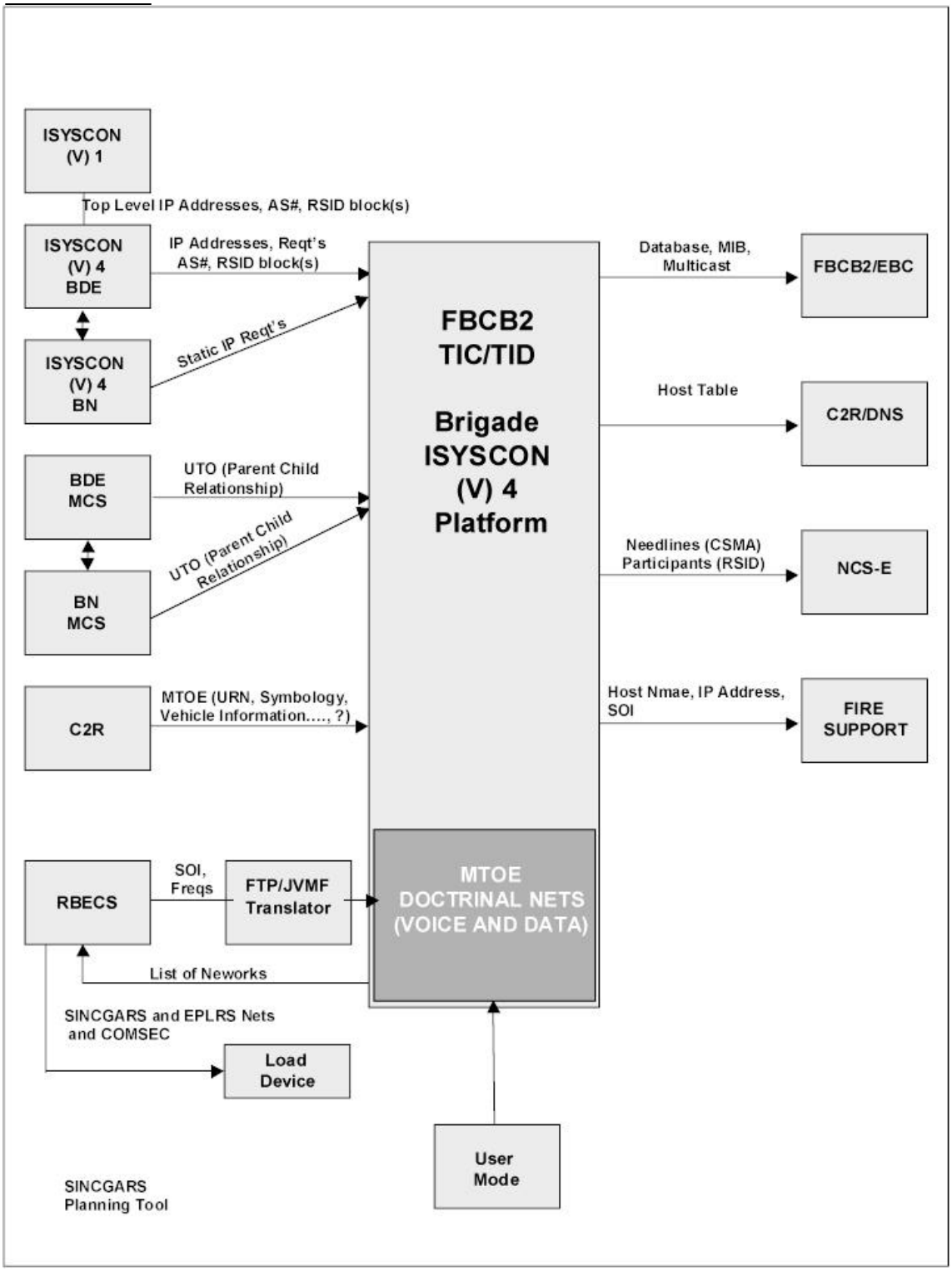

Figure. 10-11. FBCB2 Data Flow

SINCGARS SIP/ASIP

10-87. The loading of the SINCGARS SIP/ASIP voice nets is manual and requires the DTD to load the COMSEC keys and net IDs.

10-88. The INC is loaded from the local host via an unformatted Asynchronous American Code for Information Interchange (ASCII) file transfer. Currently, AFATDS is communicating to the SINCGARS SIP/ASIP via a TCIM. The AFATDS configures and loads the TCIM and configures the network; however, it is not responsible for the SOI, net ID, and COMSEC.

EPLRS

10-89. Current initialization of the EPLRS network is done through a combination of a DTD, NCS-E, and SNMP sets via the ENM.

