System of Systems Integration Lower Tactical Internet (LTI)

Vehicle Tactical Router Product Specification

Document No. V19 March 5, 2013

Table of Contents

1 Scope 1
2 Applicable Documents 1
2.1 General 1
2.1.1 Government Documents 1
2.1.1.1 Specifications, Standards and Handbooks 1
2.1.1.2 Other Government Documents 1
2.1.2 Non-Government Documents 2
2.1.2.1 Internet Engineering Task Force (IETF) Requeat For Comment (RFC) 2
3 Requirements 6
3.1 Interfaces 6
3.2 Layer 2 7
3.3 Layer 3 7
3.3.1 Route Redistribution 7
3.3.3 IPv4 8
3.3.4 IPv6 8
3.3.5 Tunneling 9
3.4 Multicast 9
3.5 Routing 10
3.5.1 RIP 10
3.5.2 OSPFv2 10
3.5.3 OSPFv3 10
3.5.4 BGP 11
3.6 QoS 11
3.7 Security 12
3.7.1 Firewall 12
3.7.2 Intrusion Detection 13
3.7.3 Router Access 15
3.7.4 Reserved 15
3.7.5 Sanitization 15
3.7.6 PKI 16
3.7.7 Access Control 16
3.8 Configuration 16
3.8.1 Configuration Modification 16
3.8.2 Configuration Files 17
3.8.3 Configuration Interface 17
3.9 Network Management 18
3.10 System Software 18
3.10. 1 System Software Upgrade 18
3.10.2 Debug Capability 18
3.11 HW Performance 18

3.12 Electrical Characteristics 19
3.13 Mechanical Characteristics 19
3.13.1 Dimensions and Weight 19
3.14 Environmental 19
3.14.1 Temperature 19
3.14.2 Humidity 19
3.14.3 Altitude 19
3.14.5 Salt Fog 20
3.14.6 Shock 20
3.14.8 Fungus 21
3.14.9 Electromagnetic Interference/Compatibility 21
3.14.10 Electromagnetic Pulse 21
3.14.11 Lightning Protection 21
3.15 Reliability and Maintainability 21
3.15.1 Reliability 21
3.15.2 Maintainability 21
3.16 Safety 22
3.16.1 Electrical Safety 22
3.16.3 Mechanical Safety 22
3.16.4 Safety Marking and Labels 22
3.16.5 Chemical Safety 22
3.16.6 Environmental Safety 23
3.17 Human Factors 23
Table 4.1 Verification Method 1

Tactical Router Product Specification

1 Scope

This document defines the requirements and functionality of the Vehicle Tactical Router to be used in the Lower Tactical Internet. Configuration Methods, Protocols, Logical and Physical interfaces are defined. This is a complete specification for the Tactical Router requirements for the tactical environment.

2 Applicable Documents

2.1 General

The following documents are listed for guidance only.

2.1.1 Government Documents

2.1.1.1 Specifications, Standards and Handbooks

MIL-HDBK-217 Reliability Prediction of Electronic Equipment

MIL-HDBK-454B Guidelines for Electronic Equipment

MIL-STD-1275D Department of Defense Interface Standard: Characteistics of 28 Volt DC Electrical Systems In Military Vehicles (29 Aug 2006)

MIL-STD-1472F, Department of Defense Design Criteria Sstandard: Human Engineering (23 Aug 1999)

MIL-STD-2169B Department of Defense Inteface Standard: High Altitude Electromagnetic Pulse (HEMP) Environment (19-Jan-2012)

MIL-STD-461E Department of Defense Interface Standard: Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems an Equipment (20 Aug 1999)

MIL-STD-464B Department of Defense Interface Standard: Electromagnetic Environmental Effects, Requirements for Systems (30 Nov 2010)

MIL-STD-810F Department of Defense Test Method Standard: Environmental Enginering Considerations and Laboratory Tests (31 Oct 2008)

2.1.1.2 Other Government Documents

Clean Air Act Amendment Title V1, Section 602

Code of Federal Regulations Title 47 Part 15

Defense security Service (DSS) Clearing and Sanitization Matrix 2007-06-28

DODI 8520.2 Public Key (PK) Infrastructure and Public Key Enabling Depatment of Defense 01 April 2004

Federal Information Processing Standards (FIPS) Publication (PUB) 197 Advanced Encryption Standard (AES)

FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997.

OSHA Code of Federal Regulations 1910 Permissible Exposure Limits

X.509 Certificate Policy for the United States Department of Defense

Tactical Router Product Specification
2.1.2 Non-Government Documents
2.1.2.1 Internet Engineering Task Force (IETF) Requeat For Comment (RFC)
[RFC 0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.
[RFC 0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.
[RFC 0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.
[RFC 0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.
[RFC 0826] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, November 1982.
[RFC 0919] Mogul, J., "Broadcasting Internet Datagrams", STD 5, RFC 919, October 1984.
[RFC 0922] Mogul, J., "Broadcasting Internet datagrams in the presence of subnets", STD 5, RFC 922, October 1984.
[RFC 0951] Croft, W. and J. Gilmore, "Bootstrap Protocol", RFC 951, September 1985.
[RFC 1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.
[RFC 1256] Deering, S., Ed., "ICMP Router Discovery Messages", RFC 1256, September 1991.
[RFC 1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation and Analysis", RFC 1305, March 1992.
[RFC 1334] Lloyd, B. and W. Simpson, "PPP Authentication Protocols", RFC 1334, October 1992.
[RFC 1388] Malkin, G., "RIP Version 2 Carrying Additional Information", RFC 1388, January 1993.
[RFC 1403] Varadhan, K., "BGP OSPF Interaction", RFC 1403, January 1993.
[RFC 1542] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, October 1993.
[RFC 1702] Hanks, S., Li, T., Farinacci, D., and P. Traina, "Generic Routing Encapsulation over IPv4 networks", RFC 1702, October 1994.
[RFC 1724] Malkin, G. and F. Baker, "RIP Version 2 MIB Extension", RFC 1724, November 1994.
[RFC 1771] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.
[RFC 1850] Baker, F. and R. Coltun, "OSPF Version 2 Management Information Base", RFC 1850, November 1995.
[RFC 1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.
[RFC 1997] Chandra, R., Traina, P., and T. Li, "BGP Communities Attribute", RFC 1997, August 1996.
[RFC 2003] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.
[RFC 2080] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.
[RFC 2082] Baker, F. and R. Atkinson, "RIP-2 MD5 Authentication", RFC 2082, January 1997.
[RFC 2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
[RFC 2205] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.
[RFC 2215] Shenker, S. and J. Wroclawski, "General Characterization Parameters for Integrated Service Network Elements", RFC 2215, September 1997.

Tactical Router Product Specification
[RFC 2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.
[RFC 2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, March 1998.
[RFC 2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.
[RFC 2362] Estrin, D., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, M., Jacobson, V., Liu, C., Sharma, P., and L. Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", RFC 2362, June 1998.
[RFC 2373] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.
[RFC 2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.
[RFC 2439] Villamizar, C., Chandra, R., and R. Govindan, "BGP Route Flap Damping", RFC 2439, November 1998.
[RFC 2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, November 1998.
[RFC 2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
[RFC 2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.
[RFC 2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.
[RFC 2463] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.
[RFC 2472] Haskin, D. and E. Allen, "IP Version 6 over PPP", RFC 2472, December 1998.
[RFC 2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.
[RFC 2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.
[RFC 2519] Chen, E. and J. Stewart, "A Framework for Inter-Domain Route Aggregation", RFC 2519, February 1999.
[RFC 2545] Marques, P. and F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing", RFC 2545, March 1999.
[RFC 2597] Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, June 1999.
[RFC 2598] Jacobson, V., Nichols, K., and K. Poduri, "An Expedited Forwarding PHB", RFC 2598, June 1999.
[RFC 2606] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, June 1999.
[RFC 2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.
[RFC 2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

Tactical Router Product Specification
[RFC 2740] Coltun, R., Ferguson, D., and J. Moy, "OSPF for IPv6", RFC 2740, December 1999.
[RFC 2766] Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.
[RFC 2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.
[RFC 2796] Bates, T., Chandra, R., and E. Chen, "BGP Route Reflection - An Alternative to Full Mesh IBGP", RFC 2796, April 2000.
[RFC 2858] Bates, T., Rekhter, Y., Chandra, R., and D. Katz, "Multiprotocol Extensions for BGP-4", RFC 2858, June 2000.
[RFC 2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.
[RFC 2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.
[RFC 2918] Chen, E., "Route Refresh Capability for BGP-4", RFC 2918, September 2000.
[RFC 2983] Black, D., "Differentiated Services and Tunnels", RFC 2983, October 2000.
[RFC 3041] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.
[RFC 3065] Traina, P., McPherson, D., and J. Scudder, "Autonomous System Confederations for BGP", RFC 3065, February 2001.
[RFC 3101] Murphy, P., "The OSPF Not-So-Stubby Area (NSSA) Option", RFC 3101, January 2003.
[RFC 3137] Retana, A., Nguyen, L., White, R., Zinin, A., and D. McPherson, "OSPF Stub Router Advertisement", RFC 3137, June 2001.
[RFC 3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.
[RFC 3246] Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", RFC 3246, March 2002.
[RFC 3260] Grossman, D., "New Terminology and Clarifications for Diffserv", RFC 3260, April 2002.
[RFC 3330] IANA, "Special-Use IPv4 Addresses", RFC 3330, September 2002.
[RFC 3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
[RFC 3392] Chandra, R. and J. Scudder, "Capabilities Advertisement with BGP-4", RFC 3392, November 2002.
[RFC 3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.
[RFC 3412] Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, December 2002.
[RFC 3413] Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.
[RFC 3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the

