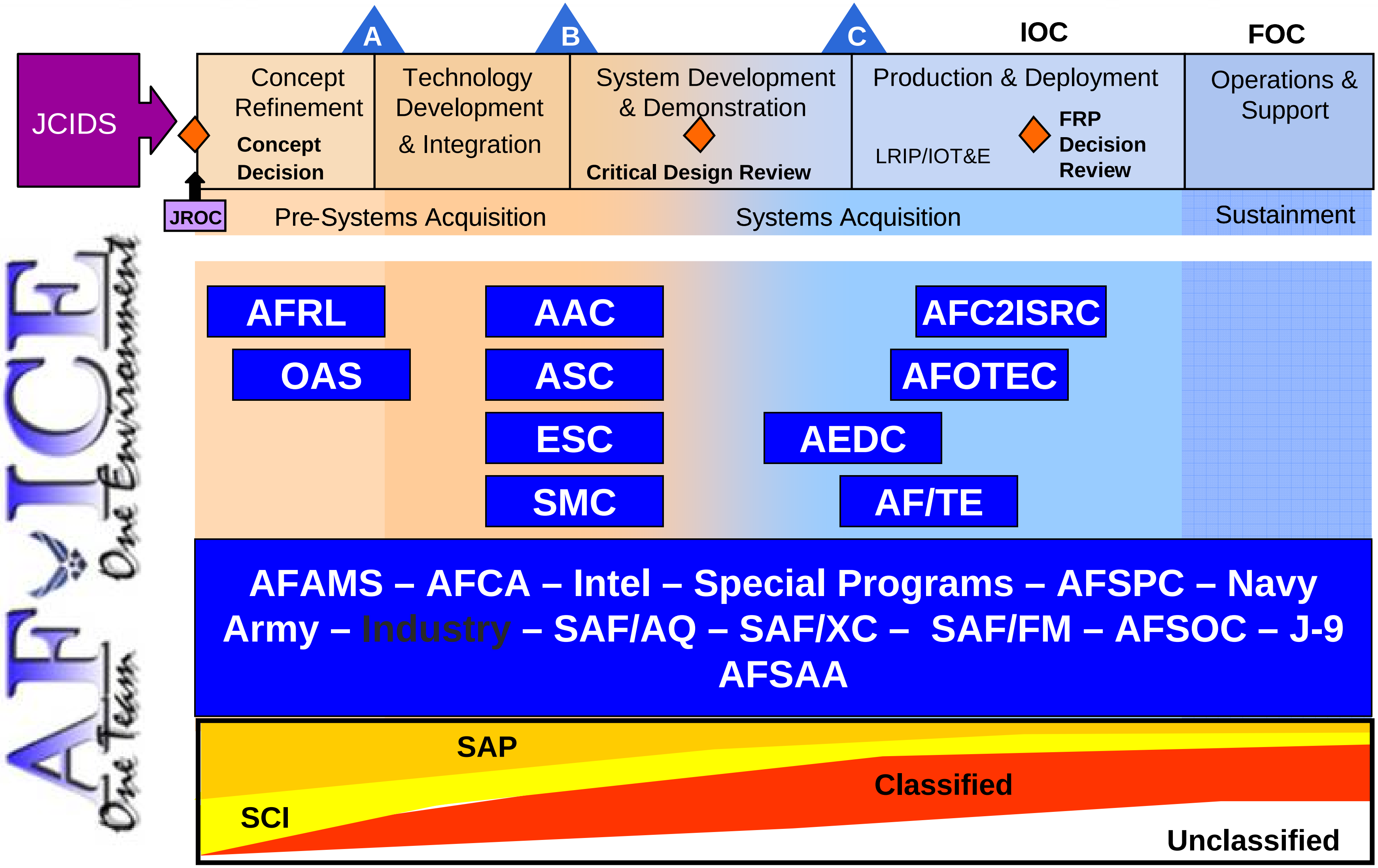
Information Assurance for Distributed M&S Standards

9th Annual NDIA SE Conference

Wednesday October 25th, 2006

Author: Scott Holben

AF-ICE Security Problem Space



A B C IOC FOC

JCIDS

Concept Refinement

Concept Decision

Technology Development & Integration

System Development & Demonstration

Critical Design Review

Production & Deployment

LRIP/IOT&E

FRP Decision Review

Operations & Support

JROC

Pre-Systems Acquisition

Systems Acquisition

Sustainment

AFRL

OAS

AAC

ASC

ESC

SMC

AFC2ISRC

AFOTEC

AEDC

AF/TE

AFAMS – AFCA – Intel – Special Programs – AFSPC – Navy
Army – Industry – SAF/AQ – SAF/XC – SAF/FM – AFSOC – J-9
AFSAA

