#SHAREorg

SHARE
Technology · Connections · Results

zEnterprise Networking Lessons Learned

Thomas Cosenza tcosenza@us.ibm.com
IBM STG Lab Services

Session Number 12850

SHARE in San Francisco 2013

Introduction

- Thomas Cosenza
  - Lab Services Leader for XI50z enablement services
  - Network and IT Security Consultant for the last 8 years
  - CISSP in good standing

Late 90s ~ Early 00's

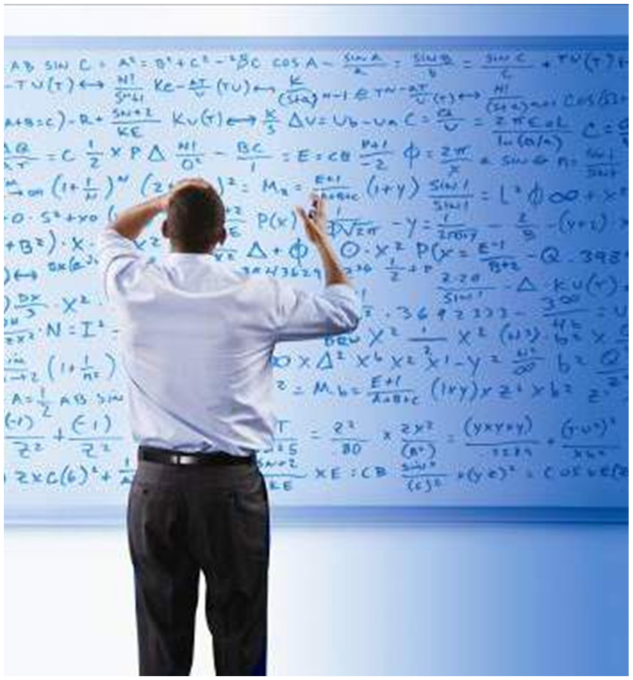
- Scaling drove performance
- Scaling drove down cost
- Performance constrained
- Active power dominates
- Focus on processor performance

Todays Enterprise

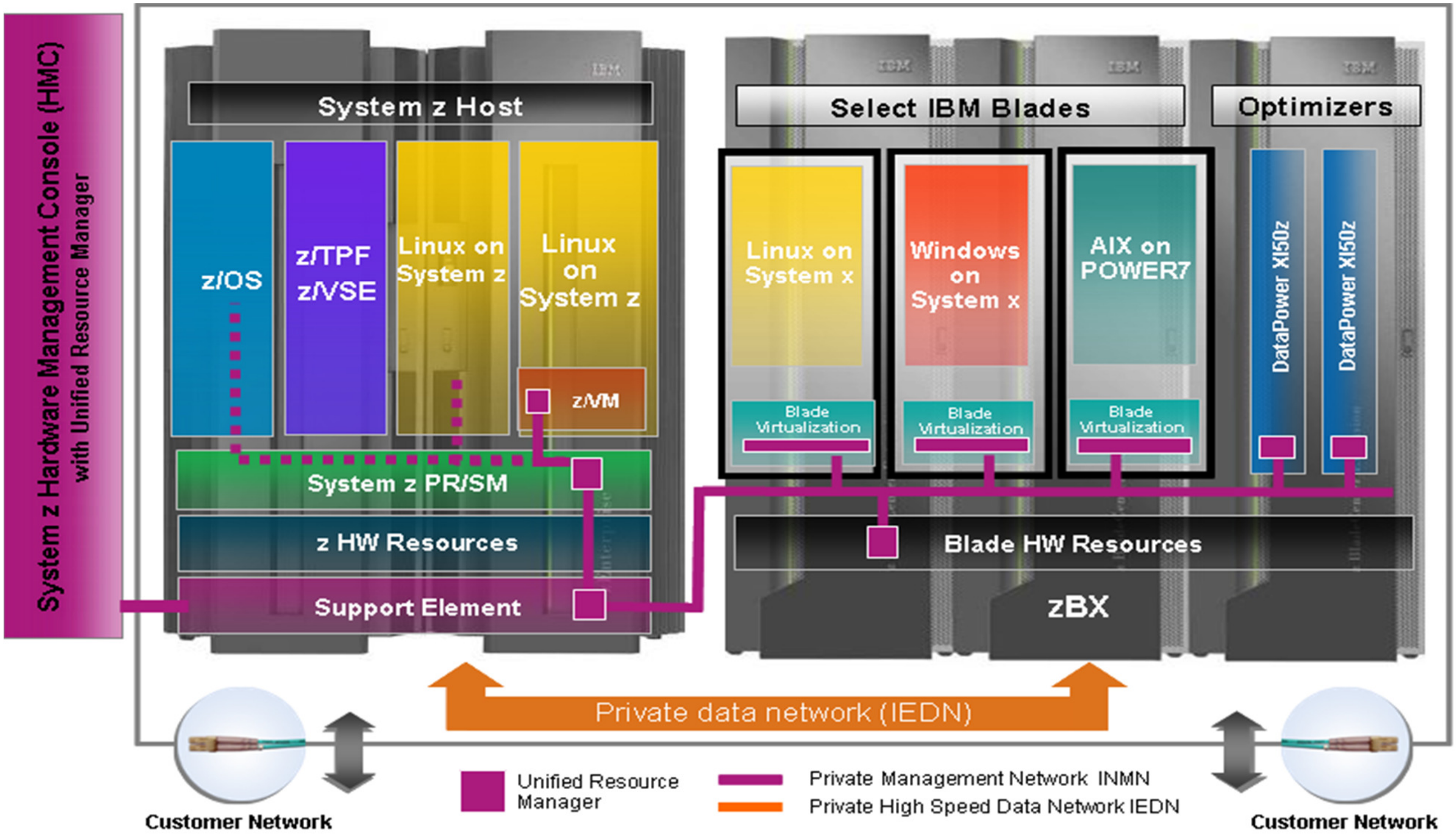
- INNOVATION drives performance
- Scaling drives down cost
- Power constrained
- Standby power dominates
- Focus on SYSTEM performance