SATCOM

10-90. SATCOM planning will take place at the division through MCPTI. The COMSEC variables are loaded via the DTD directly to the radios. For the SMART-T and SCAMP terminals, the TRANSEC variables will be loaded into a DTD, which is then auto-loaded into the radio.

TOC

10-91. Within the TOC, the routers and switches are initially loaded through a serial interface to the console port using a small laptop/palmtop. This device must have enough capacity to store several router configurations. The intent is to have a primary router configuration and several contingency configurations to reduce the burden on the responsible soldier. Several router configurations will be loaded onto the TOC server for potential push to the router if the laptop is ever unavailable. The most likely combinations of router configurations will be maintained and stored as separate files in garrison. If the network has been previously established and the switch or router can receive data from the network, a trivial FTP or Telnet session can initialize the router or switch. Alternate router configurations cannot be stored in the router or switch to be brought up on demand. Rather, once the new configuration file is loaded into the device, it begins to operate on the new file. Thus, coordination and configuration management of loaded router/switch configurations is critical to TOC operations.

NAME SERVICES DHCP INITIALIZATION

10-92. Upon initial boot, a host performs a DHCP discover and obtains an IP address. If there is no response from a known DHCP server, the host will become the DHCP server (after coordinating with the S6) or implementing other tactics, techniques, and procedures (TTP). After obtaining an IP address from the DHCP server, the user will attempt to contact the C2R for host configuration information. Once the DHCP server is established and hosts obtain IP addresses, the boot sequence continues. Before the DHCP server assigns an address, a ping and a DNS query must precede the assignment of that address to ensure that the same address has not already been assigned.

10-93. When the DHCP server assigns an IP address to a host, the server will subsequently update the DNS.

10-94. A hybrid approach of these potential solutions is also a possibility. Regardless of the method used, the FBCB2 is responsible for initializing each FBCB2 host.

NTDR

10-95. The NMT can generate radio configuration files and send these files to a floppy disk, via FTP or e-mail. The files required to configure a NTDR will be sent to a DTD over a serial connection to the NTDR NMT. Additional key information for the current and next key periods will be placed into the same DTD by a collocated RBECS (at brigade or above). Each and every NTDR in the network must be touched with the DTD to upload the configuration and key information. After the initial load, the NTDR NMT may generate or implement the next key command. Additionally, an NTDR NMT with read-write access privileges can reset MIB variables for specific radios over the air but in-band.

SECURITY DEVICES

10-96. Initially, the user will have to manually load the KG 175 to allow initial network access. All subsequent updates are via SNMP.

SBU USERS

10-97. A hard copy printout, floppy disk, or an FTP will provide the data for SBU users and the engagement operations initialization terminals.

ABCS

10-98. The C2R is the primary tool/repository used for ABCS and TOC server initialization. ABCS hosts will use both the boot and login processes for systems initialization.

FBCB2

10-99. If the network has not been established (no data in the INC or incorrect data loaded into the INC), then each host must be provided an initial load. This load is potentially through an Ethernet connection to multiple hosts using a laptop or other tool or through a default mass factory loading.

10-100. If the network is operational, initialize the network by–

- Reliably multicasting the configurations from a central location.
- Multicasting using a branching technique such that the brigade multicasts to battalion elements, battalion elements multicast to companies and so on until all hosts have received the data.
- Passing required seed data to each host and letting the host develop the configuration and pass to individual hosts.

NETWORK MONITORING

10-101. In the planning process, the COTS package did not perform the tactical planning function. However, in network monitoring, COTS packages are used in the tactical environment. The ISYSCON (V)4 will consist of a common COTS SNMP package that performs all monitoring of those devices that have SNMP agents.

10-102. The information flow from the planning process to the monitoring process includes network topology data such as unit identifiers, IP addresses, and subnet information. Figure 10-12 shows the data flow from the planning process to the monitoring process. While commercial SNMP monitoring tools have an auto-discovery mechanism, they only provide status on those devices that are established or have been previously established. The monitoring process of the ISYSCON (V)4 requires an overall network topology providing status of the network. The user will be able to drill down a path to receive specific information on a given device. For instance, the NTDR segment of the overall map changes state, and the user can identify the specific device(s) that changed state.

