GIG 3.0 Design Factors

An Architecture Proposal for
Aligning NetOps to the Operational Chain of Command

Mr. Randy Cieslak
CIO

U.S. Pacific Command
11 January 2011

This brief is classified:

UNCLASSIFIED

Cyberspace Operational Requirements

Brig Gen Brett Williams,
Director, C4 Systems Directorate

Mr. Randy Cieslak
Chief Information Officer

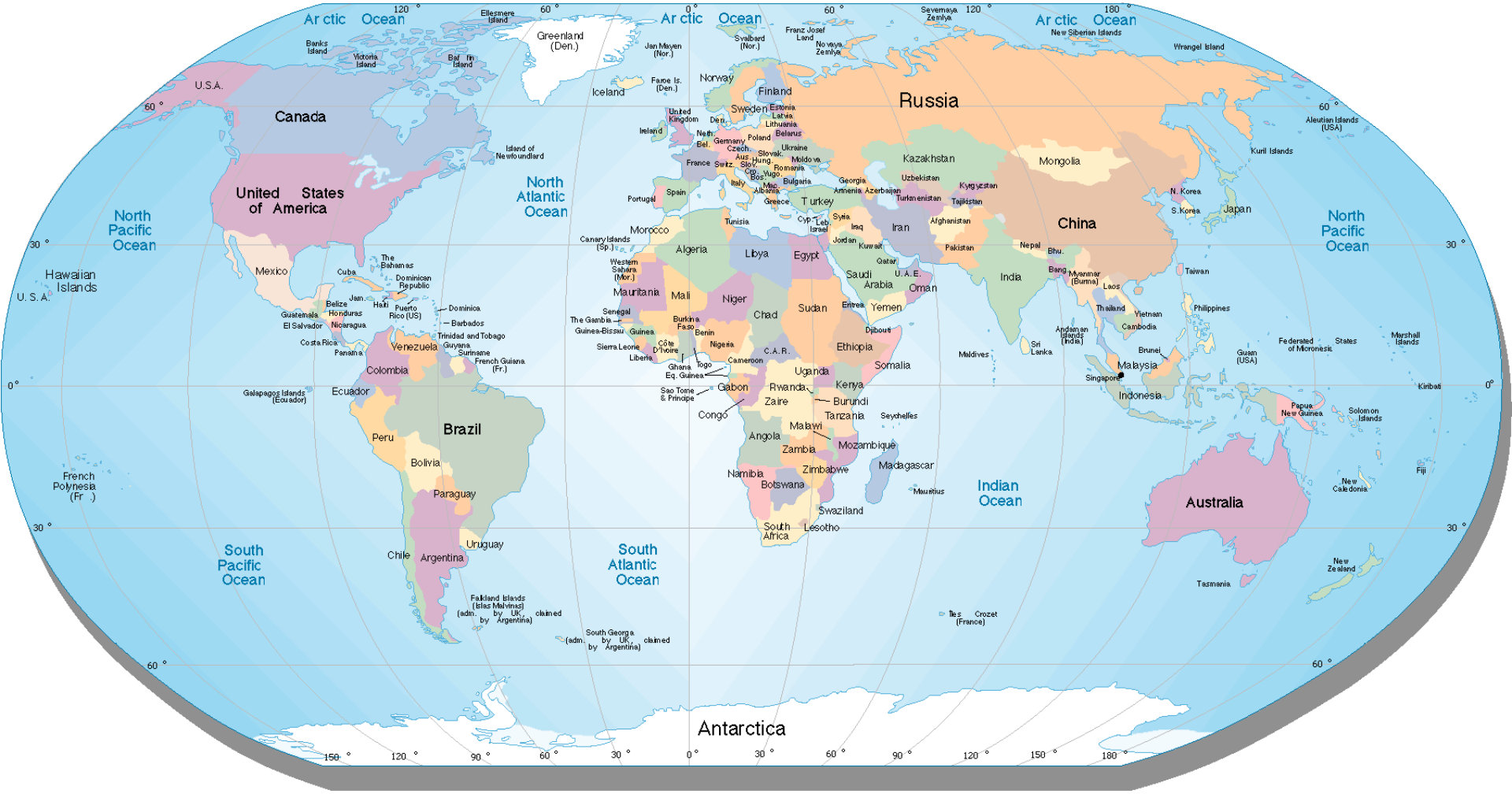
U.S. Pacific Command
12 November 2010

This brief is classified:

UNCLASSIFIED

Geographic JOAs

Where is the CYBER JOA?



- **REQUIREMENT: The JFC must C2 cyberspace operations in the same way he executes C2 in the air, land and maritime domains.**

- **CONCERNS:**
  - **JFCs lack the architecture, CONOPS, TTP, personnel, training, tools, doctrine and policy for full spectrum cyber operations**
  - **It's all one big GIG, there is no Cyber JOA."**
  - **The GIG was not built for operations.**
  - **Sensors are not effectively focused on critical C2 services**
  - **Type 1 encryption is not responsive to operational requirements**
  - **Mission-Risk authority in cyberspace is currently held by CYBERCOM and the Services, not the JFC**

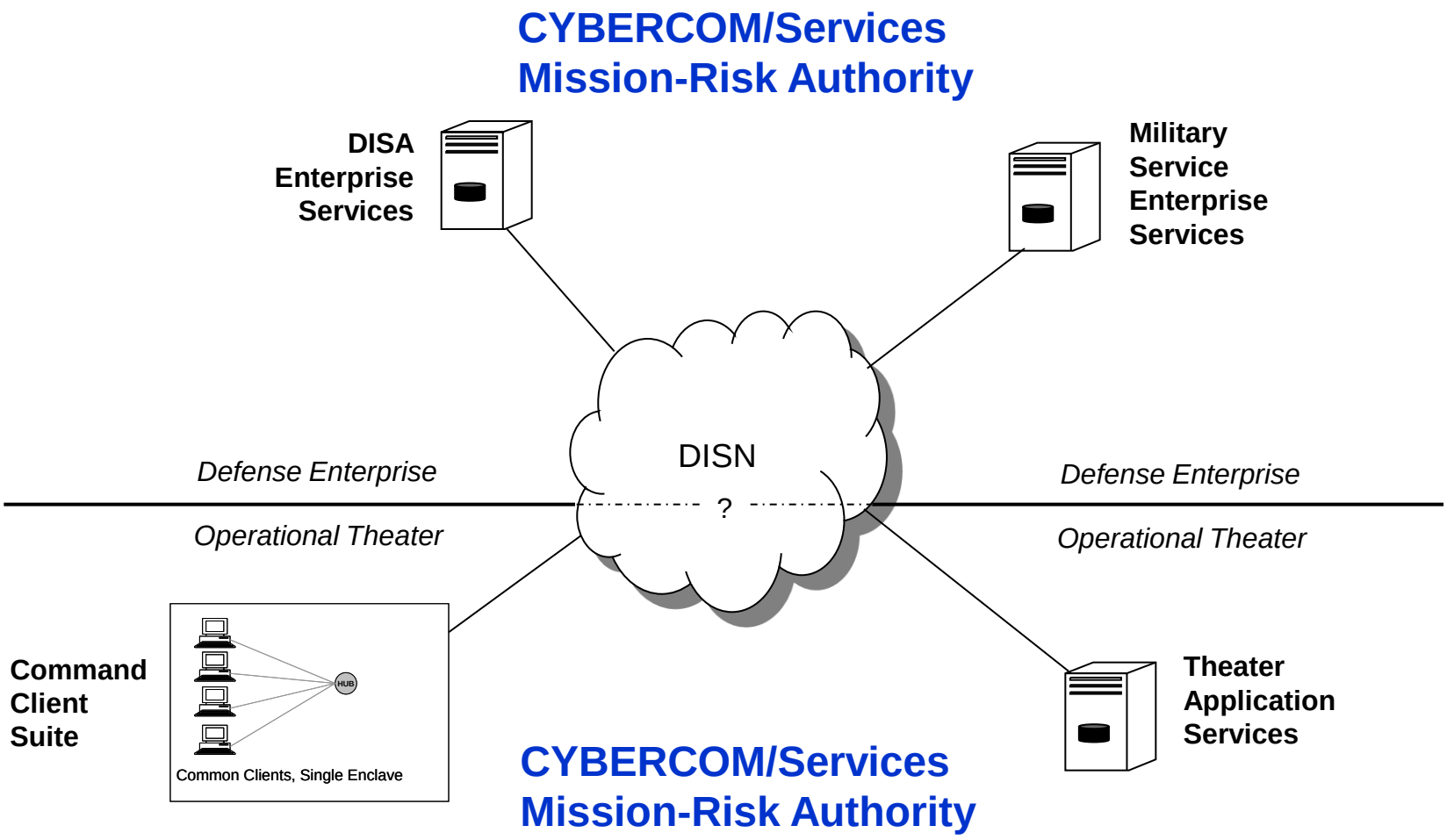
Cyberspace is the <u>only</u> man made domain.
It can and must be shaped for the JFC to make decisions, direct actions and accept risk in a way that does not affect the rest of the GIG.

GIG 3.0

- **GIG 2.0 promised an information advantage to the warfighter.**
  - **It did not address the key issue of "one big GIG"**
  - **It did not align the architecture to the chain of command.**

- **Components of GIG 3.0:**
  - **Cyber JOA defined by an Operational Network Domain (OND)**
  - **Enclaved architecture to enable defense in depth, information sharing and agility**
  - **Multi-enclave client for efficient information access**
  - **Associated personnel, training, tools and TTP to C2 Cyberspace Operations**

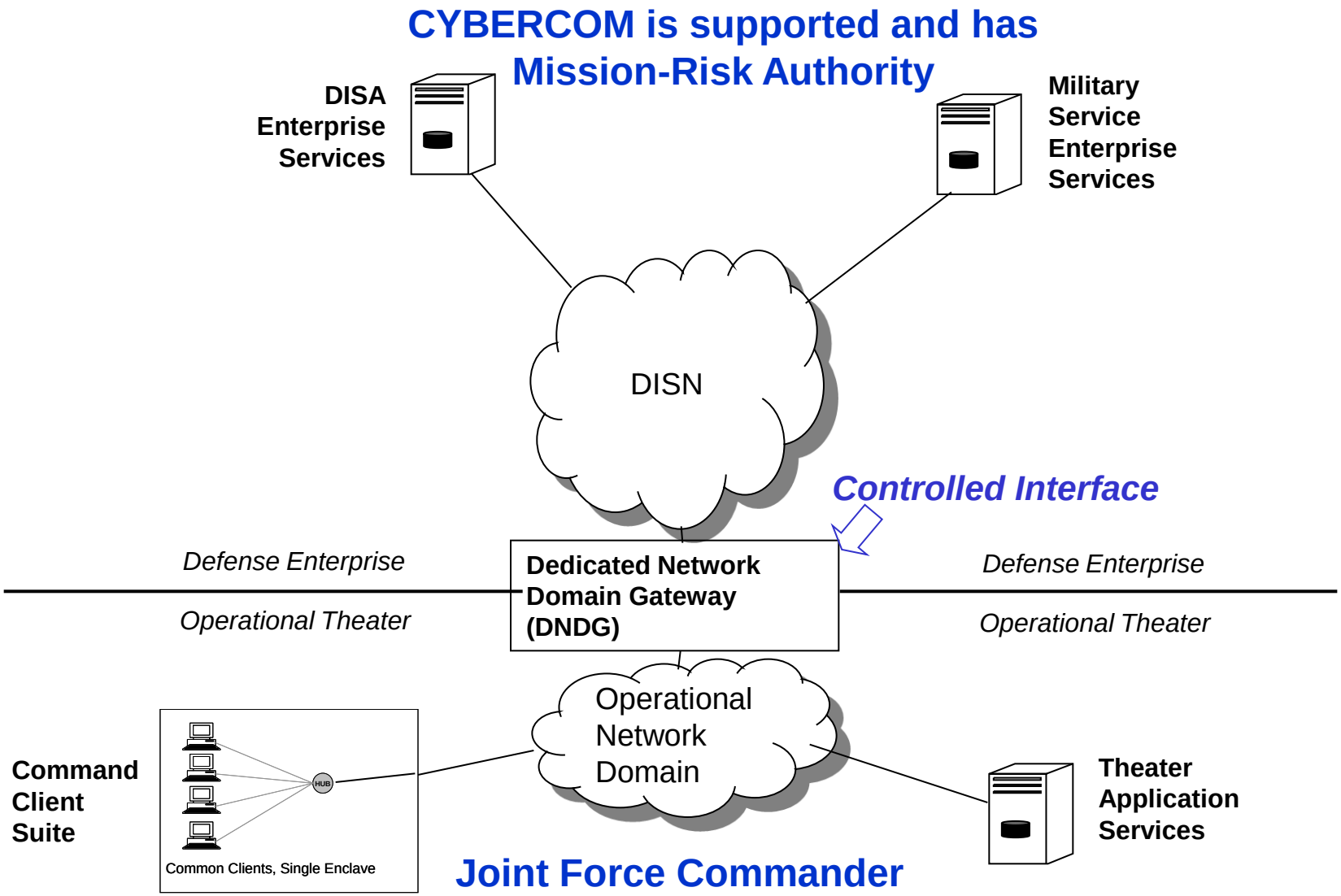
Current Architecture



Characteristics of a Cyber JOA

- **The Cyber JOA defines the friendly forces operational network domain and is focused on the operate and defend mission.**
- **The Cyber JOA provides a platform for dynamic network defense and facilitates CNA and CNE.**
- **The Cyber JOA is defined by the systems and networks critical for Joint Force Command and Control**
- **The Cyber JOA is governed by existing doctrine and policy.**
- **The Cyber JOA allows the commander to:**
  - **Sense the environment**
  - **Make decisions**
  - **Direct operations**
  - **Assume risk**
- **The Cyber JOA requires CYBERCOM and the services to execute their GIG wide responsibilities within the JOA.**

Defining the JFC's "Cyber JOA"



Tenets of an Operational Network

- **The network must be Commander Centric**
  - **Commanders balance risk against mission in all domains except cyber**
  - **An operational network addresses this issue by aligning NetOps to the Operational Chain of Command**
  - **The GIG cannot be vulnerable to risk assumed by one commander**
  - **The operational network must accommodate the scheme of maneuver**
- **Commanders must define the requirements for designing and building the Operational Network**
- **Commanders must have the authority and responsibility to operate and defend the operational network.**
- **Supported and supporting roles must be articulated**
  - **Clear delineation between the responsibilities of the service components and the operational commander**
  - **Clear definition of STRATCOM/CYBERCOM's role to support the operational network while they Operate and Defend the GIG**

Barriers to Operationalizing the Network

- **It's all one big GIG, there are no JOA boundaries in cyberspace**

- **We are burdened by the costs and policy associated with TYPE 1 encryption — works against flexibility, adaptability and robustness needed to accommodate the scheme of maneuver.**

- **Current culture and doctrine delegate OPCON of all forces <u>except</u> Cyber forces to the Operational Commander. Services and CYBERCOM retain network authority and responsibility.**

10 Propositions Regarding Cyberspace Operations

(With acknowledgement to Phil Meilinger's 10 Propositions Regarding Air Power)

1. **The commander is responsible for cyberspace operations; he must C2 cyber just as he does the air, land and maritime domains.**
2. **C2 of cyberspace is the foundation for operational C2.**
3. **There are four lines of operation in cyber—operate, defend, attack and exploit, and defense is the dominant mission.**
4. **The commander must see and understand cyberspace to defend it and he cannot defend it all.**
5. **Cyberspace operations must be fully integrated with operations in the physical domains.**
6. **Our understanding of non-kinetic effects in cyber is immature.**
7. **Operational requirements drive cyber architecture, not the other way around.**
8. **Cyber is the only manmade domain--we built it, we can change it.**
9. **Operational impact is the relevant information, not number of megabytes exfiltrated.**
10. **Networks will always be critical and vulnerable--disconnecting is not an option, we must fight through the attack.**

Operationalizing the Network

- It's all one big GIG, there are no JOA boundaries in cyberspace
- We are burdened by the costs and policy associated with TYPE 1 encryption — works against flexibility, adaptability and robustness needed to accommodate the scheme of maneuver.
- Current culture and doctrine delegate OPCON of all forces except Cyber forces to the Operational Commander. Services and CYBERCOM retain network authority and responsibility.

Proposed solution:

Operational Network Domain (OND)

- **Defines the "Commander's Cyberspace JOA"**
- **Utilizes encryption techniques that give the Operational Commander the capability to C2 Cyberspace**

Fundamental Network Challenge
And
Proposed Solution

Agile Virtual Enclave (AVE)
Virtual Secure Enclave (VSE)

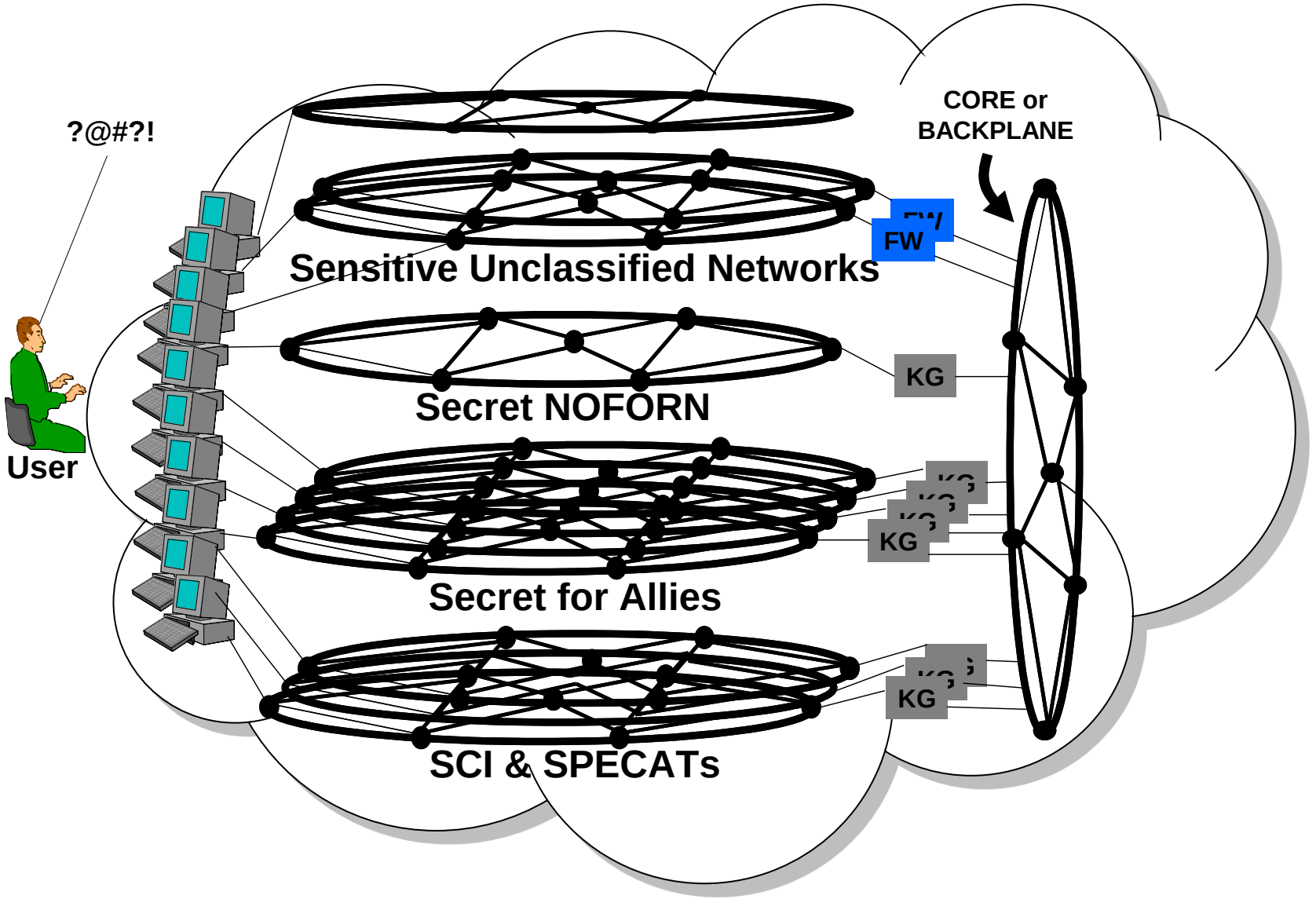
Mr. Randy Cieslak
Chief Information Officer

U.S. Pacific Command
8 December 2010

This brief is classified:

UNCLASSIFIED

Current Network Design—This needs to change



Virtual Secure Enclaves (VSE)
The foundation of the Operational Network Domain

- **The Operational Network is built on IPsec-based VSE's**

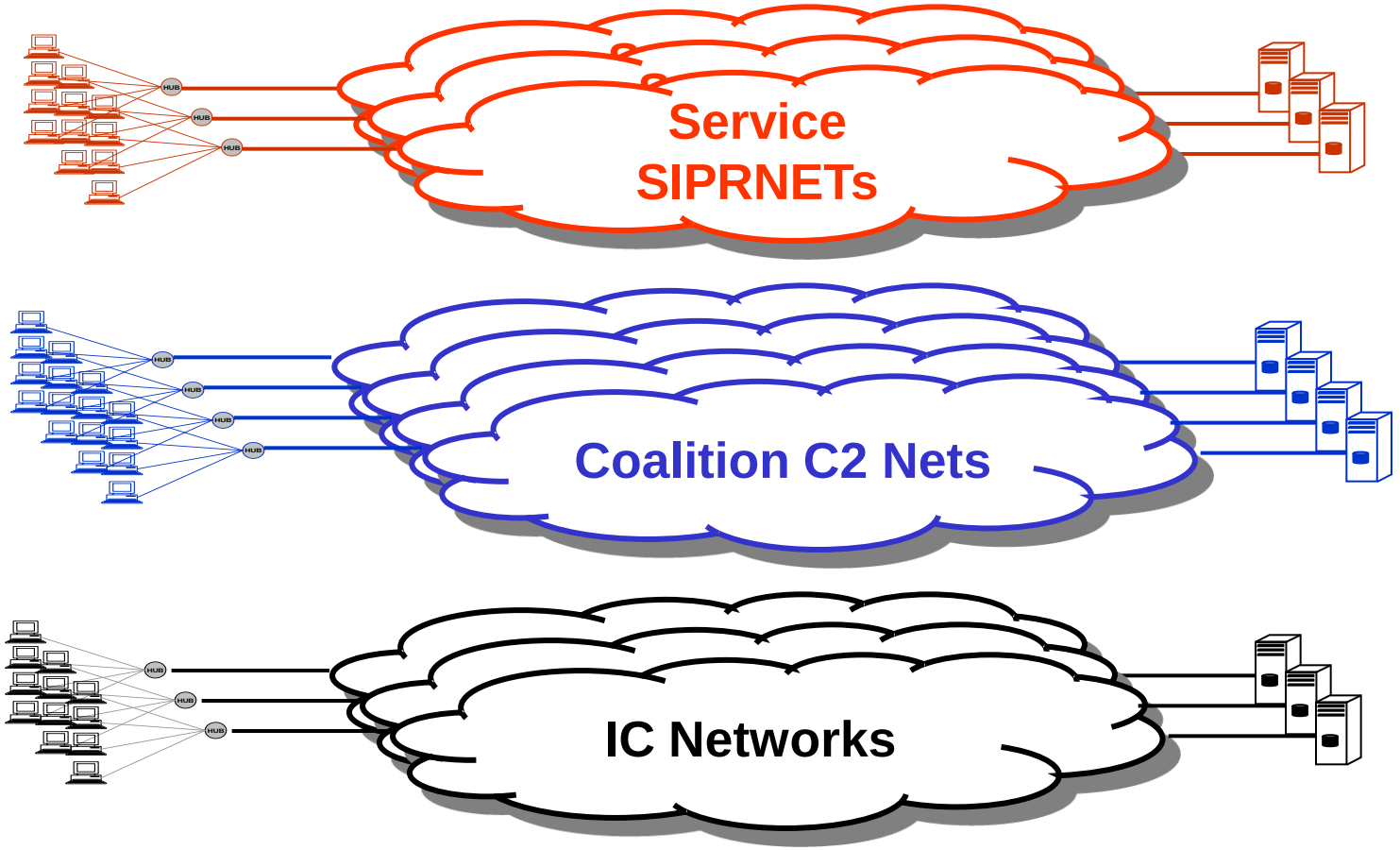
- **IPsec--Short for IP Security, a set of protocols to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement robust Virtual Private Networks (VPNs)**

- **IPsec provides a COTS/GOTS encryption capability that is certified for up to SECRET data**

- **Advantages of IPsec over TYPE 1 encryption**
  - **Reduces the Controlled Crypto "overhead"**
  - **Allows visibility into network traffic to enable use of Network Management Tools to execute QOS**
  - **Simplifies adding and removing enclaves from the OND**
  - **Potential to facilitate Computer Network Operations (CNO)**

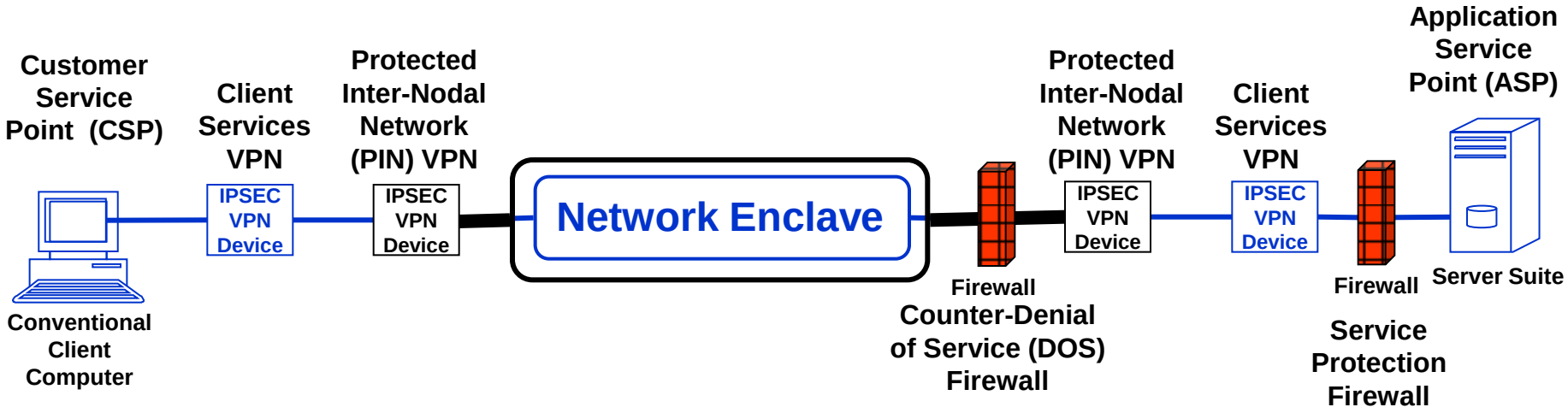
TYPE 1 without IPSec

Each enclave is a separate network requiring it's own separate infrastructure



(It's not this neat and orderly.)

Components of an IPSec Virtual Secure Enclave (VSE)



Network Enclave – A protected network environment that contains a single security domain (e.g., SECRET//REL USA)

Application Service Point (ASP) – Suite of servers dedicated to a single enclave to provide application services. (e.g., Web, E-Mail, COP and the like)

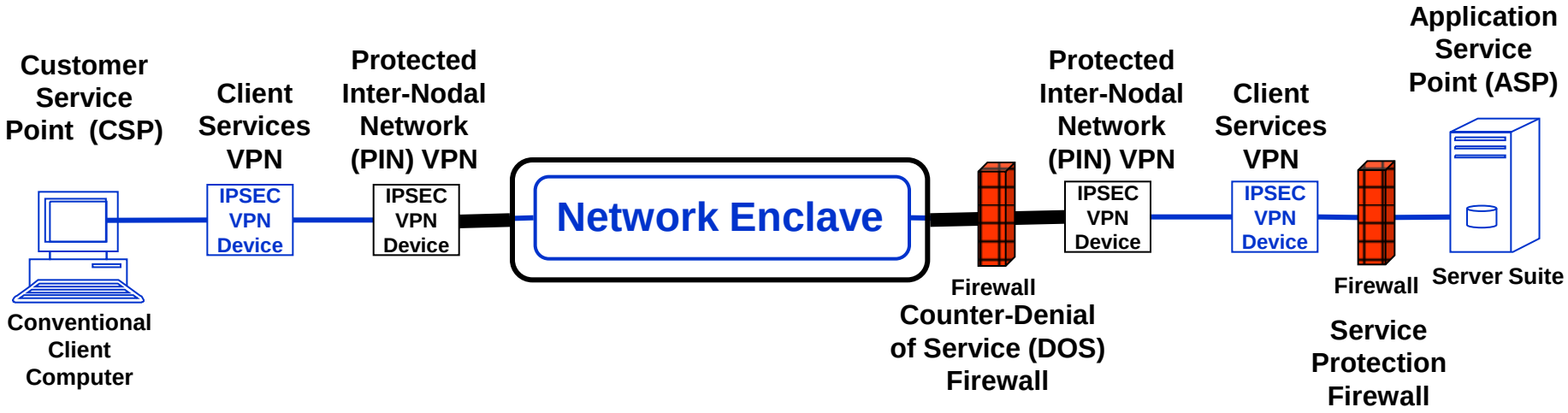
Customer Service Point (CSP) – User interface to the enclave

Client Services VPN – Protects users' data using NSA-certified IPSec encrytion. (First layer of wrapping)

Protected Internodal Network (PIN) VPN – Protects the network from intra-enclave threats such as malicious insiders, high-risk applications, or poor system hygiene.

ASP Firewalls – Protects the IPSec cypto from Denial-of-Service (DOS) attacks and adds additional robustness required for cross-domain use of a common network infrastructure by the application service.

Components of an IPSec Virtual Secure Enclave (VSE)



Network Enclave – A protected network environment that contains a single security domain (e.g., SECRET//REL USA)

Application Service Point (ASP) – Suite of servers dedicated to a single enclave to provide application services. (e.g., Web, E-Mail, COP and the like)

Customer Service Point (CSP) – User interface to the enclave

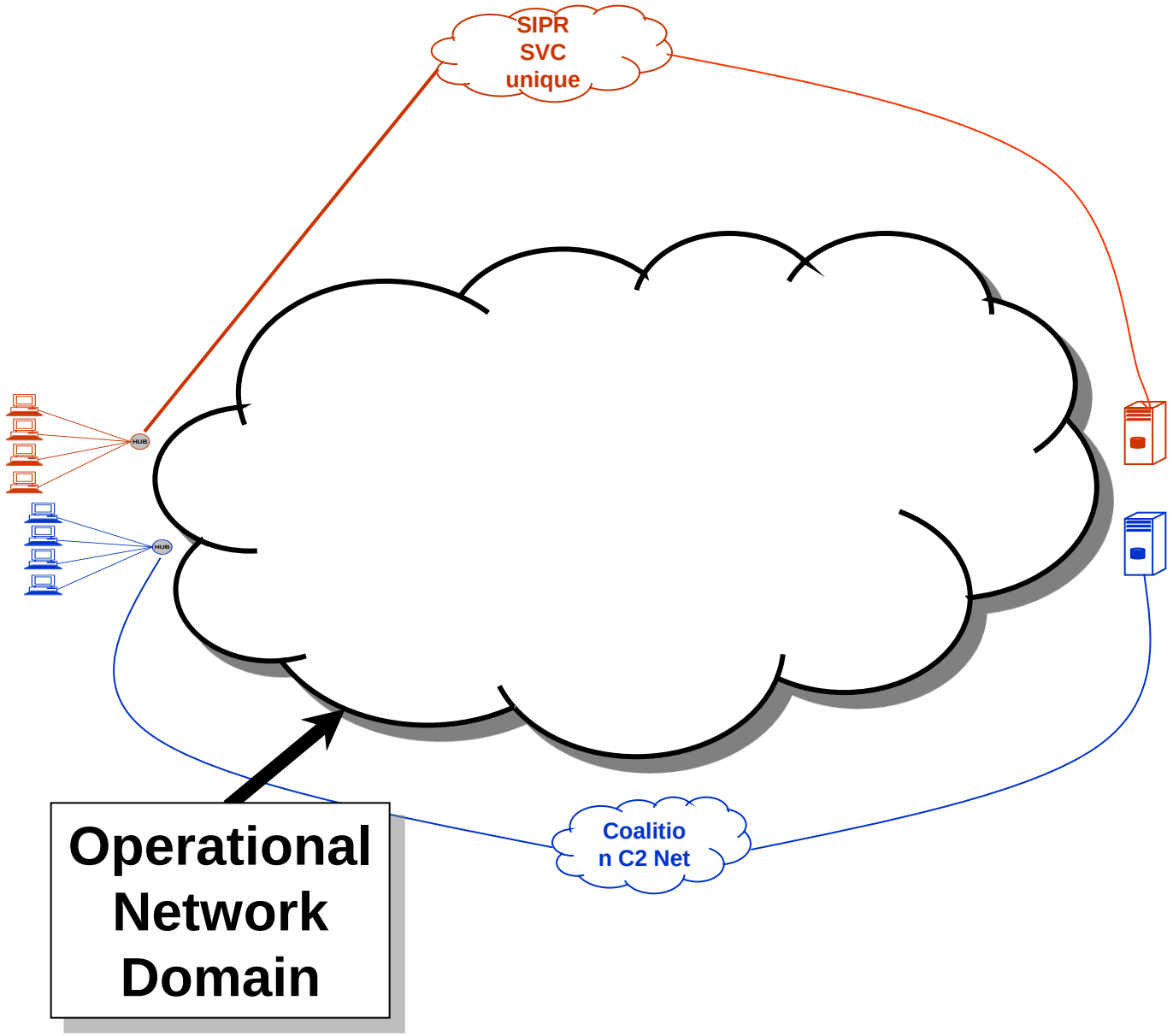
Client Services VPN – Protects users' data using NSA-certified IPSec encrytion. (First layer of wrapping)

Protected Internodal Network (PIN) VPN – Protects the network from intra-enclave threats such as malicious insiders, high-risk applications, or poor system hygiene.

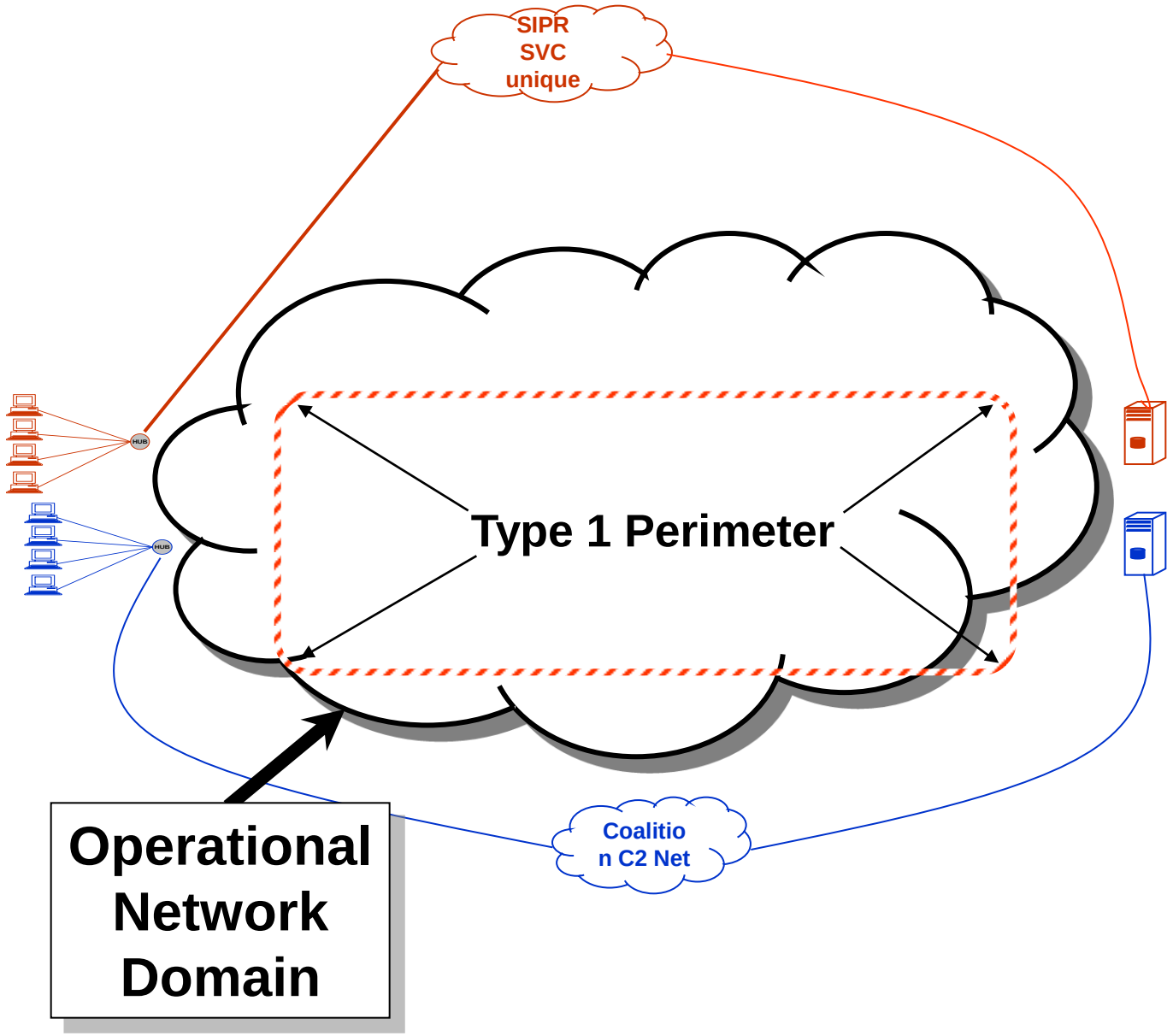
ASP Firewalls – Protects the IPSec cypto from Denial-of-Service (DOS) attacks and adds additional robustness required for cross-domain use of a common network infrastructure by the application service.