Despite the Allure of a "one size fits all" Server Approach …

- Today's enterprise computing environments are multi-platform for a reason. They're optimized to run different workloads:
  - Database and Transaction processing.
  - Analytics.
  - Web-based interactions.
  - Enterprise applications such as ERP.
  - The myriad of x86 applications.
- Complex solutions are optimally deployed on multi-tier heterogeneous infrastructures



zEnterprise was Conceived



System z Hardware Management Console (HMC) with Unified Resource Manager

System z Host

z/OS

z/TPF z/VSE

Linux on System z

Linux on System z

z/VM

System z PR/SM

z HW Resources

Support Element

Select IBM Blades

Linux on System x

Windows on System x

AIX on POWER7

Blade Virtualization

Blade Virtualization

Blade Virtualization

Optimizers

DataPower XI50z

DataPower XI50z

Blade HW Resources

zBX

Private data network (IEDN)

Customer Network

Customer Network

Unified Resource Manager

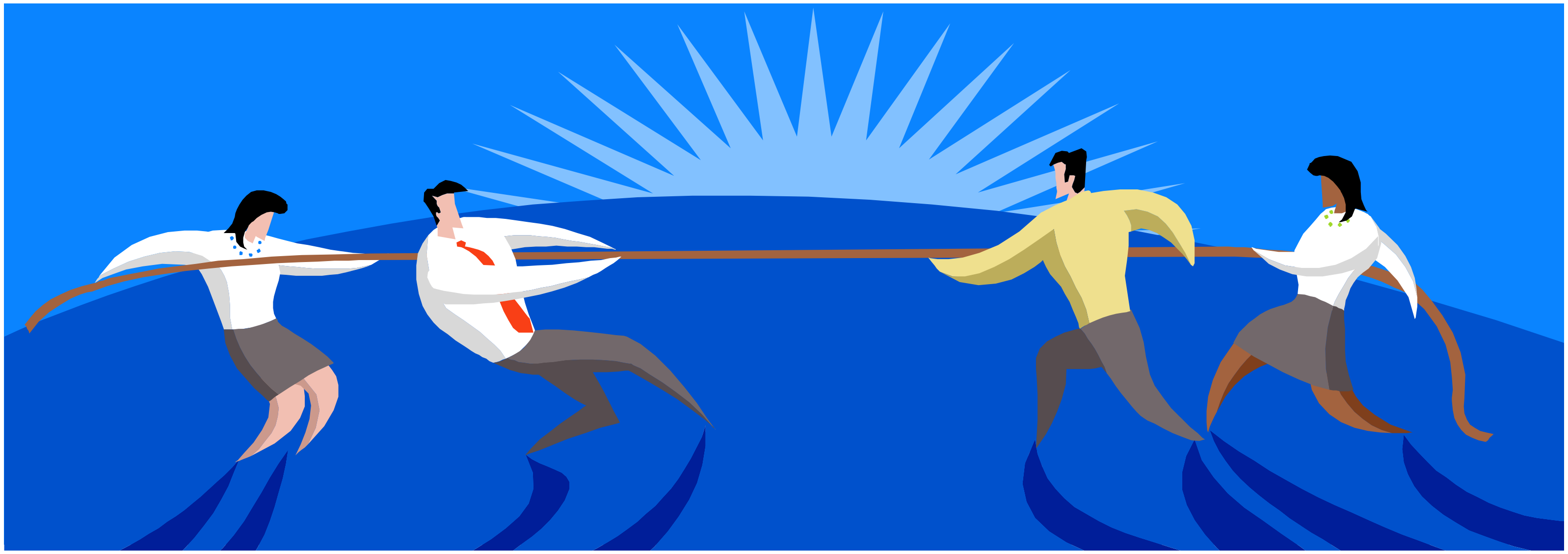
Private Management Network INMN

Private High Speed Data Network IEDN

The Only Constant is Change

- While zEnterprise creates the “Smarter Enterprise” issues arise
  - Who is going to maintain
  - What current IT security guidelines need to be met
  - How does zEnterprise fits into the current IT networking management and policies
- The rest of this presentation will discuss the issues and how what lessons we have learned on how to get around them

War of the Silos



Involving the right people

- Levels 8/9/10 of the OSI Model
  - Religion
  - Money
  - Power
- IT is usually positioned in Silos
- Hybrid Environments Cross Boundaries
- This will cause stress in your organization

Groups to add in

- IT Architects
- zOS/zVM Networking
- System Programmers
- Security
- Enterprise Network Engineers
- Distributed Server Owners

What can be done

- Talk with your Director/CTO/CIO
  - Show them the value of zEnterprise
    - Security
    - Footprint
    - Centralized Management
- Work with the Distributed Server people
  - The Operating Systems are the same
  - Windows/Linux/AIX all supported within zBX
- Talk with your Security team about policies regarding Distributed servers