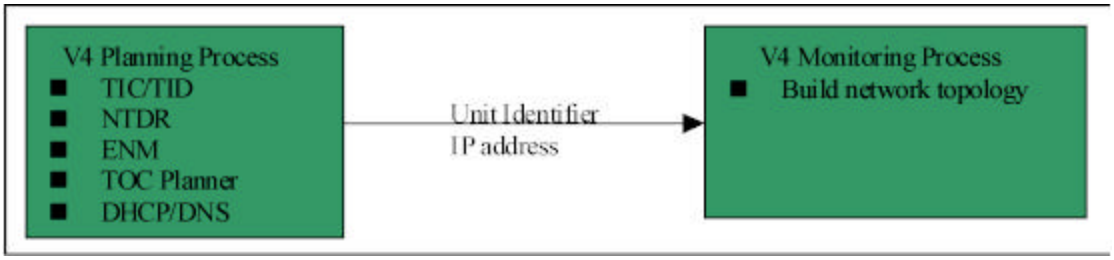

Figure 10-12. Data Flow from the Planning Process to the Monitoring Process

10-103. Figure 10-13 provides a flow of the network management function at the brigade and battalion echelons. However, each TOC, including the division and corps CPs equipped with ISYSCON (V)4 platforms, can plan and manage the network or a portion of the network. The lighter boxes represent those devices that are monitored by the ISYSCON (V)1. The ISYSCON (V)1 monitors all the devices that comprise the WIN-T WAN, such as the NCS, LENs, and SENs. The darker boxes represent the TOC LAN Manager's AOR. The local TOC manager will monitor the edge devices (the 7505 router and ATM switch in the SEN). However, the ESOP operator in the SEN is ultimately responsible for troubleshooting and repairing the system. The ISYSCON (V)4 will not be able to change configurations within the SEN.

10-104. Network monitoring provides fault management. Fault management detects, isolates, and leads to the troubleshooting/resolution of abnormal network operation. A network manager ensures that systems as a whole and each essential component are in proper working order. Nevertheless, when a fault occurs, it is important for the network manager to rapidly–

- Isolate the fault to a particular device or component.
- Isolate the rest of the network from the failure, where possible.

- Modify the network to bypass the failed component.
- Repair or replace the failed component to restore the network to its original state.

