Disconnected, Intermittent, Limited (DIL) Communications Management Technical Pattern

Alias: Disadvantaged Communications Technical Pattern
Alias: Disconnected, Intermittent, Limited (DIL) Communications Technical Pattern

Jerry Sonnenberg, Harris Corporation

1 December 2009

Version History

Version Number	Description	Author
V0.1-2009-03-09 (Draft)	This is the original documentation for this pattern. This pattern was introduced at the February 2009 Plenary meeting of the Services WG	Jerry Sonnenberg
V1.0-2009-05-27	Updated for standard format, additional detail	Jerry Sonnenberg
V1.1	Updated to conform to NSD-RM Appendix A 1.7 format	Jerry Sonnenberg
V 1.2-2009-09-15	Add additional references to related patterns	Jerry Sonnenberg
V 1.3 2009-11-19	Add material to address formal review CRs	Jerry Sonnenberg
V 1.0 2009-12-01	Incorporate approved changes from formal review: including name change to *DIL Communications Management Technical Pattern*	Jerry Sonnenberg

Abstract

The DIL Communications Management Technical Pattern describes how a network of connected links with variable link capacity operates to maintain communications service and situational awareness. This pattern describes technology-independent logic for adjusting the capacity of links in a DIL environment. The Pattern describes supporting features required at several protocol layers.

Table of Contents

List of Figures

List of Tables

1 Description

This pattern describes how to adjust the capacity of links in a disconnected, intermittent, or limited (DIL) environment. Tactical and commercial mission-critical networks can have disruptions that cause a significant drop in the aggregate data throughput of the network. Heterogeneous links in a DIL environment are often managed by technology-specific element management logic that can be unaware of the overall mesh network. This pattern describes technology-independent logic for adjusting the capacity of links in a DIL environment.

1.1 Problem Statement and Context

1.1.1 Problem Statement

A major interoperability problem in the deployment of heterogeneous networks is the coordination of the capacity allocation algorithms associated with, or embedded in, the control of each type of network device. Capacity allocation is an essential underpinning for the proper operation of network-centric services.

In the wired Internet, capacity allocation is often managed by a single management solution since the underlying technology can be quite homogeneous. For example, the Open Shortest Path First (OSPF) routing protocol or the Enhanced Interior Gateway Routing Protocol (EIGRP) can determine an optimal mesh of landline links that can range from moderate (1.5 Mbps), to high (100 Mbps – 1 Gbps), to very high (10 Gbps) rates. This mesh typically includes many redundant links that can quickly be employed to support net-centric services by invoking capacity management protocols at the link layer (e.g., Spanning Tree Protocol – IEEE Standard 802.1D) or at the network layer (e.g., OSPF – IETF RFC 2328).

In tactical wireless environments, the luxury of link over-provisioning typically does not exist. There are both technical and strategic reasons for limiting the number of links, and the wireless links themselves are subject to environmental (atmospheric, foliage, jamming) effects that are not as prevalent in the wired Internet.

So these links can become disconnected when radio frequency (RF) or free space optical (FSO transmission is blocked, intermittent when connections wax and wane, or limited when the waveform can change physical layer features such as modulation technique (bits per hertz) to maintain connection in poor conditions, but at a lower bit rate.

Capacity allocation for satellite communications paths typically has been done using Demand-Assigned Multiple Access (DAMA) and its variants. A DAMA network takes a single 25-kHz channel and breaks it up into a time division multiple access format that allows a number of users onto a single channel simultaneously. Terrestrial line-of-sight (LOS) wireless links have a number of link layer (media-access-control [MAC]) or network layer algorithms that can be used for capacity management. It is imperative that the capacity allocation for all the wired and wireless components in a services-based network be performed according to the same technical pattern. In this way, the constituent element management algorithms will work in cohesion and not inadvertently cancel or contradict each other.

1.1.2 Context

Most networks need to continue to provide the data transfer capacity that supports network services even when disruptions cause a significant drop in the aggregate data throughput of the network. Rather than just terminating an arbitrary number of service-level agreements (SLAs), a robust network implementation should attempt to determine the criticality of supported services and provide a degraded level of service that still transfers the mission-critical data.

Both wireline and wireless network links can become disconnected for a variety of reasons. A wireline link can be cut by accident or by malicious intruders. Hackers can cause wireline and wireless links to lose capacity. Wireless links can be affected by the physical environment (such as atmosphere, rain fade, and movement under a canopy of foliage, just to name a few). Tactical wireless links can be shut down by policy when they otherwise would radiate in a zone that a commander wishes to be emission silent. Such links can be intermittent when the intervening physics causes variations in signal strength.

Dynamically adaptable radios can often change modulation order at the physical layer to provide a limited data capacity even in very poor operating environments.

Operational patterns in which a robust method of dealing with DIL events would provide a better network-centric service include:

- Critical Financial Transfer[1]
- Comm Support to Secure Tactical Operating Area

The Comm Support to Secure Tactical Operating Area Operational Pattern might invoke the Call For Fire (CFF) Capability Pattern.

The CFF Capability Pattern that uses the DIL Communications Management Technical Pattern is described in Section 4.

This technical pattern addresses the sequence of actions that takes place in many network environments when DIL links are used. Often, these actions are manual. The goal of a network-centric operations pattern is to capture these sequences of actions into patterns for codification and reuse.

1.2 Participants

Figure 1 is a systems modeling language (SysML) block definition diagram that illustrates the participants in the CFF Use Case and the DIL Communications Management Technical Pattern. The example CFF Use Case in Figure 2 illustrates a sample user set for the DIL Communications Management Technical Pattern.

[1] These example Operational Patterns are not in the NCOIC pattern track horizon, but are given here as examples that could use DIL.

