US Army Network Security Reference Architecture

(Aligned to the DoD Enterprise)

Version 1.0 1 August 2013

Executive Summary

The objectives of this Network Security Architecture are to reduce network complexity, minimize the network attack surface and standardize network security. By reducing and centralizing the number security stacks, the architecture improves network performance and creates efficiencies. The architecture is aligned with the objectives of the Joint Information Environment (JIE) and will initially consist of 11 dual security "stacks" in the Continental United States (CONUS) that are organized to protect posts/camps/stations in 5 CONUS regions. The stack architecture is modeled from security in use today at the Pentagon which evolved from the consolidation of multiple networks previously operated by multiple Departments and Agencies. Besides the ability to provide security at increased speed and capacity on an upgraded backbone network, notable capabilities of the security architecture include the ability to offer virtual stacks to Joint Service, Reserve Component and potentially Coalition partners and the ability to incrementally add capacity if necessary.

Network Security provided at the regional boundaries will be owned, operated and maintained by the Defense Information Systems Agency while Army (and potentially other Joint Services) would maintain their Title X responsibilities of configuring Service-specific security settings.

The scope of this architecture includes all network security controls that will be deployed on the LandWarNet extending down from the Defense Information Systems Network (DISN) to every end user, device and networked equipment connected to the Non-Classified Internet Protocol Network (NIPRNET). This includes LandWarNet ingress/egress points to the NIPRNET and Internet, Army data centers, processing nodes and every Post/Camp/Station where Army is the executive agent or responsible for providing Command, Control, Communication, Computers and Information Management (C4IM) services.

It is not in scope of this document to address the Secure Internet Protocol Network (SIPRNET) or the tactical (non-fixed) network environment. Both of these networks will be addressed in future increments of the architecture.

Under the JIE initiative, a Single Security Architecture (SSA) and Network Optimization Reference Architecture (NORA) are being defined and developed for the Department of Defense (DoD) Enterprise. The architectural rules within this architecture are consistent with the desired outcomes of both the SSA and NORA. It is not the intent of this architecture to duplicate JIE architectures. Rather, this architecture is intended to reference or adopt JIE architectures where applicable and discuss architectural rules that the Army must adhere to now to improve its network security and ensure Army is postured to leverage JIE capabilities as they emerge.

BLOHM.GARY.W.1228949589

Digitally signed by BLOHM.GARY.W.1228949589
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=BLOHM.GARY.W.1228949589
Date: 2013.08.01 13:04:38 -04'00'

Gary W. Blohm
Director of Army Enterprise Architecture

Table of Contents

Executive Summary ..... **i**
1 Introduction **3**
1.1 Background 3
1.2 Purpose and Scope of this Document 3
1.3 Key Authoritative Sources and Draft Documents 4
1.4 Document Structure 4
2 Current and Objective Network Security Posture **5**
2.1 Current Army Network Security Posture 5
2.2 Objective Army Network Security Posture 6
2.3 Transitional Assumptions and Constraints 8
3 Army Network Security Guiding Principles and Rules **8**
3.1 Army Network Security Guiding Principles 8
3.2 Operational Rules 9
3.3 Army Network Security Rules 10
3.4 Army Network Security Service Delivery Rules 12
4 Technical Positions and Implementation Patterns **14**
4.1 Technical Positions 14
4.2 Implementation Patterns 15
Appendix A: Vocabulary and Terms **A-1**

Tables and Figures

Table 1 - Alignment to the DIEA 8
Table 2 - Presentation format for Guiding Principles and Business Rules 9
Table 3 - Guiding Principle 1 and Associated Rules 11
Table 4 - Guiding Principle 2 and Associated Rules 12
Table 5 - Army Network Security Service Delivery Rules 14
Table 6 - Enterprise Security Controls 15
Table 7 - Security Controls Provided on each P/C/S 15

Figure 1 - Current Network Security Posture 6
Figure 2 - Network Security Objective State 7
Figure 3 - CND/NETOPS Privileges by Echelon 16
Figure 4 - MPLS / Infrastructure Implementation 17

1 Introduction

Today, local Army Commanders control their own network enclaves and operate over 500 network security enclaves on the unclassified Army network. The overarching objectives of this network security architecture are to reduce network complexity, minimize the network attack surface and standardize network security. Revising the network security architecture will improve network performance and create cost efficiencies. It also enables critical enterprise initiatives, such as Enterprise Email, Unified Capabilities (UC) and data center consolidation, while facilitating integration into the Joint Information Environment.

1.1 Background

In November 2011, the Commander of the United States Cyber Command (USCYBERCOM) briefed the Joint Chiefs of Staff (JCS) on the risk associated with the inability to "see" the entire DoD network. To protect, defend, and improve visibility into the network, recommendations were made to consolidate and normalize IT infrastructure, and improve effectiveness. In response, the JCS directed the Joint Staff (JS) Command, Control, Communications, and Computers/Cyber (J6) and USCYBERCOM to work with the DoD Chief Information Officer (CIO) to develop a Joint Information Environment (JIE) with the following tasking:

> *There is currently no shared understanding of the current "state" of the Services, definition of the architecture and requirements, and way ahead. Joint Staff will convene, in concert with CYBERCOM and DoD CIO, a group of representatives from the Services and/or CYBERCOM Components to begin to work through the translation of the vision into a practical, executable roadmap that also defines what the impact of the end state will be on the tactical edge.*
>
> *Operations Deputies Information Paper, 16 November 2011*

Planning and incremental implementation of JIE is on-going and the JIE objective state is being heavily shaped and influenced by the Army. In parallel to JIE efforts, the Army is aggressively moving forward with a plan to improve its security architecture to increase operational effectiveness and gain both cost and operational efficiencies.