Tactical Router Product Specification
Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.
[RFC 3569] Bhattacharyya, S., Ed., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003.
[RFC 3587] Hinden, R., Deering, S., and E. Nordmark, "IPv6 Global Unicast Address Format", RFC 3587, August 2003.
[RFC 3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.
[RFC 3697] Rajahalme, J., Conta, A., Carpenter, B., and S. Deering, "IPv6 Flow Label Specification", RFC 3697, March 2004.
[RFC 3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
[RFC 3973] Adams, A., Nicholas, J., and W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", RFC 3973, January 2005.
[RFC 4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.
[RFC 4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
[RFC 4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.
~~[RFC 4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, May 2006.~~
[RFC 4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.
~~[RFC 4604] Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", RFC 4604, August 2006.~~
[RFC 4606] Mannie, E. and D. Papadimitriou, "Generalized Multi-Protocol Label Switching (GMPLS) Extensions for Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) Control", RFC 4606, August 2006.
[RFC 4742] Wasserman, M. and T. Goddard, "Using the NETCONF Configuration Protocol over Secure SHell (SSH)", RFC 4742, December 2006.
[RFC 4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.
[RFC 4765] Debar, H., Curry, D., and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)", RFC 4765, March 2007.
[RFC 5186] Haberman, B. and J. Martin, "Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction", RFC 5186, May 2008.
[RFC 5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.
[RFC 5578] Berry, B., Ed., Ratliff, S., Paradise, E., Kaiser, T., and M. Adams, "PPP over Ethernet

Tactical Router Product Specification
(PPPoE) Extensions for Credit Flow and Link Metrics", RFC 5578, February 2010.
[RFC 5643] Joyal, D., Ed., and V. Manral, Ed., "Management Information Base for OSPFv3", RFC 5643, August 2009.
1.2.2.2 Industry Standards
IEEE 802.1P LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization
IEEE 802.1Q-2005 Virtual Bridge local Area Networks
IEEE 802.1x Port Based Authentication Concepts
IEEE 802.3-1998 Local Area Network (LAN) protocols
IEEE 802.3-2002Local Area Network (LAN) protocols
1.2.2.3 Other Industry Documents
American Conference of Governmental Industrial Hygienists (ACGIH) Threshold Limit Values (TLV)
American National Standard for Product Safety Signs and Labels
International Standards Organization Information Technology – Telecommunnications and Information Exchange Between Systems ISO/IEC 8877:1992
Microsoft's PEAP version 0 (Implementation in Windows XP SP1)
National Electrical Code, NFPA 70-2005
RSA Laboratories Public Key Cryptography Standard 12, Personal Information Exchange Syntax Standard, version 1.0 (Draft), 30 April 1997
Support of Address Families in OSPFv3
Underwriters Llaboratories (UL) 60950 Safety of Information Technology Equipment

Requirement	Core	Growth
3 Requirements		
This section provides the detailed requirements for the Tactical Router . They include details associated with interfaces, layer 2 and layer 3 functionality, Multicast capabilities, routing protocols, quality of service (QOS), security, configuration, network management, system software, performance and supportability requirements.		
3.1 Interfaces		
3.1.1 Loopback Interface: The Tactical Router shall support loopback interface [RFC 2606], [RFC 3330]	X	
3.1.2 Routed Ports: The Tactical Router shall have a minimum of two (2) Routed ports.	X	
3.1.3 Switched Ports: The Tactical Router shall have a minimum of two (2) Ethernet Switched ports, at data rates of 10/100 Base-T [IEEE 802.3-1998] per port.	X	
3.1.4 Auto MDIx: Each Ethernet Switch port shall support Automatic Medium Dependent Interface Crossover (Auto-MDIx).	X	
3.1.5 Console Port: The Tactical Router shall have one (1) serial console port used to connect and configure the Router.	X	

Requirement	Core	Growth
3.2 Layer 2		
3.2.1 VLAN:The Tactical Router shall support IEEE STD 802.1q Virtual local Area Network (VLAN) tagging.	X	
3.2.2 Priority Queuing: The Tactical Router shall support IEEE STD 802.1q for priority/queuing (commonly referred to as 802.1p or class of service Priority Code Point within an ethernet frame).	X	
3.2.3 PPP: The Tactical Router shall support Point-to-Point Protocol (PPP) Authentication protocols - Password Authentication Protocol (PAP) [RFC 1334] and Challenge-Handshake Authentication Protocol (CHAP) [RFC 1994].	X	
3.2.4 EAP/PEAP: The Tactical Router shall support Network Layer Authentication - Extensible Authentication Protocol (EAP) framework [RFC 3748] Protected Extensible Authentication Protocol (PEAP) protocol [draft-kamath-ppptxt-peapv0-00.txt].	X	
3.2.5 EAPOL:The Tactical Router shall support the EAP over LAN (EAPOL) IEEE STD 802.1x protocol.		X
3.2.6 Fast Ethernet: The Tactical Router shall support 10/100 baseT Ethernet per Datalink Layer (Layer 2) IAW IEEE STD 802.3-1998.	X	
3.3 Layer 3		
3.3.1 Route Redistribution		
3.3.1.1 Route Distribution: The Tactical Router shall support route distribution between Routing Information Protocol version 2 (RIPv2) [RFC 1388], and Open Shortest Path First (OSPFv2) [RFC 2328] protocols.	X	
3.3.1.2 RIPv2 and OSPFv2 Route Filtering: The Tactical Router shall support route filtering between Routing Information Protocol version 2 (RIPv2) [RFC 1388], and Open Shortest Path First (OSPFv2) [RFC 2328] protocols.	X	
3.3.1.3 Default Address Filtering: The Tactical Router shall support filtering of default address 0/0	X	
3.3.1.4 Static Routing: The Tactical Router shall support static routing.	X	
3.3.1.5 Static Default Address:The Tactical Router shall support generation of a static default address 0/0	X	
3.3.1.6 Route Summarization: The Tactical Router shall support route summarization including the default address 0/0, conditioned on the receipt of a specific address within the default space	X	
3.3.1.7 Route Redistribution: The Tactical Router shall support static route redistribution between Routing Information Protocol version 2 (RIPv2) [RFC 1388] and Open Shortest Path First (OSPFv2) [RFC 2328] protocols.	X	
3.3.1.8 Default Address Distribution: The Tactical Router shall support route distribution and redistribution of the default address 0/0	X	
3.3.2 Other Protocols		

Requirement	Core	Growth
3.3.2.1 Overhead Reduction: The Tactical Router will support overhead Reduction of OSPFv3 Control Messages [RFC 5340].		X
3.3.2.2 UDP: The Tactical Router shall support the User Datagram Protocol (UDP) [RFC 768].	X	
3.3.2.3 TCP: The Tactical Router shall support Transmission Control Protocol (TCP) [RFC 793], Explicit Congestion Notification (ECN) [RFC 3168].	X	
3.3.3 IPv4		
3.3.3.1 IP: The Tactical Router shall support the Internet Protocol [RFC 791].	X	
3.3.3.2 ARP: The Tactical Router shall support Address Resolution Protocol (ARP) [RFC 826].	X	
3.3.3.3 IP Broadcast Transfers: The Tactical Router shall support IP Broadcast transfers [RFC 919].	X	
3.3.3.4 IP Broadcast Transfers in Subnets: The Tactical Router shall support IP Broadcast transfers in presence of subnets [RFC 922].	X	
3.3.3.5 ICMP Router Discovery: The Tactical Router shall support ICMP Router Discovery [RFC 1256].	X	
3.3.3.6 BOOTP: The Tactical Router shall support the Bootstrap Protocol (BOOTP) forwarding for clients [RFC 1542].	X	
3.3.3.7 ICMP: The Tactical Router shall support the Internet contol Message Protocol (ICMP) [RFC 792].	X	
3.3.3.8 NAT/PAT: The Tactical Router will support Network/Port Address Translation (NAT/PAT) [RFC 2766].		X
3.3.3.9 PPPoE: The Tactical Router shall support PPP over Ethernet (PPPoE), [RFC 2516]	X	
3.3.4 IPv6		
3.3.4.1 IPv6: The Tactical Router will support IPv6 Addressing Architecture [RFC 2373].		X
3.3.4.2 IPv6 Aggregate Global Unicast: The Tactical Router will support IPv6 Aggregatable Global Unicast Address Format [RFC 3587].		X
3.3.4.3 IPv6: The Tactical Router will support Internet Protocol, Version 6 (IPv6) Specification [RFC 2460].		X
3.3.4.4 IPv6 Neighbor Discovery: The Tactical Router will support Neighbor Discovery for IPv6 [RFC 2461].		X
3.3.4.5 IPv6 Stateless Address Auto Configuration: The Tactical Router will support IPv6 Stateless Address Auto configuration [RFC 2462].		X
3.3.4.6 ICMPv6 for IPv6: The Tactical Router will support ICMPv6 for the IPv6 Specification [RFC 2463].		X
3.3.4.7 IPv6 Data Transfer: The Tactical Router will transfer IPv6 data traffic.		X
3.3.4.8 Privacy Extension for Stateless Auto Configuration: The Tactical Router will support Privacy Extension for Stateless Auto configuration [RFC 3041].		X

