zEnterprise System - Network Architecture and Virtualization Overview

Gus Kassimis – kassimis@us.ibm.com
Alfred B Christensen – alfredch@us.ibm.com
IBM Raleigh, NC

Session 6911
Wednesday 4-Aug-2010 – 1:30 PM to 2:30 PM

SHARE in Boston

IBM

zEnterprise System - Network Architecture and Virtualization Overview

Session number:	6911
Date and time:	Wednesday 4-Aug-2010 - 1:30 PM - 2:30 PM
Location:	Room 109 (Hynes Convention Center)
Program:	Communications Infrastructure
Project:	Communications Server
Track:	Architecture, SNA/IP Integration and z/OS Systems Programming
Classification:	Technical
Speaker:	Gus Kassimis, IBM Alfred B Christensen, IBM
Abstract:	IBM's new zEnterprise System provides the ability to consolidate multi-tier, 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 configurations. 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.

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
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM eServer
- IBM (logo)®
- IBM®
- IBM zEnterprise™ System
- IMS
- InfiniBand ®
- IP PrintWay
- IPDS
- iSeries
- LANDP®

- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/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

- zEnterprise
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

* 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.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
- IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

Notes:
- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Refer to www.ibm.com/legal/us for further legal information.

Agenda

- **IBM® zEnterprise™ System Overview**

- **IBM® zEnterprise™ System Network Virtualization and Management Overview**
  - **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**
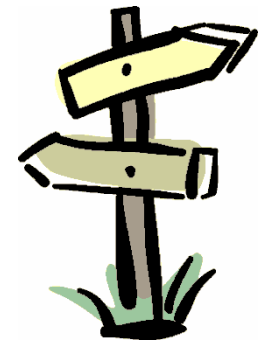
Disclaimer: All statements regarding IBM future direction or intent, including current product plans, are subject to change or withdrawal without notice and represent goals and objectives only. All information is provided for informational purposes only, on an "as is" basis, without warranty of any kind.

IBM® zEnterprise™ System

Overview

Information Technology Today: Limitations

Information technology today is limited by the technology and architecture configurations available.
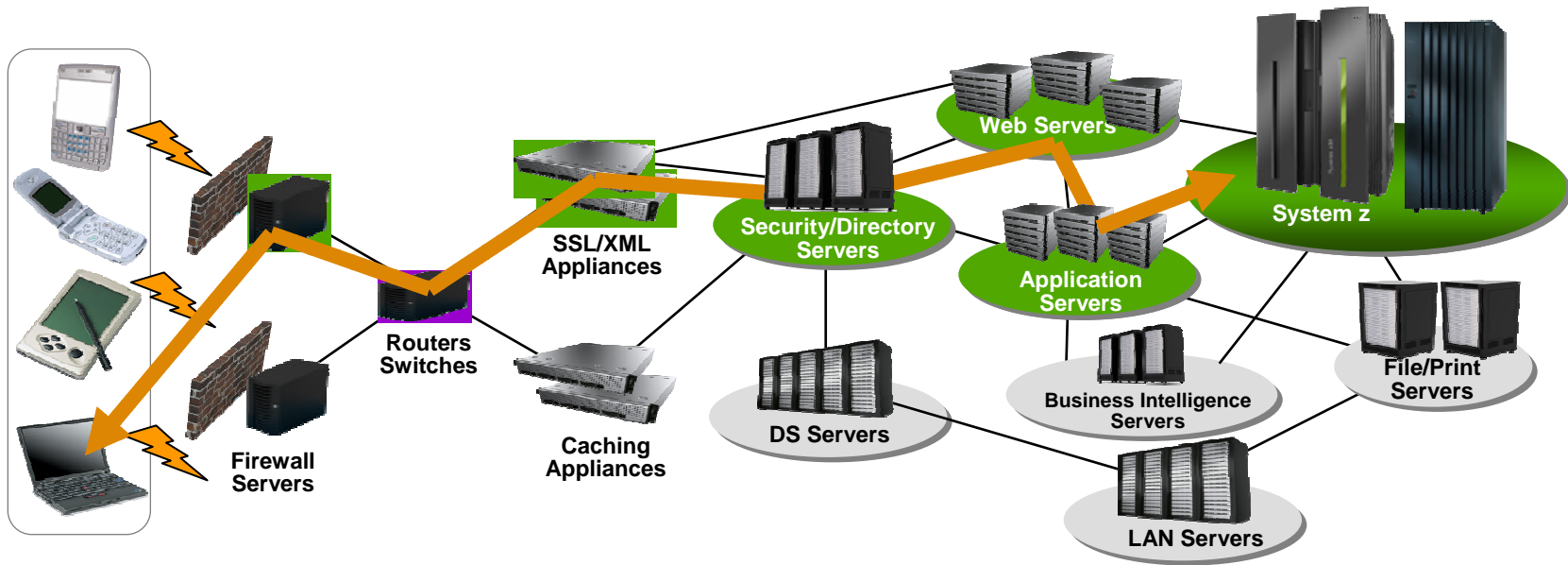
- Business processes and the applications that support them are becoming more service oriented, modular in their construction, and integrated.

- 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.**

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

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)

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

- Selected IBM POWER7® blades and IBM System x® Blades[1] for tens of thousands of AIX® and Linux applications
- High performance optimizers and appliances to accelerate time to insight and reduce cost
- Dedicated high performance private network

z/OS
z/VM
z/VSE
z/TPF
Linux

HMC

AIX
Linux

[1] All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represents goals and objectives only.

© 2010 IBM Corporation

Operating System Support for zEnterprise System

- **Currency is key to operating system support and exploitation of future servers**
- **The following are the minimum operating systems planned to run on z196:**
  - z/OS
    - z196: z/OS V1.9[1] for toleration only; exploitation starts with z/OS V1.10 with full exploitation with z/OS V1.12
    - Ensemble support: z/OS V1.10
  - Linux on System z distributions:
    - Novell SUSE SLES 10 and SLES 11
    - Red Hat RHEL 5
  - z/VM
    - z196: z/VM V5.4 or higher
    - Ensemble support: z/VM V6.1
  - z/VSE V4.1 or higher
  - z/TPF V1.1 or higher

- **Using the general purpose blades:**
  - AIX 5.3, 6.1
  - Linux on System x[2] (SOD)
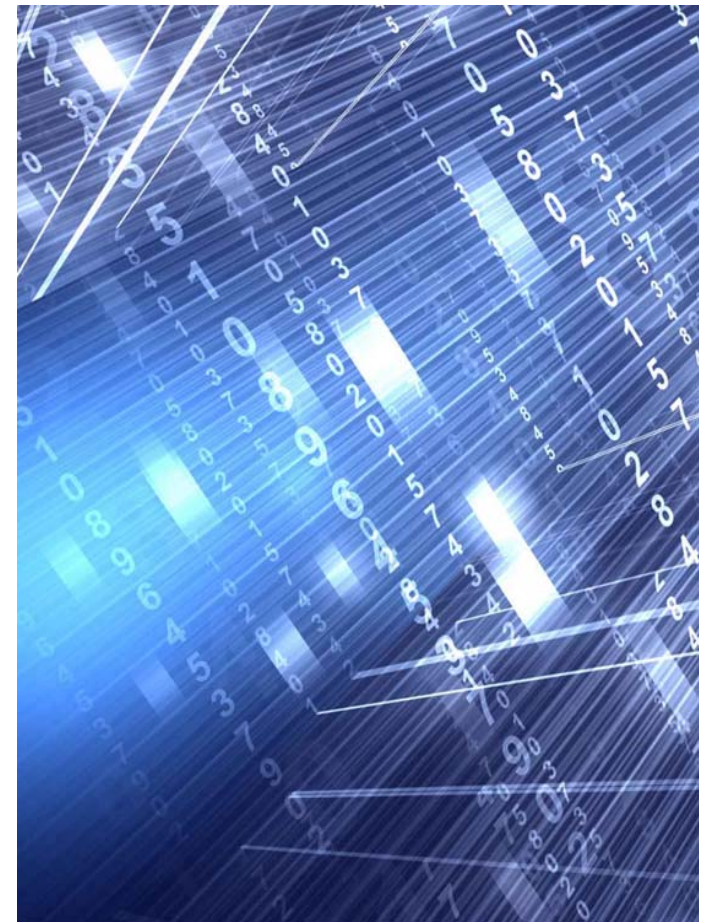
[1] z/OS V1.9 support ends on Sept. 30, 2010. Lifecycle Extension for z/OS 1.9 is available Oct. 1, 2010. Note that z/OS 1.8 with the Lifecycle Extension for z/OS 1.8 and z/OS 1.7 with the Lifecycle Extension for z/OS 1.7 are also available with toleration support only.

[2] All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represents goals and objectives only.

… 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[1]

- **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[1]**

Select IBM Blades
- **BladeCenter PS701 Express**
- **System x[1]**

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

… managed by the zEnterprise 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.

© 2010 IBM Corporation

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 WebSphere DataPower appliance[1]
    - 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[1] 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[1] 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®, or Linux on System x (SOD) [1] but have it under a single management umbrella.
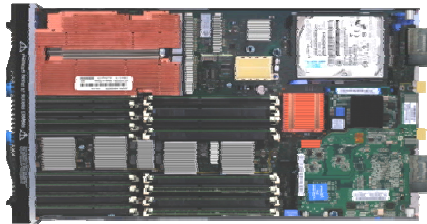
How is it different?

