Session 16545: Secure Hybrid Computing: z to Mobile Implementation plus Analytics

Zero Latency Enterprise (ZLE) for Cloud Analytics Mobile Social (CAMSS) with "Need to Know" and solid end to end Security Underpinning

George Thompson, IBM Infrastructure Architect *gthompsn@us.ibm.com*
Jeff Beck, IBM IT Architect *jbeck1@us.ibm.com*

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence**.

SHARE in Seattle 2015

New Model of Hybrid Computing…

- Move the application to the data (no longer Client Server Model)
- System of Record (large database for transactional access with all data types) for OLTP, ANALYTICS, WAREHOUSE, COGNITIVE, BIG DATA
  - This is still the primary “ingest” mechanism but Real Time Single Version of Truth for all access solutions
- System of Engagement is the “new access method”
  - Social, multimedia, multiple data sources
- Data can be presented on a “need to know” basis
  - Only what user is allowed to see
  - May not know that some data will even exist
- Don’t move data to the end user “Hotel California”
  - Show them the results via distributed presentation
  - Limits data loss/theft at the end user level
  - It can be moved closer via managed replica’s or proxy servers

New Model of Hybrid Computing

- The “System” (operating system and database) becomes responsible for security of the data
  - The security administrator and database administrator can collaborate to define and implement the “compartments” for data isolation
  - Applications wouldn’t need to modify database calls to include WHERE security processing logic as the System will handle that
  - This can reduce development costs as mistakes may be eliminated
  - Built in EAL5+ Security RACF, PKI, H/W Cryptography, SSL/TLS, ICSF, MLS

- Communications architecture is critical success
  - VPN and IPSec is critical

- Shared authentication is mandatory
  - Registration and enrollment, audit, access control

Hybrid heterogeneous delivery eliminates boundaries for CAMSS with advanced scale, availability, performance, RAS & zero latency

- Advanced Virtualization for Cloud, scalability, resource sharing, cost take-out
- Advanced Accelerators including specialty engines, WLM, SDE
- Advanced Server CPU Memory Network and I/O….eliminate latency and increase performance

  ((CPU 5.5 GHz Specialty Engines SMT & Multi Tenancy Execution, HPC,Four Level Cache, Transactional Memory on Chip, Flash, RDMA, ROCE, Hipersockets, OSA, SAPs, CAPI, FGPA))
- Advanced Cloud and Interoperability between ALL Clouds
- Advanced Development - Open Source and Traditional Access operability for engagement
- Advanced Mobile and Web engagement
- Advanced Analytics with Advanced Data Management ECM Archival
- Advanced Social Media solutions modeling tracking dissemination
- Advanced Ingest Streams for Standard and Social ingest
- Advanced Security EAL5+ with solid end to end deployment
- Advanced Storage extreme bandwidth: Flash, zEDC
- Advanced Resiliency Scalability, HA, Backup/Recovery, DR, RAS, CBU, COD, P/U Outage
- Advanced Infrastructure flexibility for Agile development Dev/Ops BlueMix, SoftLayer, etc.
- Advanced Middleware solutions providing services to client software applications

“Need to Know” DB2 Labeled Security

REQUIREMENT:

Data shared between people/organizations with different "need to know"