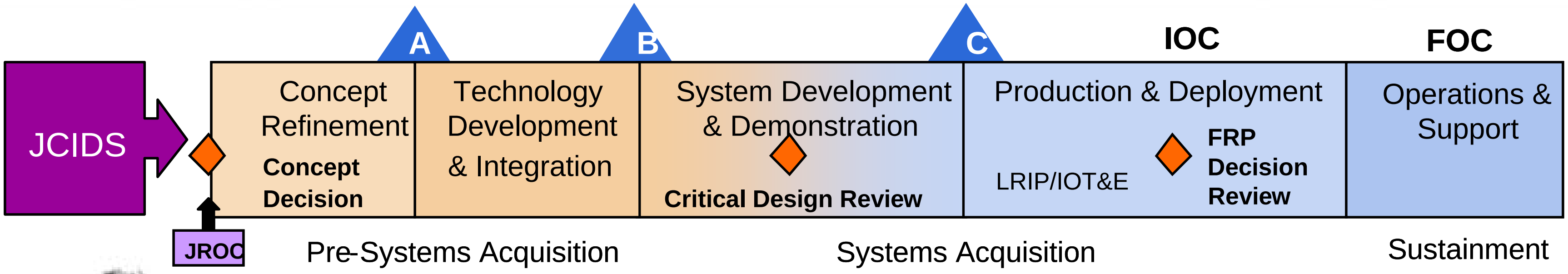
SAP

SCI

Classified

Unclassified

AF-ICE Distributed M&S Contexts



JCIDS

A

B

C

IOC

FOC

Concept Refinement

Concept Decision

Technology Development & Integration

System Development & Demonstration

Critical Design Review

Production & Deployment

LRIP/IOT&E

FRP Decision Review

Operations & Support

JROC

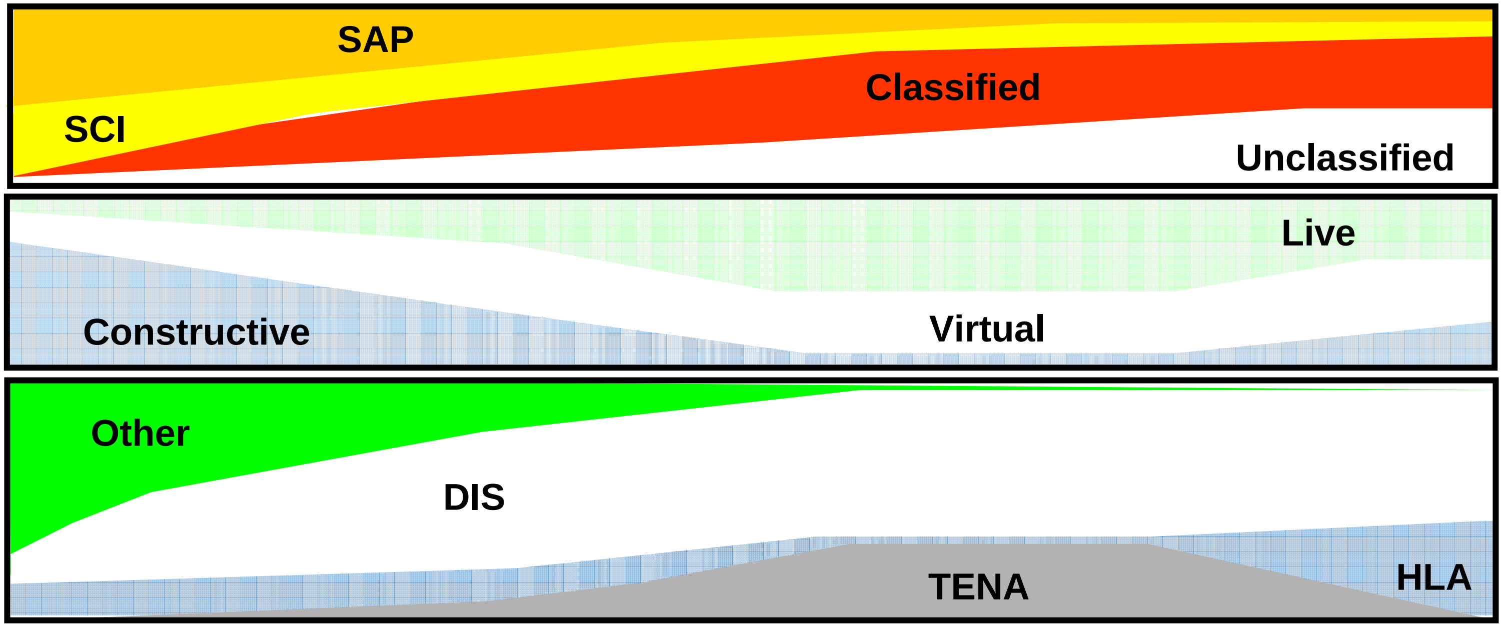
Pre-Systems Acquisition

Systems Acquisition

Sustainment

Evaluation Continuum

Mission Environment



Security Regulations (1 of 3)

•Mandatory

- All Classified Data – **NISPOM/**DoD 5220.22-M, (National Industrial Security Protection Operating Manual) regulations
  - Available at http://www.dss.mil/isec/nispom.htm, 141 pages
  - Also see 5220.22-R at http://www.cfisac.org/FSO%20Library/Misc/ISR-DRAFT.html

- SAP/SAR Data – **JAFAN 6/3** (Joint Air Force - Army - Navy) Manual regulations
  - FOUO, 162 pages

- DIA SCI Data – **JDCSISSS** (Joint DoDIIS/Cryptologic SCI Information Systems Security Standards) regulations
  - FOUO but can be found on the Internet, 111 pages
  - Available at http://www.fas.org/irp/doddir/dod/jdcsisss-rev2.doc

Security Regulations (2 of 3)

•Mandatory

- CIA SCI Data - **DCID 6/3** (Director of Central Intelligence Directive) regulations
  - Flow down requirement from JDCSISSS regulation
  - FOUO but can be found on the Internet, ~90 pages
  - Available at http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm

- IT systems on the GIG must comply with **DoD 8500** regulations
  - Available at http://iase.disa.mil/policy.html#8500s

- “Defense-In-Depth IA Computer Network Defense” **CJCSM 6510.01** Manual regulations
  - Flow down requirement of 8500 regulations, 354 pages
  - Available at www.namrl.navy.mil/FORMS/CJCSM_651001.pdf

Security Regulations (3 of 3)

•Mandatory

- Exports with Military Use – **ITAR** (International Traffic in Arms Regulations)
- Exports with Commercial Use – **EAR** (Export Administration Regulations)
- National Security Systems - **CNSS** (The Committee for National Security Systems) regulations
  - Available at http://www.cnss.gov
  - See http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf for criteria for identifying National Security Systems

Valid AF-ICE Data Type Combinations

For Each DoD Service

3rd Dimension for each Protocol or unique HLA implementation

Valid AF-ICE Data Labeling Combinations for Acquisition Centers	Edge Enclave Responsibility	Edge Enclave Responsibility	NOSC Enclave Responsibility	NOSC Enclave Responsibility	Edge Enclave Responsibility
	Intellectual Property (IP)	EAR & ITAR	Collateral	SAP	SCI
1			DTNG or RMG PL3		
2	🟩				
3		🟪			
4	🟩	🟪			
5	MCSOA with (SIParator or CASPER) and (Sidewinder or PIX or Checkpoint or …)			DTNG, RMG, or CASPER PL3 & PL4	
6	🟩				
7		🟪			
8	🟩	🟪			
9					SAVANT/ VIPRE, CASPER PL3 & PL4
10	🟩				
11		🟪			
12	🟩	🟪			
13	Sources and Methods Information (SAMI) Data Will Be Very Challenging for AF-ICE to Handle				
14	🟩				
15		🟪			
16	🟩	🟪			

Information Assurance Security Services

Gestalt

National Information Assurance (IA) Glossary, CNSS Instruction No 4009

- **Identification** is the process an Information system uses to recognize an entity.
- **Authentication** is the security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
- **Authorization** is the access privileges granted to a user, program, or process.
- **Nonrepudiation** is the assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.
    - **Accounting** is the tracing of information activities to a responsible source.
- **Confidentiality** is the assurance that information is not disclosed to unauthorized individuals, processes, or devices.
- **Integrity** is the quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.
- **Availability** is the timely, reliable access to data and information services for authorized users.