- **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 certified to run on AIX 5.3 or 6.1 will also be certified and run on the POWER7 blade. No changes to deployed guest images.

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

[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

WebSphere DataPower[1] Appliance in the zBX
Purpose-built hardware for simplified deployment and hardened security

What is it?

The IBM WebSphere DataPower appliance (SOD)[1] integrated in the zEnterprise System, 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:** VLAN support provides enforced isolation of network traffic with secure private networks. And integration with RACF® security.

- **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] All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represents goals and objectives only.

Management Stack
Building an architectural construct of hardware, software, services

Service Management

- Visibility, Control and Automation for Applications, Transactions, Databases and Data Center Resources
- End-to End Workload Management and Service Level Objectives that Align IT Management with Business Goals
- Common Usage and Accounting for business accounting
- Dynamic/Centralized Management of Application Workloads based on Policies
- Business Resilience for multi-site recovery
- End-to-end Enterprise Security

Platform Management

Hardware Management

Extending with

Unified Resource Manager

- **Hypervisor management and creation of virtual networks**

- **Operational controls, service and support for hardware / firmware**

- **Network management of private and secure data and support networks**

- **Energy monitoring and management**

- **Workload awareness and platform performance management**

- **Virtualization management – single view of virtualization across the platform**

zEnterprise extends Service Management for improved governance

Service Management

Tivoli

Platform Management

Unified Resource Manager and System Director

Hardware Management

Unified Resource Manager and System Director

zEnterprise

APP APP APP APP APP APP

MIDDLEWARE

MULTIPLE OPERATING SYSTEMS
e.g., z/OS, z/TPF, z/VSE, z/VM,
Linux on System z

AIX

Linux on System x[1]

VIRTUALIZATION – PR/SM, z/VM, PowerVM, System x Hypervisor

FIRMWARE

System z   Power   System x[1]   IBM Optimizers

Unified Resource Manager

Focused, collaborative innovation
A "complete systems" approach

… Value Made Possible By the Unified Resource Manager

Simplified installation of hypervisors

Gain significant time to market with improved speed of deployment

and

Manage and control communication between virtual server operating systems and the hypervisor.

Simplified energy management

Energy cost savings

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

Hypervisors

Energy

Operations

Performance

Networks

Virtual Servers

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

policies

Gain flexibility, consistency and uniformity of virtualization

Provide the business with faster time to market

Simplified network management for applications

Factory installed and configured network

Improved network security with lower latency, less complexity, no encryption/decryption

ge suite
■ Automate suite

Page 16

IBM® zEnterprise™ System
Network Virtualization and Management Overview

Agenda – IBM zEnterprise System Networking Overview

- ✓ 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

Notices:

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

2. The zEnterprise internal networks are provided with redundant hardware – redundancy is NOT shown in this presentation

zEnterprise Networking Value Points

❑ **Network Simplification**
  - ✓ **Single physical network and zBX "package" (physical network integration)**
  - ✓ **Central point of Management (zManager via the HMC/SE)**

❑ **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 (no encryption required)**

IBM zEnterprise System Overview

zEnterprise Node

System z Hardware Management Console With Unified Resource Manager

z196
- z/OS
- z/OS
- z/OS
- z/OS
- Linux on System z
- Linux on System z
- Linux on System z
- z/VM
- PR/SM
- Z CPU, Memory and IO
- System Element (SE)

zBX
- **X86 Blades**
  - Linux on System x
  - Linux on System x
  - Linux on System x
  - xHypervisor
- **Power Blades**
  - AIX
  - AIX
  - AIX
  - pHypervisor
- **Optimizers**
  - DataPower
  - Smart Analytics Optimizer
  - Future
- Blade Center Advanced Management Module (AMM)

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.

© 2010 IBM Corporation

IBM zEnterprise node with internal networks

Customer managed management network

HMC

zEnterprise Node

z196

OSM → **Intra Node Management Network (INMN)**

OSX → **Intra Ensemble Data Network (IEDN)**

OSD → **Customer managed data networks**

TOR **TOR**
TOR **TOR**
TOR **TOR**
TOR **TOR**

zBX **zBX**

BladeCenter chassis
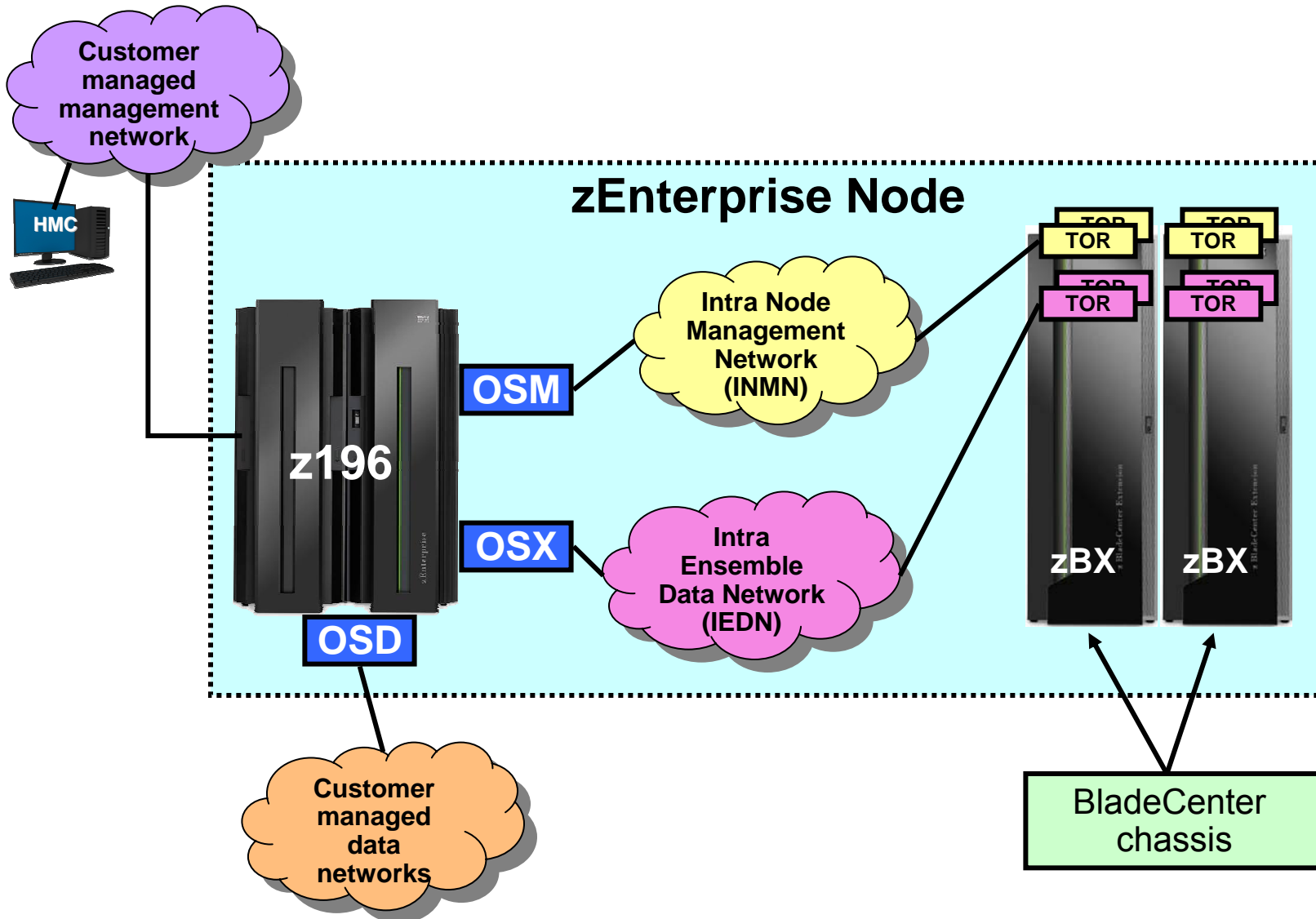
IBM zEnterprise Node with Internal Networks

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).