Original View: Suppliers could see each other’s data

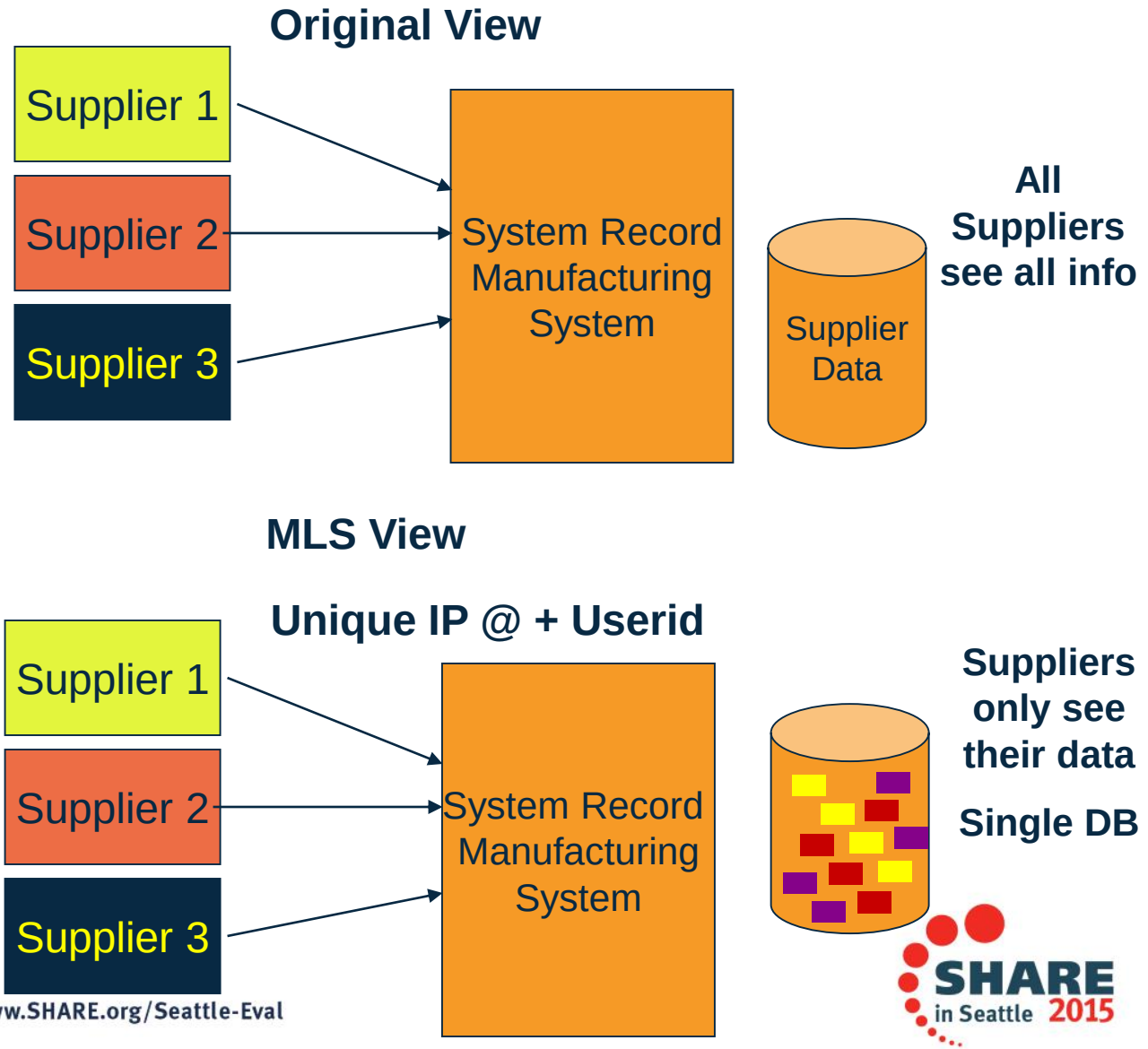
- They could collude and cheat the manufacturer on price
- Or lower their prices to compete against each other

Implementing Labeled Security:

- Additional security information gathered from suppliers during sign on
- Result is suppliers could only see their data
- Manufacturing employees see all data
- No applications were changed

MLS POC Demo Link:

https://www.youtube.com/watch?v=qJBJTAIMSrc



Technical Components – a sample list

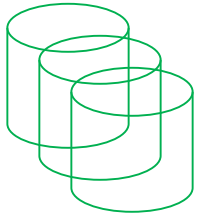
Input device

System(s) of Engagement

Softlayer
WAS
iSPatial
MQ

Managed Replica
Proxy
VDI

System of Record
Insert
Update
Analytics



Raytheon TCS
ME4Sure IBM Apple

Outsourced or Branch Office PCs, Call Centers

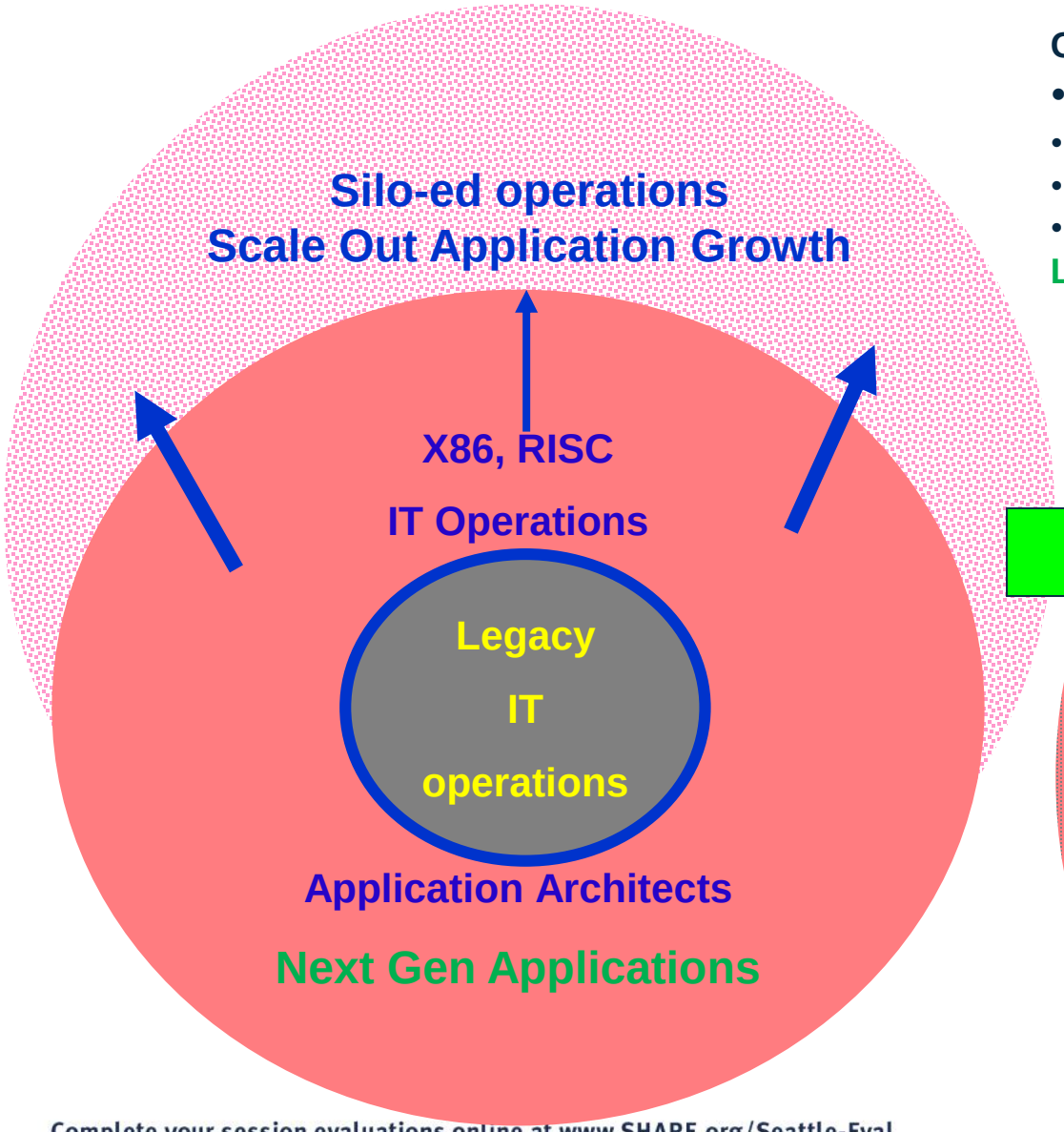
Developer Desktops

Remote / Laptop Users

DB2
Oracle
WAS
Linux
z/VM
IDAA
Secure
MQ
RACF: PKI, MLS
Veristorm zDoop

Power HPC
AIX
GPFS
Watson
Streams
Big Insights
Infosphere
Analytics
Cognos SPSS
Social

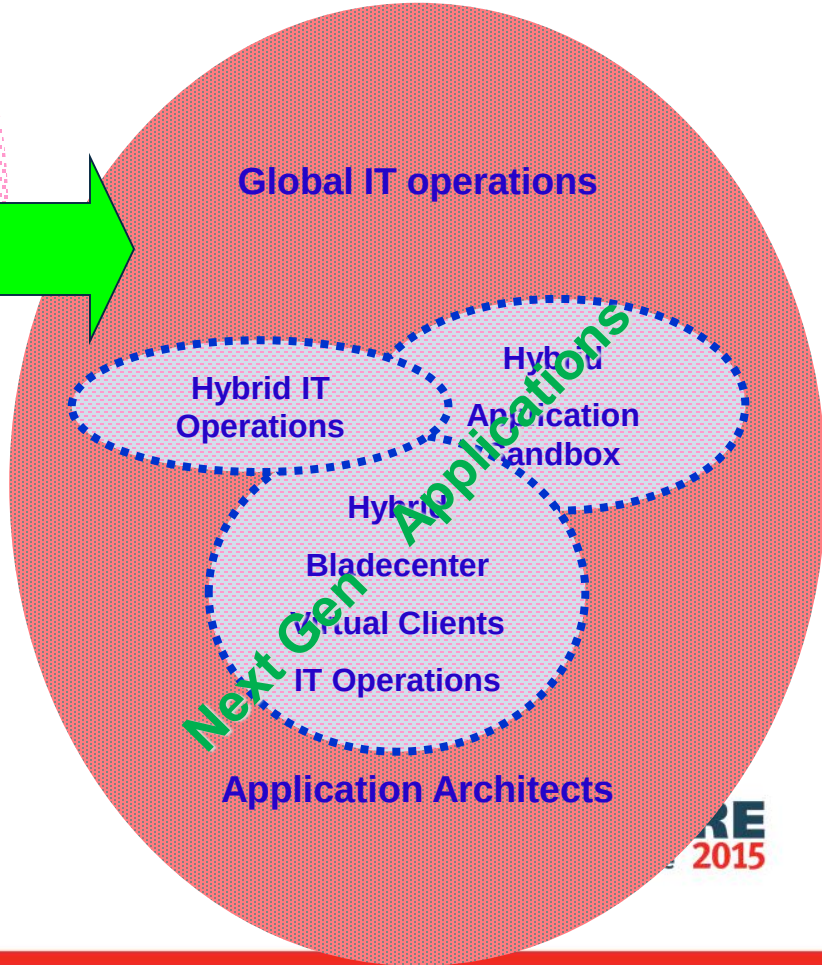
IT Management Trends are changing



Global Business Responsibilities

- Governance
- Risk and Compliance
- Business Continuity
- Privacy

Lean and Green



Global IT Opportunities

CLOUD DELIVERY	Hybrid Server consolidation	Hybrid Client consolidation
Business resilience	Help fail over (Disaster Recover) other servers' data	Faster/cheaper recovery for desktop systems
The vault	Enterprise data protected; simplifying Compliance	Enterprise data protected; simplifying Compliance
Business Process Integration	Leveraging web services for application and database access	Leveraging web services for multi channel transformation and applications
Infrastructure Simplification	Manpower, energy, floor space savings	Manpower, energy, floor space savings
Virtualization	Many server images in a single machine	Many client images in a single machine
Appl Development	Target Deployment platform	Target Development platform

