This Briefing is: UNCLASS/FOUO

United States Central Command

Monitoring the Tactical Network

13 April 2010

This Briefing is: UNCLASS/FOUO

NetOps Intent

•As troop levels increase, demand for services will increase, NetOps elements must quickly meet current demand and posture for future demand based on force packages and planned movements

•The goal of the NetOps framework is to create a culture where unity of effort takes precedence over control of effort---a departure from past NetOps constructs

•NetOps elements focus on delivery and management of IT services within the AOR.

•NetOps will focus on the critical components of Enterprise Management, Content Management and Network Assurance using a Service Management framework

NetOps Governing Tenets

• NetOps framework must be consolidated to the operational chain of command

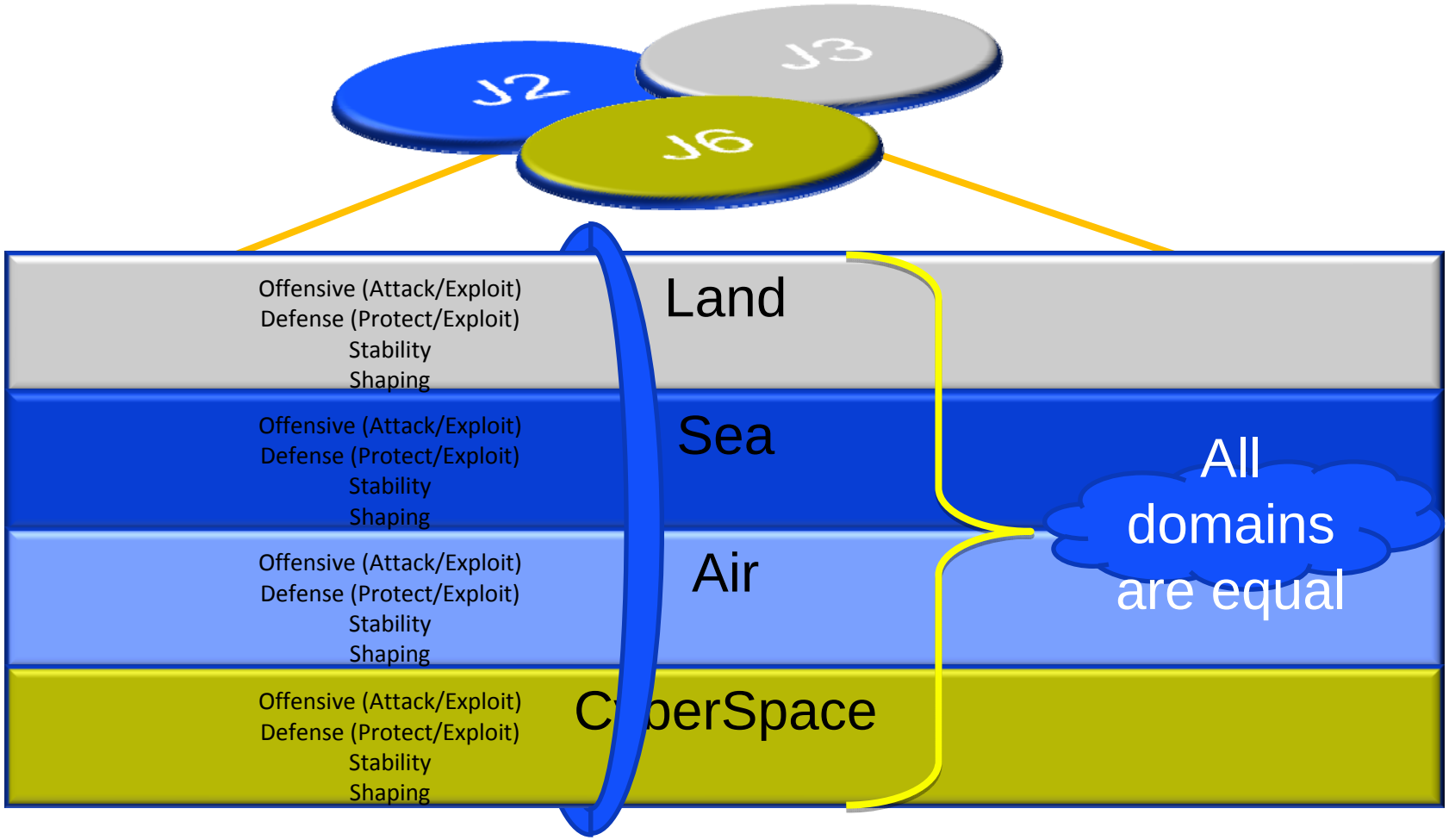
•NetOps authority can be delegated and delegation can vary by phase of operation

