# Flow Based Control Plane Situational Awareness

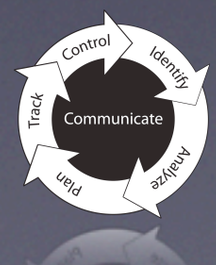
FloCon 2009

Scottsdale, Az

Carter Bullard
QoSient, LLC

carter@qosient.com



# Who Am I?

- Carter Bullard carter@qosient.com
  - Research and Development
    - Naval Research Laboratory (NRL), GIG-EF, JCTD-LD
    - DISA, NSA network performance/security research
  - Developed Argus http://qosient.com/argus
- FBI/CALEA Data Wire-Tapping Working Group
- Security Product Manager – FORE Systems
- QoS Network Management - NORTEL
- CMU/SEI CERT
  - Network Security Incident Coordinator
  - NAP Site Security Policy Development
- Standards Efforts
  - Editor of ATM Forum Security Signaling Standards
  - IETF Security Working Group (in the good ole days)

The US DoD Global Information Grid (GIG) is a massive telecommunication infrastructure built on a comprehensive approach to Service Oriented Network Design and Function.

Its basic goal is to combine the information resources of all branches into a secured infrastructure, linking desktops, supercomputers, satellites and more to provide support for intelligences, logistics and war-fighting.


The GIG is the net-centric warfare Center of Gravity ... it must be protected.

Large Data JCTD

# GIG Information Assurance (IA)

- Assured Information Sharing
  - Information and services must be known to be authentic.
- Highly Available Enterprise
  - Services must be operational when needed.
- Cyber-Situational Awareness and Network Defense (CND)
  - Near real-time awareness of threats, status, and performance, with awareness of external attacks and insider abuse/misuse.
- Assured Enterprise Management and Control
  - The GIG must operate as intended, with management, control and information protected with a secure infrastructure in place.

# Situational Awareness

## Our working definition (Endsley model)

- The perception of elements in the environment
- Within a volume of time and space
- The comprehension of their meaning
- The projection of their status in the near future

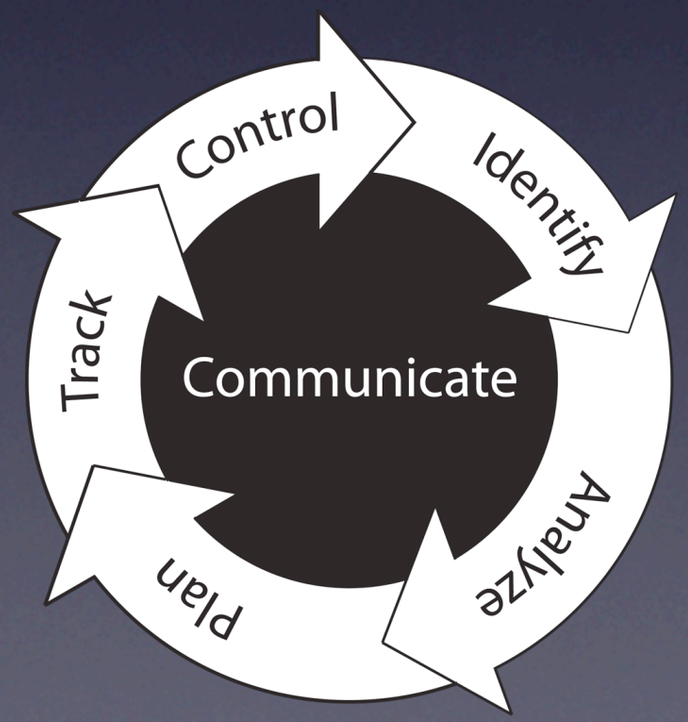
Endsley, M. R. (1995b). Toward a theory of situation awareness in dynamic systems. Human Factors 37(1), 32-64.

## Level 1 SA - Perception

- The fundamental issue is quality of information
- The principal goal is to enable Level 2 SA - Comprehension.
- Many SA systems are unfortunately designed around existing data.
- SA system design also must consider data combination, storage, retention and access.

# Control Plane Awareness

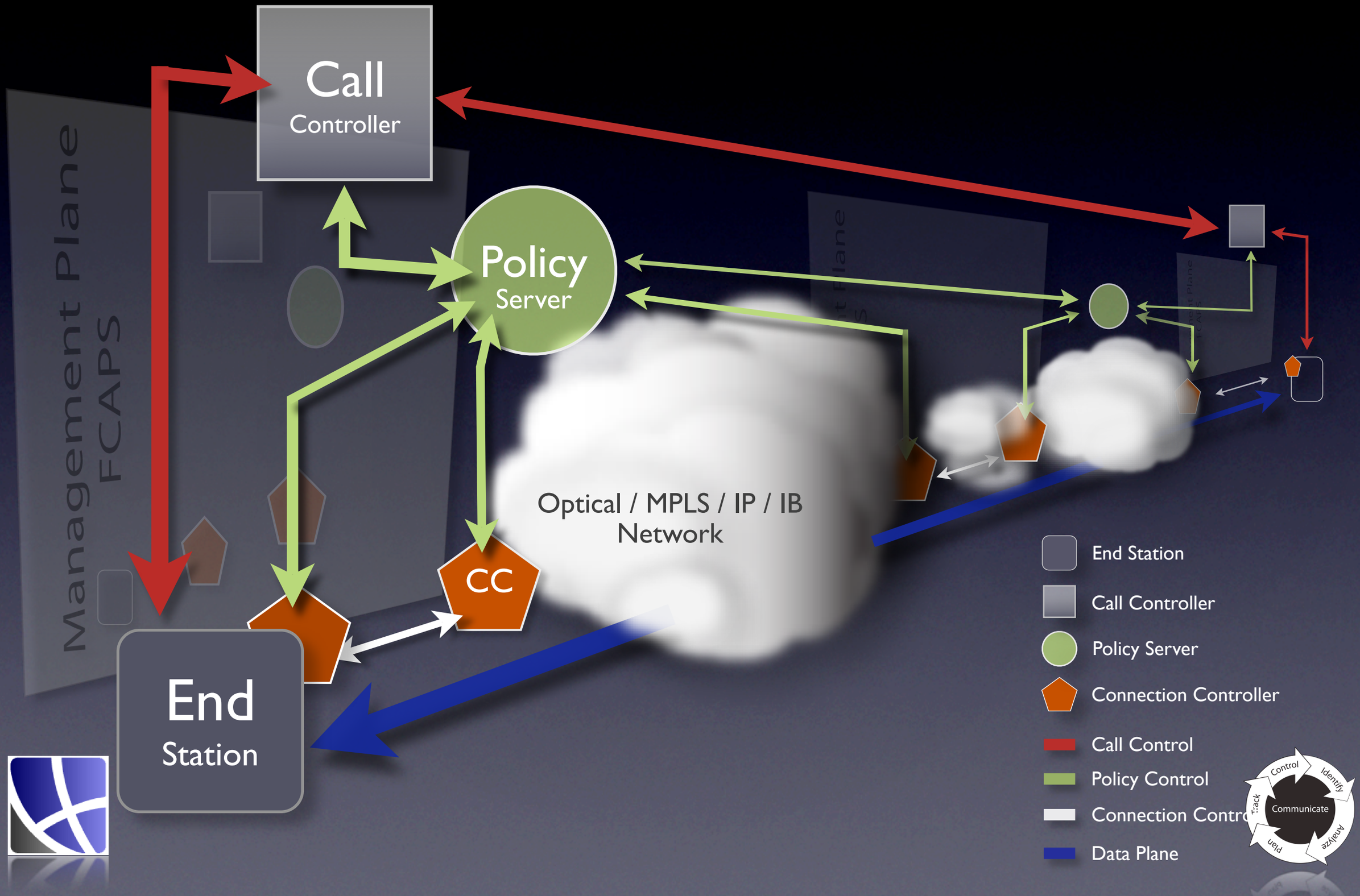
- Service Oriented Operational Status
  - Initiation, use and termination status
  - Protection and restoration status
- Functional assurance
  - Availability, Utility, Viability and Efficiency
  - Routing/Signaling Operational Correctness
  - Name Resolution Availability and Correctness
  - Security Service Functional Correctness
- Functional Verification/Validation
  - Reachability verification
  - Security policy enforcement
- Support optimization processes