1.2 Purpose and Scope of this Document

The purpose of this document is to provide CIO/G6 guidance for improving the Army's network security architecture. The guidance within this document is primarily provided as a set of business, operational or technical rules that serve three general functions:

- Inform internal and external stakeholders of the CIO's intent for securing the Army network
- Guide the delivery of security services and capabilities
- Identify constraints for the successful deployment of the objective security architecture

As required, the architectural rules within this document will be further described by a technical or operational position statement and a high-level implementation pattern to ensure the intent of the rule is understood, achievable and measurable. Depending on the nature and complexity of a rule, an associated risk statement and actionable risk mitigation strategy will also be provided. The architectural rules and associated descriptions begin in section 3.

The scope of this document includes all network security controls that will be deployed on the LandWarNet extending down from the Defense Information Systems Network (DISN) to every end user, device and networked equipment connected to the Non-Classified Internet Protocol Network (NIPRNET). This includes LandWarNet ingress/egress points to the NIPRNET and Internet, Army data centers, Processing Nodes (all variances –see appendix A), and every Post/Camp/Station where Army is the executive agent or responsible for providing Command, Control, Communication, Computers and Information Management (C4IM) services.

It is not in scope of this document to address the Secure Internet Protocol Network (SIPRNET) or the tactical (non-fixed) network environment. Both of these networks will be addressed in future increments of this architecture.

Under the JIE initiative, a Single Security Architecture (SSA) and Network Optimization Reference Architecture (NORA) are being defined and developed for the DoD Enterprise. The architectural rules within this architecture are consistent with the desired outcomes of both the SSA and NORA. It is not the intent of this architecture to duplicate JIE architectures. Rather, this architecture is intended to reference or adopt JIE architectures where applicable and discuss architectural rules that the Army must adhere to now to improve its network security and ensure Army is postured to leverage JIE capabilities as they emerge.

1.3 Key Authoritative Sources and Draft Documents

- DoD Information Technology (IT) Enterprise Strategy and Roadmap, version 1.0, 6 September 2011
- DoD Information Enterprise Architecture Version 2.0, July 2012
- JIE Single Security Architecture, version 1.1, 2 May 2013
- Network Optimization Reference Architecture version 0.9 (Draft)
- Core Data Center Reference Architecture version 1.0 (Draft)
- Information Technology Management Reform Implementation Plan, 20 February 2013
- Army Directive 2013-02 (Network 2020 and Beyond: The Way Ahead), 11 March 2013
- HQDA CIO/G6 memorandum: Army Guidance for Establishing Rules-Based Architecture, 1 May 2013
- Joint Enabling Capabilities (JEC) Service Operations Plan version 1.9 (draft)
- LandWarNet Consolidation EXORD, July 2013 (Draft)

1.4 Document Structure

An Army-wide Reference Architecture provides information, guidance, and direction that is applicable across the Army. This information, guidance and direction are provided in the following sections:

- **Section 2: Current and Objective Network Security Posture**
- **Section 3: Guiding Principles and Rules**
  - **Guiding principles**- Identifies goals and objectives of the Army network security Architecture and are aligned with DoD Information Enterprise Architecture (DIEA) as well as the Network Mission Area (NMA) capability areas
  - **Rules**– Sufficient high level foundational statements that guide and constrain how the objective network security architecture will perform and be implemented
- **Section 4: Implementation Patterns and Technical Positions**
  - **Implementation Patterns (Templates)** – Generalized architecture representations (viewpoints, graphical/textual models, diagrams, etc.) that further clarify the rules that the network security architecture must conform with
  - **Technical Positions-** Minimal set of technical guidance and standards required to conform to a given rule
- **Appendix A: Vocabulary** – Acronyms, terms, and definitions that are used in the Reference Architecture and relevant to architectures and solutions that are guided and constrained by the Reference Architecture. Also referred to as an Integrated Dictionary (AV-2).

2 Current and Objective Network Security Posture

2.1 Current Army Network Security Posture

The network security posture that is currently deployed across the LandWarNet was implemented inconsistently with varying degrees of effectiveness. Many of the network security controls were deployed in a stove-piped manner with multiple tenants within a single security enclave (P/C/S) providing their own network security stacks, using their own and in some cases conflicting security policies, and maintaining separate public/Internet network interfaces. This has resulted in additional security complexity, duplicative inspection of the same network traffic and increased external threat vulnerabilities. The following summarizes the characteristics of the current network security posture:

- Contains duplicative and redundant security controls (data inspected multiple times)
- Computer Network Defense (CND) is performed in an ineffective and inefficient manner
- Non-standard, and sometimes conflicting, security policies are implemented across the LandWarNet
- The current network attack surface is unmanageable
- Most P/C/S tenants maintain cascading and redundant boundary(enclave) protection
- Both visibility down to end-user devices and the ability to respond to an IA event are severely inhibited

Figure 1 below is a graphical illustration (showing 2 notional P/C/S's) of the current network security posture of the LandWarNet.

