Global Information Grid End-to-End Systems Engineering Advisory Activity

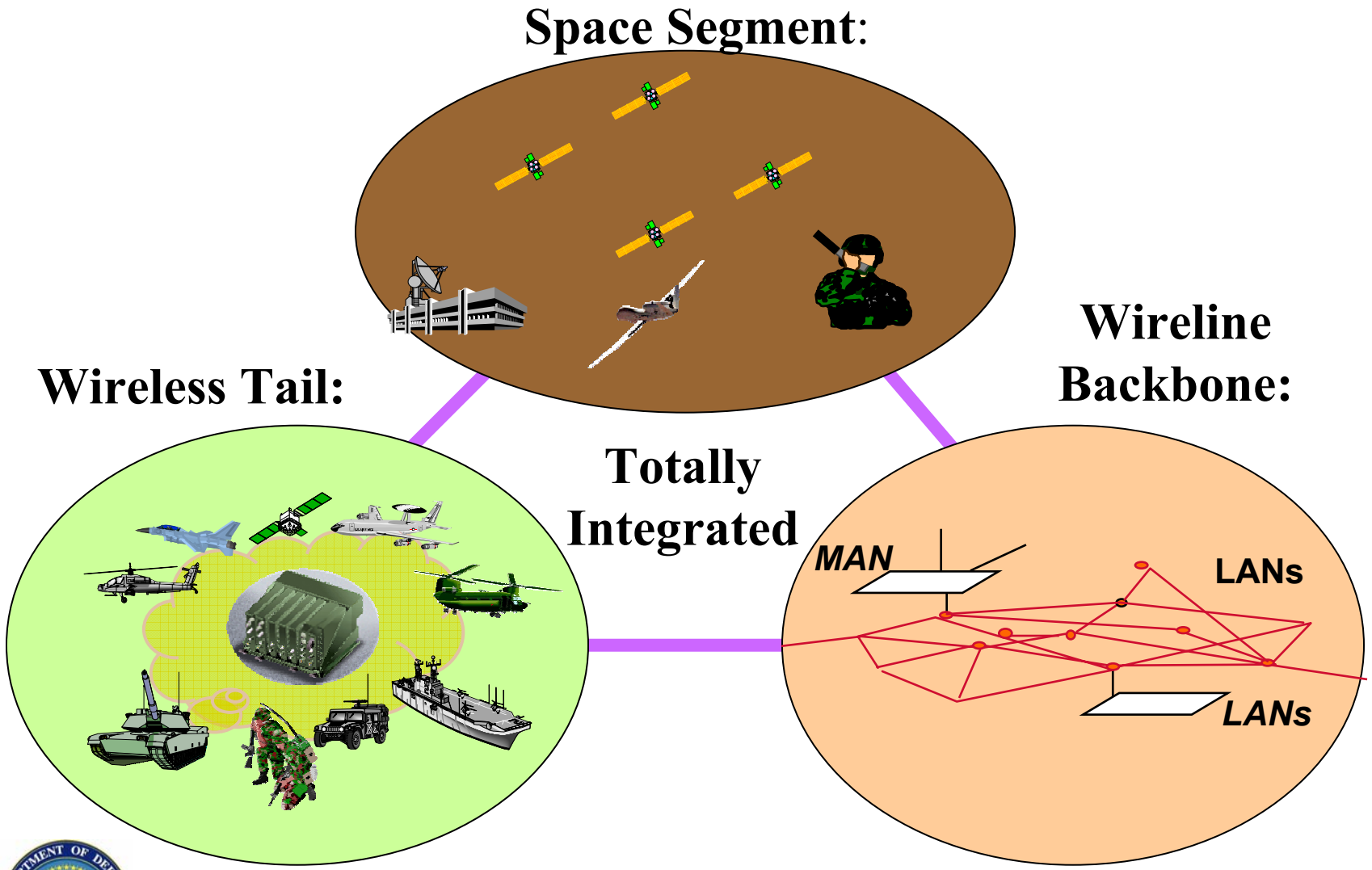
Tuesday, 16 November 2004
PEO/SYSCOM, Ft Belvoir, VA