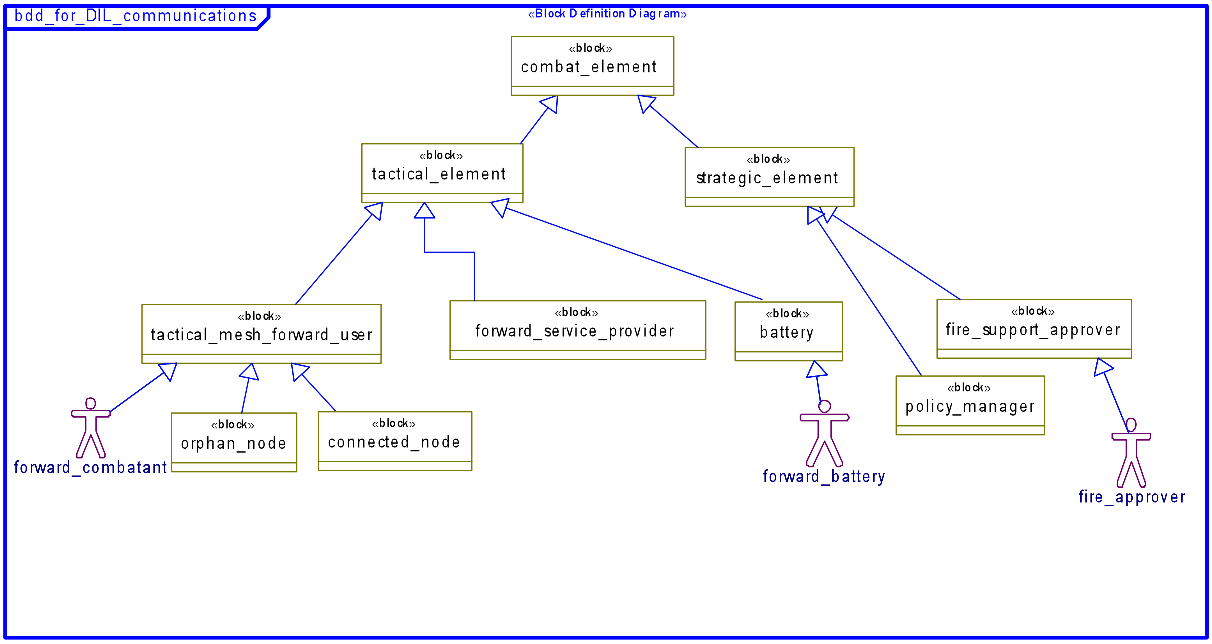

Figure 1. DIL Communications Participants
Source: NCOIC

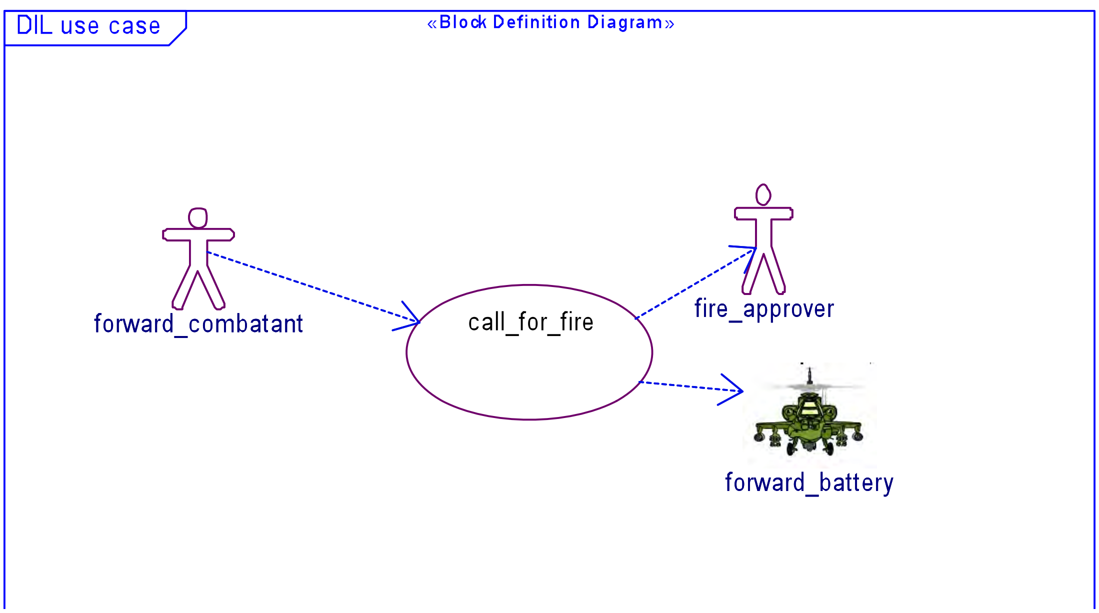

Figure 1-2. Call For Fire Use Case
Source: NCOIC

The essential participants of the DIL Communications Management Technical Pattern are as follows:

- Tactical mesh member communications nodes.
- Policy-based bandwidth manager.
- Tactical mesh communications nodes placed in a critical path by operational events.

- Tactical mesh members maintaining membership in the tactical mesh (providing capacity to and from the mesh and the policy based bandwidth manager).

Other model elements are used to support and describe the DIL pattern. The sequence of communications among these members is illustrated in Section 1.5, Figure 6.

1.2.1 Actors

Note that actor names with underscores refer to SysML entities.

forward_combatant: A user of the tactical mesh requiring critical services in a DIL communications environment.

fire_approver: A Call For Fire use case member who must receive and respond to critical service requests in a DIL communications environment.

forward_battery: A Call For Fire use case member who must react within a given time frame in a DIL communications environment.

Net-Centric Environment: communications_mesh_element (critical): A tactical mesh element that supports collaboration among systems, users, services, and service providers, and must use services in a timely manner.

Net-Centric Environment: communications_mesh_element (noncritical): A tactical mesh element that supports collaboration among systems, users, services, and service providers This element must use services in a manner that is time dependent on the state of the mesh and may be reconfigured to allow transfer (reuse by other critical mesh elements) of network resources.

1.2.2 Interfaces

Interfaces reference the SysML elements in the diagrams in Section 1.4, Structure. The major static interface is between the communications mesh element (CME) and the policy manager (PM). Section 3.1 describes the requirements for interaction across the CME-PM interface.

1.3 Pre-Conditions

This pattern is based on the following assumptions:

- The network incorporates (or has the potential to incorporate) heterogeneous link-level technologies, each with its legacy methods of managing data-link capacity.
- The Operational and Capability patterns that depend on robust network communications are not required to be aware of the addition of new, heterogeneous components to the underlying communications mesh.
- Different legacy communications systems will have varying ability to adjust capacity in a coordinated fashion. However, each legacy system should be configured to the extent possible with the DIL Communications Management Technical Pattern in mind.

The network elements have reconfiguration capabilities tied to individual element managers or even specific protocols. Each element manager is directed by the overarching policy-based network manager for the target heterogeneous network. Policy-based management is discussed in the NCOIC Net-Centric System Management Framework (NCSysMF), currently in development.

Figure 3 illustrates the recurring problem addressed by DIL.

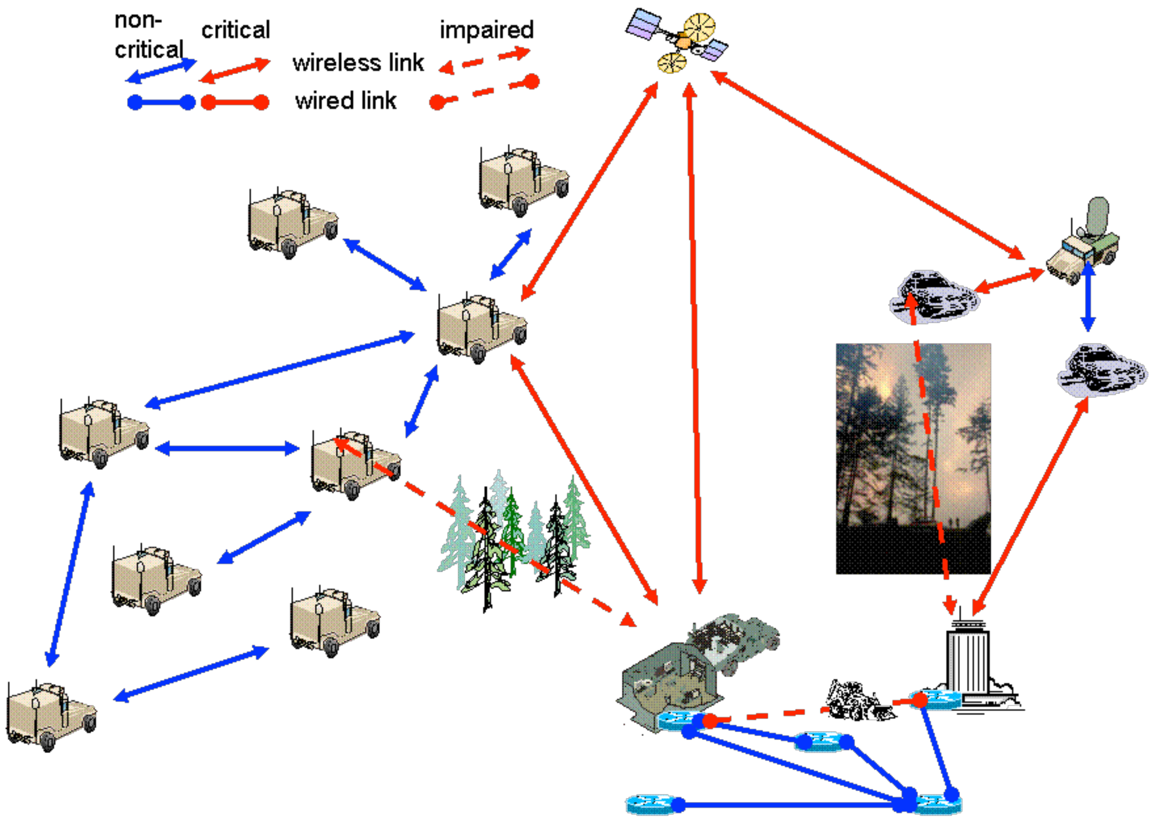

Figure 3. Heterogeneous link technologies brought together in a common mission use link-specific management techniques for communications capacity management. Source: NCOIC

The wireline, terrestrial wireless, and satellite communications components of a tactical or emergency response mission can react to loss of coverage events (natural disaster, foliage blockage, backhoe damage) in synchronization only if the logic controlling the communication capacity management adheres to a common policy. The NCOIC Legacy Services Pattern states:

> "The network adapted parts of the system in focus should have as few as possible dependencies to the actual legacy system to allow for independent life cycles for these two parts of the system."

1.4 Structure

Figure 4 shows the structure of the participants in the DIL Communications Management Technical Pattern.

