zEnterprise System – Network Architecture and Virtualization Overview (Part 1)

Gus Kassimis - kassimis@us.ibm.com
IBM Raleigh, NC, USA

Session: 9245
Tuesday August 9 - 11:00 PM to 12:15 PM
Trademarks, notices, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DataPower®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e-business(logo)®
- ESCON®
- FICON®
- GDDM®
- GDPS®
- Geographically Dispersed Parallel Sysplex
- HiperSockets
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM eServer
- IBM (logo)®
- IBM®
- IBM zEnterprise™ System
- IMS
- InfiniBand®
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment®
- MVS
- MGSeries®
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/390®
- Operating System/400®
- Parallel Sysplex®
- POWER®
- POWER7®
- PowerVM
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x®
- System z®
- System z9®
- System z10
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9®
- z10 BC
- z10 EC

* All other products may be trademarks or registered trademarks of their respective companies.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both.
- Cell Broadband Engine is a trademark of Sony Computer Ente...
zEnterprise System - network architecture and virtualization overview (Part 1)

<table>
<thead>
<tr>
<th>Session number:</th>
<th>9245</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and time:</td>
<td>Tuesday, August 9th, 2011: 11:00 AM-12:15 PM</td>
</tr>
<tr>
<td>Location:</td>
<td>Europe 10 (Walt Disney World Dolphin )</td>
</tr>
<tr>
<td>Program:</td>
<td>Communications Infrastructure</td>
</tr>
<tr>
<td>Project:</td>
<td>Communications Server</td>
</tr>
<tr>
<td>Track:</td>
<td>Tracks: Capitalizing on zEnterprise, Network Support and Management and Virtualization of Existing Resources</td>
</tr>
<tr>
<td>Classification:</td>
<td>Technical</td>
</tr>
<tr>
<td>Speaker:</td>
<td>Gus Kassimis, IBM</td>
</tr>
<tr>
<td>Abstract:</td>
<td>IBM's zEnterprise System provides the ability to consolidate multi tier and multi architecture workloads. This session will describe the networking architecture for the zEnterprise System, including an in depth review of the new Intra-Ensemble Data Network (IEDN) that provides the internal connectivity for this new system and how it relates to existing System z networking technologies. This session will also describe the IBM zEnterprise Unified Resource Manager advanced network virtualization functions that provide management of this network, including the ability to define multiple virtual networks for workload isolation.</td>
</tr>
</tbody>
</table>
Related zEnterprise Networking Sessions

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Title</th>
<th>Date and Time</th>
<th>Location</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>(9245): 9245</td>
<td>zEnterprise System - Network Architecture and Virtualization Overview (Part 1)</td>
<td>This session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(9246): 9246</td>
<td>zEnterprise System - z/OS IEDN network design and implementation (Part 2)</td>
<td>Tuesday, August 9, 2011: 1:30 PM-2:30 PM</td>
<td>Europe 10 (Walt Disney World Dolphin)</td>
<td>Gus Kassimis (IBM Corporation)</td>
</tr>
<tr>
<td>(9534): 9534</td>
<td>zEnterprise System - Secure Networking with the zEnterprise Ensemble (Part 3)</td>
<td>Tuesday, August 9, 2011: 3:00 PM-4:00 PM</td>
<td>Europe 10 (Walt Disney World Dolphin)</td>
<td>Gwen Dente (IBM Corporation)</td>
</tr>
</tbody>
</table>

Note that there are many other sessions at this SHARE focusing on various aspects of zEnterprise
- Sessions listed under “Capitalizing on zEnterprise” Track
Agenda

- Brief background
- zEnterprise Node Physical Infrastructure
- Communications within the Ensemble
- Network and OSA Types and Attributes
- External Network Access
- Network Virtualization Management
- Provisioning Virtual Networks
- Network Access Control and Security

Disclaimer: All statements regarding IBM future direction or intent, including current product plans, are subject to change or withdrawal without notice and represent goals and objectives only. All information is provided for informational purposes only, on an “as is” basis, without warranty of any kind.
Business processes and the applications that support them are becoming more service oriented, modular in their construction, and integrated.

The components of these services are implemented on a variety of architectures and hosted on heterogeneous IT infrastructures.

Approaches to managing these infrastructures along the lines of platform architecture boundaries cannot optimize: alignment of IT with business objectives; responsiveness to change; resource utilization; business resiliency; or overall cost of ownership.