Kenneth Schmidt
Communications Programs Directorate
Office of the Assistant Secretary of Defense
(Networks and Information Integration)

Overview

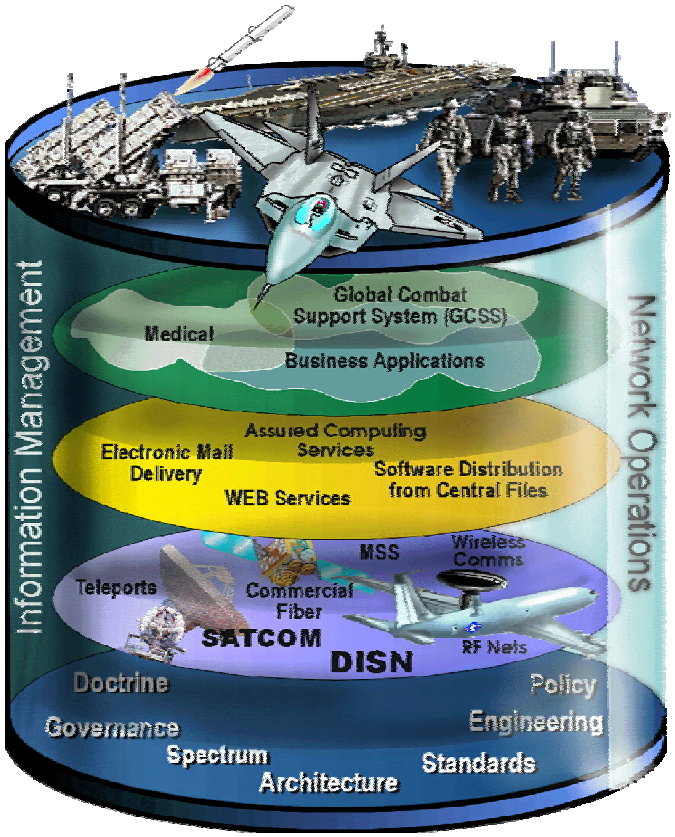
- The Global Information Grid (GIG)
- Scope of GIG End-to-End (E2E) Systems Engineering
- Building on Today's Internet
- Accomplishments
- Technical Issues
- Critical Challenges
- Summary

GIG Communications Components



Network Operations (NetOps)

- NetOps is the Operational Construct for operating and securing the GIG in support of Network Centric Operations and Warfare
- Goals of NetOps:
  - Assured System & Network Availability
  - Assured Information Delivery
  - Assured information Protection
- Supports all DoD Warfighting, Intelligence and Business operations



NetOps end–to–end across all GIG assets, in support of all Operational Environments