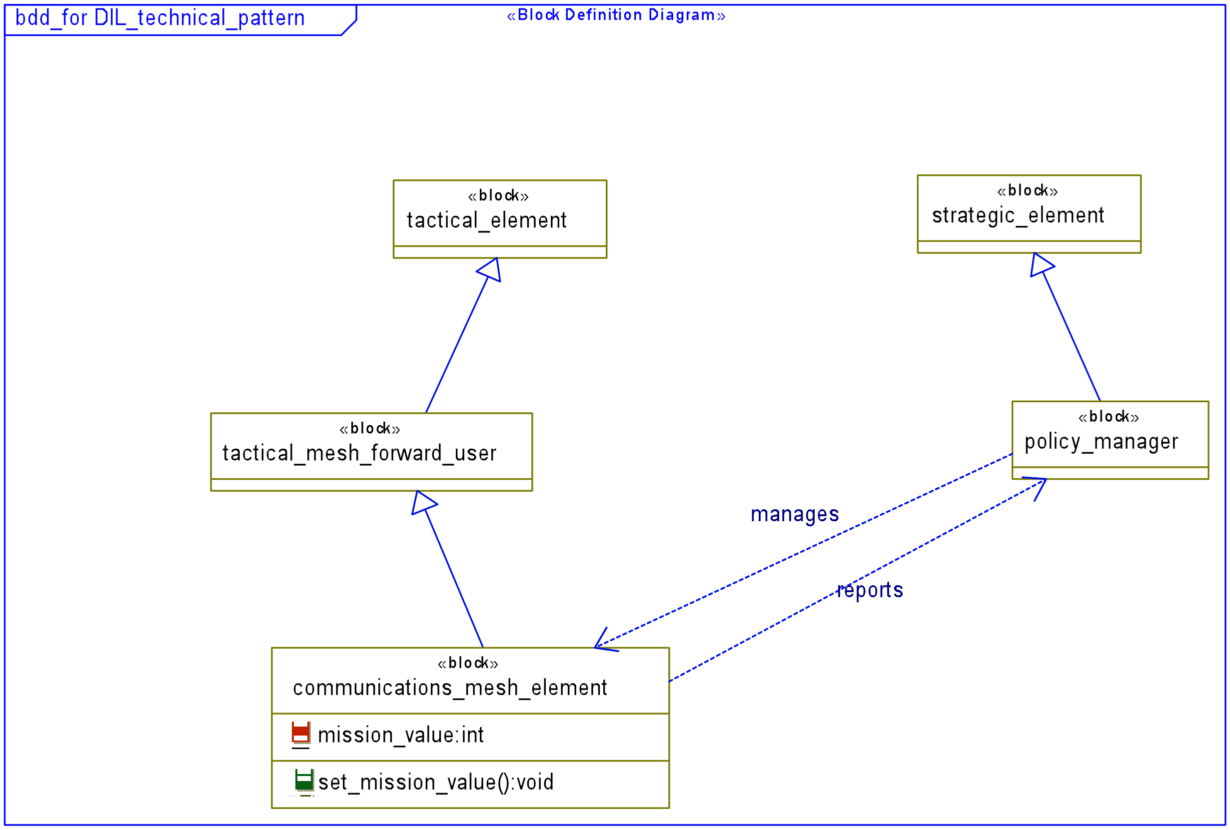

Figure 4. DIL Communications Management Technical Pattern Participants
Source: NCOIC

Communications nodes are deemed to be critical once their continued operation is needed to support mission critical communications and they provide events required for mission critical processing and action determination.

1.5 Behavior

During the course of operations, communications nodes play many roles. Once an Operational or a Capability pattern has progressed to a state of operations that includes mission-critical communications and processing, some of the communications nodes supporting the network-centric operations become critical.

Figure 5 illustrates an activity diagram for the DIL Communications Management Technical Pattern.

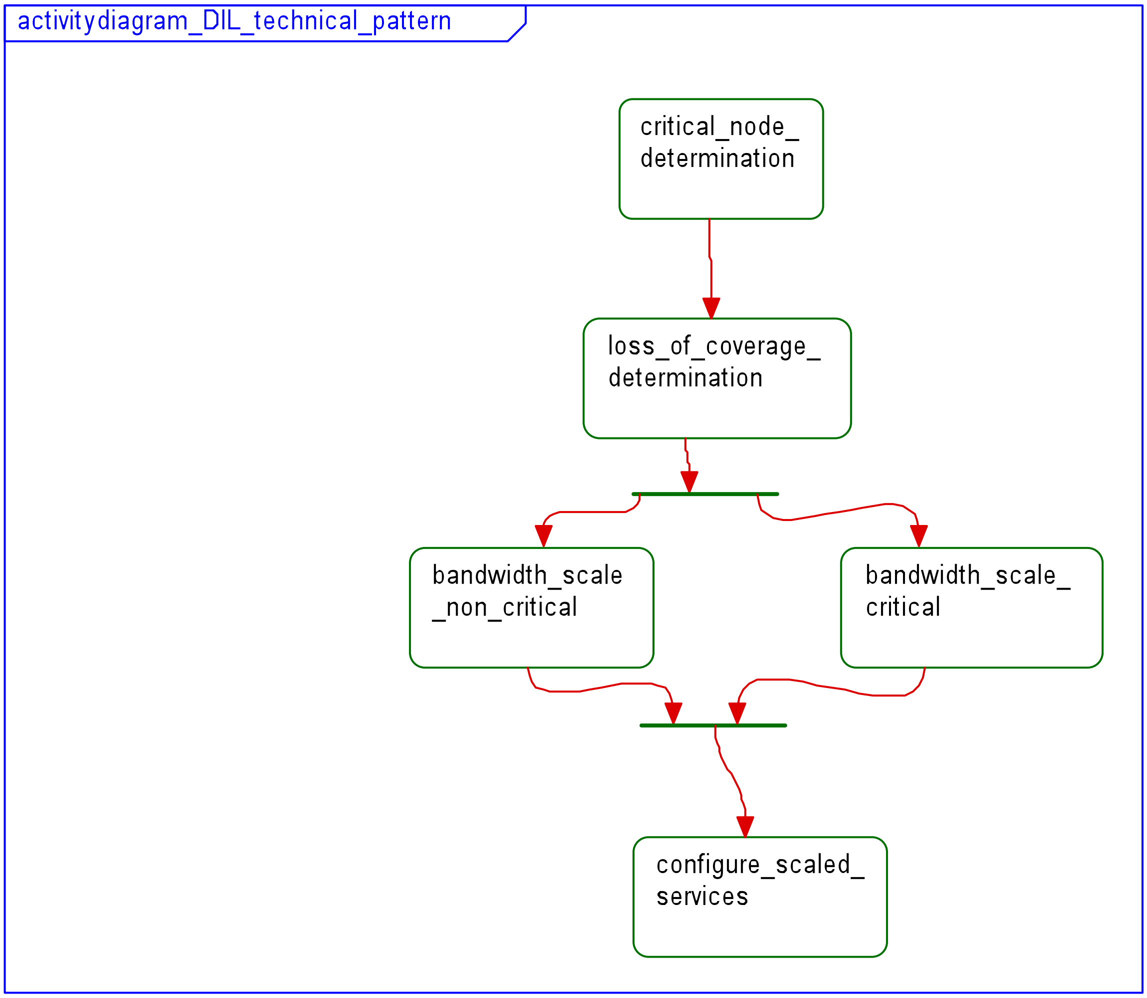

Figure 5. DIL Communication Activity Diagram
Source: NCOIC

When asynchronous network events cause the capacity of any link in the mesh to be diminished, the events are forwarded to the policy-based bandwidth manager.

The PM determines which nodes are essential to continued mission-critical operations. The policy logic and associated actions can be automatic, protocol-based, computer communications actions or they can be (and currently typically are) human-based and distributed over the geographical range of the meshed nodes. In some cases, the capacity allocation "logic" consists of parameter tables set up inside each of the associating nodes (routers, satellite access terminals, or general-purpose processors used with communications equipment that have a specific rule set installed for capacity allocation).

Once the critical nodes are identified, analysis is performed to see which critical services can be maintained. As mentioned before, robust network implementations should attempt to determine the criticality of supported services and provide a degraded level of service that still transfers the mission-critical data.

Figure 6[2] illustrates a sequence diagram for the DIL Communications Management Technical Pattern.