# Control Plane Definition(s)

- No lack of control plane specifications
  - ITU Optical Network Control Plane
    - G.8080, Architecture for the automatically switched optical network (ASON), *2006 Revision* – to be published imminently
    - G.7713, Distributed call and connection management (DCM), *2006 Revision*, to be published imminently
    - G.7718, Framework for ASON Management, February ’05
    - G.7714, Generalized automatic discovery for transport entities, August ’05 revision
    - ITU-T G.7715/Y.1706 - Architecture and Requirements for Routing in the Automatic Switched Optical Networks, July 2002
    - ITU-T G.7712/Y.1703 - Architecture and specification of data communication network*, March ’03
    - ITU-T T G.7716 - Control Plane Initialization, Reconfiguration, and Recovery, target Consent Nov. ‘06
  - IETF Control Plane Examples
    - RFC 3495, RFC 3447, RFC 3946, RFC 4139, RFC 4098, RFC 4061, RFC 4054
    - RFC 3471-3474, RFC 3945, RFC 4003, RFC 4054, RFC 4201-4208, RFC 4257-4258, RFC 4606, RFC 4783
    - RFC 4801-4803, RFC 4872, RFC 4873, RFC 4920, RFC 4927-4929, RFC 4974, RFC 5063, RFC 5145-5146, RFC 5316
  - Provides auto-discovery, auto-configuration, security association, signaling, routing, and management interfaces for network forwarding components
  - Implemented through Control Plane protocols or through the Management Plane

# Control Plane Reference Model



# Abstract CP Components

- Call controller (Session Layer)
  - Sets up and manages a communication relationship between two or more parties.

(ITU-T REC H.323 Packet Based Multimedia Systems. June 2006)

- Policy controller (PDP, PEP)
  - Represents, deploys, manages and enforces policies to control resource access and use.

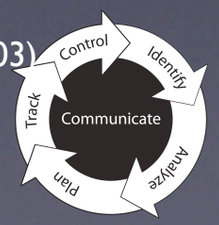
(IETF RFC 3060 Policy Core Information Model. February 2001)

- Connection controller
  - Provides connection routing, creation, modification, restoration and deletion services.

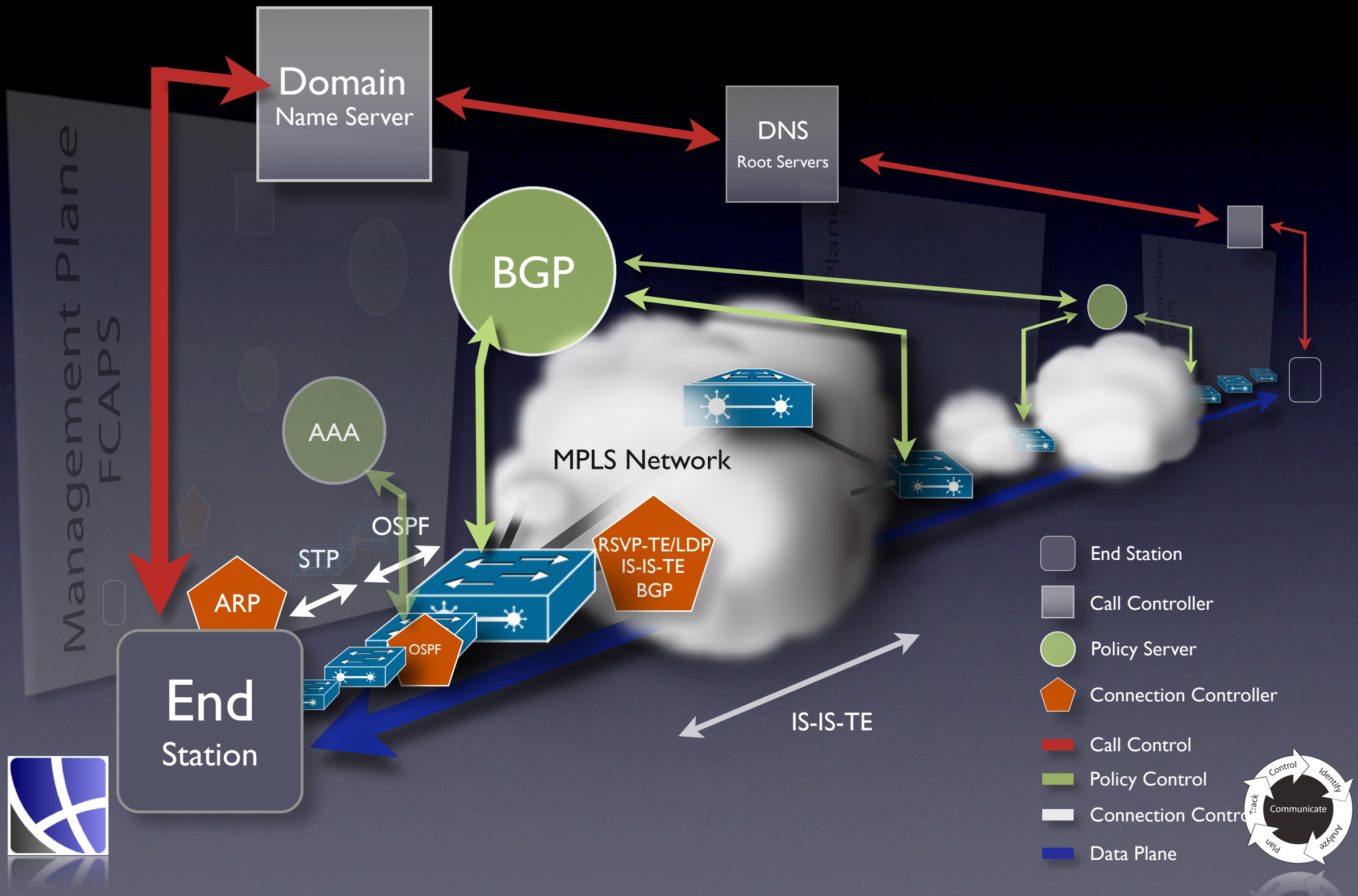
(OIF ASON/GMPLS E-NNI, UNI Implementation Agreements. September 2005)

- Applied to hierarchical service architecture
  - Infrastructure, service, and application levels

(ITU-T Rec. X.805 Security Architecture for systems providing end-to-end communications 10/2003)