NB

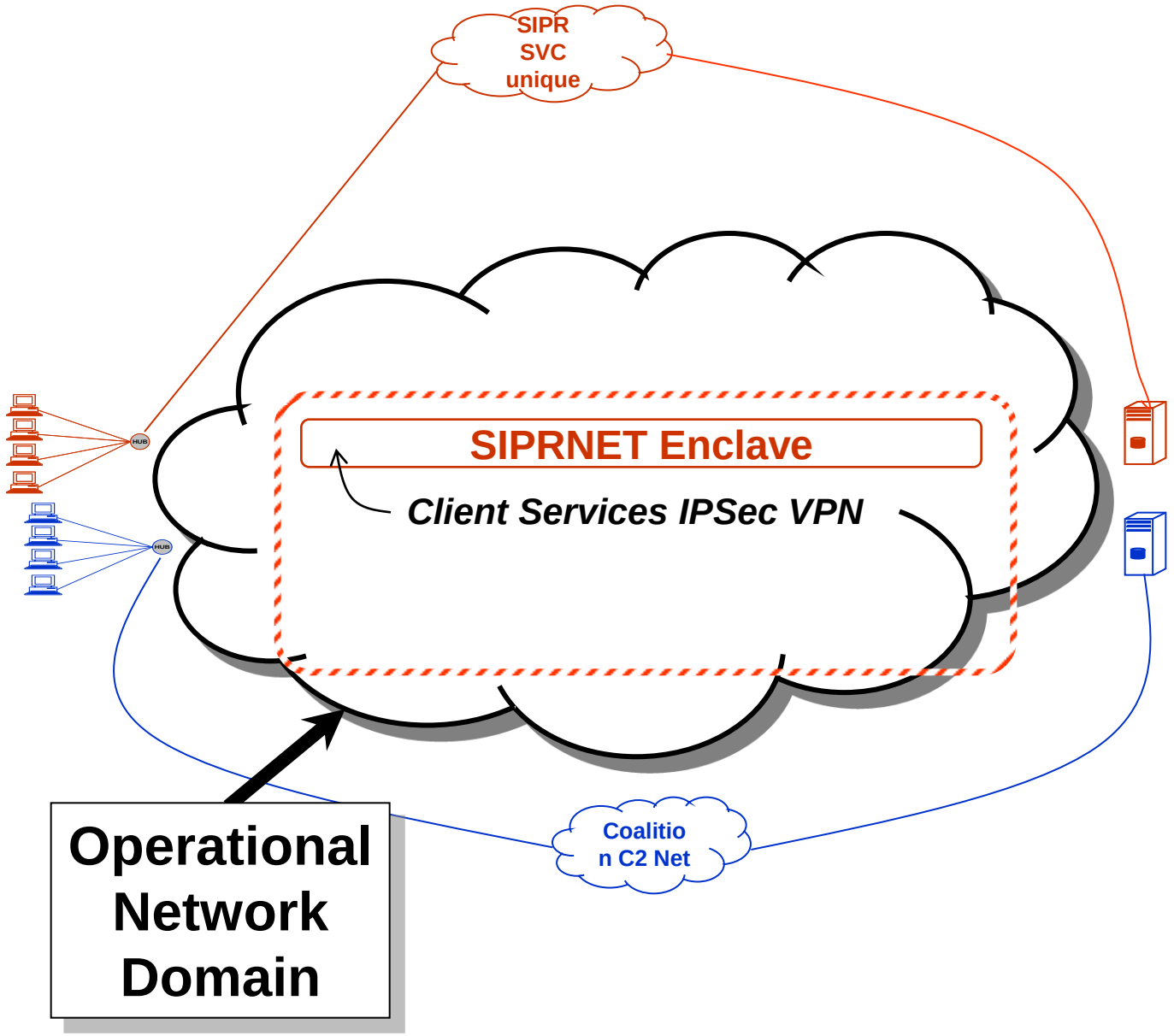
1. Establish a Perimeter for the OND



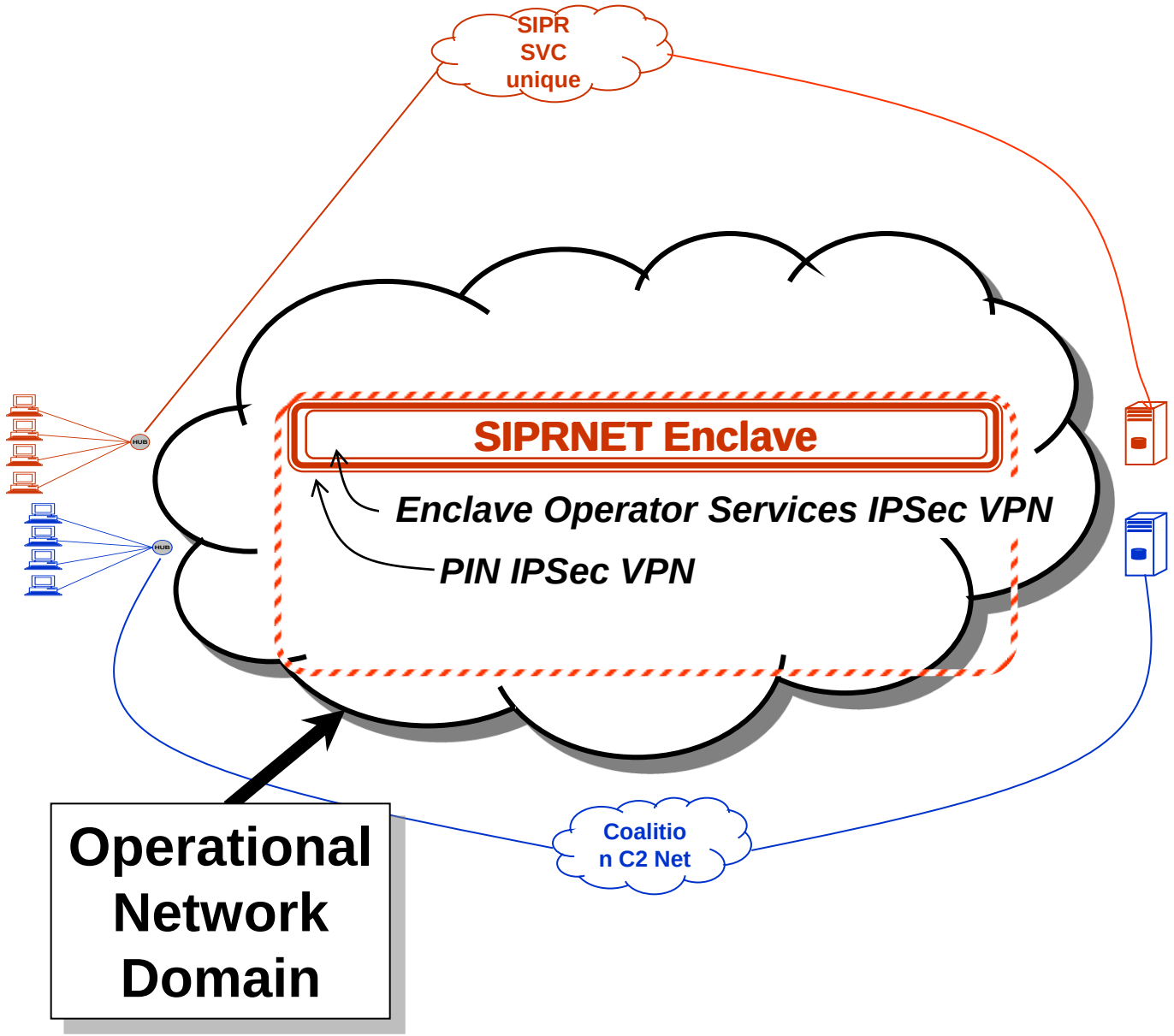
2. Establish a Type 1 Perimeter for the Classified Enclaves



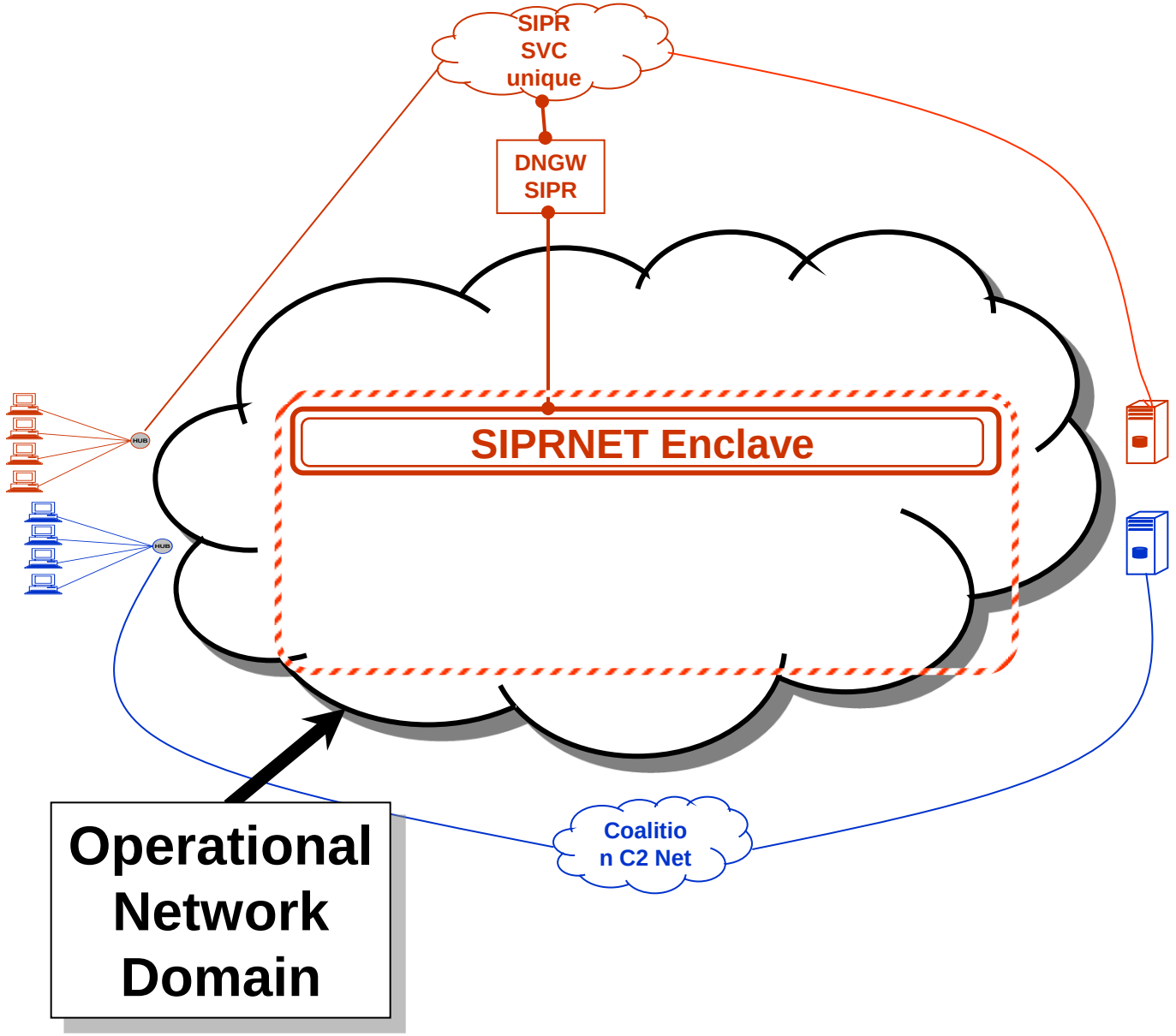
3. Establish an IPSec Tunnel for Enclave Client Services



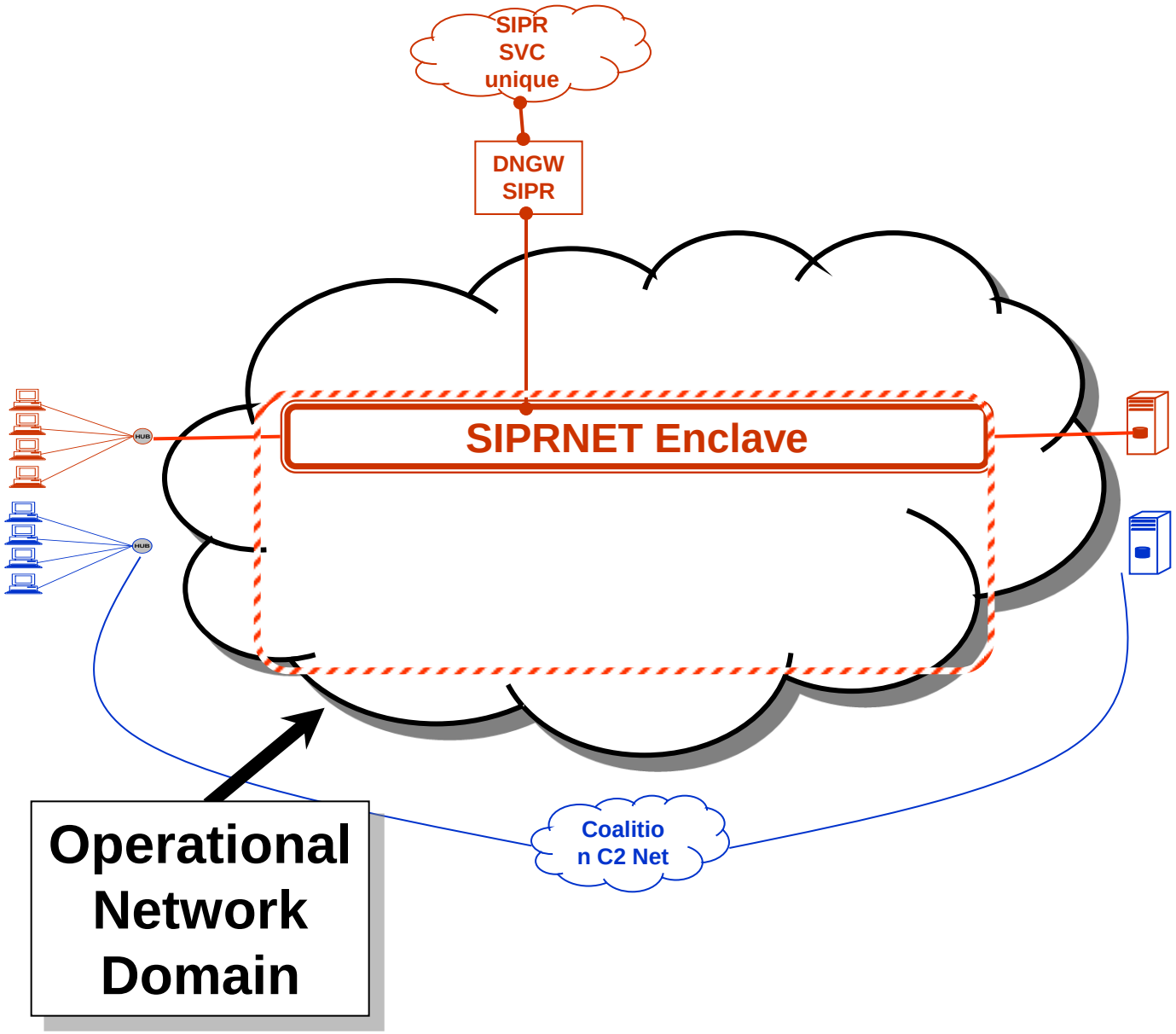
4. *Establish an outer IPSec Tunnel for Network Protection Called the Protected Inter-nodal Network (PIN)*



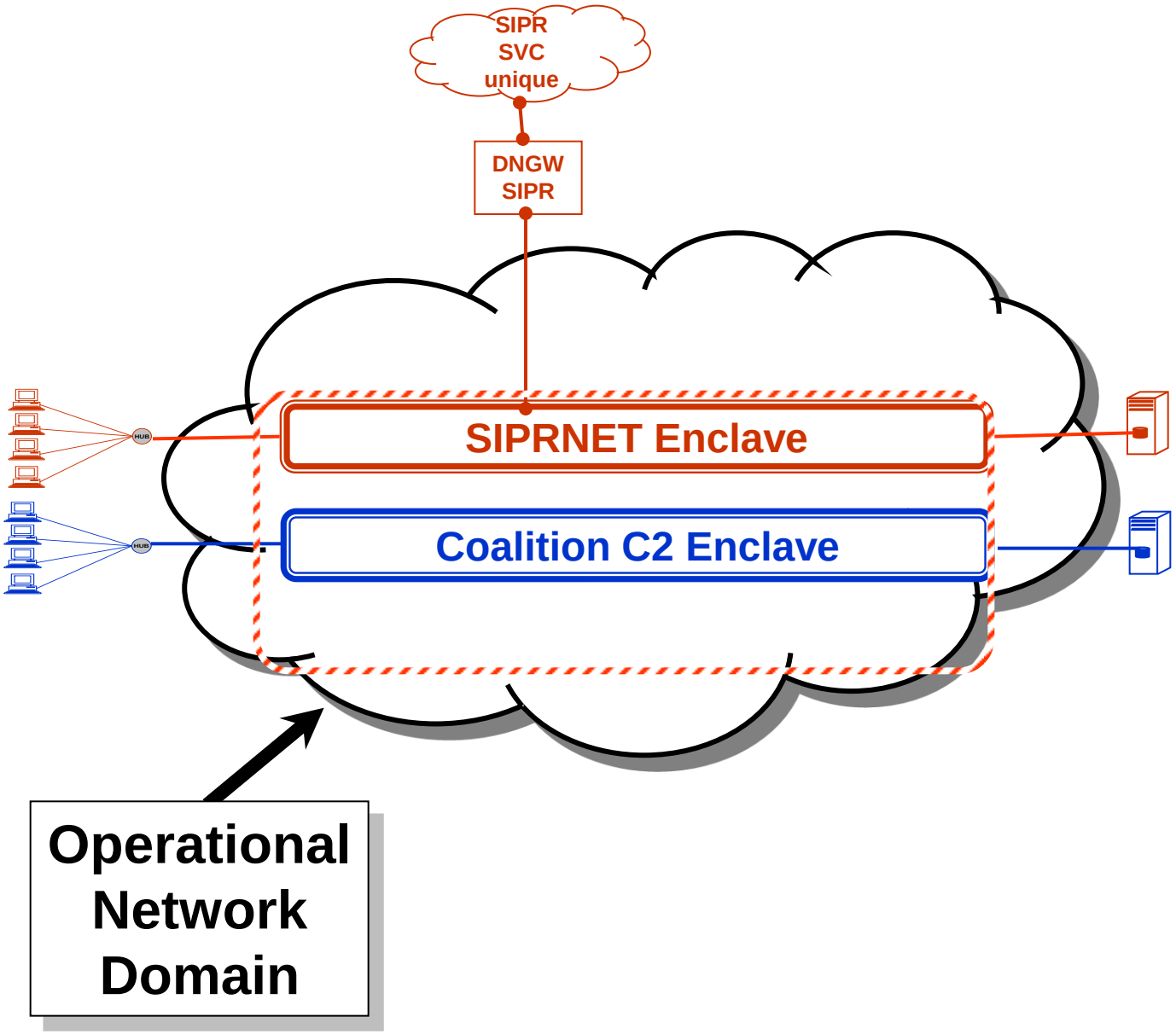
5. *Establish a controlled interface from the enterprise network to the OND Enclave*



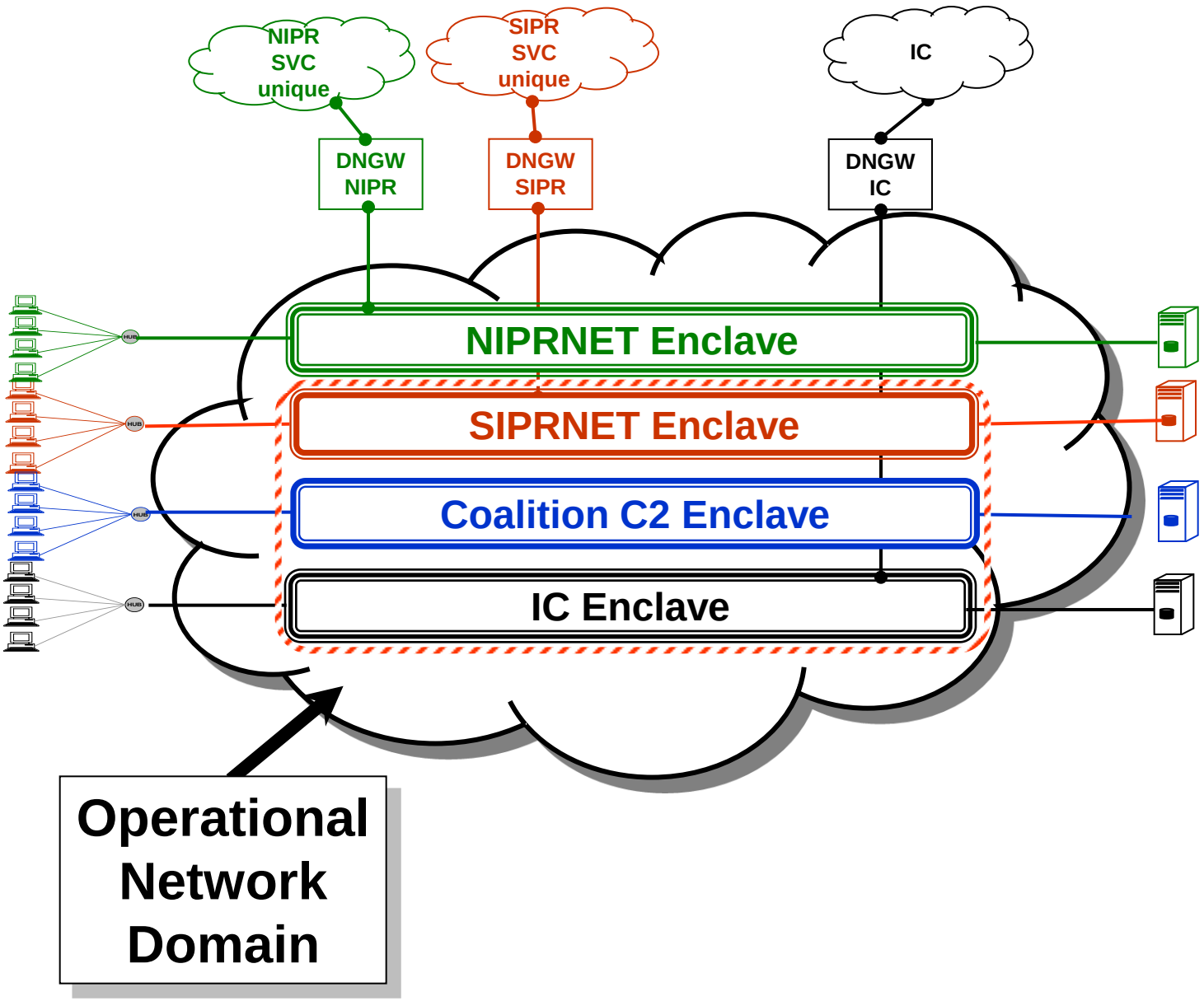
6. *Swing operational area services to the associated OND enclave*



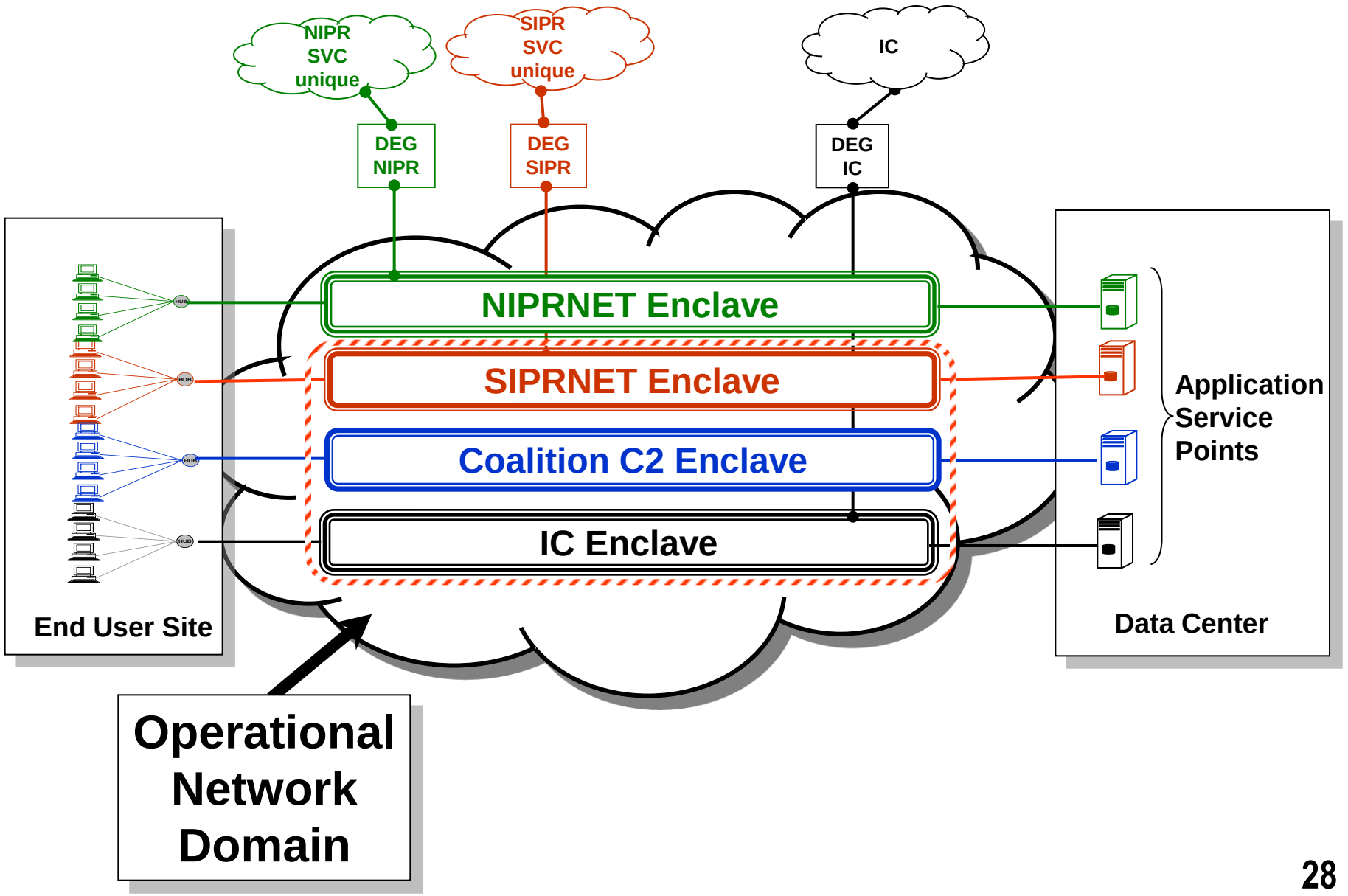
7. *Repeat this process for internal operational networks*



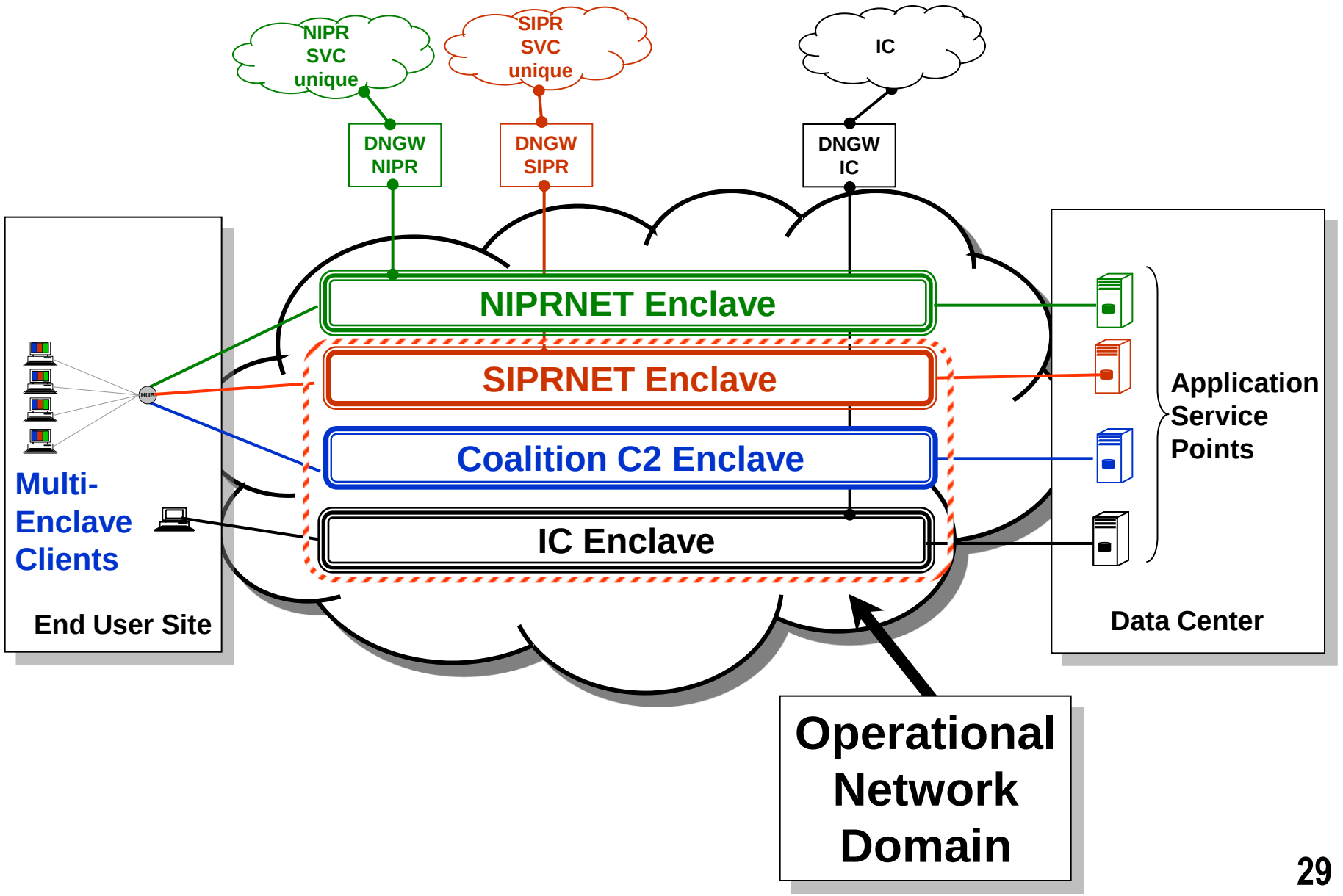
8. *Additional enclaves can be added as modules*



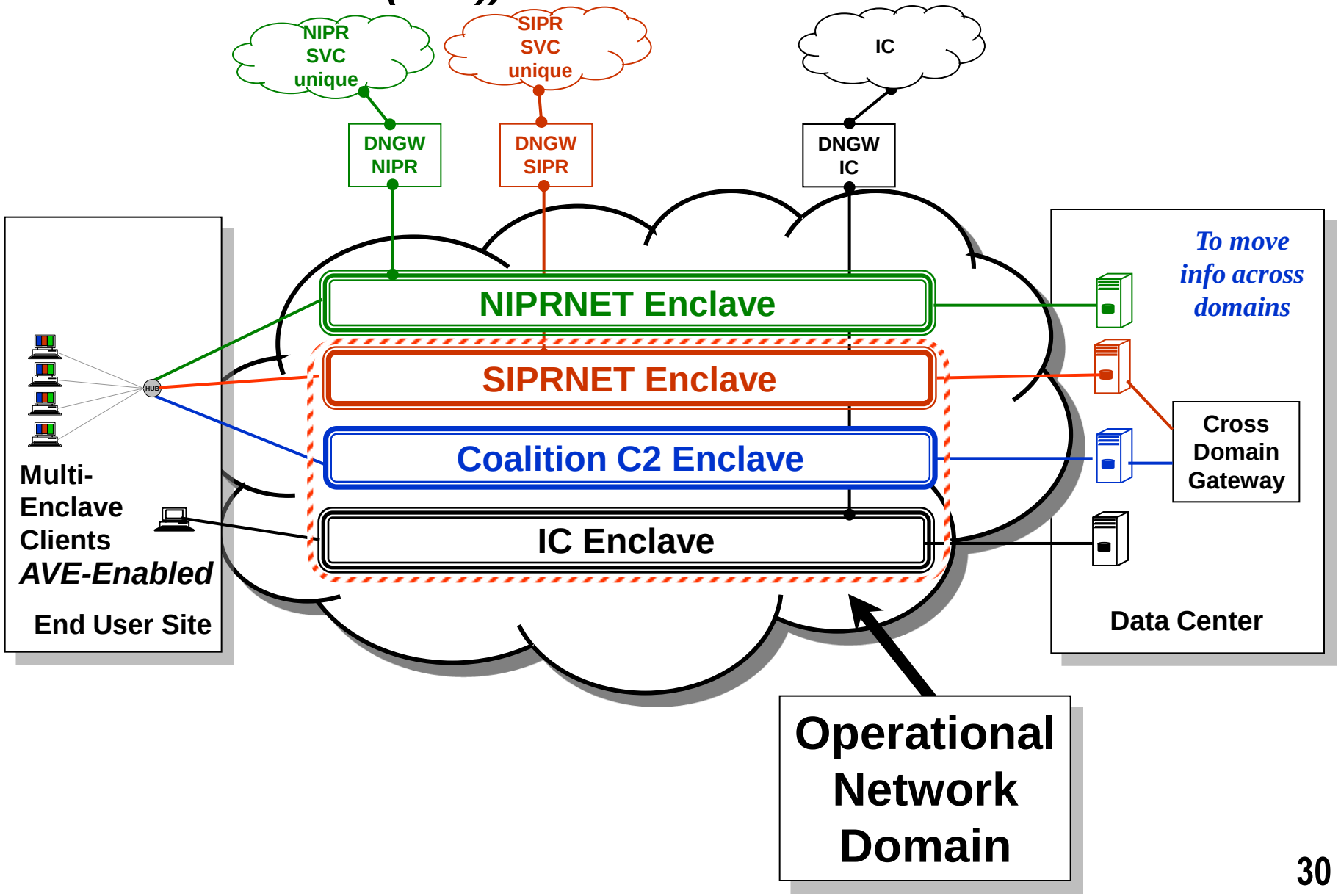
9. *Configure and provide training to end-user-sites and Data Centers accordingly*



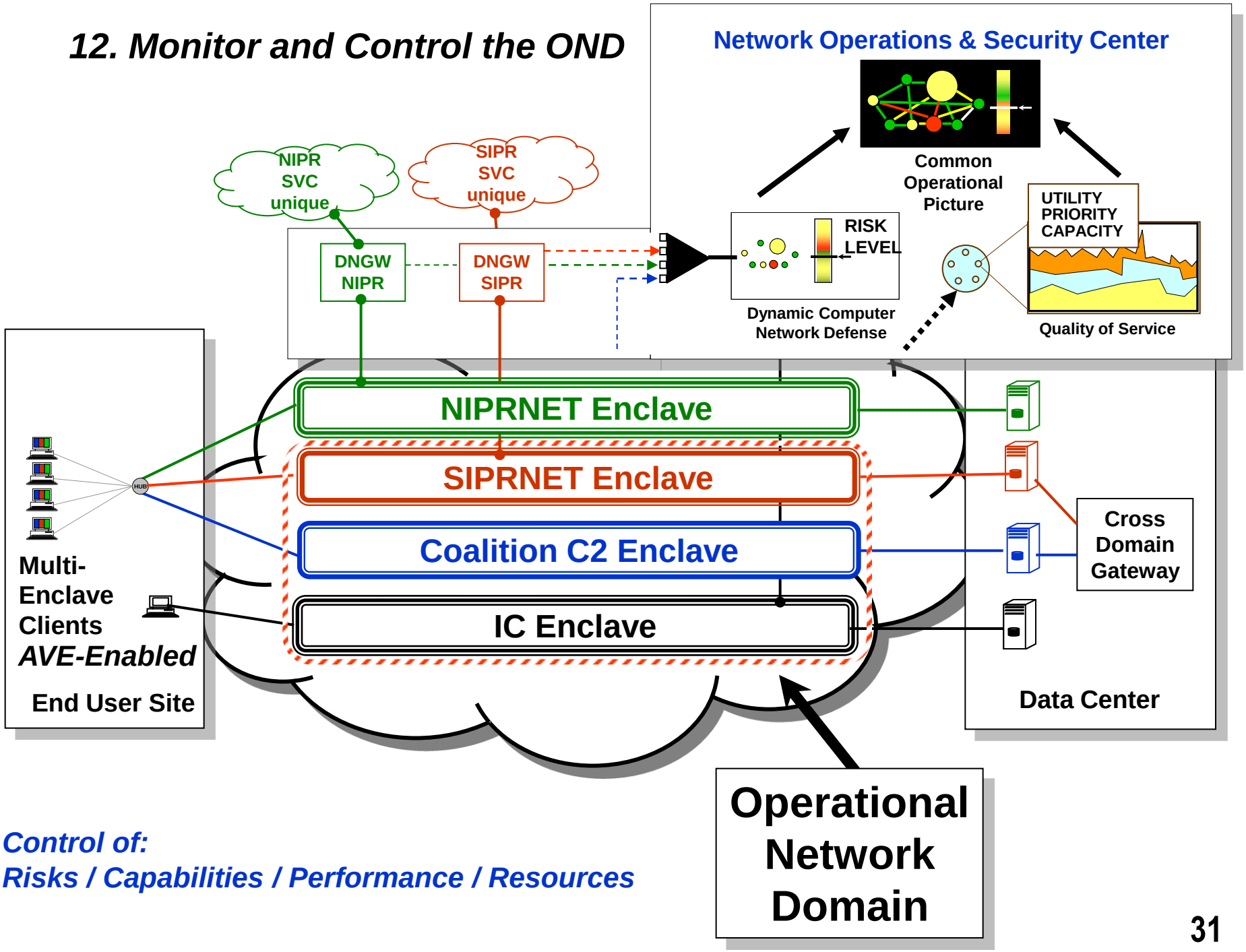
10. Take advantage of Multi-Enclave Clients from Agile Virtual Enclave (AVE) Project



11. Take advantage of cross-domain gateways and guards to move information between enclaves (e.g., Trusted Network Environment (TNE))