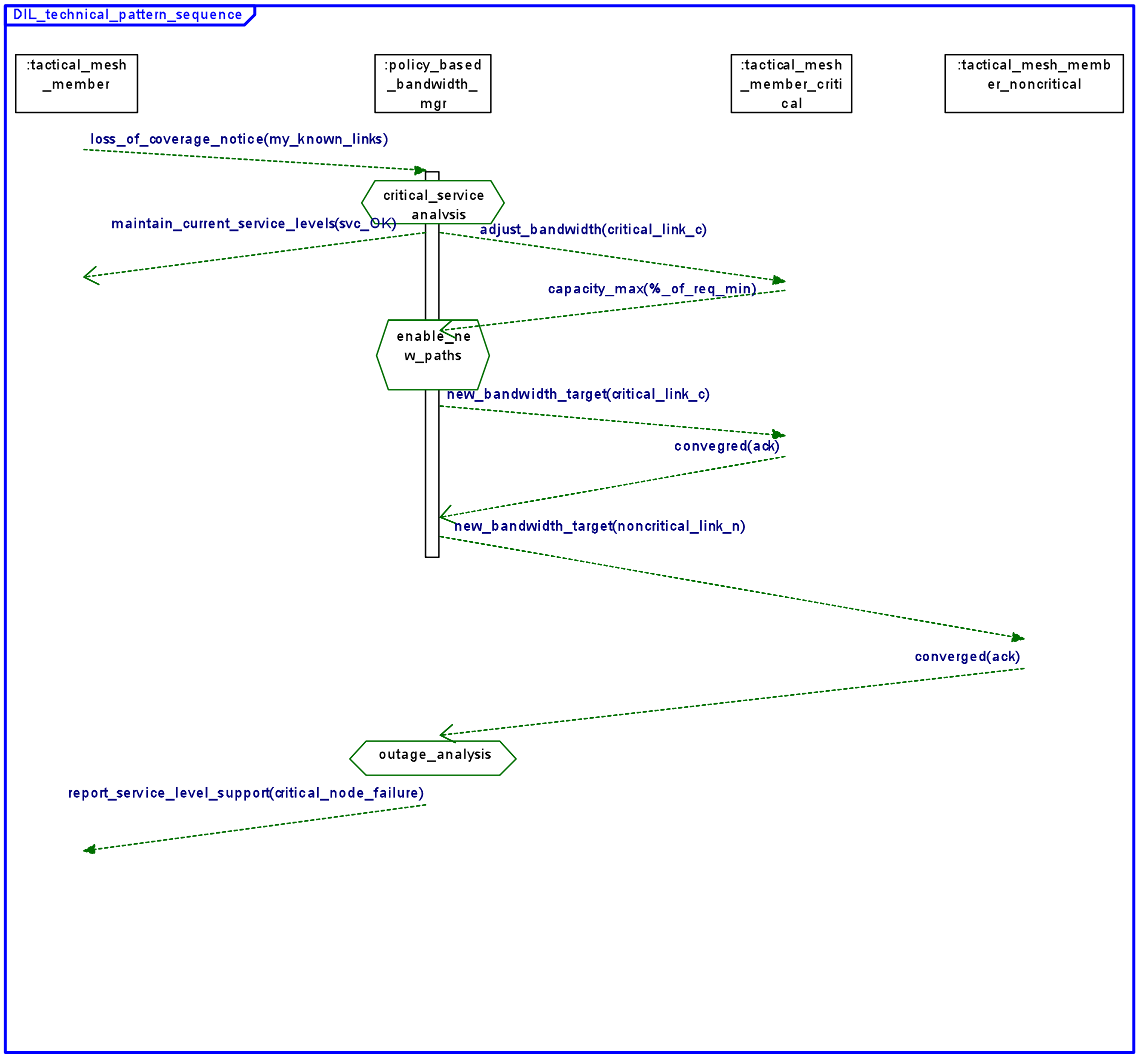

Figure 6. DIL Communications Management Sequence Diagram
Source: NCOIC

Each flow in Figure 6 is a stereotype of the many flows between the policy manager and the communications mesh nodes (critical and noncritical). In the case where the incoming event(s) do not lower the mesh capacity below the critically needed threshold, the node raising the event is responded to with a message to maintain current service levels.

The set of critical links (c_i) is informed of new bandwidth requirements by the PM and each responds with the percentage amount of that capacity that can be supported. The PM determines

[2] The security aspects of the information exchanges between nodes and the policy based bandwidth manager are not illustrated in this figure, but are, of course, part of any implementation of this pattern. Please refer to the Net-Centric Information Assurance Framework (under development by NCOIC) for the security exchange considerations of this sequence diagram

if new paths are required and invokes the physical, link, and network layer protocols to create a new mesh that will support mission-critical operations. In instances where the mission criticality can be measured in seconds rather than minutes, it is incumbent that the analysis and enabling logic be computer based.

The set of noncritical links (n_j) is informed of its new capacity assignments. For example, should a MAC-layer protocol divide capacity via time division multiple access (TDMA) or frequency division multiple access (FDMA) techniques, and the assignment of time slots or frequencies can be done dynamically, then the noncritical nodes can be set to use less total capacity if such capacity can be given to the now-critical links.

Both critical and noncritical nodes report the reconvergence of the network. Convergence has a specific meaning in the layer 3 network protocols common in the Internet. However, in this context, the convergence acknowledgement is the superset of all the mesh node responses that tell the network manager (central or distributed, human or computer) that the mesh of links supporting DIL Communications Management has settled to a new state (before the next event).

1.6 Post-Conditions

This section describes, on a high level, if and how the identified problems can be solved using the proposed solutions.

In general, network-centric services are agnostic to the underlying physical implementation. The level of service that a network of nodes can provide to an application has been treated at length in packet Quality of Service (QoS) discussions in the general Internet QoS discussions. At the time of release of this document, there are no current NCOIC patterns illustrating QoS.

However, when a mesh of nodes carrying mission-critical traffic fails to provide even the highest priority of QoS category because of link failure(s), the DIL Communications Management Technical Pattern is used to reconfigure capacity at whatever protocol level is required to ensure mission success. The fact that such reconfiguration historically has been manual, ad hoc and beyond the description of QoS for Internet Protocol (IP) packets does not negate its existence. The pattern still exists, perhaps only in the rules and procedures of a communications support team.

The key to using the DIL Communications Management Technical Pattern is to use it consistently across the multiple control capabilities within a heterogeneous network. The post-condition for its use is to have continued operations in a DIL Communications environment. Another post-condition example is shown in Section 2.2.3.4 wherein the use of DIL Communications bandwidth management enhances the overall application availability.

2 Implementation Guidance

2.1 Standards

To achieve full interoperability, all of the standards listed in Table 1 are required for the DIL Communications Management Technical Pattern. Table 2 refers to standards that are not yet considered mandatory, but may become mandatory in the future. Future revisions of this pattern may require their use, at which time they will be promoted to Table 1.

Table 1. Mandatory Standards

Standard	Name and Number	Purpose	Notes
OSPFv2	IETF RFC 2328 (STD:54)	link state advertising on DIL links	When using IP technology
OSPF Traffic Engineering	IETF RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2	traffic engineering to utilize DIL links	When using IP technology
IEEE 802.1D	Spanning Tree Protocol	link layer weighting of DIL links	When using COTS bridges
DAMA (MIL-STD-188-181)	181C - Interoperability Standard for Access to 5-kHz and 25-kHz UHF Satellite Communications Channels	DAMA	When using UHF satellite communications technology
DAMA Control (MIL-STD-188-185)	185 - Interoperability UHF Milsatcom Dama Control System	DAMA control of DIL SATCOM links	When using UHF satellite communications technology

Table 2. Optional Standards

Standard	Purpose	Notes
OSPF MANET Extensions	Extensions to OSPF to support mobile ad hoc networking draft-ietf-ospf-manet-or-01	
OSPF MPR	OSPF multipoint relay (MPR) extension for ad hoc networks	

2.2 Expert Advice

2.2.1 Guidance to Implementation Developer

Experience has shown that for best results, the implementation developer should:

- Minimize the necessary modifications of the existing parts of the legacy systems.
- Create a schema that defines network physical resources (time slots, frequencies, codes) that can be managed by common logic and rule sets.

2.2.2 Data Exchange

Data exchange for the DIL Communications Management Technical Pattern is illustrated in the sequence diagram in Figure 6.

Actions are initiated by tactical mesh members when they send a loss of coverage notice to the policy-based bandwidth manager. These notices indicate the list of known links to which a mesh member can transmit. Mesh members send this notice when the list of mesh peers changes.

After the policy-based bandwidth manager conducts a critical service analysis[3], it can send out one or both of the following messages: a note to the initiating mesh member to maintain current connection levels and a note to each of the set of critical nodes to adjust bandwidth on

[3] Note that the loss_of_coverage_notice in Figure 6 can trigger the critical-service analysis. The DIL pattern does not mandate a specific event format or even whether or not the service analysis is centralized or distributed across the meshed members of a policy-based bandwidth manager, only that such analysis occurs. While not shown in Figure 6, continuing change of coverage events can occur that would allow a link to be restored to its original coverage state. Policy within a building block implementation of the DIL pattern for a specific element set would determine whether or not the mesh elements return to a preset allocation or remain as converged until another loss_of_coverage_notice occurs.

one or more of its links, which are considered critical in a DIL environment. This may be in the form of one message to each critical node for each critical link or a single message to each critical node with a list of critical links. At this point, each tactical mesh member is considered either critical or noncritical.

Critical links respond to the policy-based bandwidth manager with a notice detailing the capacity that can be applied to each of its critical links, given the new determination of critical and noncritical nodes.

Given the responses from the critical nodes, the bandwidth manager will enable new paths. The implementation details of this enablement may involve protocols at several layers of the open systems interconnection (OSI) protocol stack – link and network being the most likely.

The policy-based bandwidth manager then sends a message to each critical node with a new bandwidth target for each critical link. Once the critical node has reconfigured its frequency/time or code capacities to accommodate the maximum (up to the bandwidth manager's request) data capacity per link, it responds to the manager with this new capacity allocation data.

The bandwidth manager then informs each noncritical node of its remaining capacity (use of frequency, time slot, or code assets). Each noncritical node responds to the bandwidth manager with a converged capacity acknowledgement. The policy-based bandwidth manager performs an outage analysis based on the reconfigurations conducted as a result of the initial loss-of-coverage event and sends the initiating node a service-level support failure notice if there is a critical node failure that cannot be reprovisioned.

2.2.3 Lessons Learned

2.2.3.1 DAMA

Current military satellite-based networks allocate physical layer resources to users based on predetermined requirements. The access methods employed are fixed access and DAMA. The allocation unit, or slot, is either a particular frequency in FDMA or a time interval in TDMA. In fixed access, slots are statically assigned based on requirements and are, like the time slots in traditional commercial circuit switches, lost capacity when not used by the assignee.