Funding Net-centric IA Efforts

- CJCSI 6212.01D "Interoperability and Supportability of Information Technology and National Security Systems" (8 March 2006)

1. Joint Interoperability Test Command (**JITC**) Joint Interoperability Test and Certification Policy:
   - IT system meets operational needs
   - Interoperable with existing and proposed IT and National Security Systems (NSS)
   - Supportable over existing and planned Global Information Grid (GIG)
   - Are interoperable with allies and coalition partners
   - Are net-ready
   - Allow US forces to protect mission essential data; detect and respond to network intrusion/system compromise; and restore mission essential data
2. Net Ready Key Performance Parameters (**NR-KPPs**) are a mandatory element of Joint Capability Integration and Development System (**JCIDS**) Capability Development Documents (**CDDs**) and Capability Production Documents (**CPDs**) and Information Support Plans (**ISPs**). Four J-6 defined NR-KPP elements:
   - Compliance with the Net-Centric Operations and Warfare Model (NCOW-RM)
   - DoDAF Integrated Architecture Products
   - Compliance with GIG Key Interface Profiles (KIPs)
   - Verification and compliance with DoD information assurance requirements (**8500 series regulations** and **DIACAP**/DITSCAP accreditation process)

Today's Internet Application Security

HTTP/S

- Supports the "**Admission Control Security Model**" understood by all CIO Security Officers for providing identification, authentication, authorization and accounting services
- Allows both the resource holder and enterprise security administrator to set explicit access control privileges to maintain confidentiality of specific Web resources

HTTP/S and SIP/S sessions are authenticated before being authorized

- **RFC 2617** uses challenges involving private keys
  - To authenticate clients or consumers
  - To optionally allow the client to authenticate the server to provide mutual authentication
- **TLS encryption**
  - Requires servers or producers to have X.509 PKI certificates
  - Since client certificates are optional, RFC 2617 may still be used to authenticate the client to provide mutual authentication

Authorization Mechanisms

- Identity Based Access Controls (**IBAC**), includes Access Control Lists (**ACL**)
- Role Based Access Controls (**RBAC**)
- Attribute Based Access Controls (**ABAC**)

DoD Regulatory Confidentiality Terms

- **Clearance** is eligibility, it requires background checks sponsored by a government agency to determine if resources can be trusted for holding or processing classified information.
- **Authorization** is determined and enforced at the enterprise-level often using Mandatory Access Controls (MAC), especially for multi-security domain transfers. Regular system users are not to be trusted to enforce authorization policies. The ISSM, NSO or ISSO will set the DoD authorization policies contained within the AIS system Security Support Structure (SSS).
- **Need-to-know** is determined and enforced by the **Data Holder** of the information with Discretionary Access Controls (DAC), e.g., Identity Based Access Controls (IBAC), Access Control List (ACL) and Role Based Access Controls (RBAC) or need-to-know is established by the **Information Owner** and enforced by RBAC.
  - *Note, an exclusive need-to-know RBAC mechanism requires a firmly established OV-7 "Logical Data Model" to demonstrate traceability to a role's operational need to access data. OV-7 diagrams are easier to develop for C2 systems than modeling and simulation networks, because data tends to belong to fewer data owners and processes are static and are not as intellectually complex.*

DoD Confidentiality Levels

Protection Levels

PL1 (Dedicated Mode)

- All resources (e.g., users, systems…) have proper clearance, formal access approval and need-to-know
- Most of today's modeling and simulation resources natively operate in a PL1 environment even when interfacing to MLS guards

PL2 (System High Mode)

- All resources have proper clearance and formal access approval
- Not all resources have need-to-know
- Requires principals to authenticate themselves before they can access resources

PL3 (Compartmented Mode)

- All resources have proper clearance
- Not all resources have formal access approval
- Not all resources have need to know
- Requires principals to authenticate themselves before they can access resources

PL4 and PL5 (Multi-level Modes)

- True Multi-Level Security (MLS)
- Requires principals to authenticate themselves before they can access resources

M&S Security Capability Gaps

•Network security requires a Network Operation Security Center (**NOSC**) to perform PL2 service-level routing and PL3 transaction-level authorization services to persist physical connectivity to mitigate the pains of establishing event specific MOAs.

•Application-level security is not part of DIS nor HLA and is new to TENA.

- Application-level **Identification & Authentication (I&A)** must be explicit, not PL1 implicit, to persistent network connections in PL2+ environments
- Application-level **Labeling** must be explicit, not PL1 or PL2 implicit, to foster persistent network connections in PL3+ environments
- Simulation architecture needs to accommodate proxy-based Policy Enforcement Points (**PEP**) and Policy Decision Points (**PDP**) to implement mediated net-centric access controlled security services

•**Data aggregation** (event OPSEC) challenges are driven by Security Classification Guidelines (**SCG**) and Program Security Directives (**PSD**). Data aggregation will remain a manual Systems Engineering process until strong data management, explicit labeling and IA minded compositioning processes are established. Simulation resources sensitive to data aggregation must have event-level access controls to mitigate chances of unauthorized disclosures to aggregated information.

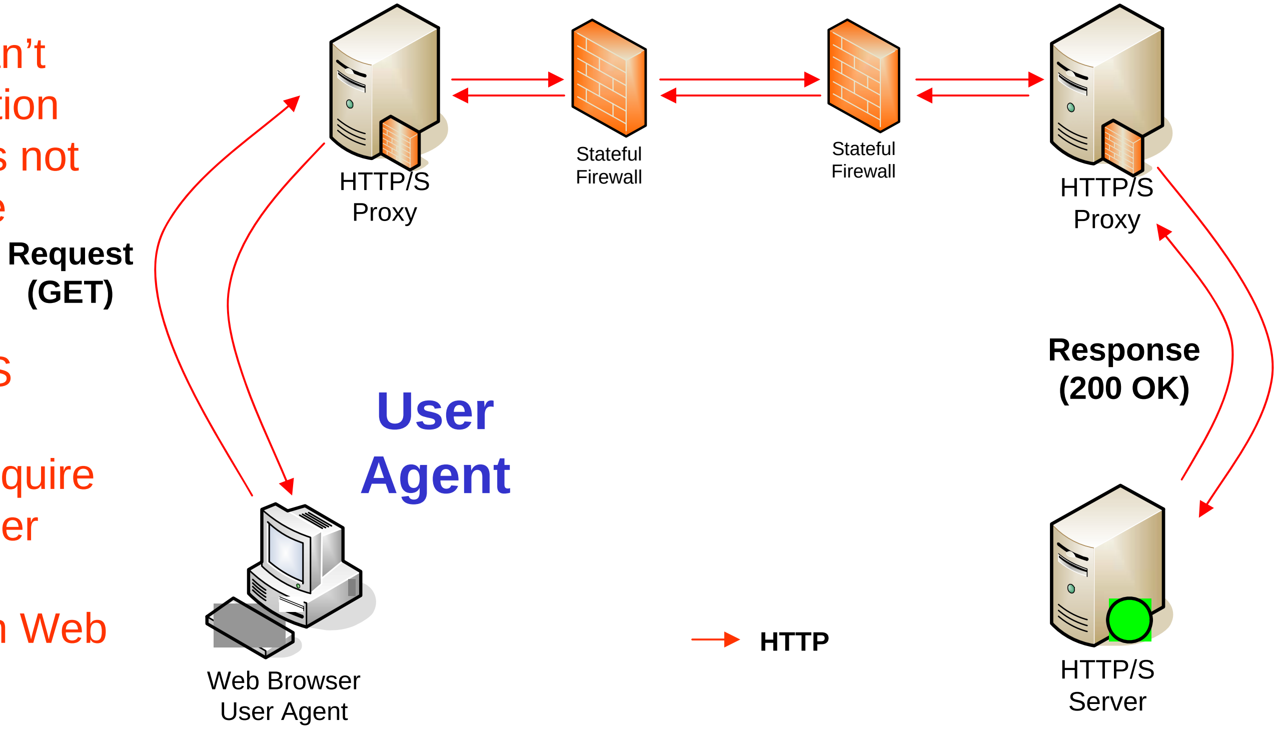
Intellectual Property (IP) Protection Requirements