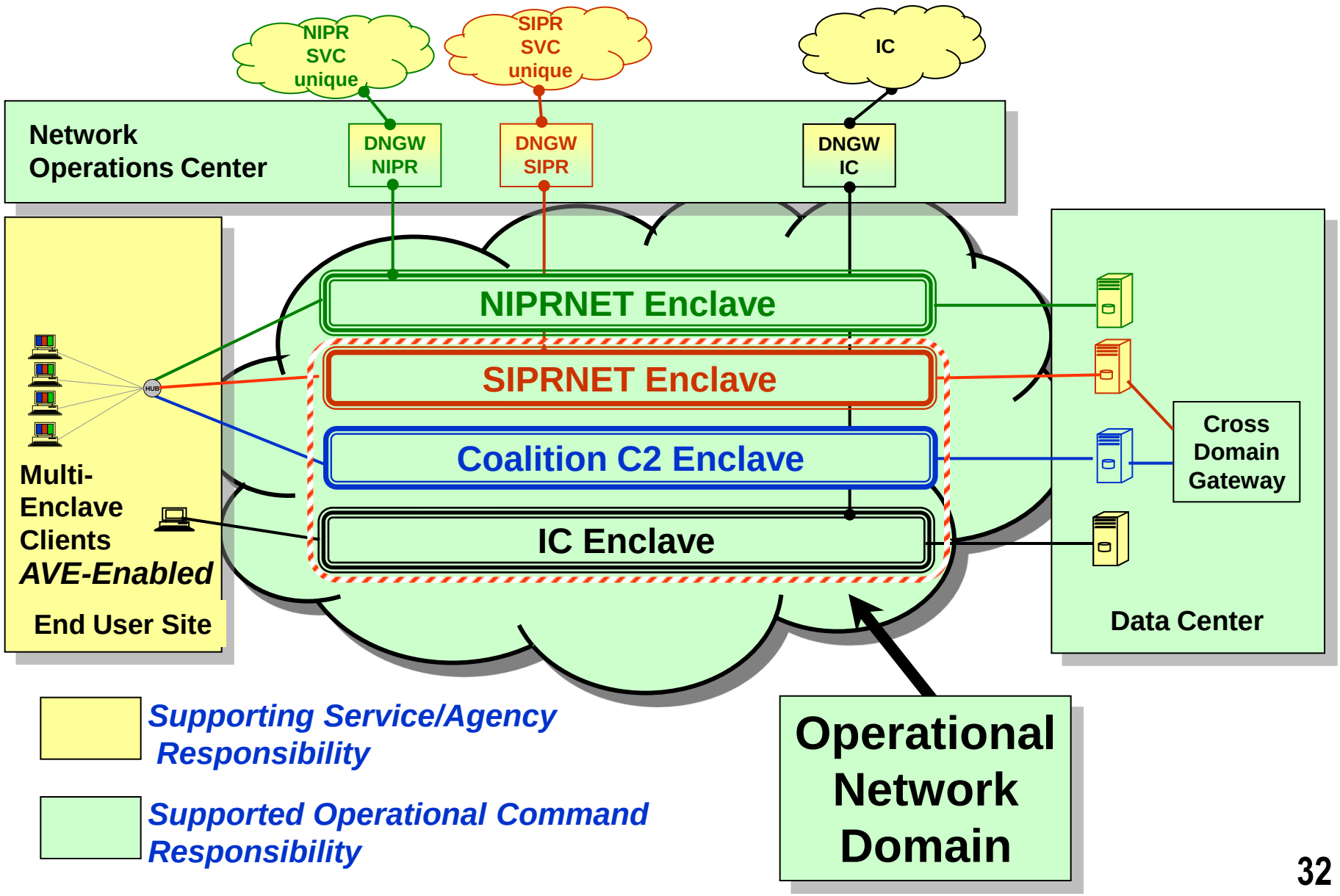


12. Monitor and Control the OND



Control of:
Risks / Capabilities / Performance / Resources

OND-related Areas of Responsibility



Operational Network Domains (OND) and Security Domain Enclaves through the Classified Military Network (CMILNet)

Mr. Randy Cieslak
CIO

U.S. Pacific Command
29 June 2010

This brief is classified:

UNCLASSIFIED

Technical Challenges

- **Challenge #1: Creation of Agile Virtual Enclaves (AVEs), which are networked security domains that allow reuse of the same network infrastructure from the client through the network cloud.**
- **Challenge #2: Creation of Operational Network Domains (ONDs) with sufficient strength of separation to support different risk jurisdictions within each AVE.**
  - **Virtual Secure Enclaves (VSEs) are the instantiation of AVEs within the OND.**
- **Challenge #3: Creation of a "black core capable" DISN designed to create Agile Virtual Enclaves (AVEs) to enable Virtual Secure Enclaves within Operational Network Domains (ONDs)**
  - **Must accommodate more than NIPRNET, SIPRNET, and JWICS**

Solution Toolkit – Network Virtualization

- **Performance-based Virtualization**
  - **Multi-Protocol Layered Switching (MPLS)**
  - **Generic Routing Encapsulation (GRE)**
  - **Virtual Local Area Networks (VLAN)**
- **Security-based Virtualization a.k.a. Virtual Private Networks (VPNs)**
  - **High Assurance Internet Protocol Encryption (HAIPE)**
  - **Internet Protocol Security (IPSec)**
  - **Transport Layer Security (TLS)**

Use these for ONDs

Use this for AVEs and VSEs

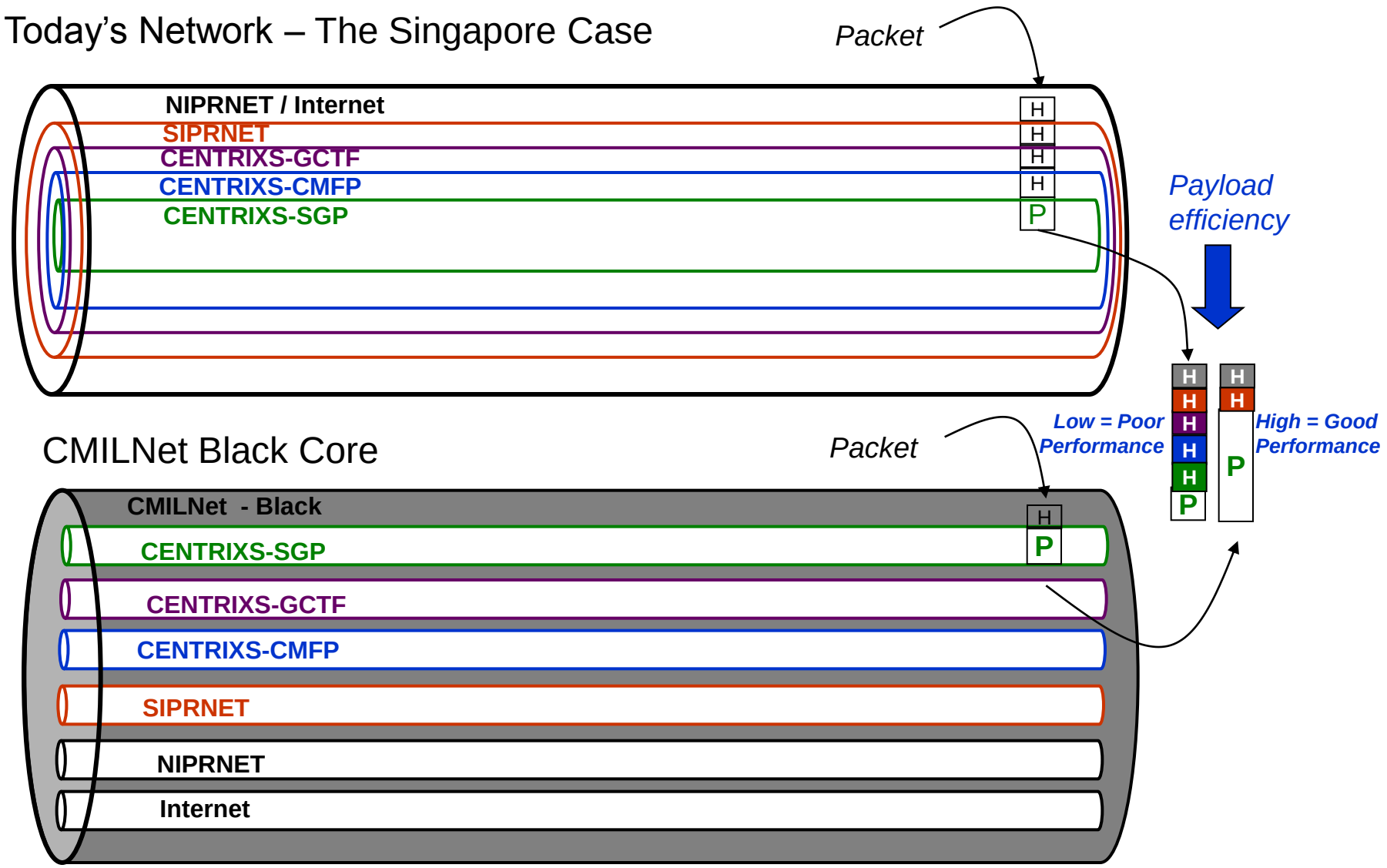
Solution must employ both types of virtualization, <u>together</u>, to optimize capability, security and performance.

Technical Solutions

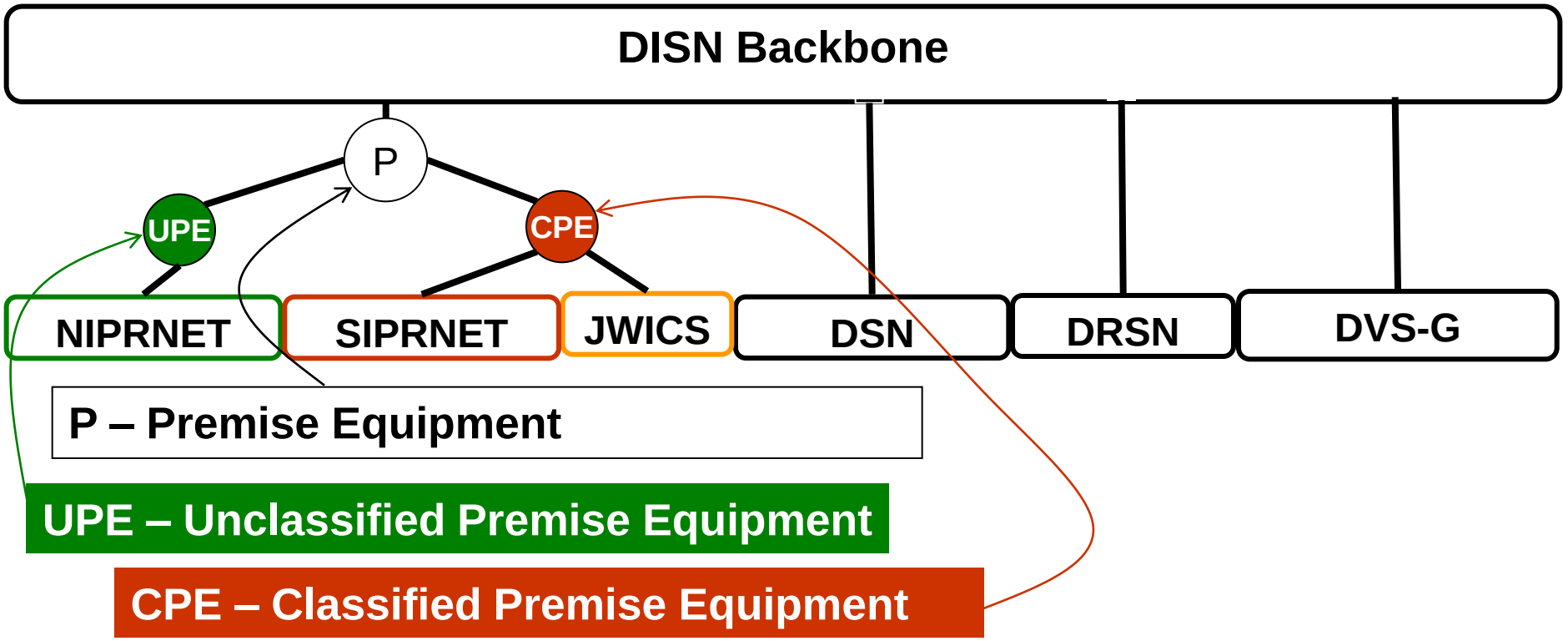
- **Challenge #1: Creation of Agile Virtual Enclaves (AVEs), which are networked security domains that allow reuse of the same network infrastructure from the client through the network cloud**
- **Solution #1: Employ rigorously tested IPSec implemented in accordance with NSA standards**
- **Challenge #2: Creation of Operational Network Domains (ONDs) with sufficient strength of separation to support different risk jurisdictions within each AVE.**
- **Solution #2: Employ Intrusion Protection System (IPS) – based firewalls with access controls and service filters**
- **Challenge #3: Creation of a "black core capable" DISN designed to create Agile Virtual Enclaves (AVEs) to enable Virtual Secure Enclaves within Operational Network Domains (ONDs).**
- **Solution #3: Employ a next-generation network strategy that accommodates solutions 1 and 2 as a fourth enterprise network domain using MPLS-based domain techniques and IPv6 improving upon how SIPRNET and NIPRNET is done on the DISN**

GIG 3.0

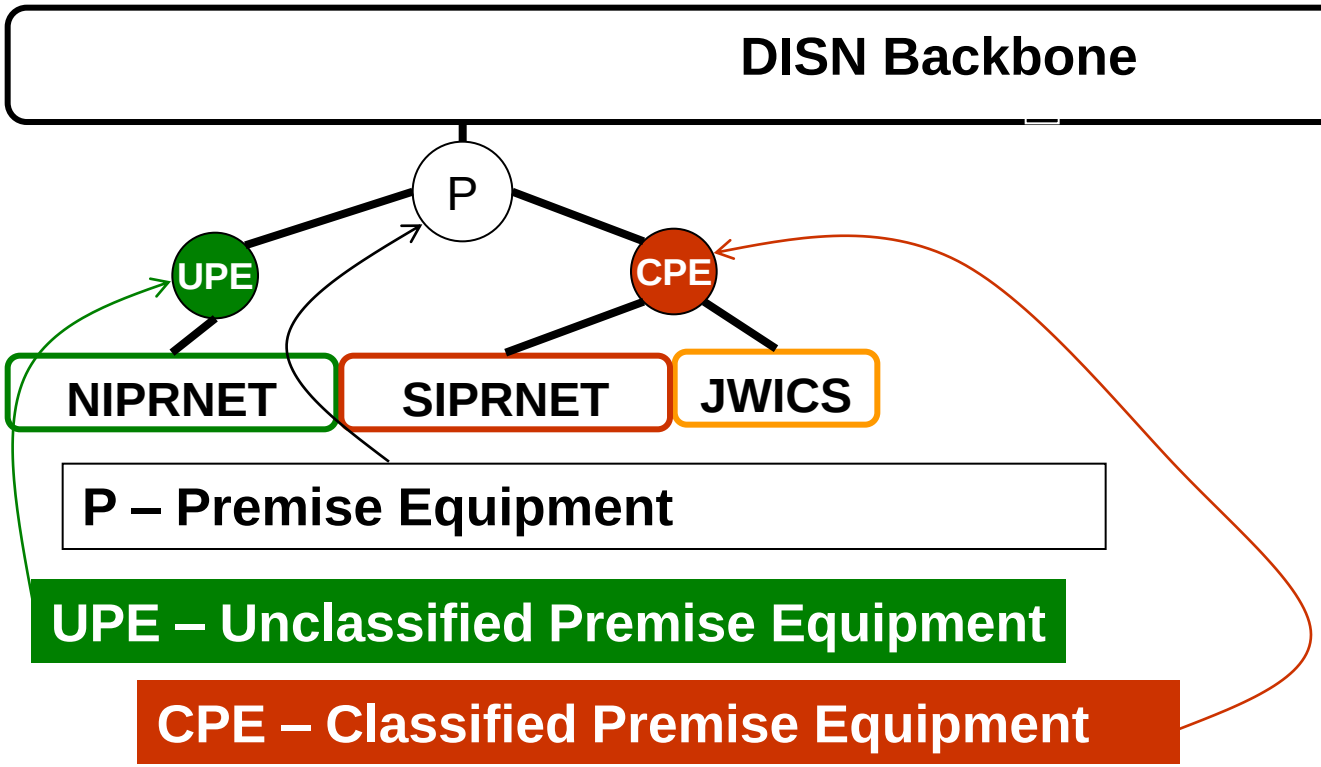
Why We Need a Black Core CMILNet



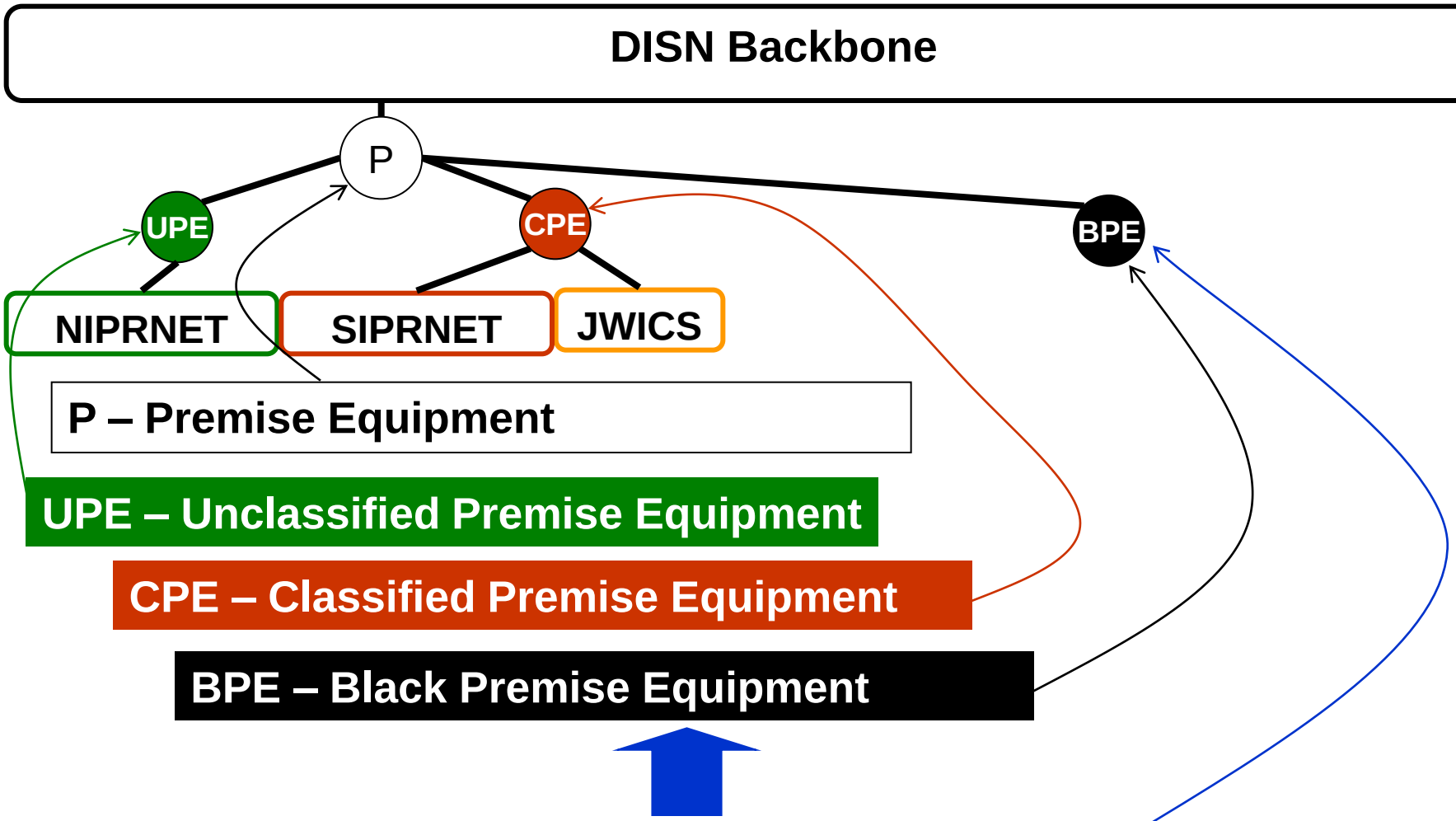
Global Enterprise OND Concept – Today's State



Global Enterprise OND Concept – Today's State



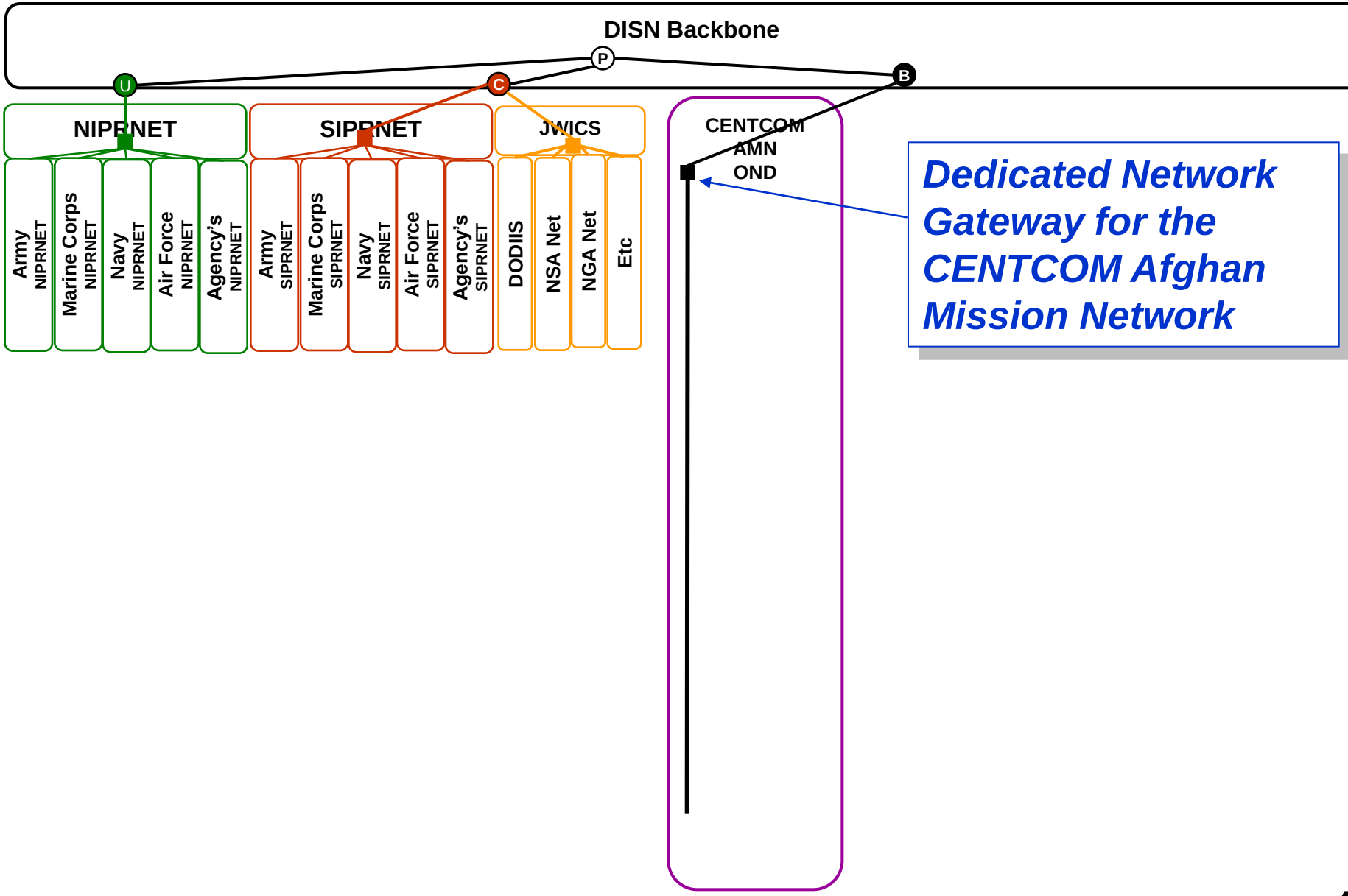
Global Enterprise OND Concept – Near Term?



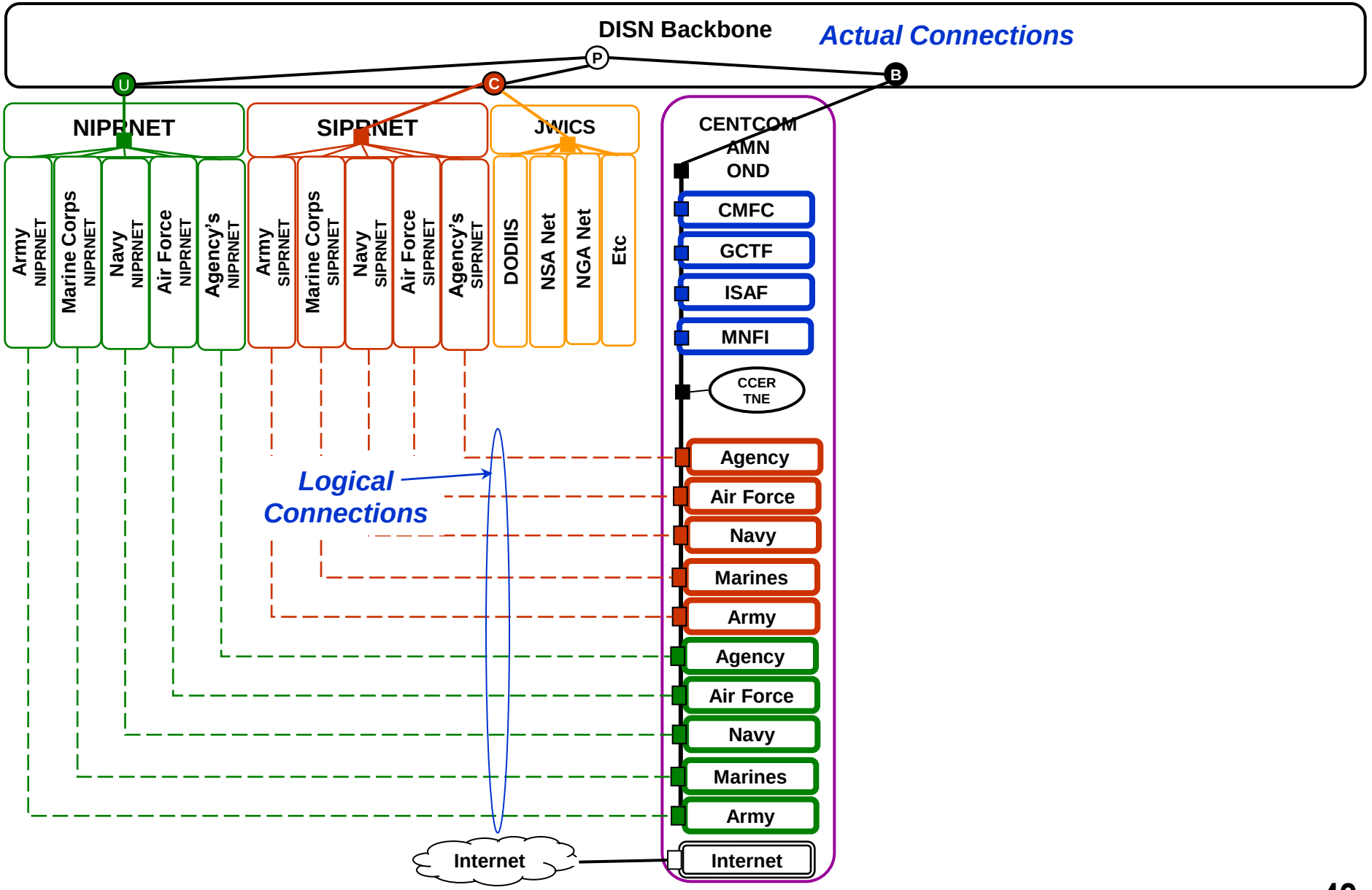
Extremely useful in the creation of CMILNet

Common Mission Network Transport (CMNT)