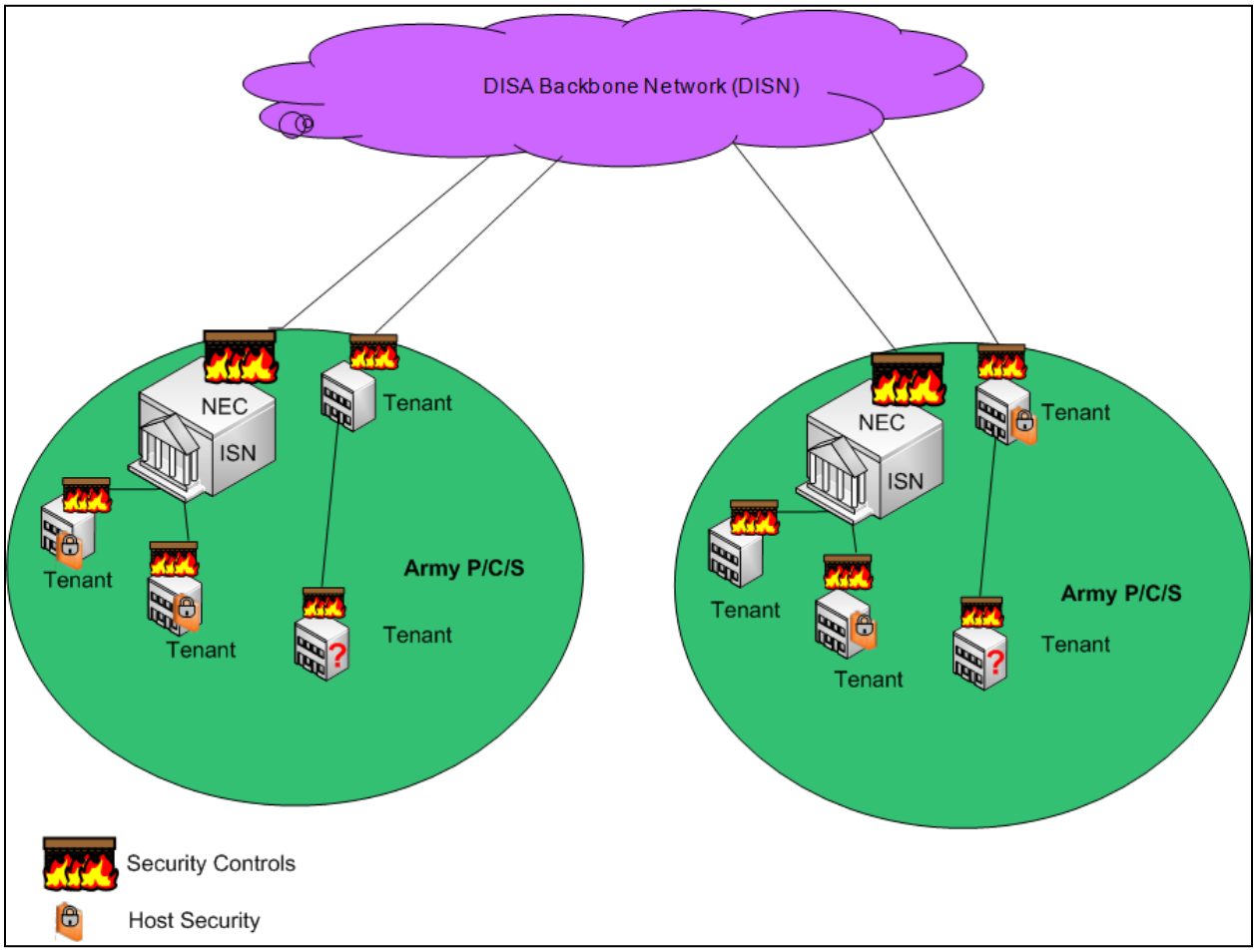

Figure 1 - Current Network Security Posture

2.2 Objective Army Network Security Posture

Within the objective network security posture, network security controls are separated in two groups:

1) Security controls that are inherited from an enterprise service provider
2) Security controls that are provided locally on P/C/S's

Inherited security controls that will be provided by the enterprise include traffic inspection, segregation and blocking capabilities to mitigate known and suspicious traffic before reaching LandWarNet data and computing centers, and collection of network packet and flow data to detect, deflect and protect against unwanted intrusion or attack. A Multiprotocol Label Switching (MPLS) network will be deployed to enable a high speed and robust IP infrastructure allowing the delivery of enterprise security controls.

Locally provided security controls consist primarily of Host Based Security Services (HBSS), Gold Master configurations, trusted boot and trusted network connect and Public Key Enabled (PKE) 802.1x network access control. A more extensive list of enterprise and locally provided security controls is provided in section 4.

The following summarizes the characteristics of the objective network security posture:

- Multiple P/C/S's receive enterprise network security controls from a single network security suite
- Enterprise defensive capabilities are deployed with standardized network security suites at optimal locations
- Network security controls are provided from the enterprise in a uniform and standardized manner
- Network security controls that are redundant to enterprise security controls are removed from each P/C/S

Figure 2 below is a graphical illustration of the objective network security posture of the LandWarNet.