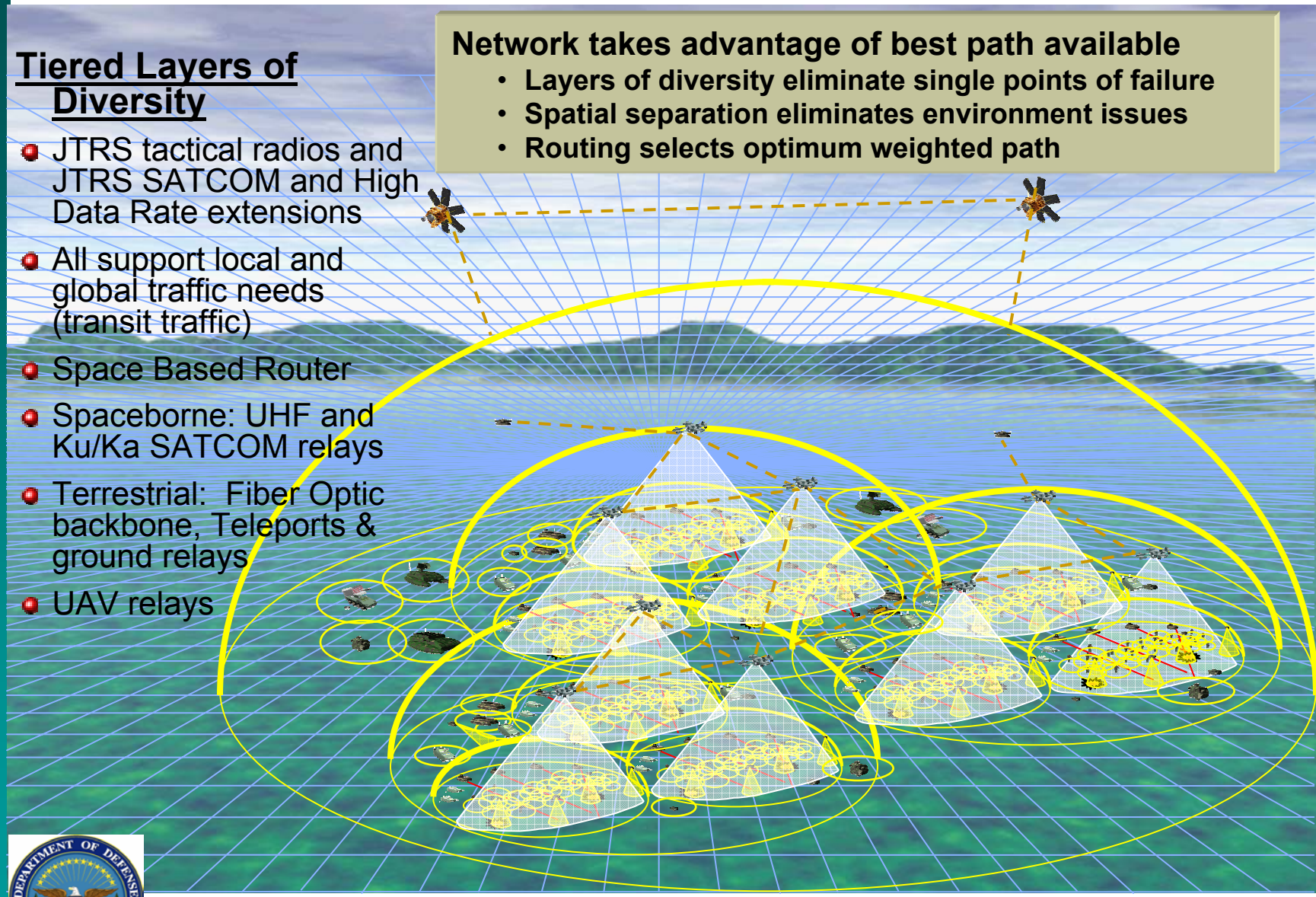
Network Communication Diversity

Network takes advantage of best path available

- **Layers of diversity eliminate single points of failure**
- **Spatial separation eliminates environment issues**
- **Routing selects optimum weighted path**