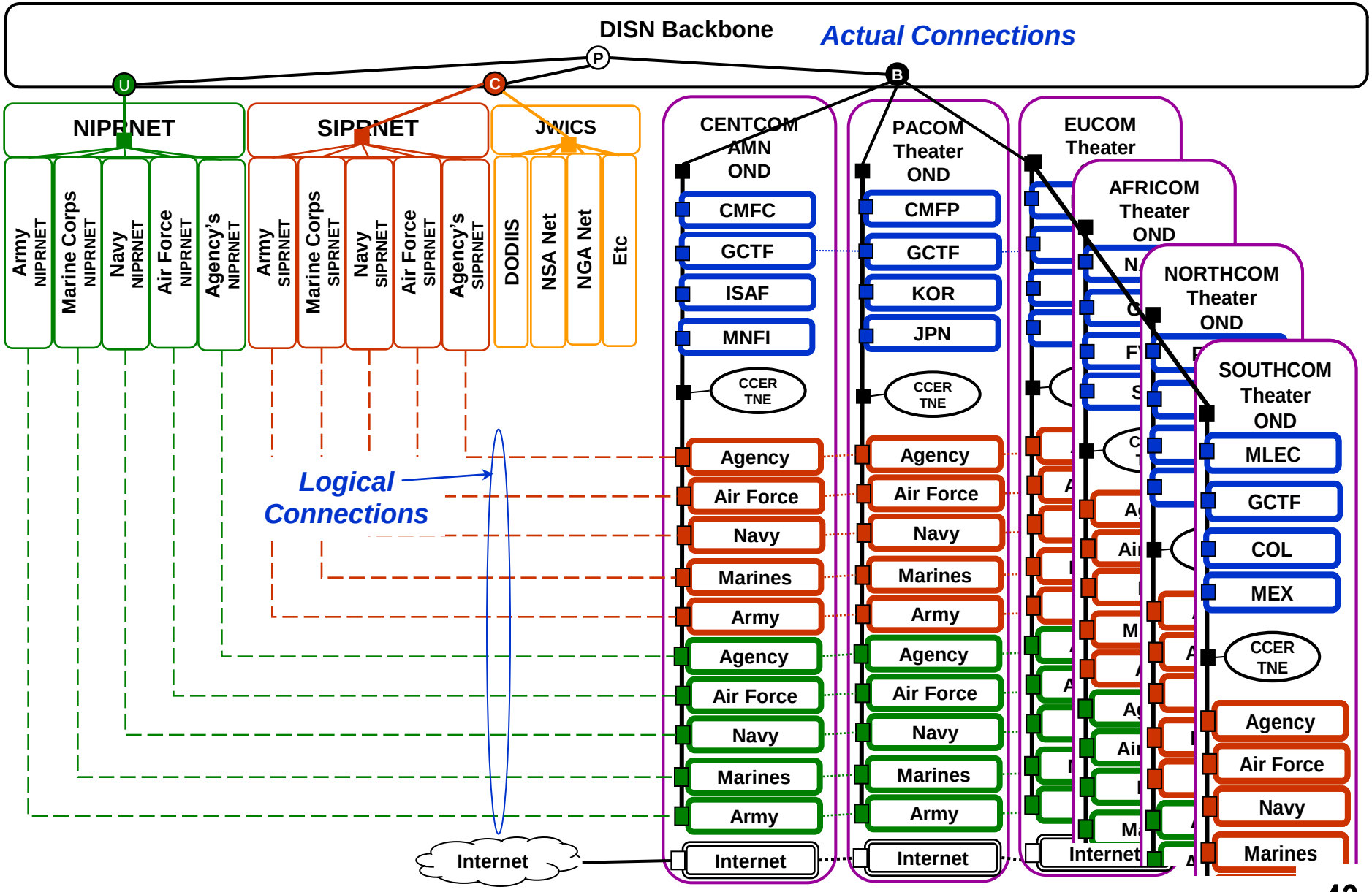
Global Enterprise OND Concept



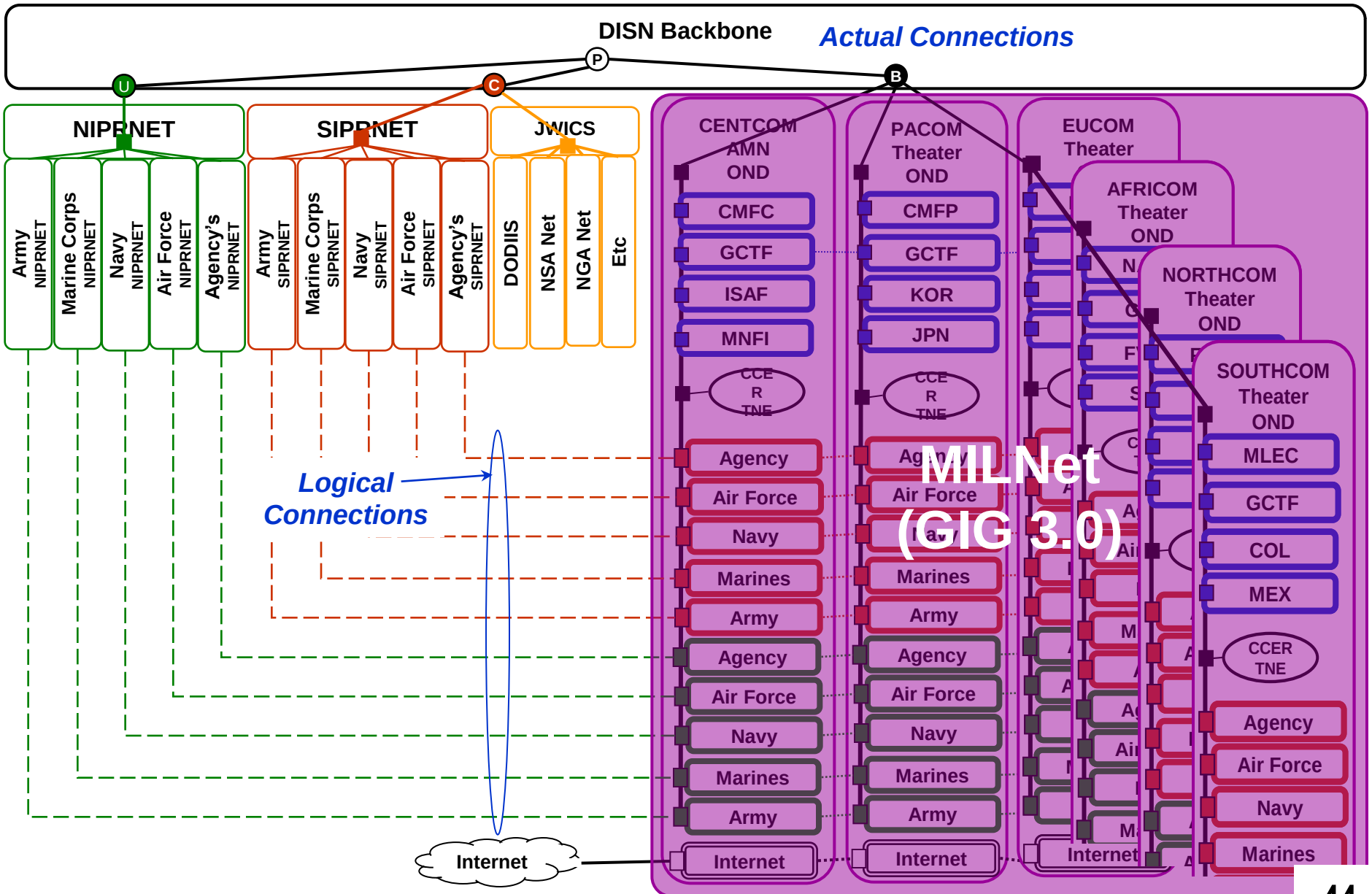
Global Enterprise OND Concept



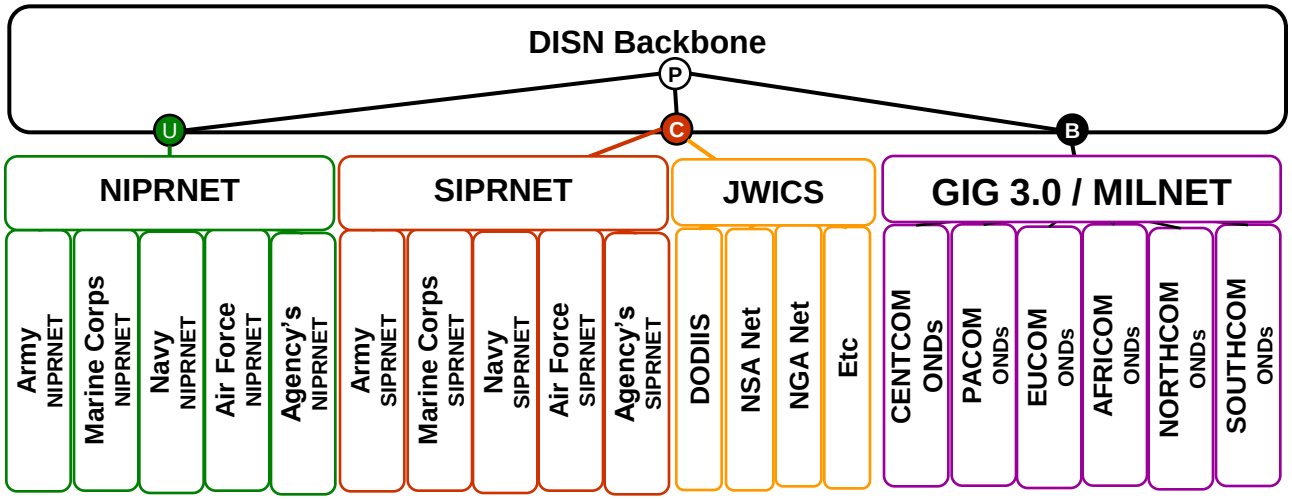
Global Enterprise OND Concept

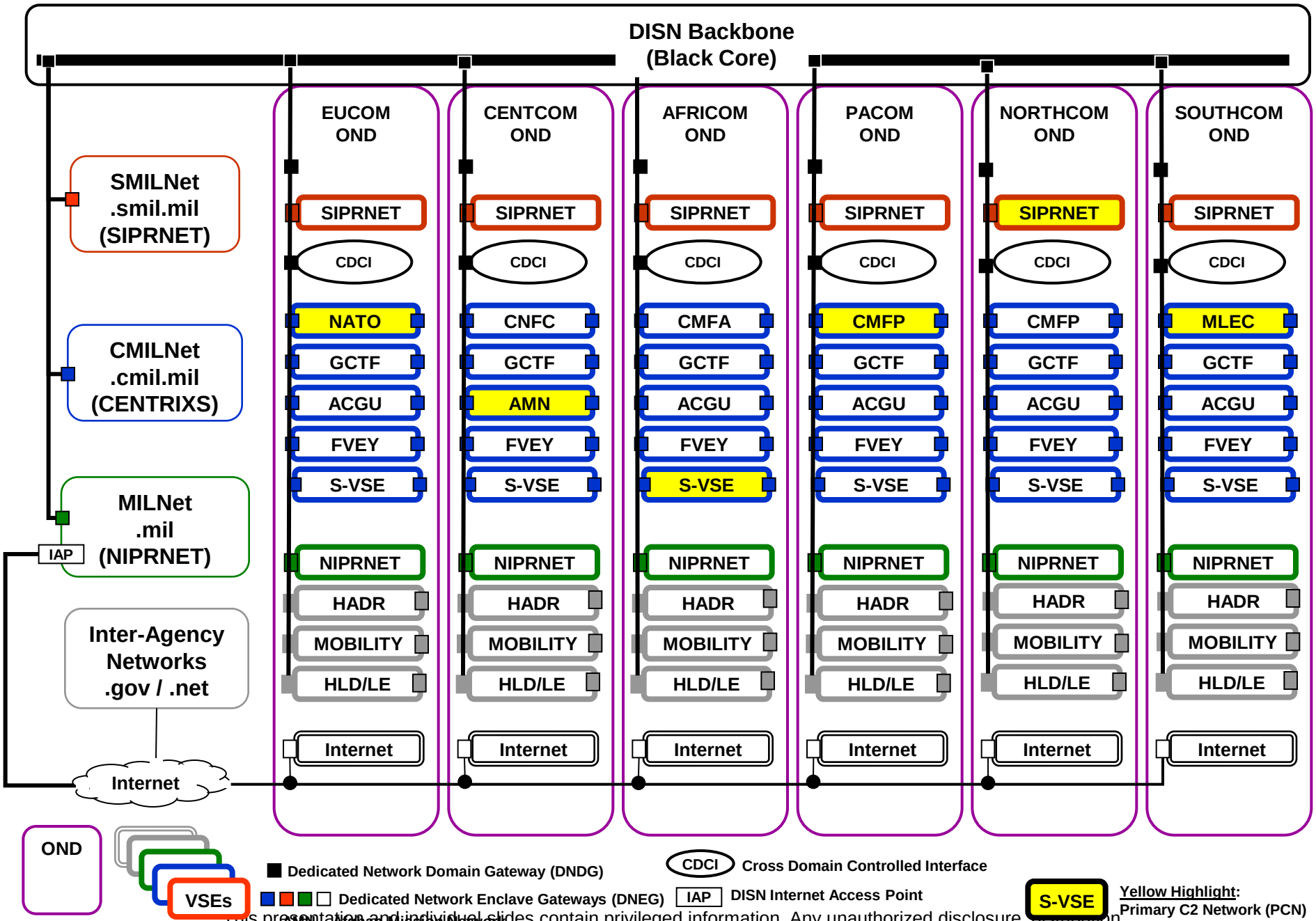


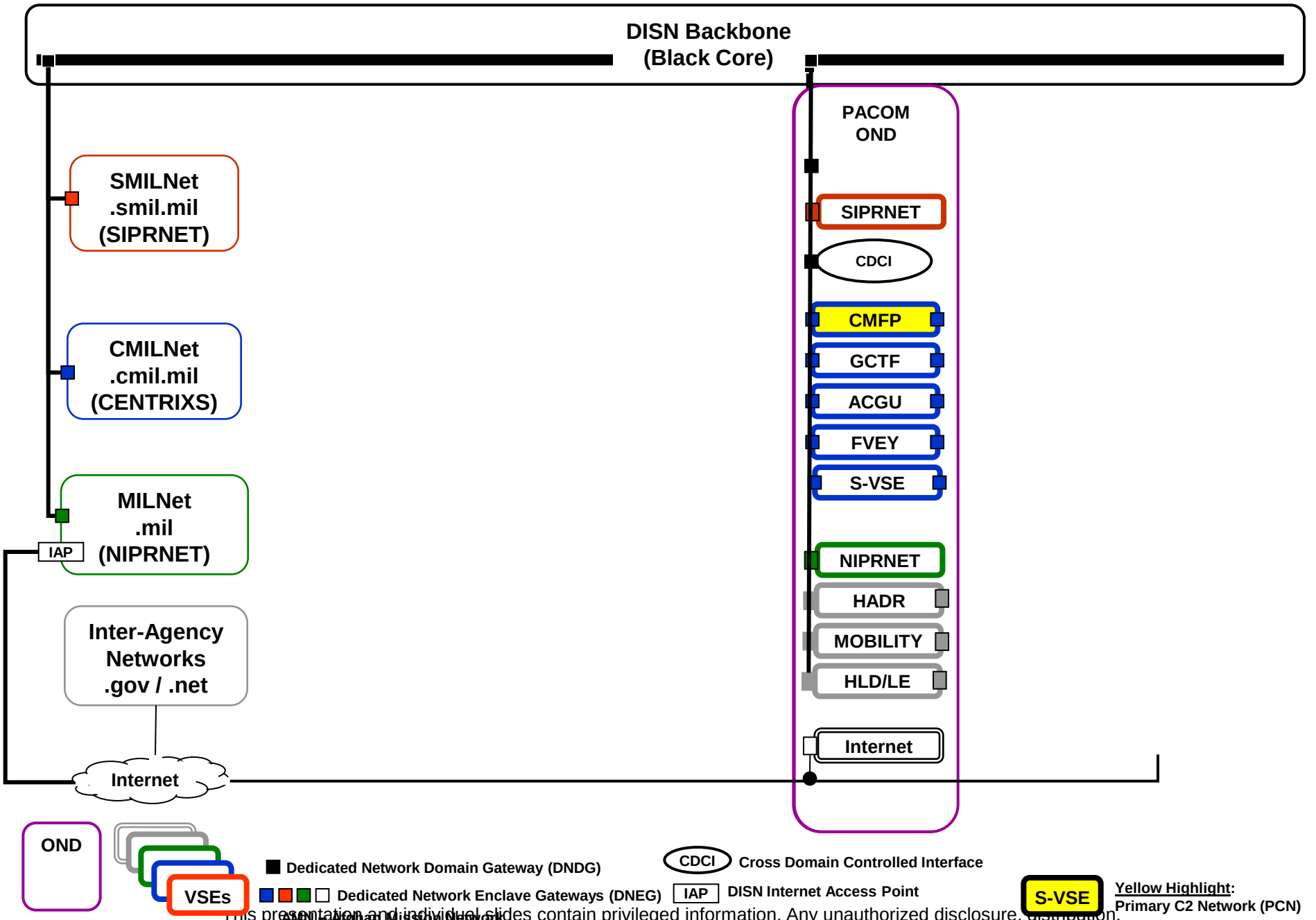
Global Enterprise OND Concept

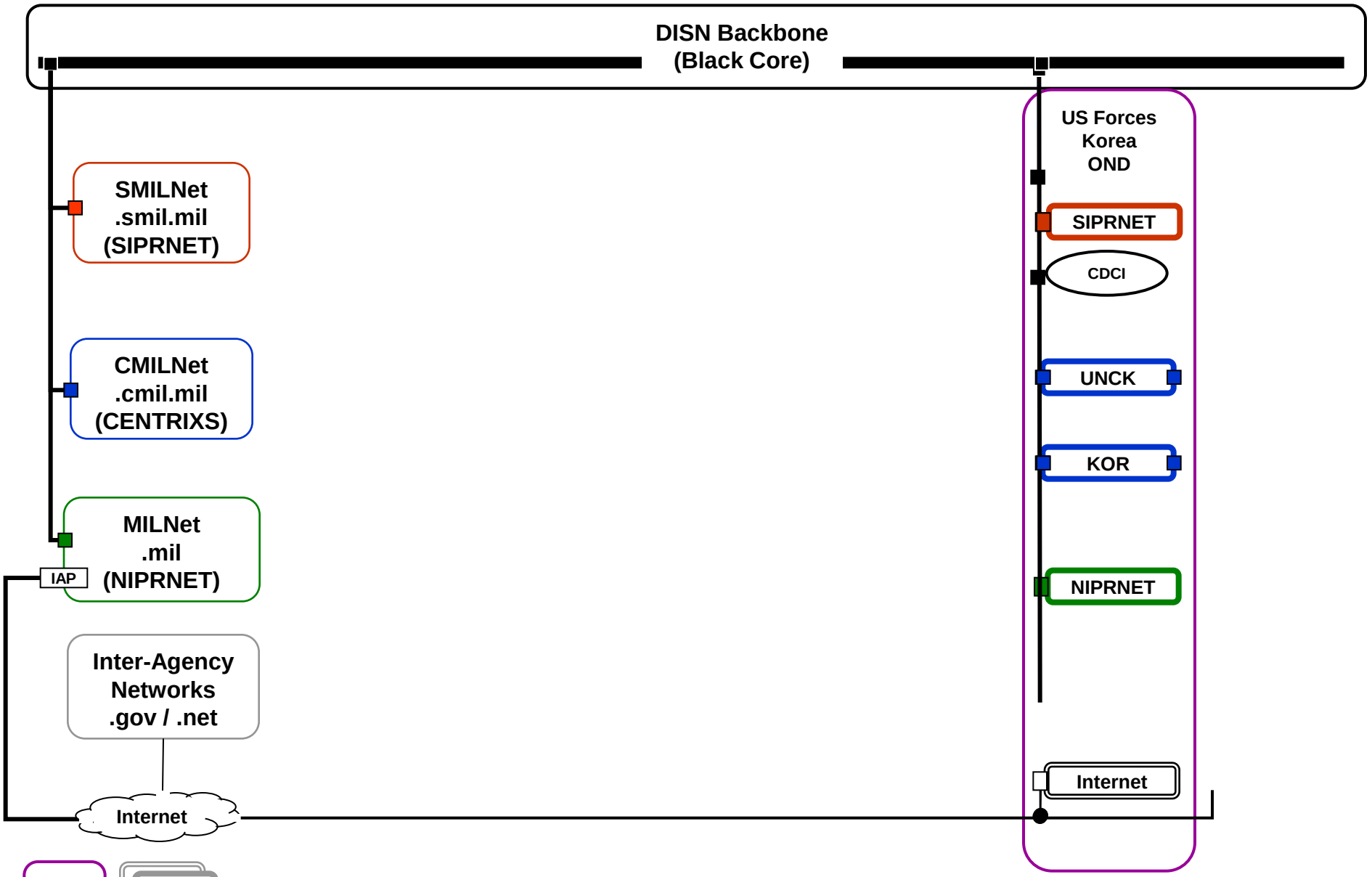


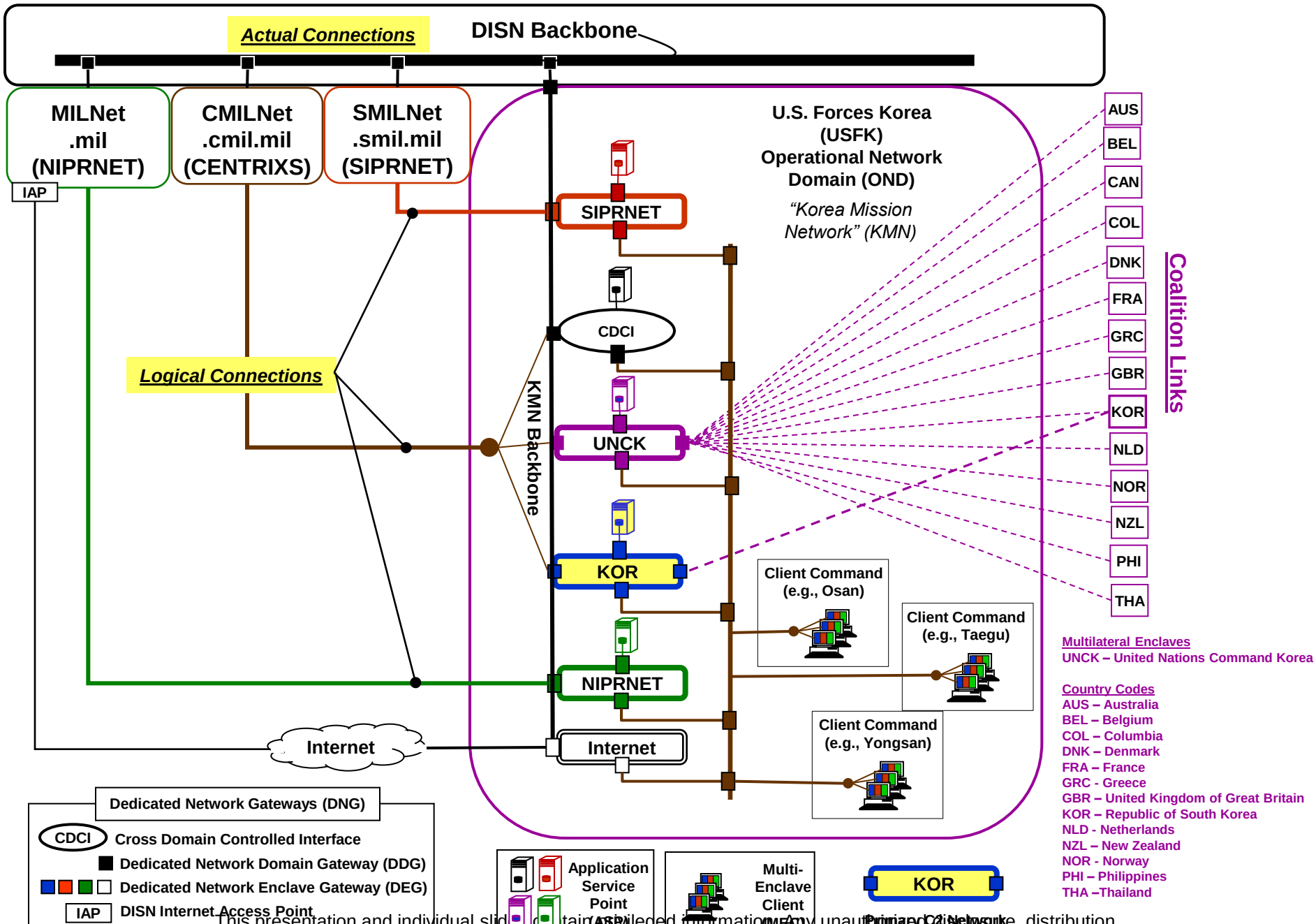
Global Enterprise OND Concept

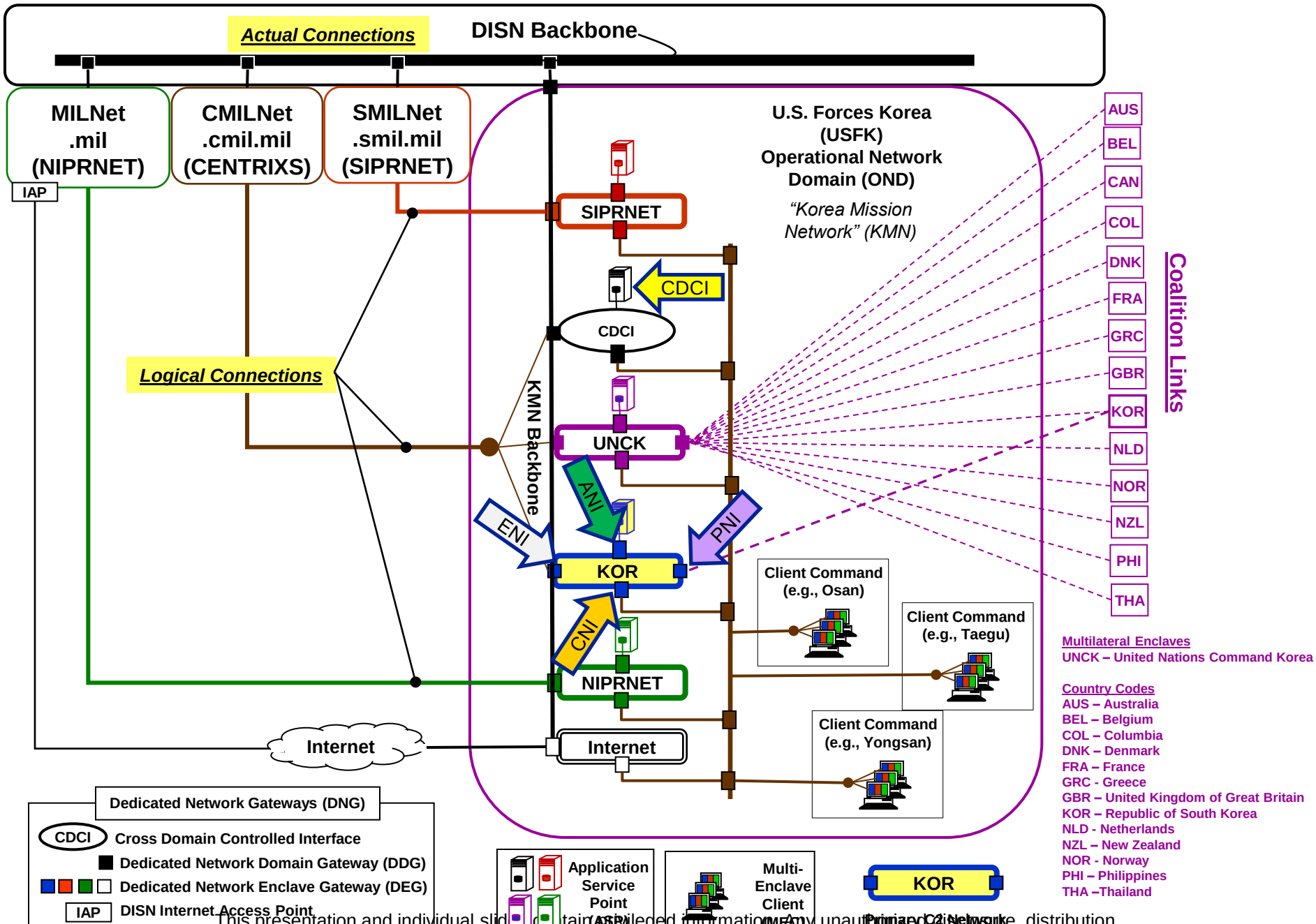




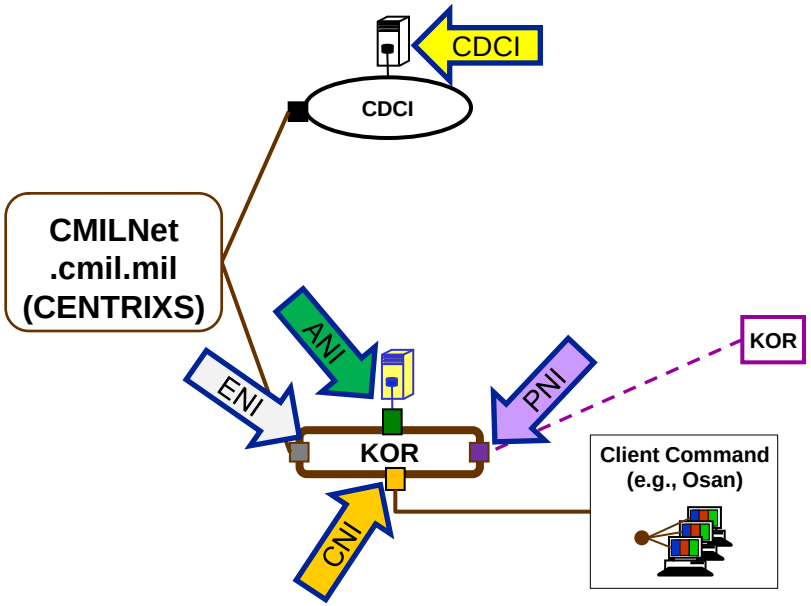






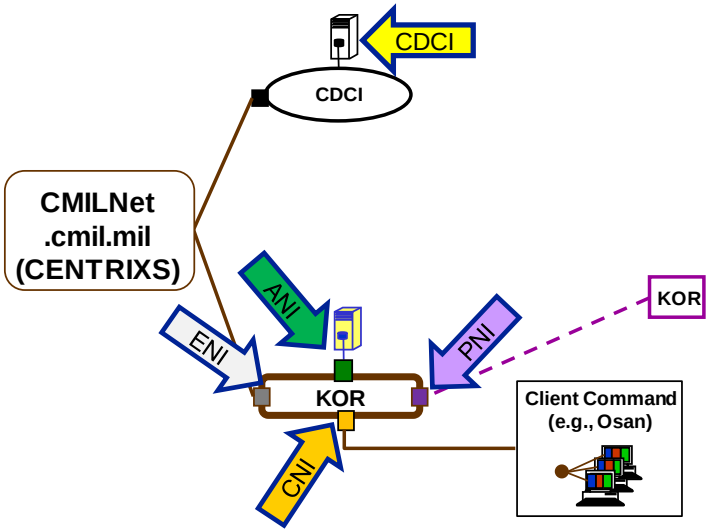


Selected GIG 3.0 Components to Show On the Next Slide – Geographic Topology for CENTRIXS-KOR

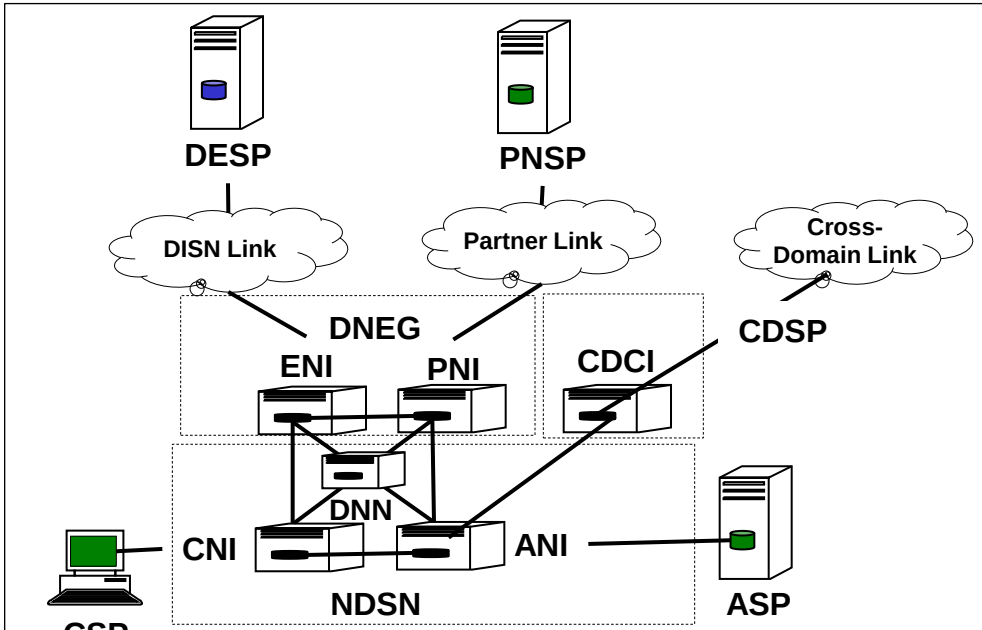


GIG 3.0 Interface Components

Internal to a single security enclave



System Design View



System Component View

Acronyms

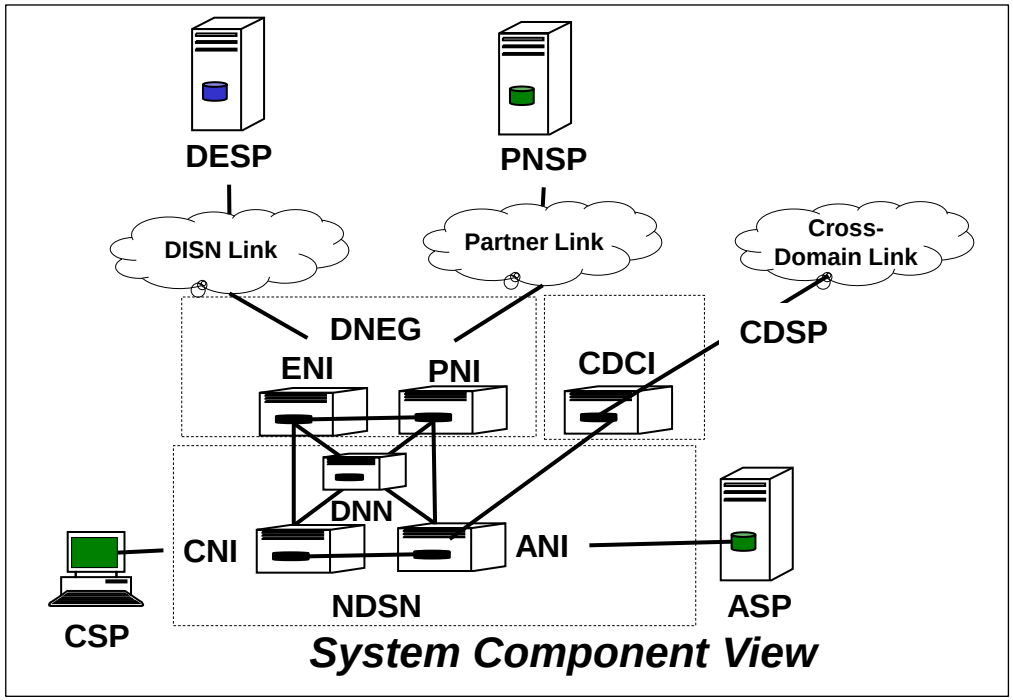
ASP – Application Service Point
ANI – Application Network Interface
CNI – Client Network Interface
CDCI – Cross-Domain Controlled Interface
CDSP – Cross-Domain Service Point
CSP – Customer Service Point
DESP – Defense Enterprise Service Point
DNEG – Dedicated Network Enclave Gateway
DNN – Domain Network Node
ENI – Enterprise Network Interface
NDSN – Network Domain Service Node
NSP – Network Service Point
PNI – Partner Network Interface
PNSP – Partner Network Service Point

GIG 3.0 Interface, Enclave and Service Point Definitions

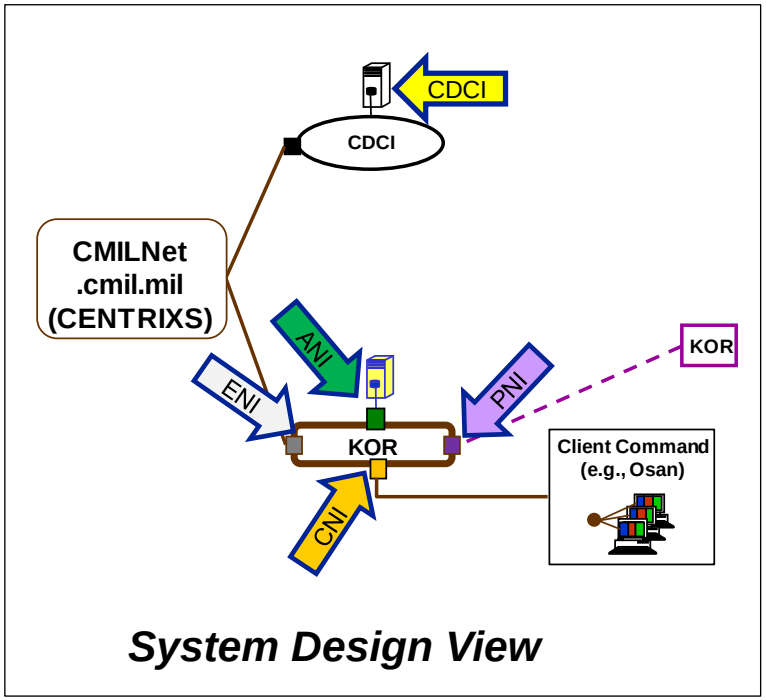
- **ASP – Application Service Point**
  - Server suite and software that provides application programs to the user.
  - Examples: Microsoft Exchange Server, Apache Web Server
- **ANI – Application Network Interface**
  - Network router or switch that connects the ASP to the network
- **AVE – Agile Virtual Enclave**
  - IPSec-based Virtual Private Network (VPN) that provides robust protection of an information sharing enclave across the enterprise. Each CENTRIXS network can be implemented on the same network infrastructure using AVEs.
- **CNI – Client Network Interface**
  - VSE IPSec crypto and network router or switch that connects the ASP to the Client VPN. Is the ASP interface for the MECs.
- **CDCI – Cross-Domain Controlled Interface**
  - High assurance filter and guard that provides for a controlled transfer of information between enclaves. (e.g., between CENTRIXS-KOR and CENTRIXS-UNCK)
- **CDSP – Cross-Domain Service Point**
  - Relative to one enclave (e.g., CENTRIXS-KOR), the service point providing information from another domain (e.g., CENTRIXS-UNCK)
  - Examples: Trusted Network Environment (TNE), Joint Cross Domain Exchange System (JCDX).
- **CSP – Customer Service Point**
  - Client point of presence to the network. Best serviced by a single MEC. Today CSPs consist of multiple client computer, each dedicated to a single networked enclave.
  - In this context CSPs are serviced by MECs.
- **DNDG – Dedicated Network Domain Gateway**
  - Generic reference to the set of DNEGs that form the perimeter of an OND.
- **DESP – Defense Enterprise Service Point**
  - ASP(s) that are in the DISN external to the OND.
  - Examples: DISA DECC, Air Force NOSC.
- **DNEG – Dedicated Network Enclave Gateway**
  - Controlled interfaces with firewalls (access control system, information protection system) that separates selected network services and activities between the external networks (e.g., DISN or coalition partner) and the OND.
  - Contains ENIs and PNIs.
- **DNN – Domain Network Node**
  - Router / switch with control and monitoring that interconnects sites, interfaces, network assets, clients, servers and network checkpoints across the GIG 3.0 infrastructure..
- **ENI – Enterprise Network Interface**
  - VSE IPSec crypto, firewall (access control system, information protection system) and network router or switch that connects the DESP to the OND VSE.
- **NDSN – Network Domain Service Node**
  - Major node on the OND that includes the ANI, DN and/or CNI providing information capability to the OND.
- **NSP – Network Service Point**
  - Point of presence for monitoring, control, configuration and maintenance of network devices.
- **OND – Operational Network Domain**
  - Network infrastructure bounded by a parameter of DNDGs that contain VSEs
- **PNI – Partner Network Interface**
  - High assurance filter and guard that provides for a controlled transfer of information between the USA's partner network (e.g., CENTRIXS) and the coalition partner's ASP – called a PNSP.
- **PNSP – Partner Network Service Point**
  - Server suite and/or network interface owned and operated by a coalition partner designated to provide information services to the USA enclave (e.g., CENTRIXS.)
- **VSE – Virtual Secure Enclave**
  - Specific instantiation of an AVE within an OND or for situations when a higher assurance protected network domain is needed within a less trusted network.
  - A VSE is a AVE aligned within an OND guarded by a controlled interface (DNEG).

GIG 3.0 Interface Components

Internal to a single security enclave



System Component View

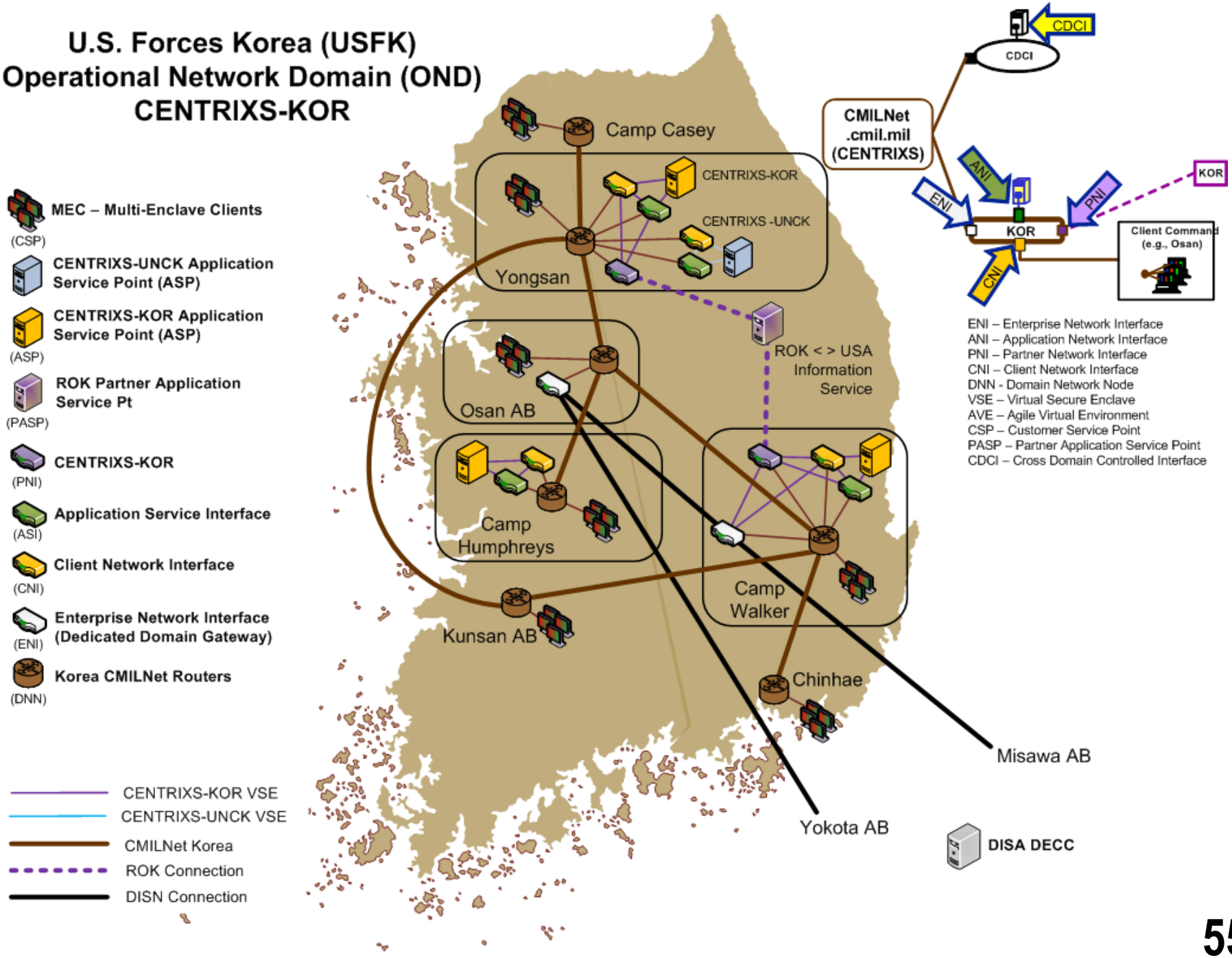


System Design View

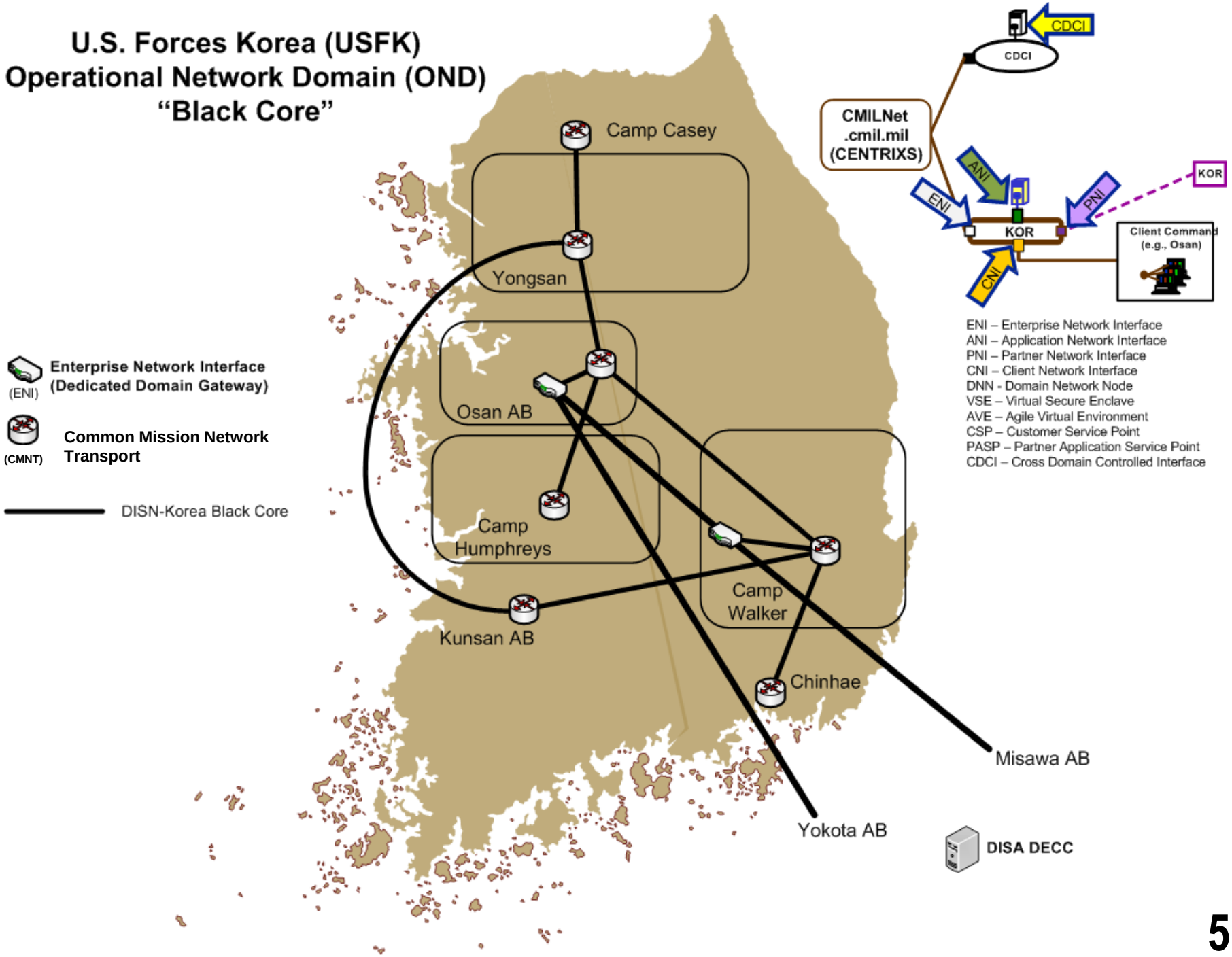
Acronyms

ASP – Application Service Point
ANI – Application Network Interface
CNI – Client Network Interface
CDCI – Cross-Domain Controlled Interface
CDSP – Cross-Domain Service Point
CSP – Customer Service Point
DESP – Defense Enterprise Service Point
DNEG – Dedicated Network Enclave Gateway
DNN – Domain Network Node
ENI – Enterprise Network Interface
NDSN – Network Domain Service Node
NSP – Network Service Point
PNI – Partner Network Interface
PNSP – Partner Network Service Point