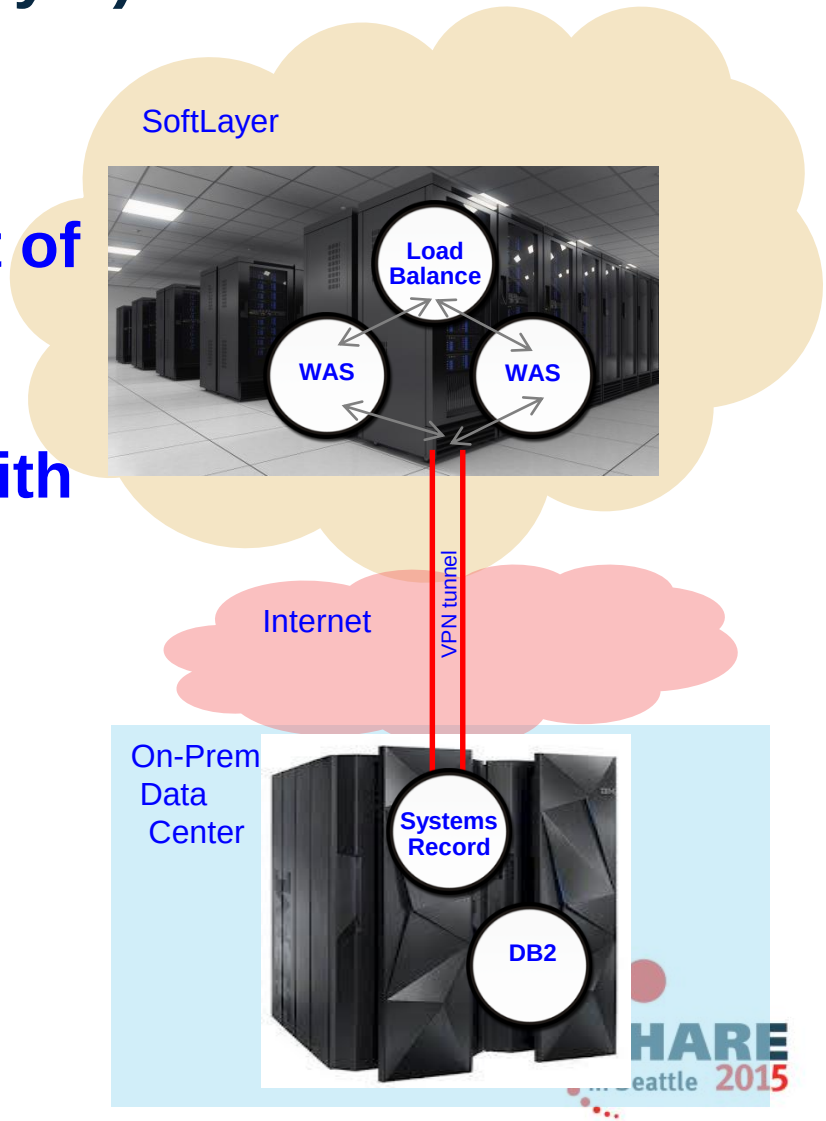
The Hybrid Server and Client are weapons, use them wisely

Cultivating growth opportunities while taking out costs

Hybrid Cloud Enterprise Architecture: Overview (System z and SoftLayer)