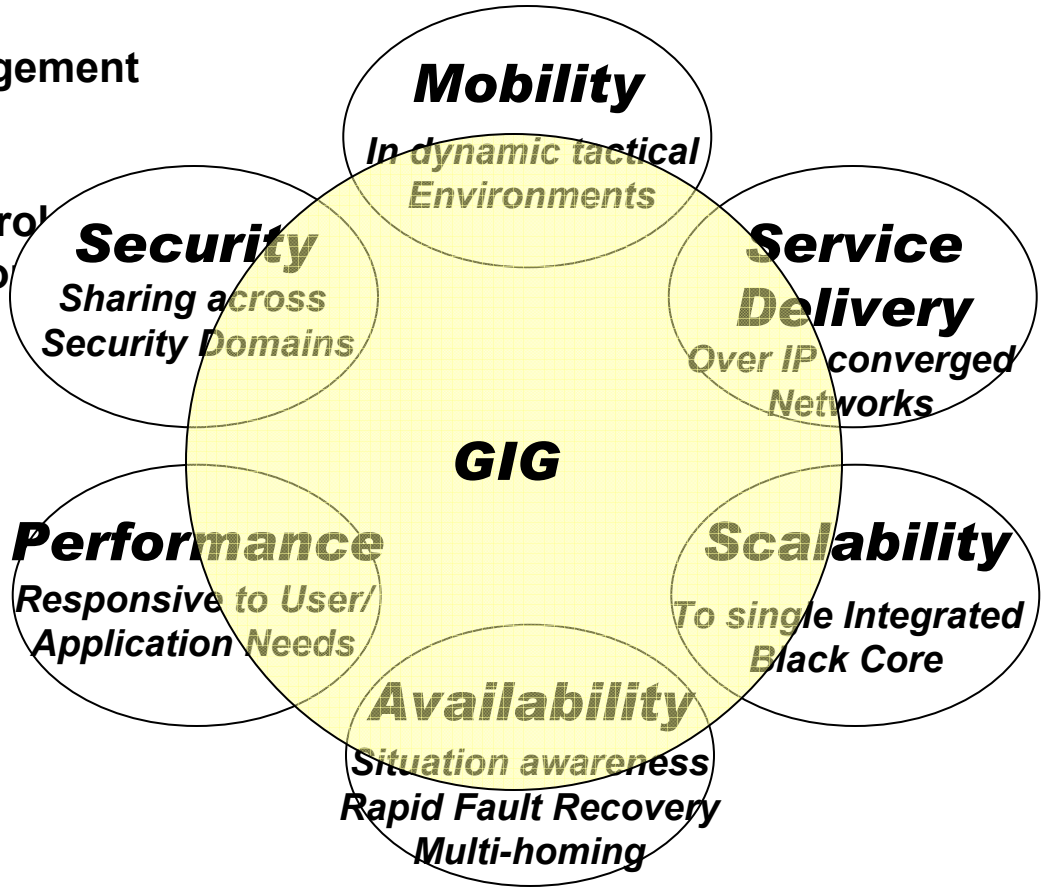
Tiered Layers of Diversity

- JTRS tactical radios and JTRS SATCOM and High Data Rate extensions
- All support local and global traffic needs (transit traffic)
- Space Based Router
- Spaceborne: UHF and Ku/Ka SATCOM relays
- Terrestrial: Fiber Optic backbone, Teleports & ground relays
- UAV relays



Leveraging Commercial Development and …

Intelligent Routing Protocols
Mobile Ad-Hoc Networking
Traffic Engineering extensions
Performance Enhancements
Policy Based Network Management
QoS Mechanisms
Traffic policing and shaping
Connection Admission Control
Key Management/ Distribution
Computer Network Defense
Intrusion Detection Systems
Automation
Multi-casting
etc. …..



… Adapting to DoD Needs as necessary

GIG E2E Systems Engineering Organization

(10/14/04)

ASD(NII) / DoD CIO

Senior GIG Systems Engineer (NII)
Mr. Mike Kern (NII)

Chair: Senior GIG Systems Engineer (NII)

GIG Senior Systems Engineering Board

Basil Decina (NRL)
GIG E2E Evaluation Facilities (NRL)

Members: Senior Sys Engineering Rep from: Army, Navy, AF, USMC, AT&L, USD(I), DOT&E, Joint Staff J-6, STRATCOM, JFCOM, IC-CIO, DISA, MDA, NSA GIG IA SPO, TCO, TCM MJPO, GIG-BE SPO, JTRS JPO, NCES SPO, GIG Architect, & E2E Evaluation Facilities (NRL)

Focus Areas Working Groups

GIG End-to-End Systems Engineering Working Group

WG POC: Brian Robinson (NII) ("acting")