•Commanders with NetOps authority will:

- Define NetOps authorities within his assigned battlespace or functional task force authorities

- •Be responsible for Information assurance/Computer Network Defense(IA/CND) posture of the network across the full scope of his NetOps authority

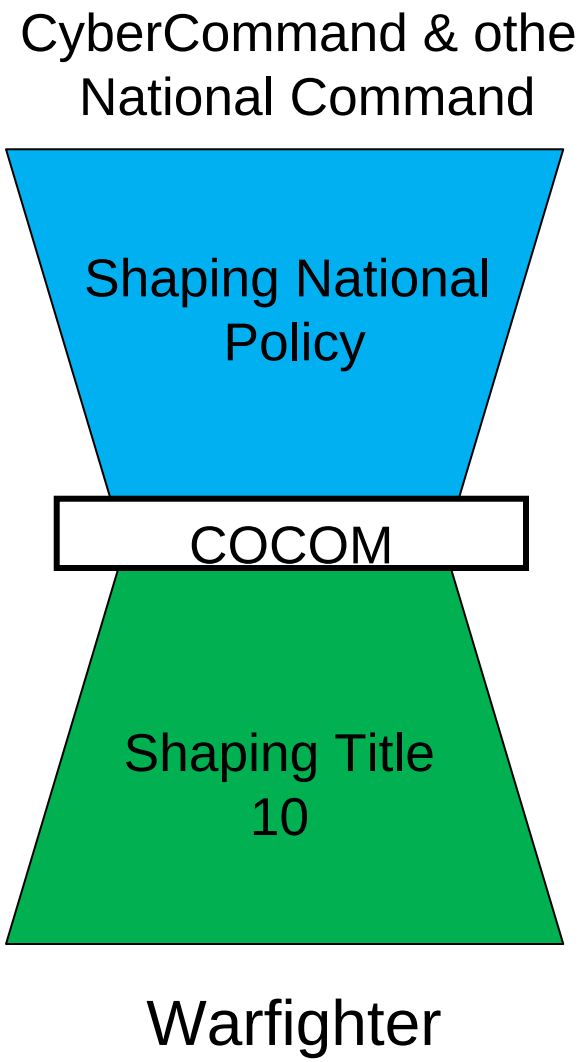
NetOps Spectrum



Integrate C4ISR approach into entire theater

Role of USCENTCOM in NetOps

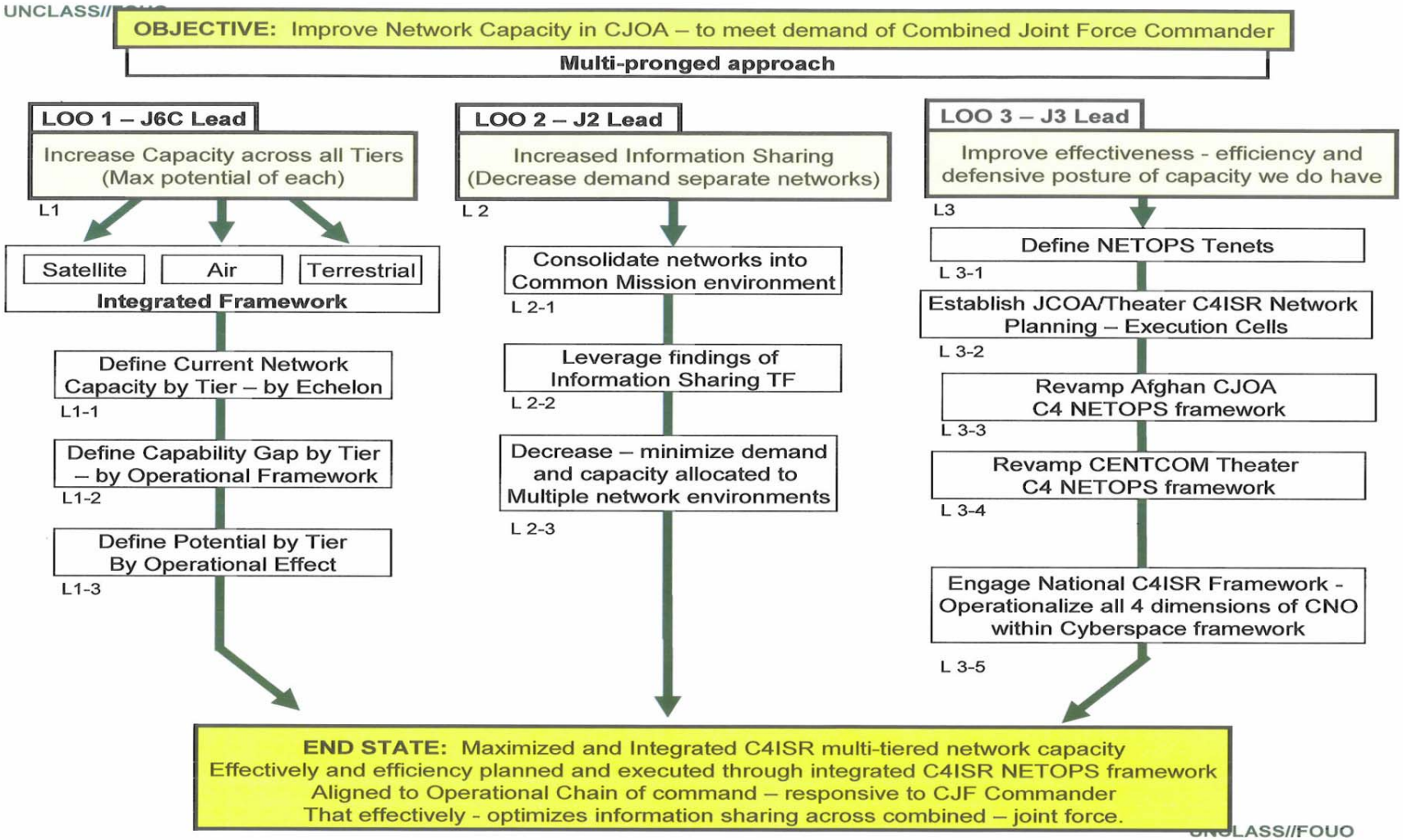
- **C4ISR approach for entire theater**
- **Ensure the full spectrum of NetOPs is enabled**
- **Linkage to J2, J3/ Cyberwarfare and to AOR**