Customers need better approach: The ability to manage the IT infrastructure and Business Application as an integrated whole.
It’s ALL about the workload…

Subset representing a specific workload

- Connected
- Integrated
- Flexible, Dynamic, and Responsive
- Aligned with Business Objectives

© 2011 SHARE and IBM Corporation
It’s ALL about the workload…

Unified Resource and Workload Management

zBladeCenter Extension

zEnterprise z196

Private, secure networks

Firewall

Web Servers

Application Servers – z/OS – zLinux - AIX

Database Server – z/OS

Storage

☑ Connected
☑ Integrated
☑ Flexible, Dynamic, and Responsive
☑ Aligned with Business Objectives

zEnterprise System
IBM zEnterprise System – Best in Class Systems and Software Technologies

A system of systems that unifies IT for predictable service delivery

Unified management for a smarter system: zEnterprise Unified Resource Manager

- Unifies management of resources, extending IBM System z® qualities of service end-to-end across workloads
- Provides platform, hardware and workload management
- Also known as zManager

Scale out to a trillion instructions per second: IBM zEnterprise BladeCenter® Extension (zBX)

- Selected IBM POWER7® blades and IBM System x® Blades for tens of thousands of AIX®, Linux, and Windows® applications
  - Linux for system x 3Q2011
  - Microsoft Windows® 4Q2011
- High performance optimizers and appliances to accelerate time to insight and reduce cost
  - DataPower XI50z
  - IBM Smart Analytics Optimizer
- Dedicated high performance private network

The world’s fastest and most scalable system: IBM zEnterprise™ 196 (z196)

- Ideal for large scale data and transaction serving and mission critical applications
- Most efficient platform for Large-scale Linux® consolidation
- Leveraging a large portfolio of z/OS® and Linux on System z applications
- Capable of massive scale up, over 50 Billion Instructions per Second (BIPS)

1 All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice.
... and the Value Extends To Heterogeneous Platforms …

*IBM zEnterprise BladeCenter Extension (zBX)*

**Machine Type: 2458 – Model 002**

- Integrated IBM Certified Components driven by System z order
  - Standard parts – TOR switch, BladeCenter Chassis, Power Distribution Units, Optional Acoustic Panels

- **System z support**
  - Problem reporting, hardware and firmware updates

- **Expanding operating system support for zEnterprise**
  - AIX, Linux on System x, Microsoft Windows¹ on System x

- **Simplified management**
  - Improved time to install and implement new applications
  - Central point of management for heterogeneous workloads
  - No change to applications

---

**Optimizers**

- IBM Smart Analytics Optimizer
- WebSphere® DataPower® appliance

**Select IBM Blades**

- BladeCenter PS701 Express
- System x HX5 (7873)

---

| One to four – 42u racks – capacity for 112 blades |
| No System z software running in zBX – Passport Advantage software licensed to blades |
| No MIPS/MSU rating |
| Configured for high availability |
| Optional rear door heat exchanger |

---

¹ All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represents goals and objectives only.
zBX … Infrastructure to Support More Resources

- **zBX houses the multiplatform solutions key to the zEnterprise System.**
  - Optimizers that are dedicated to workloads.
    - IBM Smart Analytics Optimizer and *IBM WebSphere DataPower Integration Appliance XI50z for zEnterprise*
    - Closed environments with hardware and software included in solution
    - Individualized tools for sizing and customizing – dependant on the optimizer
  - Select IBM POWER7 and System x blades – running *any* application supported by the operating system installed on the blade – with no change.
  - Mix and match Optimizer and select general purpose POWER7 and System x blades in the same rack.
  - zBX is a System z machine type for integrated fulfillment, maintenance, and support

- **Secure network connection between zBX and z196 for data and support.**
  - Fast 10 Gb Ethernet connection to the data
  - Less latency – fewer ‘hops’ to get to the data
  - Private, isolated network - potential to eliminate requirement for encryption / firewalls
  - Traffic on user networks not affected.

- **Sharing of resources – up to eight z196 servers can attach to the zBX and have access to solutions**

- **Configuration, support, monitoring, management – all by Unified Resource Manager**

---

1 All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represents goals and objectives only.
IBM POWER7 and System x Blades

General purpose processors under one management umbrella

What is it?
The zBX infrastructure can host select IBM POWER7 and System x blades. Each blade comes with an installed hypervisor that offers the possibility of running an application that spans z/OS, Linux on System z, AIX on POWER®, Linux on System x, or Windows® (SOD)¹ - but have it under a single management umbrella.