Brian Robinson (NII)	Dan Risacher (NII)	TBD	Larry Bowman (DISA	Doug Marquis (Air Force)	Doug Marquis (AF) LTC Schiller (J-6)	Chris Kubic (NSA)
Transport	Enterprise Services	Apps & Data	QoS	Net Mgt	NETOPS	Information Assurance

…for each area

"Sub-Working Groups" & Tiger Teams	Julie Tarr (NRL)	Heather Schoenborn (NII)	J-6 / Fred Kopf (DISA)	TBD	Rich Williams (DISA)	Sean O'Keeffe (NSA)
	GIG Routing	Spectrum	Mission Threads	Standards	IP Convergence	HAIPE "Tiger Team"

Matrix organization brings best talent to functionally support E2E Systems Engineering Activity

Strength's of Today's 'Internet'

- Very simple and effective forwarding plane
- Distributed route computation and execution
- Intelligence at the edge/hosts
- Highly scalable
- Common Network and transport layers
- Huge success as a productivity enhancement tool using information collection, transfer, and retrieval

Weaknesses of Today's 'Internet'

- No application awareness in the core
- No short and long term mission awareness in the core
- No comprehensive situation awareness about network, computing infrastructure, and services
- Hard to isolate failures, attacks, compromises
- Hard to guarantee QoS (broad sense including delay, jitter,losses, connection set up time and success rates, availability, security, ..)
- Single route to destination from any node, cannot find alternate routes, cannot load balance
  - Severely constrained ability to exploit multi-homing
  - Limited ability to choose routes based on route capabilities and application needs
- Easier DDoS attacks
- No Traffic Engineering, QoS, or Security policy in routing
- Hard to manage fast mobility

Implications

- 'Internet' applications somewhat limited due to weaknesses
- Extensive manual effort and over provisioning to overcome some of these weaknesses in some situations
- Operators, vendors, and researchers/technologists have recognized the need to enhance the architecture to overcome these weaknesses without giving up the simplicity and scalability of the forwarding plane
  - Initial effort in *data/user* and *control* planes
    - Differential QoS capabilities
    - Multi-Protocol Label Switching (MPLS)
    - Traffic Engineering capabilities in routing protocols, i.e. MPLS
  - Operators/carriers creating capabilities in *control* and *management* planes, and achieving E2E 'QoS' capabilities via inter-operator negotiations

---

- Need additional Research/ Standards in Control, Management and Knowledge Planes
  - BGP enhancements
  - Integrated situation awareness
  - Additional prediction and detection tools
  - Design of a Knowledge Plane (KP)

Bottom Line ....

- **Internet's success is also its weakness**
  - **Simple, transparent, and application independent core with intelligent edges/hosts**
    - **Allows easy scalability and faster introduction of new services and applications**
    - **Hard to respond quickly to mission needs, hard to figure out what has gone wrong, hard to control attacks systematically, hard to route based on application needs and route capabilities, …**
- **Telephone network (its control and management planes, in particular) is intelligent at the core and is very aware of applications**
  - **Provides E2E QoS, manageability, access controls, etc. However, it is not a multi-service network. We can learn a lot from PSTN and adapt best ideas to add to the Internet strengths**
- **Knowledge Plane may be a way to bring in application awareness, E2E network situation awareness, intelligent routing, and intelligent security in Internet without complicating the simple and effective forwarding plane.**