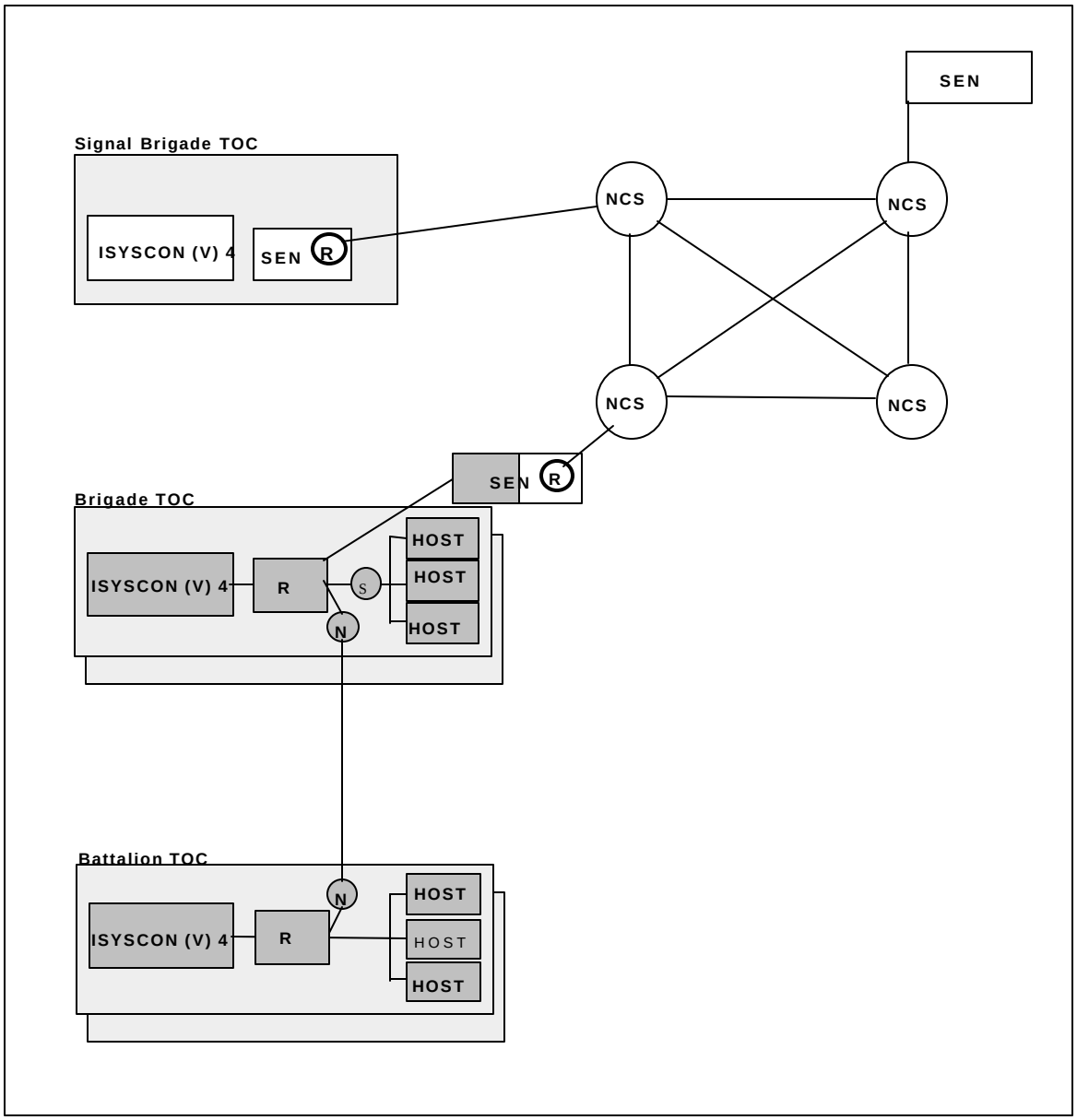

Figure 10-13. TOC Network Monitoring

10-105. Network monitoring also provides a level of performance management. Some performance issues that may concern a network manager include–

- The level of capacity utilization.
- Excessive/Moderate traffic flow.
- Unacceptable throughput levels.
- Bottlenecks/Increased response time.

10-106. Monitoring network performance provides an early indication of potential network problems that have not yet emerged. For example, if a battalion CSMA net (logical channel) is constantly 0 percent or 98 percent utilized, the most likely problems are getting traffic onto that network or a network overload condition, respectively. Table 10-4 lists the service-oriented and efficiency-oriented performances.

10-107. The service- and efficiency-oriented performance information gives the network manager access to information that allows for the troubleshooting and control of the network.

10-108. The paragraphs below discuss network monitoring for the various systems. The polling interval and data that gets polled is based on the bandwidth available and MIBs that are implemented.

Table 10-4. Service-Oriented and Efficiency Oriented Performances

Indicator	Definition
Service-Oriented Performance	
Availability	The percentage of time that a network system, a component, or an application is available for a user.
Response time	How long it takes for a response to appear as a user's terminal after a user action calls for it.
Accuracy	The percentage of time that no errors occur in the transmission and delivery of information.
Efficiency-Oriented Performance	
Throughput	The rate at which application-oriented events (transaction messages, file transfers) occur.
Utilization	The percentage of the theoretical capacity of a resource (transmission line, switch) that is being used.

SINCGARS SIP/ASIP

10-109. The SINCGARS SIP/ASIP radio has no explicit monitoring. In the voice mode, connectivity will either be established or not. If the voice communications are not established, the operator begins SINCGARS SIP/ASIP troubleshooting procedures such as increasing power, synchronizing time, and changing nets. However, an SNMP agent is located within the INC. The local host will have the ability to poll the INC using

SNMP, as necessary, to determine the local communications status on each port of the INC including both SINCGARS SIP/ASIP ports. The host's developer, not the ISYSCON (V)4, implements this SNMP query of the INC from the local host. However, the ISYSCON (V)4 will be able to perform SNMP queries on any SNMP-capable device in the network.

EPLRS

10-110. The NCS-E or ENM will monitor the EPLRS network. The ENM will be used in conjunction with the NCS-E until complete functionality is completed. At this time it will replace the NCS-E and be integrated into the ISYSCON (V)4. The capability will be inherent in the ISYSCON (V)4 COTS SNMP manager and that any scripts written under the ENM effort will be directly applicable as well.

10-111. The ENM tool, working through the SNMP agent or proxy in the radio, will utilize a local Ethernet LAN connection to the radio. SNMP queries to the local radio will be handled by the radio SNMP agent and returned to the polling management station. The RS will handle queries to remote EPLRS RSs by forwarding the encapsulated data across the EPLRS network using the inherent ability of the EPLRS network to route information. The remote agent will receive the query data, extract the data from the RS MIB, and return the response across the EPLRS network. The information is returned to the polling management terminal. Since SNMP polls originating from the management station require some degree of reliability, they would likely be transmitted via switched virtual circuits as a unicast message (this method is in-band).

10-112. Traps do not require the same degree of reliability (since the trap generator is not expecting a response from the management station) and will use the coordination net for transmission. By using the EPLRS coordination network, management actions are undertaken out-of-band and do not interfere with C2 and SA traffic flowing within the EPLRS network. Depending on the trap generated, the trap will be either forwarded to the local host or the ISYSCON (V)4. Interference with unicast C2 traffic is possible since FBCB2 unicast traffic will need to use the EPLRS coordination network to ARP link-layer addresses.

SATCOM

10-113. The GBS contains a standard SNMP MIB-2 agent within the RS. A COTS management system is used to manage the agent. Thus, the ISYSCON (V)4 can periodically poll the GBS receiver to determine its status and gather other SNMP information from the receiver.