How is it different?

- **Complete management:** Advanced management brings operational control and cost benefits, improved security, workload management based on goals and policies.

- **Virtualized and Optimized:** Virtualization means fewer resources are required to meet peak demands with optimized interconnection.

- **Integrated:** Integration with System z brings heterogeneous resources together that can be managed as one.

- **Transparency:** Applications that run on the list of supported operating systems for the zBX can be deployed in the zBX blades without changes to deployed guest images.

- **More applications:** Brings larger application portfolio to System z.

For more details on System x Blades supported in the zBX see:

¹ All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represents goals and objectives only.
IBM Smart Analytics Optimizer
Capitalizing on breakthrough technologies to accelerate business analytics

What is it?
The IBM Smart Analytics Optimizer is a workload optimized, appliance-like, add-on, that enables the integration of business insights into operational processes to drive winning strategies. It accelerates select queries, with unprecedented response times.

How is it different?
- **Performance**: Unprecedented response times to enable 'train of thought' analyses frequently blocked by poor query performance.
- **Integration**: Connects to DB2® through deep integration providing transparency to all applications.
- **Self-managed workloads**: Queries are executed in the most efficient way.
- **Transparency**: Applications connected to DB2, are entirely unaware of IBM Smart Analytics Optimizer.
- **Simplified administration**: Appliance-like hands-free operations, eliminating many database tuning tasks.

Faster insights for enabling new opportunities
IBM WebSphere DataPower Integration Appliance XI50z for zEnterprise

Purpose-built hardware for simplified deployment and hardened security

What is it?

The IBM WebSphere DataPower Integration Appliance XI50z for zEnterprise can help simplify, govern, and enhance the security of XML and IT services by providing connectivity, gateway functions, data transformation, protocol bridging, and intelligent load distribution.

How is it different?

- **Security:** Coordinated network configuration management with the zEnterprise Unified Resource Manager which includes VLAN support for enforced isolation of network traffic with secure private networks.

- **Improved support:** Monitoring of hardware with “call home” for current/expected problems and support by System z Service Support Representative.

- **System z packaging:** Increased quality with pre-testing of blade and zBX. Upgrade history available to ease growth. Guided placement of blades to optimize.

- **Operational controls:** Monitoring rolled into System z environment from single console. Time synchronization with System z. Consistent change management with Unified Resource Manager.

1 Announced on February 15, 2011


© 2011 SHARE and IBM Corporation
... Value Made Possible By the Unified Resource Manager

**Simplified installation of hypervisors**
- Gain significant time to market with improved speed of deployment
- Save time, cost and simplify asset management
- Decrease problem determination and resolution time for cross-platform resources
- Improve and simplify cross-platform availability procedures
- Enable broader and more granular view of resource consumption

**Factory installed and configured network**
- Improved network security with lower latency, less complexity, no encryption/decryption

**Simplified energy management**
- Energy cost savings

**Virtual Servers**
- Manage and control communication between virtual server operating systems and the hypervisor.
- Allow critical workloads to receive resources and priority based on goal-oriented policies established by business requirements
- Smart business adjustments based on workload insight
- Provide deep insight into how IT resources are being used

**Hypervisors**
- Gain flexibility, consistency and uniformity of virtualization
- Provide the business with faster time to market
- Simplified network management for applications

**Networks**
- Gain significant time to market with improved speed of deployment
- Simplified installation of hypervisors
- Factory installed and configured network
- Improved network security with lower latency, less complexity, no encryption/decryption

**Performance**
- Monitor resource use within the context of a business workload
- Define workloads and associated performance policies

**Operations**
- Monitor and control communication between virtual server operating systems and the hypervisor.
- Manage and control communication between virtual server operating systems and the hypervisor.
- Save time, cost and simplify asset management
- Decrease problem determination and resolution time for cross-platform resources
- Enable broader and more granular view of resource consumption

**Energy**
- Allow critical workloads to receive resources and priority based on goal-oriented policies established by business requirements
- Smart business adjustments based on workload insight
- Provide deep insight into how IT resources are being used