In DAMA, slots are allocated according to requests on an order wire. Allocation of slots from the current pool of resources is made in real time. User-priority-based scheduling schemes have been proposed for DAMA, but only consider local information. Next-generation satellite systems will attempt to incorporate network-wide (global) information into the physical layer dynamic resource allocation schemes.

The dynamic access and allocation of resources that are implemented as an instantiation of the DIL Communications Management Technical Pattern should be aware of the following conditions:

- Available bandwidth and power capacity of the satellite transponder.
- Available user terminal capacity.
- Network-wide priority of supported users.
- Criticality of the application data being transported.

Continuous monitoring of the status of the transponder and user terminal assets, RF, and power-measuring activities and bit error rate (BER) calculation are key to performing DIL Communications when satellite links are part of the heterogeneous mesh.

2.2.3.2 Internet

Routing protocols such as OSPF use link state advertisements (LSAs) from a router to its peers across links to advertise its local part of the routing domain. LSAs advertising point-to-point links [LS type 1] or network segments (broadcast or nonbroadcast, multiple access) [LS type 2] have been augmented by optional protocol extensions with additional LS types. When Type of Service (TOS)-based routing was introduced, operation typically assumed that all routers within a routing domain were capable of routing based on the TOS (T-bit) option.

In a heterogeneous network, it is more likely that certain routers support TOS and others do not. OSPF routers are not required to store or forward LSAs with an unrecognized LS type. Implementing the logic described here as DIL Communications has depended on full support of TOS-based routing in OSPF. Likewise, any DIL Communications Management Technical Pattern instantiations must be aware of the mix of resource allocation entities in the heterogeneous network and will work only when a critical mass of those entities support the policy-based management inherent in this pattern.

2.2.3.3 Dynamic Line-of-Sight Wireless

Current generation mobile tactical radios provide an IP-based network, with links capable of supporting voice-over Internet Protocol (VoIP); video; and command, control, communications, computers, and intelligence (C4I) services. The radios work equally well fully mobile or fixed. The radios automatically link with others located in LOS. Using a directive-beam antenna, adaptive LOS radios can automatically create the entire network using only a single frequency. A directive beam also permits simultaneous use of the same frequency and time slots between nodes not in each other's RF path.

As the nodes in a mobile network move, temporary blocks to LOS links are automatically routed around. When LOS is obtained, connectivity is reestablished and the "orphan" node automatically rejoins the network.

The radios autonomously negotiate among themselves the allocated time and data rates to pass traffic. Radios can discover and establish direct wireless links with a set of neighbors that are in view. Radios associate with neighbors' neighbors and keep track of their locations, facilitating connectivity among nodes where LOS may not exist.

In addition to allowing time-slot reuse within a single frequency, directive-beam technology extends range and improves throughput. Directive antennas also provide inherent low probability of intercept and low probability of detection (LPI/LPD) capability.

LOS radios with a software communications architecture (SCA)-compliant waveform in the Joint Program Executive Office (JPEO)/Joint Test and Evaluation Lab (JTEL) library and certification will enable reuse. Current LOS radios are designed to reduce crew sizes and training requirements by operating with a policy-driven control interface. The radio waveform is designed to boot from an initial startup configuration defined by the user. Once booted, an external controller can redefine the operational states of the waveform within the radio. For example, management logic can restrict (or permit) the spectral bandwidth, modulation type, power level, data rates, number of permissible links, or other controllable parameters given the current battlefield scenario. Control is achieved via an SCA-compliant interface to an external radio manager function. The radio then operates autonomously within these policy constraints.

There is an effort by all nodes to beacon and respond to neighbors to form a mesh network. The competition for time slots causes the nodes to establish links with the first neighbors they find. Prioritization of radio neighbors is another waveform feature that can be controlled by policy. Unless a neighbor limit is set by policy, the number of simultaneous links increases with additional time slots. For example, if a waveform can be configured to support 80 or 100 time slots per transmission epoch, cross-layer metric reporting may increase system throughput.

LOS radio waveforms that require coordination of antenna steering at both the receiver and transmitter ends of the link operate in a manner that is different than traditional mobile ad hoc network (MANET) link activation protocols. Care must be taken to avoid the pitfalls of coupling link and network layer metrics within the operation of the waveform, but the benefits of careful cross-layer interaction are clear.

2.2.3.4 Preplanned Airborne-to-Ground Link Outages

There are numerous situations where the outages in a DIL environment are both temporary and known *a priori* in both severity and duration. DIL Communications policies should be able to consider such planned, known outages.

In tactical or emergency response environments, either manned or unmanned aircraft may execute a "racetrack pattern" to provide a high-position "advantaged" node for LOS radio communications. Figure 7 shows a plot of the communication connectivity from the airborne node to ground during a typical communications connectivity experiment. Time is represented on the vertical axis to illustrate the individual laps of the racetrack test.

Due to antenna placement (both ground and air), wing blockages disconnect communications on the turns. This, in effect, represents a planned outage. These outages can be anticipated by looking into the flight planning system. The turns also give an estimate of how long the outage typically will last. One level of use for this data is to add the "anticipated disconnection" parameters into a policy model for a heterogeneous mesh network of links that include such air-to-ground links.

Many other use cases exist. Examples include intermittent jamming, maintenance, and communications platform handover/changeover.

Without other link options, applications using intermittent links fail when packet loss exceeds the threshold required to keep the sessions supporting applications intact. Figure 7 represents on-orbit link availability of 88% with a steady 20 – 200 kbit/s stream and peak rates of approximately3.5 Mbit/s for 10s of seconds**.**

The same link measuring application availability for a command and control application is illustrated in Figure 8. The figure represents an on-orbit application availability of 52%.

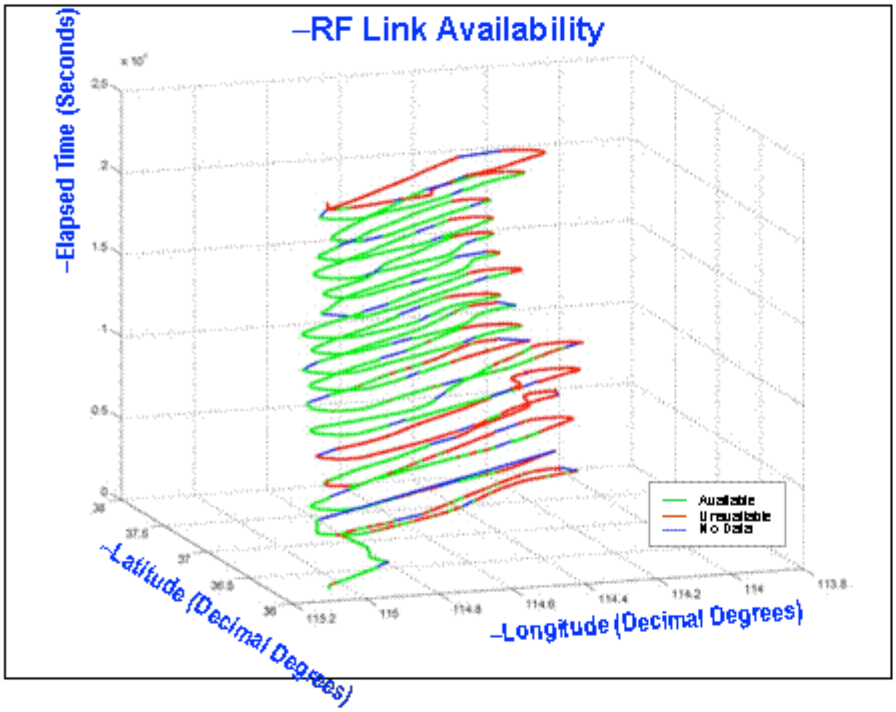

Figure 7. RF Link Availability in an Airborne Racetrack Test
Source: MIT Lincoln Laboratory

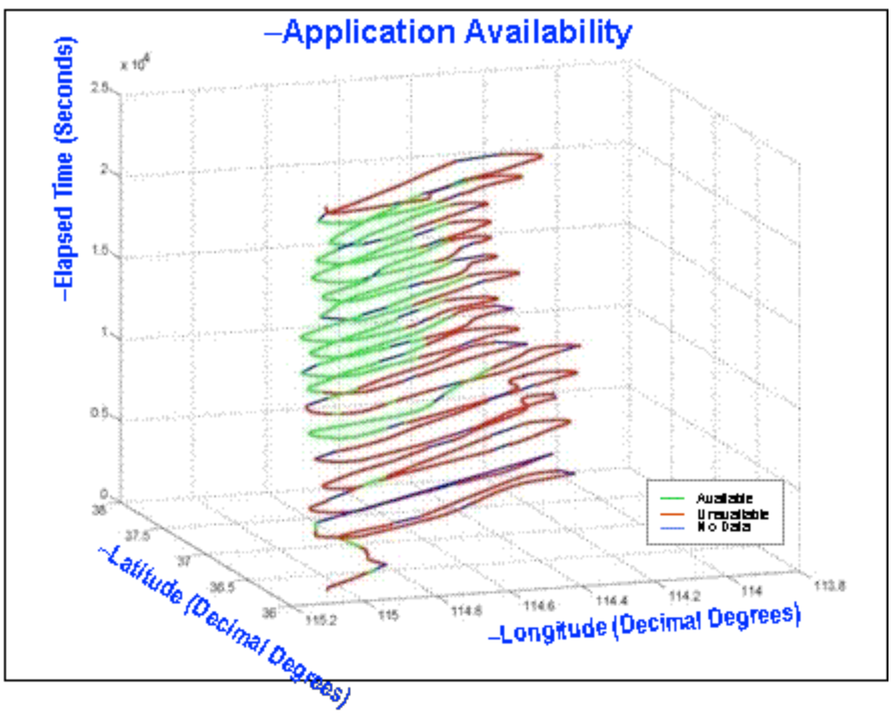

Figure 8. Application Availability on the Racetrack Air-to-Ground Link
Source: MIT Lincoln Laboratory

When applications do not take advantage of the knowledge of DIL communications environments, they have availability far lower than the raw link availability.