10-114. The other SATCOM devices in the digitized division, SCAMP, Spitfire, and SMART-T are not SNMP-manageable. Therefore, the SATCOM controller monitors the network to infer network status using a unique RSID based on who is on the air. This SATCOM controller is not included as part of the ISYSCON (V)1 or (V)4.

TOC

10-115. The ISYSCON (V)4 will use standard SNMP and commercial network management for network monitoring. The network topology map viewed on the ISYSCON (V)4 screen will be created from the results of the planning process (device addresses, host addresses, and router and switch loopback addresses) and not from a discovery process. DNS information may also be useful to generate hosts on the network topology map. This map will consist of all managed objects containing SNMP agents, such as routers, Ethernet switches, wireless LANs, printers, and hosts.

10-116. The polling interval for devices is either reduced or turned off when TOCs jump. This change is to reduce the bandwidth associated with sending data over the WAN. Data exchange between echelons of ISYSCON (V) 4s or other network management systems is via an HTML web page. The rationale is that the LAN manager has responsibility for the TOC LAN elements. SNMP queries cannot be allowed to cross the WAN unless absolutely critical for an understanding of network status/performance. Instead, the upper level network managers, who are interested in the overall status, use the web page. Only TTPs and the LAN manager configuration prevent an upper layer manager from sending SNMP requests or receiving traps. Hosts within the TOC concerned with the network status only need a standard COTS web browser to obtain LAN status or host status.

10-117. Each managed object will be periodically polled to determine the network status. The polling interval is user-selectable and can last several seconds or several minutes. Given that the network devices are all located on the same LAN bandwidth, polling should not be a problem.

10-118. Remote monitor probes may be capable of supplying additional information, but their relative complexity compared to the utility provided within this simplified management model makes their use unnecessary for the initial digitization efforts.

10-119. For the ABCS hosts to be manageable, standard SNMP MIB-2 agents are required to be integrated into each host. No private or special MIBs are required to manage hosts in the TOC.

NTDR

10-120. Each NTDR is accessible over the air via in-band SNMP polls and can generate SNMP traps on events. Each radio must have a properly configured NMT access parameter. This parameter points to a file which contains authorized management station information (IP address, community string, and access type. If this file is not installed or if the information does not match that in the SNMP poll, the radio will not respond or generate the trap. Also, for traps, specific MIB parameters must be entered to enable the events upon which a trap will be generated (for example, NTDR SystemError and NTDR FirewallAlert).

10-121. Systems other than the NTDR NMT can be configured to generate polls to some or all radios on the network. A radio can be configured to send traps to a management station other than an NTDR NMT. However, since the NTDR sends traps to the first entry of the NMT access control table, only

a single management station can be the recipient of SNMP traps from any particular radio.

10-122. The NTDR NMT can use SNMP polls and traps to display an NTDR network topology. This topology is created from the planning information generated by the NTDR NMT. Icons representing each RS will appear on the screen. As radios return the SNMP polls or traps to the management terminal, the color changes indicating status will be generated.

NTDR

10-123. A different shape icon represents RSs that enter the NTDR network but were not planned by the local NTDR NMT. The NTDR NMT can shutdown all NTDR functions and zeroize keys with a single command. Flash memory is overwritten so recycling or examining the memory would not be productive.

SECURITY DEVICES

10-124. Monitoring for the TAC LAN INE will be through standard SNMP calls.

SBU USERS

10-125. An additional ISYSCON (V)4 is required to monitor the SBU portion of the LAN. Because of bandwidth constraints and SOS requirements, no network or host monitoring will take place on the engagement operations networks.

ABCS

10-126. The current ABCS network monitoring function consists of periodically polling the workstations within a TOC to gather the status of the network device (operational/nonoperational). Since ABCSs obtain their IP addresses from the DHCP server and host names via the C2R, each host will have to update the standard MIB-2 system group to include the sysDesc and/or sysName components. That associates the MIB/host with a particular user. When the MIB is updated, two means of distribution are possible. The first is to create and send a trap to the net management platform each time the system group is updated. The other is to periodically auto-discover the hosts for each subnet in the TOC. In either case, the ABCS hosts update the system group in the host agent using a standard SNMP put statement. Once the system group data is sent to the network manager, the sysDesc or sysName must be placed as the label for the managed object. The easiest approach is to auto-discover hosts for each subnet and use host names that were obtained from the C2R as the topology label. This assumes the role/workstation of the host can be derived from the host name that is selected.

FBCB2

10-127. The TI monitoring (TIM) portion of the FBCB2 will also be able to provide implied status monitoring of the EPLRS by rolling up information obtained within each TI-equipped platform on the battlefield. Because these resources are in-band, and bandwidth is severely limited in the present versions of the TI, FBCB2 monitoring should be of limited use for technical troubleshooting and reconfiguration. The effectiveness of the FBCB2 is highly coupled to the roll-up information propagated and the way this can be displayed on a screen.