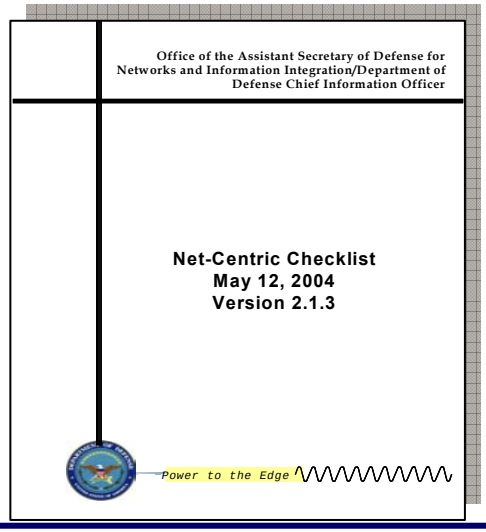
Helping the GIG Come Together

OSD Oversight For Critical Cross-Organization Programs

- Develop the detailed technical Architectures
- Recommend incremental deployments in GIG capability
- Maintain the architectural vision and monitor the implementation of the resulting system(s)
- Perform comprehensive Risk Management across the multiple GIG domains
- Ensure approved standards, protocols, and processes implemented and tested across programs
  - DoD IT Standards Registry
  - Global Information Grid Architecture
- End-to-end Systems Engineering Oversight and Recommendations
  - Each program will have its own system engineering activities
  - Programs will work with OSD to ensure standards and protocols are implemented from end-to-end

Key to GIG E2E SE: Net-Centric Assessment

- Net Centric Checklist as starting point to collect information
- Program office provides response and discusses issues with assessment team



- **Transport Tenets — Transport Team**
  - IPv6
  - Packet Switched infrastructure
  - Layering, Modularity
  - Transport Goal
  - Network Connectivity
  - Concurrent Transport of Information Flows
  - Differentiated Management of Quality of Service
  - Inter Network Connectivity
  - DoD IT Standards Registry (DISR)
  - Joint Net Centric Capabilities
  - Opertion/Management of Transport and Services

- **Data Tenets — Data/Apps Team**
  - Make Data Visible
  - Make Data Understandable
  - Make Data Accessible
  - Make Data Trustable
  - Make Data Interoperable
  - Be Responsive to User Needs

- **Service Tenets — Enterprise Services Team**
  - Service-Oriented Architecture
  - Open Architecture
  - Scalability
  - Availability
  - Accommodate Heterogeneity
  - Decentralized O&M
  - Enterprise Service Management

- **Information Assurance — IA Team**
  - Identify Management and Authentication
  - Mediate Security Assertions
  - Cross Security Domains Exchange
  - Manage Identity and Privileges
  - Encryption and HAIPE
  - Wireless Technologies

Accomplishments 2003-2004

- Working Group operating since Jan 2003
- First Meeting of Senior Systems Engineering Board, April 2004
- Charter signed (17 organizations) August 2004
- Delivered GIG Information Assurance architecture guidance, June 2004
- Coordinated user requirements in IPsec device specification
- Proposed transition plan to a single Black Core architecture
- GIG-EF build and initial experimentation (Sept 2004)
- NetOps/Net Mgt: Initial DoD Architecture Framework Products: Architecture, AV-1, OV-1, SV-5, SV-6
- Completed E2E threads interoperability analysis Aug 2004
- Coordinating the IP convergence for Defense Information Systems Network Services and JTRS Network services
- Leading bi-weekly engineering meetings between representatives from Army, Navy, AF, USMC, AT&L, USD(I), DOT&E, Joint Staff J-6, STRATCOM, JFCOM, IC, DISA, NSA GIG IA SPO, TCO, TSAT MJPO, GIG-BE SPO, JTRS JPO, NCES SPO, GIG Architect, and GIG EF (NRL)

Technical Issues

- "Black Core" Network Operations
  - Interconnecting segments of Core Network (GIG-BE, TSAT, etc.)
  - Facilitate multiple routes destination from any node (multi-homing)
  - Including Traffic Engineering, QoS, and security policy in Routing
  - Computer Network Defense & Traffic Limiting
- Comprehensive situation awareness about network, computing infrastructure, and services
- Guaranteeing QoS (in a broad sense including delay, jitter,losses, connection set up time and success rates, availability, and security)
- Defining the interface between Service networks and Core networks
- GIG-issued Identity to all Users (Human, Device, Services)
- Label All Information
- Detect and adaptively respond to system and network degradations, outages, and changes in operational priorities