Requirement	Core	Growth
3.3.4.9 IPv6 over PPP: The Tactical Router will support IPv6 Over PPP [RFC 2472].		X
3.3.4.10 IPv6 Global Address: The Tactical Router will support IPv6 Global Address [RFC 3587].		X
3.3.4.11 IPv6 Flow Label Specification: The Tactical Router will support IPv6 Flow Label Specification [RFC 3697].		X
3.3.5 Tunneling		
3.3.5.1 RSVP Tunneling: The Tactical Router will allow Resource Reservation Protocol (RSVP) [RFC 2205] packets to pass through tunnels.		X
3.3.5.2 Reserve Bandwidth Exclusion: The Tactical Router will not act on RSVP [RFC 2205] messages to measure and reserve bandwidth across the network.		X
3.3.5.3. DSCP Data: The 6-bit Differentiated Service Control Point (DSCP) field information in the IPv4 header [RFC 2474] shall be carried from the inner Internet Protocol (IP) packet header to the tunneled IP header [RFC 2983]	X	
3.3.5.4 RSVP: The Tactical Router will support RSVP as defined in the RSVP version 1 Functional Specification [RFC 2205].		X
3.3.5.5 IPSec: The Tactical Router shall support Internet Protocol Security (IPsec) tunneling [RFC 4301] and [RFC 4309].	X	
3.3.5.6 IPv4 Tunneling: The Tactical Router shall support IPv4 tunneling [RFC 2003]	X	
3.3.5.7 IPv6 Tunneling: The Tactical Router will support IPv6 tunneling.		X
3.3.5.8 GRE: The Tactical Router shall support Generic Routing Encapsulation (GRE) [RFC 1702] and [RFC 2784].	X	
3.4 Multicast		
3.4 1 Port Mirroring: The Tactical Router will support port mirroring	X	
3.4.2 IP Multicast Routing: The Tactical Router shall support IP multicast routing.	X	
3.4.3 Static Provisioning of IP Multicast Routing: The Tactical Router shall support static provisioning of IP multicast routing.	X	
3.4.4 IGMP Transfers: The Tactical Router shall support Internet Group Management Protocol (IGMP) v3 transfers [RFC 3376] and [RFC 4606].	X	
3.4.5 IP Multicast Host Extensions: The Tactical Router shall support Host Extensions for IP Multicasting [RFC 1112].	X	
3.4.6 Multicast on all Interfaces: The Tactical Router shall support Multicast on all interface types.	X	
3.4.7 PIM-SM: The Tactical Router shall support PIM-SM [RFC 2362], [RFC 4601].	X	
3.4.8 PIM-DM: The Tactical Router shall support Protocol Independent Multicast-Dense Mode (PIM-DM) [RFC 3973].	X	
3.4.9 MLD: The Tactical Router will support Multicast Listener Discovery (MLD) (IPv6) [RFC 2710].		X
3.4.10 IGMPv3: The Tactical Router shall support Internet Group Management Protocol version 2 (IGMP) v3 [RFC 5186].	X	

Requirement	Core	Growth
3.4.11 Source Specific Multicast: The Tactical Router will support Source Specific Multicast [RFC 3569].	X	
3.4 12 PIM-SM ASM: The Tactical Router shall support PIM-SM Any Source Multicast (ASM) [RFC 2362].	X	
3.4.13 Multicast Packet Replication: The Tactical Router shall support multicast packet replications.	X	
3.4.14 MSDP: The Tactical Router shall support Multicast Source Discovery Protocol (MSDP) [RFC 3618].	X	
~~**3.4.15 IGMPv3 Proxy: The Tactical Router shall provide an Internet Group Management Protocol version 3 (IGMP v3) [RFC 4604] proxy [RFC 4541]**~~	~~**X**~~	~~-~~
3.4.16 MLD Proxy: The Tactical Router will provide an Multicast Listener Discovery (MLD) proxy.		X
3.5 Routing		
3.5.1 RIP		
3.5.1.1 RIPv2: The Tactical Router shall support RIPv2 in accordance with [RFC 453].	X	
3.5.1.2. RIPv2 MIB: The Tactical Router shall support RIPv2 Management Information Base (MIB) Extension [RFC 1724].	X	
3.5.1.3 RIPv2 MD5: The Tactical Router shall support RIPv2 Message-Digest Algorithm (MD5) Authentication [RFC 2082].	X	
3.5.1.4 RIP/NG: The Tactical Router will support the RIP/NG protocol [RFC 2080].		X
3.5.2 OSPFv2		
3.5.2.1 OSPFv2: The Tactical Router shall support Open Shortest Path First version 2 (OSPFv2) [RFC 2328].	X	
3.5.2.2 Stub Router Advertisement: The Tactical Router shall support Stub Router Advertisement [RFC 3137].	X	
3.5.2.3 NSSA: The Tactical Router shall support Not-so stubby area (NSSA option) [RFC 3101].	X	
3.5.2.4 OSPFv2 MIB: The Tactical Router shall support the OSPFv2 management Information Database (MIB) [RFC 1850].	X	
3.5.2.5 BGP-OSPF Interaction: The Tactical Router will support BGP-OSPF Interaction [RFC 1403].		X
3.5.3 OSPFv3		
3.5.3.1 OSPFv3: The Tactical Router will support OSPFv3 [RFC 5340].		X
3.5.3.2 OSPFv3 MIB: The Tactical Router will support OSPFv3 MIB [RFC 5643].		X
3.5.3.3 OSPFv3 Route Exchanges: The Tactical Router will support exchanges (import/export) of routes from OSPFv2 [RFC 2328] and OSPFv3 [RFC 5340].		X
3.5.3.4 Link Cost Calculation: The Tactical Router will utilize network topology and link characteristics to calculate the link cost.		X

Requirement	Core	Growth
3.5.3.5 Destination IPv4 Address: The Tactical Router will utilize the destination IPv4 address to route traffic.		X
3.5.3.6 Destination IPv6 Address: The Tactical Router will utilize the destination IPv6 address to route traffic.		X
3.5.3.7 Address Families: The Tactical Router will support Address Families in OSPFv3 per IETF [draft-ietf-ospf-af-alt-05.txt], updated draft or formalized RFC.		X
3.5.4 BGP		
3.5.4.1 BGP4: The Tactical Router will support BGP4 protocol [RFC 1771].		X
3.5.4.2 Capabilities Advertisment: The Tactical Router will support Capabilities Advertisement [RFC 3392].		X
3.5.4.3 Autonomous System Configuration: The Tactical Router will support Autonomous System Confederation [RFC 3065].		X
3.5.4.4 Routes Refresh: The Tactical Router will support Routes Refresh [RFC 2918].		X
3.5.4.5 Routes Reflection: The Tactical Router will support Route Reflection [RFC 2796].		X
3.5.4.6 BGP4 Extension for IPv6: The Tactical Router will support BGP4 Extension for IPv6 [RFC 2545].		X
3.5.4.7 Route Aggregation: The Tactical Router will support Route Aggregation [RFC 2519].		X
3.5.4.8 Route Flap Damping: The Tactical Router will support Route Flap Damping [RFC 2439].		X
3.5.4.9 BGP Protection: The Tactical Router will support BGP Protection over TCP using MD5 [RFC 2385].		X
3.5.4.10 BGP Communities Attributes: The Tactical Router will support BGP Communities Attributes [RFC 1997].		X
3.5.4.11 M-BGP: The Tactical Router will support M-BGP [RFC 2858].		X
3.5.4.12 Route Exchange over OSPF: The Tactical Router will support route exchange (Import/Export) across OSPF v2/v3 [RFC 2328]/[RFC 5340]and BGP.		X
3.6 QoS		
3.6.1 DSCP IPv4 Marking: The Tactical Router shall support marking the Differentiated Services Code Point (DSCP) [RFC 2474] field of the IPv4 header.	X	
3.6.2 DSCP IPv6 Marking: The Tactical Router will support marking the DSCP field of the IPv6 header.		X
3.6.3 Deep Packet Inspection: The Tactical Router shall support deep packet inspection to **classify on the IP header to** mark DSCPs.	X	
3.6.4 Multiple DSCP Classes: The Tactical Router shall support multiple user defined DSCP classes.	X	
3.6.5 Packet Filtering: The Tactical Router shall support filtering of packets based upon DSCP into predefined classes.	X	