10-128. The TI network monitoring concept for the FBCB2 provides for a bottom-up approach where the operator has the ability to constantly monitor, via local SNMP queries, the local network status. This includes–

- Radio status.
- Packets discarded.
- Queue size.
- Transmitted and received packet summaries.
- Server information.
- A top level SINCGARS SIP/ASIP communications display.

10-129. Using the periodicity of SA messages, the status at the local host for a specific community of interest can be derived. Figure 10-14 shows an example of local FBCB2 management.

10-130. At the higher levels, a neighbor host status can be obtained by requesting data from a specific hosts. Additionally, roll-up information is provided to the network manager for each echelon. This roll-up data will be exchanged with both the brigade and each battalion ISYSCON (V)4. SNMP queries for host and INC status may be used to collect empirical data on specific mission critical hosts such as the brigade commander's airborne platform Army Airspace Command and Control Element (A2C2S). The EPLRS SNMP status is being collected via the ENM. Given that SNMP resides on top of the user datagram protocol stack, excessive bandwidth should not be consumed. The network manager and select key personnel will have greater precision on select network elements and will primarily be implemented during training to allow the network to capture network characteristics prior to battle.

10-131. When vehicles exit one AS and enter another one, a mechanism is added to the INC to distribute exception addresses (those that fall outside the AS address space) to the border routers. This will only occur if hosts task organize across brigade boundaries and no time supports replanning into the new brigade. The network manager can utilize this information as data points to perform network troubleshooting and initialization. This information can only be used if it were available at key routers or a central router, and if modeling proved that there was a finite limit (~100) to the number of exception addresses that were allowed into the network without causing network degradation.

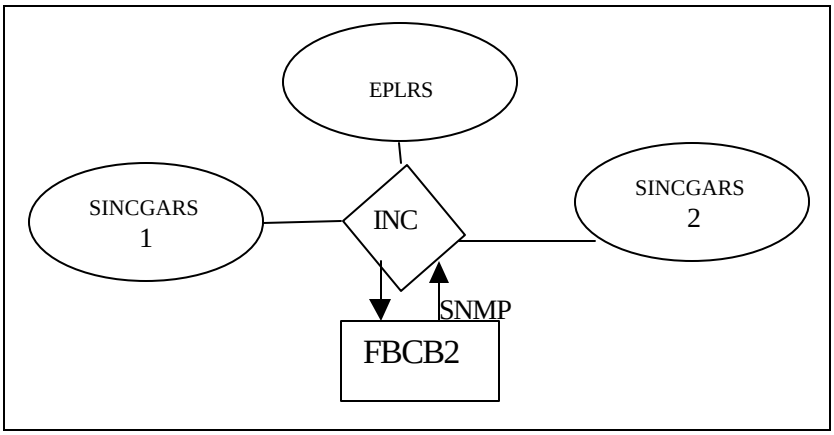

Figure 10-14. Example of Local FBCB2 Management

10-132. Figure 10-15 provides a summary of the TIM functionality. Each FBCB2 host has the same capability including both a TIM and a TIC. However, by using the implicit network status data of the FBCB2 monitor and the empirical out-of-band network monitoring of the ENM, the network manager should have a good representation on the network status.

