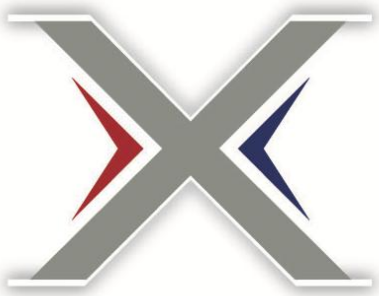

Network Specification 2016

Version 3.0

Purpose of this Document

This directive serves as a functional specification for all Blue Cell networks during Cyber Defense Exercise 2016 (CDX 2016).

Document Revision History

Version	Change Description	Change Owner	Date
1.0	FIRST DRAFT	Jim Titcomb	29 Oct 2015
2.0	SECOND DRAFT	Jim Titcomb	21 Jan 2016
3.0	FINAL	Jim Titcomb	25 Feb 2016

1.0 Overview

1.0.1 This document is intended to provide rules and guidelines for the design of Blue Cell networks during the build phase of the Cyber Defense Exercise (CDX).

1.0.2 A second important document, the *CDX 2016 Exercise Directive*, lays out rules and requirements for the operation of Blue Cell networks during the active phase of CDX 2016. A third document, the *CDX 2016 Scoring Specification* provides details on the CDX scoring components and guidelines. Other rules and guidelines may be published as needed in the form of tasking orders or specifications from the CDX White Cell.

2.0 BLUENET Required Services

2.0.1 The following sections specify the required services that must be available on each BLUENET. These services must be available both to local users, including White Cell and Gray Cell users, and external users.

2.0.2 These services may be configured on any number of physical or virtual machines. Blue Cells are encouraged to consider the tradeoff associated with having multiple services running on one computer as opposed to spreading these services over multiple computers.

2.0.3 The availability scoring system (RubberNeck) will test for the required services being available from a wide variety of locations:

- Gray Cell user workstations
- Gray Cell user workstations at other BLUECELLs
- CDX Headquarters
- SIMNET

2.0.4 Blocking of traffic in CDX 2016 is allowed, but it might seriously affect availability scoring due to the potential of blocking RubberNeck traffic.

2.0.5 For required services where authentication is necessary, RubberNeck will require a user ID and password. For each of these services, the following shall be used:

User ID **rubberneck**
Password **Rubb3r#N3ck**

2.0.6 Failure to use this authentication information shall result in a loss of availability scoring because RubberNeck will not be able to verify that password protected services are available.

2.1 Domain Name Service

2.1.1 Required port usage: UDP 53

2.1.2 Each Blue Cell team must provide name resolution for all "outward-facing" systems within their network; i.e., those that will be directly accessed by other BLUENET or SIMNET sites.

2.1.3 Domain names for the various BLUENET subnets shall be:

Organization	**Domain Name**
HQ	hq.bluenet
RMC	rmc.bluenet
RMC-U	rmcu.bluenet
USCGA	uscga.bluenet
USMA	usma.bluenet
USMMA	usmma.bluenet
USNA	usna.bluenet
USCC	uscc.bluenet

2.1.4 Some of the required services described elsewhere in this document must be associated with specific domain names:

Server	**Domain Name**
Domain Name Service (DNS)	ns1.xxxx.bluenet ns2.xxxx.bluenet (and so on)
Email (SMTP) service	smtp.xxxx.bluenet
Email (IMAP) service	imap.xxxx.bluenet
FTP service	ftp.xxxx.bluenet
IPv6 Web service	www6.xxxx.bluenet
Web service	www.xxxx.bluenet
Gray Cell Remote Admin	grayadmin.xxxx.bluenet

2.1.5 One outward-facing DNS server must be placed at IP address 10.1.xx.5. Optionally, a secondary outward facing DNS server may be employed by placing it at 10.1.xx.6. The CDX HQ DNS server will be set up to forward all requests for a given Blue Cell subnet to that address. This convention will not be changed for the duration of the exercise.

2.1.6 The primary DNS server at HQ will be placed at IP address 10.1.10.5. Each Blue Cell team should set up its DNS server(s) to forward requests outside the local subnet to the HQ DNS. A secondary DNS server for CDX HQ will be placed at 10.1.10.6.