# Control Plane Internet Model

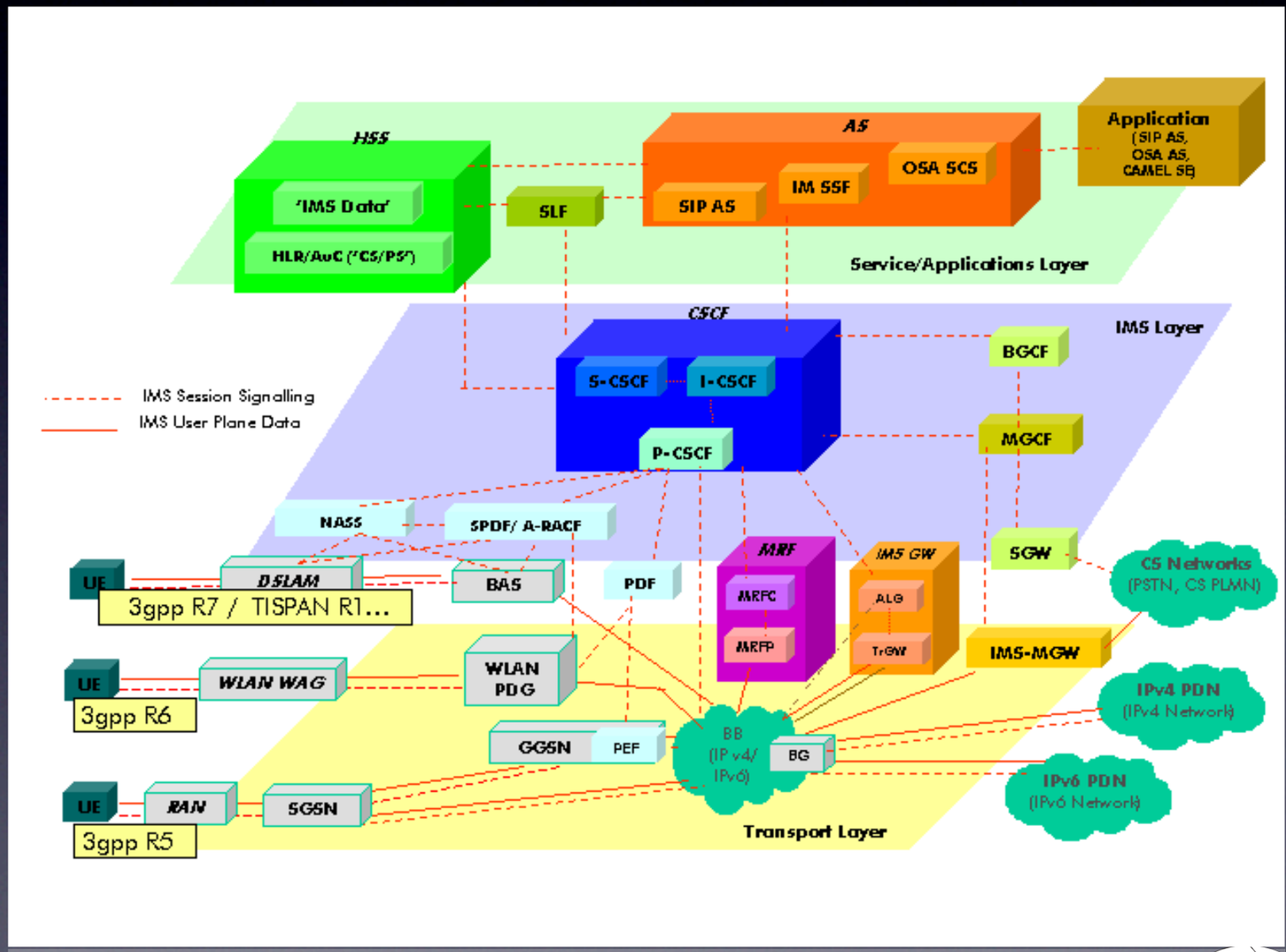


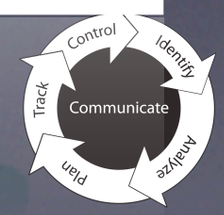
# Internet CP Protocols

- Call Control
  - ICMP, DNS, TCP (SYN, SYN/ACK, FIN), IKE
- Policy Control
  - ICMP, telnet, SNMP, RADIUS, LDAP
  - STP, RIP, OSPF, IS-IS, BGP
- Connection Control
  - ICMP, ARP, STP, RIP, RSVP
  - MPSL, LDP, RSVP-TE, OSPF-TE

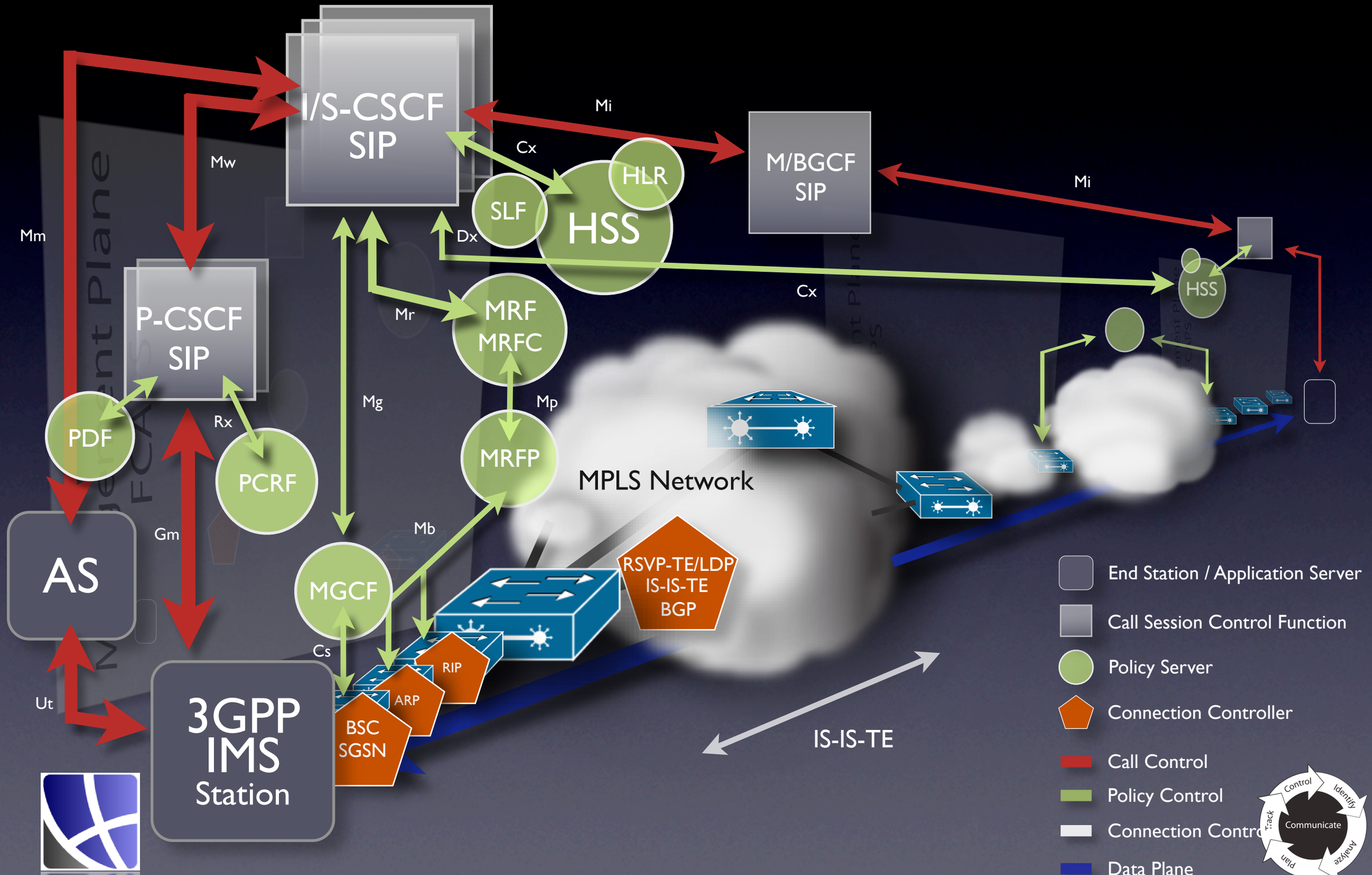
# 3GPP / TISPAN IMS
## Architecture Overview