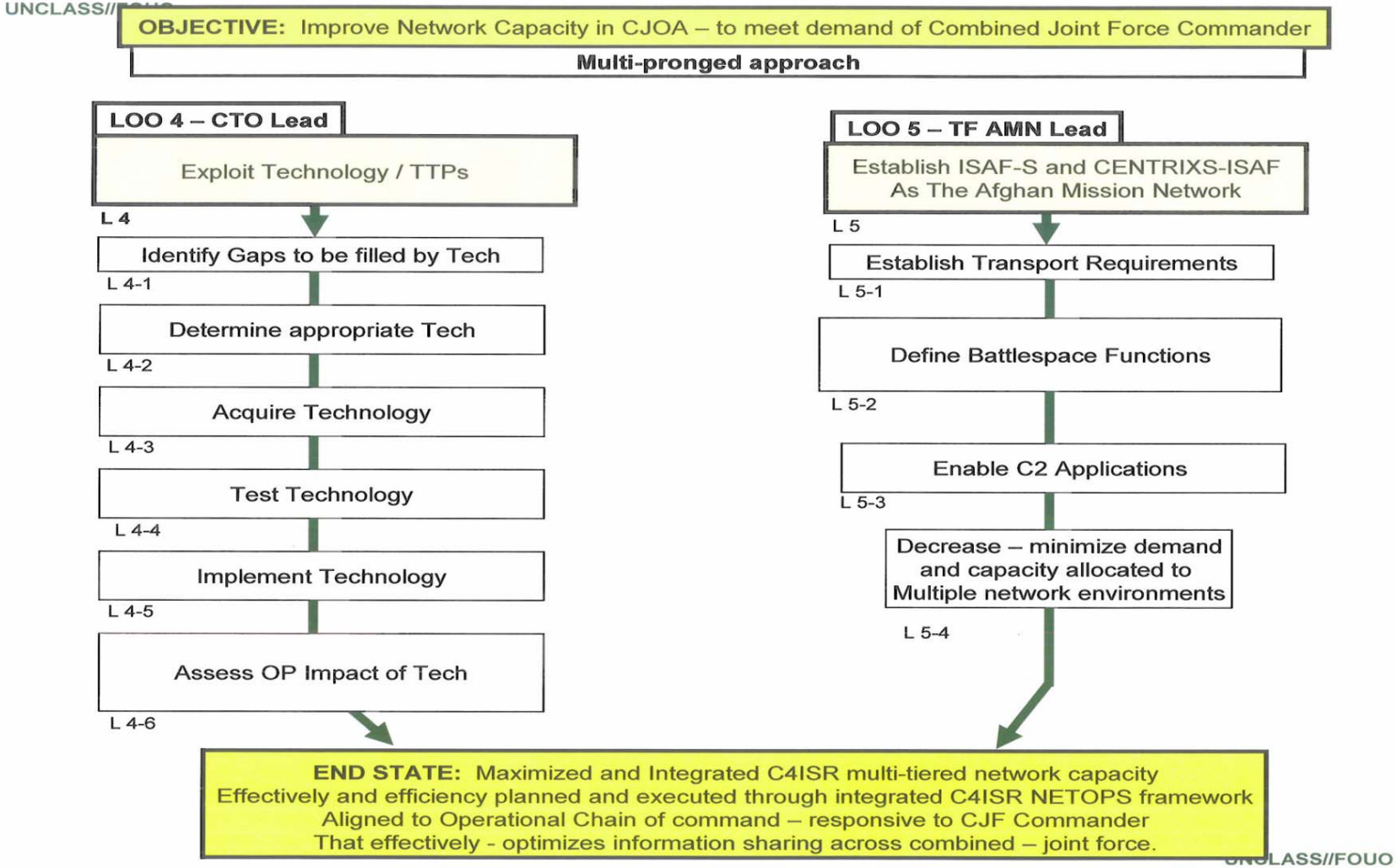
TF 236

- Coordinate and synchronize efforts of J2, J3 and J6
- Provide network support to the CJOA
- Increase capacity, optimize and gain efficiency
- Improve information sharing by creating a common mission network