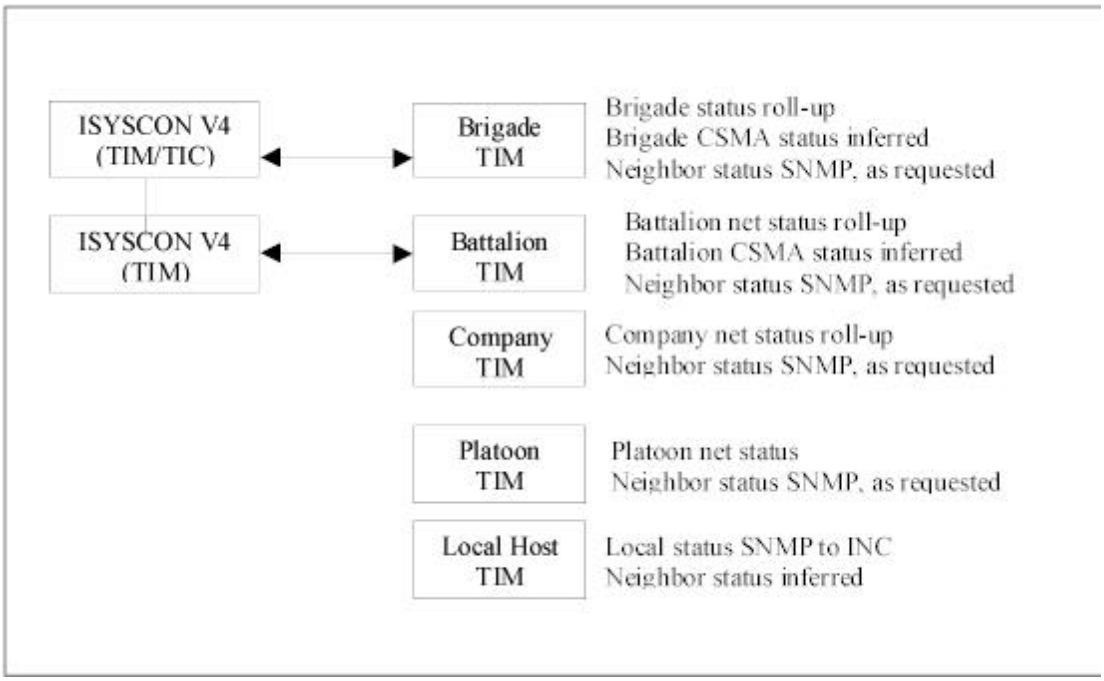

Figure 10-15. TI Monitoring Functionality

NETWORK TROUBLESHOOTING/RECONFIGURATION

10-133. To maintain proper operation of a complex network, the network manager must ensure that the system as a whole and each component is correctly operating. When the monitoring process detects a hardware performance error, the S6 can begin the troubleshooting or fault management process. For the purposes of this document, the terms troubleshooting and fault management will be used interchangeably. The fault management process includes–

- Identifying the exact location of the faulty device to the card level, where possible.
- Providing a work around to by-pass the failure without further interruption of service.
- Reconfiguring and modifying the network to lessen the impact of the failed component.
- Repairing and/or replacing the failed component to return the network to its original state

10-134. Fault management consists of three phases:

- Fault detection — faults can be detected by either monitoring the error report generation (traps) or lack of poll response.
- Fault diagnosis — faults are diagnosed by implementing diagnostics on a component (managed object) by:
  - Reproducing the error.
  - Analyzing the error.
  - Receiving reports from the managed objects.
- Fault correction — fault correction is accomplished using other facilities such as configuration management.

10-135. The network manager needs to differentiate faults from errors. An error is a single event, albeit a recurring event. However, a fault is an abnormal condition requiring the attention of the network manager. An exceptionally high error rate, or a failure to operate correctly, if at all, indicates that a fault has occurred. For example, an unterminated LAN cable will not allow any data onto the network, whereas a faulty terminator, one not providing the correct resistance, may allow traffic onto the network but with a high error rate. The network manager troubleshoots the network to isolate and resolve the faults. To aid the network manager in fault management, several troubleshooting tools have been identified. These tools include–

- Serial port loopback connectors/test software for hosts.
- Fiber optic cable tester/protocol analyzer/network diagnostics (10/100 Based T and 10/100 Based 2).
- Miscellaneous components (T and barrel connectors, terminators, cable, and small hub).

10-136. Operating troubleshooting tools, fault isolation, diagnosis, and correction must be included as part of the network manager training process and included in the appropriate systems manuals.

10-137. Occasionally, the network components will require reconfiguration. The reconfiguration may be planned and unplanned. In the planned reconfiguration, the S6 is aware of the potential configuration change based on commander's desires to fight, and the user prescribes the changes in garrison or a staging area prior to mission execution. In this case, the network manager or TOC server operator re-initializes the devices with the new configuration. In an unplanned reconfiguration, the planning process is revisited in the tactical environment. The communications should already be established so the new configuration information can be distributed via the network. Also, a network is in place, therefore, the reconfiguration process should effect parts of the network rather than the entire network. On rare occasions the entire existing network will require reconfiguration.

SINCGARS SIP/ASIP

10-138. The operator can troubleshoot the SINCGARS SIP/ASIP on a limited basis. The operator checks the RF cables, handset, and receiver/transmitter (RT) to power amplifier (PA)) for damage and correct connectivity IAW the appropriate technical manual. The operator must ensure that the net ID, time, Julian date, and COMSEC are the same as the other subscribers in the net. If the radio continues to be inoperative, exchange the radio with a known good unit to isolate the fault to the vehicle mount or the R/T. Refer to the SINCGARS SIP/ASIP operators' manuals for more information on troubleshooting.

10-139. If the voice is operating correctly and data is not being transmitted onto the SINCGARS SIP/ASIP net, voice communications should be established to ensure the SINCGARS SIP/ASIP radio is communicating correctly. If voice connectivity is established, then the cables from the host to the INC and from the INC to the SINCGARS SIP/ASIP should be checked for damage and proper connectivity. Next, the INC should be re-initialized from the host. If all user level checks are performed and the system continues to work below expected performance levels, contact S6 personnel.