Requirement	Core	Growth
3.6.6 DiffServ Architecture: The Tactical Router will support the Differentiated Services (DiffServ) architecture according to IETF standards [RFC 2475] and [RFC 3260].	X	
3.6.7 EF PHB: The Tactical Router shall support Expedited Forwarding (EF) Per Hop Behavior (PHB) [RFC 2598] and [RFC 3246].	X	
3.6.8 AF PHB: The Tactical Router shall support Assured Forwarding (AF) PHB [RFC 2597].	X	
3.6.9 Integrated Services Architecture: The Tactical Router shall support the Integrated Services Architecture according to IETF standards [RFC 2215]	X	
3.6.10 Traffic Prioritization: The Tactical Router shall ensure that the voice traffic and high priority data traffic is processed before low priority traffic.	X	
3.6.11 Egress Queuing: The Tactical Router shall identify traffic based on the DSCP field of the IP header [RFC 2474] for use in Router egress queuing.	X	
3.6.12 Queuing Classes: The Tactical Router shall provide a minimum of four (4) classes or queues per interface.	X	
3.6.13 RED Queuing Classes The tactical Router shall be able to apply four (4) Random Early Detection (RED) classes to each queue.	X	
3.6.14 QoS Queues: The Tactical Router shall support QoS queues for each virtual, logical, and physical interface.	X	
3.6.15 Queue Prioritization: The Tactical Router shall enable the setting of the priority of each queue in the configuration.	X	
3.6.16 Queue Management Techniques: The Tactical Router shall provide active queue management techniques that enable DSCP per hop behaviors for voice, video and data. At a minimum Random Early Detection, Weighted Fair Queue and Priority Queue will be implemented.	X	
3.6.17 Credit Based Flow Control: The Tactical Router shall provide PPPoE Extensions for Credit Based Flow Control [RFC 5578]	X	
3.6.18 Queue Management In the Configuration: The Tactical Router shall have queue management techniques specified in the configuration.	X	
3.7 Security		
3.7.1 Firewall		
3.7.1.1 Modification of Firewall Rules: The Tactical Router shall provide access to the Firewall to add, remove and modify individual firewall rules.	X	
3.7.1.2 Modification of Firewall Rule-sets: The Tactical Router shall provide access to the Firewall to add, remove and modify firewall rule-sets.	X	
3.7.1 .3 Modification of Firewall Packet Acounting Rules: The Tactical Router shall provide access to the Firewall to add, remove and modify packet accounting rules.	X	
3.7.1.4 Packet Acounting: The Tactical Router **shall** provide access to the Firewall to read and reset packet accounting counters.	X	

Requirement	Core	Growth
3.7.1.5 Packet Logging: The Tactical Router **shall** provide access to the Firewall to Set, add, remove and modify Firewall packet logging.	X	
3.7.1.6 Firewall SNMP Alert Configuration: The Tactical Router **shall** provide access to the Firewall to Set, add, remove and modify Firewall SNMP alert configuration.	X	
3.7.1.7 Running Firewall Configuration: The Tactical Router **shall** provide access to the Firewall to bulk upload/download of the entire running firewall configuration.	X	
3.7.1.8 Ruleset Processing Rate: The Tactical Router firewall **shall** be able to process 150 dynamic rule-set updates per second.	X	
3.7.1.9 Operation During Rule-Set Update: The Tactical Router firewall shall continue packet handling during a dynamic rule-set update.	X	
3.7.1.10 Flexible Specification of Rule-sets: The Tactical Router firewall shall support flexible specification of the rule-set, providing for general rules, prefixes, operators and ranges less than or greater than.	X	
3.7.1.11 Firewall Traffic-Filter Protection Profile: The Tactical Router shall comply with the "U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments" version 1.1	X	
3.7.1.12 Concurrent Session Performance: The Tactical Router shall support a minimum of **100** concurrent session **of traffic analysis** through the firewall.	X	
3.7.1.13 Router Protection Profile: The Tactical Router shall comply with the "U.S. Government Router Protection Profile for Medium Robustness Environments"	X	
3.7.1.14 Router Protection Common Criteria: The Tactical Router firewall will be validated by a Common Criteria Test Lab as complying with the latest validated US Government Router Protection Profile for Medium Robustness environments or the latest validated Consistency Instruction Manual for development of US Government Protection Profiles for use in Medium robustness Environments.		X
3.7.1.15 Traffic Filter Common Criteria: The Tactical Router firewallwill be validated by a Common Criteria Test Lab as complying with the latest validated U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments.		X
3.7.2 Intrusion Detection		
3.7.2.1 Stateless Packet Filtering Rules: The Tactical Router shall provide the ability to establish rules that handle stateless packet filtering.	X	
3.7.2.2 Stateful Packet Filtering Rules: The Tactical Router shall provide the ability to establish rules that handle stateful packet filtering.	X	
3.7.2.3 Packet Inspection: The Tactical Router will be able to do both stateful and stateless packet inspection at the same time.	X	
3.7.2.4 Modification of IDS Rules: The Tactical Router will provide access to the IDS to set, add, remove, and modify an individual IDS rule.		X

Requirement	Core	Growth
3.7.2.5 Modification of IDS Rule Groups: The Tactical Router will provide access to the IDS to Create, add, remove, and modify an entire group of IDS rules.		X
3.7.2.6 Modification of IDS Logging: The Tactical Router will provide access to the IDS to Set, add, remove and modify IDS logging.		X
3.7.2.7 Modification of IDS SNMP Alert Configuration: The Tactical Router will provide access to the IDS to set, add, remove and modify IDS SNMP alert configuration.		X
3.7.2.8 IDS Running Configuration: The Tactical Router will provide access to the IDS to bulk upload/download of the entire running IDS configuration.		X
3.7.2.9 Network Attack Detection: The Tactical Router shall detect 95% of the known network attacks.		X
3.7.2.10 Analysis of Data Stream Rate: The Tactical Router shall support a full analysis of a data stream at a minimum of 10M**bits**/sec.		**X**
3.7.2.11 Intrusion Reporting: The Tactical Router will be able to report maximum 95% of intrusion events.		X
3.7.2.12 Network Attack Defense: The Tactical Router will be able to defend against 95% of the known network attacks.		X
3.7.2.13 Reserved		
3.7.2.14 Reserved		
3.7.2.15 Intrusion Logging: The Tactical Router shall log any potential intrusions via the Logging Function (syslog).	X	
3.7.2.16 SNMP Traps: The Tactical Router shall send an SNMP trap, within 5 seconds upon detection of any potential intrusions, to the SNMP manager.	X	
3.7.2.17 Protection Profile System Sensor Compliance: The Tactical Router shall comply with the Consistency Instruction Manual for development of US Government Protection Profiles for use in Medium robustness Environments" Release 3.0 or the latest validated Intrusion Detection System Sensor Protection for Medium Robustness Environments.		**X**
3.7.2.18 Protection Profile System Analyzer Compliance: The Tactical Router shall comply with the Consistency Instruction Manual for development of US Government Protection Profiles for use in Medium robustness Environments" Release 3.0 or the latest validated Intrusion Detection System Analyzer Protection for Medium Robustness Environments.		**X**
3.7.2.19 Intrusion Detection Sensor System Common Criteria Validation: The Tactical Router intrusion detection system will be validated by a Common Criteria Test Lab as complying with the latest validated Intrusion Detection System Sensor Protection for Medium Robustness Environments or the latest validated Consistency Instruction Manual for development of US Government Protection Profiles for use in Medium robustness Environments.	-	X
3.7.2.20 Intrusion Detection Analyzer System Common Criteria Validation: The Tactical Router intrusion detection system will be validated by a Common Criteria		X

Requirement	Core	Growth
Test Lab as complying with the latest validated Intrusion Detection System Analyzer Protection for Medium Robustness Environments or the Consistency Instruction Manual for development of US Government Protection Profiles for use in Medium robustness Environments.		
3.7.2.21 IDMEF: The Tactical Router shall use Intrusion Detection Message Exchange format (IDMEF) [RFC 4765] or Structure System Log open standard for IA event exchange (the intrusion event exchange drafts are in the process of being standardized).		X
3.7.2.21 IPv4 Intrusion Detection Functions: The Tactical Router shall support IPv4 intrusion detection functions.	X	
3.7.2.22 IPv6 Intrusion Detection Functions: The Tactical Router will support IPv6 intrusion detection functions.		X
3.7.2.23 Upgrade of the IDS Signature: The Tactical Router intrusion detection signature shall be software upgradeable.	X	
3.7.3 Router Access		
3.7.3.1 Disabling of BOOTP and HTTP: The Tactical Router **shall** support the selective disabling of BOOTP [RFC 951] and HTTP [RFC 2616] provisioning network services.	X	
3.7.3.2 DHCP on Physical and Logical Interfaces: The Tactical Router shall support DHCP on physical and logical interfaces [RFC 2131].	X	
3.7.3.3 DHCP Relay: The Tactical Router shall support DHCP relay on its Router interfaces [RFC 2131]	X	
3.7.3.4 Disabling of Physical Interfaces: The Tactical Router shall support selective disabling of any physical interface.	X	
3.7.3.5 Disabling of Logical Interfaces: The Tactical Router shall support selective disabling any logical interface.	X	
3.7.3.6 Diasbling of Sub-interfaces: The Tactical Router shall support selective disabling any sub-interfaces.	X	
3.7.4 Reserved		
3.7.5 Sanitization		
3.7.5.1 Sanitization Function: The Tactical Router shall support a sanitization function in accordance with the Defense Security Service (DSS) Clearing and Sanitization Matrix 2007-06-28.		X
3.7.5.2 AES File System: The Tactical Router shall provide a public key enabled 128-bit AES encrypted file-system for the operating system and router configurations.		X
3.7.5.3 Deletion of Encrypted File System: The Tactical Router shall provide a method of deleting the encrypted file-system key to sanitize the file-system.		X
3.7.5.4 Sanitization of Volitile Memory: The Tactical Router shall sanitize data in volatile memory before normal module shutdown and reset.		X