Hybrid Architecture provides best of both worlds

Secure Transactions combined with the dynamic of Cloud



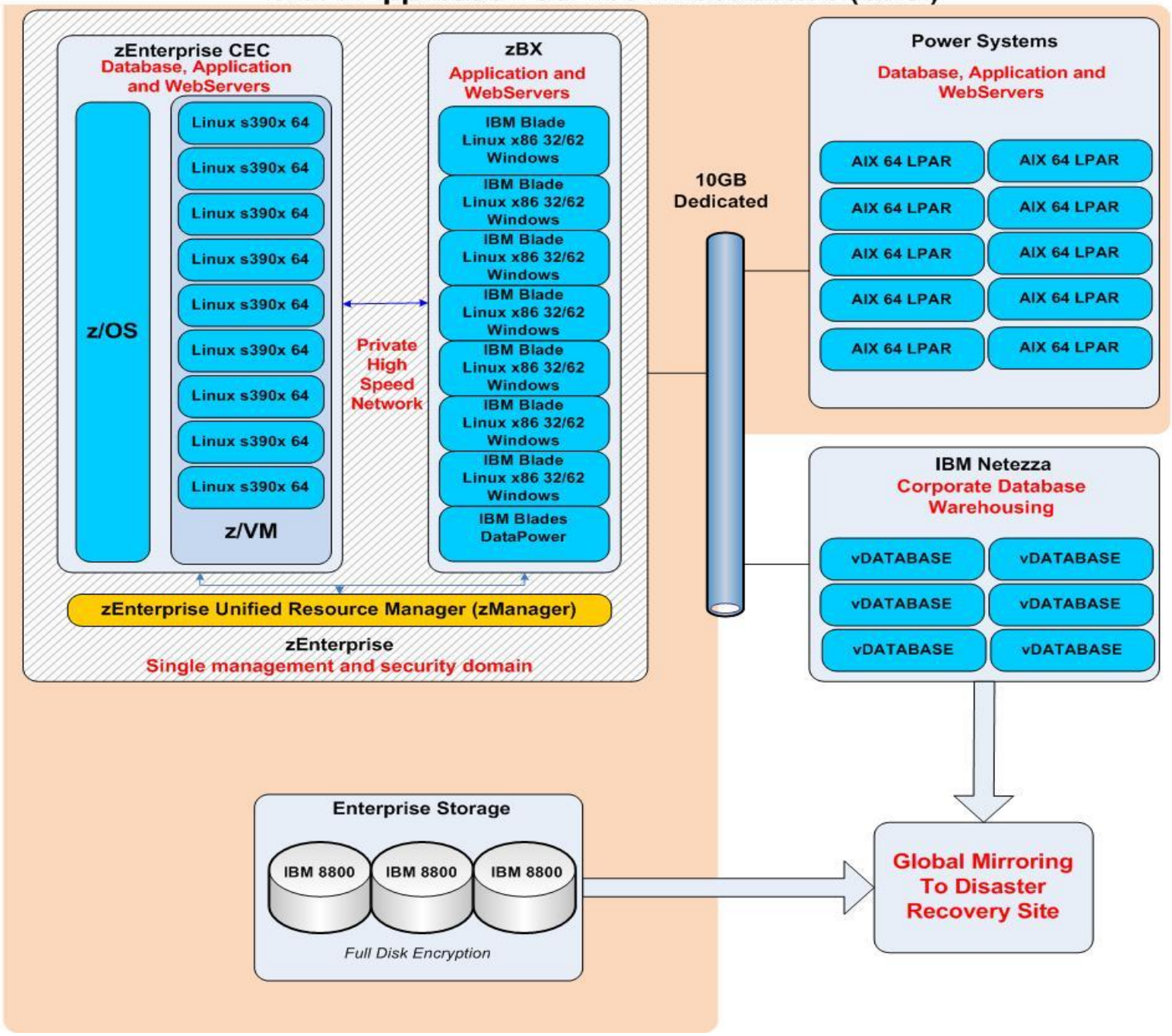
Cloud Application Service Infrastructure ("CASI")

- "CASI" is a hybrid hardware infrastructure designed to allow for the deployment of applications using a Fit-for-Purpose architecture approach.
  - "CASI" infrastructure consists of:
    - z Systems (z/OS and RedHat Linux on z Systems)
    - Power Systems (AIX)
    - System x via zBX (Windows and RedHat Linux on x86)
    - WebSphere DataPower via zBX
    - Netezza (Data Warehousing)
    - 10GbE Layer 3 switches
- Developed by the Agency Enterprise Server Division (AESD)
- The multiple hardware platforms allow for the deployment of application components based on an applications' specific requirements:
  - Most applications are 3-tiered: HTTP web server -> Application server -> Database
  - Example: HTTP server/x86 specific components on x86 Windows or Linux -> Application server (WAS) on Power Systems -> Oracle or DB2 Database on Linux on z Systems
- 10GbE L3 switches allow for private data communication between all "CASI" systems without the need for routing or firewalls (i.e. Layer 2 networking), or a single router hop between systems (Layer 3 networking).
- "CASI" leverages existing Disaster Recovery infrastructure via GDPS/XRC to provide recovery for new and existing applications.

"CASI" currently supports:

- All major hardware architectures
  - X86, s390x, RISC
  - Run application components on native hardware architecture
  - Reduced need to rewrite code for easier application porting
- High-speed, private 10GbE network
  - Co-locates application to data sources
  - Eliminates need for firewalls within "CASI" infrastructure
- z/VM, PowerVM, KVM hypervisors
- DR solution via GDPS/XRC
  - Most “CASI” applications
  - End-user piece of mind
- Quick deployment of virtual servers and hardware resources
  - All "CASI" platforms are 100% virtualized
  - Most "CASI" client requests fulfilled within hours or a few days