Moving the Castle Wall

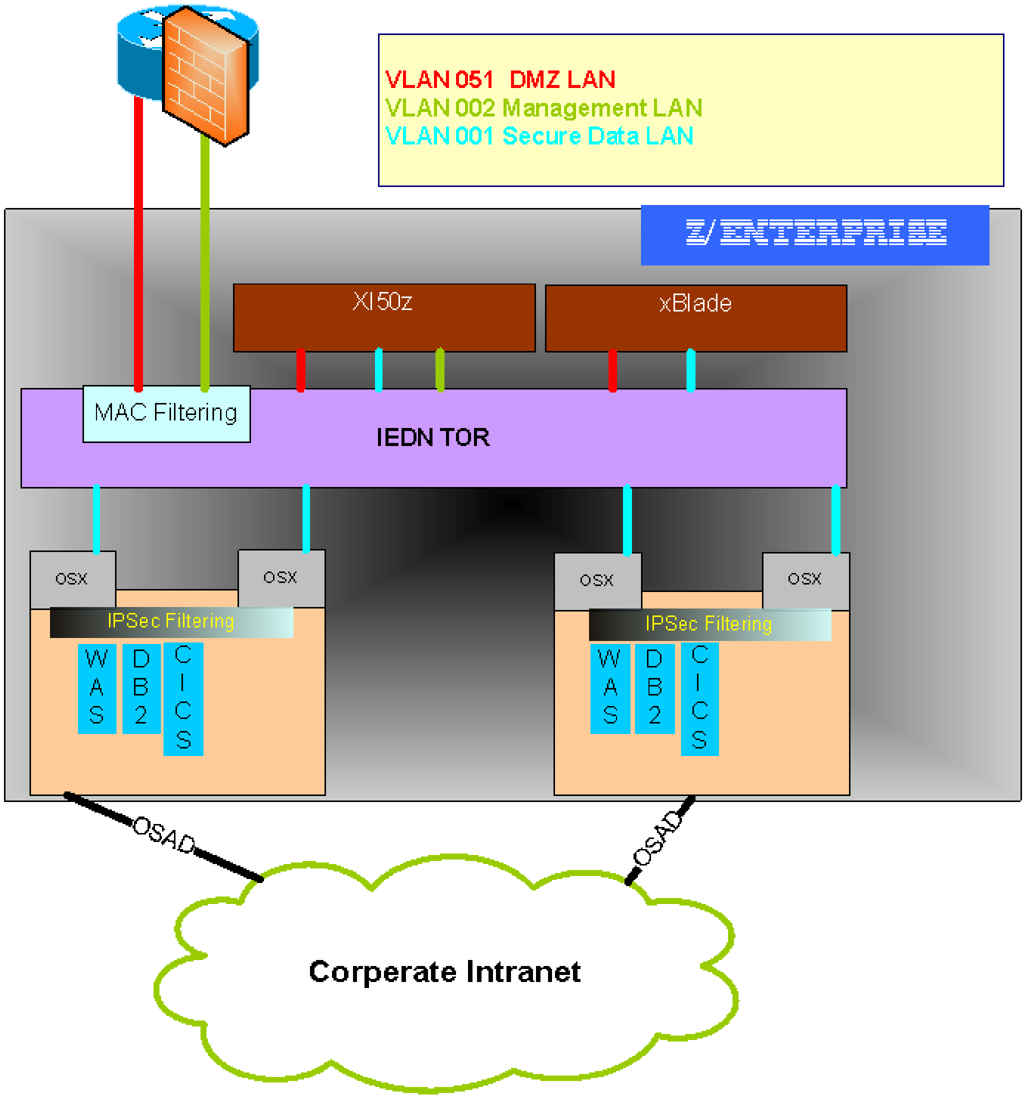
Hybrid Environments cross zones

- The current Hybrid-Environments you have may traverse several security zones
- Work with your IT security group on what the current security architecture is
- You will have to look at the ways to either
  - Eliminate
  - Accept
  - Remediate the risks

One Real world example

- One company wanted to use zEnterprise to house their Distributed devices
- However this moved their devices from their DMZ to their Enterprise zone
- Once the Security folks heard .. lets say this was interesting

One Real world example



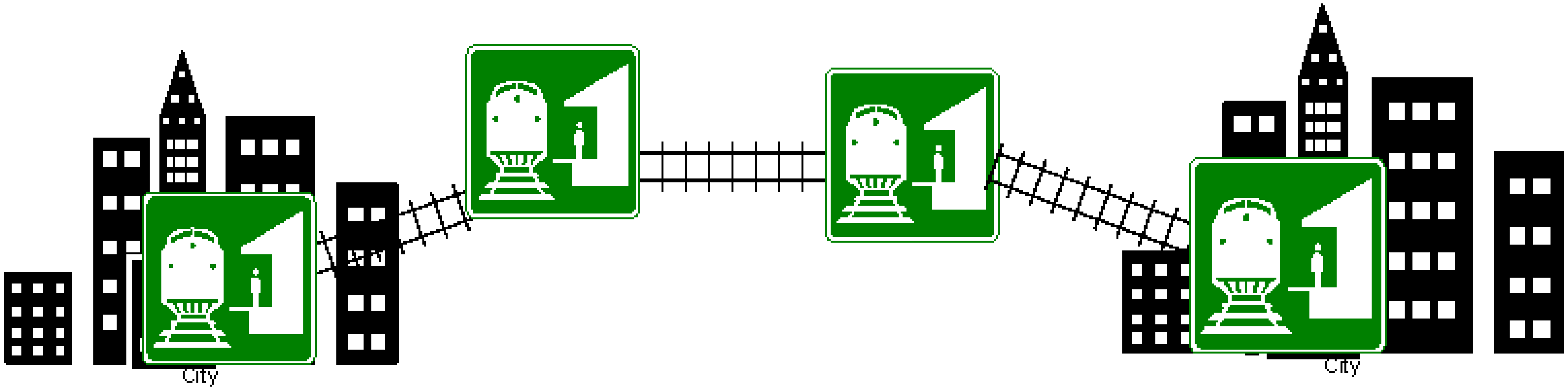
Keeping the Heart Beat Going

High Availability and Blades

- The blades do not support OSPF by default
  - Static Routes
  - Default Gateway Routing
- Would you really want to?
  - Want more CPU dedicated for Transactions
- So use a DVIPA with the same IP Address Subnet as the IEDN subnet
  - Using LAYER 2 Routing