- 3rd Generation Partnership Project
- Telecoms and Internet Converged Services and Protocols for Advanced Networks (ETSI)
- IP Multimedia Subsystem
- Intended as Next Generation Networking (NGN) architecture for voice, video, multimedia and data.

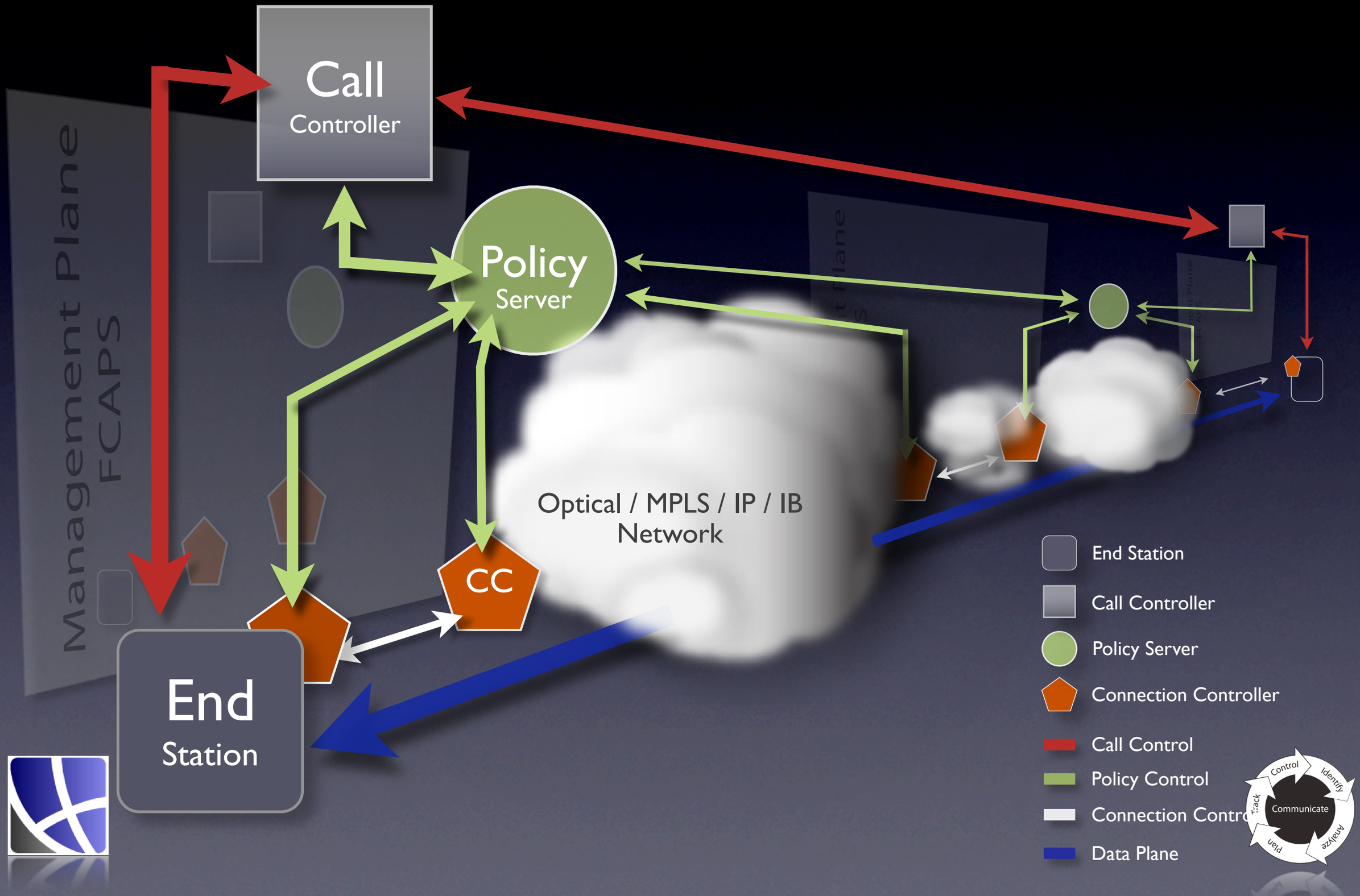


# Control Plane 3GPP / IMS / TISPAN



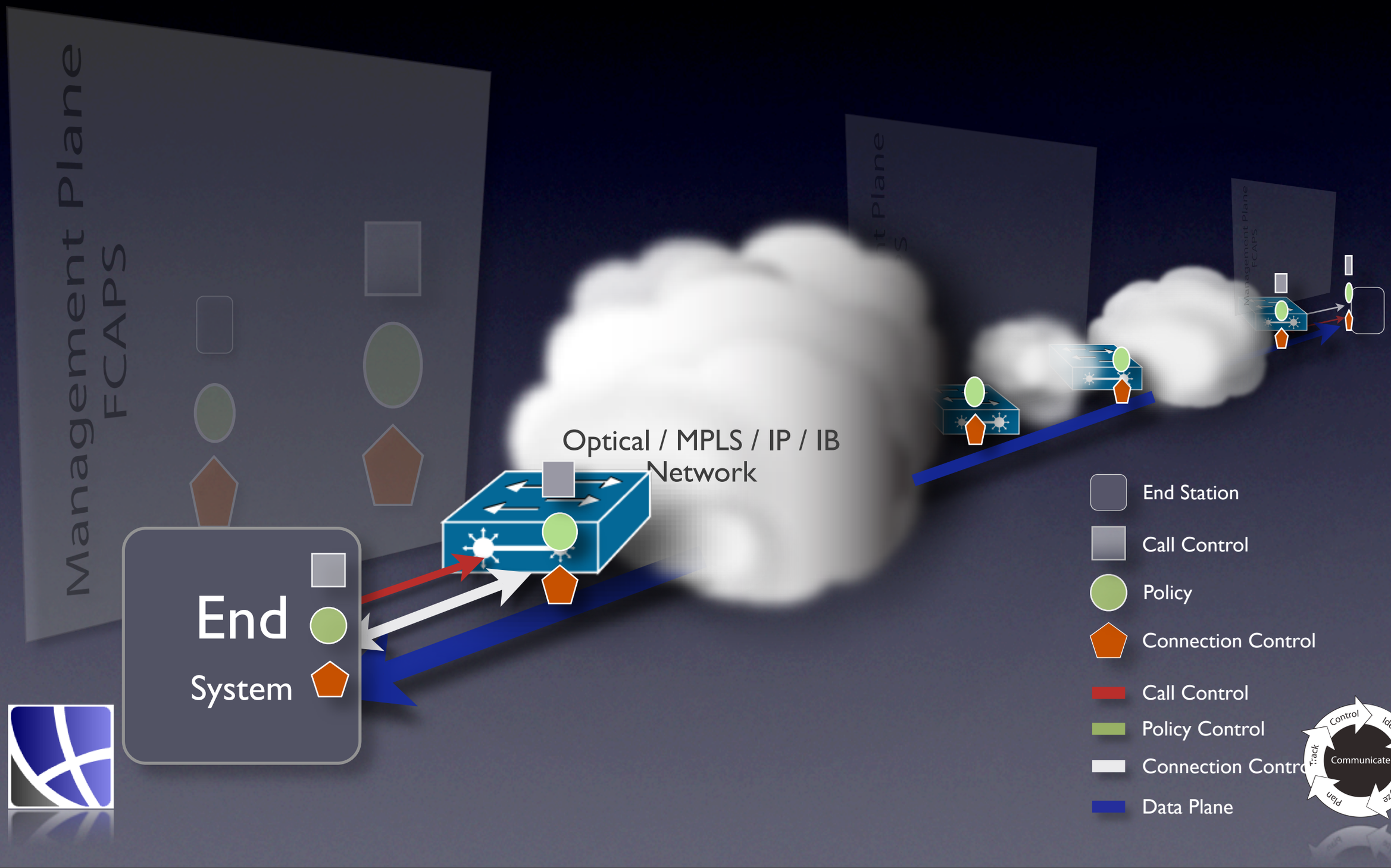
# Control Plane Reference Model



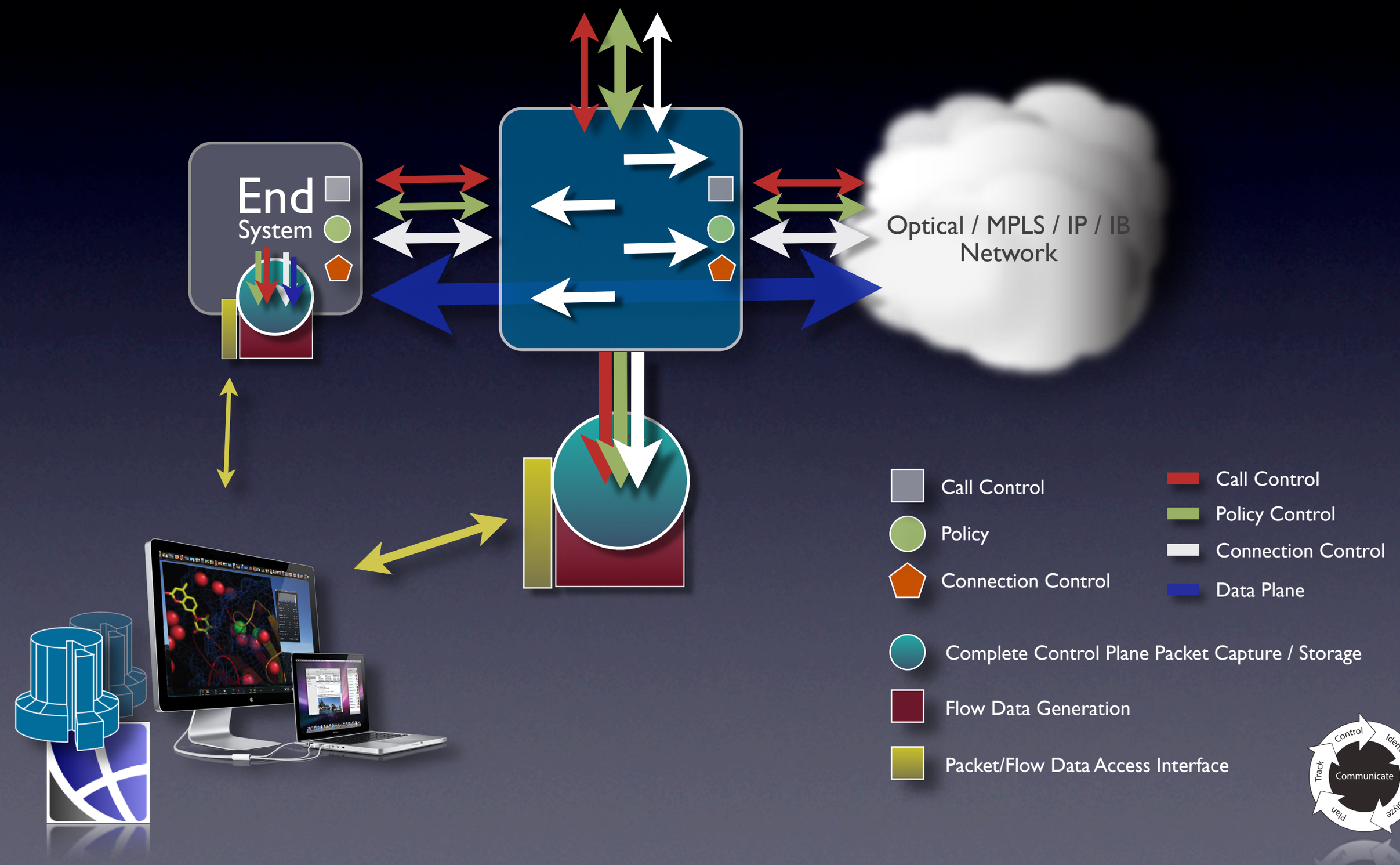
# CP Perception Goals

- Total Semantic Capture (Comprehension)
  - State initializations and transitions
  - Policy dissemination and enforcement
  - Topology, resource allocations, error conditions
- Context Awareness
  - Multi-Layer Identifiers (ethernet, MPLS labels, etc....)
  - Globally sychronized uSec timestamps
- Enable Near Real-Time State Awareness
  - Large scale access and data sharing
  - Multi-dimensional Correlation
- Complete Historical Reconstruction

# Control Plane Implementation Model



# Control Plane Sensor Strategy



# CP Sensing Strategy

- Third-party Control Plane monitor/sensors
  - Can't really rely on the network switch/router vendors to do this.
- Each network device must provide complete Control Plane packet capture
  - Any packet that originates from or terminates on the device must be captured in its entirety.
  - Data must include port of origination/transmission, direction and UTC time stamp.
  - Before and after any encryption/decryption.
- Packet data is converted to flow data for sharing, status reporting, and archival.
- Now we have the data we need to drive Control Plane Situational Awareness.