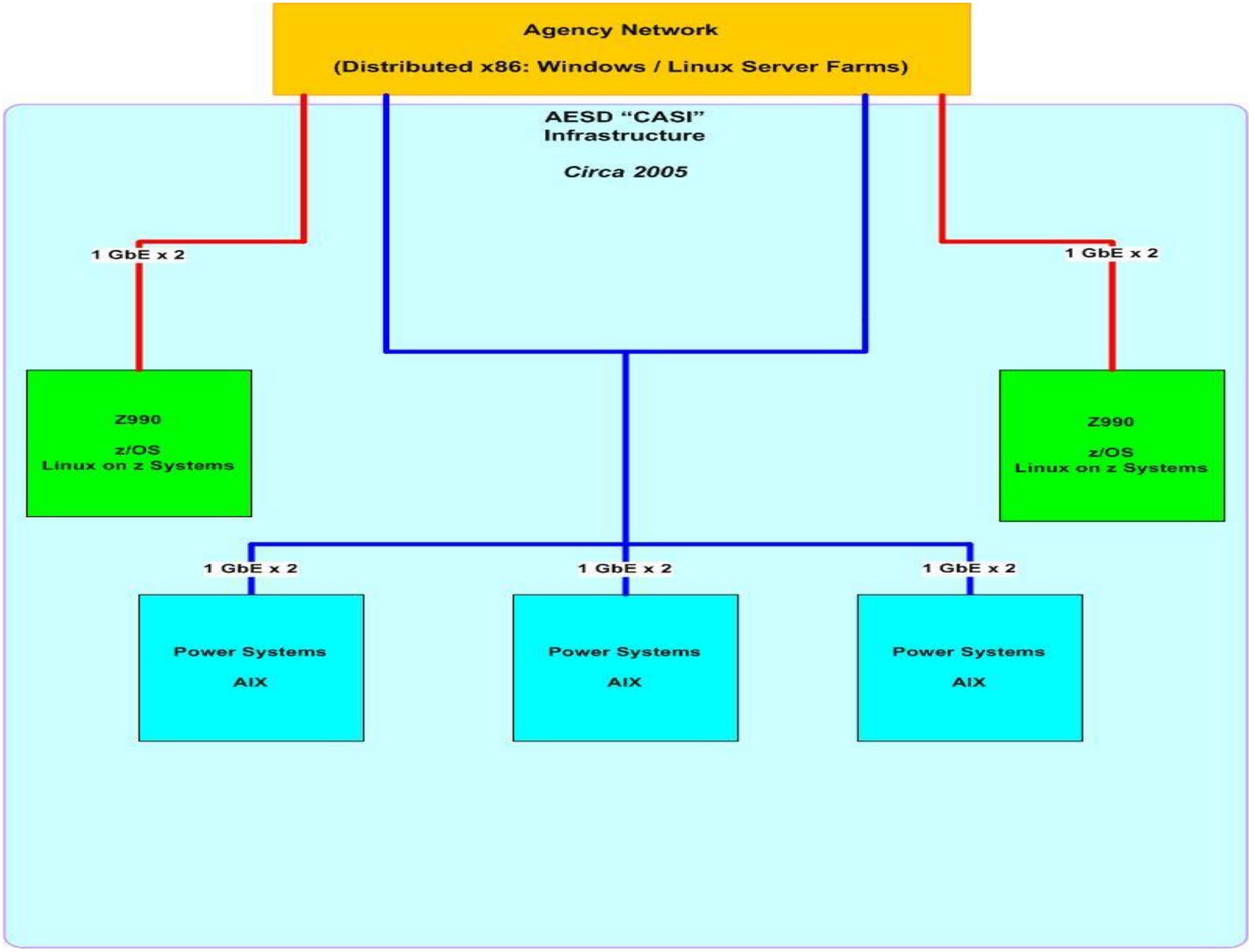
"Cloud Application Service Infrastructure (CASI)"



AESD's "CASI" service started with existing Mainframe and Power Systems infrastructure