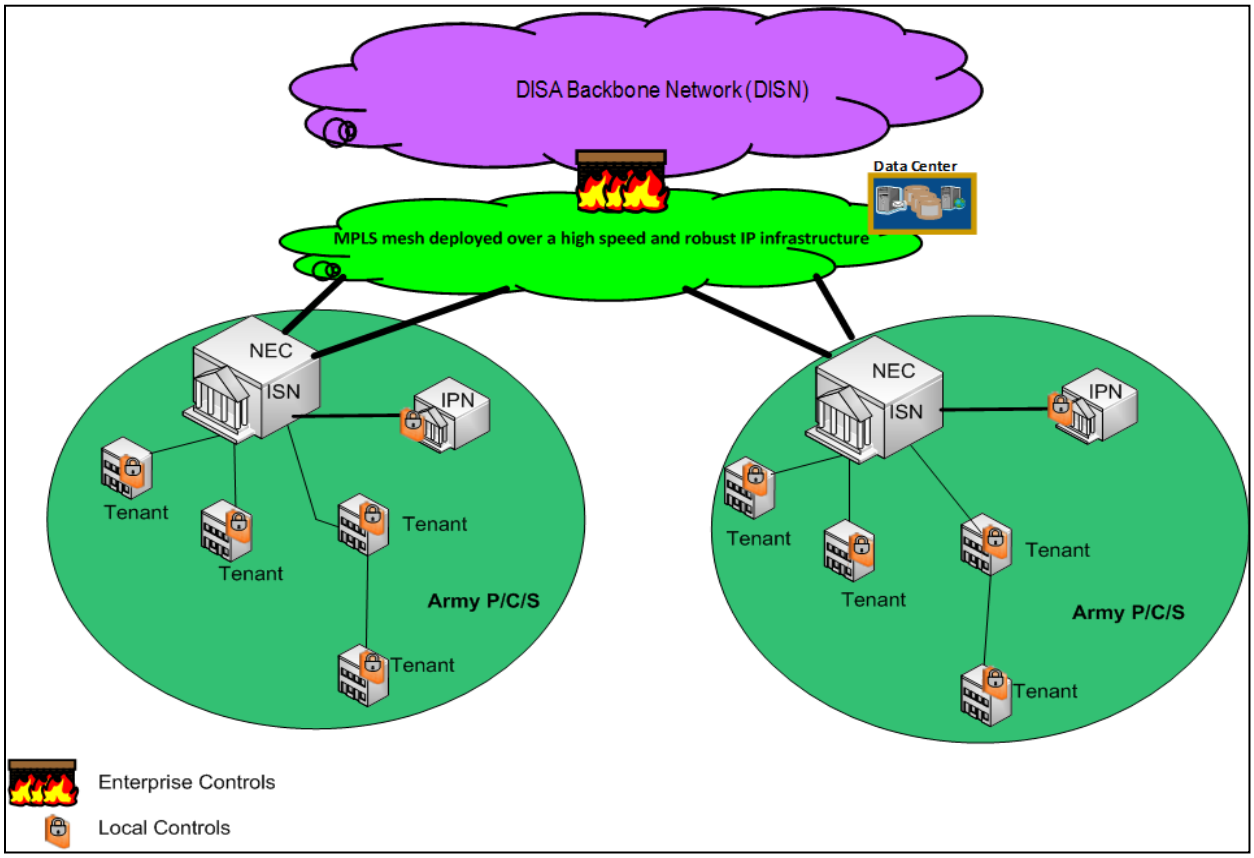

Figure 2 - Network Security Objective State

2.3 Transitional Assumptions and Constraints

As of the publication of this architecture, multiple concurrent initiatives are on-going that will enable the transition to the objective network security posture. Based on these initiatives, the following high level assumptions are made:

- Regional security stacks will be connected to the DISN via high-speed (10 Gbps or more) IP circuit(s)
- An MPLS mesh is operational and provides the required quality of service and capabilities identified in section 3.4 (Army Network Security Service Delivery Rules)
- Each enterprise security suite is fault tolerant and has sufficient redundancy IAW the operational rules in section 3.3.2 (Army Network Security Rules)
- The executive agent has the ability to manage and shape traffic flow entering and leaving the P/C/S
- The LandWarNet Consolidation EXORD is published
- All ARCYBER CONOPS and annexes are complete and describe Computer Network Defense/ Network Operations (CND/NETOPS) roles and responsibilities

Operational patterns (sections 4.2.1 and 4.2.2) depict the high-level MPLS / infrastructure implementation and CND/NETOPS privileges required to support the objective security architecture.

The following constraints must be mitigated prior to implementing the objective network security posture:

- Enterprise and local security controls of the objective security posture are tested before current security controls are removed
- Required local security controls are effectively applied and managed by the executive agent of each P/C/S IAW (to be developed) TTP's and CONOPS

3 Army Network Security Guiding Principles and Rules

3.1 Army Network Security Guiding Principles

Guiding principles represent the highest level of guidance for IT planning and decision making. They are high-level statements that apply to specific business/warfighting requirements. The Defense Information Enterprise Architecture (DIEA) guiding principles are aligned with the JIE. The following Army guiding principles (Table 1) were derived from the DIEA and apply to the Army network security architecture:

DoD Guiding Principles and Rules	Army Guiding Principle
• DoD shall operate and defend the GIG as a unified, agile, end-to-end information resource	• Army shall operate and defend the LandWarNet as a unified, agile, end-to-end information resources IAW Computer Network Defense Service Provider (CNDSP) requirements and metrics
• GIG infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster	• The LandWarNet infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster

Table 1 - Alignment to the DIEA

3.2 Operational Rules

The two tables in section 3.3 below identify the operational rules that must be adhered to in order to achieve the capabilities of the objective network security architecture. Section 3.3 also provides additional detail for each rule and known risks that would inhibit successful implementation of any given rule. If a known risk is identified, an associated risk mitigation statement will also be identified.

The following table illustrates how the operational rules will be presented within this document. The table is organized as follows:

1. An enterprise guiding principle (derived from DIEA) is associated with a required DIEA/ Joint Information Enterprise (JIE) capability. The DIEA/JIE capability is then cross-walked to a Network Mission Area (NMA) capability area. This mapping facilitates traceability to DoD/ JIE as well as alignment to the three domains within the NMA.
2. Gaps within the current NMA network security architecture (desired capabilities Army wishes to achieve) are then identified
3. From the identified gaps, a set of operational rules are listed that will produce the listed desired outcomes.

If implementation of an operational rule warrants additional consideration (or if a known risk exists) this information will be provided to facilitate future risk mitigation and serve as documentation of the current challenges associated with the Army's network security architecture.

Guiding Principle ***Guiding Principle that is derived From the Defense Information Enterprise Architecture (DIEA)***	
DoD Capability	**NMA Capability**
Required Capability from DIEA/JIE	*DIEA Capability aligned to the Network Mission Area (NMA) capability areas*
Capability Gap(s)	
Identified Gaps in a specific NMA capability area	
Architectural Rule(s) that mitigate Capability Gap	**Desired Outcome(s)**
Architectural rules (constraints /guidance) that need to be adhered to in order to satisfy the capability gap	Specific outcomes that will be achieved with successful implementation of the rules
Considerations and Known Risk(s)	
Identified considerations, risk, and challenges associated with implementing the identified rules	

Table 2 - Presentation format for Guiding Principles and Business Rules

3.3 Army Network Security Rules

3.3.1 Principle 1: Army shall operate and defend the LandWarNet as a unified, agile, end-to-end information resource IAW CNDSP requirements and metrics