**Network Management**
- Management of virtual networks including access control
- Single view of virtualization across platforms
- Ability to deploy multiple, cross-platform virtual servers within minutes
- Management of virtual networks including access control

**Virtual Server Lifecycle Management**
- Wizard-driven management of resources in accordance with specified business service level objectives
- HMC provides a single consolidated and consistent view of resources
- Monitor resource use within the context of a business workload
- Define workloads and associated performance policies

**Workload Awareness and Platform Performance Management**
- Gain flexibility, consistency and uniformity of virtualization
- Provide the business with faster time to market
- Simplified network management for applications
zEnterprise Networking Value Points

- **Network Simplification (“Network in a Box”)**
  - Single physical network and zBX “package” (physical network integration)
  - Central point of Management (Unified Resource Manager via the HMC/SE)
  - Reduced network path length; reduced number of hops

- **Secure communications**
  - Physical security (internal / dedicated network equipment)
  - Logical security (controlled access)
  - Network Virtualization and Isolation

- **High Availability**
  - Redundant network hardware
  - Logical failover

- **Unique System z QoS**
  - Isolated / dedicated equipment
  - Special purpose dedicated data network & OSA-Express (potential for reduced network encryption)
IBM zEnterprise System Overview

Connecting the pieces with zManager (aka. Unified Resource Manager)!

1 All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represents goals and objectives only.
IBM zEnterprise node – the networks

**Intra Ensemble Data Network (IEDN)**
- OSA-E3 1000Base-T ports: Cables are 3.2 meters long from OSM to BPH in CEC and 26 meters from BPH to TOR.

**Intra Node Management Network (INMN)**
- OSA-E3 10 GbE ports: Cables are maximum of 26 meters long from zEnterprise to TOR & 10km long-reach (or up to 300m short-reach) to another zBX.

**Private system control network**

**Customer managed data networks**

**Customer managed management network**

**BladeCenter rack**
**zEnterprise ensemble**

**zEnterprise Ensemble**
A collection of one or more zEnterprise Nodes (including any optionally attached zBX) that are managed as a single logical virtualized system by the zManager using a Hardware Management Console (HMC).

**Ensemble Member**
A zEnterprise node that has been added to an ensemble using the HMC.

**Intra Ensemble Data Network (IEDN)**
Intra ensemble data network

Intra Ensemble Data Network - key attributes:

1. Single dedicated physical / flat layer 2 10GbE network
2. Comprised of IBM zEnterprise (redundant) equipment (no external / customer hardware)
3. Can span nodes (can be shared by all co-located nodes within the Ensemble)
4. No layer 3 IP Routing required to communicate within the Ensemble
5. IP addresses (IPv4 or IPv6) are customer controlled and provisioned
6. MAC addresses (prefixes) are provisioned / coordinated by zManager (HMC)
7. Access to the network is controlled by the zManager (HMC) via SE via OSX, hypervisors and physical switches
8. Virtual servers can be isolated into multiple groups on the physical network by defining multiple virtual networks (multiple VLANs) based on workloads and other isolation requirements
IBM zEnterprise – OSA and Network Types

zEnterprise node

LP1 z/OS
LP2 z/OS
LP3 z/OS
LP4 z/OS
LP5 z/VM

OSD
OSX
OSM

BC1
BC2
BC3

TOR
TOR

Intra Ensemble Data Network (IEDN) OSA OSX 10 GbE

Intra Node Management Network (INMN) OSA OSM 1 GbE (1000BaseT)

Customer external data network access OSA OSD

Firewall

Customer external data network

IEDN may extend to other zEnterprise nodes within an ensemble

z196

zBX

© 2011 SHARE and IBM Corporation
External Network Access – Option 1 – System z (LP) IP Router

Route via OSD and one or more z/OS images

Firewall

Customer external data network

 TOR

BC1 ESM

BC2 ESM

BC3 ESM

TOR

ESM

TOR

ESM

ESM

ESM

ESM

HMC

SE

OSD

OSX

OSM

LP1 z/OS

LP2 z/OS

LP3 z/OS

LP4 z/OS

LP5 z/VM

VS1

VS2

VS3

VS4

z/VM virtual switch

z196

zBX

HMCHMC

z/VM virtual switch

z/VM virtual switch
External Network Access – Option 2 – External IP Router

zEnterprise node

And to System z LPARs
Must be a layer 3 router!