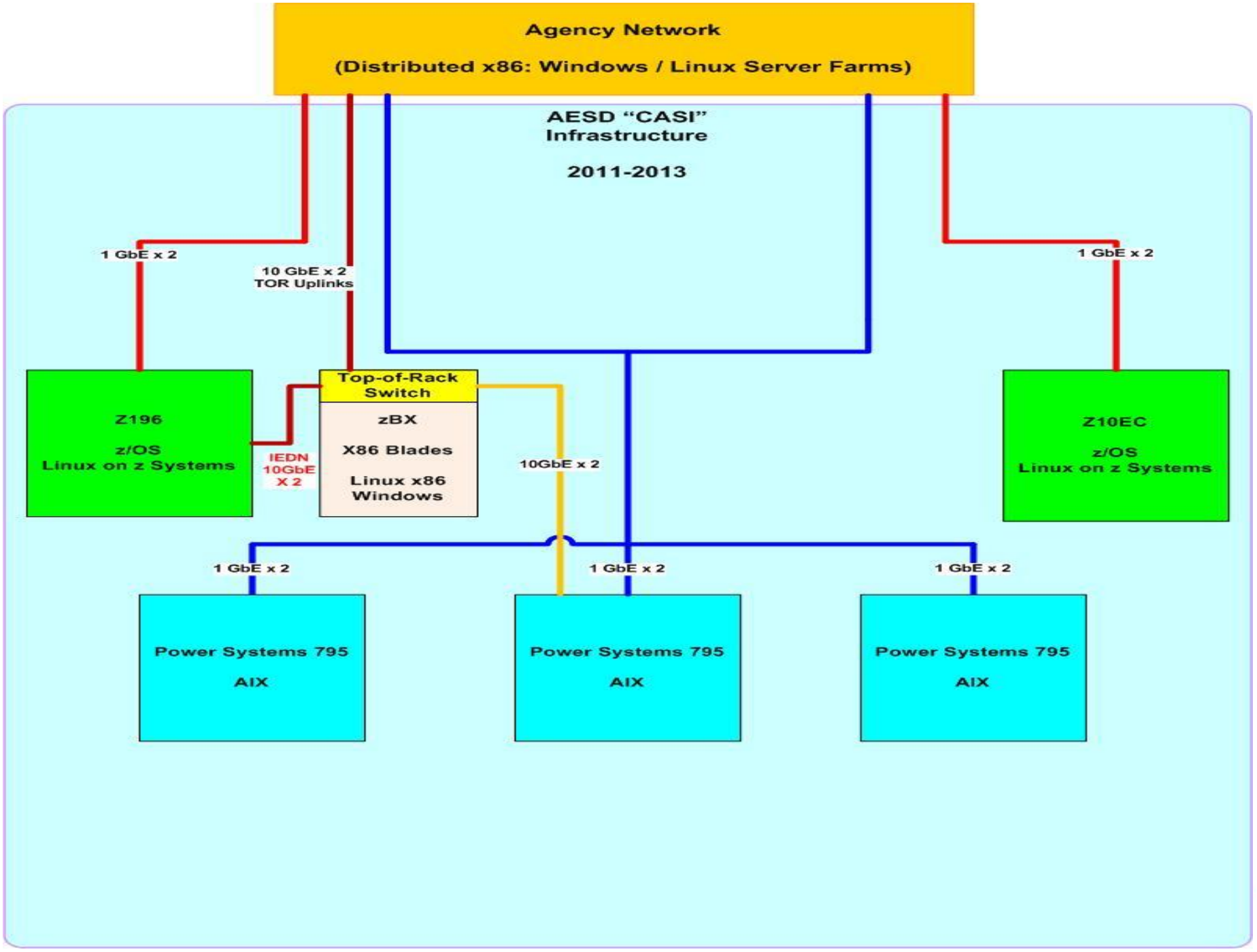
- 2004-2005: Evaluated Linux on z Systems using IFLs
- Advertised new Linux on z Systems service to end users throughout the agency
- Ability to host database and web service applications with various SLA's: Production and DEV environments
- Provided disaster recovery for hosted applications

- Limitations:
  - Applications must be certified to run on Linux on z Systems or Power Systems
  - Limited bandwidth and IP addresses


Agency Network
(Distributed x86: Windows / Linux Server Farms)
AESD "CASI"
Infrastructure
Circa 2005
1 GbE x 2
1 GbE x 2
Z990
z/OS
Linux on z Systems
Z990
z/OS
Linux on z Systems
1 GbE x 2
1 GbE x 2
1 GbE x 2
Power Systems
AIX
Power Systems
AIX
Power Systems
AIX