2.1.7 The HQ DNS server *will not accept zone transfers* from any Blue Cell subnet at any time.

2.1.8 The IPv6 Web server must have an appropriate AAAA record on the DNS server

2.1.9 To facilitate email routing, DNS may be configured for reverse lookups.

2.1.10 To facilitate availability scoring from RubberNeck clients and to provide for user access, DNS shall resolve both externally and internally originated domain name requests.

2.1.11 To facilitate availability scoring from RubberNeck clients and to provide for user access, the domain controller at each BLUENET shall be named "**dc1**".

2.1.12 The following network device names must be resolved within each BLUENET:

- alpha
- beta
- delta
- gamma
- dc1
- smtp
- imap
- ns1
- ns2

2.1.13 The following service names must be resolved publicly:

- www
- www6
- ftp
- imap
- grayadmin

2.2 Domain Controller supporting LDAP

2.2.1 Required port usage: TCP 389

2.2.2 Each Blue Cell team must create and maintain a domain controller holding a centralized credentials repository for its own BLUENET subnet.

2.2.3 Within each BLUENET, all Windows user workstations, all Linux user workstations, domain controller, the email server, the internal DNS server (if separate from the domain controller) and at least one administrative workstation (Windows or Linux) must authenticate through the domain controller. Any other servers or clients may authenticate through the domain controller if desired.

2.2.3.1 The administrative users of the administrative workstation(s) shall be able to log on to the workstation(s) using domain credentials and then seamlessly connect to the servers in the domain (i.e., domain controller, email server, DNS server) by using domain credentials and perform various administrative functions. White Cell shall monitor to determine compliance.

2.2.4 Each Blue Cell domain will be stand-alone and will not perform replication with the HQ domain controller or with any other Blue Cell's domain controller.

2.3 Network Time Protocol (NTP) Service

2.3.1 Required port usage: UDP 123

2.3.2 Each BLUENET must synchronize time services with the CDX Headquarters' Network Time Server, available at ntp.hq.bluenet.

2.4 E-Mail Service

2.4.1 Required port usage: SMTP TCP 25, IMAP TCP 143

2.4.2 E-mail shall be used as the primary means of communication throughout the execution of CDX 2016. Implementation of email services must meet the following requirements:

- Each Blue Cell must create the following valid and working email addresses for the unit commander (or duty officer) and the White Cell liaison (acting as Coalition Partner):

Commander (Duty Officer)	CDR@xxxx.bluenet
Coalition Partner	CP@xxxx.bluenet

- Official correspondence, tasking orders from White Cell HQ, and other exercise messages will be sent to the above addresses
- Unofficial correspondence may also arrive at the above addresses
- Blue Cells will create working email addresses for their own individual members that may be used as convenient. White Cell HQ will not contact individual members directly without notice to the unit commander and the White Cell liaison.
- All email servers must support the Simple Mail Transfer Protocol (SMTP) when communicating with other Blue Cell enclaves, White Cell HQ or with SIMNET
- IMAP must be supported as a public service with connections expected from other BLUENET domains, CDX HQ and SIMNET; IMAP will, in effect, be supporting traveling users
- Must support unencrypted connections to the IMAP service
- Must support RubberNeck credentials (see section 2.0.5)
- Default mailbox for RubberNeck user must be “Inbox”
- No connection limits are allowed
- Mailboxes must have a capacity of at least 10GB
- No “auto-ban” mechanism for connections/failed attempts are allowed
- Spam filtering must be disabled

It is suggested that the message queuing time for sent emails be reduced to one minute to minimize message failures and to ensure message timeliness.

2.5 File transfer Protocol (FTP) Service

2.5.1 Required port usage: TCP 21 control port + some range of BLUENET chosen data TCP ports
Note: Choosing a small range of data ports may result in connection failures during the exercise. A range of at least 1000 ports should be sufficient.

2.5.2 The FTP folders shall include at least two primary folders: */private* and */public*. The */private* folder shall be accessible only to local users, to include the local

Gray Cell user. The */public* folder shall be accessible to local users as well as anonymous users from other Blue Cells, CDX HQ, and SIMNET.