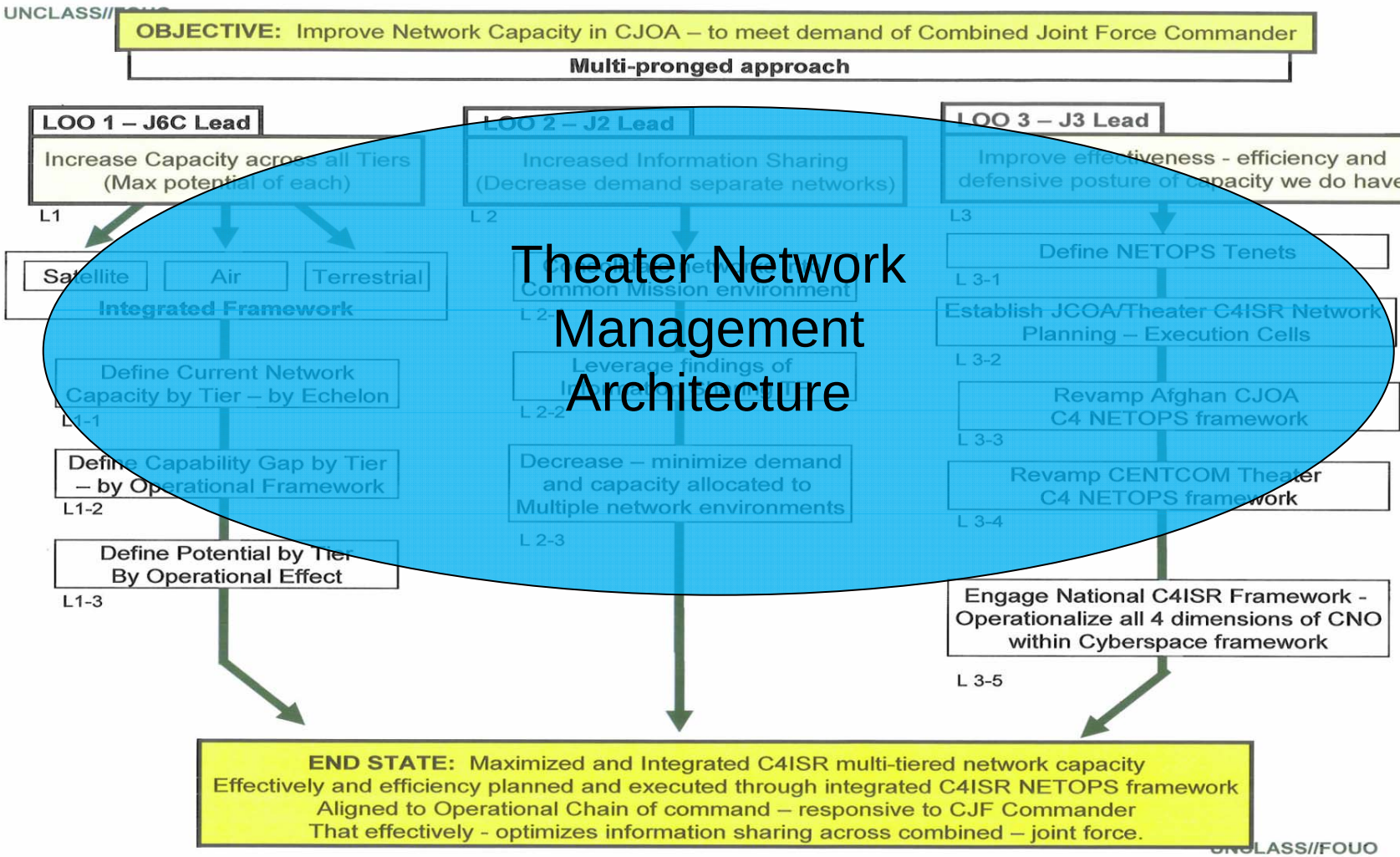
TF 236 Lines Of Operation



TF 236 Lines Of Operation (cont)



Baselining the Network



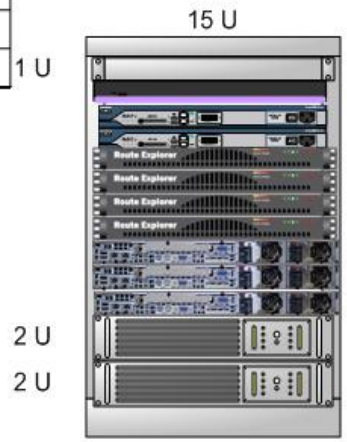
Challenges

- **Vendors traditionally prefer appliance based solutions**
- **Rack, Power, Ping are a scare resource within the CJOA**
- **Tiered information sharing and access to Network Management information**
- **Visibility to Security devices and information, has traditionally been second hand through the Title 10 organizations**
- **Interoperability with indigenous tools**
- **Training and Sustainment**

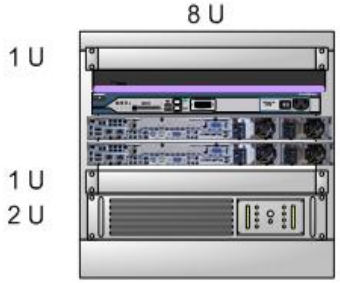
Virtualized and Ruggedized

THEATER NETWORK MANAGEMENT ARCHITECTURE (TNMA)