Protecting IP on Classified Networks

- Identities must be established to prevent unauthorized disclosure
  - Identities can be established local to the private enterprise
  - Identities can be established and asserted by a trusted 3rd party
- Accounts are provisioned internal to the enterprises owning the IP
- Auditing will be similar to **PL2 auditing requirements**
- Authentication will be mutual similar to **PL4 authentication requirements**
- Authorization to IP must be implemented by private enterprises owning the IP
- WAN communications for IP within NSA Type I encrypted tunnels must be encrypted once again using industrial strength hop-by-hop or end-to-end commercial encryption (e.g., FIPS 140-2) similar to non Sources and Methods Information (SAMI) **PL3 encryption mechanisms**

Cross Enterprise HTTP/S Transactions

- Supports the “Admission Control Security Model” and DoD PL3+ Confidentiality services
- RFC 2617 digest-based challenge produced by a proxy server or user agent prompts the user with an identity-based challenge and realm
- HTTP/S proxy server acts as a Policy Enforcement Point (PEP)
- User supplies the appropriate username and password
- Unfortunately HTTP/S can’t provide real-time application services because there is not a separation between the real-time streams and controlling transactions
- To scale, distributed M&S synchronous real-time streaming applications require asynchronous peer-to-peer (P2P) communication, preferably using a proven Web user agent technology



Simulation Entity User Agents

SIP Modeling & Simulation User Agents (UA)

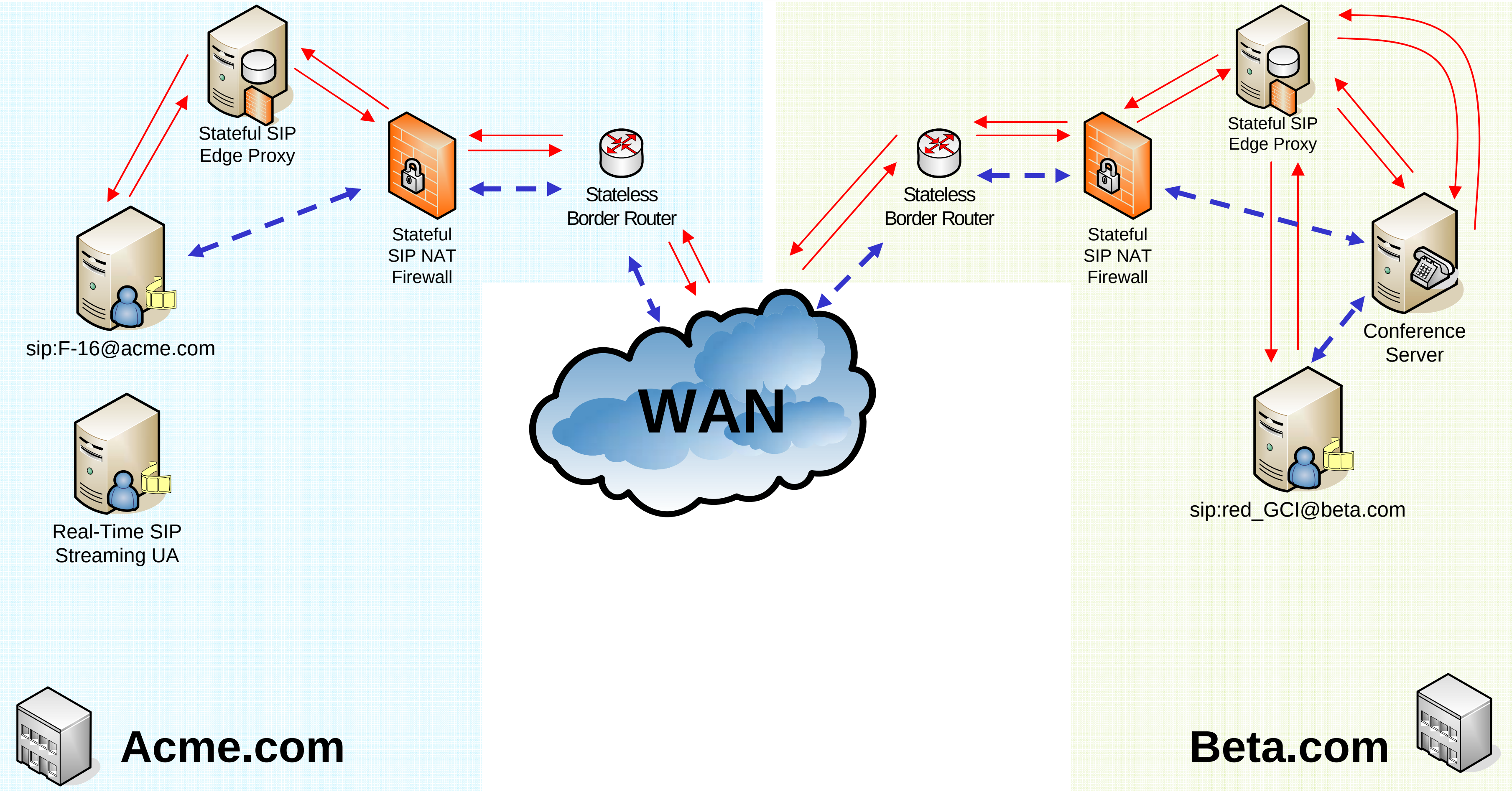
- Is the convergence of **scalable** VoIP phone technology
- SIP UAs have URIs associated with them that are **routed at the session-layer** to establish, modify and tear-down SIP sessions
- Once sessions are established SIP UAs are the **sources and sinks of real-time information**, typically Real-time Protocol (RTP) streams
  - RTP is a Web standard like SIP and RTP can carry DIS payloads
  - RTP is built on top of UDP