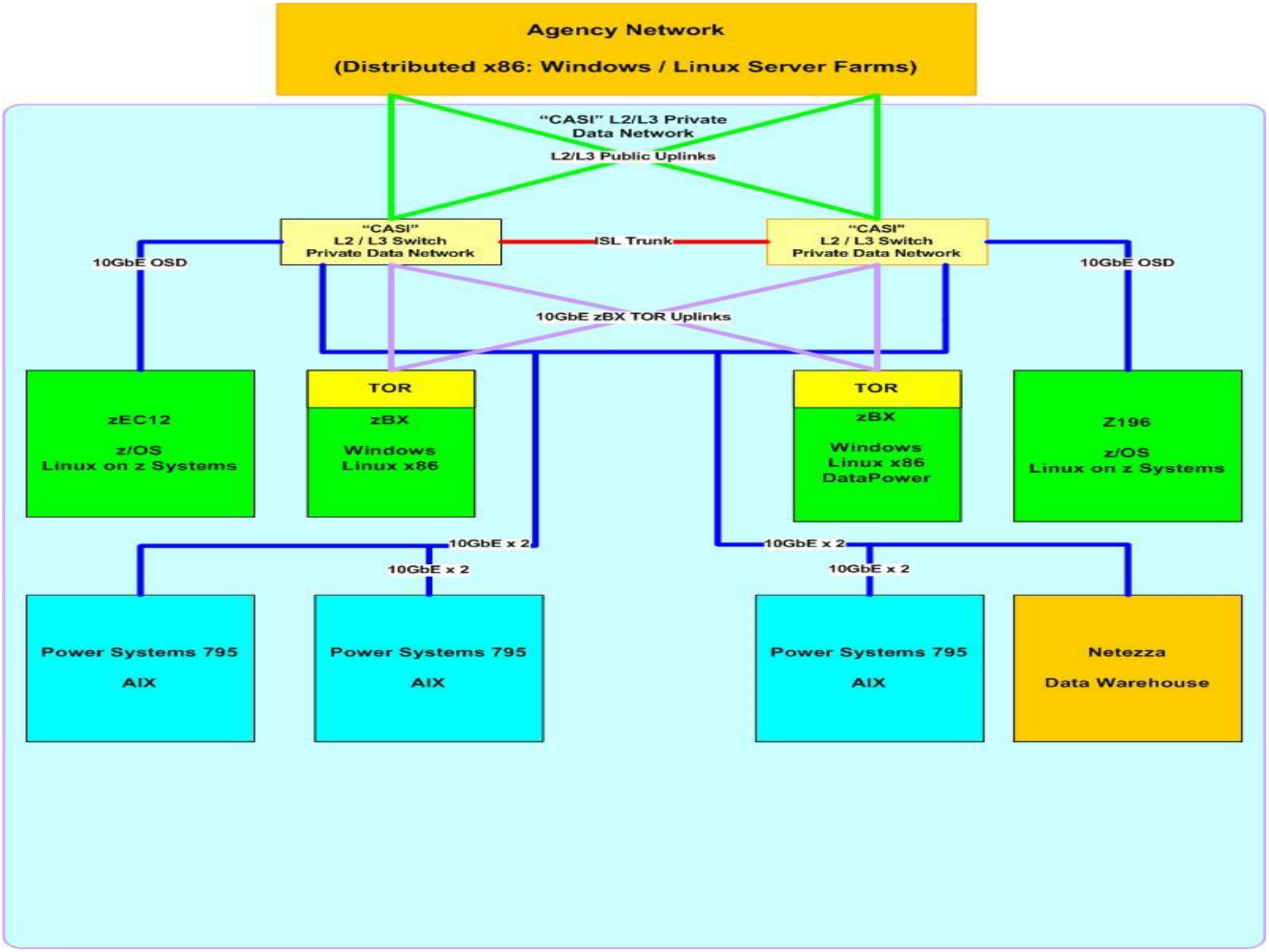
IBM Announces zEnterprise in July 2010

- zEnterprise 196
- zEnterprise BladeCenter Extension (zBX)
  - Ability to host native x86 applications on blades
  - Tightly integrated with z Systems security and long-standing operational policies
  - Communication between zBX and z CEC occur over secure, private high-speed network (IEDN)
  - Mainframe viewed as a “Fit-for-Purpose” cloud server
- 2011: AESD acquires zBX and x86 blades to expand "CASI" capabilities:
  - Multi-tier applications across "CASI" platforms for enhanced qualities of services
  - End-user applications communicate fast and securely over zEnterprise IEDN network
- Limitations:
  - Private, high-speed networking limited only to zEnterprise, not external platforms (i.e. Power Systems)


Agency Network
(Distributed x86: Windows / Linux Server Farms)
AESD "CASI"
Infrastructure
2011-2013
1 GbE x 2
10 GbE x 2
TOR Uplinks
1 GbE x 2
Z196
z/OS
Linux on z Systems
IEDN
10GbE
X 2
Top-of-Rack
Switch
zBX
X86 Blades
Linux x86
Windows
10GbE x 2
Z10EC
z/OS
Linux on z Systems
1 GbE x 2
1 GbE x 2
1 GbE x 2
Power Systems 795
AIX
Power Systems 795
AIX
Power Systems 795
AIX

Future AESD outlook for “CASI”

- Implement Layer 3 switches to provide 10GbE network backbone across all "CASI" platforms
- Provide private VLANs to end-users that expand across platforms
  - Limit amount of public IP addresses required for applications
  - Ability to host hundreds or more applications
- Expand service offerings using hardware appliances and software solutions
- Consider multi-vendor hardware offerings
  - Architecture designed to be open


Agency Network
(Distributed x86: Windows / Linux Server Farms)
"CASI" L2/L3 Private Data Network
L2/L3 Public Uplinks
"CASI" L2 / L3 Switch Private Data Network
ISL Trunk
"CASI" L2 / L3 Switch Private Data Network
10GbE OSD
10GbE OSD
10GbE zBX TOR Uplinks
zEC12
z/OS
Linux on z Systems
TOR
zBX
Windows
Linux x86
TOR
zBX
Windows
Linux x86
DataPower
Z196
z/OS
Linux on z Systems
10GbE x 2
10GbE x 2
10GbE x 2
10GbE x 2
Power Systems 795
AIX
Power Systems 795
AIX
Power Systems 795
AIX
Netezza
Data Warehouse

THANK YOU

George Thompson
IBM Infrastructure Architect
gthompsn@us.ibm.com

Jeff Beck
IBM Client IT Architect
jbeck1@us.ibm.com