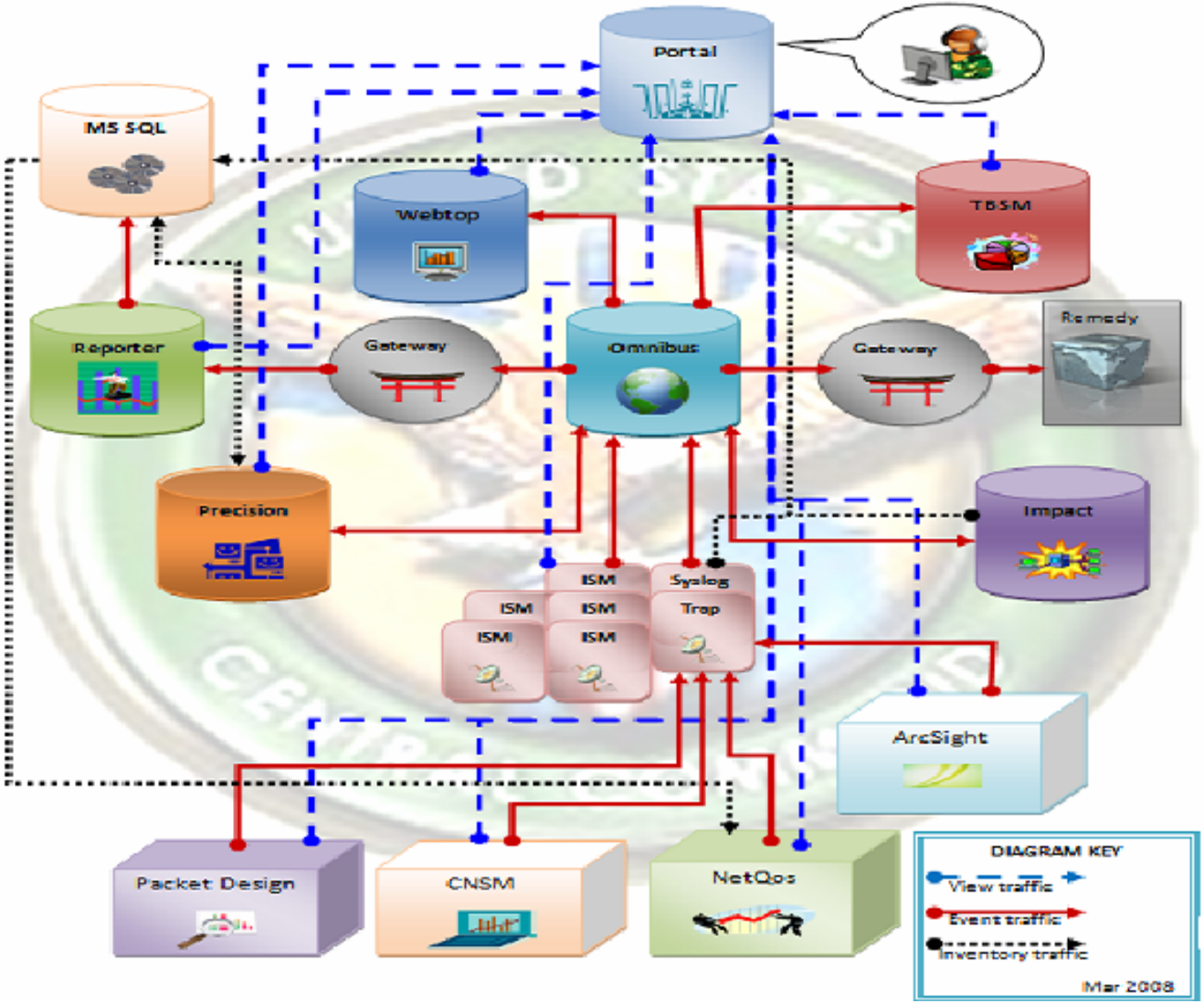
Total Amps: **27A**
Total Heat Dissipation:
18000 BTU/h
Half-Load UPS
Backup: **7min**