Firewall

Customer external data network

Extend IEDN to external router and route via TOR

LP1 z/OS
LP2 z/OS
LP3 z/OS
LP4 z/OS
LP5 z/VM
VS1
VS2
VS3
VS4
z/VM virtual switch

z196

TOR
BC1
BC2
BC3

TOR
zBX

ESM
ESM
ESM
ESM
ESM
ESM

HMC
What is a Virtual LAN (a VLAN)?

**Wikipedia:**

- A **virtual LAN**, commonly known as a **VLAN**, is a *group of hosts* with a common set of requirements that communicate as if they were *attached* to the same *broadcast domain*, regardless of their physical location.

- A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.

- Network reconfiguration can be done through software instead of physically relocating devices.
z/OS and VLANs

- Depending on switch configuration, the switch may interconnect the VLANs using a layer-3 IP router function.
- The subnets may belong to different routing domains or OSPF areas:
  - Test, production, demo
- The subnets may belong to different security zones:
  - Intranet, DMZ

VLAN is a LAN media virtualization technology that allows multiple independent IP networks (IP subnets) to share one physical media, such as a cable, an adapter, or a layer-2 switch. Connectivity between VLANs is under control of IP routers.
Some basic LAN technology overview

- The LAN infrastructure transports “Frames” between Network Interface Cards (NICs) that are attached to the LAN media (Copper or fiber optic)

- Each NIC has a hardware address
  - A Media Access Control (MAC) address
    - Burned in (world-wide unique by vendors) or alternatively locally administered

- Every frame comes from a MAC and goes to a MAC
  - There are special MAC values for broadcast and multicast frames

- Every frame belongs to the physical LAN or to one of multiple Virtual LANs (VLAN) on the physical LAN
  - A VLAN ID is in the IEEE801.Q header if VLAN technologies are in use

- A frame carries a payload of a specified protocol type, such as ARP, IPv4, IPv6, SNA LLC, etc.

![LAN Frame Diagram]

The VLAN tag (the IEEE801.Q header) is only present if VLANs are used by the network interface.
Virtual Network Concepts – Creating Virtual Networks

The Unified Resource Manager and System zEnterprise leverage VLAN technology in a unique way creating Virtual Networks

– **Step 1.** Create / Define a Virtual Network

“Production Net”
VLAN ID = 300

… from the zManager (HMC)
Virtual Network Concepts – Adding Virtual Servers

... once you have a Virtual Network...

- **Step 2.** add (associate / authorize) Virtual Servers to the Virtual Network

Virtual Networks in the zEnterprise consist of two key properties:

1. VLAN ID (along with an IP subnet)
2. List of Authorized Servers
Deploying a Virtual Network – Example 1

Single Virtual Network, Single IP subnet, and VLAN ID

“Production Net”
VLAN ID = 300

All servers can have a single IP interface and all IP addresses are from the same IP subnet (such as 10.0.1.x/24) Multiple Interfaces may be created for redundancy!
Deploying Multiple Virtual Networks – Example 2 - Isolation

Multiple Virtual Networks, each having unique IP subnets and VLAN IDs

Step 1: Define a “Production Net” VLAN and add virtual servers to it.

Step 2: Define a “Development Net” VLAN and add virtual servers to it.

which isolates “Production Servers” from “Development Servers”
zEnterprise virtualization and network access control

A systems administrator cannot by mistake or deliberately mis-configure a virtual server to use a VLAN to which it is not authorized through the HMC.

zManager pushes virtual network access control information to the node and the SE propagates to control points over the intra node management network (INMN).
Putting It All Together…with secure access control!

Note that all network components are duplicated to provide full redundancy. Redundancy is not shown.

zEnterprise zManager controls network access at the physical and at the virtual switches (hypervisors)!
Use of multiple VLANs on the IEDN – no routing, but “application layer gateways” between VLANs

Virtual servers that act as “application layer gateways” have, under zManager control, access to two VLANs.

These nodes “should” be configured with forwarding disabled. z/OS is by default prevented from routing between IEDN VLANs.
Use of multiple VLANs on the IEDN – Routing between VLANs using an external firewall

TOR, under zManager control, extends the two VLANs to an external firewall.

TOR may optionally also implement MAC filters.

TOR, under zManager control, extends the two VLANs to an external firewall.