Requirement	Core	Growth
3.7.6 PKI		
3.7.6.1 PKI Function Compliance: The Tactical Router shall comply with DoD Tactical Public Key Infrastructure (PKI) for all PKI-enabled functions as specified in DODI 8520.2 and X.509 Certificate Policy for the United States Department of Defense	X	
3.7.6.2 PKI Interface: The Tactical Router shall provide an interface for managing its PKI-enabled capabilities including setting up trusted root certificates.	X	
3.7.6.3 SSH Interface: If the Tactical Router employs a PKI-enabled protocol Secure Shell (SSH) for its management interface, the router shall provide an interface for managing its PKI-enabled capabilities including setting up trusted root certificates and importing its public and private keys.	**X**	
3.7.6.4 SSH Certificate and CRL Retreival If the Tactical Router employs a PKI-enabled protocol (SSH) for its management interface, the router shall be able to retrieve certificates and Certificate Revocation Lists (CRL) from a directory and perform path validation.	X	
3.7.6.5 Storing Private Keys: If the Tactical Router management interface employs PKI, the Tactical Router shall use the RSA Laboratories Public Key Cryptography Standard 12, Personal Information Exchange Syntax Standard, version 1.0 (Draft), 30 April 1997, for storing private key material that is unprotected by hardware means.	X	
3.7.6.6 Entity Authentication: If the Tactical Router management interface employs PKI, the Tactical Router shall support entity authentication in compliance with FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997.	X	
3.7.6.7 Digitally Signed Data Format: The Tactical Router digitally signed data shall comply with the format specified for PKI-based signatures in IETF RFC-2315, (Public Key Cryptography Standard (PKCS) #7, Cryptographic Message Syntax, Version 1.5, March 1998).		**X**
3.7.7 Access Control		
3.7.7.1 RADIUS Accounting: The Tactical Router will support the Remote Authentication Dial In User Service (RADIUS) based accounting for Authentication, Authorization and Accounting (AAA), [RFC 2865] and [RFC 2866].		X
~~**3.7.7.2 Diameter Authentication: The Tactical Router will support the Diameter based protocol authentication for AAA. [RFC 3588].**~~	-	~~**X**~~
~~**3.7.7.3 Diameter Accounting: The Tactical Router will support the Diameter protocol for accounting for AAA [RFC 3588].**~~	-	~~**X**~~
3.8 Configuration		
3.8.1 Configuration Modification		
3.8.1.1 Stand Alone Configuration Modification: The Tactical Router **shall** be capable of being modified while in a standalone configuration.	X	

Requirement	Core	Growth
3.8.1.2 Network Connected Configuration Modification: The Tactical Router **shall** be capable of being modified through network connectivity	X	
3.8.1.3 Configuration Modification while Operating: The Tactical Router **shall** be capable of being modified while operating from a previously stored configuration.	X	
3.8.2 Configuration Files		
3.8.2.1 Previously Laoded Configuration: The Tactical Router shall be able to start from a previously loaded configuration.	X	
3.8.2.2 Reload With a New Configuration: The Tactical Router shall be able to be reloaded with a new configuration from an operational state.	X	
3.8.2.3 Multiple Configuration Files: The Tactical Router shall support multiple configuration files	X	
3.8.2.4 Configuration File Readibility: The Tactical Router configuration files shall be in human readable form.		X
3.8.2.5 Dymnamic Configuration: The Tactical Router shall be able to be configured dynamically (i.e. while it is already routing traffic).	X	
3.8.2.6 Hardware Version Number: The Tactical Router shall be capable of displaying the hardware Version number.	X	
3.8.2.7 Software Version Number: The Tactical Router shall be capable of displaying the software Version number.	X	
3.8.2.8 Initialization on Power Up: The Tactical Router shall start its initialization process when power is applied.	X	
3.8.2.9 Automatic Operational State: The Tactical Router shall reach the full operational state without operator intervention.	X	
3.8.2.10 Load of Previous Configuration: The Tactical Router shall load the configuration used the last time it was saved.	X	
3.8.2.11 Configuration Load During Start Up: The Tactical Router configuration shall be loaded during start-up.	X	
3.8.2.12 The Tactical Router configuration shall be able to be loaded during run time.	X	
3.8.2.13 Configuration Modification during Run Time: The Tactical Router configuration shall be able to be modified during run time.	X	
3.8.3 Configuration Interface		
3.8.3.1 Configuration From Network interface: The Tactical Router must have the capability to be configured while operational and connected to a network.	X	
3.8.3.2 Configuration From Stand Alone: The Tactical Router must have the capability to be configured when in a standalone configuration.	X	
3.8.3.3 Configuration From the Console Port: The Tactical Router shall be able to be configured from a non-configured state without network connectivity through the console port.	X	

Requirement	Core	Growth
3.9 Network Management		
3.9.1 Management from an Network Management Station: The Tactical Router shall be able to be managed remotely from a network management station.	X	
3.9.2 Management from a Local Management Station: The Tactical Router shall be able to be configured from a local management station.	X	
3.9.3 User Authentication Prior to Configuration: The Tactical Router shall authenticate users prior to permitting router configuration to ensure the user attempting to configure the Router is valid.	X	
3.9.4 Configuration Security: Management and configuration of the Tactical Router shall be executed through a secure protocol.	X	
3.9.5 SNMP: The Tactical Router shall support an Simple Network Management Protocol version 3 (SNMP V3) [RFC 3411], [RFC 3412], [RFC 3413], [RFC 3414], emerging [RFC 3415], and [RFC 3418].	X	
3.9.6 SSHv2: The Tactical Router shall support Secure Shell version 2 (SSHv2) [RFC 4742].	X	
3.9.7 CA Operations: The Tactical Router shall be able to retrieve certificates and Certificate Revocation Lists (CRL) from a Certificate Authority (CA) and perform certification path validation.	X	
3.10 System Software		
3.10. 1 System Software Upgrade		
3.10.1.1 Secure System Software Upgrade: The Tactical Router shall support a secure method to upgrade its operating system.	X	
3.10.2 Debug Capability		
3.10.2.1 Troubleshooting: The Tactical Router shall provide debug features to troubleshoot routing functionality.	X	
3.10.2.2 Debug Toggling: The Tactical Router shall allow the debug function to be able to be toggled ON or OFF in real time.	X	
3.10.2.3 Debug Output Readable: The Tactical Router debug output shall be in a human readable format.	X	
3.10.2.4 NTP: The Tactical Router shall support Network Time Protocol (NTP) [RFC 1305] for timestamps on debug messages and log files.	X	
3.11 HW Performance		
3.11.1 Minimum Throughput Required: The Tactical Router shall support a minimum throughput of 2MB bits per second at 64 bytes packet size with Multicast and QoS features of 3.6.1, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9 and 3.6.11 are enabled.	X	
3.11.2 Throughput: The Tactical Router will support a throughput of **up to** 500K packets per second at 64 bytes packet size with Multicast and QoS features of 3.6.1, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9 and 3.6.11 are enabled.		X

Requirement	Core	Growth
3.12 Electrical Characteristics		
3.12.1 Maximum Power Consumption Required: The Tactical Router shall consume no more than 50 watts when powerd by 28V DC vehicle power.	X	
3.12.2 Vehicle Power: The Tactical Router shall accept power from 28V DC vehicle power IAW the power quality standards of MIL-STD-1275D.	X	
3.12.3. Maximum Power Consumption: The Tactical Router swill consume no more than 20 watts when powerd by 28V DC vehicle power.		X
3.13 Mechanical Characteristics		
3.13.1 Dimensions and Weight		
3.13.1.1 Maximum Volume Required: The Tactical Router shall not exceed 300 cubic inches in volume excluding cables.	X	
3.13.1.2 Maximum Volume: The Tactical Router will not exceed 100 cubic inches in volume excluding cables.		X
3.13.1.3 Maximum Weight Required The weight of the Tactical Router shall not exceed ten (10) lbs excluding cables.	X	
3.13.1.4 Maximum Weight: The weight of the Tactical Router will not exceed 6 lbs excluding cables.		X
3.14 Environmental		
3.14.1 Temperature		
3.14.1.1 Operating Temperature: The Tactical Router shall be capable of operating in temperatures between -25 degrees F and +125 degrees F IAW MIL-STD-810F, Method 501.4, Procedure II (for High Temperature); MIL-STD-810F, Method 502.4, Procedure II (for Low Temperature).	X	
3.14.1.2 Non-operating Temperature: The Tactical Router packaged for shipping shall not sustain physical or electrical damage or performance degradation as a result of being exposed to non-operating external temperatures between -28 degrees Fahrenheit (F) and +160 degrees F IAW MIL-STD-810F, Method 501.4, Procedure I (High Temperature) and Method 502.4, Procedure I (Low Temperature).	X	
3.14.2 Humidity		
3.14.2.1 High Humidity: The Tactical Router shall operate without performance degradation during and after prolonged exposure to relative humidity as high as 95% at all air temperatures up to 105°F, and as low as 5% at temperatures up to 120 °F IAW MIL-STD-810F, Method 507.4.	X	
3.14.3 Altitude		
3.14.3.1 Operating Altitude: The Tactical Router shall be capable of operating at altitudes from sea level to 22,000 ft above sea level IAW MIL-STD-810F, Method 500.4, Procedure II.	X	