zEnterprise Node 1

zEnterprise Node 2
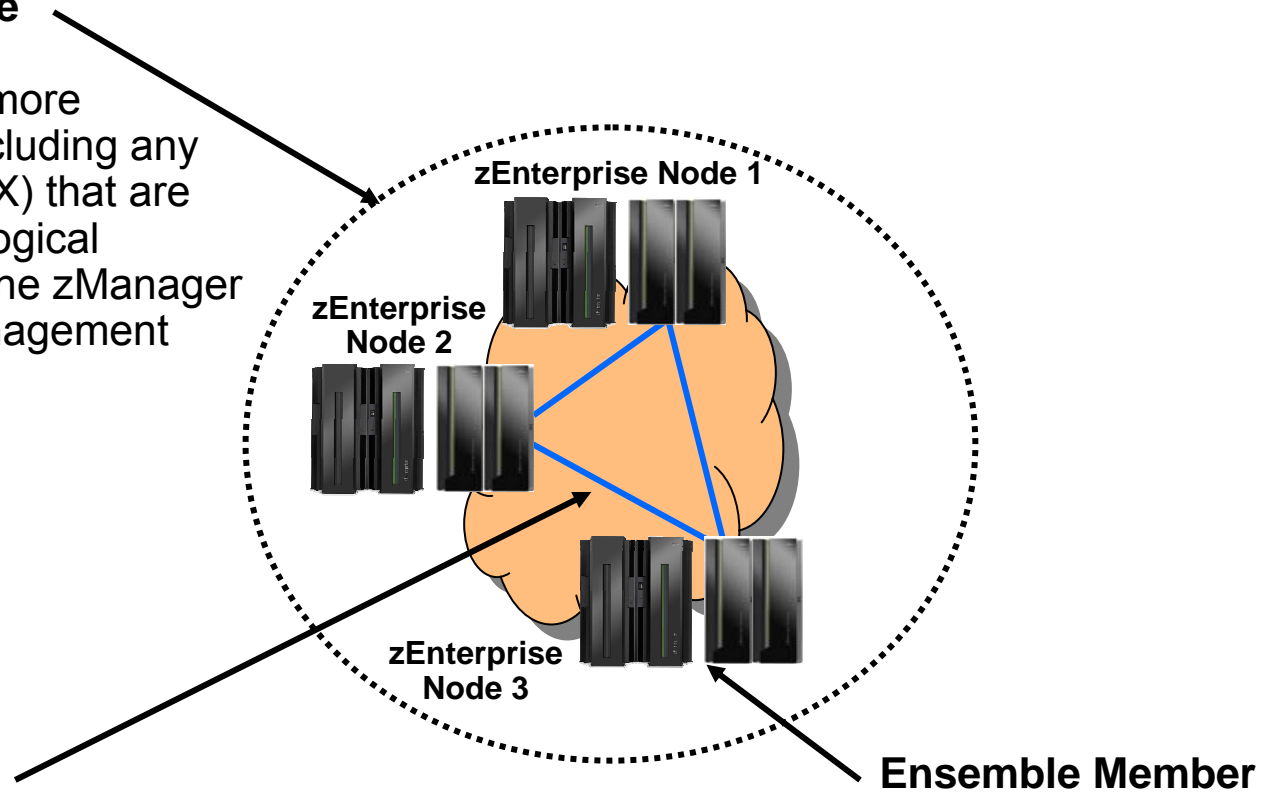
zEnterprise Node 3

Intra Ensemble Data Network (IEDN)
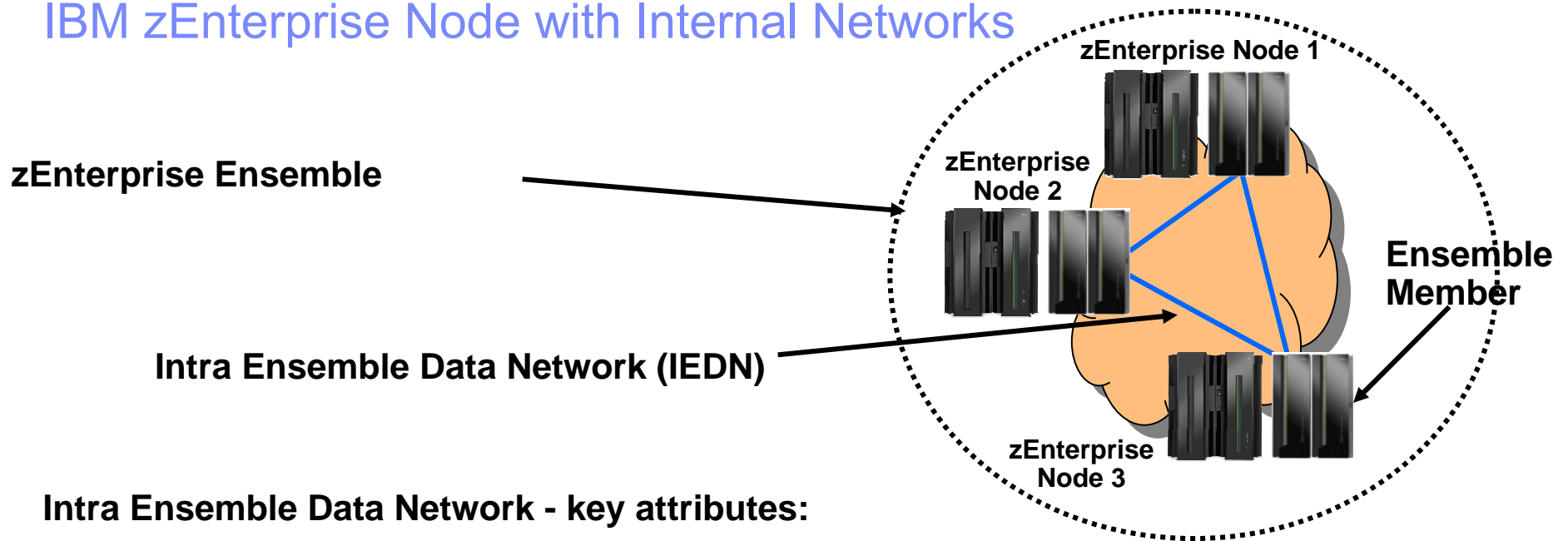
Ensemble Member

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

IBM zEnterprise Node with Internal Networks

zEnterprise Node 1

zEnterprise Node 2

zEnterprise Ensemble
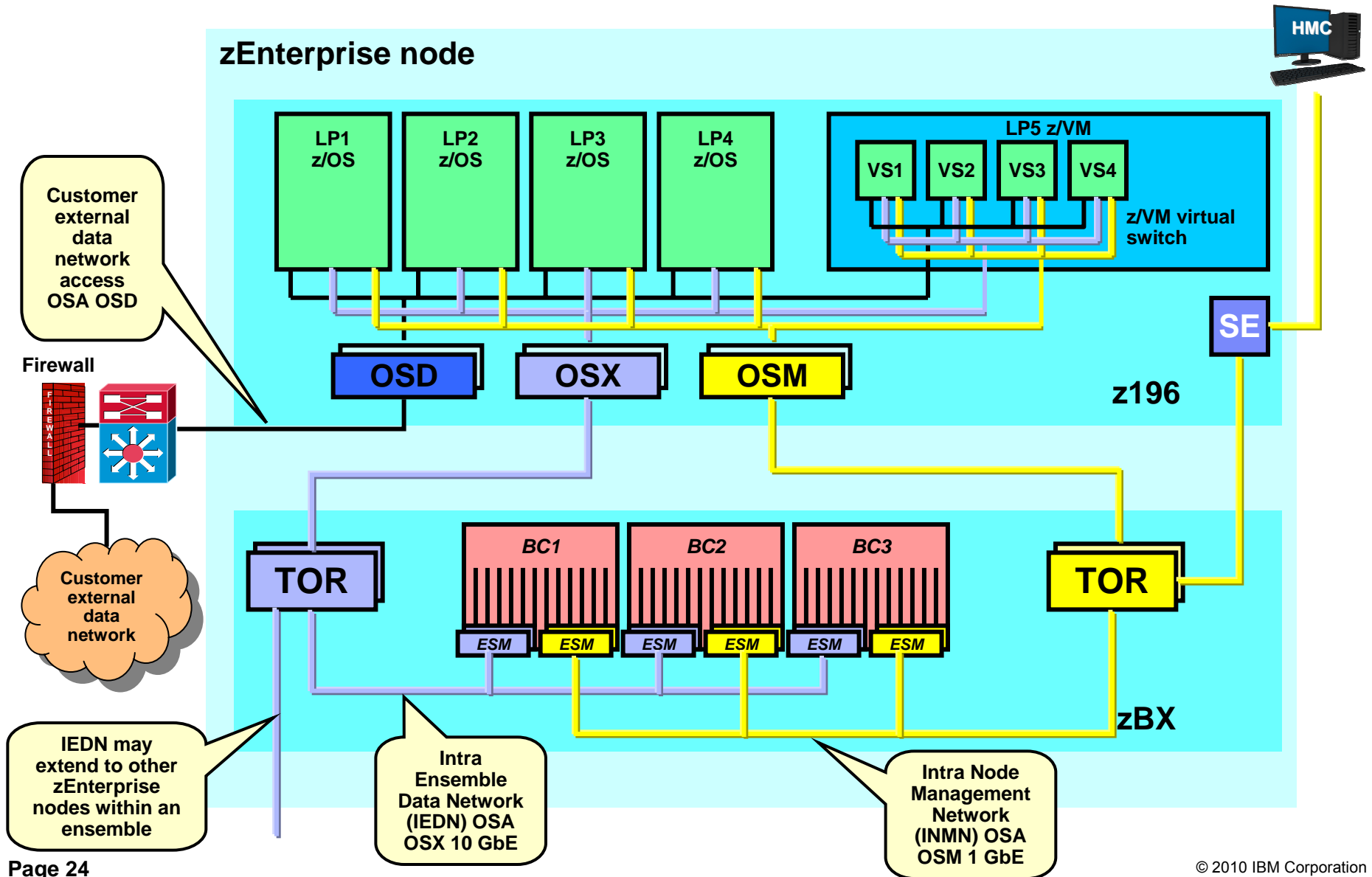
Ensemble Member

Intra Ensemble Data Network (IEDN)

zEnterprise Node 3

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 (i.e. can be shared by all co-located nodes within the Ensemble - 10km limit)
4. No layer 3 IP Routing required to communicate within the Ensemble
5. IP addresses (IPv4 or IPv6) are customer controlled (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