TOR may optionally also implement MAC filters.

TOR, under zManager control, extends the two VLANs to an external firewall.

TOR may optionally also implement MAC filters.

TOR, under zManager control, extends the two VLANs to an external firewall.

TOR may optionally also implement MAC filters.
Configuring TOR - External Network Access

Two Use Cases:

1. Non-IEDN CEC access to ISAO blade
2. External IP Router
OSA redundancy and IEDN network bandwidth

- The design of the zEnterprise is such that the use of a dynamic routing protocol on the IEDN, is not needed
- z/OS must be configured to use its existing layer-2 redundancy and availability functions
  - Configure at least two OSX ports to each VLAN
    - Establishing LAN groups where IP addresses move dynamically between the OSX ports in case one of them becomes unavailable
    - Assign VIPA addresses out of the same subnet as the IEDN VLAN
      - ARP processing will be used to control which z/OS LPAR in a Sysplex currently owns a specific Dynamic VIPA address
- The IEDN is based on 10 Gbit Ethernet, so there is lots of bandwidth from start
  - z/OS does not support link aggregation (z/VM virtual switch does)
  - For outbound bandwidth management, z/OS can be configured to use multipath where it will distribute outbound packets over all OSX ports that are configured to the same VLAN
zEnterprise IEDN without Hipersockets

Intra Ensemble Data Network with platform managed virtualization, isolation and access controls

HiperSockets is another type of System z internal network that is a System z differentiator!

...yet HS is missing from the IEDN … in order to exploit HS it requires explicit and separate network config (IP address, IP route, OS config etc.)
IEDN enabled HiperSockets

Intra Ensemble Data Network with platform managed virtualization, isolation and access controls

- HiperSockets becomes part of the IEDN
  - Support planned for z/OS V1R13
  - Statement of Direction¹ for future support in zEnteprise and and zVM

- In a transparent manner
  - The virtual servers present a single IP address (their IEDN address) for both internal (HiperSockets) and external (IEDN) access
    - No IP topology changes or routing changes required
    - The optimal path is selected automatically without requiring unique routing configuration
  - Also enables relocation of System z virtual servers across z CECs without reconfiguration
    - Same IP address used
    - Current HiperSockets IP topology is CEC specific

¹ All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice.
IEDN enabled HiperSockets - z/OS “Converged IQDX Link” Concepts

The OSX link provides access to the “External IEDN fabric” and provides access to all servers on both the Internal and External Network.

The IQDX link provides access to the “Internal CPC IEDN fabric” (optimal path) and provides access to just the subset of servers on the “Internal (IQDX portion of the) IEDN”.

The z/OS administrator only configures / manages the OSX interface.

The zEnterprise Ensemble network administrator only configures VLANs for OSX.

With AUTOIQDX… the IQDX interface is dynamically / transparently configured / added (“tucked” under OSX).

With AUTOIQDX… the IQDX interface is dynamically / transparently configured / added (“tucked” under OSX).

Only OSX connectivity must be configured!

All IP traffic to / from this IP subnet.

The OSX link provides access to the “External IEDN fabric” and provides access to all servers on both the Internal and External Network.

The IQDX link provides access to the “Internal CPC IEDN fabric” (optimal path) and provides access to just the subset of servers on the “Internal (IQDX portion of the) IEDN”.

Communications Server transparently splits and converges network traffic to this interface.

With AUTOIQDX… the IQDX interface is dynamically / transparently configured / added (“tucked” under OSX).

Only OSX connectivity must be configured!

Communications Server transparently splits and converges network traffic to this interface.

The z/OS administrator only configures / manages the OSX interface.

The zEnterprise Ensemble network administrator only configures VLANs for OSX.

With AUTOIQDX… the IQDX interface is dynamically / transparently configured / added (“tucked” under OSX).

Only OSX connectivity must be configured!

All statements regarding IBM’s plans, directions, and intent are subject to change or withdrawal without notice.