10-140. From the reconfiguration standpoint, the COMSEC fill and net IDs must be changed to another preloaded net ID or re-filled with a new net ID and COMSEC fill when the user changes to another SINCGARS SIP/ASIP net. For example, if a battalion is task organized to another brigade, the platoon and company nets will remain. However, those users participating on the brigade command or operations and intelligence nets may require new net IDs and COMSEC keys loaded into the SINCGARS SIP/ASIP.

EPLRS

10-141. EPLRS troubleshooting consists of ensuring that the radio is cabled correctly and that the correct COMSEC fill is loaded. The NCS-E accomplishes much of the troubleshooting by changing settings and logical channels in the RS, assuming the NCS-E can reliably reach the RS that needs to be changed.

10-142. From the reconfiguration standpoint, once an RS has been designated for reconfiguration, the NCS-E or ENM can set the new parameters such as a new CSMA logical channel. The FBCB2 will load the INC with a proper

router configuration. Within a brigade area, the EPLRS can roam and remain a part of the CSMA RA that is based on the unit organization rather than geographic location. On the other hand, the EPLRS will likely require a re-key when it gets task organized into a different brigade.

SATCOM

10-143. Troubleshooting is limited to voice connectivity and the controller since there is no SNMP monitoring in the SATCOM terminals. A verification of the planned parameters (including ephemeris data, TRANSEC, and COMSEC settings) and other parameters that were manually or automatically entered into the terminal can be checked. All other troubleshooting will be provided IAW the appropriate technical manuals for each terminal.

10-144. For MILSTAR, and maybe the other SATCOM terminals, OTAR is available. OTAR advantages include reducing hard-copy key requirements, allowing crypto rollover without operator intervention, and providing a quick and effective recovery from compromise. For OTAR of both COMSEC and TRANSEC to be effective, a chaining key (key encryption key [KEK]) must be loaded onto the terminal.

TOC

10-145. Once the network manager has detected outages on any part of the TOC LAN or experiences performance problems (sluggish performance, high collision rates, or dropped packets in the network), he can begin maintenance. If an outage occurs, the manager can open a trouble ticket and dispatch repairmen to resolve the problems within the TOC or to arrange a meeting with the jump portion of the TOC. In the reconfiguration of network devices (such as switches and routers), the network manager will be provided with a small hand held device such as a mini notebook computer or personal digital assistant. The notebook is used to store and load router configurations via a command-line interface from the console port on the device. During sluggish performance, the network manager may be able to increase performance by adjusting network or messaging parameters, to include–

- Modifying protocol distribution rules (BVTC, whiteboarding).
- Modifying EPLRS needlines (MSG, PVCs).
- Modifying/Enhancing networking parameters (TCP/IP time to live parameters).
- Manually configuring changes from the command line based on TTP and manuals/users guides.
- Running network replanning models based on all possible combinations with organic units, so that completed and modeled templates do not require extensive modifications at inopportune times.

10-146. Other than minimizing the risk through preplanning, the planning process described above needs to be performed for major changes.

NAME SERVICES

10-147. The DHCP server must be updated when the pool of addresses is exhausted and needs changing and when hosts with static addresses must be updated or changed. The desire is to require as few updates as possible to the DHCP server while in the field. Most of the planning process should take place in garrison and should not require frequent updates during mission execution.

NTDR

10-148. No specific troubleshooting tools are provided with the NTDR NMT other than those inherent in the functioning of the implemented SNMP MIB variables.

SECURITY DEVICES

10-149. No specific troubleshooting tools are provided to the INE or firewalls other than those inherent in the functioning of the implemented SNMP MIB variables.

SBU USERS

10-150. No specific troubleshooting tools are provided to the SBU community other than those inherent in the functioning of the implemented SNMP MIB variables. An SNMP tool is used in troubleshooting on the unclassified side of the network.

ABCS

10-151. No specific troubleshooting tools are provided for the ABCS other than those inherent in the functioning of the implemented SNMP MIB variables.

FBCB2

10-152. The S6 begins maintenance when he detects outages that cannot be repaired by the individual user (check cables, check power, reboot, reload INC, or performance problems–sluggish performance and dropped packets in the network). If an outage occurs, the S6 personnel can request assistance or a contact team from a higher echelon. During sluggish performance, the network manager may be able to increase performance by adjusting network or messaging parameters, to include–

- Changing SA reporting parameters.
- Modifying message distribution rules (acknowledgments, frequency of retries).
- Modifying EPLRS needlines (MSG, CSMA).
- Modifying/Enhancing networking parameters (time to live).

10-153. Run network replanning models based on current or perceived task organization.