# Packet / Flow Strategies

- Packet data for complete comprehension
- Flow data provides multi-tiered data model.
  - Data Reduction / Semantic Preservation
    - Service Oriented Transactional Abstractions
    - Complex Data Representations
    - Flexible Compression Strategies
    - Multiple Flow Content Representations
  - Semantic Access Control Schemes
    - Inter/Intra Domain Data Sharing
    - Complex Data Aggregation Scoping
    - Anonymization
  - Cross Domain/Dimensional Correlation
    - Unified Object Specifications
    - Self-Synchronization Methodologies
    - High Resolution Timestamping

# CP Information Model

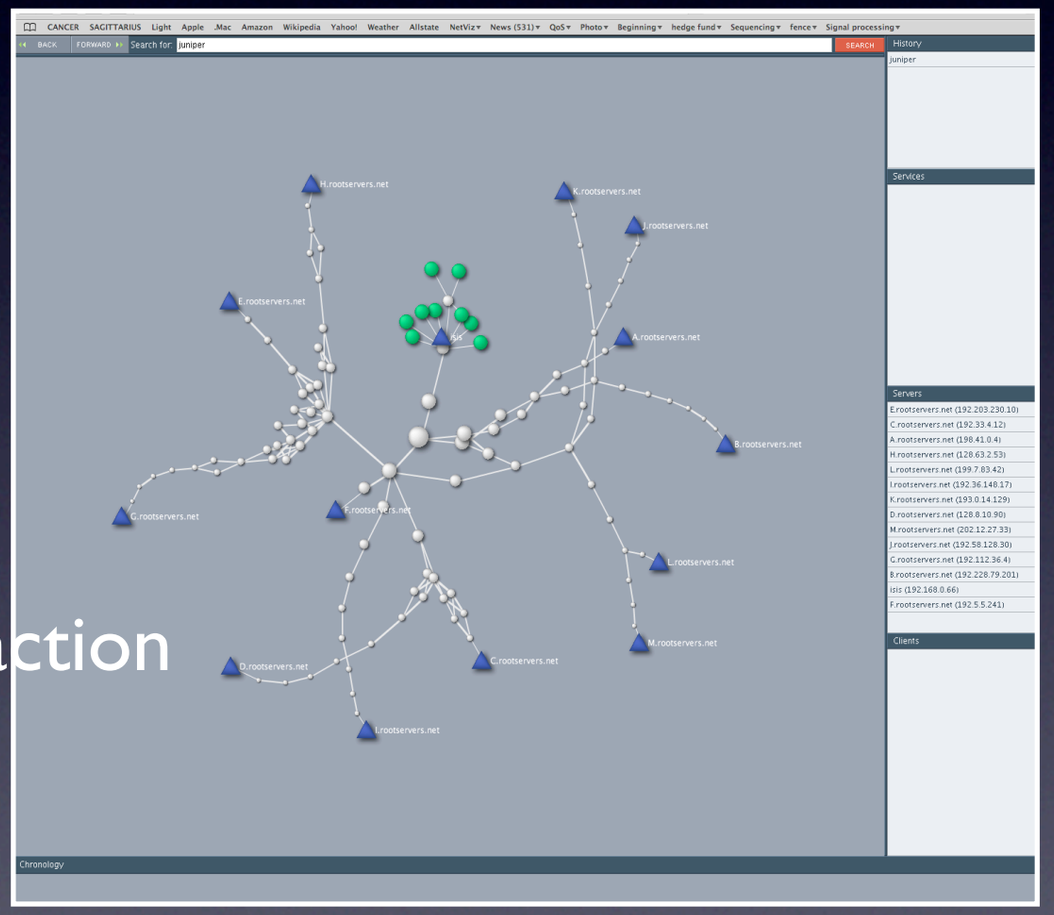
- Multi-tiered Information Model
  - Not every application needs the same type of information
  - System needs to allow "customer" to define what it wants
- And, as conditions change, level of detail and frequency of status reports also needs to change

1. Control Plane Service Existence Flow Strategy
   - 1.1. Matrix Flow with Service Identifiers
   - 1.2. Operational/Security Fault Status Flow Records
2. CP Service Performance Flow Strategy
   - 2.1. Transactional Flow with Ops and Performance Attributes
   - 2.2. Operational Fault Status Flow Records
3. Total Packet Content Flow Strategy
   - 3.1. Transactional Flow with Aggregated Content
   - 3.2. Complete Remote Packet Capture

# CP Flow Strategy Examples

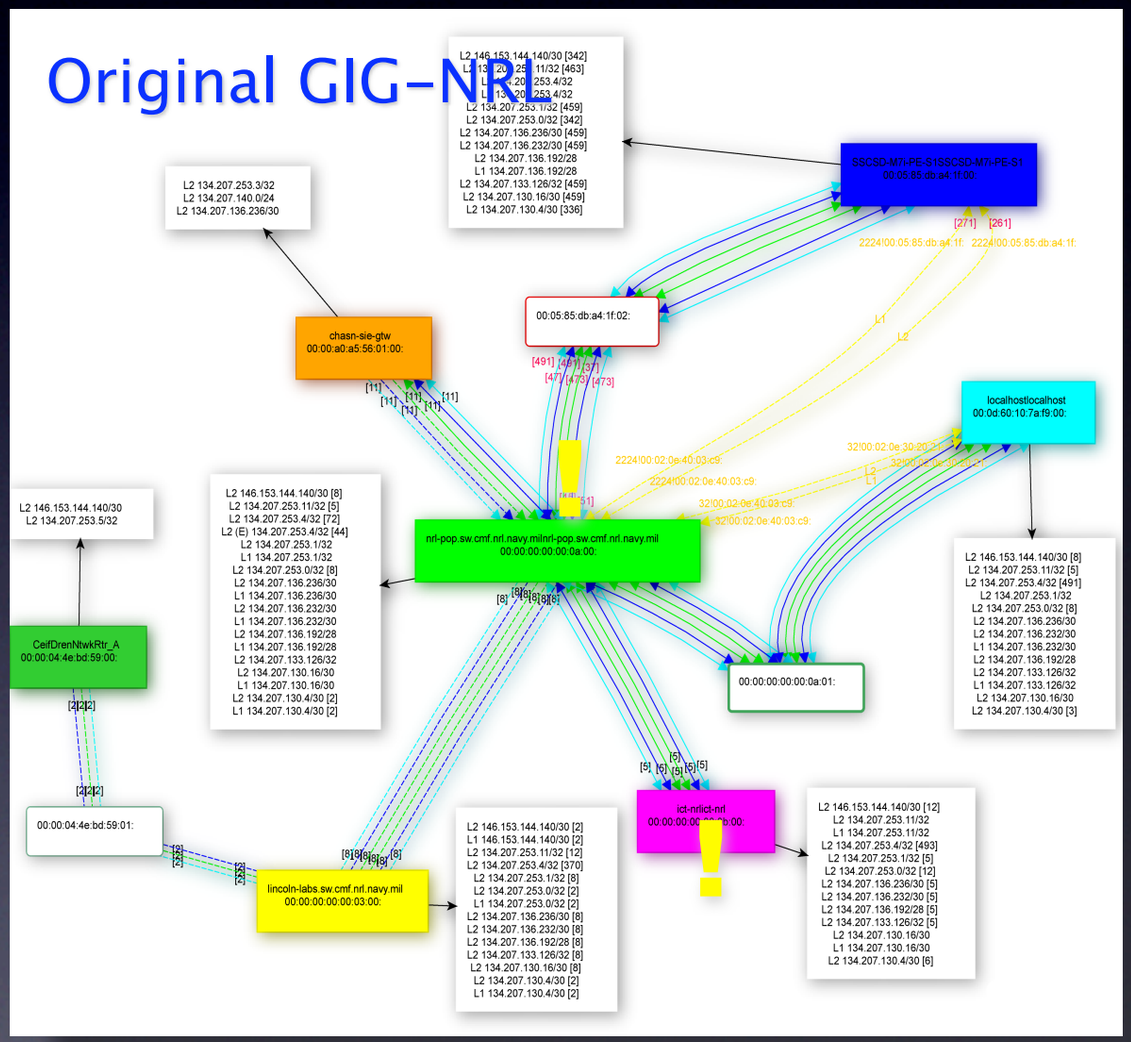
- Control Plane Protocol Flow Goals
  - Functional Correctness
  - Performance
  - Complete Semantic Capture
  - Globally Correlatable Data