HMC

zEnterprise node

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

VS1 **VS2** **VS3** **VS4**

z/VM virtual switch

Customer external data network access OSA OSD

SE

Firewall

OSD **OSX** **OSM**

z196

Customer external data network

TOR

BC1	BC2	BC3

ESM **ESM** **ESM** **ESM** **ESM** **ESM**

TOR

zBX

IEDN may extend to other zEnterprise nodes within an ensemble

Intra Ensemble Data Network (IEDN) OSA OSX 10 GbE

Intra Node Management Network (INMN) OSA OSM 1 GbE

External Network Access – Option 1 – System z (LP) IP Router

zEnterprise node

Route via OSD and one or more z/OS images

HMC

LP1 z/OS — IP Router

LP2 z/OS

LP3 z/OS

LP4 z/OS

LP5 z/VM

VS1 VS2 VS3 VS4

z/VM virtual switch

Firewall

OSD OSX OSM

z196

SE

Customer external data network

TOR

BC1 BC2 BC3

ESM ESM ESM ESM ESM ESM

TOR

zBX
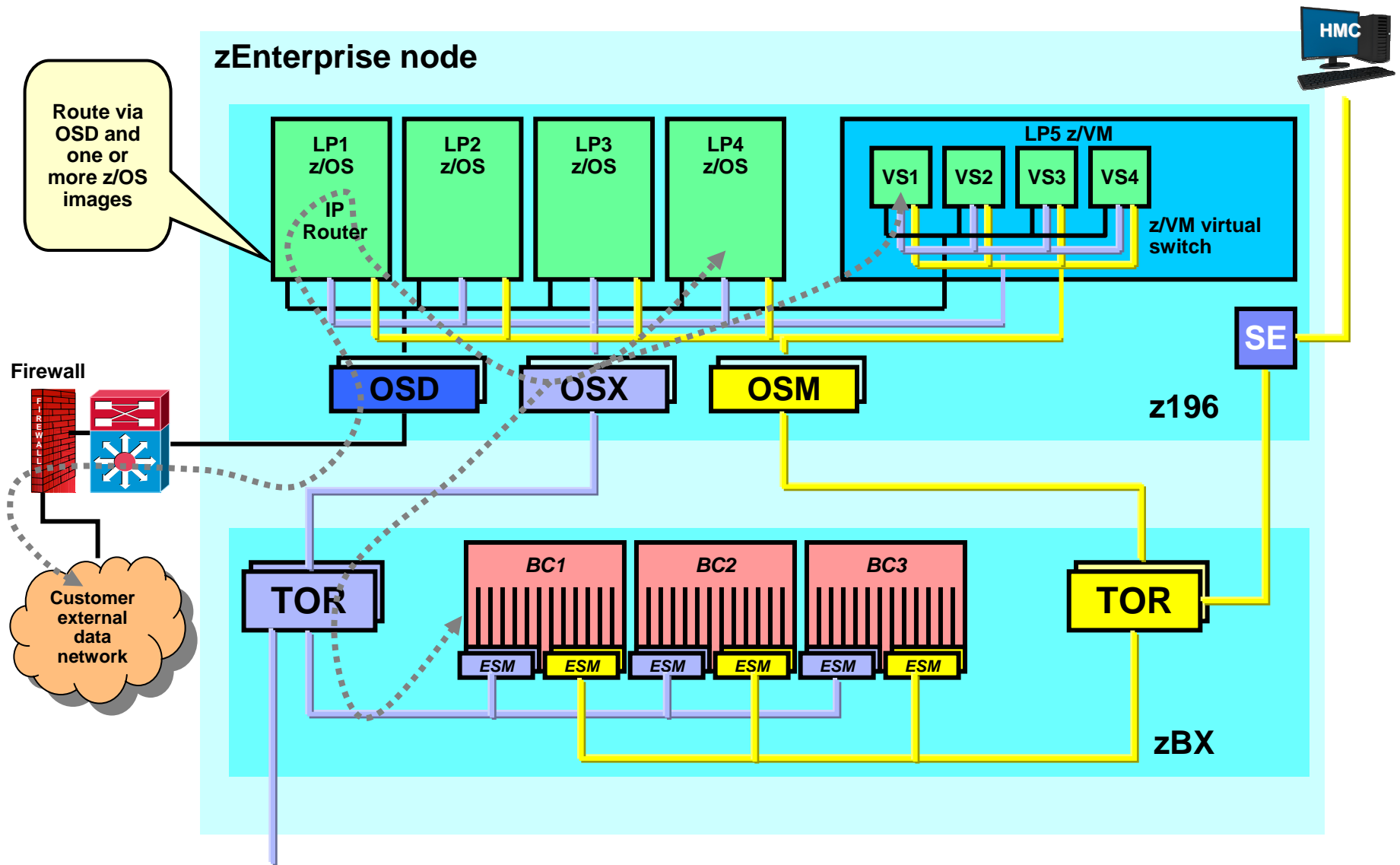
External Network Access – Option 2 – External IP Router

HMC

zEnterprise node

And to System z LPARs

LP1 z/OS	LP2 z/OS	LP3 z/OS	LP4 z/OS

LP5 z/VM

VS1 VS2 VS3 VS4

z/VM virtual switch

Firewall

FIREWALL

OSD OSX OSM

z196

SE

Customer external data network

TOR

BC1	BC2	BC3

ESM ESM ESM ESM ESM ESM

TOR

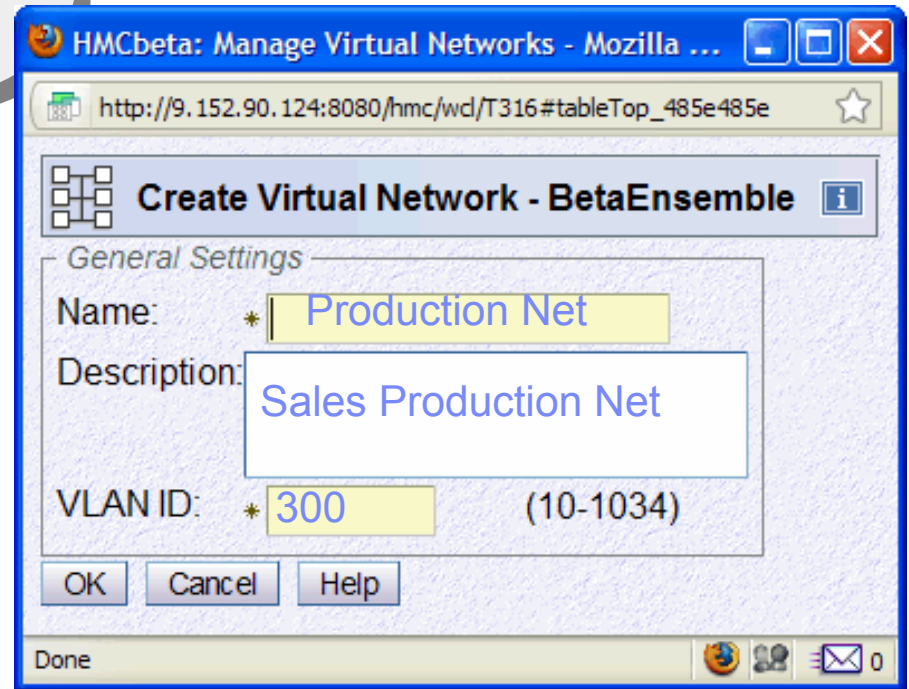zBX

Extend IEDN to external router and route via TOR
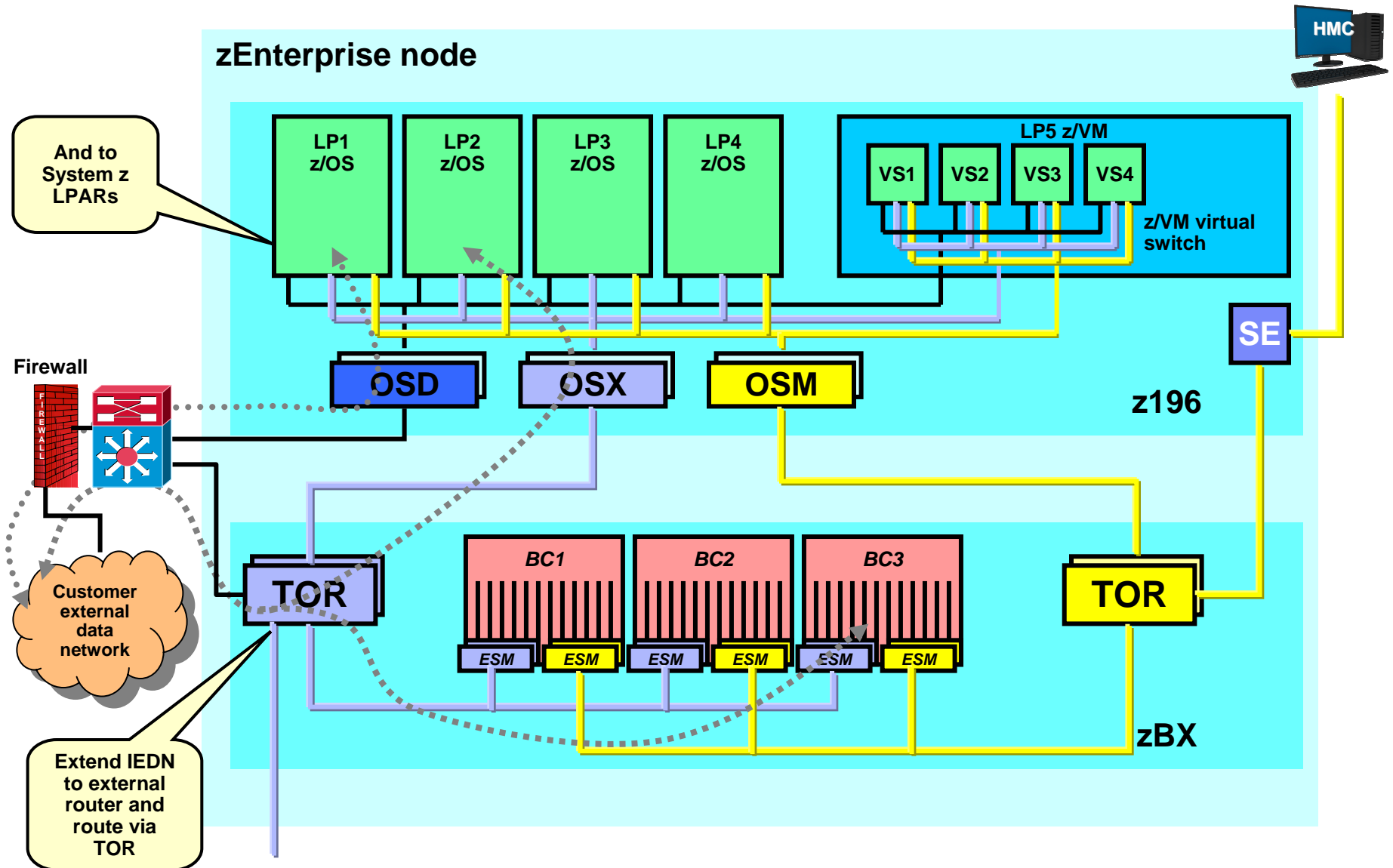
Virtual Network Concepts – Creating Virtual Networks