Requirement	Core	Growth
3.14.3.2 Non-operating Altitude: The Tactical Router shall withstand a non-operating (i.e. storage or transit) altitude range from sea level to 40,000 ft above sea level with the rate of change of altitudes not exceeding 2500 ft per minute IAW MIL-STD-810F, Method 500.4, Procedure I.	X	
3.14.4 Sand and Dust		
3.14.4.1 Dust Accumulation: The Tactical Router in their operational configurations shall be resistant to dust that may accumulate within the enclosure as a result of operator activities IAW MIL-STD-810F, Method 510.4, Procedure III.	X	
3.14.5 Salt Fog		
3.14.5.1 Exposure to Salt Fog: The Tactical Router in their operational configurations shall show no signs of physical or electrical damage or performance degradation when exposed to alternate 24-hour periods of salt fog exposure and standard ambient conditions for a minimum of four 24-hour periods IAW MIL-STD-810F, Method 509.4.	X	
3.14.6 Shock		
3.14.6.1 Functional Shock: The Tactical Router, in its operational configuration, shall show no sign physical or electrical damage that would impair operation or performance or cause degradation following exposure to a shock pulse with a peak acceleration of 20 g's for 11 ms IAW MIL-STD-810F, Method 516.5, Procedure I, Figure 516.5-10 and Table II.	X	
3.14.6.2 Transit Drop: The Tactical Router in its transportable configurations (packaged in transport cases) shall show no signs of physical or electrical damage that would impair operation or performance or cause degradation following a 30-inch drop on each face, edge, and corner IAW MIL-STD-810F, Method 516.5, Procedure IV Table 516.5-VI.	X	
3.14.6.3 Transportation Shock: The Tactical Router (packaged for transportation) shall operate after the shock loads generated by the rail impact test, in their transportable configuration IAW MIL-STD-810F, Method 516.5, Procedure VII.	X	
3.14.7.1 Operational: The Tactical Router in its transit (operational) configurations shall operate during and after vibration testing without degradation per MIL-STD-810F, Method 514.5, Procedure I, (Ground mobile) Operational, Category 20, Figure 514.5C-3, 30 minutes per axis.	X	
3.14.7.2 Non-Operational Truck Transport: There **shall** be no physical or electrical damage or performance degradation to the Tactical Router in its transportable configurations (non-operational), due to exposure to the random truck vibration environment as defined in MIL-STD-810F, Method 514.5, category 4, figure 514.5C-1 and using the values of table 514.5C-VII for vertical, transverse (lateral) and longitudinal (forward and aft) spectrums with an exposure duration of 4.0 hour per axis.	X	
3.14.7.3 Non-Operational Rail Transport: In its transportable (non-operational) configuration, the Tactical Router shall operate after the random vibration	X	

Requirement	Core	Growth
environment of MIL-STD-810F, Method 514.5, Category 11 (Train), Figure 514.5C-7. Exposure duration shall be 2.0 hour in each of 3 orthogonal axis.		
3.14.7.4 Non-Operational Aircraft Transport: In its transportable (non-operational) configuration, the Tactical Router shall operate after the random vibration environment of MIL-STD-810F, Method 514.5, Category 11 (Train), figure 514.5C-7. Exposure duration shall be 2.0 hour in each of 3 orthogonal axis.	X	
3.14.7.5 Non-Operational Helicopter Transport: In its transportable (non-operational) configuration, the Tactical Router shall operate after the random vibration environment of MIL-STD-810F, Method 514.5, Category 14 (Helicopter), Figure 514.5C-10 using the values of table 514.5C-IV for CH-47D helicopter to determine main rotor frequencies. Exposure duration shall be 4 hours in each of 3 orthogonal axis.	X	
3.14.8 Fungus		
3.14.8 Fungus Resistance: The Tactical Router shall be resistant to fungi.	X	
3.14.9 Electromagnetic Interference/Compatibility		
3.14.9.1 EMI/EMC The Tactical Router shall comply with the electromagnetic interference (EMI) and electromagnetic compatibility (EMC) requirements for Federal Communications Commission (FCC) Class A equipment IAW Code of Federal Regulations Title 47 Part 15.	X	
3.14.9.2 Conducted and Radiated Susceptibility: The Tactical Router shall comply with CE102, CS101, CS114, CS115, CS116, RE102, RS103 requirements of MIL-STD-461E.	X	
3.14.10 Electromagnetic Pulse		
3.14.10.1 HAEMP: The Tactical Router shall be protected from High-Altitude Electromagnetic Pulse (HAEMP) as defined in MIL-STD-2169.	X	
3.14.11 Lightning Protection		
3.14.11.1 Near Strikes: The Tactical Router shall be protected from a Near Strike Lightning (NSL) environment as specified in MIL-STD-464.	X	
3.15 Reliability and Maintainability		
3.15.1 Reliability		
3.15.1.1 MTBF: The Tactical Router shall have a Mean Time Between Failures (MTBF) of not less than 40,000 hours, based upon the MIL-HDBK-217 basic reliability model (all equipment accounted for serially), calculated in hours in a ground fixed operating mode and a local ambient temperature of 50°C.	X	
3.15.2 Maintainability		
3.15.2.1 MTTR: The Tactical Router shall have a Mean Time to Repair (MTTR) no more than 0.25 hours.	X	
3.15.2.2 Maintenance Concept: The Integrated Logistics Support Maintenance	X	

Requirement	Core	Growth
Concept applicable to the Tactical Router shall be "repaired by replacement".		
3.15.2.2 Special Tools: No special tool shall be required for maintaining the unit.	X	
3.15.2.3 Scheduled Maintenance: The Tactical Router shall require no scheduled maintenance or adjustment.	X	
3.16 Safety		
3.16.1 Electrical Safety	X	
3.16.2.1 Incorrect Power or Voltage Levels The Tactical Router with multiple-input power capabilities shall be protected from damage when connected to incorrect input power/voltage levels.	X	
3.16.2.2 National Electric Code: The Tactical Router shall meet the requirements of the National Electrical Code, NFPA 70-2005	X	
3.16.2.3 Protection from Electric Shock: The Tactical Router shall be designed so that under all conditions of normal use (installation, operation, and maintenance) and under a likely fault condition (including human error), it protects against the risk of electric shock and other hazards.	X	
3.16.3 Mechanical Safety	X	
3.16.3.1 Personnel Safety: The equipment/configuration design shall provide personnel with safe access for installation, operation, and maintenance tasks.	X	
3.16.3.2 Temperature Limits: Operator accessible parts shall comply with the temperature limits in UL 60950, Section 4.5.1, Table 4B, part 2.	X	
3.16.3. Physical Stability: Following initial setup, equipment shall remain physically stable for use under operational conditions, including normal use, wind loading, inclined, at the halt	X	
3.16.4 Safety Marking and Labels	X	
3.16.4.1 Marking of Potentail Hazards: Safety markings and labels shall be provided identifying any potential hazards to personnel.	X	
3.16.4.2 Safety markings and Labels: Safety markings and labels shall comply with either section 1.7 of UL 60950 or ANSI Z535.4.	X	
3.16.4.3 Visibility of Safety markings: Markings shall be readily visible, including when a barrier or access door is opened/removed.	X	
3.16.5 Chemical Safety	X	
3.16.5.1 Hazardous Chemical Exposure: Hazardous chemical exposure to personnel shall be controlled to levels below the Occupational Safety and Health Administration (OSHA) Permissible Exposure Limits and the American Conference of Governmental Industrial Hygienists (ACGIH) Threshold Limit Values (TLV).	X	
3.16.5.2 Ozone Depleting Substances: Class 1 and Class 2 Ozone depleting substances shall not be used. (Refer to Clean Air Act Amendment Title V1, Section 602.)	X	