Guiding Principle 1 **Army shall operate and defend the LandWarNet as a unified, agile, end-to-end information resource IAW CNDSP requirements and metrics**	
DoD Capability	**NMA Capability**
An event/incident and threat remediation strategy based on analysis of the computing environment and a proactive assessment and mitigation effort	Secure the Network -> Respond: The capability to formulate and execute the proper responses to attacks and/or intrusion to the network, including the reconstitution and reactivation of the network as necessary
Capability Gap(s)	
• Inability to "see" into the network due to multi layers of redundant and non-standardized security controls • Consisting of over 500 ingress /egress points, the network attack surface is unmanageable and difficult to defend • CND tools and resources are inconsistently deployed and inefficiently used	
Architectural Rule(s) that mitigate Capability Gaps	**Desired Outcome(s)**
• Installation tenants will not provide network security controls that are duplicative of those provided by the installations executive agent. The overarching network security design showing placement of security controls is identified in figure 2 (section 2.2) and the technical profile is located within section 4	• The removal of duplicative and non-standard security controls will provide network defenders a view of the network down to the desktop
• P/C/S border network security controls will be removed and aggregated to a centralized network security construct. The high level pattern is identified in figure 2 (section 2.2)	• Security controls will be inherited from an optimal amount of Regional Security Stacks (RSS) allowing the removal of over 500 instantiations of TLA's which in turn will allow existing CND expertise, tools and resources to be reallocated and able to satisfactorily defend the reduced attack surface
• CND training and tools will only be deployed at the appropriate level of the security architecture. Training requirements and tool procurement will be driven by the Joint Enabling Capabilities (JEC) Service Operations Plan and related PEO-EIS MPLS / Security Architecture Engineering Documentation. Section 4 depicts a notional high-level pattern as to what NETOPS capabilities are required across the enterprise and at what	• Guides the optimal placement of where CND expertise, tools and resources need to exist and what capability is required to efficiently perform the CND mission

Guiding Principle 1 Army shall operate and defend the LandWarNet as a unified, agile, end-to-end information resource IAW CNDSP requirements and metrics	
echelon. • Network Data and information collected for Traffic and Malware analysis and forensic analytics will be stored and analyzed as close to the collecting sensor as practical	• Enables efficient CND predictive analysis using big data technology without congesting the network infrastructure
Considerations and Known Risk(s)	
• Risk: Resources, CONOPS and TTPs must be in place to perform transitional activities that need to be accomplished to deploy RSS capabilities (i.e. test and evaluation) in parallel to the current NETOP/CND missions • Removal of existing controls could present a migration problem if not coordinated properly. A standardized template that addresses the Army standard security posture that will be implemented for all tenants, with changes coordinated and validated by ARCYBER, will improve security and greatly facilitate adoption and migration • Risk: Cultural resistance to removal of existing tenant owned TLA equipment may delay the benefit and capability of this architecture • Security Controls Provided Locally on each P/C/S by the Executive Agent (Table 7 below) must be fully deployed and operational	

Table 3 - Guiding Principle 1 and Associated Rules

3.3.2 Principle 2: The LandWarNet infrastructure capabilities must be survivable, resilient, redundant, reliable and available to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.

Guiding Principle 2 The LandWarNet infrastructure capabilities must be survivable, resilient, redundant, reliable and available to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.	
DoD Capability	**NMA Capability**
The process of preparing and equipping a network to allow it to provide services to its users	Enterprise Service -> Service Management The capability that ensures segments or components of the network have the ability to "fail" without causing failure to other parts of the Army Enterprise so the operational mission continues
Capability Gap(s)	
• The current network security architecture has varying degrees of survivability and was not designed in a holistic fashion under a single set of standards. This has inevitably created resilience and survivability vulnerabilities	

Guiding Principle 2 The LandWarNet infrastructure capabilities must be survivable, resilient, redundant, reliable and available to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.	
• RSS deployment can potentially increase risk and an inability to provide the required security controls if resilience, survivability continuity of operations and disaster recovery are not primary implementation considerations	
Architectural Rule(s) that mitigate Capability Gap	**Desired Outcome(s)**
• Army network security services will be provided from the most effective /efficient location possible regardless of executive agent	• Army will utilize the most strategically aligned physical location to provide RSS capabilities regardless of location executive agent to ensure optimal physical diversity and survivability is achieved
• Locations that provide regional security network controls will meet the operational, physical and environmental survivability requirements IAW with Defense Threat Reduction Agency (DTRA) guidelines for physical security, protection and survivability of critical infrastructure (also see UCR2013)	• Army RSS locations are survivable, resilient and are optimally protected against man-made or natural catastrophic events
• Locations that deliver regional security controls must be connected to the DISN via physically diverse DISA owned or leased transport that provides response time < 80ms for each service request	• Security services delivery from RSS locations is reliable, robust and provides P/C/S's with the required security controls
Considerations and Known Risk(s)	
• RSS deployment can potentially increase risk and an inability to provide the required security controls if resilience, survivability continuity of operations and disaster recovery are not primary implementation considerations	

Table 4 - Guiding Principle 2 and Associated Rules

3.4 Army Network Security Service Delivery Rules

The following Service delivery rules (Table 5) provide design and engineering guidance to be considered during system design and adhered to during implementation of the security service. These service rules were primarily derived from the draft Network Optimization Reference Architecture (NORA) and are consistent with Army architectural direction and guidance. Figure 4 (section 4.2.2) provides a graphical representation of equipment connectivity and placement within the infrastructure.