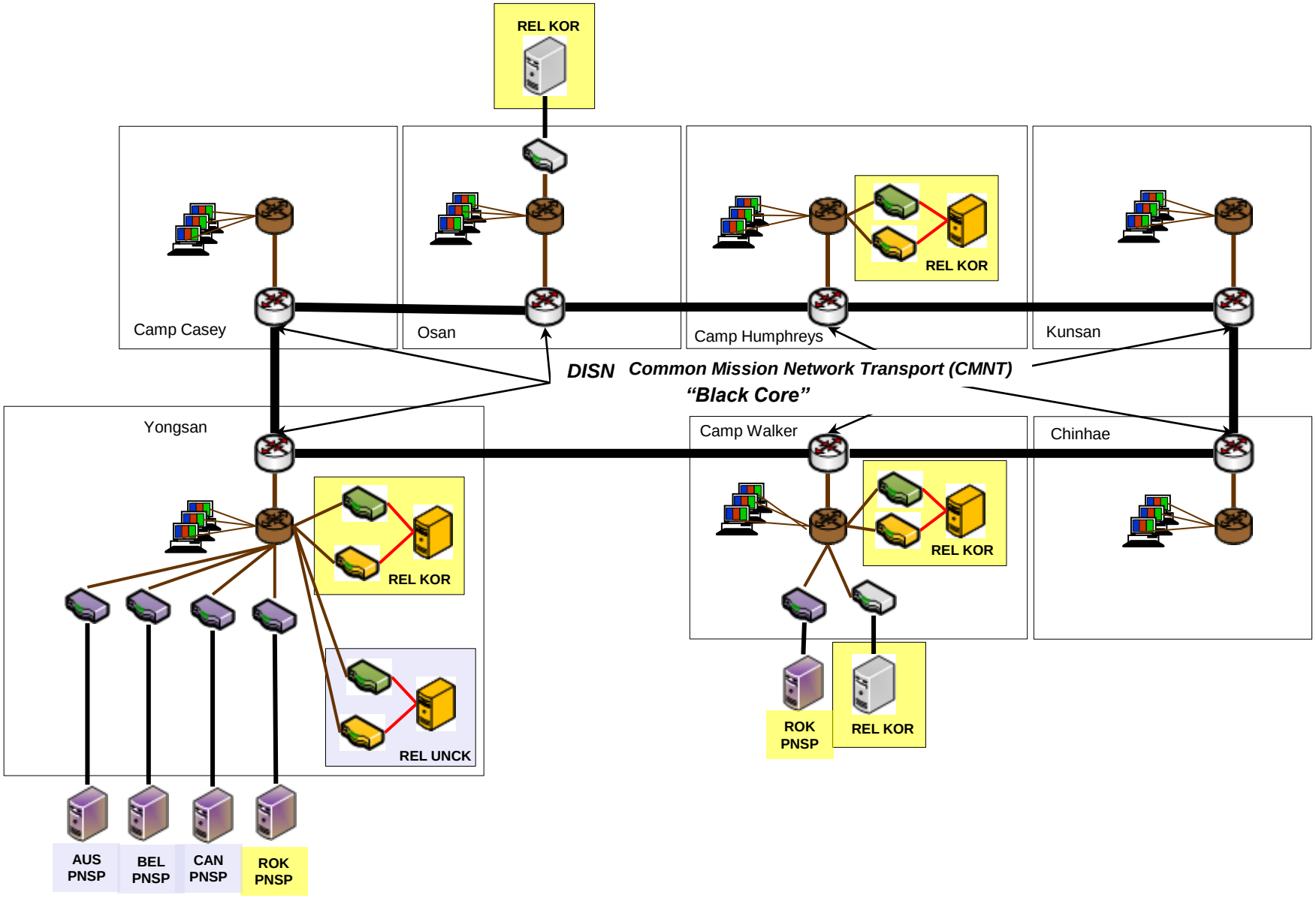
U.S. Forces Korea (USFK)
Operational Network Domain (OND)
CENTRIXS-KOR



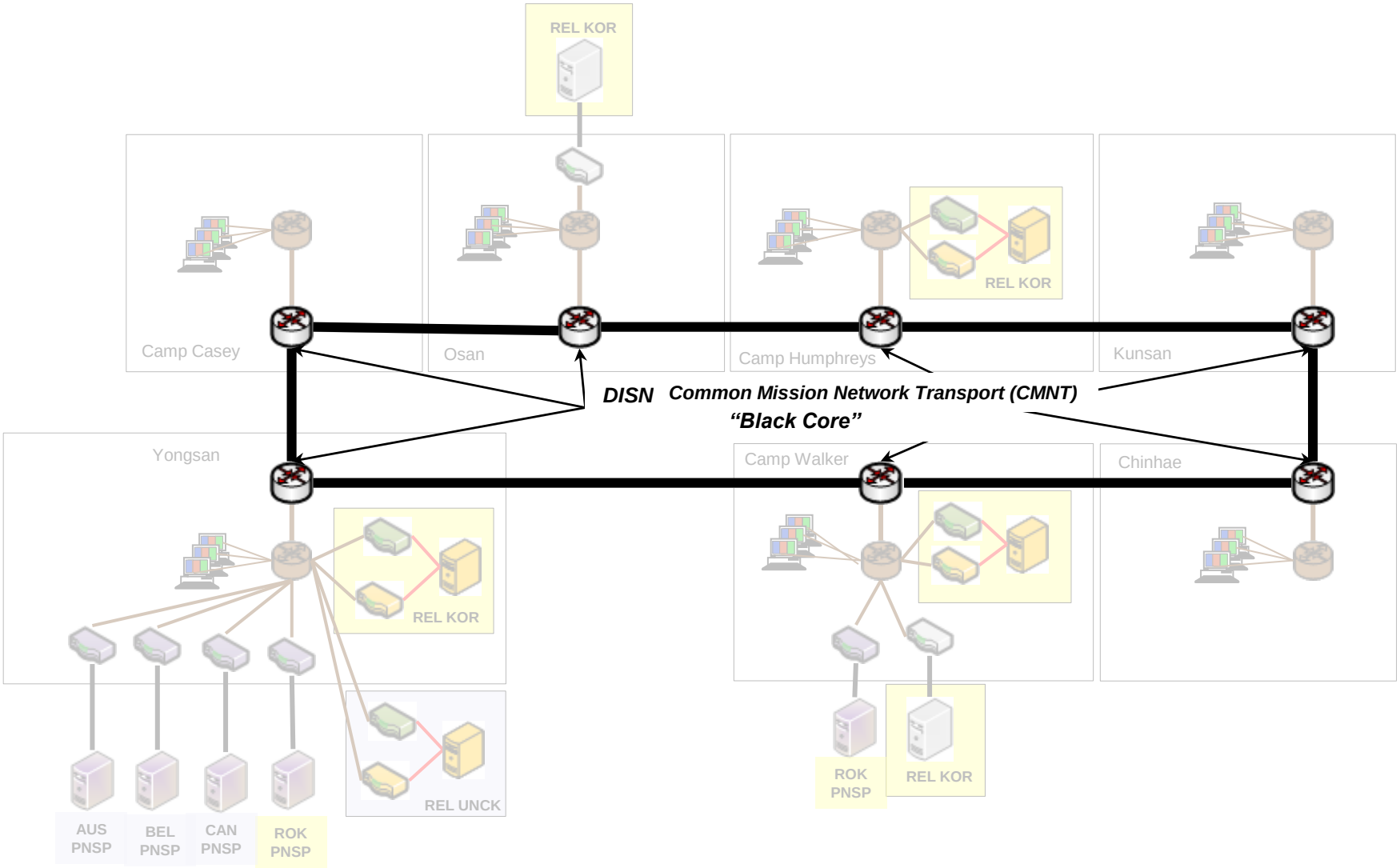
U.S. Forces Korea (USFK)
Operational Network Domain (OND)
"Black Core"



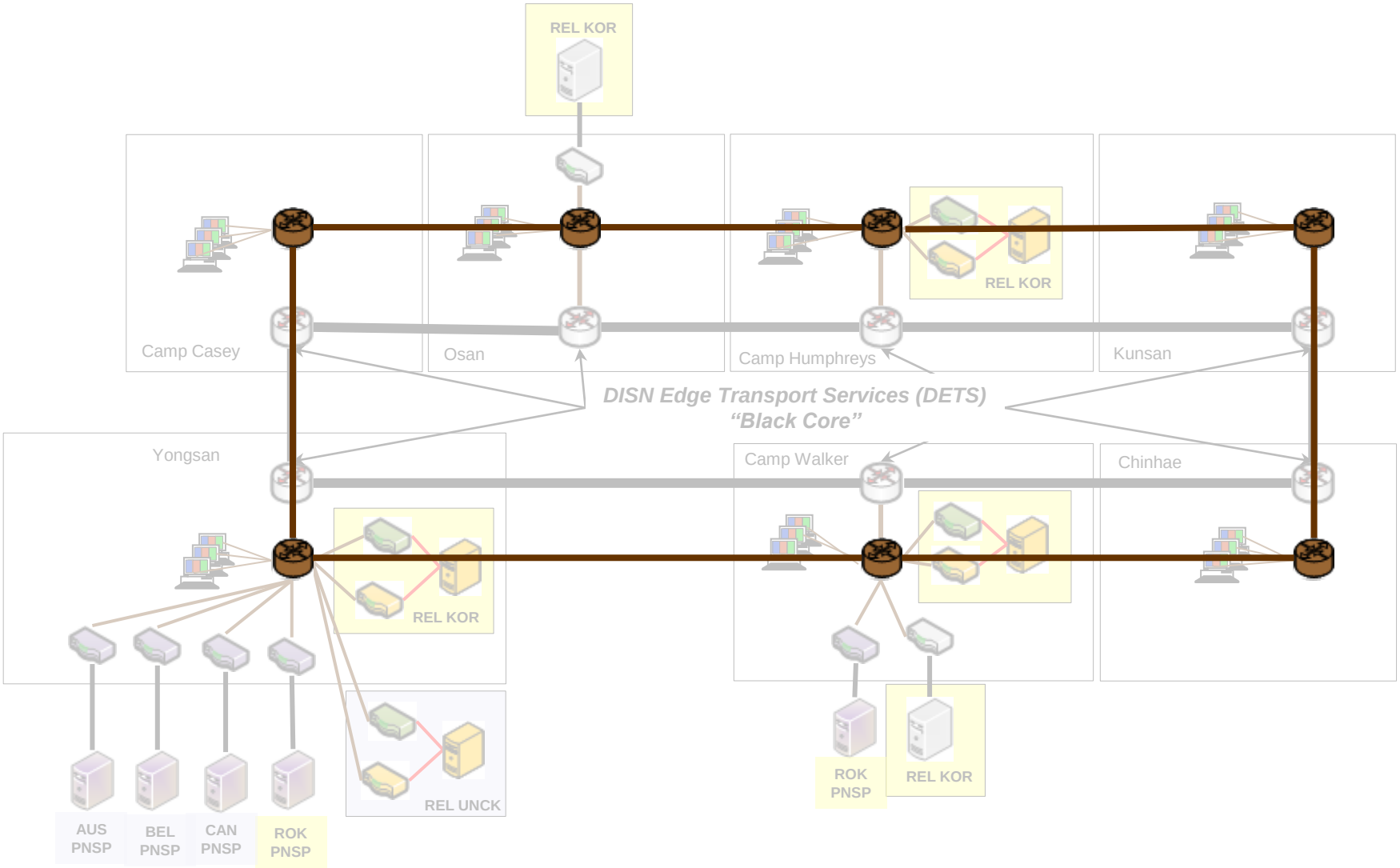
Example Korea System Topology



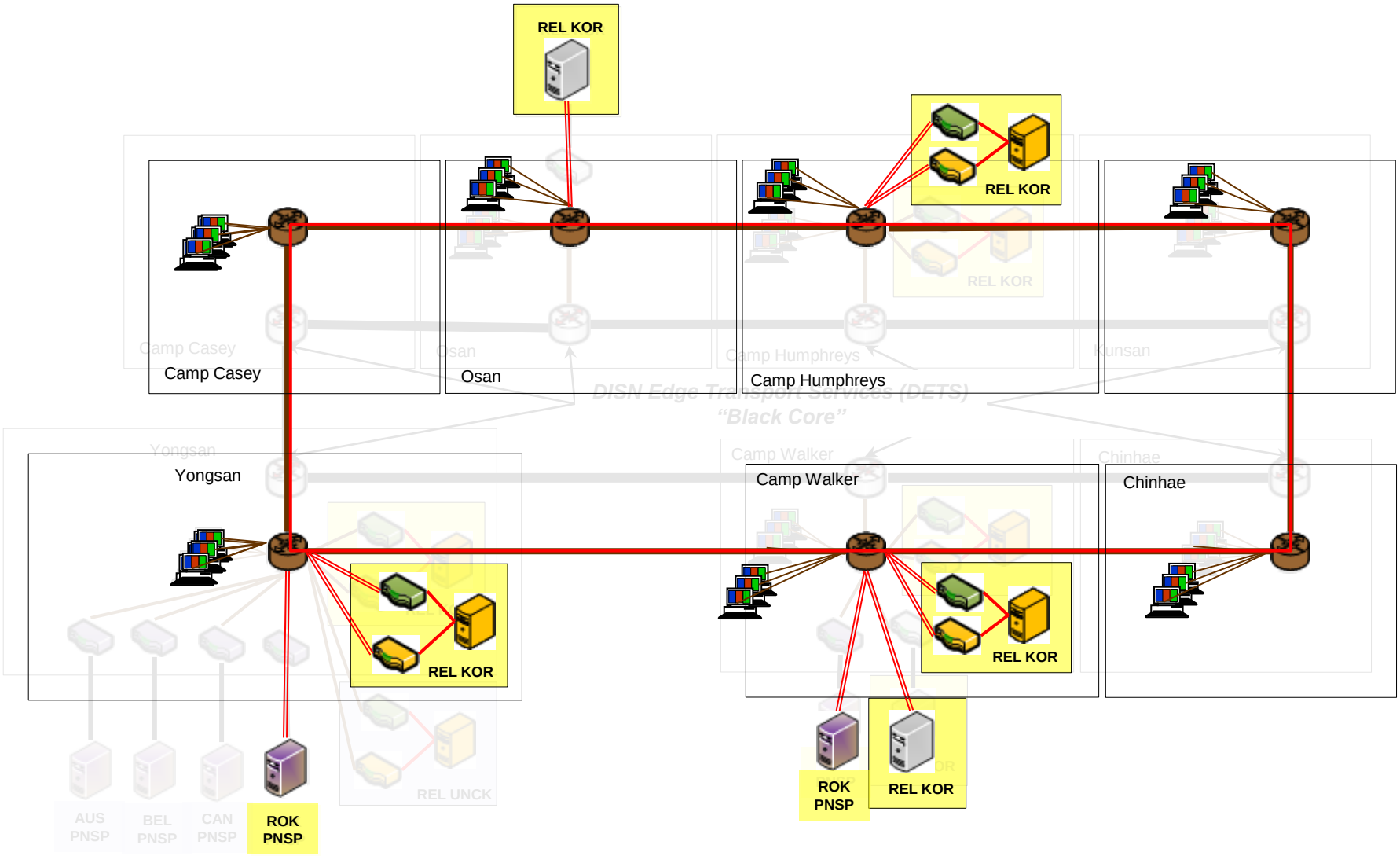
DISN Edge Transport Services “black core”



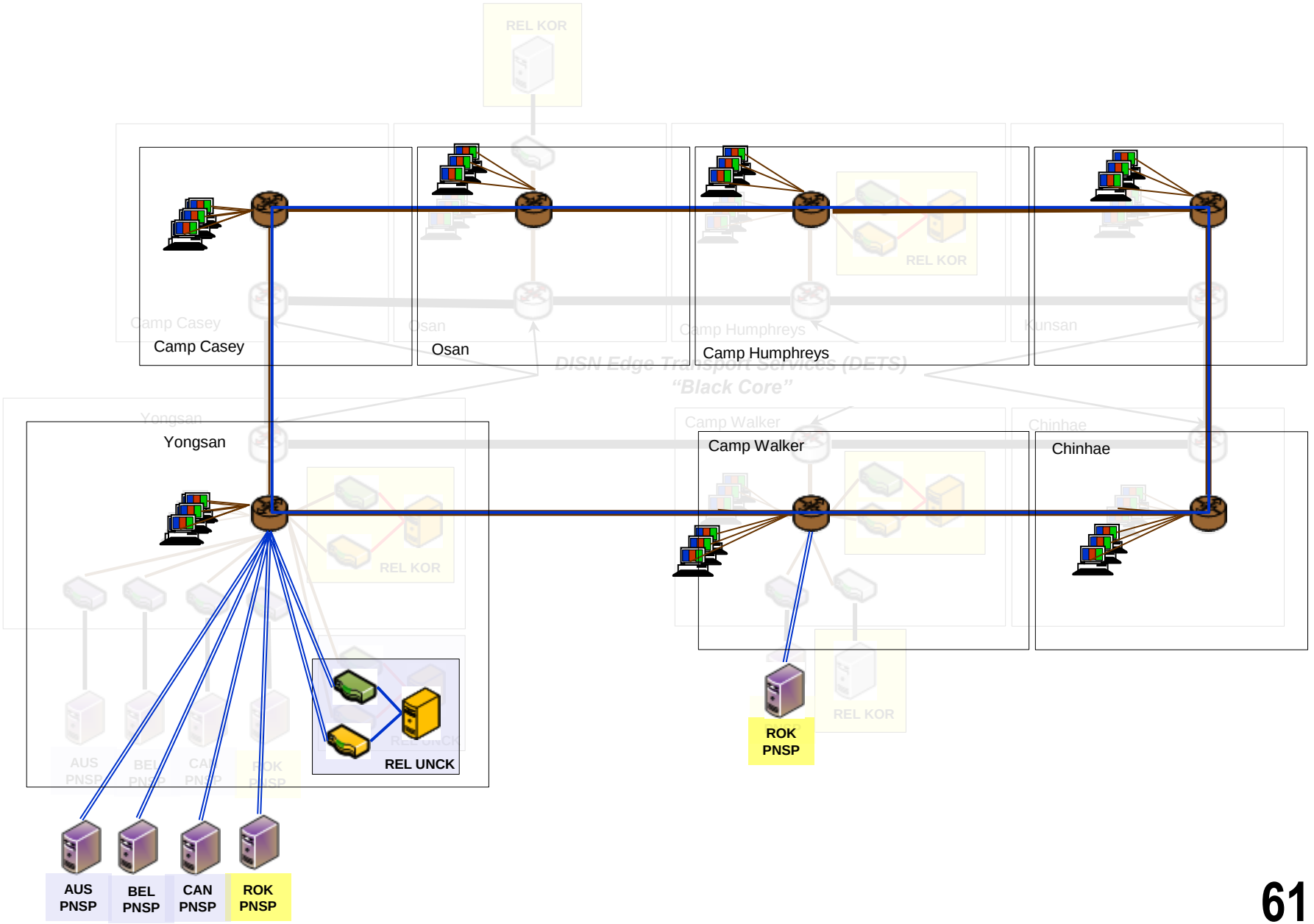
GIG 3.0 CMILNet / SMILNet / MILNet "brown core"



CENTRIXS-KOR

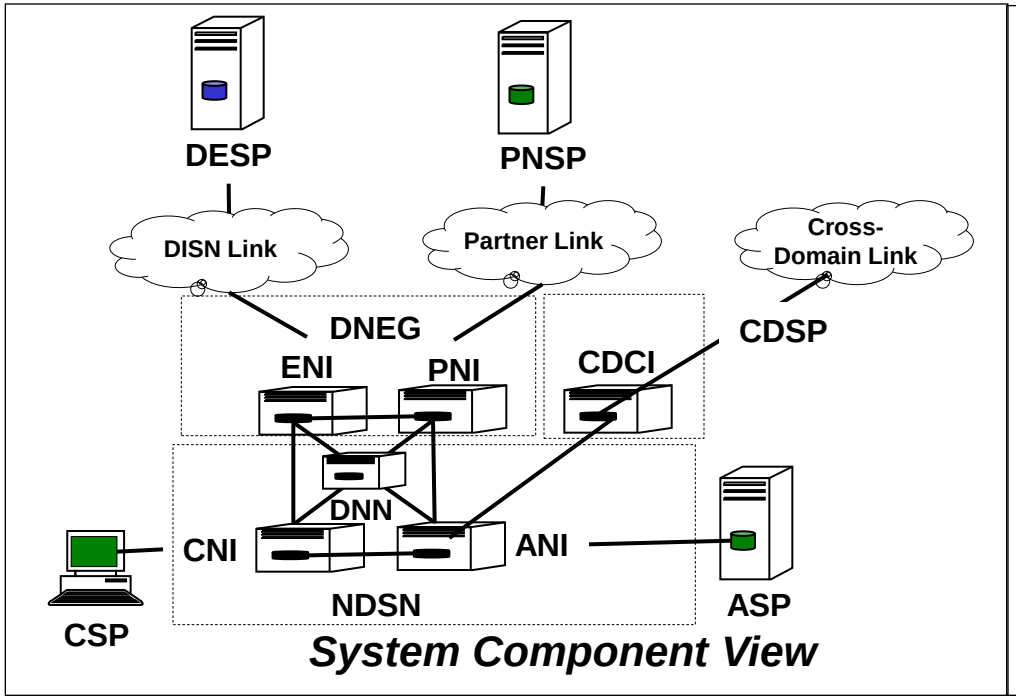


CENTRIXS-UNCK



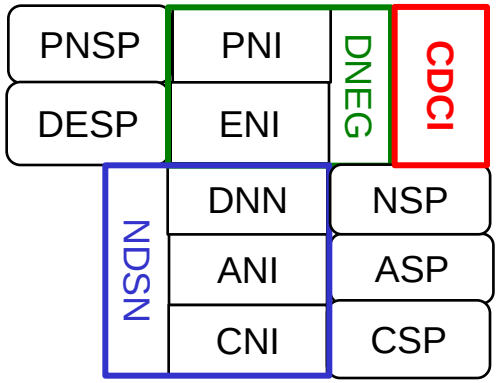
GIG 3.0 Interface Components

Internal to a single security enclave



System Component View

For Governance

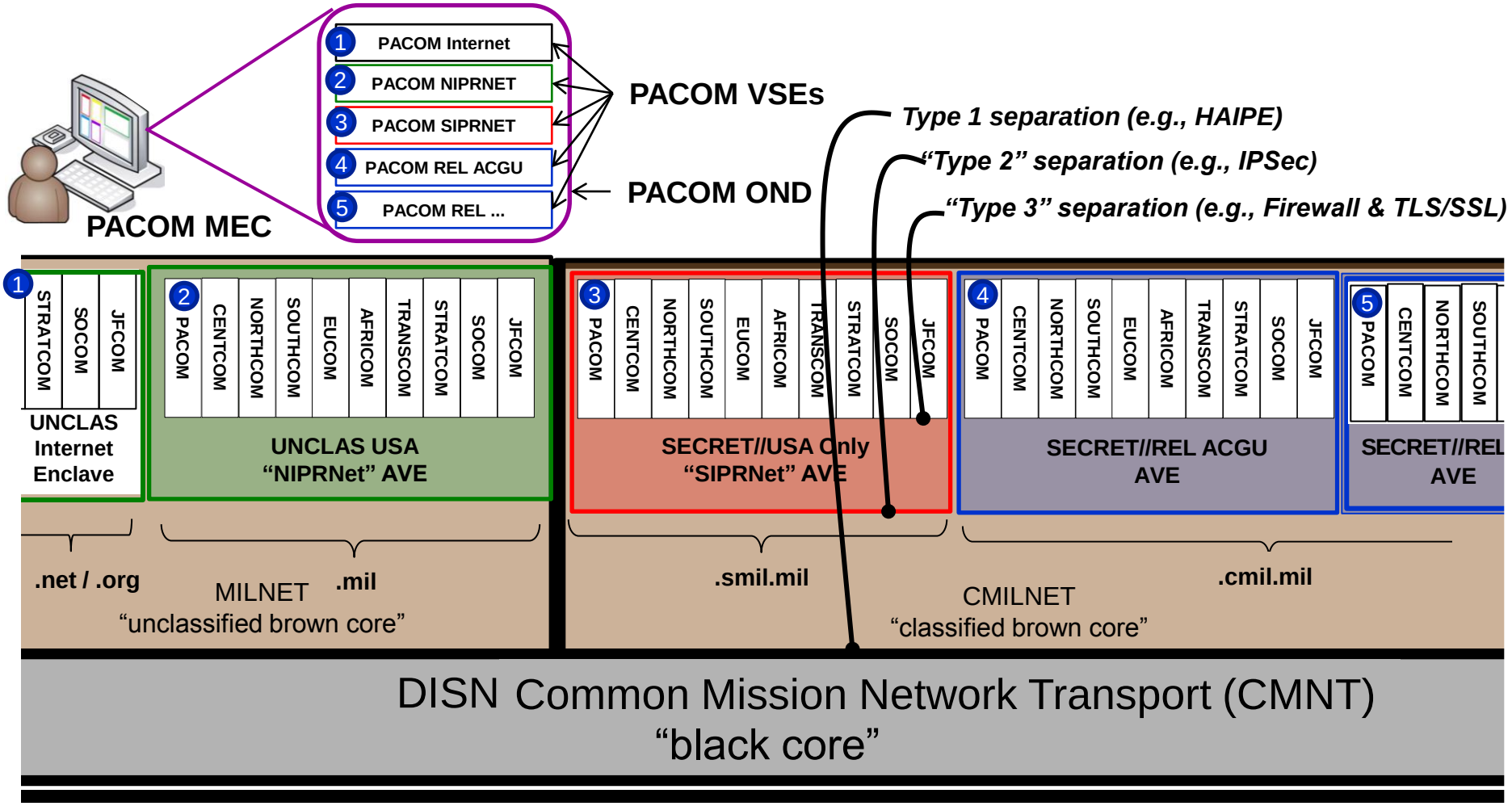


Block Diagram View

Acronyms

ASP – Application Service Point
ANI – Application Network Interface
CNI – Client Network Interface
CDCI – Cross-Domain Controlled Interface
CDSP – Cross-Domain Service Point
CSP – Customer Service Point
DESP – Defense Enterprise Service Point
DNEG – Dedicated Network Enclave Gateway
DNN – Domain Network Node
ENI – Enterprise Network Interface
NDSN – Network Domain Service Node
NSP – Network Service Point
PNI – Partner Network Interface
PNSP – Partner Network Service Point

GIG 3.0 Network Layers



Global Cyberspace Telecommunications Transport

AVE – Agile Virtual Enclave
DETS – DISN Edge Transport Service
HAIPE – High Assurance IP Encryption
IP – Internet Protocol
IPSec – IP Security
MEC – Multi Enclave Client
OND – Operational Network Domain
SSL – Secure Socket Layer
TLS – Transport Layer Security
VSE – Virtual Secure Enclave

GIG 3.0

VPN Enclave Control
&
User Client Cases

Mr. Randy Cieslak
CIO

U.S. Pacific Command
25 Octover 2010

This brief is classified:

UNCLASSIFIED

CMILNet VPN and Client Components for Enclave Protection

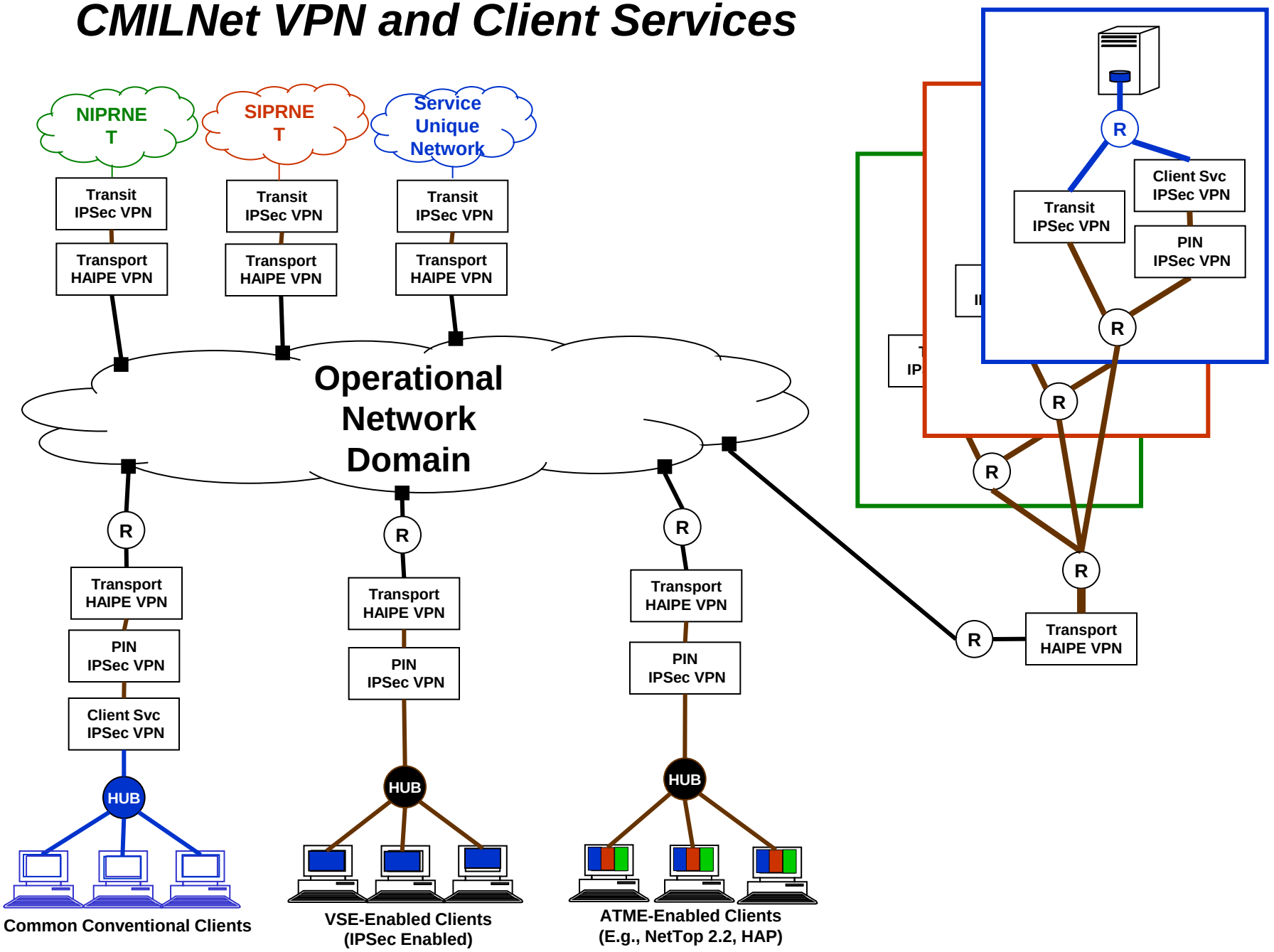
Virtual Private Networks (VPNs)

- Transport VPN (Type 1 / HAIPE)
- Transit VPN
- Protected Internodal Network
- Client Service VPN

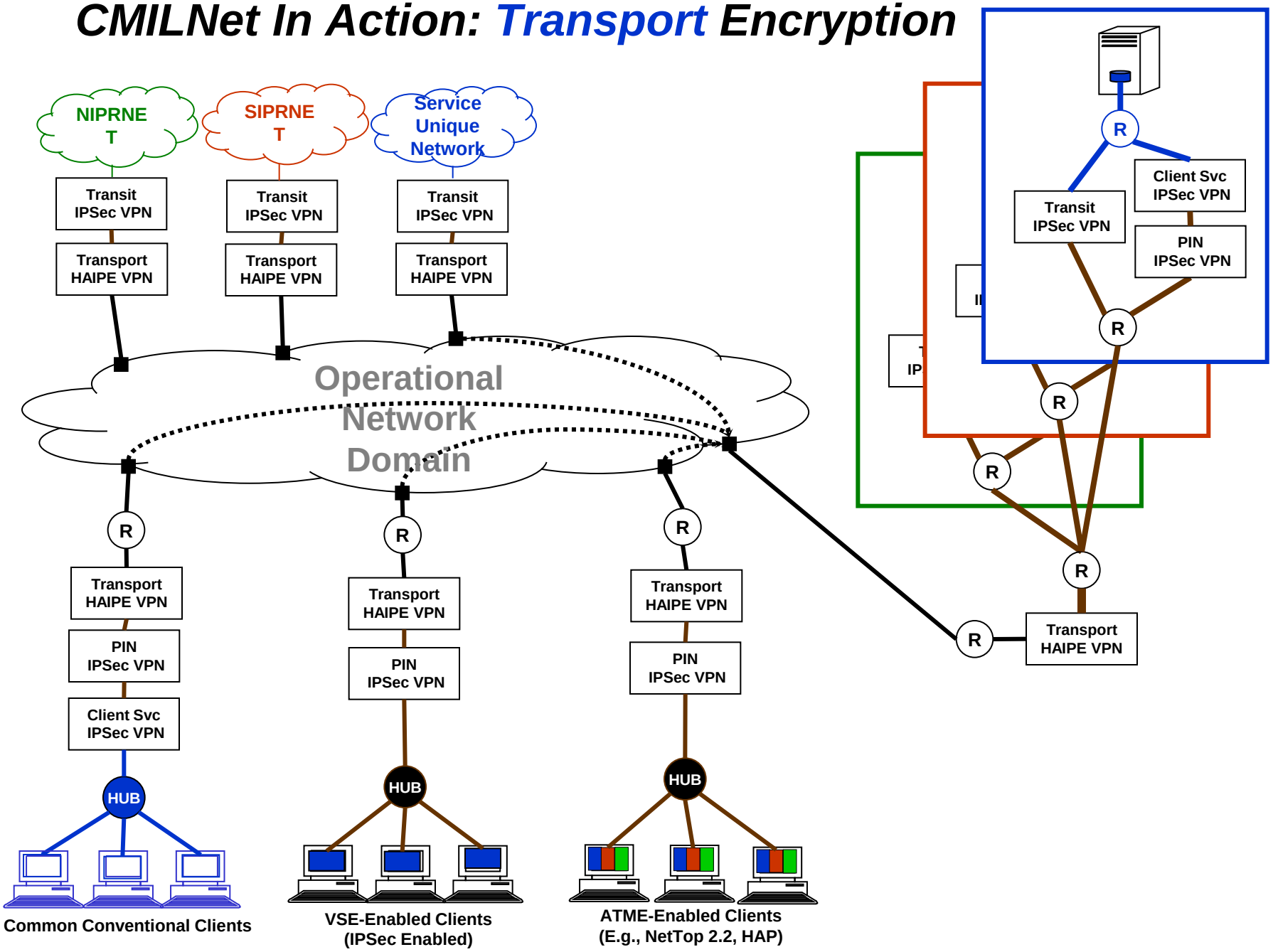
User Client Workstations (UCWS)

- Common Conventional
- Virtual Secure Enclave (VSE) Enabled
- Agile Trusted Multi Enclave (ATME)