SIP UA Integration with DIS

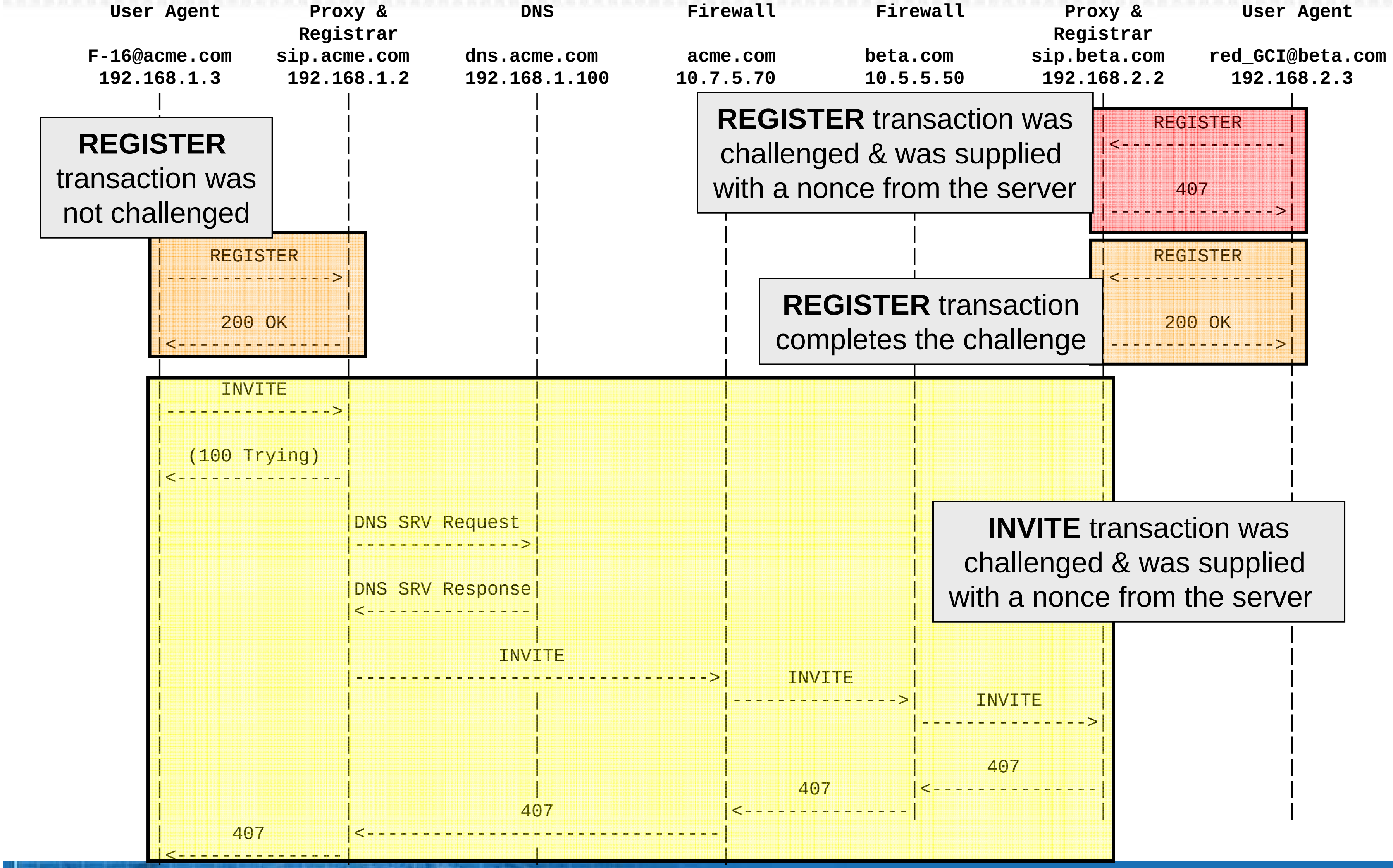
- User agents can be integrated with DIS simulations by one of three means:
  - UAs act as dedicated **very loosely coupled hardware relays** on separate hosts
  - UAs are **loosely coupled software shims** that are installed on existing simulation hosts
    - capture broadcast traffic with a virtual network adapter
    - user agent listens on that port, bundles traffic in RTP packets and relays them via RTP sessions
  - UA APIs support two forms of **tight coupling** using an API
    - Tightly integrated RTP stack with loosely coupled SIP stack
    - Tightly integrated RTP and SIP stacks

Protecting Real-Time Streaming Intellectual Property (IP)

Gestalt



RFC 3261 SIP Call Flow Diagram



```
   User Agent       Proxy &           DNS          Firewall         Firewall         Proxy &        User Agent
                   Registrar                                                        Registrar

 F-16@acme.com   sip.acme.com    dns.acme.com      acme.com         beta.com      sip.beta.com   red_GCI@beta.com
  192.168.1.3     192.168.1.2    192.168.1.100    10.7.5.70        10.5.5.50      192.168.2.2      192.168.2.3
    |                |                |                |                |                |                |
    |                |                |                |                |                |    REGISTER    |
    |                |                |                |                |                |<---------------|
    |                |                |                |                |                |      407       |
    |                |                |                |                |                |--------------->|
    |    REGISTER    |                |                |                |                |    REGISTER    |
    |--------------->|                |                |                |                |<---------------|
    |     200 OK     |                |                |                |                |     200 OK     |
    |<---------------|                |                |                |                |--------------->|
    |     INVITE     |                |                |                |                |                |
    |--------------->|                |                |                |                |                |
    |  (100 Trying)  |                |                |                |                |                |
    |<---------------|                |                |                |                |                |
    |                |DNS SRV Request |                |                |                |                |
    |                |--------------->|                |                |                |                |
    |                |DNS SRV Response|                |                |                |                |
    |                |<---------------|                |                |                |                |
    |                |             INVITE              |                |                |                |
    |                |-------------------------------->|     INVITE     |                |                |
    |                |                |                |--------------->|     INVITE     |                |
    |                |                |                |                |--------------->|                |
    |                |                |                |                |      407       |                |
    |                |                |                |      407       |<---------------|                |
    |                |               407               |<---------------|                                 |
    |      407       |<--------------------------------|
    |<---------------|
```