Identifier	Service Delivery Rules	Rule Rationale
1.	P/C/S demarcation of DoD and Army network security responsibilities will occur at the Provider Edge/Customer Edge (PE/CE) router	MOA currently under development with DISA to achieve this capability
2.	Enterprise Layer 3 VPN connectivity between P/C/S's and enterprise long haul network is supported on the PE/CE router owned by DISA layer 3 connectivity adheres to the following standards: a. Access Bandwidth per site: 10 to 100 Gbps b. Access Interface: Fast Ethernet or Gigabit Ethernet c. Number of sites per VPN: unlimited	Provides standard service profile for Layer 3 VPN service
3.	Layer 2 VPN connectivity (Ethernet Private Line and Ethernet Private LAN) between P/C/ S's is supported on the PE/CE router; layer 2 connectivity adheres to the following standards: a. Access Bandwidth per site: 10 to 100 Gbps b. Access Interface: Fast Ethernet or Gigabit Ethernet c. IPT-PE Interconnection: Ethernet or EITF 802.1q-2005 d. Number of sites per VPN: unlimited	Provides standard service profile for Layer 2 VPN service
4.	Community Of Interest (COI) VPN spanning multiple P/C/S's, must be implemented using standard services that leverage the MPLS VPN capability of the enterprise long haul transport network a. Enterprise Layer 3 VPN: Enterprise provides any-to-any layer 3 connectivity between P/C/S's and manages VPN routing for a single VPN per CE router b. P/C/S's leverage the enterprise layer 3 VPN service and provides multiple layer 3 VPN's from a single PE/CE router c. COI VPNs will internally support IP Multicast traffic	Supports mission effectiveness by providing standard VPN architecture that eliminates the need for individual tenants to develop unique architectures that hinder interoperability and information sharing; at the same time, the architecture provides a number of VPN service options to support varied tenant networking requirements
5.	Each deployed RSS provides boundary protection for all P/C/S's	All traffic from connected P/C/S's traverses a PE/CE router en route to remote destinations
6.	The RSS must support VPN implementation using an enterprise MPLS transport to overlay multiple RSS security regions	Provides the ability to implement logically separated VPN's that span multiple RSS regions
7.	Each regionally deployed virtual security stack provides the following security functions for all attached P/C/S's a. Deep Packet Inspection (DPI) b. Intrusion Detection Systems (IDS) c. Intrusion Preventions Systems (IPS) d. Data Logging e. Remote Access VPN Services	Standard security functions required to successfully support network boundary protection and improve overall security posture

Identifier	Service Delivery Rules	Rule Rationale
	f. Web Proxy and Proxy A/V services g. Network and Application Protocol Analysis and reporting	
8.	As network boundary protection is provided by the enterprise, the network security mission of each P/C/S's owner shifts to host-based security and Anomalous Behavior Detection (ANBD) within the P/C/S's	Individual components no longer need to provide their own network boundary protection and may redirect those resources toward providing host-based security functions
9.	Server computing is cleanly separated from end user computing, which is accomplished through the relocation of servers from user local area networks (LANs) into dedicated multi-tenant data centers or IPN's	Simplifies network security mission by separating server bound traffic flows from end user traffic flows
10	The enterprise long haul transport network will provide an IP service edge that enables any-to-any IP data service between all P/C/ S's and enables customer access to value-added services such as VPN, IP QoS, and Multicast. Peer to Peer communications will be limited to authorized applications and services (initially VOIP and UC)	Provides delivery of converged IP-based networking and value-added communication services required to support mission effectiveness

Table 5 - Army Network Security Service Delivery Rules

4 Technical Positions and Implementation Patterns

4.1 Technical Positions

4.1.1 Enterprise and Local Network Security Controls

As referenced in section 2.2 (enterprise and local security controls), the following tables identify the minimal security controls that will be provided at each level.

Security Controls Inherited from the Enterprise RSS	
FW/IDS/IPS (Next Gen FW)	Enterprise Collaborative Operational Sensor (ECOS) Suite (Trickler, Netflow, IDS, Packet Capture)
IC Strategic sensors	Network Anomalous Behavior Detection (Data Loss Prevention)
Edge Border Controller (EBC)	Distributed Denial of Service (DDoS) Detection/Mitigation
Enterprise Email Security Gateway (EEMSG)	Access Control List (ACL)/Whitelist
.mil proxy	Web Content Filters (WCF)
SSL/TLS Proxy (For Data Applications)	Enterprise Recursive Service
Reverse Web Proxy	Web Application Filter
Database Firewall	Network Mapping
ePO Server	Honeypot
Vulnerability Scanner	Centralized Patch Management

Table 6 - Enterprise Security Controls

Security Controls Provided Locally on each P/C/S by the Executive Agent	
User ID (CAC)	Secure Storage (DAR)
Secure Operating system (AGM)	Patch Services
Secure Applications (AGM)	802.1x port access controls utilizing Machine Identity PKI protected by device TPM)
Secure Browser (AGM)	VLAN Separation
Host Firewall (HBSS)	Virtual Route Separation
Host Intrusion (HBSS)	Subnet Isolation
Host Antivirus (HBSS)	Black Listing / White Listing Applications via GPO
PC Health Checks implemented using Trusted Network Connect standards (NAC)	Device Control Module / Data Loss Prevention (USB Control)
Standardization of Installation VLANs to include Management, Army Production, Army Remediation, DoD User and Guest	Secure BIOS

Table 7 - Security Controls Provided on each P/C/S

4.2 Implementation Patterns

4.2.1 CND/NETOPS Privileges by Echelon

The following pattern (draft / notional) depicts required CND /NETOPS capabilities, across the enterprise and by echelon, as referenced in section 3.3.1 . The USCYBERCOM/DISA echelon will own and operate the RSS and provide the SC(T)/TNOSC/CND-SP echelon with the administrative privileges required to fulfill Army's Title X mission. When the Joint Enabling Capabilities (JEC) Service Operations Plan is finalized this graphic will be updated according.