Step 1. Create / Define a
Virtual Network

Network Name =
Production Net

VLAN ID = 300

… from the
zManager (HMC)

HMC

HMCbeta: Manage Virtual Networks - Mozilla ...

http://9.152.90.124:8080/hmc/wcl/T316#tableTop_485e485e

Create Virtual Network - BetaEnsemble

General Settings

Name: * Production Net

Description: Sales Production Net

VLAN ID: * 300 (10-1034)

OK Cancel Help

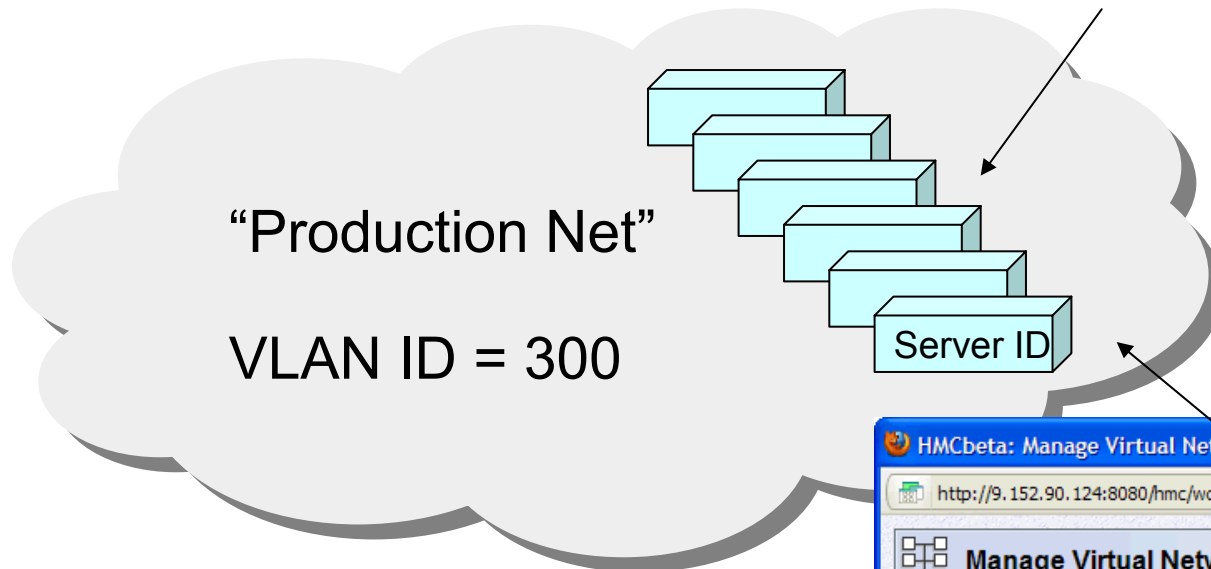Done

Virtual Network Concepts – Adding Virtual Servers
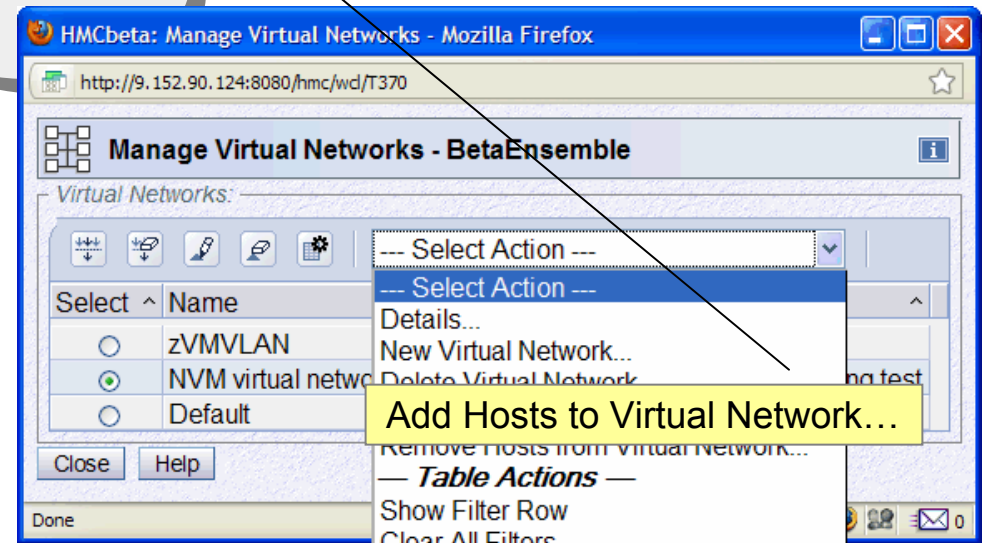
… once you have a Virtual Network…

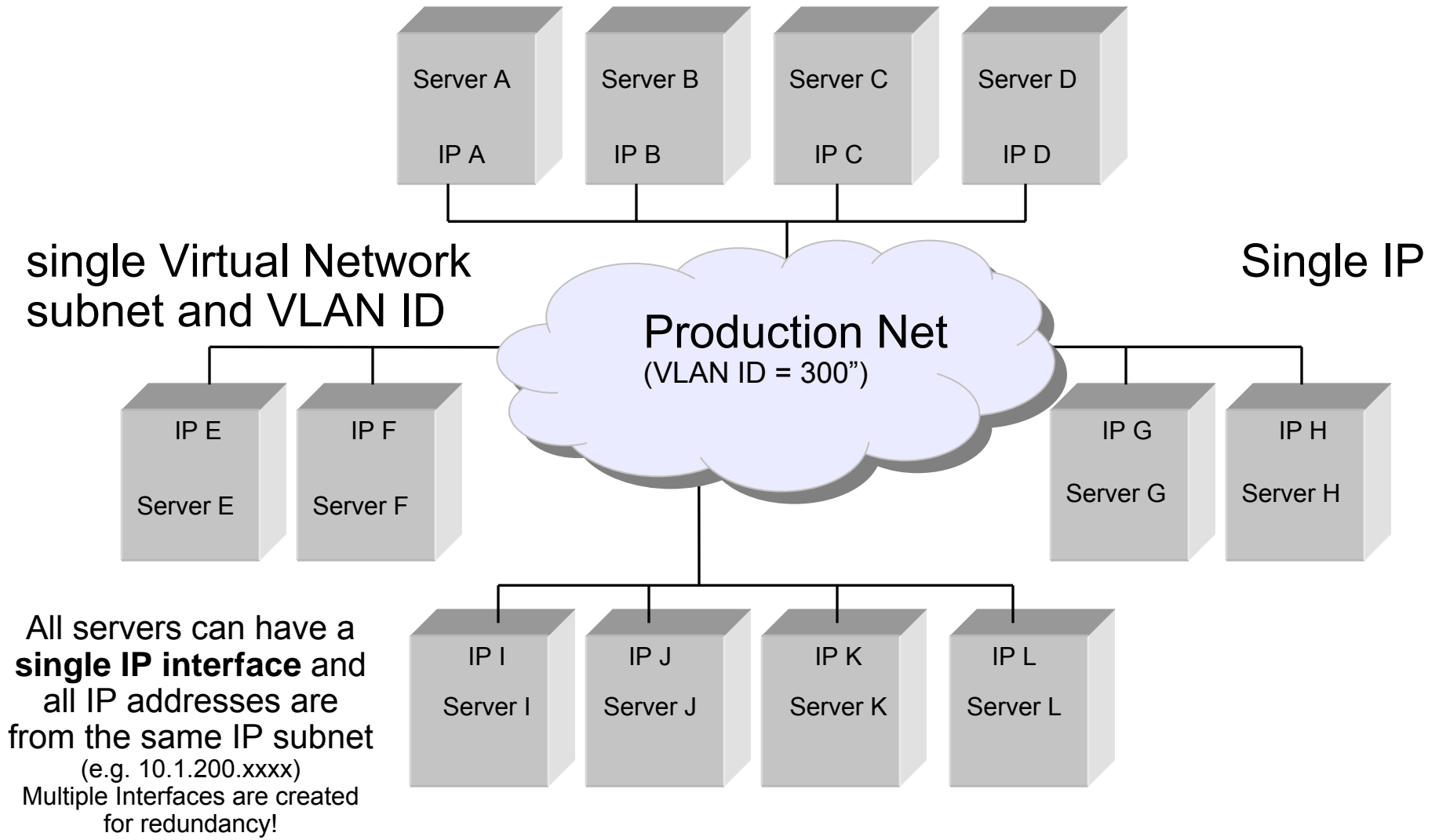Step 2. …as necessary …add (associate / authorize) Virtual Servers to the Virtual Network