2.5.3 Each Blue Cell must provide an FTP server configured as follows:

- Must support passive mode
- Must support Anonymous access
- Anonymous users must have the following permissions in at least the /public folder and sub-folders:
    - Create
    - Rename
    - Read
    - Write
    - Delete
    - Append
- Local users must have the following permissions in at least the /private folder, /public folder, and sub-folders:
    - Create
    - Rename
    - Read
    - Write
    - Delete
    - Append
- No restriction on file types
- No maximum number of concurrent users

2.6 Web Server Service

2.6.1 Required port usage: HTTP TCP 80; HTTPS TCP 443

2.6.2 Each Blue Cell team must maintain at least one outward-facing web server. This server must be responsive to HTTP and HTTPS requests from all valid BLUENET and SIMNET addresses. Blue Cells are free to redirect request from HTTP to HTTPS (or the reverse). What is important is that the web server be able to service the user's request using both formats.

2.6.3 Each Blue Cell website must include a page or pages, visible to any visitor to the site from anywhere in the BLUENET or SIMNET, linked from the front page of the site, providing the following static information:

- Organization chart detailing the Blue Cell's command structure.

- Watch bill detailing watch officer schedule.
- Name, rank, position, email address for all members of the local Blue Cell team.
- A list of all Blue Cell point of contact telephone numbers (e.g., Watch Officers, White Cell, etc.).
- A means of obtaining public keys for all participants on the local BLUENET subnet. All Blue Cell team members (e.g., Watch Officers, White Cell, Gray Cell) will make their public keys available on their local web site.

2.6.4 Each Blue Cell website must provide a dynamic message board or "forum," linked from the front page of the site, meeting the following criteria:

- The message board must be "threaded," collecting posts into threads or topics for convenient reading.
- Users must have the ability to create new threads, post to existing threads, edit or delete their own existing posts, quote text from earlier posts, and define signature blocks that will automatically be appended to their posts.
- Users must be able to embed hyperlinks and images into their posts, and must be able to use standard HTML markup to format their posts.
- Users must be able to create personal profiles, to include at least a full name, email address, personal web site URL, and personal description.
- Users must have the ability to upload and download files to the forums. In particular, users must have the ability to upload "avatar" images that will be automatically displayed as part of their own posts.
- At a minimum, the board must have two sections titled *Customer Support* and *Public Discussion*, in which any user on the BLUENET or SIMNET may participate. At their own discretion, Blue Cell teams may create additional sections with more limited access.
- The board may require user registration and password authentication before granting posting access. If so, a new user must be able to register without requiring any action on the part of the Blue Cell team. The user registration process may include automated methods for verifying an applicant's legitimacy (i.e., verification of an email address, a CAPTCHA code, and so on).
- Users must be able to recover their account passwords if forgotten, without requiring any action on the part of the Blue Cell team.

2.7 IPv6 Web Server Service

2.7.1 All BLUENET web servers must be configured as dual-stacked machines that respond to both IPv4 and IPv6. The web server(s) must be able to service the user's request using both formats.

2.8 Secure SHell (SSH)

2.8.1 Required port usage: TCP 22

2.8.2 All Linux workstations must respond (full session) to SSH logins from the all of the local BLUENET user workstations and Gray Cell Relay boxes using domain credentials.

2.9 Remote Desktop Protocol (RDP)

2.9.1 Required port usage: TCP 3389

2.9.2 All Windows workstations must respond (full session) to RDP logins from the all of the local BLUENET user workstations and Gray Cell Relay boxes using domain credentials.

2.9.3 Gray Cell's Relay box must be able to respond (full session) to Gray Cell user RDP logins from the HQ subnet.

3.0 User Workstations

3.0.1 White Cell will provide user workstation images to each Blue Cell in the course of exercise setup. For each BLUENET, user workstations shall share a common subnet and will be used by White Cell and Gray Cell personnel. During the active phase of the exercise:

3.0.1.1 User workstations shall not be available to Blue Cell in any fashion while White Cell or Gray Cell is using them: Blue Cell shall not use these workstations, log into them locally or remotely, monitor or execute processes on them, or monitor White or Gray Cell workstation activity through physical or virtual means.

3.0.1.2 During active duty hours, if Blue Cell wishes to perform maintenance on a user workstation, Blue Cell must gain permission of the local White Cell representative who will take into consideration the mission needs of the Gray Cell user prior to allowing for Blue Cell access. Blue Cell may

perform user workstation maintenance without White Cell permission if the Gray Cell has left for the day.