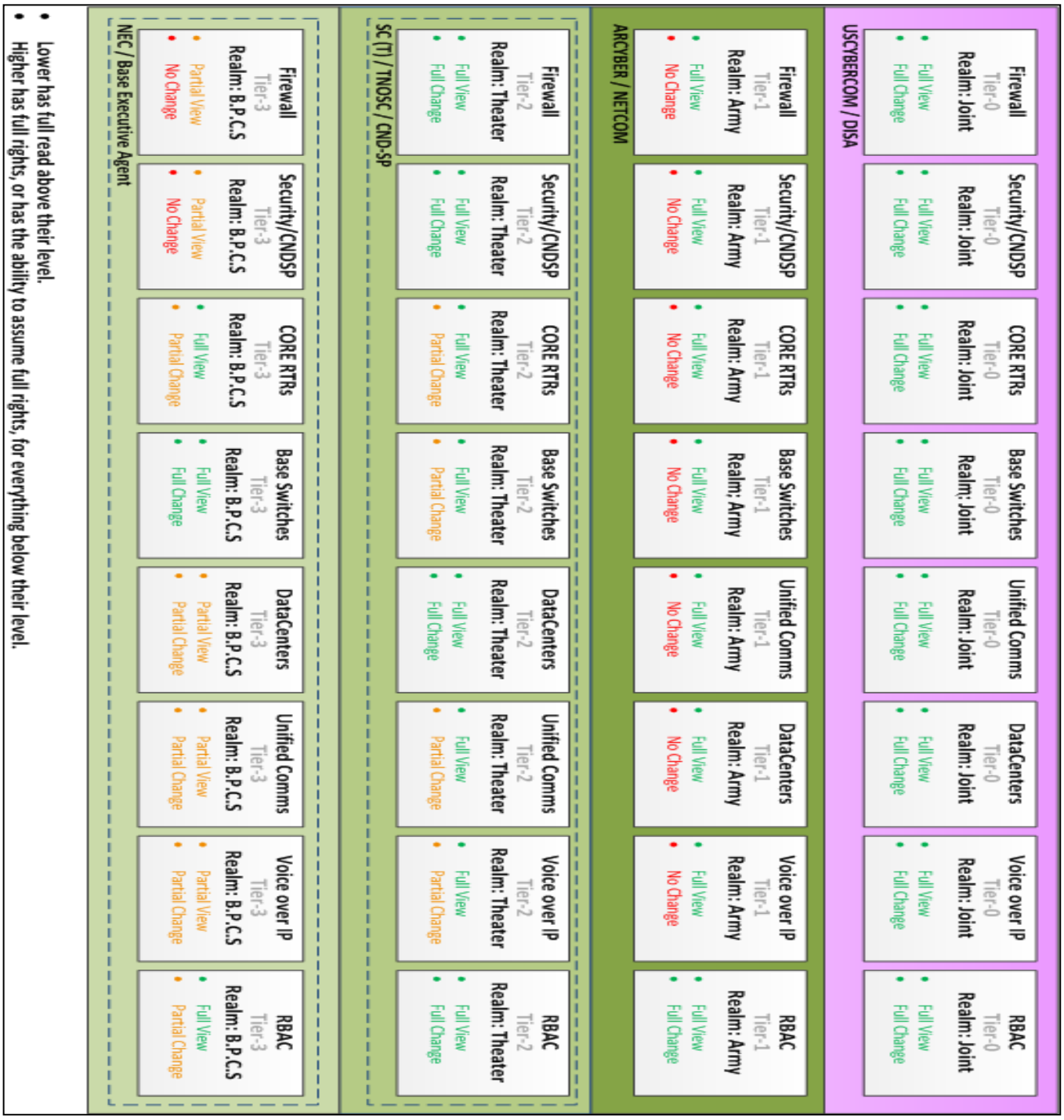

Figure 3 - CND/NETOPS Privileges by Echelon

4.2.2 MPLS / Infrastructure Implementation

The following pattern depicts the high-level view of the desired MPLS implementation, required network connectivity /diversity and the line of demarcation between enterprise and local security control deployment. Local security control placement is annotated in green and extends down into the P/C/S (not shown).