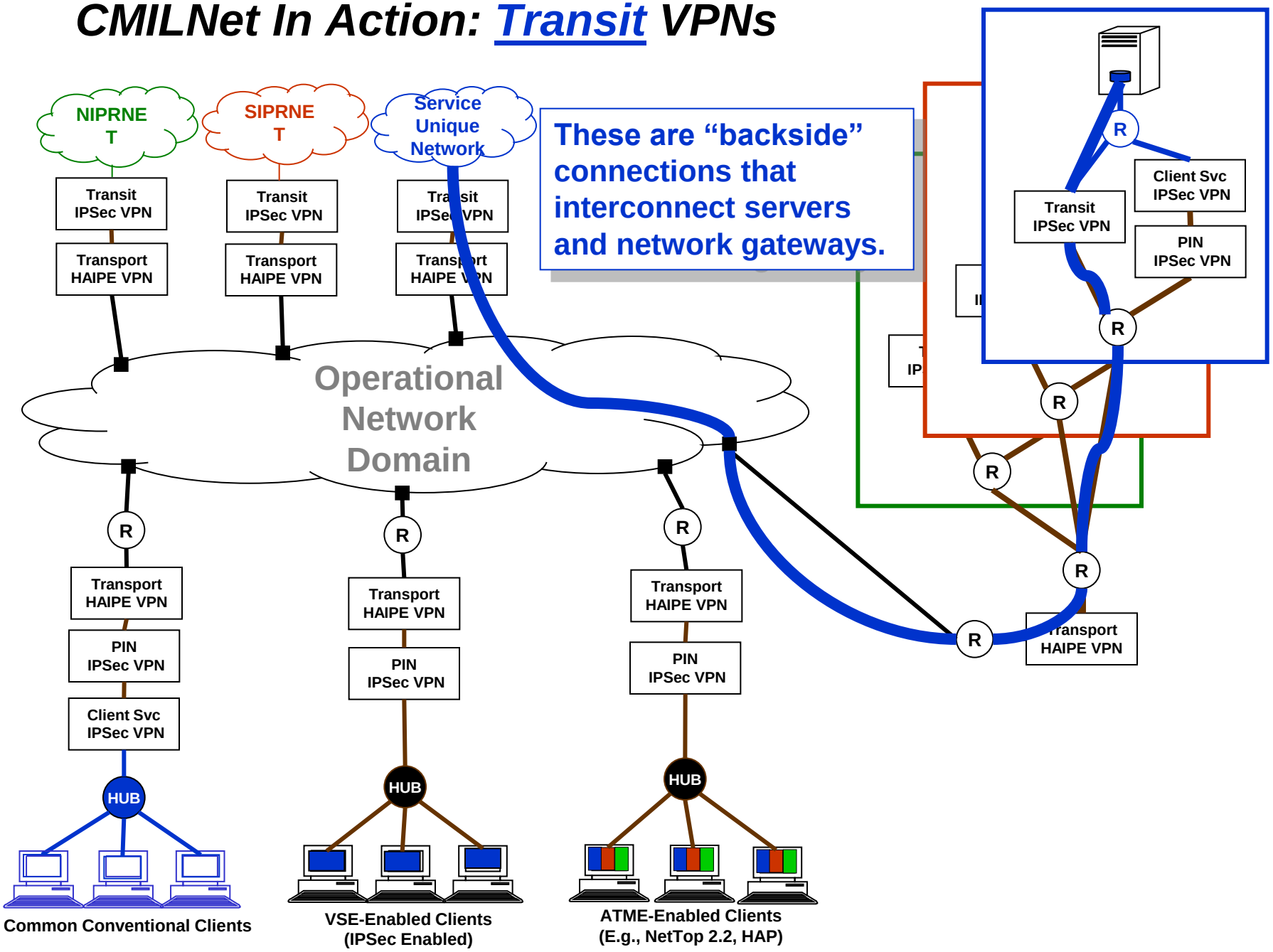
CMILNet VPN and Client Services



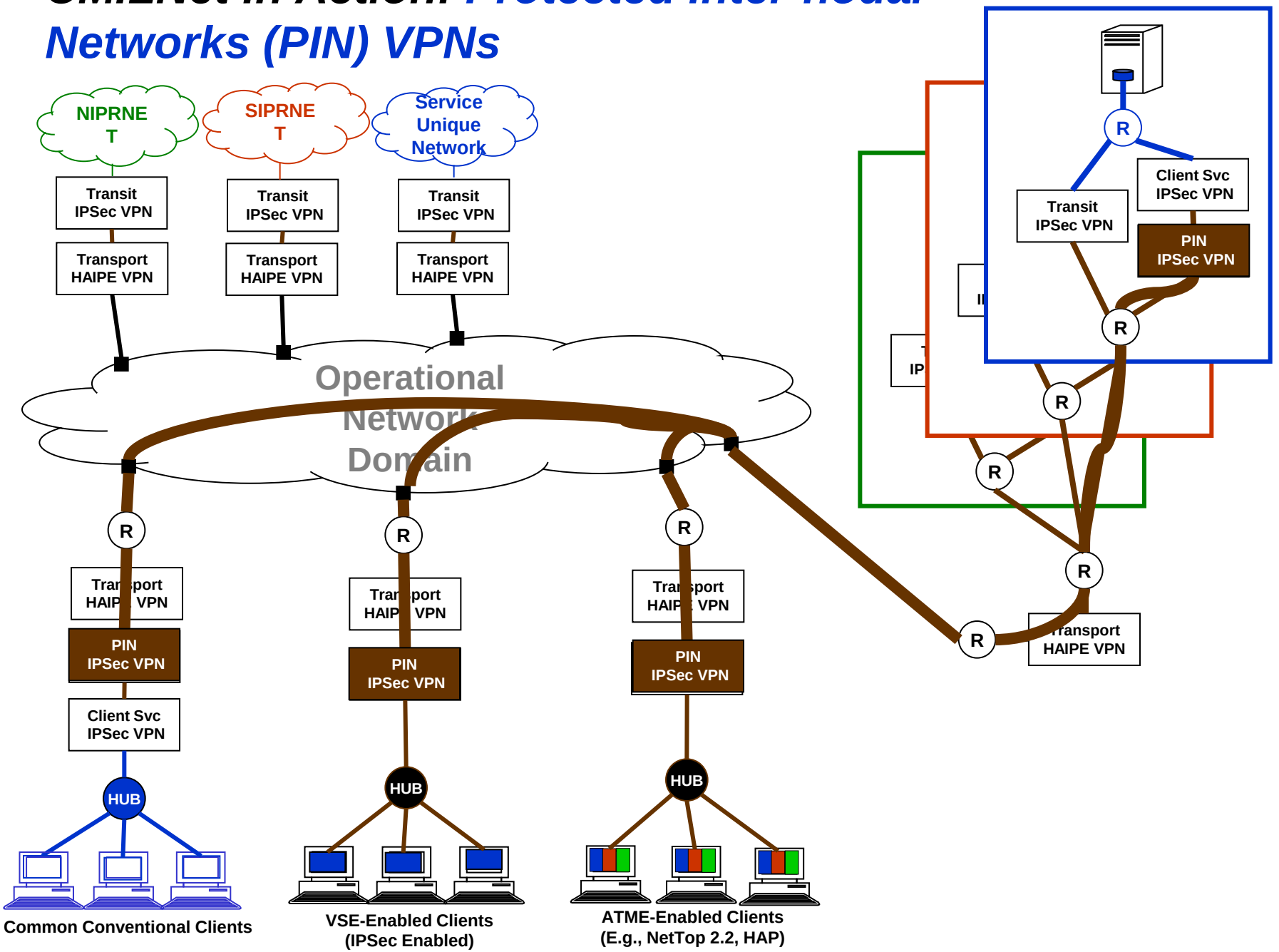
CMILNet In Action: Transport Encryption



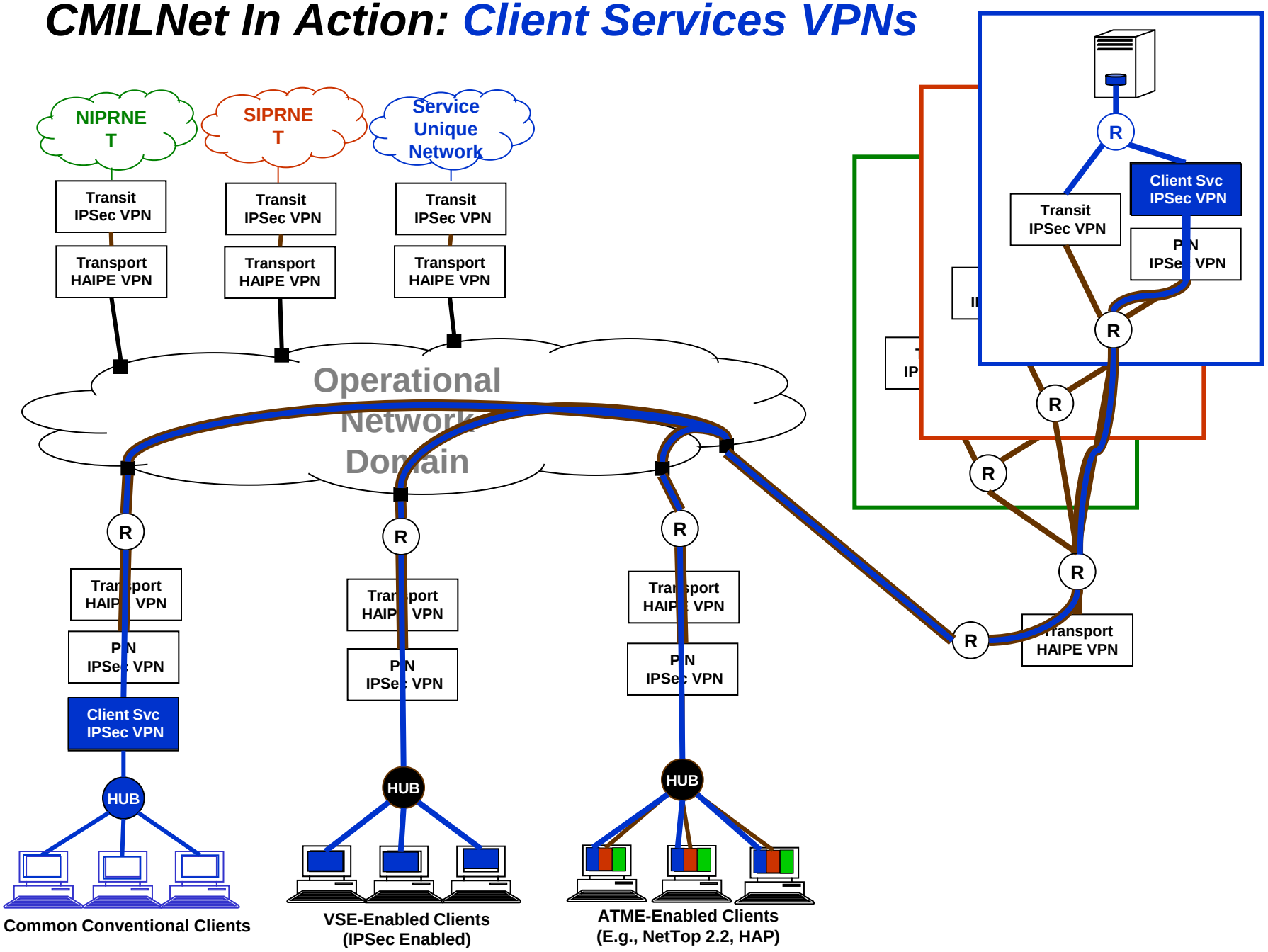
CMILNet In Action: Transit VPNs



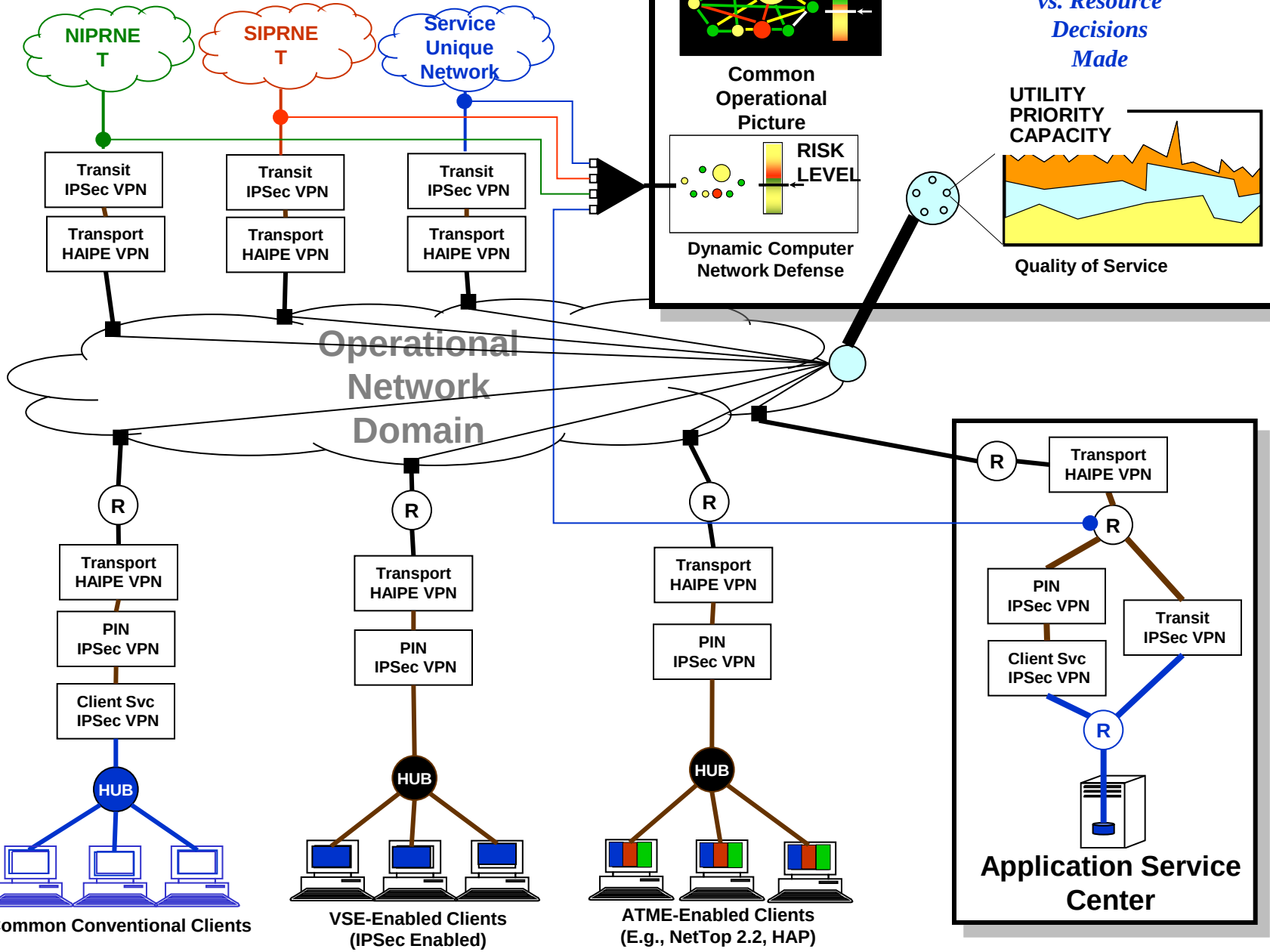
CMILNet In Action: Protected Inter-nodal Networks (PIN) VPNs



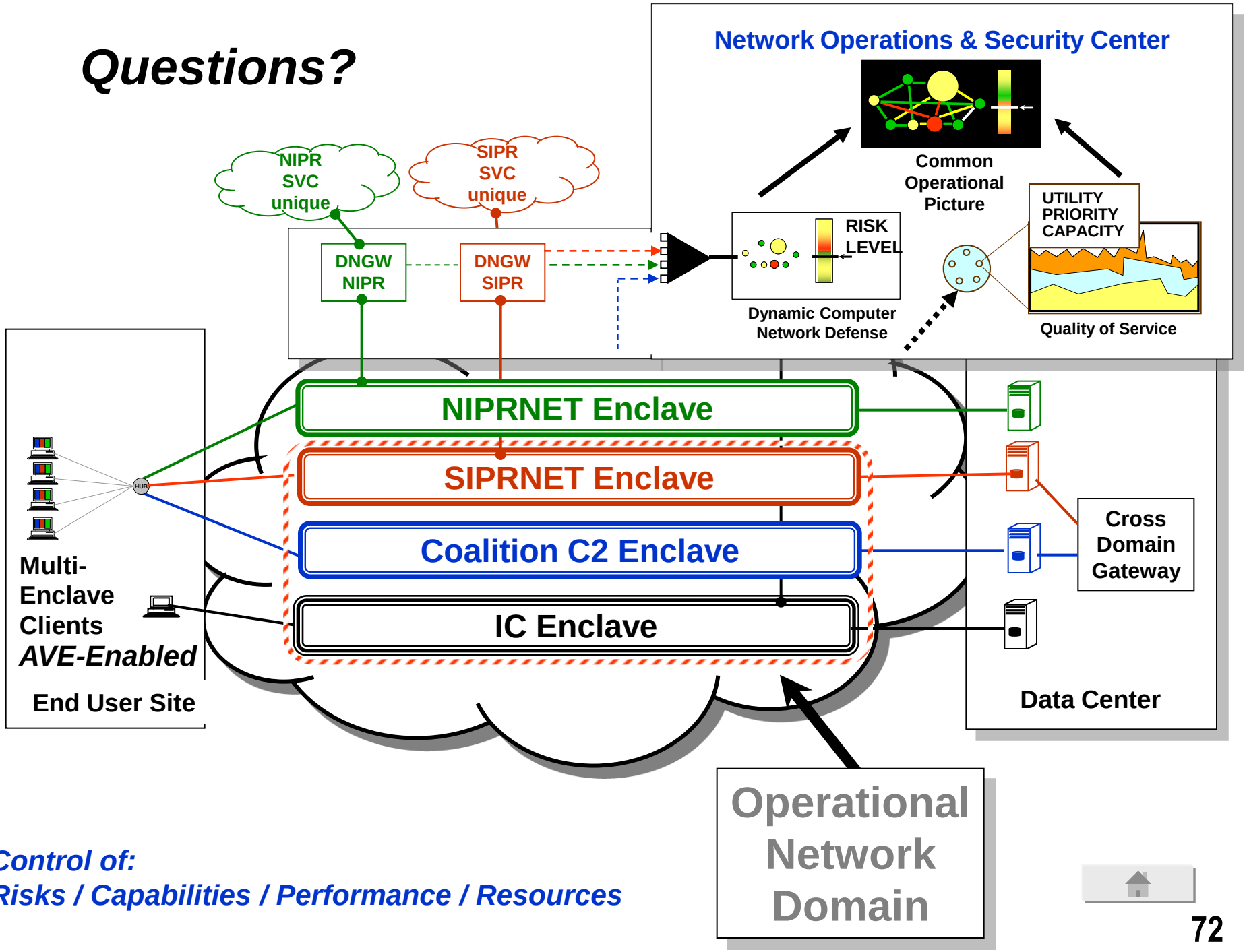
CMILNet In Action: Client Services VPNs



OND Network Operations



Questions?



Control of:
Risks / Capabilities / Performance / Resources

Agile Virtual Enclaves (AVE) Version 1.2 / 1.3
"Multi Enclave Client"
(MEC)

Randy Cieslak
Chief Information Officer

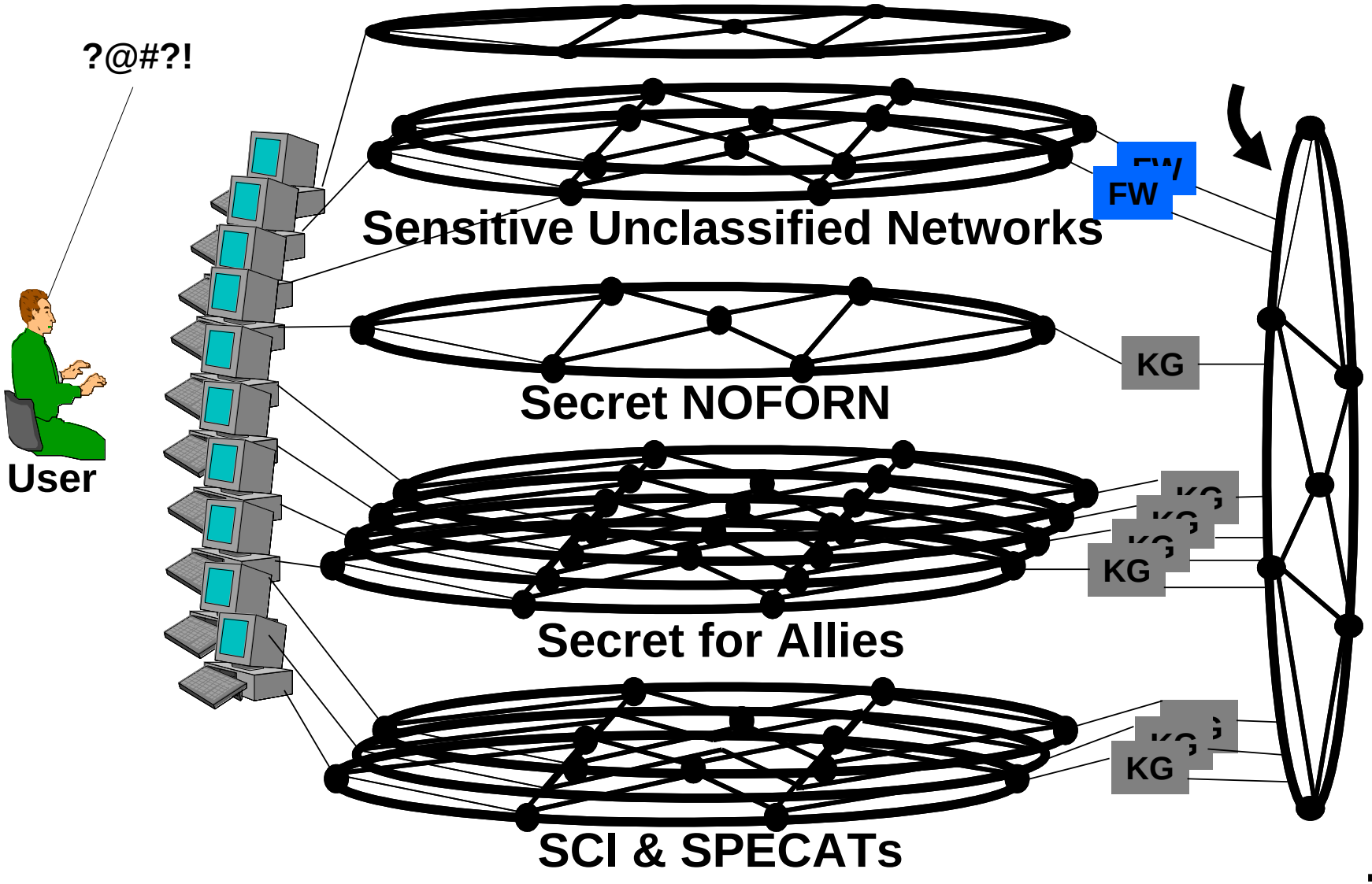
Jim Fordice
Referentia, Inc.

29 June 2010

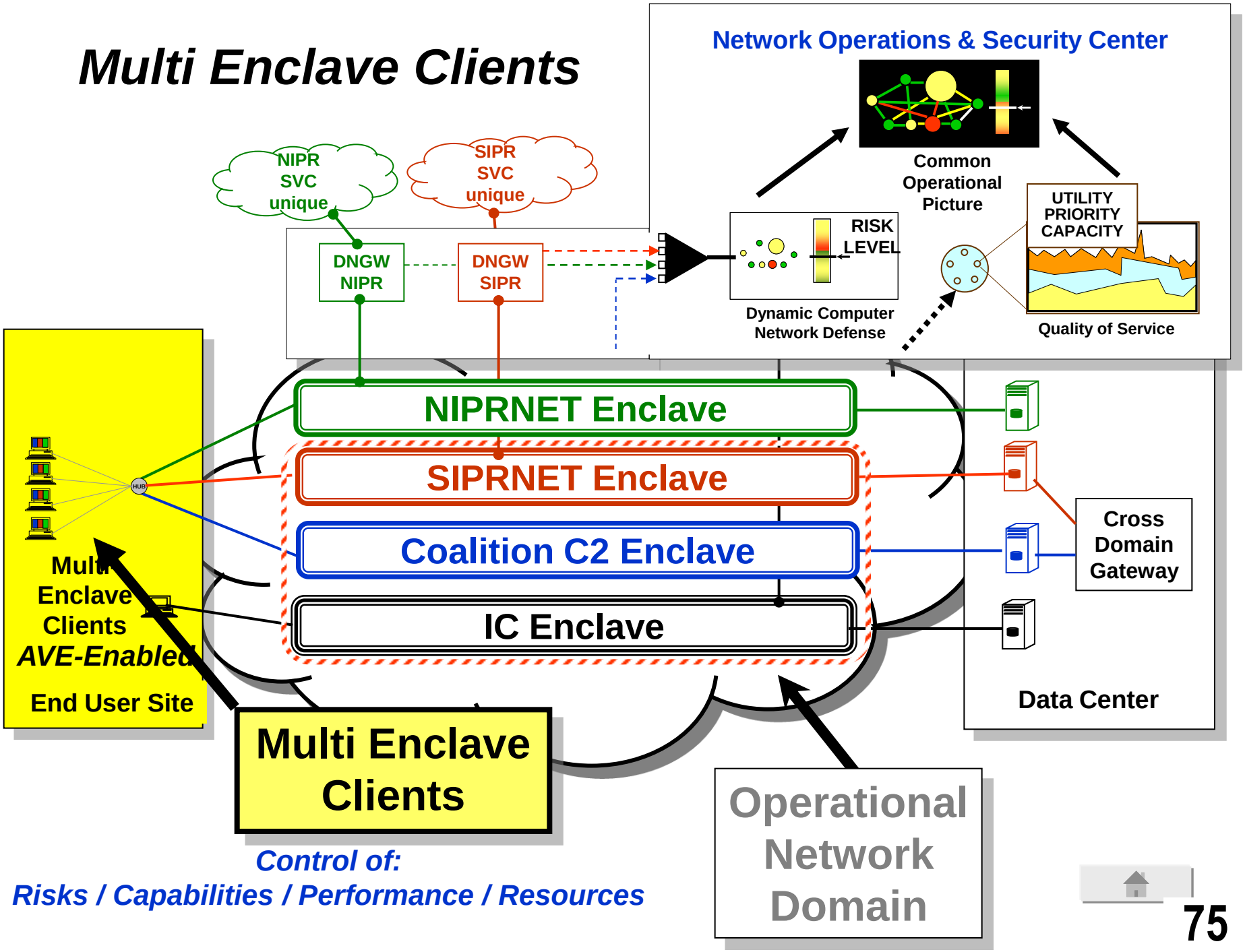
This brief is classified:

UNCLASSIFIED

How We Build Networks in Cyberspace Today



Multi Enclave Clients



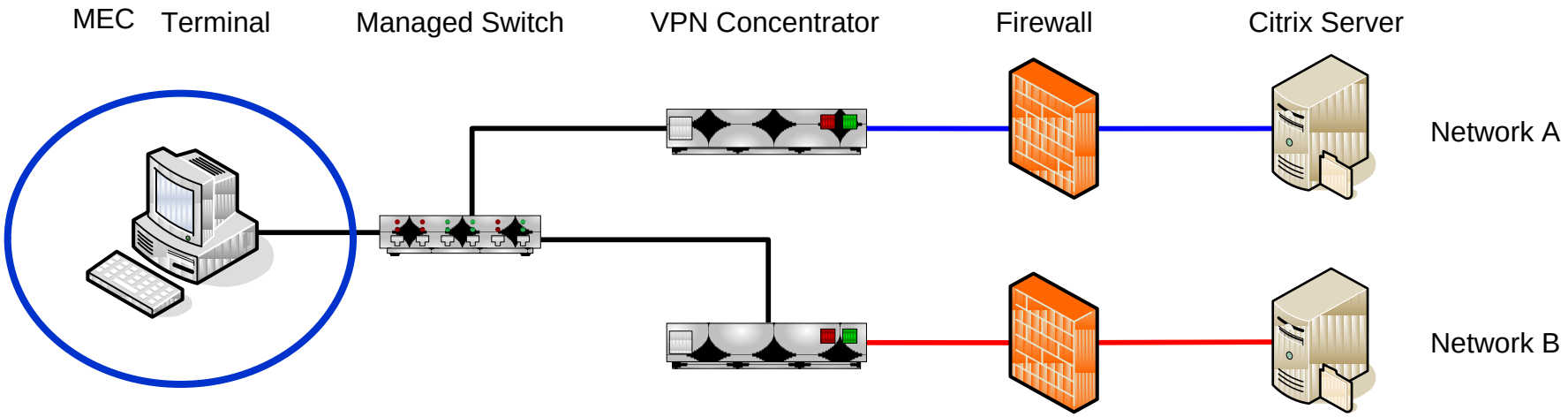
MEC Candidates Assessed

Solution Candidate	Performance Score	Key Characteristic
• Multi-Level Thin Client (MLTC) 3.0	10	Dedicated Infrastructure
• DoDIIS Trusted Workstation (DTW) 4.0	17	Dedicated Infrastructure
• Network on a Desktop (NetTop)	29	Modular / Single-Wire
• Secure Office Thin Client (SOTTC)	26	Dedicated Infrastructure
• Trusted Multi-Net (TMN)	22	Dedicated Infrastructure
• High Assurance Platform (HAP)	37	Multi-Wire
• Trusted Virtual Environment (TVE)	29	Multi-Wire

- **Dedicated infrastructure normally means single vendor and often proprietary**
- **Multi-Wire means that each network enclave requires its own physical network link**
- **Modular / Single Wire means standards-based. As long as COTS or GOTS products meet the standard and are tested (UCDMO baseline) they can be used.**

MEC Candidate Selected

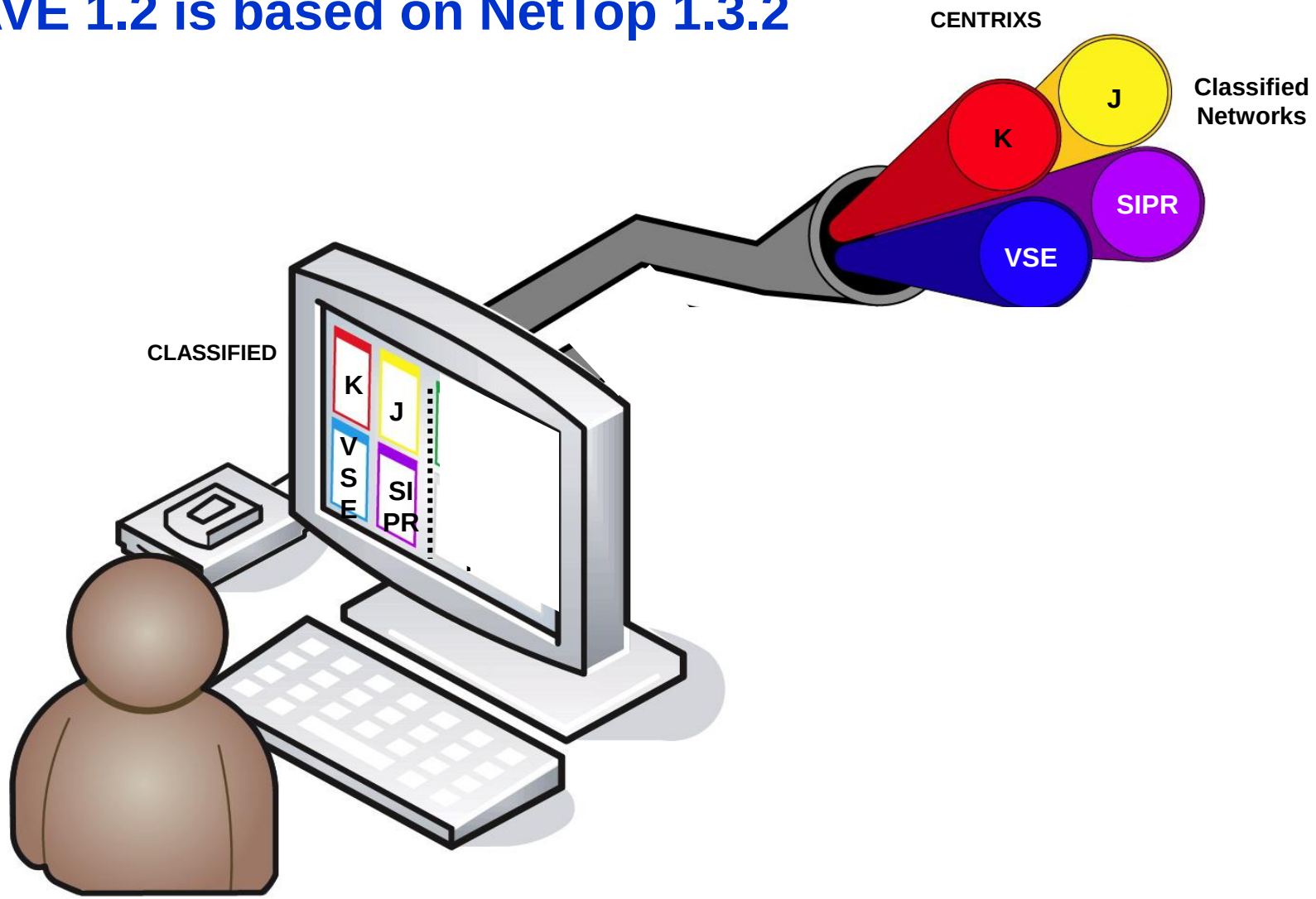
Solution Candidate	Performance Score	Key Characteristics
• Network on a Desktop (NetTop)	29	Modular / Single-Wire



- **MEC Terminal: NetTop 1.3.2 (Version 2.2 under NSA review)**
- **Managed Switch: Cisco Catalyst 2960**
- **VPN Concentrator: Cisco ASA 5510**
- **Firewall: McAfee Sidewinder 410F**
- **Terminal Services Server: Citrix**

MEC User Terminal View – AVE 1.2

AVE 1.2 is based on NetTop 1.3.2



MEC based on AVE 1.2 On The UCDMO Baseline

Cross Domain Baseline
V 3.4.0
18 June 2010

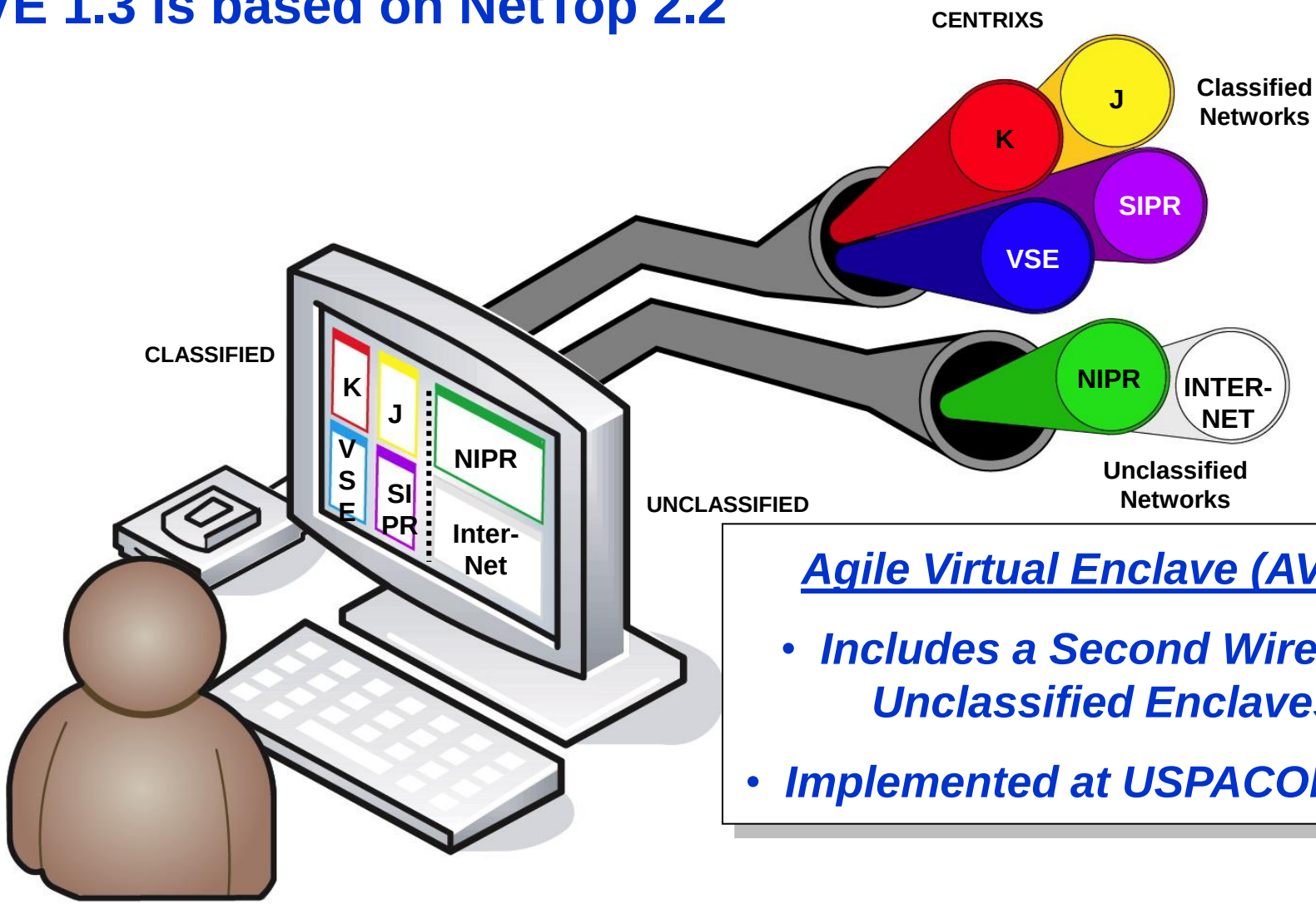
AVE 1.2 is a known configuration of HP NetTop 1.3.2 such that multiple SECRET and SECRET/REL networks can pass through a single wire using COTS IPSec VPNs to provide the network transmissions separation while transiting the LAN or WAN.