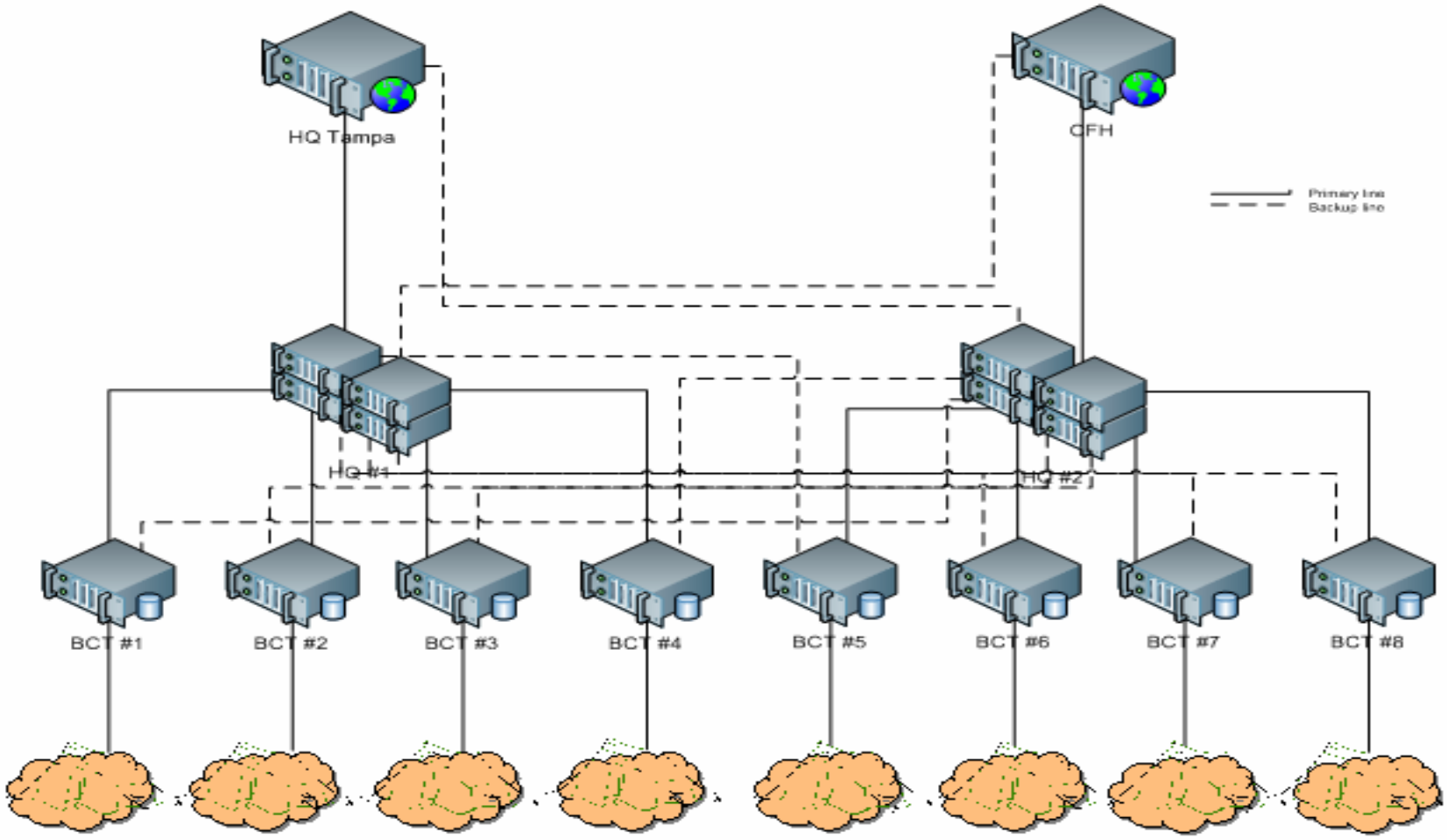
Total Amps: 14**A**
Total Heat Dissipation:
9000 BTU/h
Half-Load UPS
Backup: 10**min**



USCENTCOM TNMA AV-1(U)

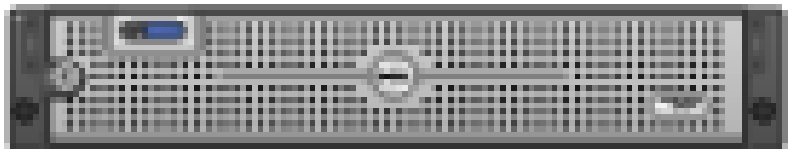


Mulit- Tiered End-to-End Visibility



Collection Enhancement

Harvester



Harvester
- Collect and store NetFlow traffic

VMWare
- Enhancement to the Architecture through Virtualization

Harvester
- Collect and store Netflow traffic

SNMP / SYSLOG
- Optional Features
- SNMP Probes collect data locally
- SYSLOG probes collect data locally
- Condenses chatter across the network(s)
- Increases Net-Defense visibility

Object Server
- Optional Feature
- Repository for event data
- Access using SQL
- Deliver future tools
- Performs automations
- Manages de-duplication and correlation
- Interface to external systems

Theater Network Management Architecture

- **Implement a fully integrated, robust tool suite supporting real-time, correlated configuration, performance, status/event, and topology information in a common format enabling analysis and modeling capabilities available to all Components, JTFs, and Agencies**
- **Makes Service Assurance and Service Delivery possible across the network**
- **Enhances network defense through information exposure**
- **TNMA deployed on SIPR, NIPR and CX-I networks in the CJOA**

Questions?

Points of Contact

- **Donn Westerhoff, USCENTCOM CCJ6 Chief Technology Officer, 813-827-4557, westerda@centcom.mil**
- **Allen Noble, FedtechServices, 813-774-8060, anoble@ezfts.com**