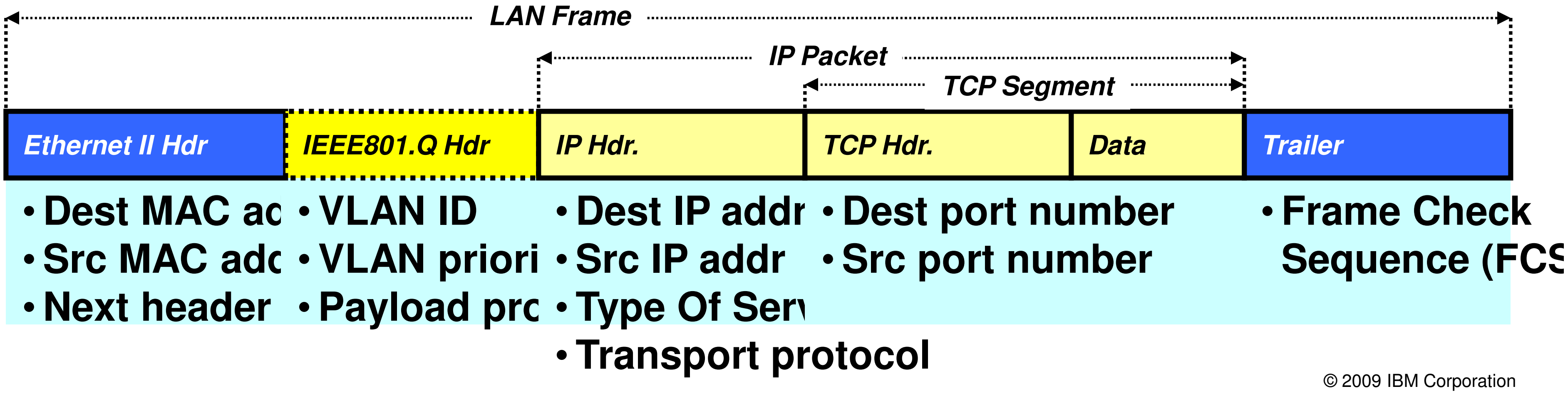
What is Layer 2 Routing

- Think of it as traveling between cities on a train.   You will not have a direct route?
- IP addresses are the Cities
- MAC addresses are the Train Stations.



What is Layer 2 Routing

- The LAN infrastructure transports “Frames” between Network Interface Cards (NICs)
- Each NIC has a physical hardware address –called Media Access Control (MAC)
- Every frame comes from a MAC and goes to a MAC
- A frame carries a payload of a specified protocol type, such as ARP, IPv4, IPv6, SNA LLC2, etc.
- Uses a Protocol Called ARP in order to discover other MAC address and their corresponding IPv4 addresses