(U//FOUO)

Product/Solution Name	Type	Fur				
HP NetTop Ver. 1.3 Ver. 1.3.2	Access	HP NetTop multiple net different cla virtual envir enforcing st Control on a objects. Us from 'guest' operating sy application and support both thin and fat client requirements. It is a Virtual Machine Monitor application (VMWARE) installed on a Security Enhanced Linux (SELinux) host.				443-454-0102 rick.supplee@hp.com
		AVE 1.2 is a known configuration of HP NetTop 1.3.2 such that multiple SECRET and SECRET/REL networks can pass through a single wire using COTS IPSec VPNs to provide the network transmissions separation while transiting the LAN or WAN.	NSA	20080404 Regression: 20081003	SECRET and SECRET REL	**AVE Sponsor** USPACOM Randall Cieslak 808-477-7466 randall.cieslak@pacom.mil **AVE Support** Referentia Systems James Fordice 505-345-1641 jfordice@referentia.com

MEC User Terminal View – AVE 1.3

AVE 1.3 is based on NetTop 2.2



Agile Virtual Enclave (AVE)

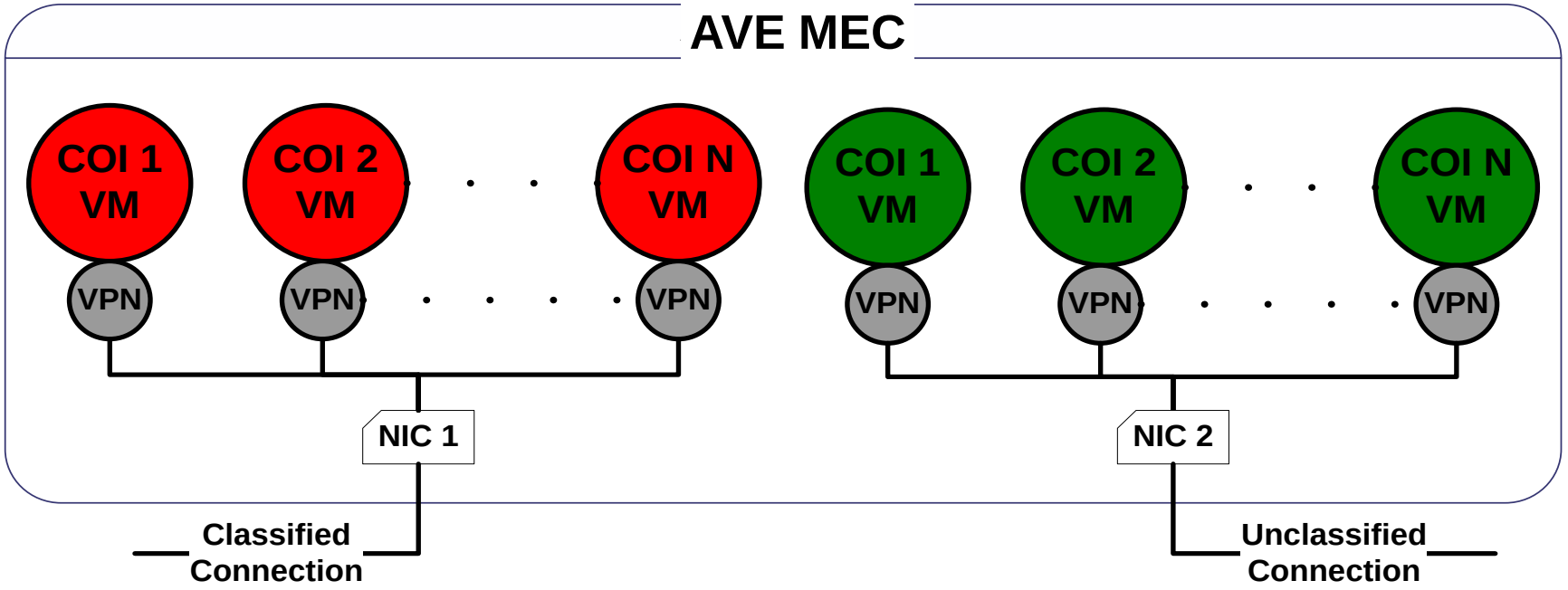
- ***Includes a Second Wire for Unclassified Enclaves***
- ***Implemented at USPACOM HQ***

AVE Certification & Accreditation

- **AVE 1.2 (COMTHIRDFLT)**
  - **DSAWG approved ATC**
  - **Navy ODAA approved ATO**
  - **Approved for UCDMO Baseline v3.4.0 update - June 2010**

- **AVE 1.3 (HQ USPACOM)**
  - **Demo approved by DSAWG**
  - **USPACOM DAA approved IATT**
  - **NSA has completed AVE 1.3 CT&E**
    - **Evaluating results of NSA testing**
  - **Next step is CDTAB/DSAWG to approve use of the technology**
  - **Long term plan is to submit for UCDMO Baseline**

Underlying Virtual Machines (AVE 1.3)



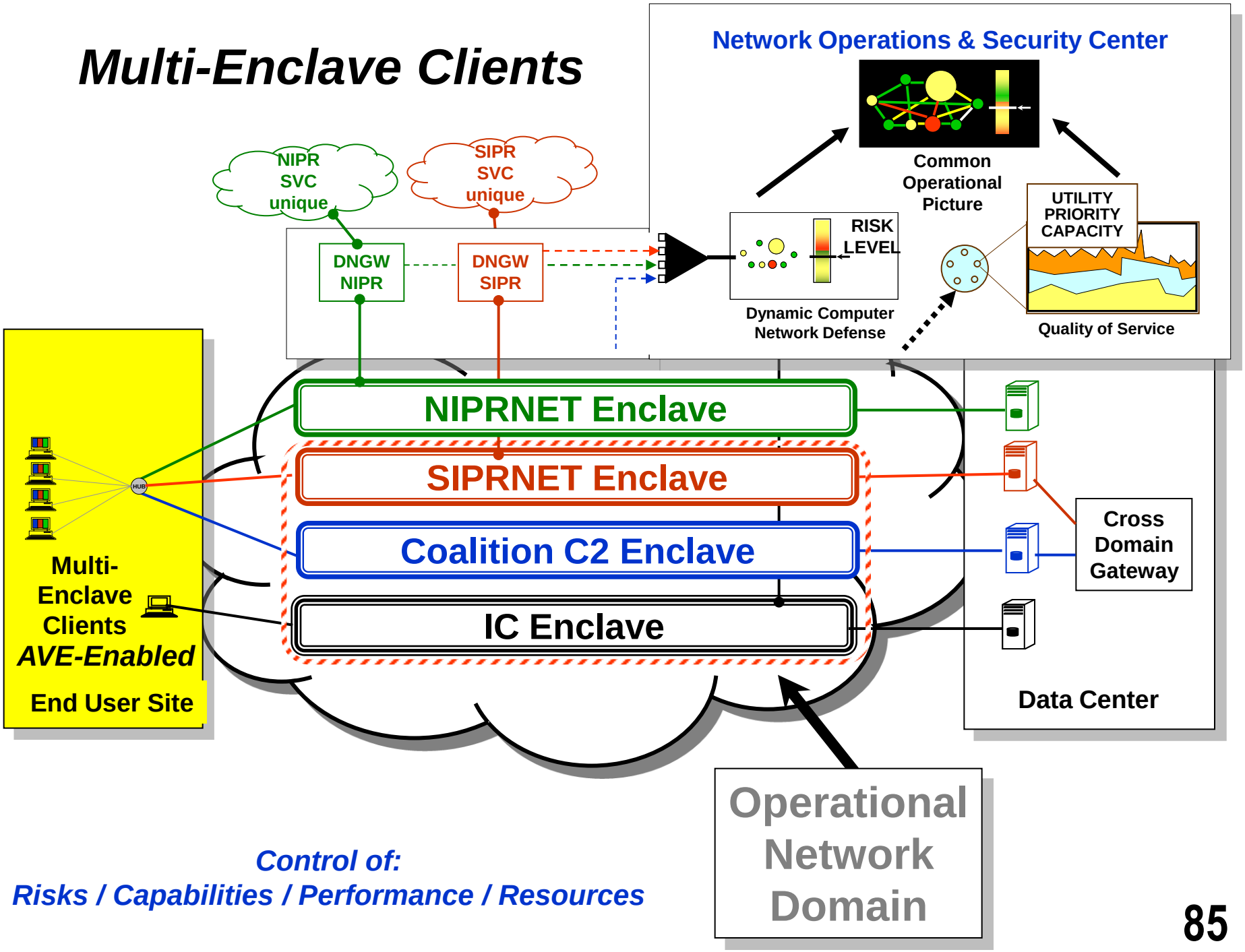
Enclaves for the USPACOM MEC

Network	Start Menu Name	Classification Marking
USA	USA Thick	SECRET
ACGU	ACGU Thin	SECRET//REL ACGU
JPN	JPN Thin	SECRET//REL JPN
JPN	JPN Thick	SECRET//REL JPN
KOR	KOR Thin	SECRET//REL KOR
SIPR	SIPR Thick	SECRET
GCTF	GCTF Thin	SECRET//REL GCTF
VSE	SIPR VSE Thin	SECRET
APAN	APAN	UNCLASSIFIED
CMFP	CMFP Thin	SECRET//REL CMFP
FVEY	FVEY Thin	SECRET//REL FVEY
NIPR	NIPR Thin	NIPRNET UNCLASSIFIED//FOUO
SGP	SGP Thin	SECRET//REL SGP
UNCK	UNCK Thin	SECRET//REL UNCK

14 Virtual Machines:

- **2 UNCLAS, 12 SECRET**
- **4 Thick, 10 Thin**

Multi-Enclave Clients



Control of:
Risks / Capabilities / Performance / Resources

GIG 3.0
Design Approach

Randy Cieslak

U.S. Pacific Command

Chief Information Officer

19 November 2010

Confluence of Concerns & Solutions (1 of 2)

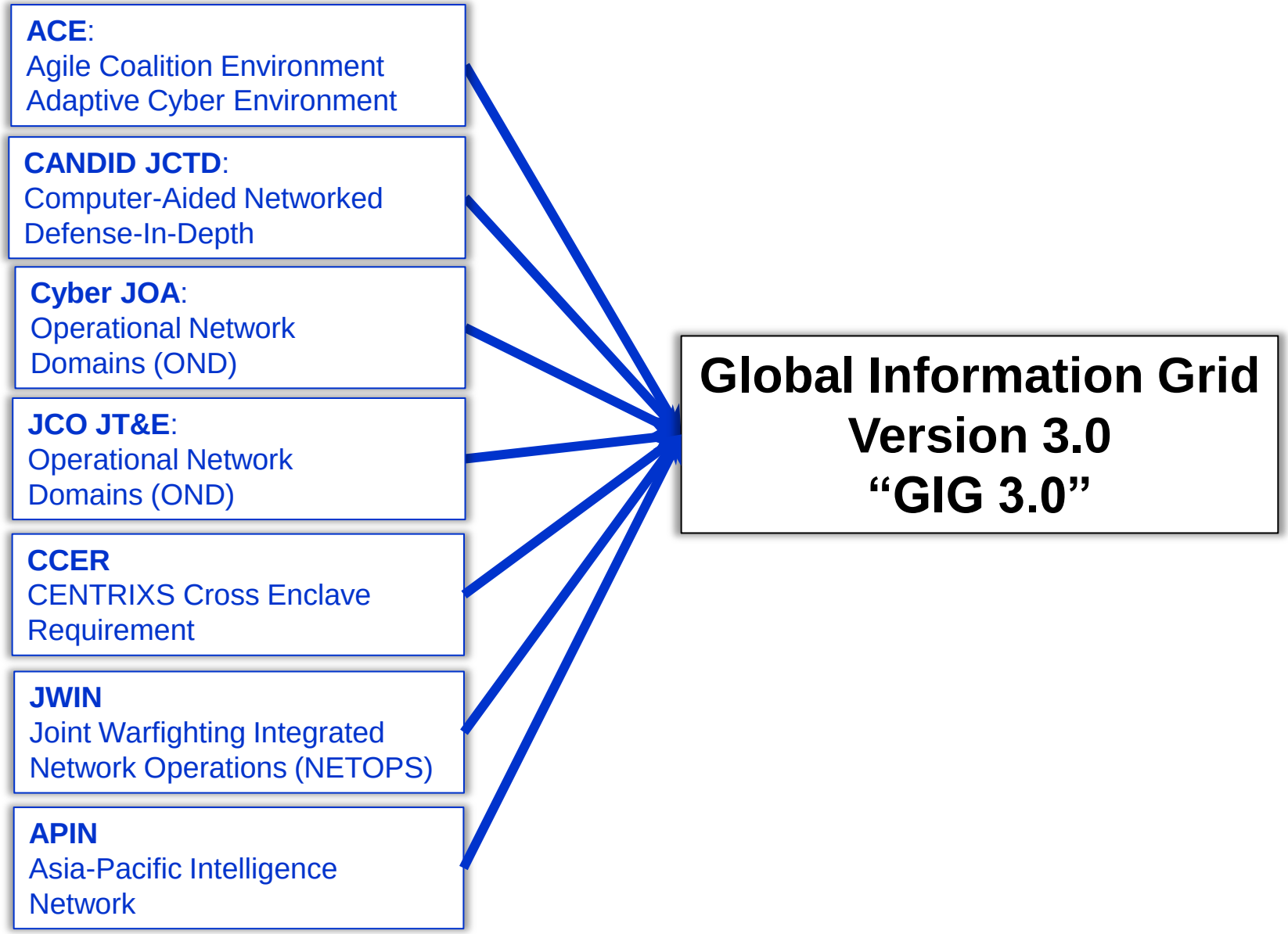
- **CONCERN 1**
  - **We need to use the same infrastructure to create network enclaves to replace the expensive and cumbersome CENTRIXS networks**
    - **SOLUTION:** Agile Coalition Environment

      *** Adaptive Cyber Environment (ACE)**
- **CONCERN 2**
  - **We need to create defendable network enclaves to fight through cyber attacks that have left our main networks vulnerable**
    - **SOLUTION: Computer Aided Network Defense in Depth (CANDID)**
- **CONCERN 3**
  - **We need to create network zones that will permit operational commanders to manage their own risk to their own mission**
    - **SOLUTION: Cyber Joint Operational Area (JOA) formed by Operational Network Domains (OND)**
- **CONCERN 4**
  - **We need tactics, techniques and procedures to surveil, control and operate this new network environment**
    - **SOLUTION: Joint Cyber Operations (JCO) Joint Test & Evaluation (JT&E)**

Confluence of Concerns & Solutions (2 of 2)

- **CONCERN 5**
  - **We need a means to safely and securely move authorized information between enclaves and a simple way to access enclaves not normally used**
    - **SOLUTION: Combined Enterprise Regional Information Exchange System (CENTRIXS) Cross Enclave Requirement (CCER)**
- **CONCERN 6**
  - **We need to understand and display network and information system activities, determine the associated mission risk and provide associated decision support displays**
    - **SOLUTION: Joint Warfighting Integrated Network Operations (NETOPS) (JWIN) Joint Concept Technical Demonstration (JCTD)**
- **CONCERN 7**
  - **We need to take advantage of current and planned network initiatives that "almost" take advantage of modern network technology methods and steer them to an effective, coherent, consistent overarching approach.**
    - **SOLUTIONS:**
      - **ASIA-PACIFIC Intelligence Network (APIN)**

Integrating the Solutions: "GIG 3.0"



Integrating the Solutions: "GIG 3.0"

ACE:
Agile Coalition Environment
Adaptive Cyber Environment

CANDID JCTD:
Computer-Aided Networked Defense-In-Depth

Cyber JOA:
Operational Network Domains (OND)

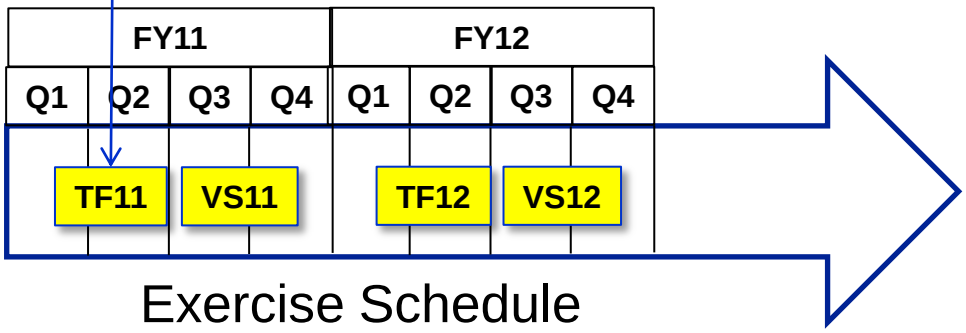
JCO JT&E:
Operational Network Domains (OND)

CCER
CENTRIXS Cross Enclave Requirement

JWIN
Joint Warfighting Integrated Network Operations (NETOPS)

APIN
Asia-Pacific Intelligence Network

Global Information Grid Version 3.0 "GIG 3.0"



Building GIG 3.0 – A Two-Phase Approach

Phases to be done concurrently

- **Phase 1: Build a agile information infrastructure that:**
  - **Compartmentalizes the network to enforce information protection and control policies**
  - **Compartmentalizes the network to separate risk-postures between the enterprise and the commander's mission area**
  - **Leverages and reuses common infrastructure to support compartmentalization**
  - **Provides controlled interfaces into and between the compartments**
  - **Provides access controls and minimizes customer service points**
- **Phase 2: Control, instrument and conceal the network to:**
  - **Monitor and control the interfaces for optimal performance**
  - **Detect sources of intrusion and react accordingly**
  - **Determine and display the level of associated risk to the mission**
  - **Posture network appearance to maintain information dominance**

Phase 1:

Agile, Compartmented Information Infrastructure

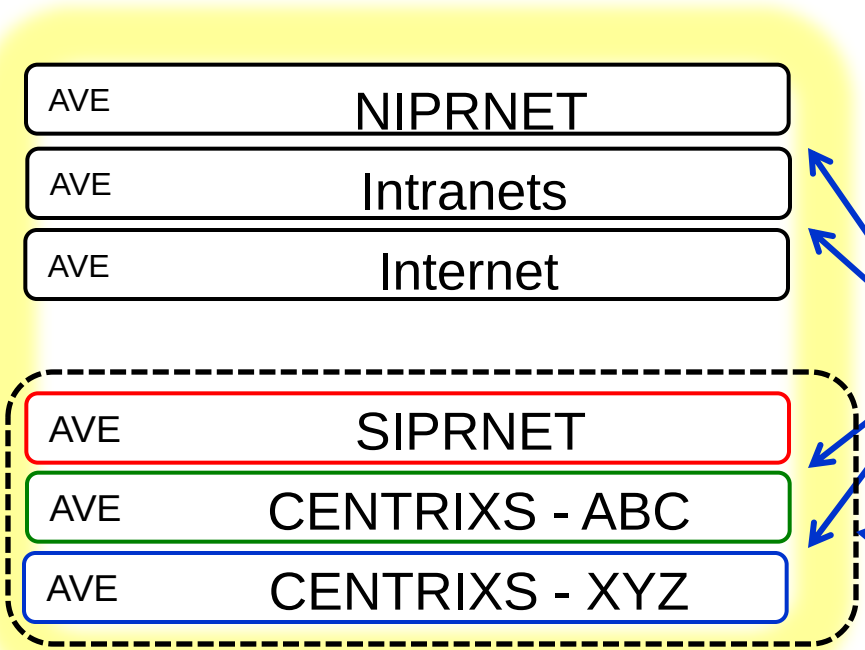
Primary Design Driver – Agile Virtual Enclaves (AVE)

Adopted from ACE

Associated Projects / Efforts

AVE

- **IPSec – Internet Protocol Security**
- **IPv6 – Internet Protocol Version 6**
- **IKE – Internet Key Exchange**
- **Naming convention**
- **IP Addressing**
- **DCSP – Differential Code Service Point**
- **DNS – Domain Naming Service**
- **DNN – Domain Network Node**



IPSec Provides Sufficient Strength of Separation.

But classified networks need a protected environment.

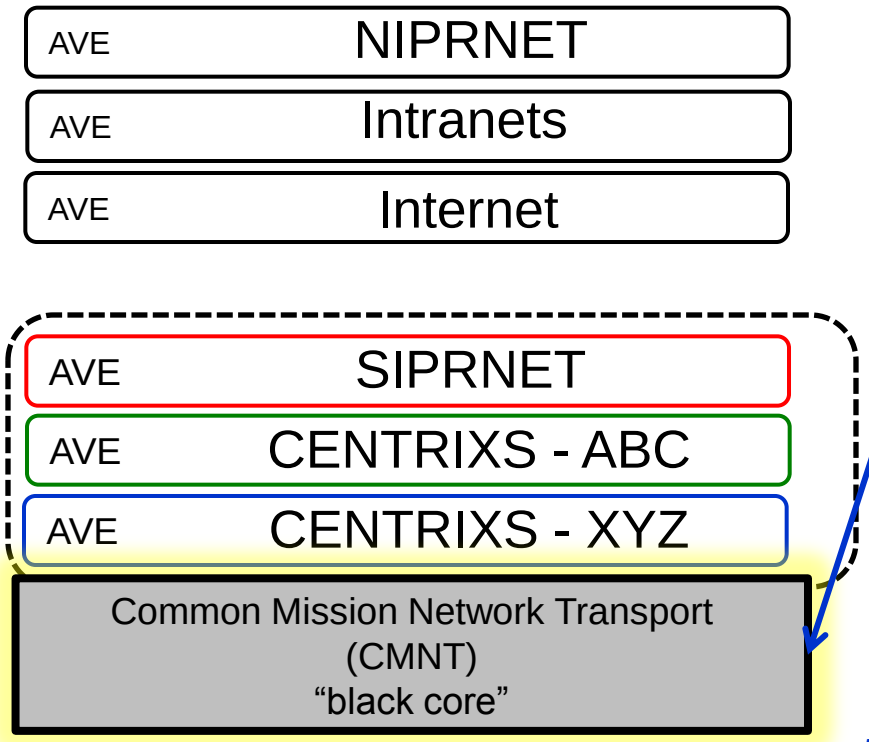
This design feature technologically enforces information classification, release, exposure and disclosure policies.

Foundation for the AVEs:

Defense Information Systems Network (DISN)

Common Mission Network Transport (CMNT)

Internet Protocol (IP) – Based Telecommunication Services



Provides the wide area network to deploy and extend AVEs worldwide.

Employs a separate MPLS from SIPRNET, NIPRNET, JWICS

Associated Projects / Efforts

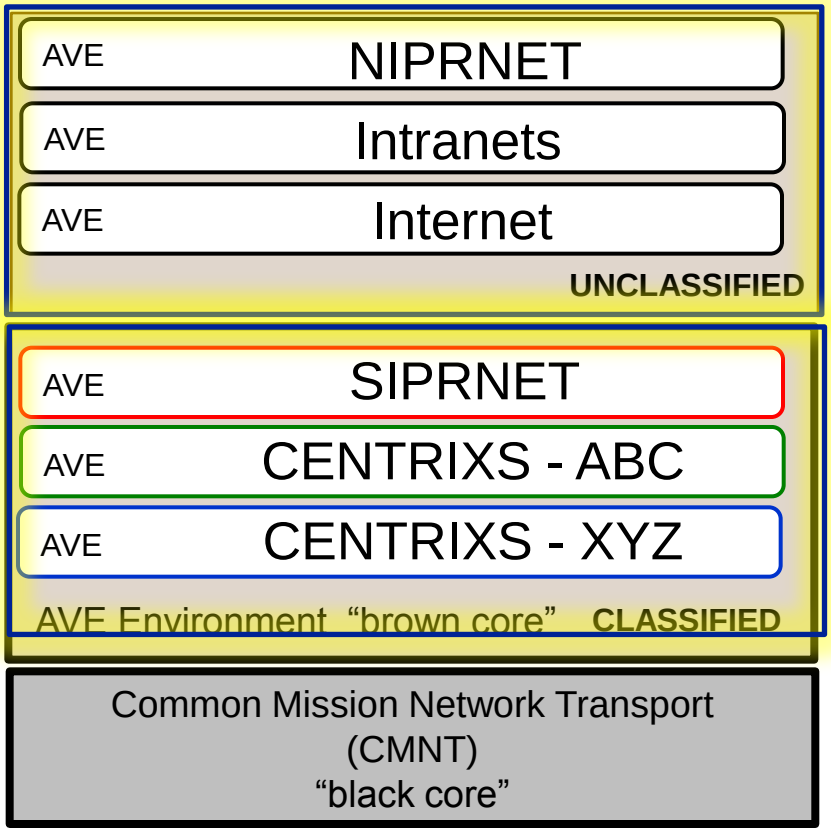
CMNT (black core) – Common Msn Net Trans.
- **MPLS – Multi-Protocol Layered Switching**
- **HAIPE – High Assurance IP Encryption**
- **IPv6**
- **Naming convention**
- **IP Addressing**
- **DNS**
- **DNN**

*AVEs drive the design requirements of the CMNT Provides **both** QOS and VPNs.*

Because it forms the foundation or core of the network and almost all traffic is encrypted it is referred to as a "black core"

Employing both rigid transport security (TRANSEC) ("black traffic") with enclave security ("brown traffic")

- Exposed data is "red"
- Encrypted data is "black"
- Traffic that is de-encrypted at the black core is "red" to the black core, but still "black" to the customer service point.
- Hence – the Agile Virtual Enclaves are a combination of red and black, or "brown."

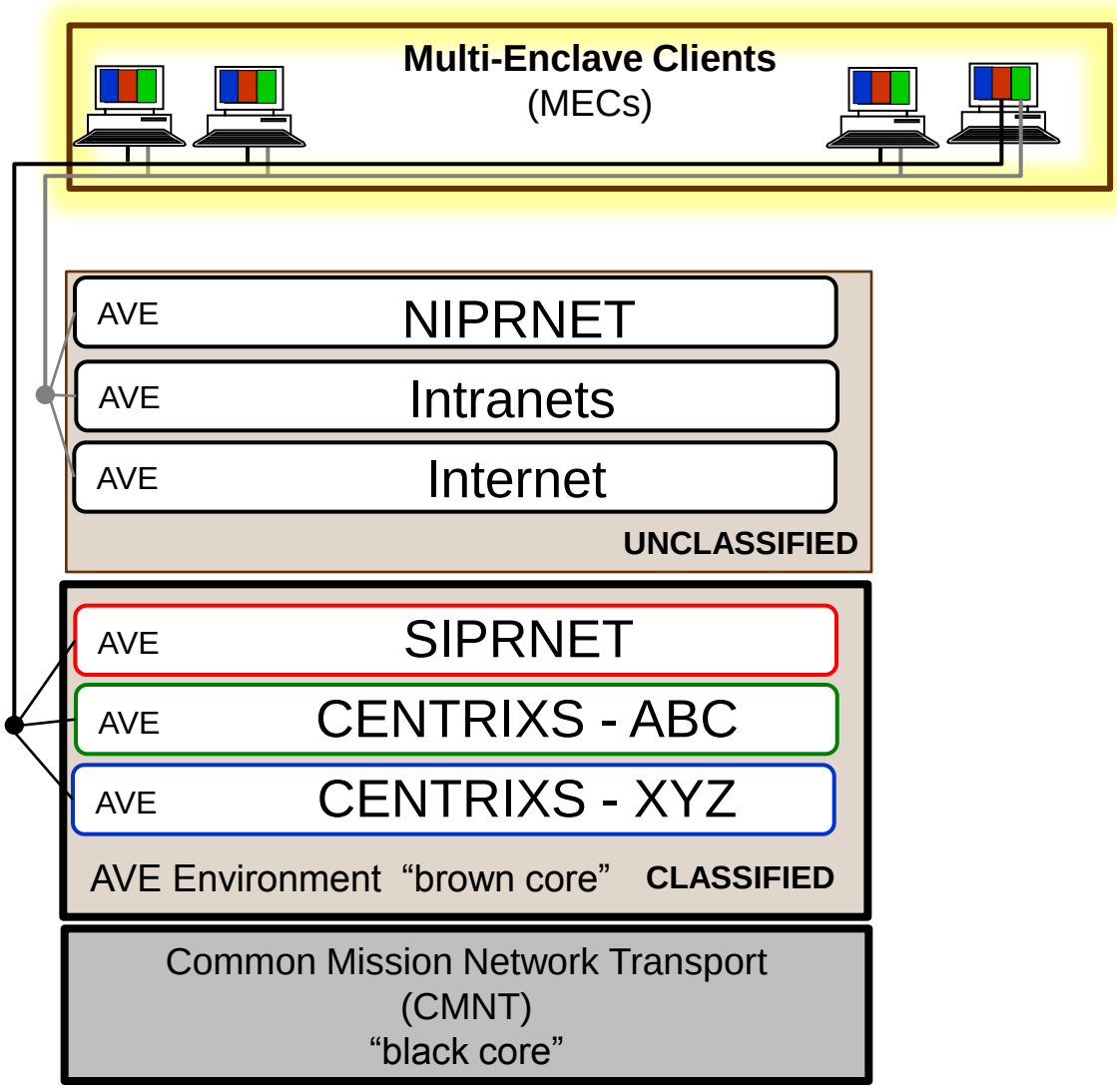


Associated Projects / Efforts

AVE (brown core)
- **IPSec – Internet Protocol Security**
- **IPv6 – Internet Protocol Version 6**
- **IKE – Internet Key Exchange**
- **Naming convention**
- **IP Addressing**
- **DCSP – Differential Code Service Point**
- **DNS – Domain Naming Service**
- **DNN – Domain Network Node**
- **VSE – Virtual Secure Enclaves**
- **PINS – Protected Inter-nodal Network**
- **ENIs - Enterprise Network Interface**
- **PNIs - Partner Network Interface**
- **ANIs – Application Network Interface**
- **CNIs – Client Network Interface**

CMNT (black core) – Common Msn Net Trans.
- **MPLS – Multi-Protocol Layered Switching**
- **HAIPE – High Assurance IP Encryption**
- **IPv6**
- **Naming convention**
- **IP Addressing**
- **DNS**
- **DNN**

Implement Multi-Enclave Clients (MECs) to access the multiple enclaves from a single Customer Service Point (CSP)



Associated Projects / Efforts

AVE (brown core)
- IPSec – Internet Protocol Security
- IPv6 – Internet Protocol Version 6
- IKE – Internet Key Exchange
- Naming convention
- IP Addressing
- DCSP – Differential Code Service Point
- DNS – Domain Naming Service
- DNN – Domain Network Node
- VSE – Virtual Secure Enclaves
- PINS – Protected Inter-nodal Network
- ENIs - Enterprise Network Interface
- PNIs - Partner Network Interface
- ANIs – Application Network Interface
- CNIs – Client Network Interface

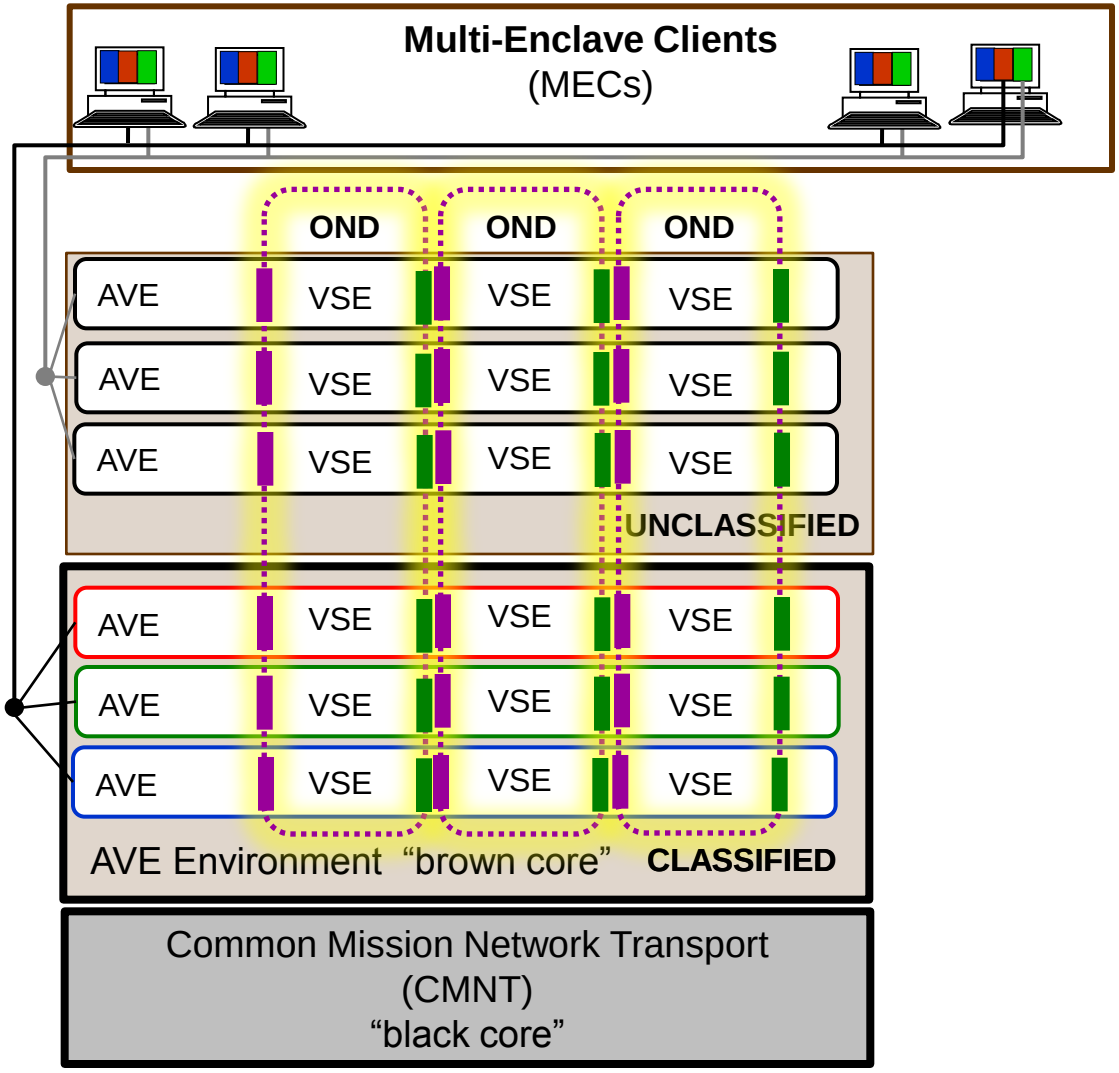
CMNT (black core) – Common Msn Net Transport
- MPLS – Multi-Protocol Layered Switching
- HAIPE – High Assurance IP Encryption
- IPv6
- Naming convention
- IP Addressing
- DNS
- DNN

MEC
- **NetTop – "Network on a Desktop"**

For organizations and commands that must operate in multiple security domains, MECs reduce workstation area, improve information access and improve maintainability and security through virtualization.

Implement Operational Network Domains (ONDs)

Intra-Enclave Controlled Interfaces To Contain Application and Configuration Risk within a Commander's Area of Responsibility



Associated Projects / Efforts

AVE (brown core)
- IPSec – Internet Protocol Security
- IPv6 – Internet Protocol Version 6
- IKE – Internet Key Exchange
- Naming convention
- IP Addressing
- DCSP – Differential Code Service Point
- DNS – Domain Naming Service
- **DNN – Domain Network Node**
- **VSE – Virtual Secure Enclaves**
- **PINS – Protected Inter-nodal Network**
- **ENIs - Enterprise Network Interface**
- **PNIs - Partner Network Interface**
- **ANIs – Application Network Interface**
- **CNIs – Client Network Interface**

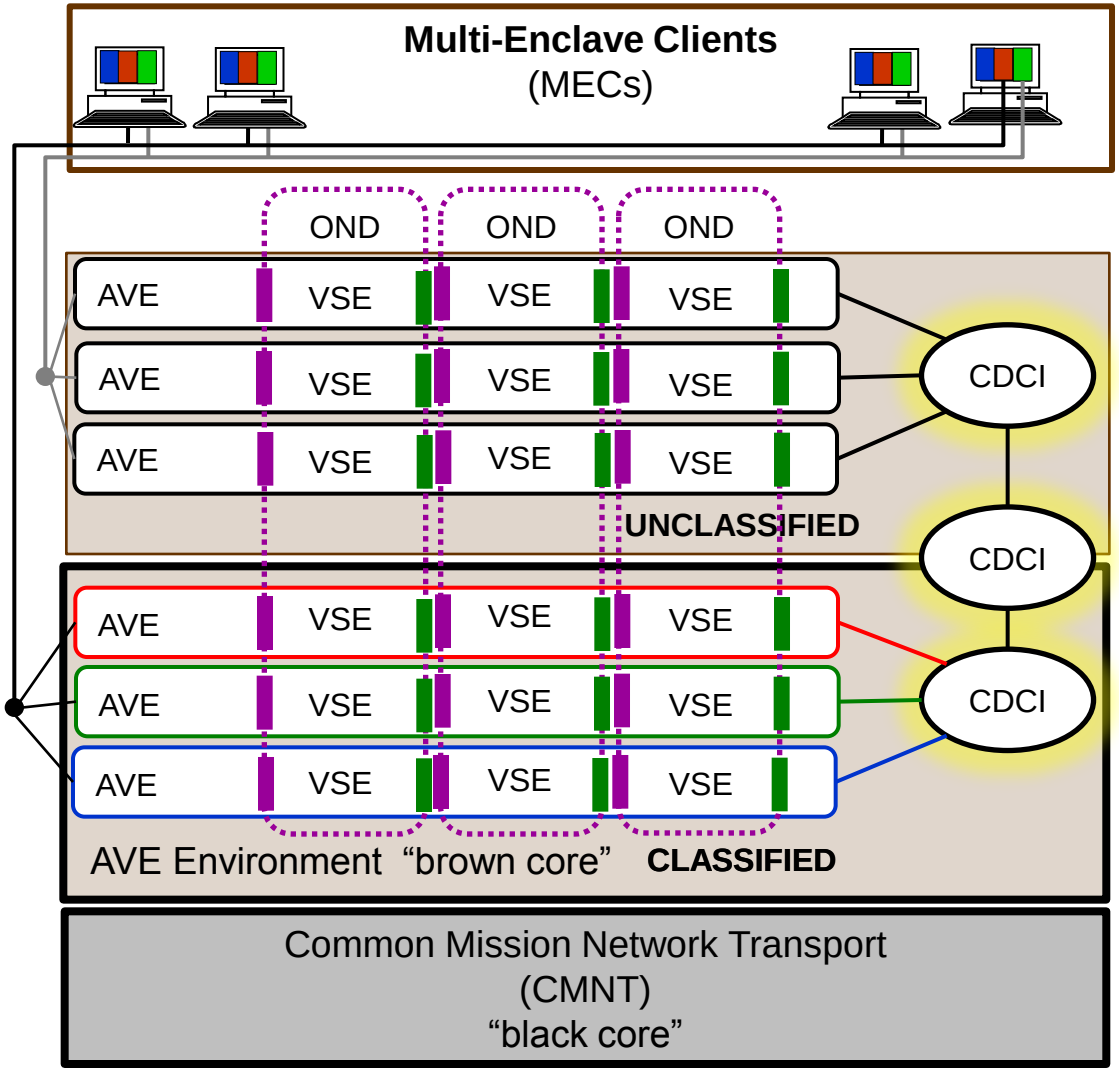
CMNT (black core) – Common Msn Net Transport
- MPLS – Multi-Protocol Layered Switching
- HAIPE – High Assurance IP Encryption
- IPv6
- Naming convention
- IP Addressing
- DNS
- DNN

MEC
- NetTop – "Network on a Desktop"

OND (Cyber JOA)
- **ENIs**
- **PNIs**
- **ANIs**
- **CNIs**

Enables "Cyber JOAs." Solves the "risk assumed by one is a risk assumed by all" dilemma. Allows commanders to take risk against their own mission in their own operational area – as is true for all the other domains.

Implement Cross-Domain Controlled Interfaces (CDCI) to safely move authorized information across security domains



Satisfies the CENTRIXS Cross Enclave Requirement (CCER). Currently done by Trusted Network Environment (TNE).