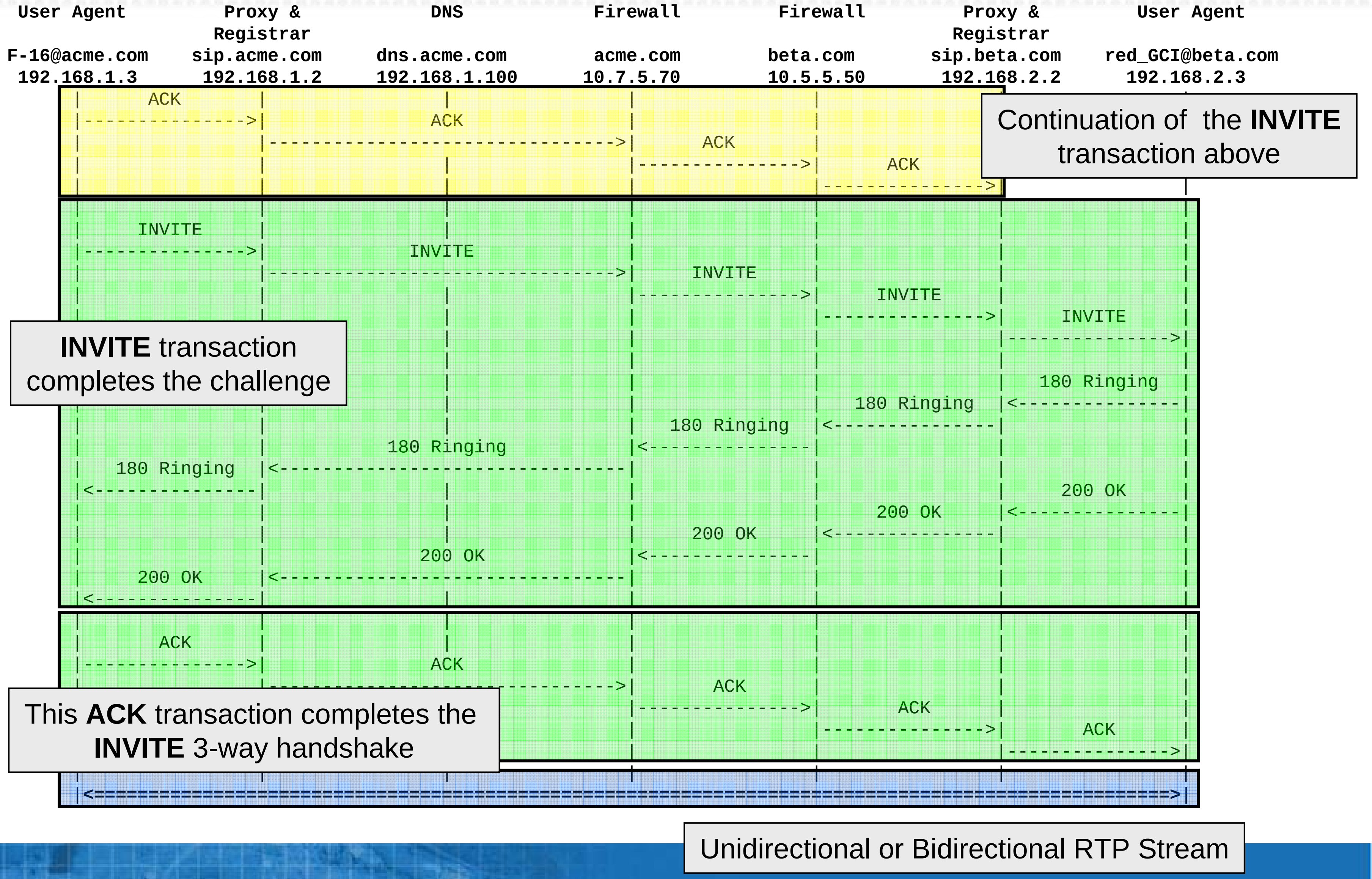
REGISTER transaction was not challenged

REGISTER transaction was challenged & was supplied with a nonce from the server

REGISTER transaction completes the challenge

INVITE transaction was challenged & was supplied with a nonce from the server

RFC 3261 SIP Call Flow Diagram



```
  User Agent     Proxy &         DNS          Firewall       Firewall        Proxy &      User Agent
                Registrar                                                   Registrar
F-16@acme.com  sip.acme.com  dns.acme.com     acme.com       beta.com      sip.beta.com  red_GCI@beta.com
 192.168.1.3   192.168.1.2   192.168.1.100   10.7.5.70      10.5.5.50      192.168.2.2    192.168.2.3
     |      ACK      |               |               |               |
     |-------------->|              ACK              |               |
     |               |------------------------------>|      ACK      |
     |               |               |               |-------------->|      ACK
     |               |               |               |               |-------------->

     |    INVITE     |               |               |               |               |
     |-------------->|            INVITE             |               |               |
     |               |------------------------------>|    INVITE     |               |
     |               |               |               |-------------->|    INVITE     |
     |               |               |               |               |-------------->|    INVITE     |
     |               |               |               |               |               |-------------->|
     |               |               |               |               |               |  180 Ringing  |
     |               |               |               |               |  180 Ringing  |<--------------|
     |               |               |               |  180 Ringing  |<--------------|               |
     |               |          180 Ringing          |<--------------|               |               |
     |  180 Ringing  |<------------------------------|               |               |               |
     |<--------------|               |               |               |               |    200 OK     |
     |               |               |               |               |    200 OK     |<--------------|
     |               |               |               |    200 OK     |<--------------|               |
     |               |            200 OK             |<--------------|               |               |
     |    200 OK     |<------------------------------|               |               |               |
     |<--------------|               |               |               |               |               |

     |      ACK      |               |               |               |               |               |
     |-------------->|              ACK              |               |               |               |
     |               |------------------------------>|      ACK      |               |               |
     |               |               |               |-------------->|      ACK      |               |
     |               |               |               |               |-------------->|      ACK      |
     |               |               |               |               |               |-------------->|

     |<=============================================================================================>|
```