2.2.4 Constraints and Opportunities

Each physical layer and many MAC layer protocols have mechanisms to reallocate capacity. These are usually done via simple network management protocol (SNMP) or even via hard-coded algorithms in the transmission mechanism. Hard-coded mechanisms limit the use of the DIL pattern. SNMP allows management logic to intervene.

The primary opportunity is to have the logic that can perform reallocation operate from the same policies—entered into a system at the highest common level for all the elements of a heterogeneous network.

2.3 NIF Overarching and Specialized Frameworks

2.3.1 NIF Framework Conformance

NIF Overarching Architecture (OAA) defines the overall, high-level, long-term system of systems architecture that will be refined into reference architectures (RA).

2.3.2 Specialized Frameworks Conformance

2.3.2.1 Net-Centric Services Framework (NCSF)

This pattern uses the following pattern topics from the NCSF Pattern Check List:

- Service Discovery
- Service/User Trust
- Dynamism
- Robustness
- Policies and Aspects
- System Management

2.3.2.1.1 Service Discovery

DIL Communications depends on a service realization that externalizes the capacity limits of the mesh network at the network edge. Referencing Figure 2 in the NCSF, if a Service (SysML entity) is discoverable in a System, the attributes and operations must be visible to the resource user (the application). If DIL Communications is a Service, an attribute might be “minimum link capacity as critical link.” An operation might be “Perform critical service analysis on target link.”

2.3.2.1.2 Service/User Trust

Service-level metrics are key to the DIL Communications Management Technical Pattern. Critical links that cannot support the full capacity required by even the minimum requested by the SLA might still be the only way to get *any* information across to a edge user. If the need for some mission-critical information can be met by reconfiguring critical links and/or scaling mission data formats, the DIL Communications Management Technical Pattern will attempt to do this.

User Trust principles are a key part of the Net-Centric Information Assurance Framework (under development by NCOIC).

2.3.2.1.3 Dynamism

Multiple time scales for adjusting the mission-critical capacity of DIL Communications links are supported.

2.3.2.1.4 Robustness

Failure of links does not cause the logic within the DIL Communications entities to fail. The reallocation of capacity from other links is key to the operation of the DIL Communications Management Technical Pattern. The enable new paths process conducted by the policy-based bandwidth manager in Figure 6 is an example of how the DIL pattern instantiates robustness. Reallocation of time slot, frequency, code, or other resources in existing links as shown by this sequence diagram makes the DIL network more robust.

2.3.2.1.5 Policies and Aspects

DIL Communications Management depends on a policy-based bandwidth manager. Section 3.1 lists policy requirements. Policy is just one dimension of system management as it is being developed in the Net-Centric System Management Framework (NCSysMF). A core policy management technical pattern is planned to emerge along with the NCSysMF that will support the DIL pattern.

2.3.2.1.6 System Management

DIL Communications Management implements features and encompasses principles of the NCSysMF.

2.3.2.2 Net-Centric Semantic Information Framework

Information exchanged by services through the net-centric environment is done using accepted standards and information models in the net-centric environment. For services that interact with legacy systems (for example, legacy capacity allocation management systems), translations must be performed of information between the information model used by the legacy system and the net-centric environment.

2.3.2.3 Net-Centric System Management Framework (NCSysMF)

This pattern uses the following pattern topics from the NCSysMF Pattern Check List:

- Fault Isolation
- Capacity Management
- Service Management
- Root Cause Analysis

2.3.2.3.1 Fault Isolation

This pattern relies on detection of link faults and isolating the impact of any given link failure from the mission success.

2.3.2.3.2 Capacity Management

This pattern manages capacity on links deemed mission critical.

2.3.2.3.3 Service Management

This pattern extends the service management paradigm for mission-critical links to include fall-back modes of operation that would not exist if the system merely terminated all SLAs that fell below a set threshold.

2.3.2.3.4 Root Cause Analysis

This pattern relies on the management logic to winnow out extraneous underlying alarms and react to the root cause of a failure. For example, the loss of acceptable signal strength might result in a large number of port errors on an upper layer protocol. The action of the DIL pattern is to allocate capacity in stressed conditions, not react to the largest number of higher layer errors.

2.4 Known Uses

2.4.1 Internet Traffic Engineering

Commercial Internet backbone service providers offer global transport services for IP traffic from customer access networks. Backbone providers establish agreements with customer networks to ensure that IP transport of user traffic remains within specified performance bounds. Example metrics provided by commercial SLAs include latency, availability, and packet loss rate. Within each service provider domain, traffic is managed edge-to-edge to ensure adherence to SLAs and peering agreements. Failure of commercial links to business (mission)-critical processes is unacceptable. Business-critical links are usually overprovisioned by hot-standby links. DIL Communications may be disconnected or intermittent, but is rarely limited. Capacity allocation is accomplished by having considerably more peak capacity on standby.

2.4.2 MILSATCOM Traffic Control

The Transformational Communications Architecture (TCA), which includes Wideband MILSATCOM, enables the US DoD vision for a Global Information Grid (GIG) by simplifying the core transport system through open and interoperable protocols. The widespread adoption of IP at the network layer helps to establish a simple, interoperable backbone. The TCA leverages IP, adapting the architecture approach taken in the commercial Internet.

Applying the commercial model to military and other critical (e.g., first responder) networks, the terrestrial infrastructure may be viewed as one domain while deployed networks, such as the Army WIN-T or regional emergency networks, may be viewed as another. Traditionally, these disparate domains were connected through FDMA satellite links, a wireless link-layer solution for point-to-point communications.

In this context, the satellite communications domain has been traditionally limited to RF communications, and performance monitored in terms of transmitted power and allocated bandwidth for efficient loading of links on the transponder.

New IP modems in the MILSATCOM domain are requiring the development of combined RF and IP management. The DIL Communications Management Technical Pattern is part of the overall heterogeneous mesh network management.

2.5 Increased Capability Potential

The potential is for very critical data to be transmitted across the network under high stress conditions.

2.6 Related Patterns

There are several patterns in development by NCOIC that relate to this pattern and could benefit from consideration of the contents herein.

2.6.1 All Hazards Alert and Warning (AHAW) Capability Pattern

This pattern describes Emergency Management Response pattern of operation. Inherent in a robust emergency response discipline is the ability to react to lost resources with information "triage." When communications services and SLAs that depend on communications services fail, emergency response systems must have the ability to designate critical links and reconfigure link capacity as described in the DIL Communications Management Technical Pattern. This must happen automatically since human life and emergency crew safety can depend on critical communications across a DIL network.

2.6.2 Space Air Ground Maritime (SAGM) Operational Pattern

This pattern describes an overarching mobile networking pattern related to the global problem of end-to-end multimedia transmission through heterogeneous networks. The DIL capacity allocation pattern for heterogeneous networks is part of this issue.

2.7 References

[1] US Army SMDC/ARSTRAT, "Transformational IP Services Over Transponded SATCOM (TIPSOTS) Joint Concept of Operations," 4 March 2004.
[2] Rippon, J, "Joint Management Operations System (JMOS)," MILCOM 2006.
[3] Parikh, B., Fritz, D., "Network Centric Operations Over Transponded SATCOM," MILCOM 2004, Monterey, CA, October 2004.
[4] Hicks, J. *et al,* "Transformational IP Services Over Transponded SATCOM (TIPSOTS)," MILCOM 2007, Orlando, FL, October 2007.
[5] Bennet, B. *et al,* "Remote IP SATCOM Monitoring and Management," MILCOM 2008, San Diego, CA, November 2008.
[6] Sonnenberg, J. *et al,* "MANET Route Optimization Using Cross-Layer Enhancements in Tactical Radio Waveforms," MILCOM 2007, Orlando, FL, October 2007.
[7] Sonnenberg, J. *et al,* "A Framework for Net-Centric Services and Usage Patterns in Military Networks," MILCOM 2009, Boston, MA, October 2009.