3.0.1.3 Participants *must* use the workstation images provided for the exercise. Removal and replacement of the images with *clean* images is strictly prohibited and will result in scoring penalties to be determined by the White Cell.

3.0.2 Two Windows user workstations will be provided in the form of virtual machine images about one month before STARTEX. They will be based on Windows 7 (Service Pack 1). Both workstations may be tainted with pre-positioned configuration errors and malware. Blue Cell is encouraged to closely examine these workstations and remove any suspicious files and change security settings – keeping in mind the users' operational needs and White Cell's approved software list (published separately and available on the CDX HQ web site). Blue Cell shall advise White Cell of each file removed or modified. To facilitate scoring, these Windows workstations shall be named:

- **delta**
- **gamma**

** Note – Both DNS *and* Machine Name must resolve as their represented names: "delta" / "gamma"

3.0.3 Two Linux user workstations will be provided in the form of virtual machine images about one month before STARTEX. They will be based on RedHat Centos or Ubuntu. Both workstations may be tainted with pre-positioned configurations errors and malware. Blue Cell is encouraged to closely examine these workstations and remove any suspicious files and change security settings – keeping in mind the users' operational needs and White Cell's approved software list (published separately and available on the CDX HQ web site). Blue Cell shall advise White Cell of each file removed or modified. To facilitate scoring, these Linux workstations shall be named:

- **alpha**
- **beta**

** Note – Both DNS *and* Machine Name must resolve as their represented names: "alpha" / "beta"

3.0.4 The user workstations will simulate systems controlled by each Blue Cell, but not necessarily properly configured or maintained by those units. White Cell and

Gray Cell will use the user workstations to generate traffic on the exercise network, evaluate service availability, and simulate the behavior of normal users.

3.0.5 The user workstations will come preloaded with software from the Approved Software List – which shall remain installed throughout the active phase of the exercise. Software may be removed (or added) during a maintenance period but, no software that is on the White Cell Approved Software List shall be permanently removed (or added) from the user workstations without explicit White Cell approval.

3.0.6 During active operations, Blue Cell shall not add, in any fashion, any software, task, process, or any other component on the user workstations unless it is specifically provided by White Cell and designated in a tasking order during the course of the exercise. If a workstation is taken off line for maintenance, diagnostic software may be run on the system. Before bringing the machine back online, this diagnostic software must be removed.

3.0.7 It is to be known that the user workstations *will not* have up-to-date patches at STARTEX. Blue Cell teams *may update them* using provided patches located on HQS update servers and in accordance with White Cell advisories and instructions. Necessary patching instruction will be provided by White Cell during the course of the exercise.

3.0.8 If files are thought to be of suspicious origins, Blue Cell teams may *replace* specific files already installed on any of the user workstations with a known-good copy of the same software (available from White Cell at the CDX HQ web site). The new files must be from exactly the same software version and patch level as the files being replaced. Files that are not available from the White Cell at the CDX HQ web site shall not be introduced to the user workstations without approval from White Cell.

3.0.9 Any additional workstations built by Blue Cell personnel will be considered administrative workstations, and will not be subject to the provisions of this section. They may be used by Blue Cell personnel, will not normally be required to support White Cell or Gray Cell activities, and may be patched at Blue Cell discretion.

3.0.10 User workstations may be configured to operate in a virtual machine (VM) environment. However, White Cell and Gray Cell users are very active and

require continuous access to the network. Points will be lost if these workstations are not simultaneously available.

3.0.11 For maintenance reasons, Blue Cells may find it convenient to rollback workstation VMs to a previous versions. The scoring system will survive VM rollbacks but points shall be lost for this action due to the resetting of the configuration files and version control features that are on each user workstation – it will look like the scoring system has been tampered. And, rolling back might interfere with White or Gray Cell local file systems – resulting in further loss of points.

3.0.12 Any software preloaded on user workstations (as provided by White Cell) may be reconfigured or implemented by Blue Cell.

4.0 Traffic Generator / Scoring System

4.0.1 Each user workstation shall run a White Cell provided traffic generator (RubberNeck) that will be used for checking service availability and play a significant role in scoring. Failure to keep these workstations running will negatively impact scoring.