Technical Issues: Continued

- Global Digital Policy Driving All Actions
- GIG Key Management
- Performance Enhancing Proxy (PEP) for SATCOM Networks
- Scalable Dynamic Discovery
- IPv6 Addressing Plan
- IPv4 to IPv6 Migration
- Multicast Operation
- Converge on Voice over IP solution (multi-vendor compatible)
- Extending Network Enabled Capabilities to NATO

Critical Challenges

- **Deliver Quality of Service in the GIG**
- **Promote Knowledge Plane concepts as a way to bring in application awareness, E2E network situation awareness, intelligent routing, and intelligent security in Internet without complicating the simple and effective forwarding plane.**
- **Extend JTRS Networking Services to SATCOM Terminals and High Capacity 'Networked' Data Links**
- **Extend Network Enabled Capabilities to Coalition Partners**

Quality of Service

- **DoD is moving towards IP to take advantage of it's benefits**
  - Interoperability
  - Flexibility in using network resources
  - Standards-based
- **However, IP networks traditionally support 'transport' for applications requiring best effort service**
  - Applications leading to popularity of Internet (e.g., email, www) resilient to packet delay, jitter, and loss
    - Do not demand stringent level of service from the network
- **Real-time and mission critical traffic will need better than traditional best effort service (i.e., Quality of Service) but still retain the benefits of IP**
- **Quality of Service (QoS) refers to the capability to provide differentiated/guaranteed service to selected network traffic**
  - Services defined in terms of bandwidth, jitter, latency (required by some real-time/interactive traffic), and loss characteristics
  - QoS is an end-to-end function

QoS Mechanisms and GIG Networks

- Determine mechanisms needed in Control and Data planes
  - Identify how MLPP requirements and real-time/inelastic traffic requirements can be satisfied
- Identify GIG network types to determine applicable mechanisms
  - "One size does not fit all"
  - By understanding network types, can begin to define how different types of networks can interface to offer consistent QoS E2E
- Document management plane needs as it relates to Service Level Capabilities (SLCs) and QoS provisioning
  - Coordinate with Network Management and Control (NeMaC)
- Understand the Black Core boundary as it relates to QoS signaling and packet markings
- Consider implications of instituting E2E QoS signaling on edge devices

JTRS Clusters and Extensions beyond 2 GHz

JTRS Cluster 1-Software Defined Radio

- JTRS 4 channel LRU
  - Network Interface Unit (NIU)
  - Universal Transceiver (UT)
  - Power Amplifier (PA)

JTRS Cluster 1 LRU provides 4 channels of communications capability

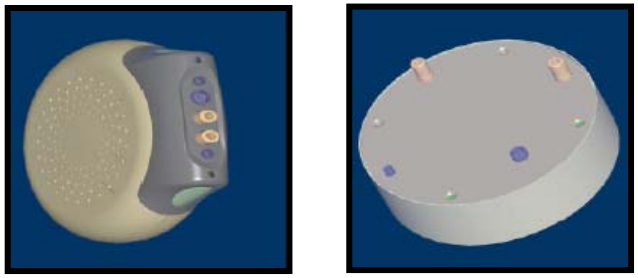
JTRS-Network Data Link – Software Defined Radio

- **NDL Hardware**
  - Extension of JTRS cluster 1 HW
  - Adds broadband transceiver and RF group
- **NDL Waveform**
  - JTRS JPO responsible for waveform development
  - Competitive procurement

NDL occupies 1 or 2 Universal Transceiver (UT) slot(s)

JTRS Cluster 5 - Software Defined Radio

- **JTRS small form factor (SFF)**
  - 11 small form factor configurations
  - 4 handheld configurations
  - 1 manpack configuration



SLICE conceptual drawing

JTRS SCA Compliant Waveforms

- Wideband Networking Waveform (WNW)
- Soldier Radio Waveform (SRW)
- Network Data Link (NDL)
- 23 current force waveforms

Extending Network Enabled Capabilities to NATO

QUESTIONS?