"Production Net"

VLAN ID = 300

Server ID

Virtual Networks consist of two key properties:

1. *VLAN ID (IP subnet)*
2. *List of Authorized Servers*

HMCbeta: Manage Virtual Networks - Mozilla Firefox

http://9.152.90.124:8080/hmc/wcl/T370

Manage Virtual Networks - BetaEnsemble

Virtual Networks:

--- Select Action ---

Select ^	Name
○	zVMVLAN
⊙	NVM virtual netwo
○	Default

--- Select Action ---
Details...
New Virtual Network...
Delete Virtual Network...

Add Hosts to Virtual Network…

Remove Hosts from Virtual Network...
— *Table Actions* —
Show Filter Row
Clear All Filters

Close   Help

Done

Deploying a Virtual Network – Example 1

Server A

IP A

Server B

IP B

Server C

IP C

Server D

IP D

single Virtual Network subnet and VLAN ID

Single IP

Production Net
(VLAN ID = 300")

IP E

Server E

IP F

Server F

IP G

Server G

IP H

Server H

All servers can have a **single IP interface** and all IP addresses are from the same IP subnet
(e.g. 10.1.200.xxxx)
Multiple Interfaces are created for redundancy!

IP I

Server I

IP J

Server J

IP K

Server K

IP L

Server L

Deploying Multiple Virtual Networks – Example 2 - Isolation

Server A

IP A

Server B

IP B

Server C

IP C

Server D

IP D

1. Define Multiple Virtual Networks

… each having unique VLAN IDs and IP subnets

"Production Network" VLAN ID 300

"Development Network" VLAN ID 500

IP E

Server E

IP F

Server F

IP G

Server G

IP H

Server H

2. Then add virtual servers to each virtual network as needed…

IP I

Server I

IP J

Server J

IP K

Server K

IP L

Server L

…which isolates "Production Servers" from "Development Servers"

Deploying Multiple Virtual Networks – Isolation

Server A	Server B	Server C	Server D
IP@ A.1	IP@ A.2	IP@ A.3	IP@ A.4

1. Define Multiple Virtual Networks

… each having unique VLAN IDs and IP subnets

"Marketing Network"
VLAN ID 300
(subnet "A")

"Development Network"
VLAN ID 500
(subnet "B")

Server E — IP@ A.5

Server F — IP@ A.6

Server G — IP@ B.1

Server H — IP@ B.2

2. Then add virtual servers to each virtual network as needed…

Server I — IP@ B.3

Server J — IP@ B.4

Server K — IP@ B.5

Server L — IP@ B.6

… zManager isolates "Marketing Servers" from "Development Servers"