4.0.2 RubberNeck checks the availability of all user workstations on the local BLUENET by accessing remote administration functionality. Windows workstations must have RDP configured. Linux workstations must have SSH configured. Note: this functionality only needs to be accessible within the BLUENET; RubberNeck does not perform this validation from external locations (RDP on the user workstations still must be accessible to Gray Cell users remotely from CDX HQ). RubberNeck also checks the availability of all services across the exercise network, both public services from other BLUENETs, and local services within the local BLUENET.

4.0.3 Automated scoring will also take into account elements of information confidentiality and integrity. Scoring software (TokenAgent) will distribute and validate unique “Tokens” that shall be loaded on (ALL NODES) to BLUENET servers. Details, including the location of token directories and the operation of TokenAgent, are provided in the *CDX Scoring Specification.*

5.0 White Cell Connectivity on Each BLUENET

5.1 Each BLUENET implementing the locally physical infrastructure option for CDX 2016 shall maintain two dedicated connections into its local network for potential use by the local White Cell liaison. Each BLUENET implementing the remote virtual infrastructure shall also permit connections to its virtual network by White Cell, and White Cell will establish two virtual hosts at any point within the BLUENET. These two access points and their IP addresses shall be off limits to the Red Cell.

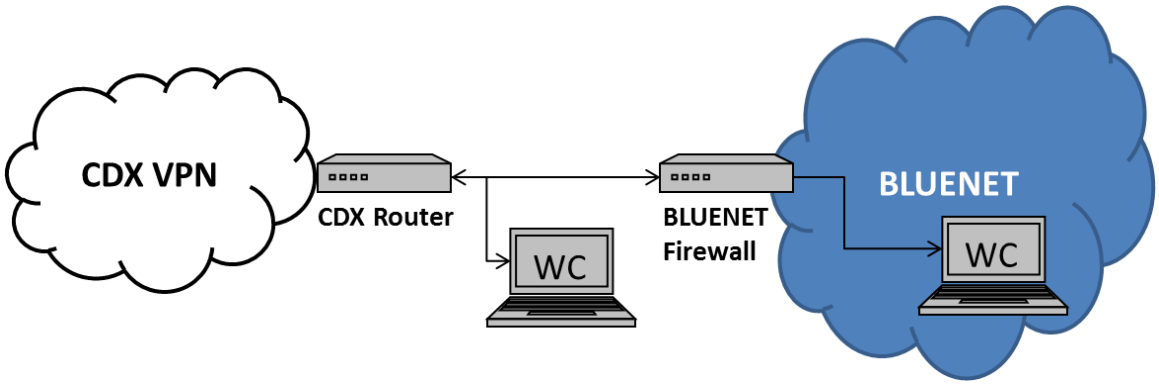

Figure 1, White Cell Connectivity

5.2 The first network connection is for network diagnostic purposes only and shall be placed within the inner VPN interface, but outside of the outermost Blue Cell firewall.

5.3 The second network connection is for White Cell email and other operational uses and shall be placed inside the Blue Cell's interior network, preferably in the same subnet as the Gray Cell user workstations, with full access to all BLUENET user services.

5.2 These two access points and their IP addresses shall be provided to the White Cell and shall be used solely for White Cell testing, diagnostics, and messaging purposes – they shall be off limits to the Red Cell.

6.0 Public Key Infrastructure

6.1 Blue Cells may use Public Key Infrastructure (PKI) to digitally sign and encrypt sensitive data. To facilitate this, White Cell shall establish a root Certificate Authority within the CDX HQ domain.

6.2 White Cell shall create valid certificates for all required accounts. Blue Cells shall be expected to install the certificates in the appropriate manner.

7.0 Network Performance Standards

7.1 Each BLUENET shall maintain a network connection to the CDX Network with minimum bandwidth of 1 megabit per second and with an average latency of 200 milliseconds or less. Not maintaining these standards will negatively affect Blue Cell scores.

7.2 Network performance will be monitored by CDX HQ throughout the exercise. Allowable bandwidth between each Blue Cell and CDX HQ shall be actively balanced to allow for uniform throughput by each Blue Cell participant.

7.3 Blue Cells may block network traffic but care should be taken not to block traffic associated with scoring.

7.4 Blue Cells shall not perform any traffic shaping – neither inbound nor outbound. This includes temporarily blocking or delaying inbound connections (otherwise known as tarpitting).