LAN Frame

IP Packet

TCP Segment

Ethernet II Hdr
- Dest MAC ac
- Src MAC adc
- Next header

IEEE801.Q Hdr
- VLAN ID
- VLAN priori
- Payload prc

IP Hdr.
- Dest IP addr
- Src IP addr
- Type Of Serv
- Transport protocol

TCP Hdr.
- Dest port number
- Src port number

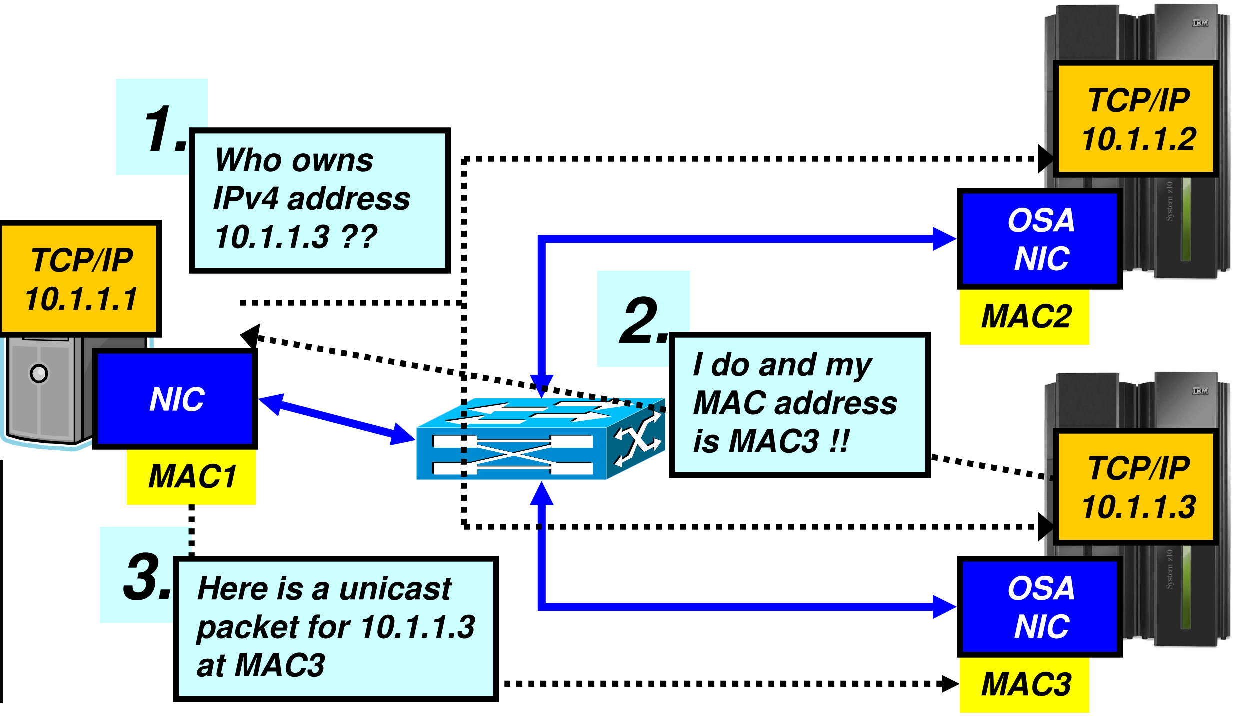
Data

Trailer
- Frame Check Sequence (FCS

So lets look at this process

ARP Cache

IP address	MAC
10.1.1.2	MAC2
10.1.1.3	MAC3

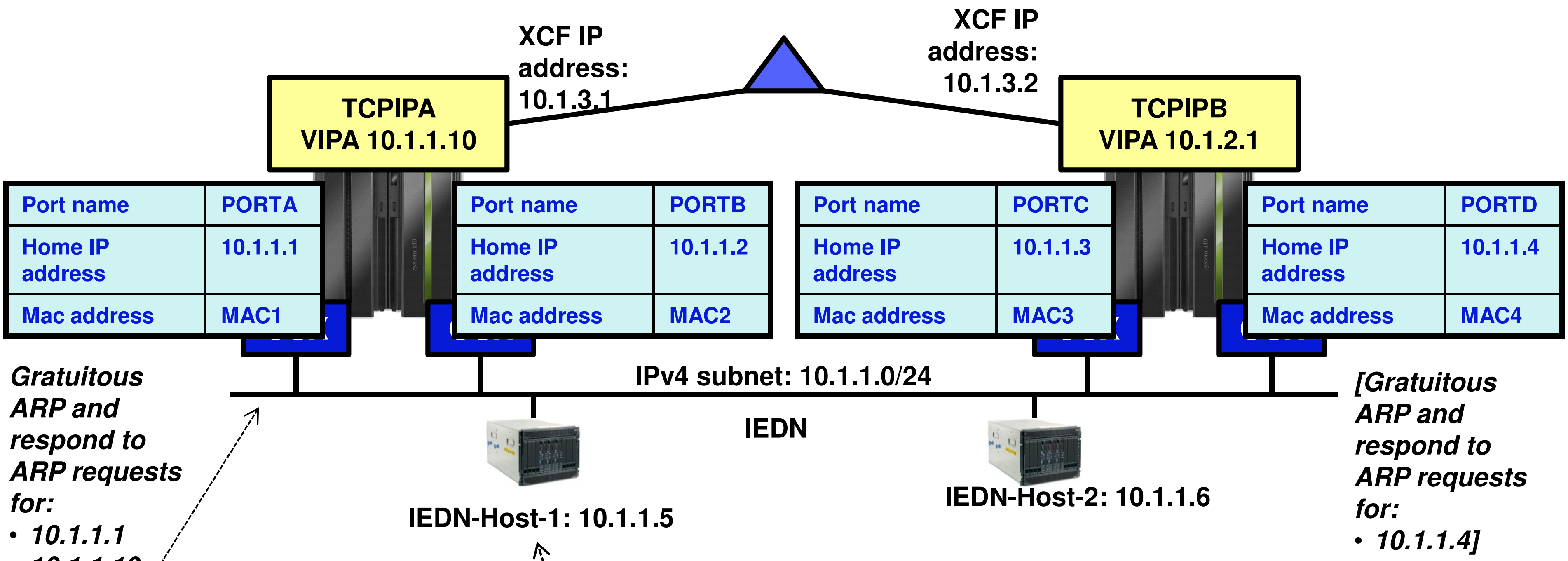


1. *Who owns IPv4 address 10.1.1.3 ??*

2. *I do and my MAC address is MAC3 !!*

3. *Here is a unicast packet for 10.1.1.3 at MAC3*

z/OS VIPA address visibility on the IEDN



Port name	PORTA
Home IP address	10.1.1.1
Mac address	MAC1

Port name	PORTB
Home IP address	10.1.1.2
Mac address	MAC2

Port name	PORTC
Home IP address	10.1.1.3
Mac address	MAC3

Port name	PORTD
Home IP address	10.1.1.4
Mac address	MAC4

Gratuitous ARP and respond to ARP requests for:

- ***10.1.1.1***
- ***10.1.1.10***

[Gratuitous ARP and respond to ARP requests for:

- ***10.1.1.4]***

OSA PORTA's OAT

IP Address	ARP Owner
10.1.1.1	Yes
10.1.1.10	Yes
10.1.1.2	No
10.1.3.1	No

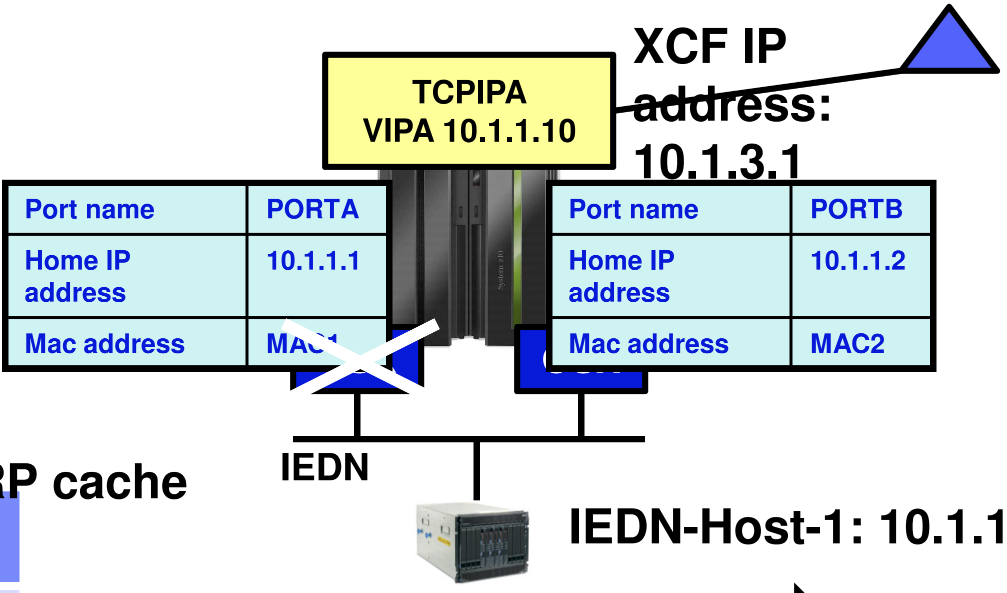
IEDN-Host-1's ARP cache

IP Address	MAC Address
10.1.1.1	MAC1
10.1.1.2	MAC2
10.1.1.3	MAC3
10.1.1.4	MAC4
10.1.1.10	MAC1

- OSX interfaces must be defined with the INTERFACE statement
- With VMAC and ROUTEALL, only addresses for which OSA has to perform ARP are registered in the OAT
- In all other cases, all HOME IP addresses will be registered in the OAT and the OAT content will be changed as the HOME lists change due to (dynamic) movement of IP addresses.
- OSX interfaces will do gratuitous ARP for the OSA interface IP address and for VIPA addresses that belong to the ***same*** subnet as the OSA interface.

Network connectivity resilience on the IEDN

z/OS TCP/IP supports interface recovery if multiple network interfaces to the same subnet exist.
In this example, both OSA PORTA and PORTB are connected to the IEDN (10.1.1.0/24 subnet).



Port name	PORTA
Home IP address	10.1.1.1
Mac address	MAC1

Port name	PORTB
Home IP address	10.1.1.2
Mac address	MAC2

When PORTA fails, PORTB is given ARP ownership of the addresses PORTA previously had. PORTB sends gratuitous ARPs to enable downstream hosts to update their ARP cache.