zEnterprise Virtualization and Network Access Control
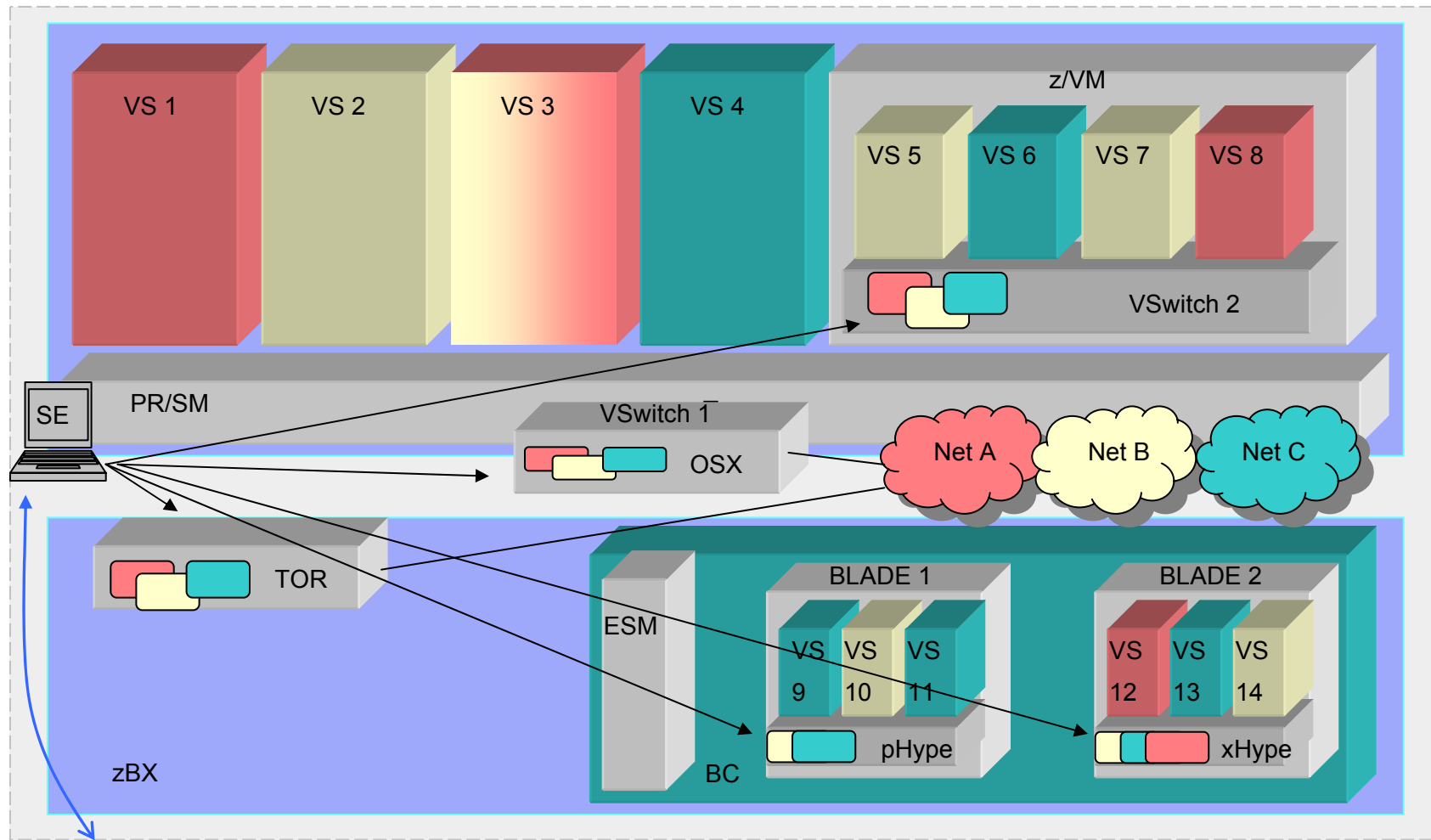
zManager pushes virtual network access control information to the node and the SE propagates to control points (OSX and Hypervisors)
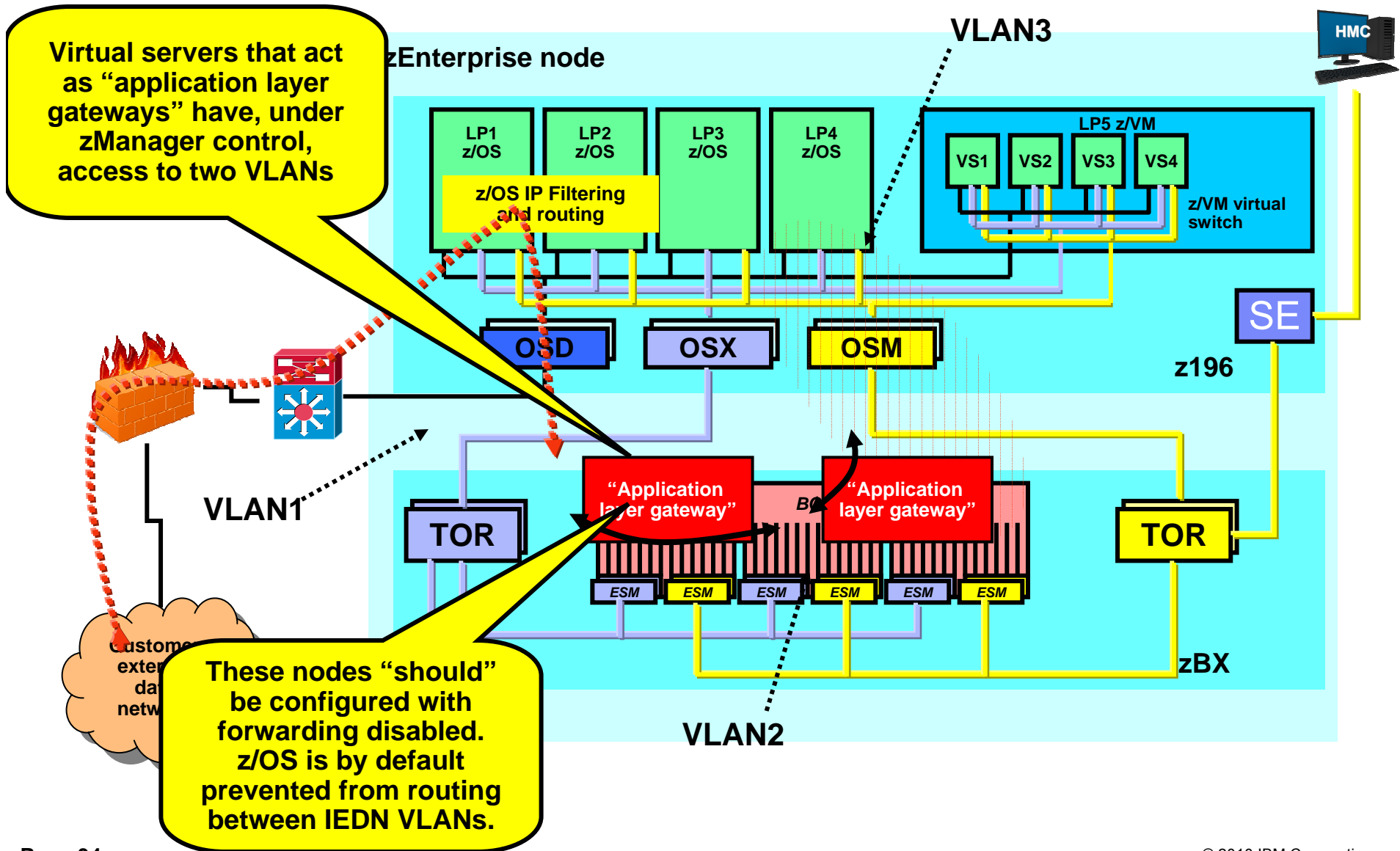
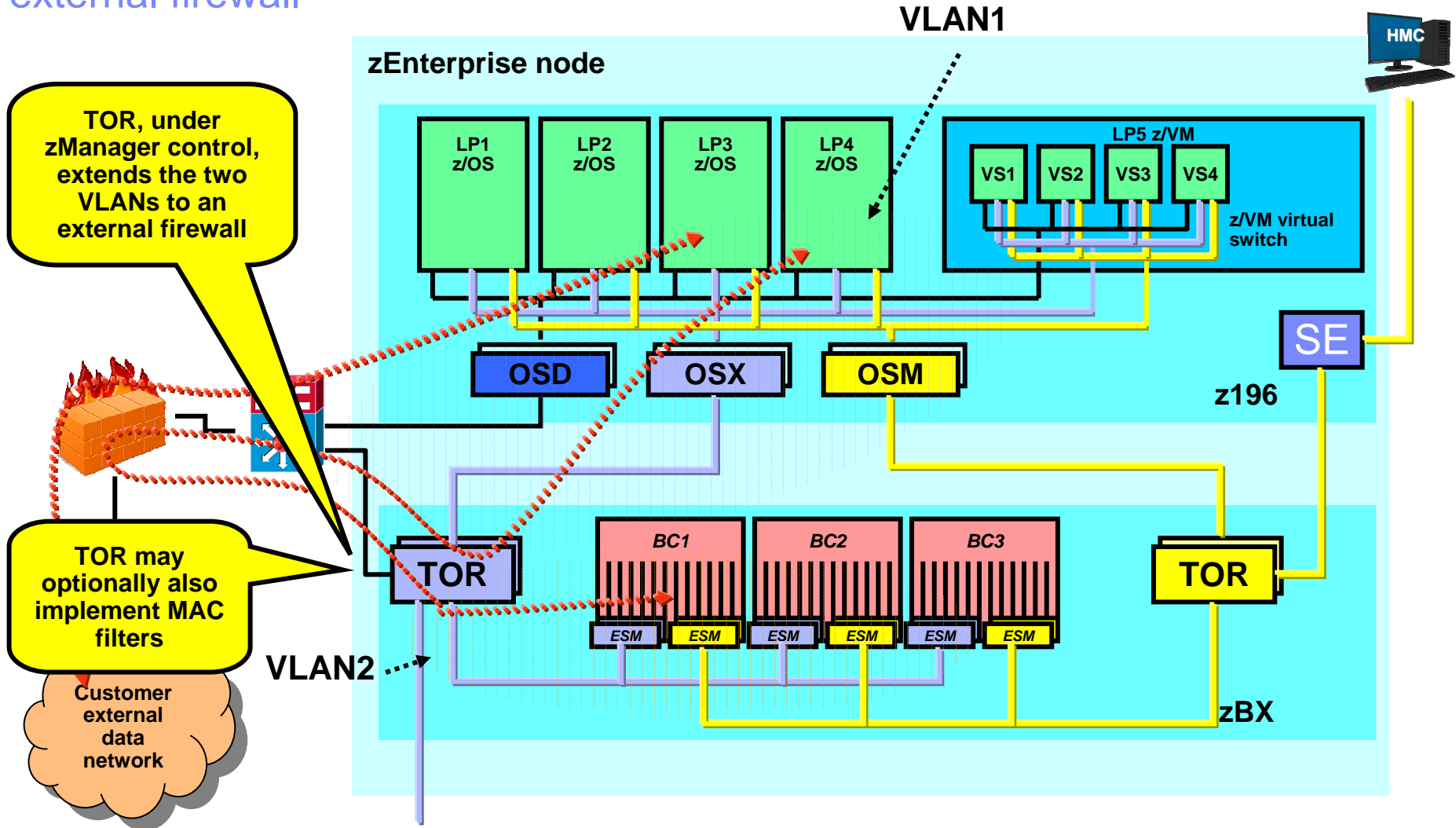# Putting It All Together…with secure access control !

System z

Server A (G0) z/OS

Server B (G1)

Server C (G2)

Server D

zVM VSwitch B

VSwitch A   OSX   OSA

OSA Port 0

Blade Center Chassis

Server E

Server F

Server G

Optimizer A

ISAOpt (Server ID Y)

pHype VSwitch C

Blade A Image

Blade B Image

NVM configures specific VLANs

External Ports   TOR A   Internal Ports   External Ports   ESM A   ESM (A)   Blade A

TOR (A) Port 0   Port 0   Port 2

IEDN Core Physical Network

Port 1

Internal Ports   Blade B

Port 2

Management Port   Management Port

IEDN Physical Edge (System z side)

zBX

Configure (allow) all VLANs

IEDN Physical Edge (blade side)

HMC

BPH Ports

SE

zEnterprise zManager controls network access at the physical and at the virtual switches (hypervisors) !

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

Use of multiple VLANs on the IEDN – "application layer gateways" between VLANs

VLAN3

HMC

zEnterprise node

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

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

VS1 VS2 VS3 VS4

z/VM virtual switch

z/OS IP Filtering and routing

OSD **OSX** **OSM**

SE

z196

VLAN1

TOR

"Application layer gateway"

B0

"Application layer gateway"

TOR

ESM ESM ESM ESM ESM ESM

Customer external data network

These nodes "should" be configured with forwarding disabled. z/OS is by default prevented from routing between IEDN VLANs.

VLAN2

zBX

Use of multiple VLANs on the IEDN – Routing between VLANs using an external firewall

VLAN1

HMC

zEnterprise node

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

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

VS1 VS2 VS3 VS4

z/VM virtual switch

OSD   OSX   OSM

SE

z196

TOR may optionally also implement MAC filters

TOR

BC1   BC2   BC3

ESM ESM ESM ESM ESM ESM

TOR

VLAN2

Customer external data network

zBX

Configuring TOR - External Network Access

Two Use Cases:

1. z10 Access

2. External IP Router

© 2010 IBM Corporation
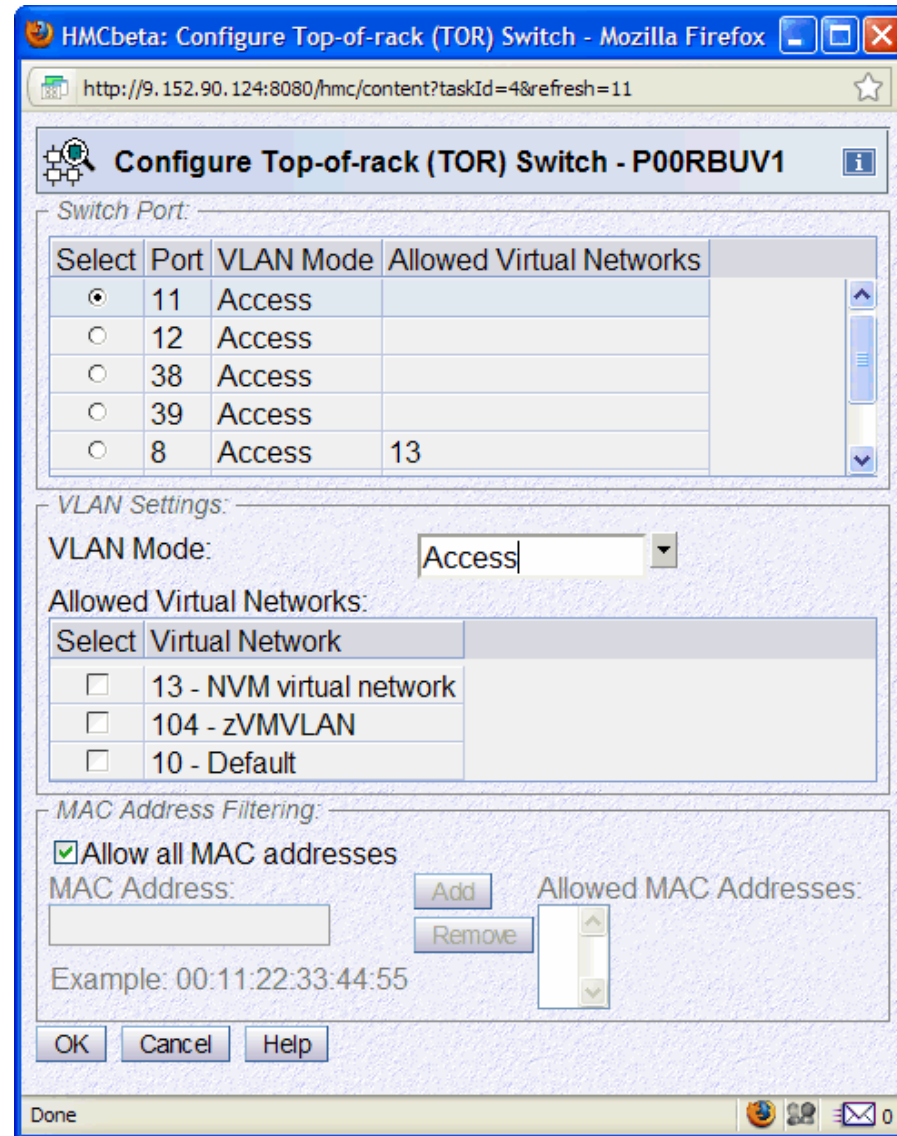
z/OS Communications Server and OSM connectivity

- z/OS LPAR must participate in the ensemble
  - New VTAM start option: ENSEMBLE=YES
    - Required for both OSM and OSX connectivity

- LPAR must be IPv6-enabled for OSM connectivity

- Two IPAQENET6 interface definitions are dynamically generated and started
  - If OSM CHPIDs are defined to the z/OS image, the two CHPIDs with the lowest device numbers are assigned to these interfaces

- TRLEs dynamically generated if connectivity allowed and CHPIDs found

- Only port 0 supported

- IPv6 link-local address only

- Uses VLAN in access mode
  - Switch handles VLAN tagging, stack unaware

- Not reported to OMPROUTE

- Cannot add static or dynamic routes

- Supports stop, start, packet trace, NTA

- Only applications permitted to EZB.OSM.sysname.tcpname can communicate over OSM interfaces
  - The GPMP is the only application that needs to

Guest Platform Management Provider (GPMP)

z/OS TCP/IP
Two IPAQENET6 and TRLEs dynamically built and started

OSM   **OSM**
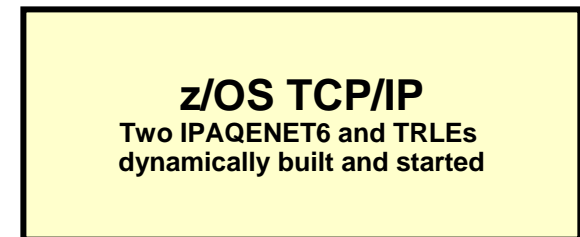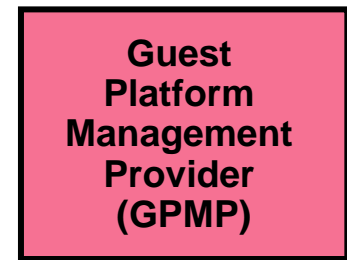
How bad is it enabling IPv6?

- Add a NETWORK stmt. for AF_INET6 to your BPXPRMxx PARMLIB member

- No changes needed to your TCP/IP Profile
  - Unless you want to exploit and test specific IPv6 features

```
FILESYSTYPE TYPE(INET) ENTRYPOINT(EZBPFINI)
  NETWORK DOMAINNAME(AF_INET)
          DOMAINNUMBER(2)
          MAXSOCKETS(2000)
          TYPE(INET)
  NETWORK DOMAINNAME(AF_INET6)
          DOMAINNUMBER(19)
          MAXSOCKETS(3000)
          TYPE(INET)
```

- Testing needed in the network management area
  - Netstat reports will use the LONG format
  - Home-written Netstat "scraping" logic will need to be changed
  - Network management products may fail if they are not prepared for IPv6 addresses

```
MVS TCP/IP NETSTAT CS V1R12        TCPIP Name: TCPCS        13:02:52
User Id  Conn      State
-------  ----      -----
MYINETD1 00000022 Listen
  Local Socket:   9.42.130.98..23
  Foreign Socket: 0.0.0.0..0
TN3270A  0000004D Establsh
  Local Socket:   ::ffff:9.42.105.45..23
  Foreign Socket: ::ffff:9.76.144.213..4211
  Application Data:  EZBTNSRV TCPABC80 TSO10001 ET B
TN3270A  0000003F Listen
  Local Socket:   ::..23
  Foreign Socket: ::..0
  Application Data:  EZBTNSRV LISTENER
```

It's a piece of cake

z/OS Communications Server and OSX connectivity

- Configure with INTERFACE statement
  - IPAQENET and IPAQENET6

- Either specify CHPID
  - Dynamically created TRLE similar to HiperSockets

- Or configure TRLE and point to it
  - Useful in VM guest LAN environment where CHPID is unpredictable

- Always uses VLAN in trunk mode
  - VLANID required and must be authorized at HMC
    - If not authorized, OSA activation fails

- Prevents IP forwarding from OSX ⇨ OSX
  - Sysplex distributor forwarding is allowed when using VIPAROUTE

- Supports stop, start, packet trace, NTA

- To prevent external traffic from being routed to the OSX VLAN
  - Define OSX as INTERFACE or IPV6_INTERFACE
  - Do not enable IMPORT_DIRECT_ROUTES function
  - Alternatively, do not define the OSX interfaces to OMPROUTE and tell OMPROUTE to ignore undefined interfaces

- To allow external traffic to be routed to the OSX VLAN
  - Define OSX as OSPF_INTERFACE or IPV6_ISPF_INTERFACE
  - Configure a non-0 value for ROUTER_PRIORITY

Normal z/OS Applications and Subsystems (CICS, IMS, DB2, MQ, WAS, etc.)

z/OS TCP/IP
Define IPAQENET or IPAQENET6 Interfaces with VLAN ID that matches HMC definitions

OSX   **OSX**

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 zManager network related configuration 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

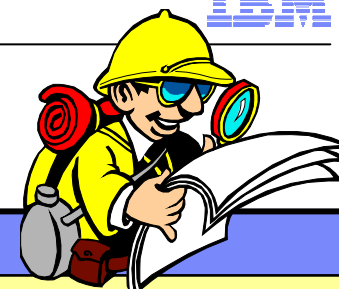3. Virtual Switch configuration (if applicable – N/A to native LPs)
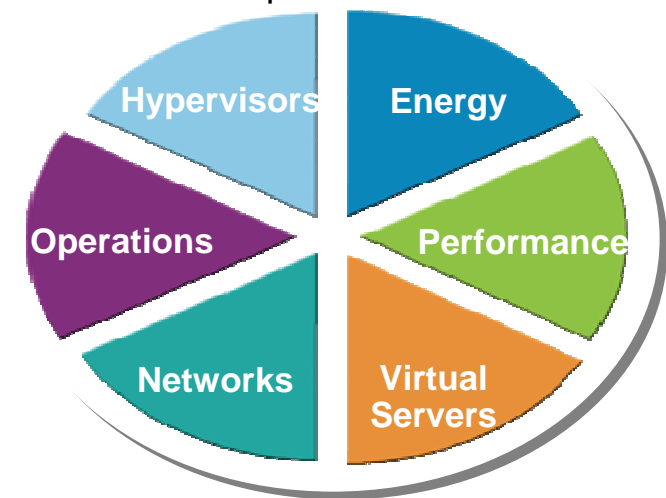
Finally - Operating System network configuration tasks (IP address, VLAN ID, etc.) remain within the OS – the OS VLAN ID must match the HMC VLAN ID configuration

Questions? - Thank You !

For more information

URL	Content
http://www.twitter.com/IBM_Commserver	IBM Communications Server Twitter Feed
http://www.facebook.com/IBMCommserver	IBM Communications Server Facebook Fan Page
http://www.ibm.com/systems/z/	IBM System z in general
http://www.ibm.com/systems/z/hardware/networking/	IBM Mainframe System z networking
http://www.ibm.com/software/network/commserver/	IBM Software Communications Server products
http://www.ibm.com/software/network/commserver/zos/	IBM z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	IBM Communications Server for Linux on System z
http://www.ibm.com/software/network/ccl/	IBM Communication Controller for Linux on System z
http://www.ibm.com/software/network/commserver/library/	IBM Communications Server library
http://www.redbooks.ibm.com	ITSO Redbooks
http://www.ibm.com/software/network/commserver/zos/support/	IBM z/OS Communications Server technical Support – including TechNotes from service
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs	Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)
http://www.ibm.com/systems/z/os/zos/bkserv/	IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server

For pleasant reading ….