Associated Projects / Efforts

AVE (brown core)
- IPSec – Internet Protocol Security
- IPv6 – Internet Protocol Version 6
- IKE – Internet Key Exchange
- Naming convention
- IP Addressing
- DCSP – Differential Code Service Point
- DNS – Domain Naming Service
- DNN – Domain Network Node
- VSE – Virtual Secure Enclaves
- PINS – Protected Inter-nodal Network
- ENIs - Enterprise Network Interface
- PNIs - Partner Network Interface
- ANIs – Application Network Interface
- CNIs – Client Network Interface

CMNT (black core) – Common Msn Net Transport
- MPLS – Multi-Protocol Layered Switching
- HAIPE – High Assurance IP Encryption
- IPv6
- Naming convention
- IP Addressing
- DNS
- DNN

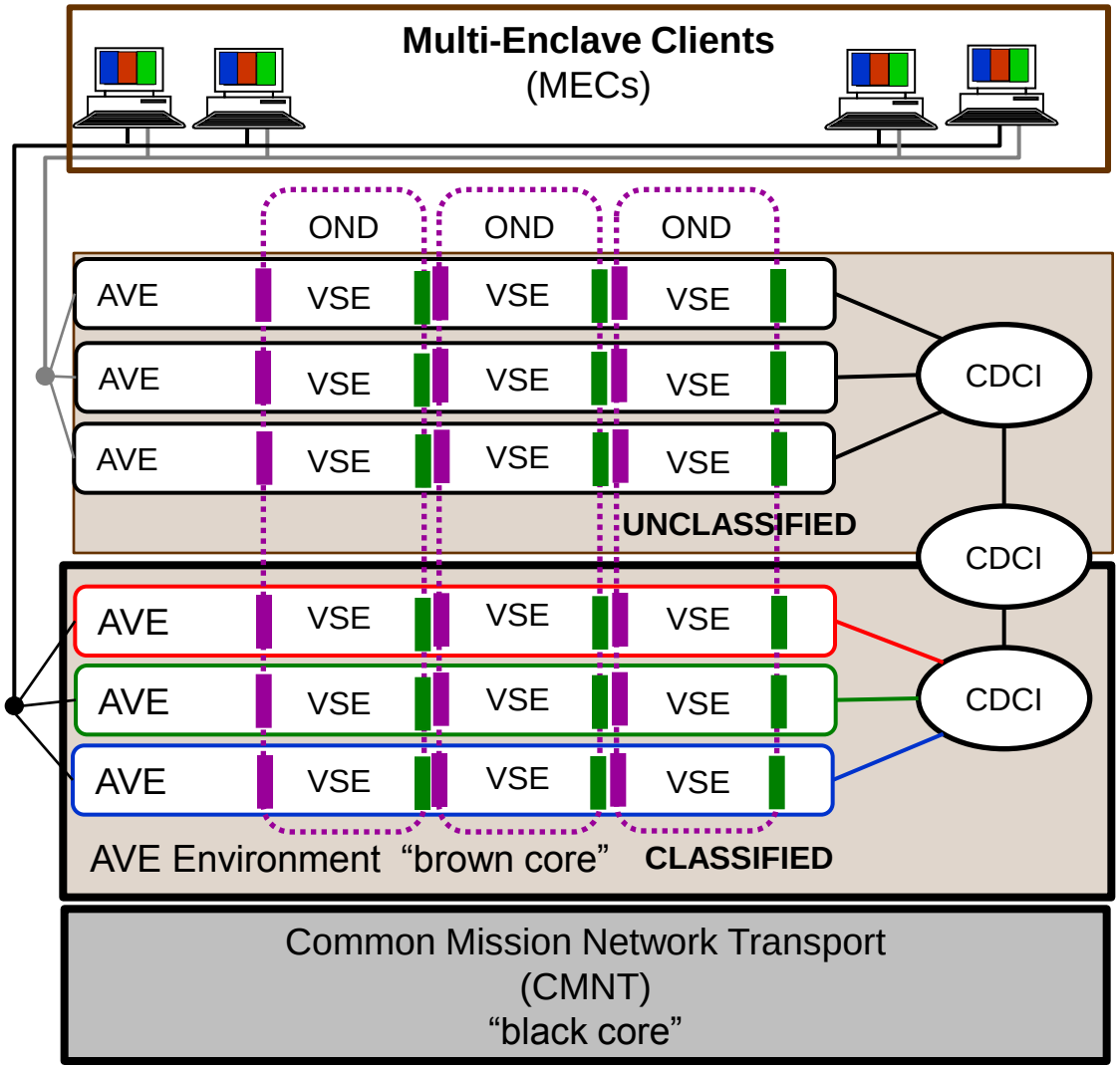
MEC
- NetTop – "Network on a Desktop"

OND (Cyber JOA)
- ENIs
- PNIs
- ANIs
- CNIs

CDCI – Cross-Domain Controlled Interface

CCER – CENTRIXS Cross Enclave Req't

GIG 3.0 Building Blocks – Phase 1 Summary



Associated Projects / Efforts

AVE (brown core)
- IPSec – Internet Protocol Security
- IPv6 – Internet Protocol Version 6
- IKE – Internet Key Exchange
- Naming convention
- IP Addressing
- DCSP – Differential Code Service Point
- DNS – Domain Naming Service
- DNN – Domain Network Node
- VSE – Virtual Secure Enclaves
- PINS – Protected Inter-nodal Network
- ENIs - Enterprise Network Interface
- PNIs - Partner Network Interface
- ANIs – Application Network Interface
- CNIs – Client Network Interface

CMNT (black core) – Common Msn Net Transport
- MPLS – Multi-Protocol Layered Switching
- HAIPE – High Assurance IP Encryption
- IPv6
- Naming convention
- IP Addressing
- DNS
- DNN

MEC
- NetTop – "Network on a Desktop"

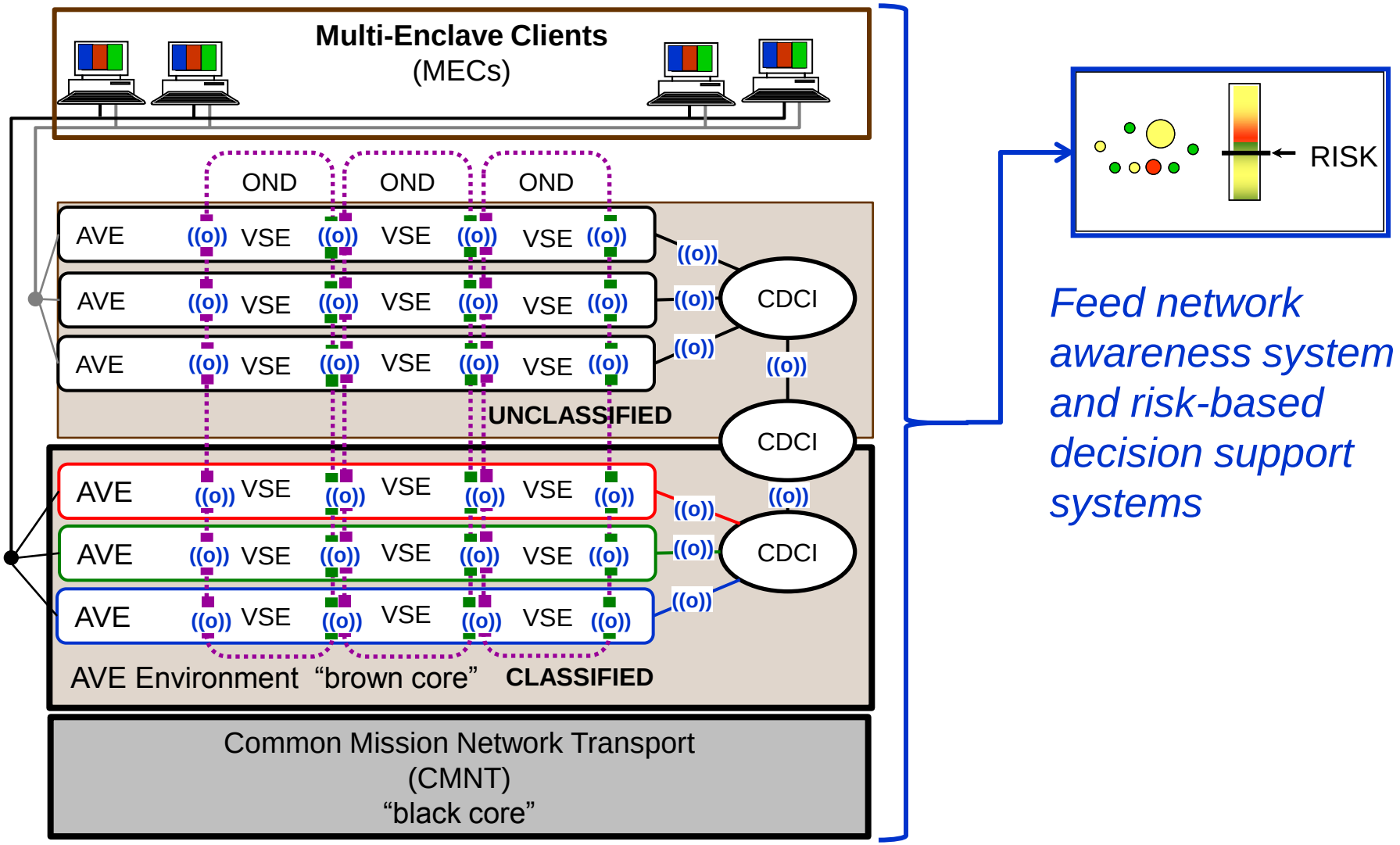
OND (Cyber JOA)
- ENIs
- PNIs
- ANIs
- CNIs

CDCI – Cross-Domain Controlled Interface
- CCER – CENTRIXS Cross Enclave Req't

Phase 2:

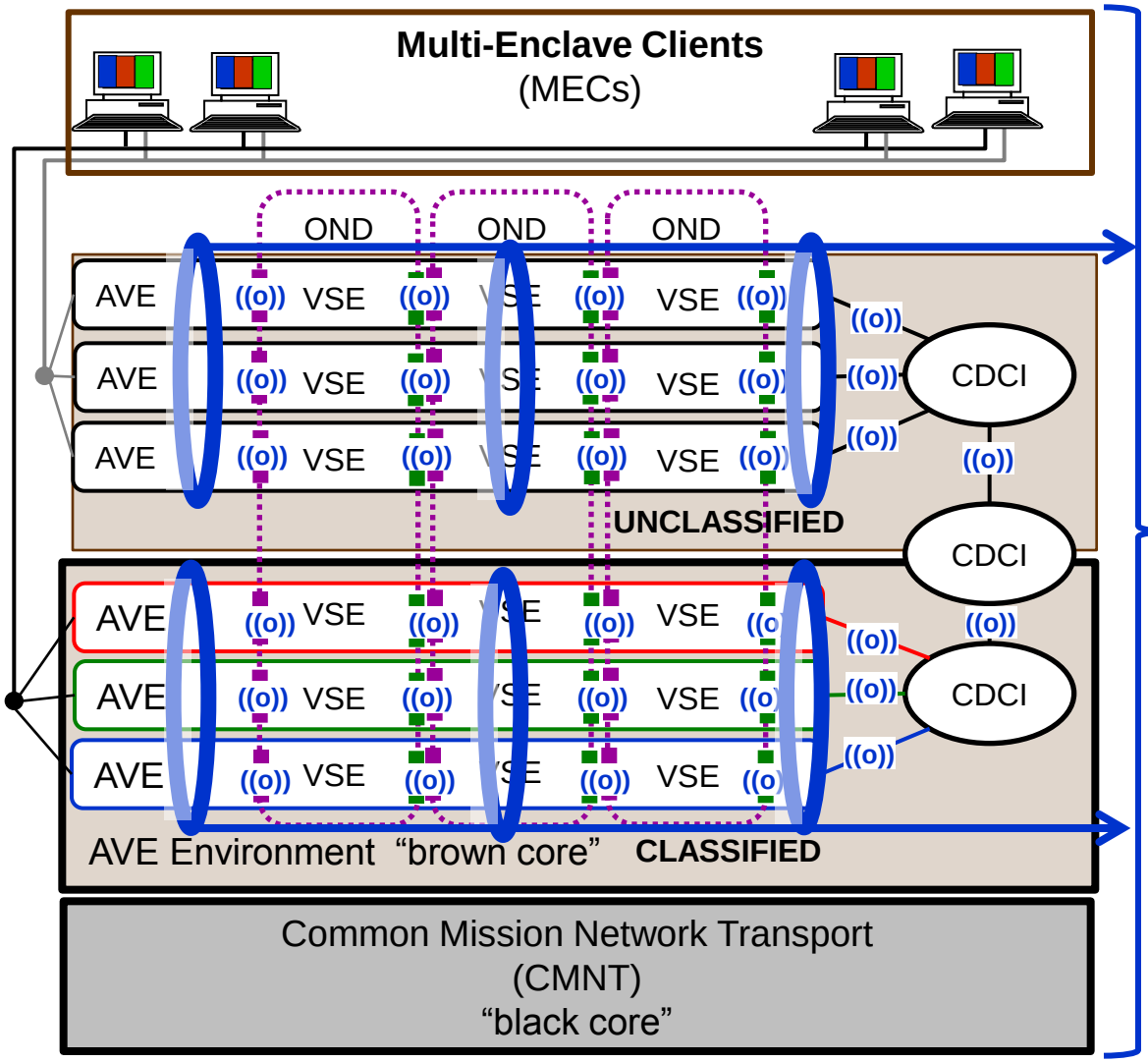
Control, Instrument and Conceal the Information Infrastructure

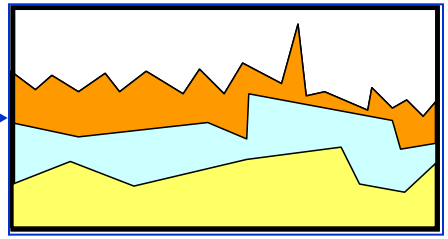
Instrument the network with sensors at strategic points



Feed network awareness system and risk-based decision support systems

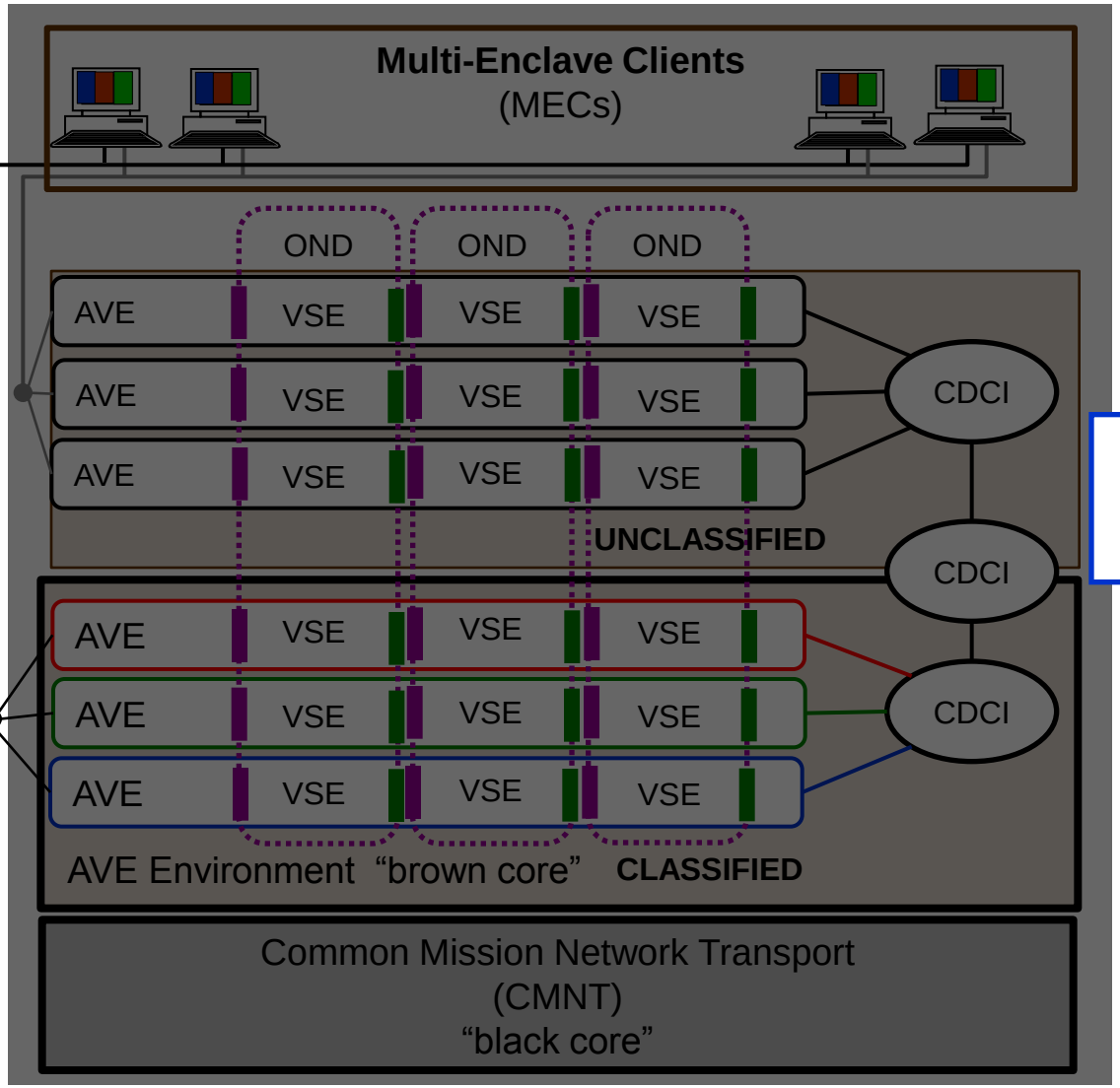
Provide network control and quality of service tools

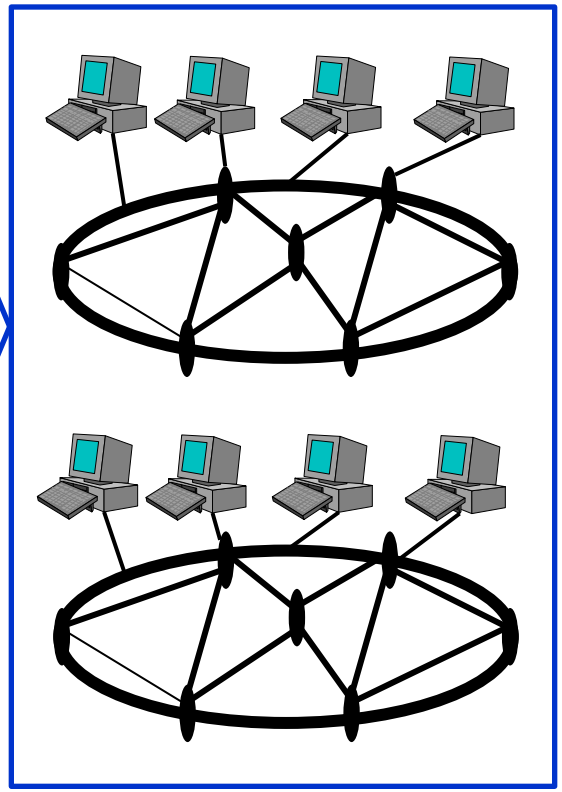




Monitor and control traffic precedence based on both Virtual Private Networking and Quality of Service

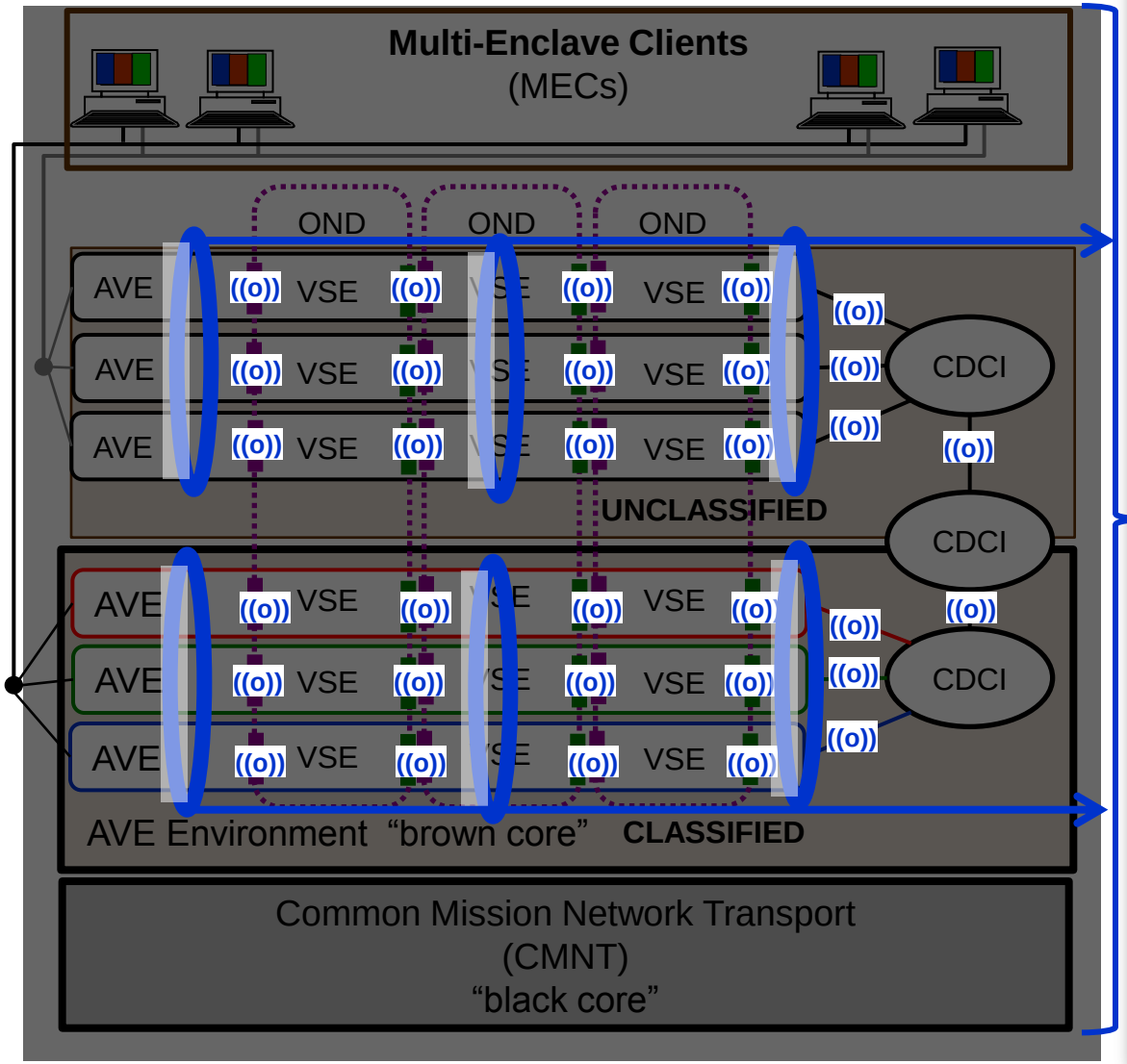
Develop concealment tools, techniques and procedures

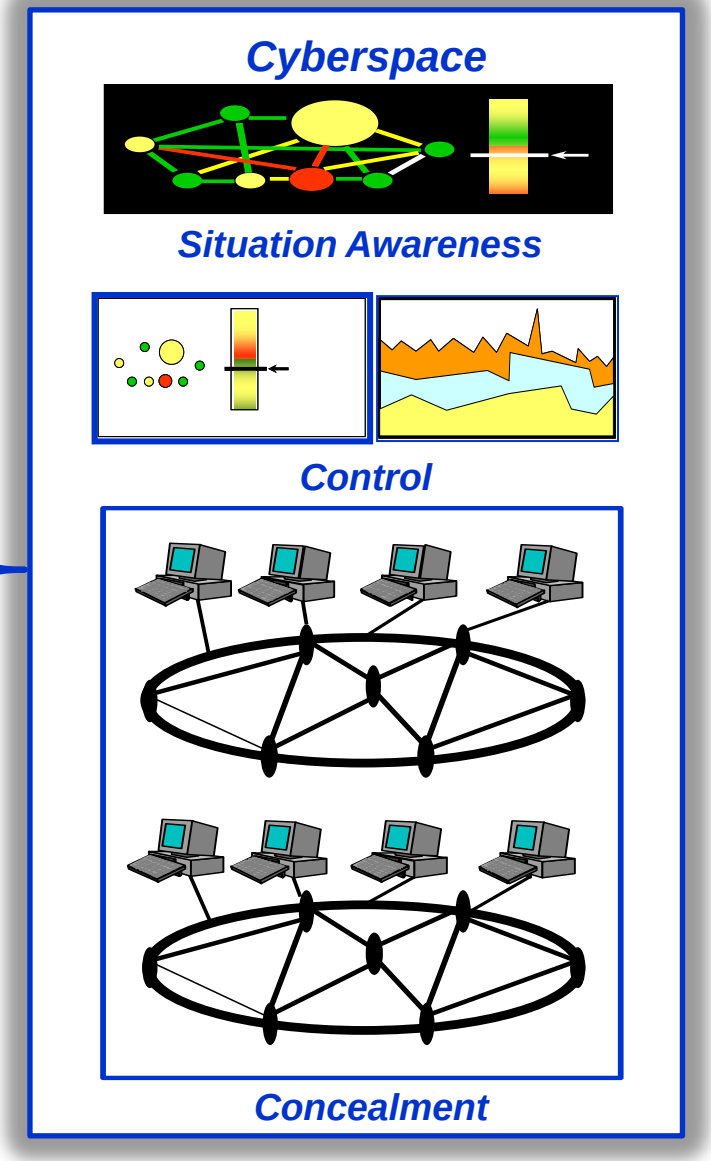




System visibility and access is controlled

GIG 3.0 Building Blocks – Phase 2 Summary





GIG 3.0
Design Approach

Questions / Discussion

GIG 3.0

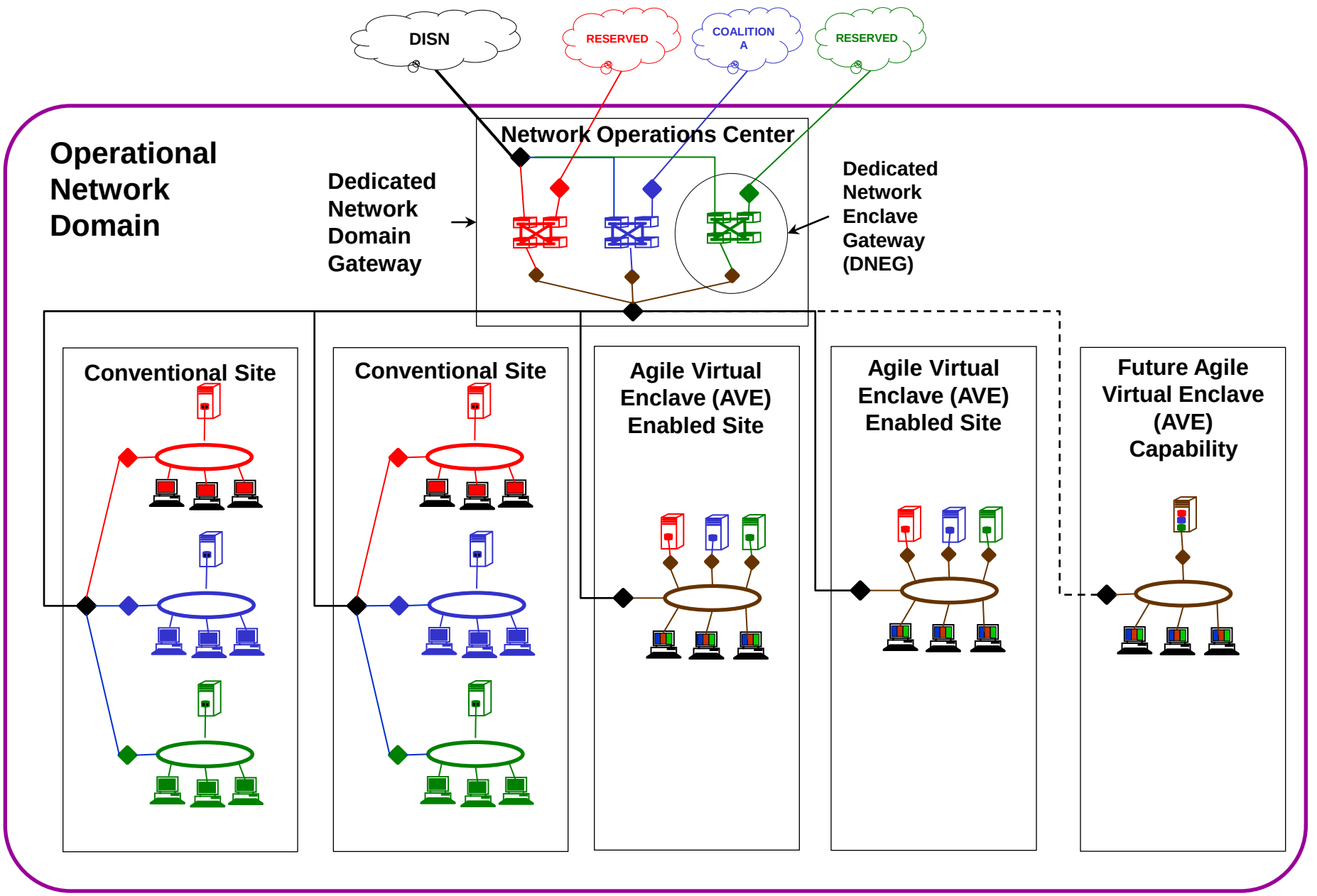
Governance

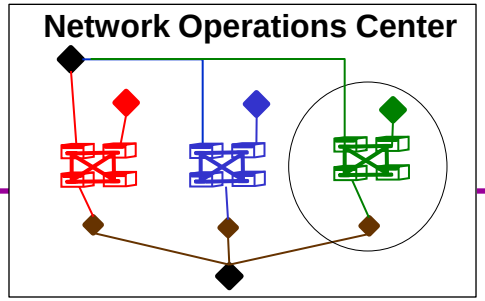
Mr. Randy Cieslak
CIO

U.S. Pacific Command
25 October 2010

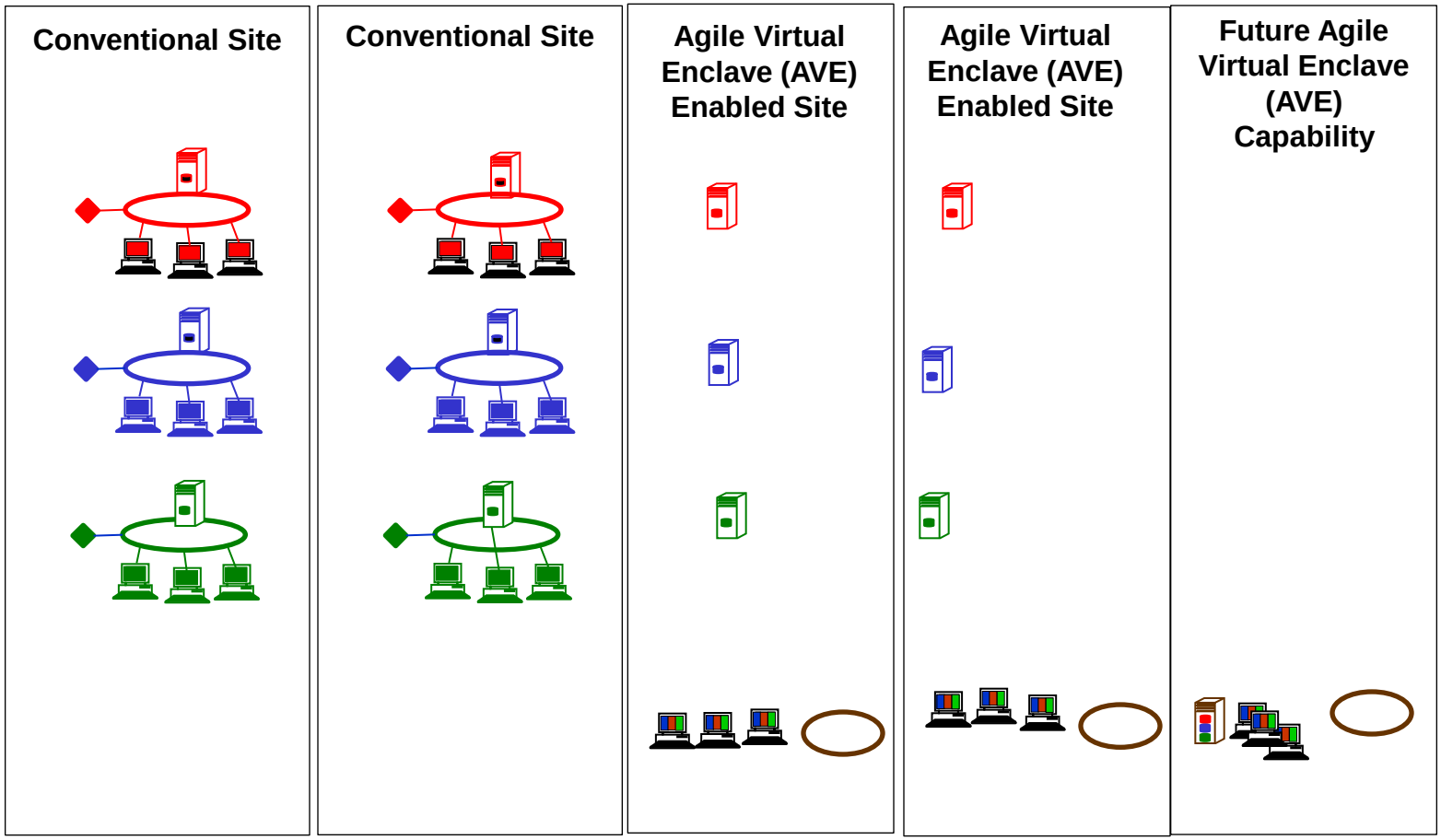
This brief is classified:

UNCLASSIFIED

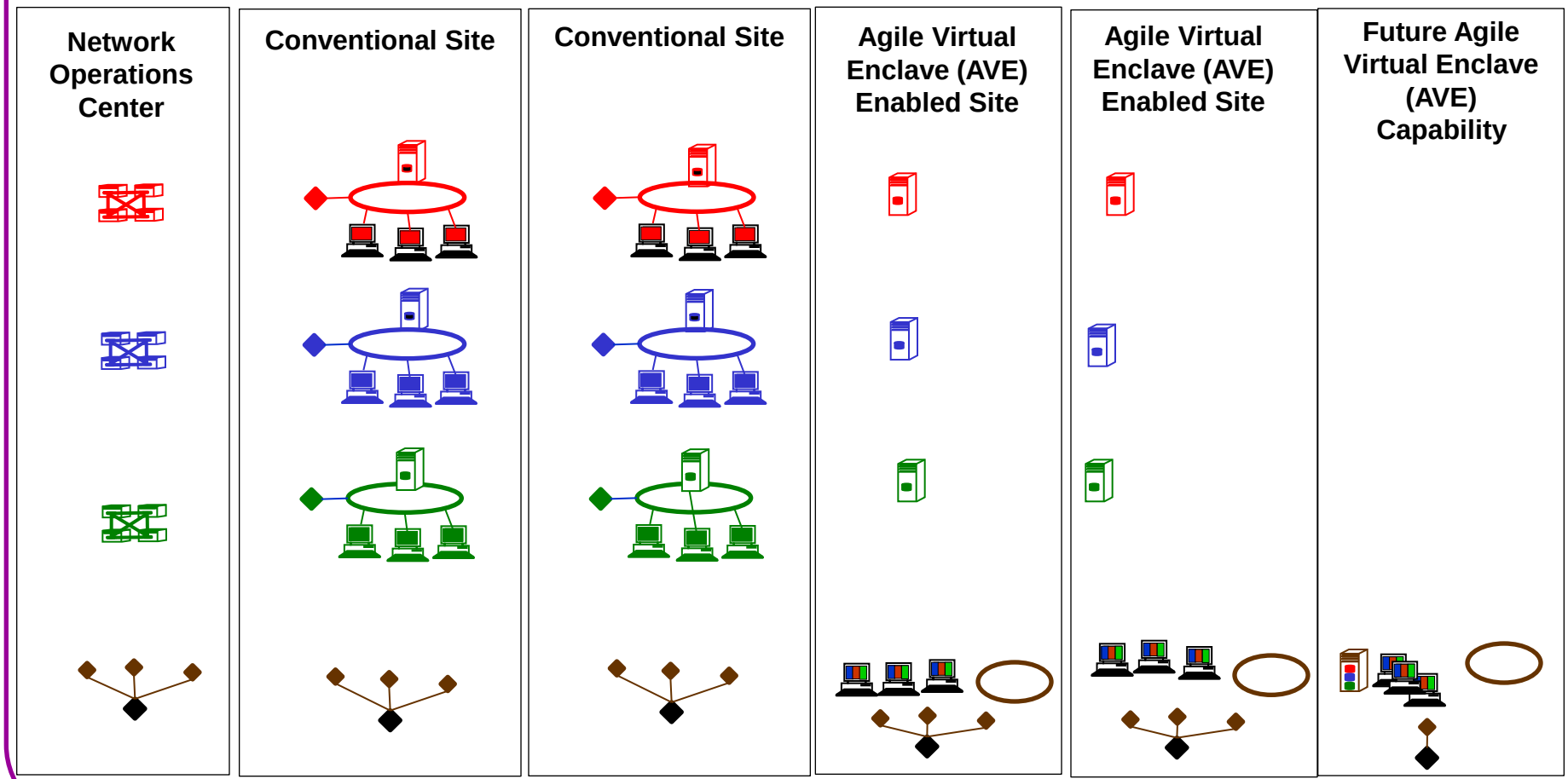




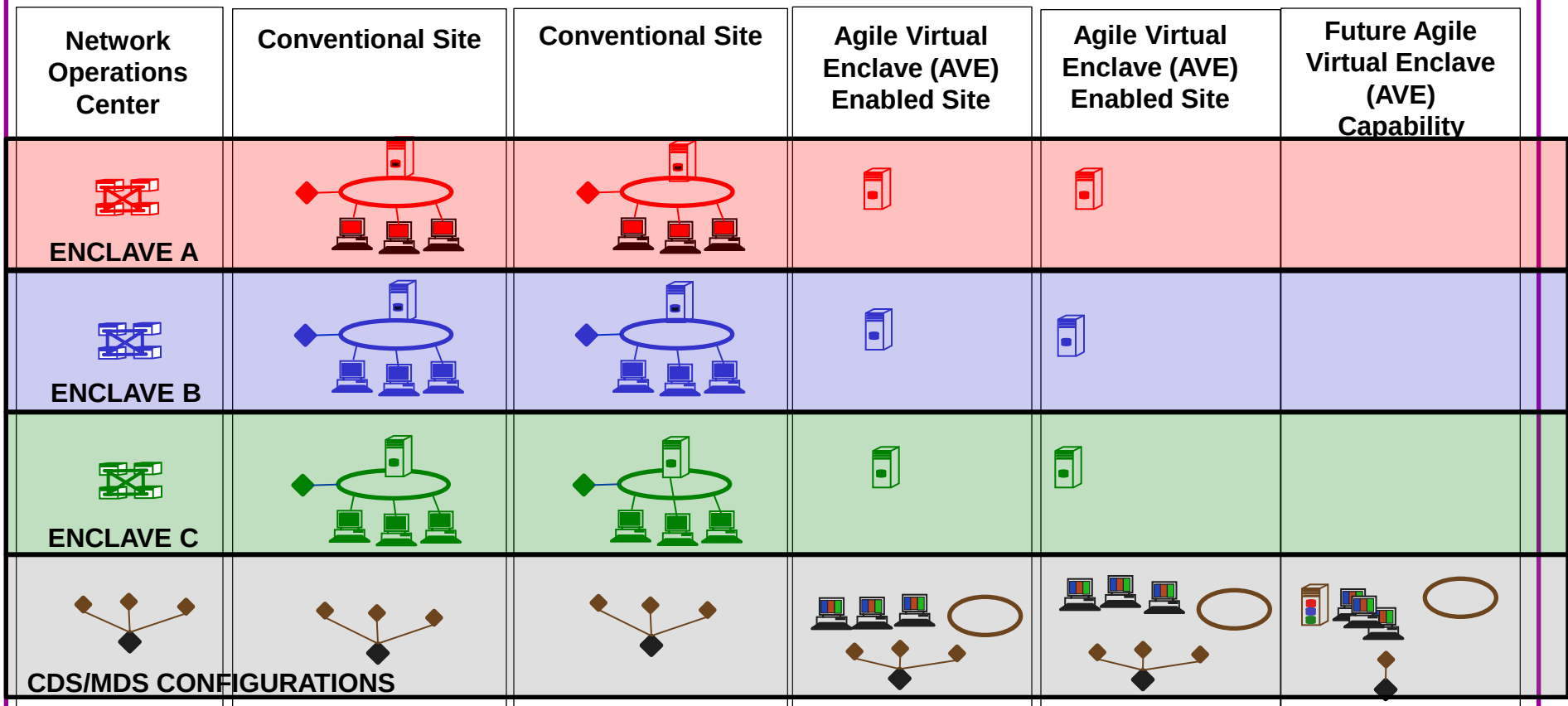
Operational Network Domain



Operational Network Domain



Operational Network Domain



CDS/MDS = Cross Domain System / Multi-Domain System