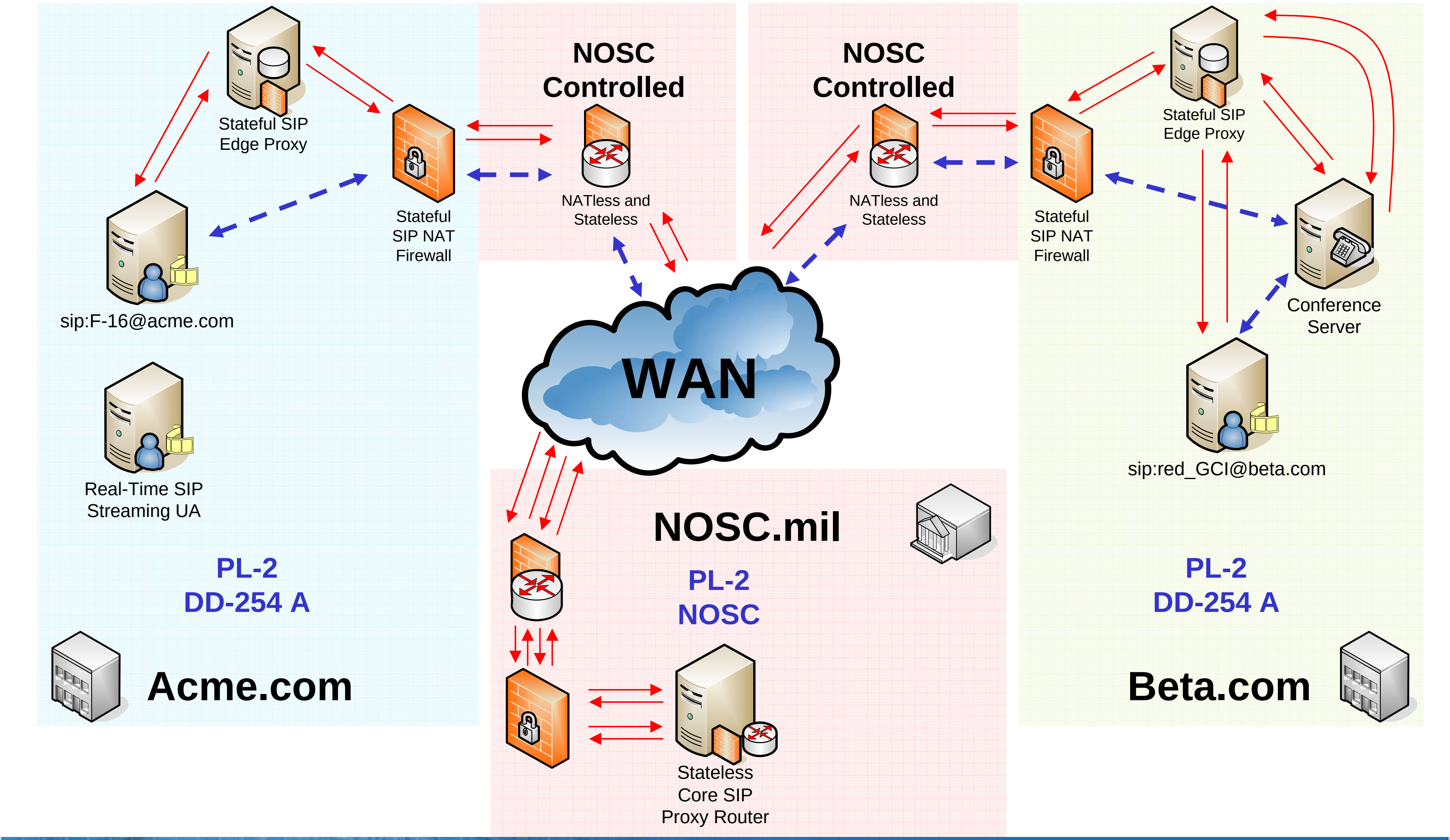
Continuation of the **INVITE** transaction above

INVITE transaction completes the challenge

This **ACK** transaction completes the **INVITE** 3-way handshake

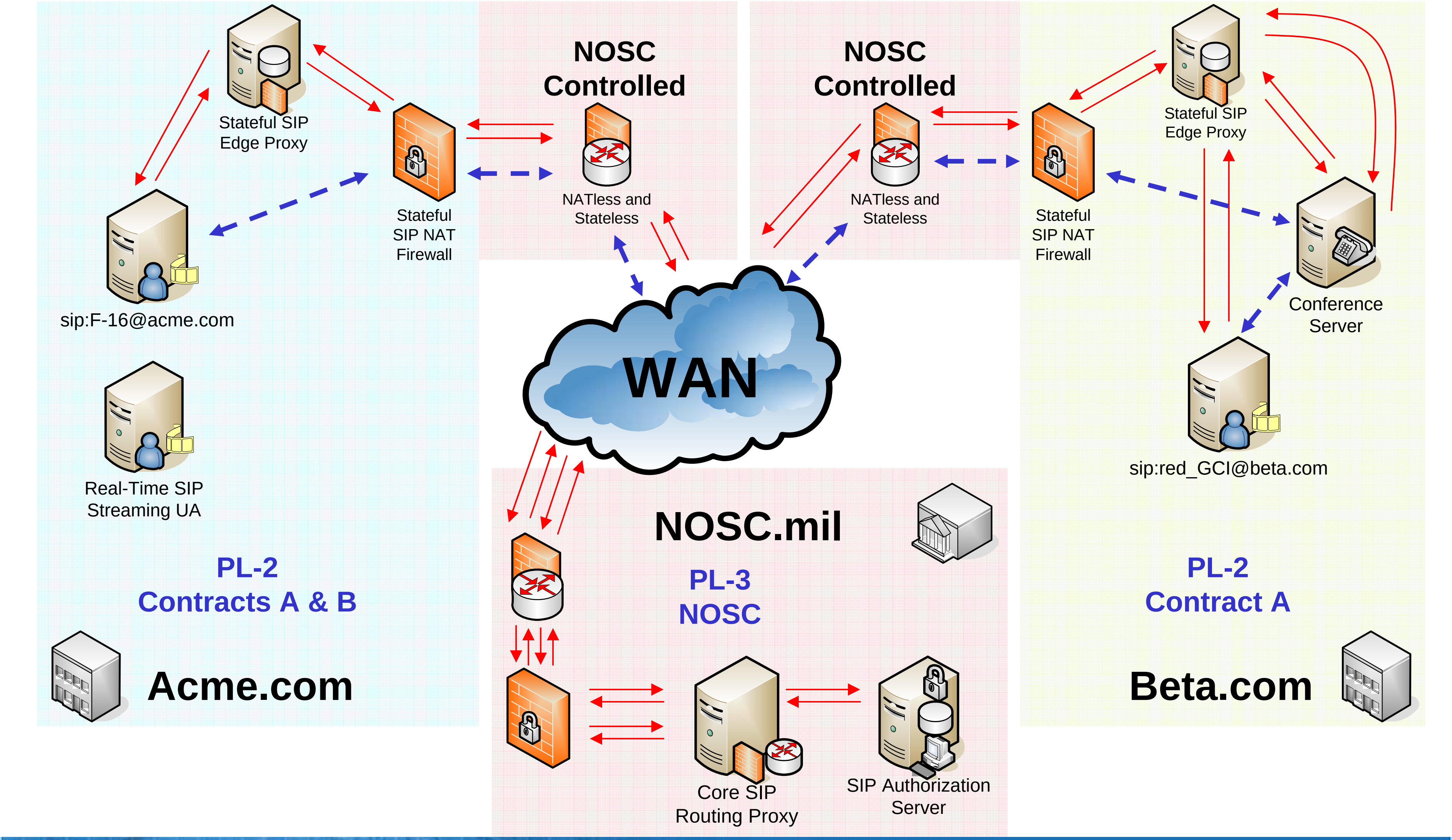
Unidirectional or Bidirectional RTP Stream