3 Verification and Conformance

3.1 General Requirements

1. An instantiation of the DIL Communications Management Technical Pattern shall perform critical-link optimization.
2. Determination of critical-link status **shall** be by an adjustable policy threshold.

3. An instantiation of the DIL Communications Management Technical Pattern **shall** be managed by policy.
4. Policy **shall** be entered and maintained in an industry-standard format such as SNMP MIB, XML, XACML, or OWL.
5. Policy **shall** be entered at the highest level within the Policy-Based Network Management (PBNM) hierarchy that can be automatically translated to actionable commands to network equipment. The PBNM levels are: Business view, System view, Network view, Device view, Instance view.
6. The Business view is described by artifacts such as SLAs, processes, guidelines, and goals. If policy is entered at the Business view level, policy **shall** be automatically translatable to System view policy statements.
7. The System view describes Device and technology independent operation. If policy is entered at the System view level, policy **shall** be automatically translatable to Network view policy statements.
8. The Network view describes device-independent, but technology-specific operation. If policy is entered at the Network view level, policy **shall** be automatically translatable to Device view policy statements.
9. The Device view describes device- and technology-specific operation. If policy is entered at the Device view level, policy **shall** be automatically translatable to Instance view policy statements.
10. The Instance view is described by device-specific MIBs and Command Line Interface statements. Implementations of the DIL Communications Management Technical Pattern **shall** automatically translate Instance view policy statements to actionable equipment commands.
11. The CME **shall** recognize loss of coverage conditions.
12. The CME **shall** send loss of coverage notices to the PM.
13. The CME **shall** include known affected links in the loss of coverage notice.
14. The CME **shall** accept capacity allocation policy instructions from the PM.

4 Appendices

4.1 Appendix A: Call For Fire (CFF) Capability Pattern[4]

According to the NCSF (Section 3.1.8), Service Orchestration includes participant and role definition, variables, access control, and exception handlers. The formal definition of the user and providers roles, the variables transferred (access credentials, payment method, etc.,) would be the Service Orchestration parts of this example.

NCSF Section 3.1.9 describes Service Choreography as the ability to combine services into composite applications and invoke them through standard protocols. In this case, protocol means a deterministic send-respond sequence of exchanges that initiate and complete an action.

In conducting military missions, the mission pattern illustrated might include determining the situation and calling for help. In this pattern, User A requests friendly (blue forces) and enemy (red forces) location, given the current User A position, and then asks for fire support (battery or close air support). Figure 9 illustrates how this pattern could be viewed as a choreographed sequence of protocol exchanges (service invocations).

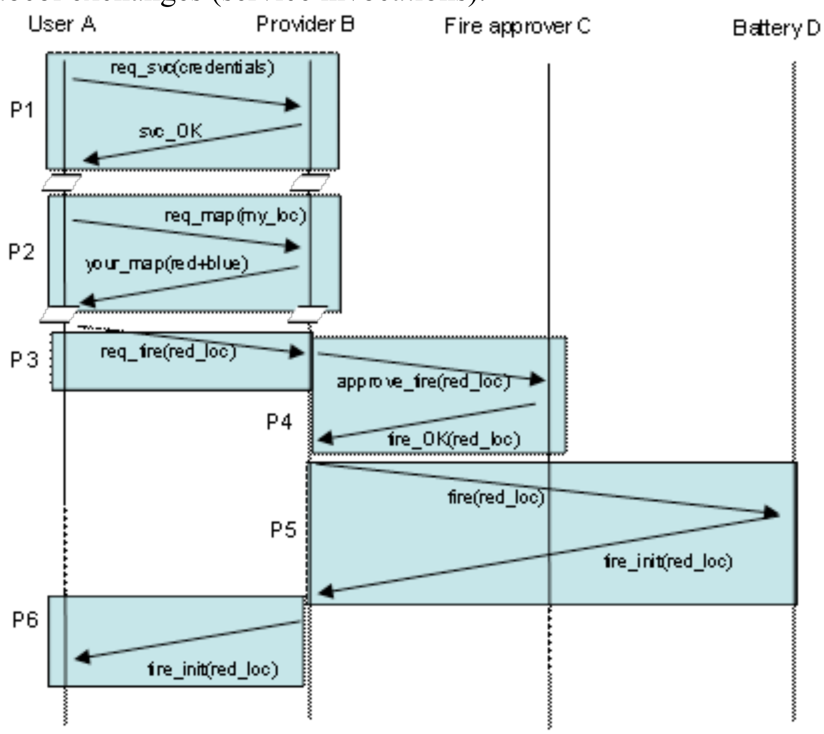

Figure 9. Call For Fire Choreography
Source: NCOIC

This simple example of choreography is a sequence of triplets:

- P1; A,B
- P2; A,B

[4] This example Capability Pattern is not in the NCOIC pattern track horizon, but is given here as an example that could use DIL.

- P3; A,B
- P4; B,C
- P5; B,D
- P6; B,A

where the first member of the triplet is the protocol (or service), the second is the initiator, and the third is the responder.

Once the req_fire(red_loc) has been sent, it is critical that fire actually happens and that User A knows it is coming. In this case, links AB, BC, and BD become critical. These examples use the term “link” in a generic sense. It is the paths (which may have multiple layer 2 links) that are critical. Ensuring these paths is the focus of the DIL Communications Management Technical Pattern.

More formally, we can describe the CFF Capability Pattern with the activity diagram in Figure 10.

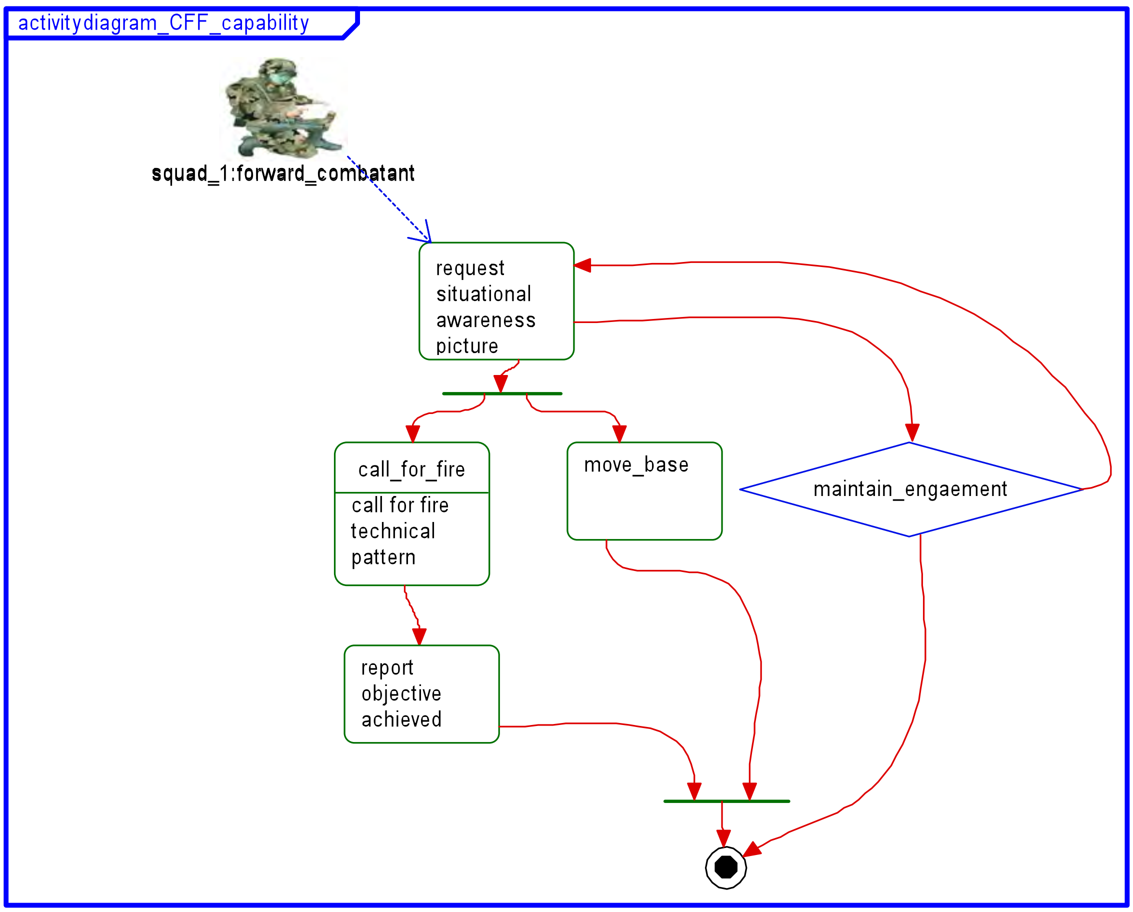

Figure 10. CFF Capability Pattern Activity Diagram
Source: NCOIC

The CFF Technical Pattern is illustrated in Section 4.2, Figures 11 and 12.