© 2011 SHARE and IBM Corporation
Summary - Exploiting the intraensemble data network

Once all hardware / physical installation and System z HCD configuration tasks are complete… then you are ready to exploit the IEDN:

Key concepts / reminders:
1. All network traffic on the IEDN must use an “authorized” VLAN ID!
2. The VLAN ID maps to a corresponding Virtual Network
3. All host images (Operating Systems) on all platforms within the Ensemble are represented as a Virtual Server

Key Unified Resource Manager network related tasks:
1. Virtual Network Configuration (at the HMC) consist of:
   - defining a virtual network (VLAN ID)
2. Virtual Server configuration:
   - Define each virtual server
   - Associate each virtual server with the proper Virtual network
3. Virtual Switch configuration (if applicable – N/A to native LPs)

Finally - Operating System network configuration tasks (IP address, VLAN ID, etc.) remain within the OS – the OS VLAN ID must match the HMC VLAN ID configuration
zBX Top of Rack (TOR) Switch

1. Intra-Node Management Network
2. Intra-Ensemble Data Network
3. Existing Customer Network

InMN TOR SWITCH

IEDN TOR SWITCH
References (White Papers, FAQs, Presentations)

- **zEnterprise System Frequently Asked Questions (FAQs)**
  - www.ibm.com/systems/z/faq

- **zEnterprise Network Security White Paper (ZSW03167-USEN-00) and Other Resources**
  - www.ibm.com/systems/z/resources (Select “Literature” Entries)

- **zEnterprise Network Security Frequently Asked Questions:**
  - http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/FQ130131

- **IBM zEnterprise System Network Virtualization, Management, and Security (Parts 1 and 2: Overview and Detail)**
  - http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS4160

- **IBM System z Hardware Management Console Security White Paper**
  - Author Kurt Schroeder (schroedk@us.ibm.com), Sept. 2008
References (Software and Security)

- **z/OS Ensemble Implementation**
  - z/OS Communications Server V1R12 SNA Network Implementation Guide (SC31-8777)
  - z/OS Communications Server V1R12 SNA Network Definition Reference (SC31-8778)
  - z/OS Communications Server V1R12 IP Configuration Guide (SC31-8775)

- **IPv6 Information**
  - IPv6 Network and Application Design Guide Version 1 Release 12 (SC31-8885)

- **z/VM Ensemble Implementation**
  - z/VM: CP Planning and Configuration (SC24-6083)

  - [www.redbooks.ibm.com](http://www.redbooks.ibm.com)

- **Security on the IBM Mainframe**, SG24-7803-00 Redbooks®, published 30 April 2010
  - [www.redbooks.ibm.com](http://www.redbooks.ibm.com)

  - [www.redbooks.ibm.com](http://www.redbooks.ibm.com)
Questions? - Thank You!

For more information on network security implications for the zEnterprise System see the following white paper:
For more information

<table>
<thead>
<tr>
<th>URL</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.twitter.com/IBM_Commsserver">http://www.twitter.com/IBM_Commsserver</a></td>
<td>IBM Communications Server Twitter Feed</td>
</tr>
<tr>
<td><a href="http://www.facebook.com/IBMCommsserver">http://www.facebook.com/IBMCommsserver</a></td>
<td>IBM Communications Server Facebook Fan Page</td>
</tr>
<tr>
<td><a href="http://www.ibm.com/systems/z/">http://www.ibm.com/systems/z/</a></td>
<td>IBM System z in general</td>
</tr>
<tr>
<td><a href="http://www.ibm.com/systems/z/hardware/networking/">http://www.ibm.com/systems/z/hardware/networking/</a></td>
<td>IBM Mainframe System z networking</td>
</tr>
<tr>
<td><a href="http://www.ibm.com/software/network/commserver/zos/">http://www.ibm.com/software/network/commserver/zos/</a></td>
<td>IBM z/OS Communications Server</td>
</tr>
<tr>
<td><a href="http://www.ibm.com/software/network/ccl/">http://www.ibm.com/software/network/ccl/</a></td>
<td>IBM Communication Controller for Linux on System z</td>
</tr>
<tr>
<td><a href="http://www.redbooks.ibm.com">http://www.redbooks.ibm.com</a></td>
<td>ITSO Redbooks</td>
</tr>
<tr>
<td><a href="http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs">http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs</a></td>
<td>Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)</td>
</tr>
<tr>
<td><a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a></td>
<td>Request For Comments (RFC)</td>
</tr>
<tr>
<td><a href="http://www.ibm.com/systems/z/os/zos/bkserv/">http://www.ibm.com/systems/z/os/zos/bkserv/</a></td>
<td>IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server</td>
</tr>
</tbody>
</table>

For pleasant reading ....