Requirement	Core	Growth
3.16.6 Environmental Safety	X	
3.16.6.1 Hazardous Material Exposure: Hazardous material exposure to personnel shall be controlled to levels below the OSHA Code of Federal Regulations 1910 Permissible Exposure Limits and the ACGIH Threshold Limit Values.	X	
3.17 Human Factors		
3.17.1 Frequently used Controls: The most frequently used controls shall be directly accessible.	X	
3.17.2 HFE Concepts: The Tactical Router shall employ Human Factors Engineering (HFE) concepts using MIL-STD-1472F as a guideline.	X	
3.17.3 Accidental Actuation: Controls shall be designed to prevent accidental actuation in accordance with MIL-STD-1472F, paragraph 5.4.1.8.	X	
3.17.3 Control Spacing: Minimum spacing between controls shall be in accordance with MIL-STD-1472F, paragraph 5.4.1.3.7.	X	
3.17.4 Connector Spacing: Minimum spacing between connectors shall be in accordance with MIL-STD-1472F Table VII and paragraph 5.9.14.7.	X	
3.17.5 Control Operation with Hand Wear: Controls shall be compatible with hand wear to be used in all anticipated environments.	X	
3.17.6 Accessibility of Controls and Displays: Operator controls and displays shall be readily accessible during operations.	X	
3.17.7 Critical and Frequently Used Controls: Critical and frequently used controls shall be the most accessible	X	
3.17.8 Connector Spacing for 8P8C Connectors: 8P8C (ISO 8877:1992) connectors shall have a minimum clearance of 25mm between the male connector latching tab and any portion of the router chassis above the latching tab to facilitate connector insertion and removal.	X	

3.18 TERMINOLOGY

3.18.1 SUPPORT: The term support is used consistently in this specification in reference to features of protocols and standards. In this context the terms "support" and supports" mean that the router incorporates these features into its design and operation and will interoperate with other equipment using the same protocol or standard when the router and such other equipment are properly configured to incorporate cited features of the protocol or standard as called out in the refernced document.

Table 4.1 Verification Method	Core	Growth	Proposal	Phase II	LBRR
Table 4.1 Verification Method					
This table indicates the verification method to be used for the NIE and for Production. A T in the event column indicates the verification is to be conducted with a test of the capability. The Letter D in the event column indicates the verification will be conducted by reviewing contractor supplied supporting documentation and certifications.					
3.1 Interfaces					
3.1.1 Loopback Interface	X		D		
3.1.2 Routed Ports	X				
3.1.3 Switched Ports	X				
3.1.4 Auto MDIx	X				
3.1.5 Console Port	X				
3.2 Layer 2					
3.2.1 VLAN	X		D		
3.2.2 Priority Queuing	X		D		
3.2.3 PPP	X				
3.2.4 EAP/PEAP	X				
3.2.5 EAPOL		**X**			
3.2.6 Fast Ethernet	X		D		
3.3 Layer 3					
3.3.1 Route Redistribution					
3.3.1.1 Route Distribution	X		D		
3.3.1.2 RIPv2 and OSPFv2 Route Filtering	X		D	T	
3.3.1.3 Default Address Filtering	X		D		
3.3.1.4 Static Routing	X		D	T	
3.3.1.5 Static Default Address	X		D		
3.3.1.6 Route Summarization	X		D		
3.3.1.7 Route Redistribution	X		D	T	
3.3.1.8 Default Address Distribution	X		D		
3.3.2 Other Protocols					
3.3.2.1 Overhead Reduction		X			
3.3.2.2 UDP	X		D		
3.3.2.3 TCP	X		D		
3.3.3 IPv4					
3.3.3.1 IP	X				
3.3.3.2 ARP	X				
3.3.3.3 IP Broadcast Transfers	X				

Table 4.1 Verification Method	Core	Growth	Proposal	Phase II	LBRR
3.3.3.4 IP Broadcast Transfers in Subnets	X				
3.3.3.5 ICMP Router Discovery	X		D	T	
3.3.3.6 BOOTP	X				
3.3.3.7 ICMP	X				
3.3.3.8 NAT/PAT		X			
3.3.3.9 PPPoE	X		D	T	
3.3.4 IPv6					
3.3.4.1 IPv6		X			
3.3.4.2 IPv6 Aggregate Global Unicast		X			
3.3.4.3 IPv6		X			
3.3.4.4 IPv6 Neighbor Discovery		X			
3.3.4.5 IPv6 Stateless Address Auto Configuration		X			
3.3.4.6 ICMPv6 for IPv6		X			
3.3.4.7 IPv6 Data Transfer		X			
3.3.4.8 Privacy Extension for Stateless Auto Configuration		X			
3.3.4.9 IPv6 over PPP		X			
3.3.4.10 IPv6 Global Address		X			
3.3.4.11 IPv6 Flow Label Specification		X			
3.3.5 Tunneling					
3.3.5.1 RSVP Tunneling		X			
3.3.5.2 Reserve Bandwidth Exclusion		X			
3.3.5.3. DSCP Data	X		D	T	
3.3.5.4 RSVP		X			
3.3.5.5 IPSec	X		D		
3.3.5.6 IPv4 Tunneling	X		D		
3.3.5.7 IPv6 Tunneling		X			
3.3.5.8 GRE	X		D		
3.4 Multicast					
3.4 1 Port Mirroring	X		D	T	
3.4.2 IP Multicast Routing	X				
3.4.3 Static Provisioning of IP Multicast Routing	X		D	T	
3.4.4 IGMP Transfers	X				
3.4.5 IP Multicast Host Extensions	X				
3.4.6 Multicast on all Interfaces	X				
3.4.7 PIM-SM	X		D	T	
3.4.8 PIM-DM	X		D	T	
3.4.9 MLD		X			
3.4.10 IGMPv3	X		D	T	
3.4.11 Source Specific Multicast	X				

Table 4.1 Verification Method	Core	Growth	Proposal	Phase II	LBRR
3.4 12 PIM-SM ASM	X				
3.4.13 Multicast Packet Replication	X				
3.4.14 MSDP	X				
~~3.4.15 IGMPv3 Proxy~~	~~X~~	~~-~~	~~D~~	~~T~~	
3.4.16 MLD Proxy		X			
3.5 Routing					
3.5.1 RIP					
3.5.1.1 RIPv2	X		D	T	
3.5.1.2. RIPv2 MIB	X		D	T	
3.5.1.3 RIPv2 MD5	X		D	T	
3.5.1.4 RIP/NG		X			
3.5.2 OSPFv2					
3.5.2.1 OSPFv2	X		D	T	
3.5.2.2 Stub Router Advertisement	X		D	T	
3.5.2.3 NSSA	X				
3.5.2.4 OSPFv2 MIB	X				
3.5.2.5 BGP-OSPF Interaction		X			
3.5.3 OSPFv3					
3.5.3.1 OSPFv3		X			
3.5.3.2 OSPFv3 MIB		X			
3.5.3.3 OSPFv3 Route Exchanges		X			
3.5.3.4 Link Cost Calculation		X			
3.5.3.5 Destination IPv4 Address		X			
3.5.3.6 Destination IPv6 Address		X			
3.5.3.7 Address Families		X			
3.5.4 BGP					
3.5.4.1 BGP4		X			
3.5.4.2 Capabilities Advertisment		X			
3.5.4.3 Autonomous System Configuration		X			
3.5.4.4 Routes Refresh		X			
3.5.4.5 Routes Reflection		X			
3.5.4.6 BGP4 Extension for IPv6		X			
3.5.4.7 Route Aggregation		X			
3.5.4.8 Route Flap Damping		X			
3.5.4.9 BGP Protection		X			
3.5.4.10 BGP Communities Attributes		X			
3.5.4.11 M-BGP		X			
3.5.4.12 Route Exchange over OSPF		X			
3.6 QoS					
3.6.1 DSCP IPv4 Marking	X		D	T	

Table 4.1 Verification Method	Core	Growth	Proposal	Phase II	LBRR
3.6.2 DSCP IPv6 Marking		X			
3.6.3 Deep Packet Inspection	X				
3.6.4 Multiple DSCP Classes	X				
3.6.5 Packet Filtering	X				
3.6.6 DiffServ Architecture	X		D		
3.6.7 EF PHB	X		D	T	
3.6.8 AF PHB	X		D	T	
3.6.9 Integrated Services Architecture	X				
3.6.10 Traffic Prioritization	X		D	T	
3.6.11 Egress Queuing	X				
3.6.12 Queuing Classes	X		D		
3.6.13 RED Queuing Classes	X				
3.6.14 QoS Queues	X		D		
3.6.15 Queue Prioritization	X				
3.6.16 Queue Management Techniques	X		D		
3.6.17 Credit Based Flow Control	X		D		
3.6.18 Queue Management In the Configuration	X				
3.7 Security					
3.7.1 Firewall					
3.7.1.1 Modification of Firewall Rules	X		D		
3.7.1.2 Modification of Firewall Rule-sets	X		D		
3.7.1 .3 Modification of Firewall Packet Acounting Rules	X				
3.7.1.4 Packet Acounting	X		D		
3.7.1.5 Packet Logging	X				
3.7.1.6 Firewall SNMP Alert Configuration	X				
3.7.1.7 Running Firewall Configuration	X				
3.7.1.8 Ruleset Processing Rate	X				
3.7.1.9 Operation During Rule-Set Update	X				
3.7.1.10 Flexible Specification of Rule-sets	X				
3.7.1.11 Firewall Traffic-Filter Protection Profile	X				
3.7.1.12 Concurrent Session Performance	X				
3.7.1.13 Router Protection Profile	X				
3.7.1.14 Router Protection Common Criteria		X			
3.7.1.15 Traffic Filter Common Criteria		X			
3.7.2 Intrusion Detection					
3.7.2.1 Stateless Packet Filtering Rules	X		D		
3.7.2.2 Stateful Packet Filtering Rules	X		D		
3.7.2.3 Packet Inspection	X		D		
3.7.2.4 Modification of IDS Rules		X			