4.2 Appendix B: Call For Fire (CFF) Technical Pattern[5]

The CFF Technical Pattern activity diagram is illustrated in Figure 11.

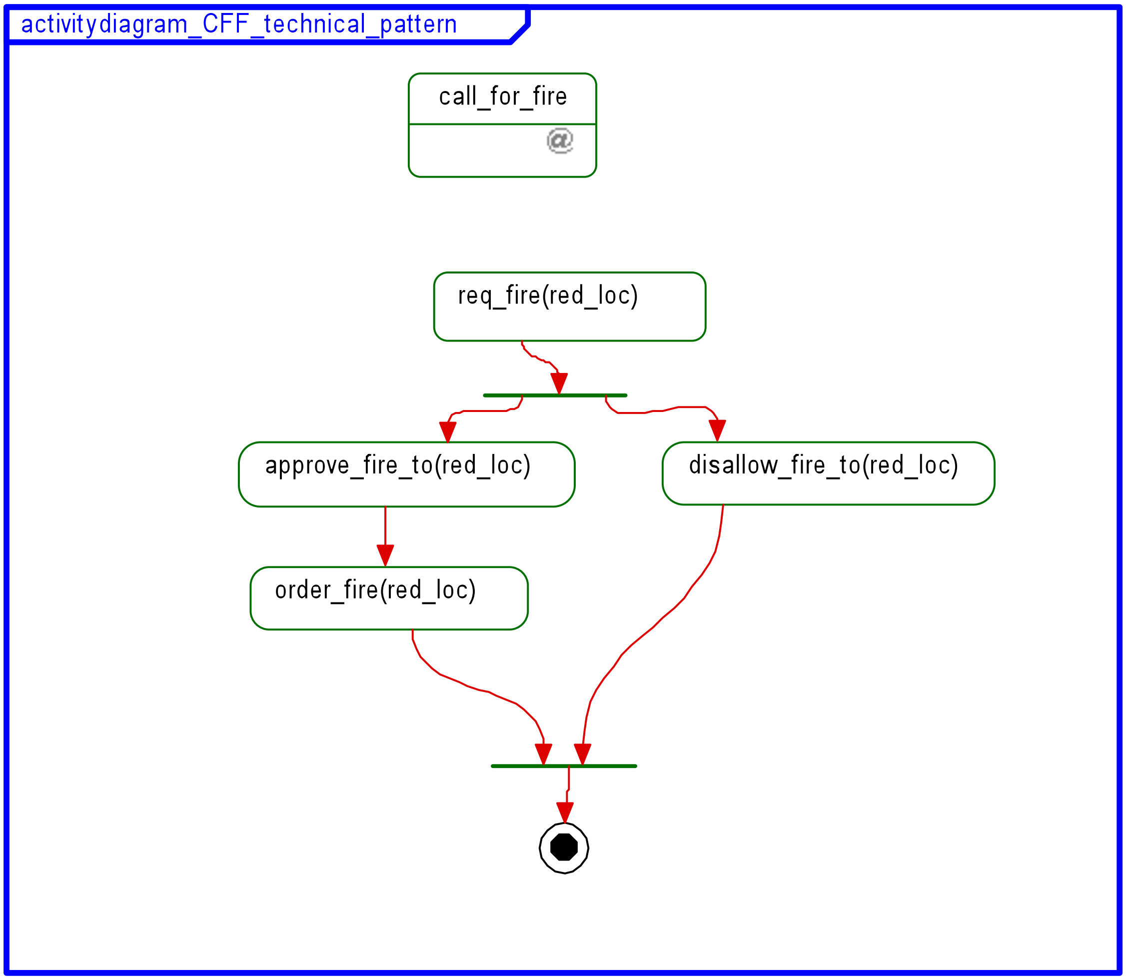

Figure 11. CFF Technical Pattern Activity Diagram
Source: NCOIC

The CFF Technical Pattern sequence diagram is illustrated in Figure 12.

[5] This example Activity Diagram is not in the NCOIC pattern track horizon, but is given here as an example that could utilize DIL.

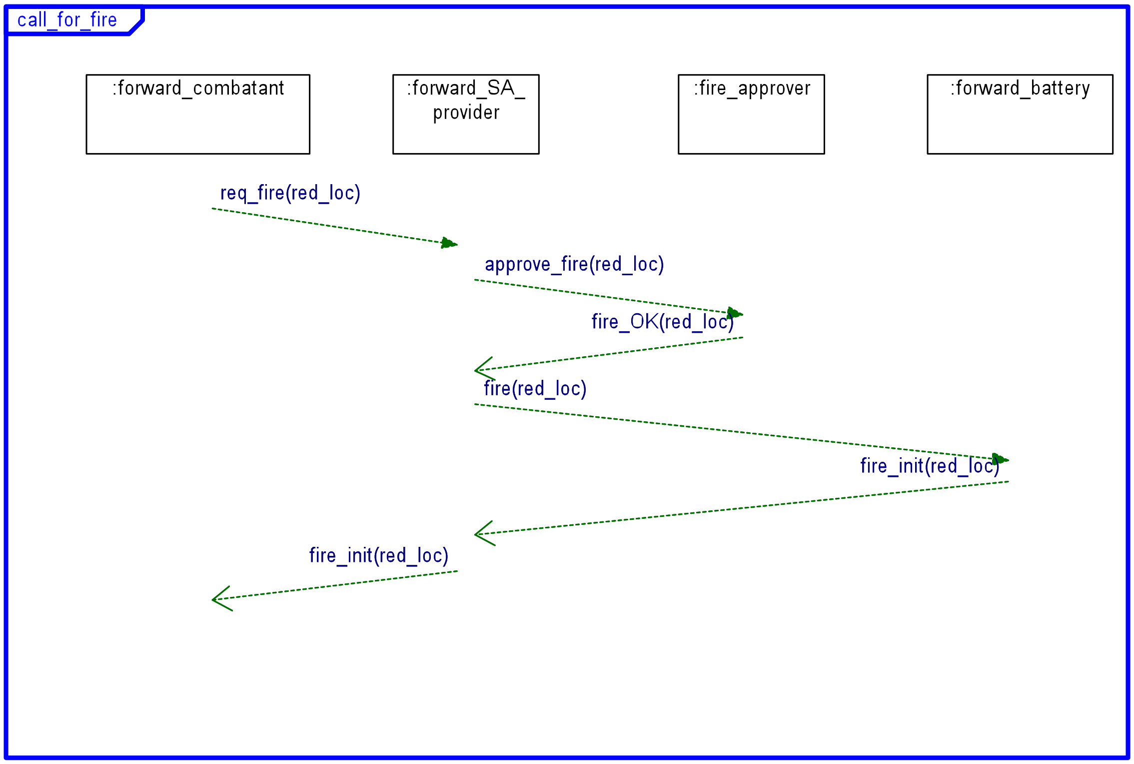

Figure 12. CFF Technical Pattern Sequence Diagram
Source: NCOIC

4.3 Appendix C: Acronyms

AHAW	All Hazards Alert and Warning
BER	Bit Error Rate
C4I	Command, Control, Communications, Computers, Intelligence
CME	Communications Mesh Element
COTS	Commercial Off the Shelf
DAMA	Demand Assigned Multiple Access
DIL	Disconnected, Intermittent, Limited
DoD	Department of Defense (United States)
EIGRP	Enhanced Interior Gateway Routing Protocol
FDMA	Frequency Division Multiple Access
FSO	Free Space Optical
Gbps	Giga Bits per second
GIG	Global Information Grid
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
JPEO	Joint Program Executive Office
JTEL	Joint Test and Evaluation Lab
KHz	kilokertz
LOS	Line of Sight
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LS	Link State
LSA	Link State Advertisement
MAC	Media Access Control
MANET	Mobile Ad Hoc Network
MIB	Management Information Base
MIL STD	Military Standard
MILSATCOM	Military Satellite Communications
MIT	Massachusetts Institute of Technology
MPR	Multipoint Relay
NCSF	Net-Centric Services Framework
NCSysMF	Net-Centric System Management Framework
NIF	NCOIC Interoperability Framework
NCOIC	Network Centric Operations Industry Consortium
OAA	Overarching Architecture
OSI	Open Systems Interconnection

OSPF	Open Shortest Path First
OWL	Ontological Web Language
PBNM	Policy-Based Network Management
PM	Policy Manager
QoS	Quality of Service
RA	Reference Architecture
RF	Radio Frequency
RFC	Request for Comments
SAGM	Space Air Ground Maritime
SCA	Software Communications Architecture
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
STD	Standard
SysML	Systems Modeling Language
TCA	Transformational Communications Architecture
TDMA	Time Division Multiple Access
TE	Traffic Engineering
TOS	Type of Service
UHF	Ultra High Frequency
VoIP	Voice over Internet Protocol
WG	Working Group
WIN-T	Warfighter Information Network – Tactical
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language