- DNS Protocol Flow Goals
  - IP Flow Record for every DNS transaction
  - Contain complete packet contents
  - At least uSec global synchronization



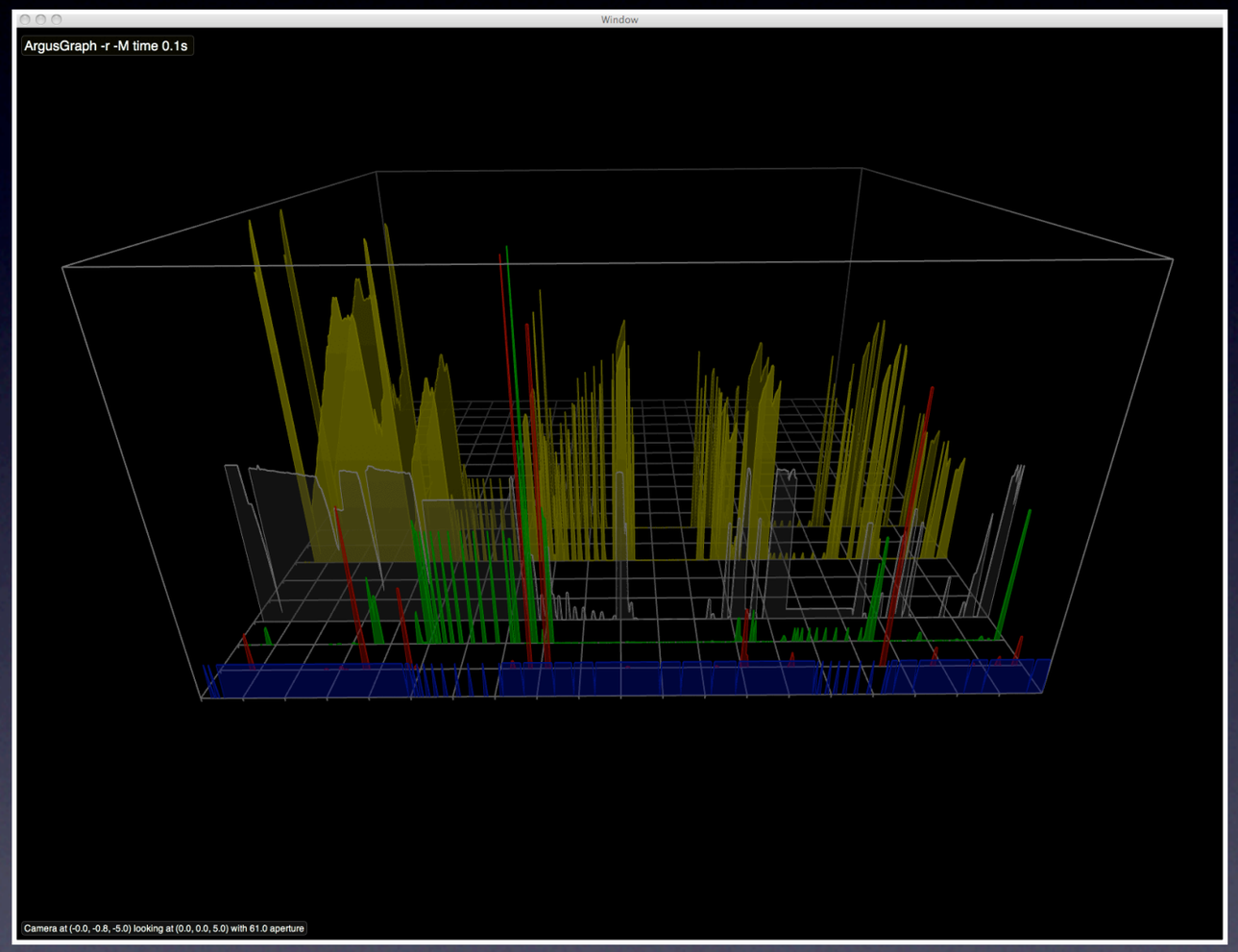

# Flow Strategy Examples

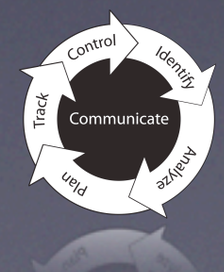
- Routing Protocol Flow Goals
  - Perceive Objects
  - Realize Operational State
  - Derive Topology
  - Reconstruct Link State Database
- IS-IS Implementations
  - LSA Flow Tracking
  - Global and local semantics
  - Extended state tracking
- Modeled using Internet2 IS-IS data



# Flow Strategy Examples

- Infiniband
  - Massive bandwidth capabilities change monitoring strategies
    - Currently capable of 80 Gbps sustained
    - 8 Gbps is slowest link speeds.
  - Multiple Service Models
    - Subnet Manager mediated call control (need to track SM as a distinct entity)
    - New identifiers (local and global addresses, virtual lanes, queue pairs)
  - Protocol capabilities change flow models
    - RDMA primitives in transport protocol demand differing flow triggering models
  - IP over Infiniband drives complex tunnel representations
  - Multiple transport services
    - Connection(less) Oriented / (Un) Reliable