Table 4.1 Verification Method	Core	Growth	Proposal	Phase II	LBRR
3.7.2.5 Modification of IDS Rule Groups		X			
3.7.2.6 Modification of IDS Logging		X			
3.7.2.7 Modification of IDS SNMP Alert Configuration		X	D		
3.7.2.8 IDS Running Configuration		X	D		
3.7.2.9 Network Attack Detection		X			T
3.7.2.10 Analysis of Data Stream Rate		**X**			
3.7.2.11 Intrusion Reporting		X			T
3.7.2.12 Network Attack Defense		X			T
3.7.2.13 Reserved					
3.7.2.14 Reserved					
3.7.2.15 Intrusion Logging	X		D		
3.7.2.16 SNMP Traps	X		D		
3.7.2.17 Protection Profile System Sensor Compliance		**X**			
3.7.2.18 Protection Profile System Analyzer Compliance		**X**			
3.7.2.19 Intrusion Detection Sensor System Common Criteria Validation	-	X			
3.7.2.20 Intrusion Detection Analyzer System Common Criteria Validation	-	X			
3.7.2.21 IDMEF		**X**			
3.7.2.21 IPv4 Intrusion Detection Functions	X		D		
3.7.2.22 IPv6 Intrusion Detection Functions		X			
3.7.2.23 Upgrade of the IDS Signature	X				
3.7.3 Router Access					
3.7.3.1 Disabling of BOOTP and HTTP	X		D	T	
3.7.3.2 DHCP on Physical and Logical Interfaces	X		D	T	
3.7.3.3 DHCP Relay	X				
3.7.3.4 Disabling of Physical Interfaces	X		D	T	
3.7.3.5 Disabling of Logical Interfaces	X				
3.7.3.6 Diasbling of Sub-interfaces	X				
3.7.4 Reserved					
3.7.5 Sanitization					
3.7.5.1 Sanitization Function		**X**			
3.7.5.2 AES File System		**X**			
3.7.5.3 Deletion of Encrypted File System		**X**			
3.7.5.4 Sanitization of Volitile Memory		**X**			
3.7.6 PKI					
3.7.6.1 PKI Function Compliance	X		D		

Table 4.1 Verification Method	Core	Growth	Proposal	Phase II	LBRR
3.7.6.2 PKI Interface	X				
3.7.6.3 SSH Interface	**X**				
3.7.6.4 SSH Certificate and CRL Retreival	X				
3.7.6.5 Storing Private Keys	X		D		
3.7.6.6 Entity Authentication	X				
3.7.6.7 Digitally Signed Data Format		**X**			
3.7.7 Access Control					
3.7.7.1 RADIUS Accounting		X			
~~**3.7.7.2 Diameter Authentication**~~	-	~~**X**~~			
~~**3.7.7.3 Diameter Accounting**~~	-	~~**X**~~			
3.8 Configuration					
3.8.1 Configuration Modification					
3.8.1.1 Stand Alone Configuration Modification	X				
3.8.1.2 Network Connected Configuration Modification	X		D		
3.8.1.3 Configuration Modification while Operating	X		D	T	
3.8.2 Configuration Files					
3.8.2.1 Previously Loaded Configuration	X		D	T	
3.8.2.2 Reload With a New Configuration	X		D		
3.8.2.3 Multiple Configuration Files	X				
3.8.2.4 Configuration File Readibility		X			
3.8.2.5 Dymnamic Configuration	X		D		
3.8.2.6 Hardware Version Number	X				
3.8.2.7 Software Version Number	X				
3.8.2.8 Initialization on Power Up	X				
3.8.2.9 Automatic Operational State	X		D		
3.8.2.10 Load of Previous Configuration	X				
3.8.2.11 Configuration Load During Start Up	X				
3.8.2.12 Configuration Load During Run Time	X				
3.8.2.13 Configuration Modification During Run Time	X		D	T	
3.8.3 Configuration Interface					
3.8.3.1 Configuration From Network interface	X		D	T	
3.8.3.2 Configuration From Stand Alone	X				
3.8.3.3 Configuration From the Console Port	X				
3.9 Network Management					
3.9.1 Management from an Network Management Station	X		D		
3.9.2 Management from a Local Management	X				

Table 4.1 Verification Method	Core	Growth	Proposal	Phase II	LBRR
Station					
3.9.3 User Authentication Prior to Configuration	X				
3.9.4 Configuration Security	X				
3.9.5 SNMP	X				
3.9.6 SSHv2	X				
3.9.7 CA Operations	X				
3.10 System Software					
3.10. 1 System Software Upgrade					
3.10.1.1 Secure System Software Upgrade	X		D		
3.10.2 Debug Capability					
3.10.2.1 Troubleshooting	X		D		
3.10.2.2 Debug Toggling	X				
3.10.2.3 Debug Output Readable	X		D		
3.10.2.4 NTP	X				
3.11 HW Performance					
3.11.1 Minimum Throughput Required	X		D		
3.11.2 Minimum Throughput		X			
3.12 Electrical Characteristics					
3.12.1 Maximum Power Consumption Required	X		D	T	
3.12.2 Vehicle Power	X		D		
3.12.3 Maximum Power Consumption		X			
3.13 Mechanical Characteristics					
3.13.1 Dimensions and Weight					
3.13.1.1 Maximum Volume Required	X		D		
3.13.1.2 Maximum Volume		X			
3.13.1.3 Maximum Weight Required	X		D		
3.13.1.4 Maximum Weight		X			
3.14 Environmental					
3.14.1 Temperature					
3.14.1.1 Operating Temperature	X		D		
3.14.1.2 Non-operating Temperature	X		D		
3.14.2 Humidity					
3.14.2.1 High Humidity	X		D		
3.14.3 Altitude					
3.14.3.1 Operating Altitude	X		D		
3.14.3.2 Non-operating Altitude	X		D		
3.14.4 Sand and Dust					
3.14.4.1 Dust Accumulation	X		D		
3.14.5 Salt Fog			D		
3.14.5.1 Exposure to Salt Fog	X				

Table 4.1 Verification Method	Core	Growth	Proposal	Phase II	LBRR
3.14.6 Shock					
3.14.6.1 Functional Shock	X		D		
3.14.6.2 Transit Drop	X				
3.14.6.3 Transportation Shock	X				
3.14.7.1 Operational	X		D		
3.14.7.2 Non-Operational Truck Transport	X				
3.14.7.3 Non-Operational Rail Transport	X				
3.14.7.4 Non-Operational Aircraft Transport	X				
3.14.7.5 Non-Operational Helicopter Transport	X				
3.14.8 Fungus					
3.14.8 Fungus Resistance	X		D		
3.14.9 Electromagnetic Interference/Compatibility					
3.14.9.1 EMI/EMC	X		D		
3.14.9.2 Conducted and Radiated Susceptibility	X		D		
3.14.10 Electromagnetic Pulse					
3.14.10.1 HAEMP	X				
3.14.11 Lightning Protection					
3.14.11.1 Near Strikes	X				
3.15 Reliability and Maintainability					
3.15.1 Reliability			D		
3.15.1.1 MTBF	X				
3.15.2 Maintainability					
3.15.2.1 MTTR	X				
3.15.2.2 Maintenance Concept	X				
3.15.2.2 Special Tools	X				
3.15.2.3 Scheduled Maintenance	X				
3.16 Safety					
3.16.1 Electrical Safety	X		D		
3.16.2.1 Incorrect Power or Voltage Levels	X				
3.16.2.2 National Electric Code	X				
3.16.2.3 Protection from Electric Shock	X				
3.16.3 Mechanical Safety	X				
3.16.3.1 Personnel Safety	X				
3.16.3.2 Temperature Limits	X		D		
3.16.3. Physical Stability	X				
3.16.4 Safety Marking and Labels	X				
3.16.4.1 Marking of Potentail Hazards	X				
3.16.4.2 Safety markings and Labels	X		D		
3.16.4.3 Visibility of Safety markings	X				

Table 4.1 Verification Method	Core	Growth	Proposal	Phase II	LBRR
3.16.5 Chemical Safety	X				
3.16.5.1 Hazardous Chemical Exposure	X				
3.16.5.2 Ozone Depleting Substances	X				
3.16.6 Environmental Safety	X				
3.16.5. Hazardous Material Exposure	X				
3.17 Human Factors	X				
3.17.1 Frequently used Controls	X				
3.17.2 HFE Concepts	X				
3.17.3 Accidental Actuation	X		D	T	
3.17.3 Control Spacing	X				
3.17.4 Connector Spacing	X				
3.17.5 Control Operation with Hand Wear	X				
3.17.6 Accessibility of Controls and Displays	X				
3.17.7 Critical and Frequently Used Controls	X				
3.17.7 Connector Spacing for 8P8C Connectors	X		D	T	