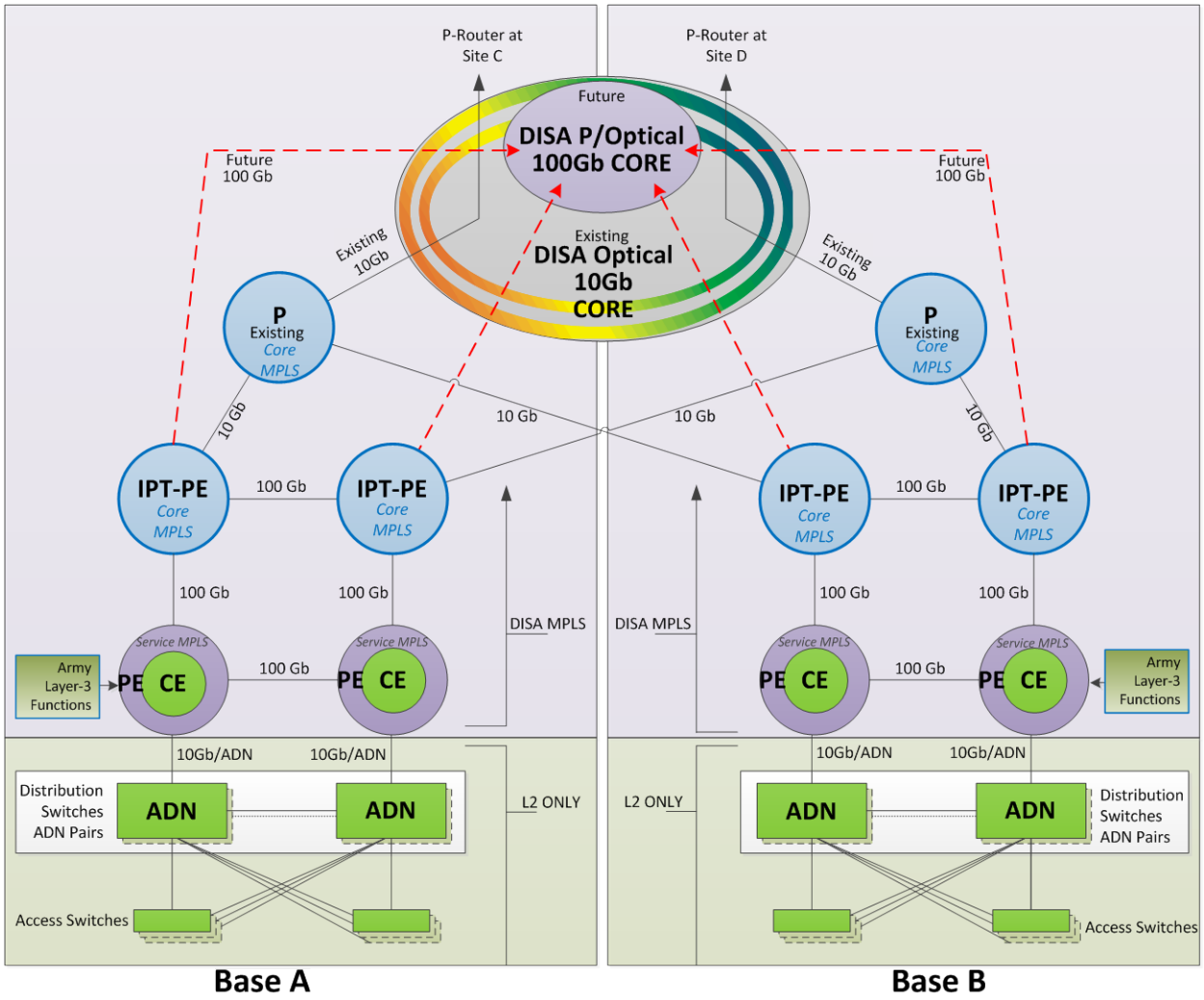

Figure 4 - MPLS / Infrastructure Implementation

Appendix A: Vocabulary and Terms

Term	Definition
Assured Bandwidth	The ability to determine and analyze bandwidth implications of data storage, applications and services across the enterprise network and to account for those implications during implementation and operations.
Assured End to End Communications	The ability to deliver the information transport required for assured end-to-end communications. This capability enables a joint infrastructure providing global, interoperable communications across the enterprise and with mission partners.
Big Data Analytics	The ability to provide big-data storage for indexing, data reduction and data analytics.
Community Of Interest (COI) Virtual Private Network (VPN)	A scalable multi-VPN capability within a single physical network based on traffic source and destination using Layer 3 routing.
Defend the Network	A comprehensive network defense strategy based on identifying and mitigating vulnerabilities within the network, establishing visibility of network behavior, identifying and analyzing anomalous behavior, and maneuvering to disrupt malicious network activity.
End-to-End Quality of Service	The ability to proactively monitor and control service levels and quality of service on an end-to-end basis. End-to-end monitoring and control will be integrated across networks, computing platforms, systems, applications, and services.
Installation Processing Node (IPN)	A fixed (i.e., not designed to be relocated or transported) data center serving a single installation and local area (installations physically or logically behind the network boundary) with local services that cannot (technically or economically) be provided from a core data center.
Installation Service Node (ISN)	A facility containing the requisite localized equipment necessary to provide the minimum basic functionality to an installation should it become disconnected from the Global Information Grid (GIG). There is no application hosting or data processing in an ISN. Potential services include read only Active Directory (AD) servers, DNS servers, Assured Compliance Assessment Solution (ACAS) servers, Host Based Security System (HBSS) servers, and print servers. In addition ISNs may also host UC capabilities that must remain on the Installation to enable emergency services even when the connection to the GIG is interrupted.
Special Purpose Processing Node (SPPN)	A fixed data center supporting special purpose functions that cannot (technically or economically) be supported by CDCs or IPNs due to its association with mission specific infrastructure or equipment (e.g., communications and networking, manufacturing, training, education, meteorology, medical, modeling & simulation, test ranges, etc.). No general purpose processing or general storage can be provided by or through an SPPN. SPPNs do not have a direct connection to the GIG; they must connect though CDC or IPN
Tactical/Mobile Processing Node (TPN)	Tactical/Mobile Processing Nodes will provide services similar to a CDC but optimized for the tactical or deployed environment. Depending upon the circumstances, TPNs may connect to the GIG through DoD Satellite Gateways.
Land Warrior Network (LandWarNet)	The Army's portion of the DoD GIG. LandWarNet is a universally accessible, standardized, protected, and economical network enterprise. LandWarNet seamlessly delivers network capabilities and services supporting the Army's Joint, interagency, intergovernmental, multinational operations, and business missions.
Logically and Physically Separated Networks	The ability to dynamically allocate bandwidth to separate distinct networks (e.g. Management Plane; Data Replication and Synchronization Plane; and User Plane) based on usage.

Term	Definition
MPLS-VPN Meshed Network	A scalable multi-VPN capability within a single physical network using Layer 3 routing.
Network Defense	The ability to defend network infrastructure against known and postulated attacks and against new threats that have not previously been seen, while reducing network vulnerabilities. This includes defense against both kinetic and cyber attacks.
Network Monitoring	The ability to monitor situational awareness of the network across domains and identify when unauthorized users attempt to gain access, especially by hostile means.
Network Traffic Segmentation	The ability to logically segregate/group network assets, resources, and applications together into compartmentalized areas that have no trust of each other and to control traffic flows on the backbone from users based on destination and service required (keep in separate VPN tunnels).
Securing the Computing Environment	An event/incident and threat remediation strategy based on analysis of the computing environment and a proactive assessment and mitigation effort
Segmentation and Isolation	The introduction of VLAN and VPN technologies into the network environment to provide isolation and segmentation
Situational Awareness	The ability to identify, process, and comprehend the critical elements of information about what is happening within the enterprise
Service Level Agreement (SLA)	Part of a service contract where the level of service is formally defined including references to the contracted delivery time (of the service) or performance
Threat Assessment	The ability to assess the intent and effects produced by the threat in a timely manner in near real-time situational awareness of the entire enterprise along with command and control cyberspace operations under its control. It must be able to assess the effectiveness of its offensive operations through the development and assessment of valid MOE/BDAs (Measure of Effectiveness)/(Battle Damage Assessment).
Unified Communications	The ability to seamlessly integrate voice, video, and data applications services for mobile and fixed communications services so they are delivered ubiquitously across a secure and highly available single protocol network infrastructure.
Virtual Route Forwarding (VRF)	The virtual routing and forwarding table, which is separate from the global routing table that exists on PE routers. Routes are injected into the VRF from the CE-PE routing protocols for that VRF and any MP-BGP announcements that match the defined VRF route targets (RTs).
WAN	A Wide Area Network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, or national boundaries) using private or public network transports.