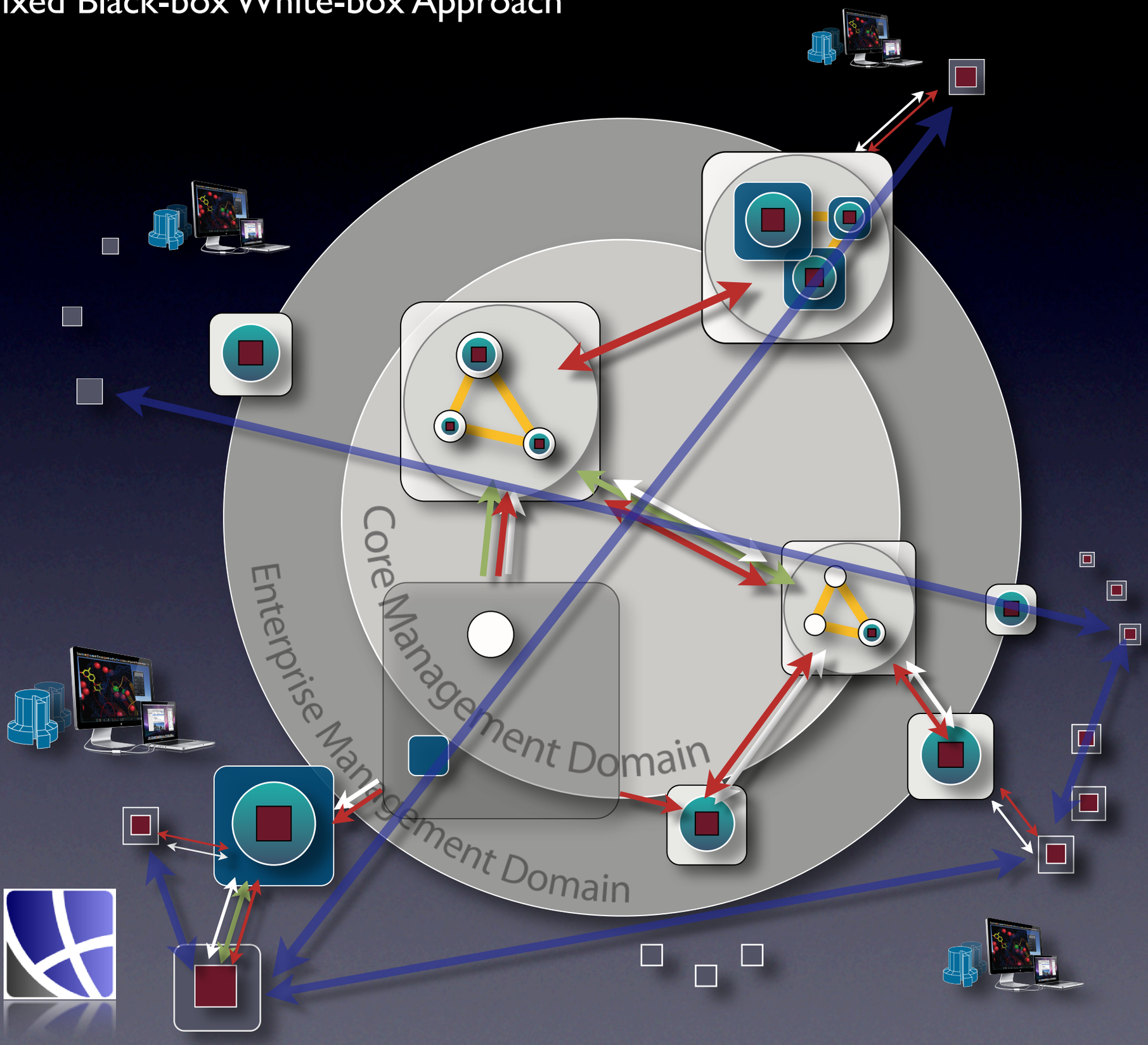
# Situational Awareness System

Basic design is local sensing, data collection and management, with local near real time data processing and large scale data sharing to support multi-dimensional control plane comprehension.

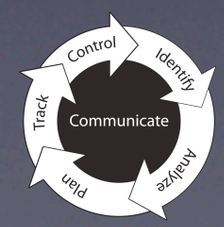
- Federated Database Model
  - Access controlled by local administrative domain (scoping)
  - Cloud-like distributed processing and query support
  - Flexible data management strategies
  - Large numbers of simultaneous users
- Near real-time information availability
  - Register for information of interest
  - Complex data processing / aggregation / enhancement / advertisement
  - Large scale data correlation processing
  - Anonymization

# Control Plane Monitor Strategy

## Mixed Black-box White-box Approach

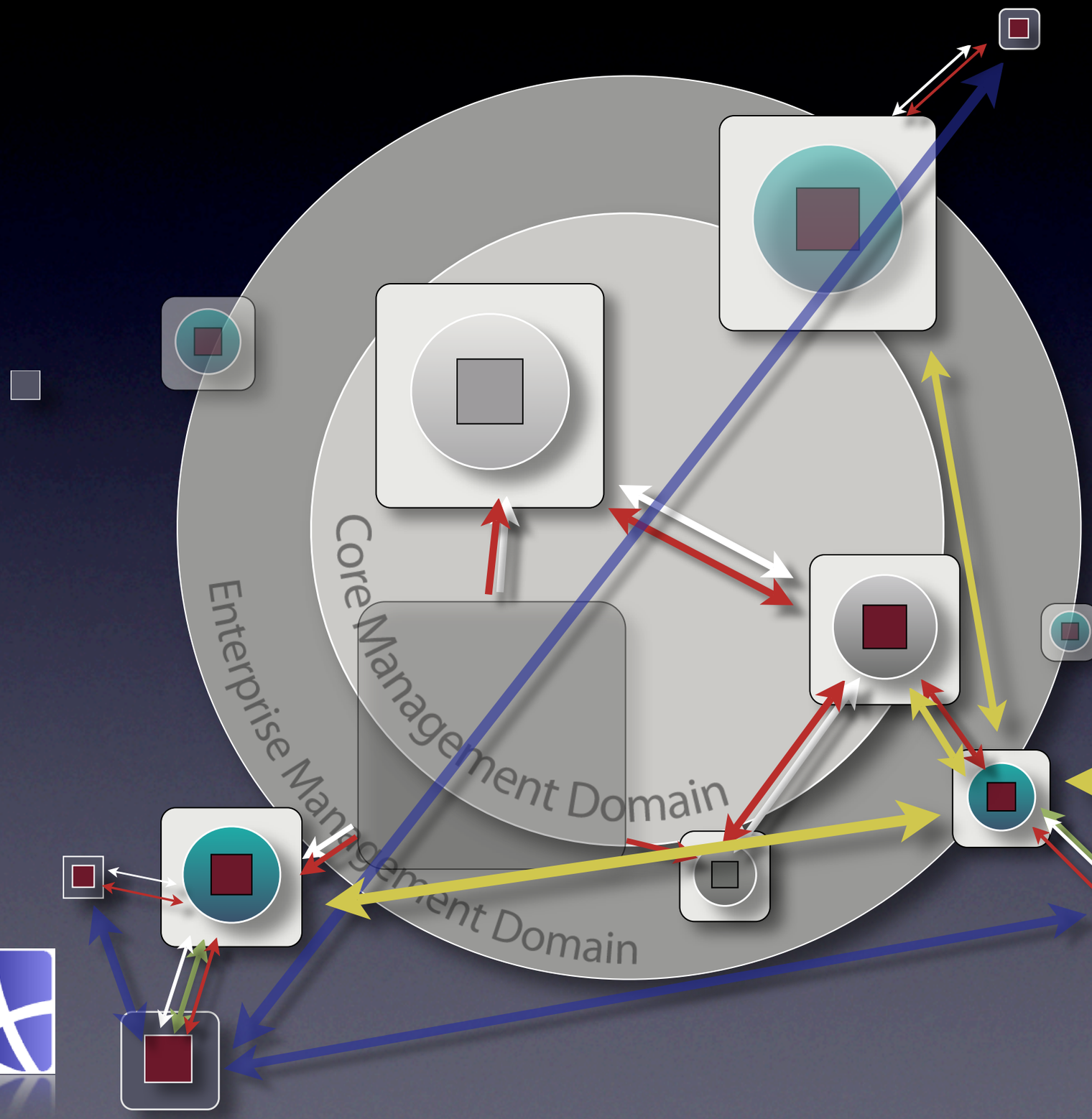



- White/Visible Network
- Black/Non-Visible Network
- Router / Switch
- Node / Nodes
- Complete Control Plane Monitored
- Flow Data Generation
- Call Control
- Policy Control
- Connection Control
- Data Plane



# Control Plane Situational Awareness System

## Mixed Black-box White-box Approach




White/Visible Network

Black/Non-Visible Network

Router / Switch

Node / Nodes

Control Plane Packet Capture

Flow Data Generation

Call Control

Policy Control

Connection Control

Data Plane

Situational Awareness Data

# Conclusions

- Control plane situational awareness is becoming a very important part of the puzzle
- Getting at the required primitive data is the principal problems.
- Many of the basic data models are still research topics, but systems are being developed now
- Strategies that can provide global awareness are more than “doable”.
- Improving human awareness is the key!!!!