Protecting Intellectual Property and DoD Classified Information



Protecting Intellectual Property and Classified Multi-contract Information

Gestalt



Benefits of SIP VoIP Technologies

- SIP network resources (C2 systems, simulators, etc.) are **treated as opaque URIs**
- SIP components may be integrated into a **Multi Channel Service Oriented Architecture (MCSOA)** with Web Service Description Language (WSDL) interfaces
- SIP supports both perimeter and application-level security models for real-time applications
- **SIP URI resources can have privileges** (e.g., IBAC, RBAC or ABAC) associated with them to implement discretionary or mandatory access controls
- SIP can utilize **RFC 2617 or TLS authentication mechanisms** that can take advantage of LDAP, RADIUS, or Diameter services
  - These technologies are understood and trusted by many CIO Security Officers
- SIP supports stateful NAT firewalls used by most enterprises to **protect intellectual property** and export controlled information
- SIP allows existing enclaves to be added into larger networks without requiring IP **address re-alignments**
- SIP can support **persistent PL2+ networks** without requiring re-accreditation of networks, PL1 rated systems require frequent re-accreditation
  - Zero network configuration
- **SIP is strong candidate for providing common integrated wire-level net-centric Security and Quality of Service (QoS) capabilities to DIS, HLA and TENA**

Gestalt

Extra Slides

AF-ICE Event Management Process

Gestalt

Process Steps Below Must Be Neutral to the DIS, TENA and HLA Standards and Workflow Services are Innate to all Seven Steps

1. **Formulate Event**
2. **Specify Battlespace**
   - Scheduling/Reservation Services
   - Discovery Services
3. **Build Battlespace**
   - Composition Services
   - Orchestration Services
     - Resource Provisioning Services
4. **Integrate Battlespace**
   - Registration Services
   - Presence Services
   - Availability Services
5. **Execute Event**
   - Resolve Resource Services
   - **Distributed Dynamic Networks Services**
   - Monitoring Services
   - Execution Services
   - Network Bandwidth Throttling and Packet Latency Services
6. **Analyze and Report on Event**
7. **Sustain Event Documentation and Environment**

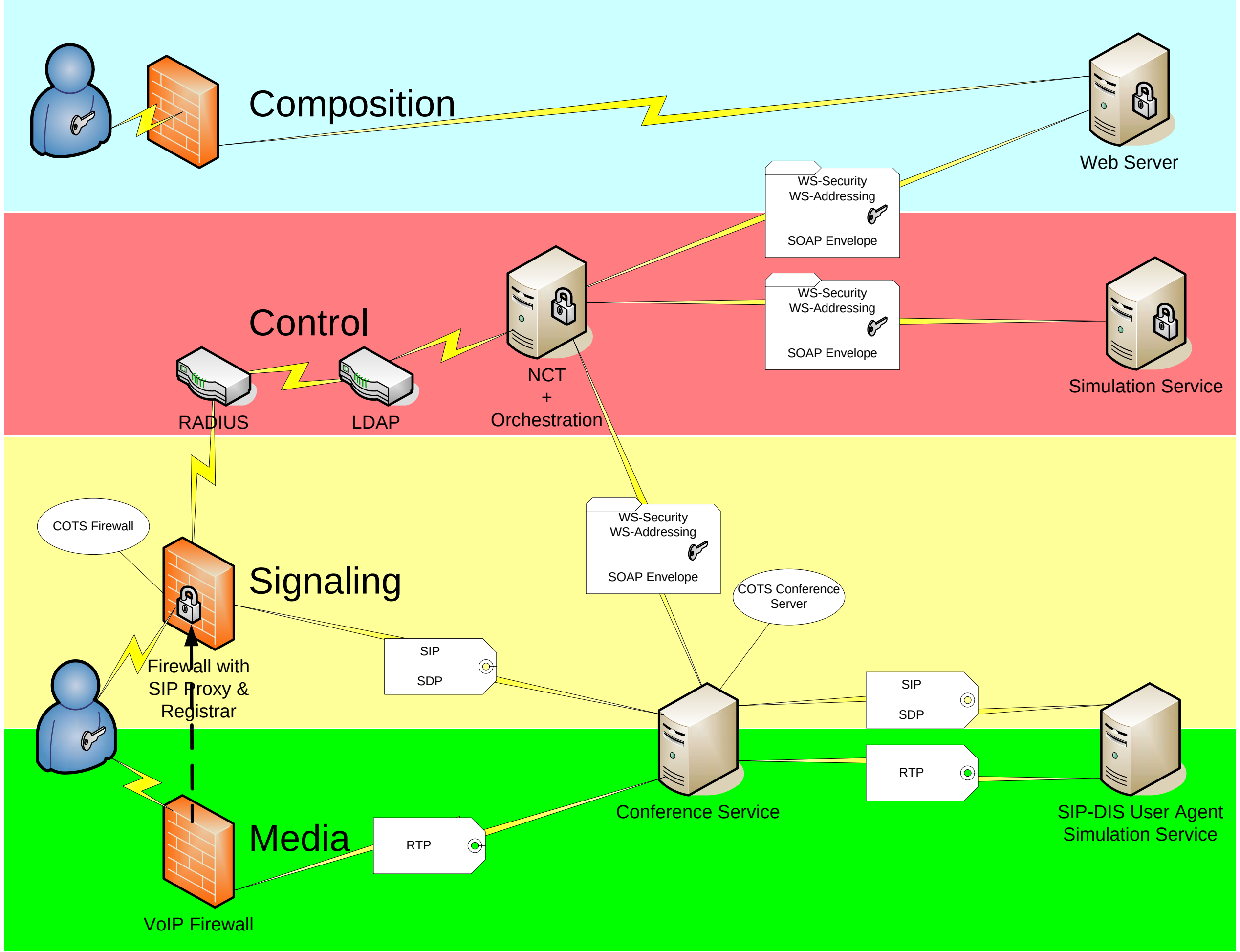
Dynamic Distributed Network IA

Gestalt

Single Enclave View

External Web Browser

External SIP User Agent



Questions?

Scott Holben sholben@gestalt-llc.com

Gestalt, LLC
9432 Baymeadows Road Suite 155
Jacksonville, FL 32256
904-899-0290 x1702