IEDN-Host-1's ARP cache

IP Address	MAC Address
10.1.1.1	MAC1
10.1.1.2	MAC2
10.1.1.10	MAC1

OSA PORTA fails

IEDN-Host-1's ARP ca

IP Address	MAC Address
10.1.1.1	MAC2
10.1.1.2	MAC2
10.1.1.10	MAC2

OSA PORTA's OAT

IP Address	ARP Owner
10.1.1.1	Yes
10.1.1.10	Yes
10.1.1.2	No
10.1.3.1	No

OSA PORTB's OAT

IP Address	ARP Owner
10.1.1.1	No
10.1.1.10	No
10.1.1.2	Yes
10.1.3.1	No

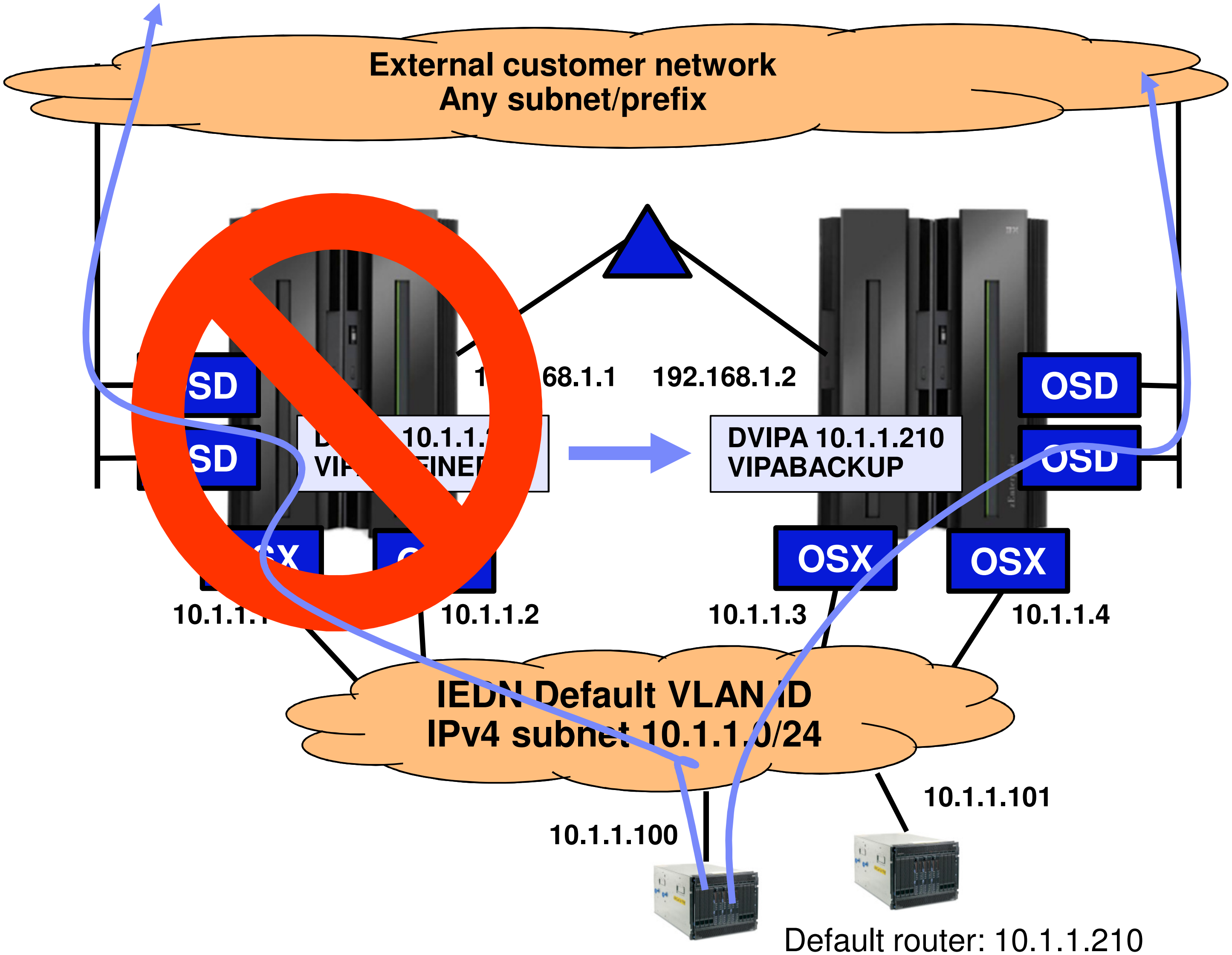
OSA PORTA's OAT

IP Address	ARP Owner
10.1.1.1	Yes
10.1.1.10	Yes
10.1.1.2	No
10.1.3.1	No

OSA PORTB's OAT

IP Address	ARP Owner
10.1.1.1	Yes
10.1.1.10	Yes
10.1.1.2	Yes
10.1.3.1	No

So Lets look at how the infrastructure DVIPA would work



Default router: 10.1.1.210

Iron Hand

Isolating traffic

- You may have multiple systems within your ensomble
- These systems may have to communicate to different levels of security
  - Example: XI50z DataPower might be an appliance that you are using for both Test and Production work
- Simple VLAN security may not be sufficient

Use AT-TLS

- You can use AT-TLS to segregate traffic at the application level
- Allows for strong authentication
- Server does not need to have any changes
  - Client needs to be TLS enabled
  - For XI50z the backside connector can be TLS
- Only have to perform the authentication not encryption
  - IEDN is secure

Other Notes

- IEDN does not allow connections external to the TOR to connect via L2
  - TOR does not support SPANNING TREE ALG
- IEDN is only Fiber and does not allow Copper connections
- Note connections in the TOR can be at 8992 but if the route is outside the TOR best to keep it at 1500
- Plan for your TCPIP changes to avoid unnecessary restarts
  - You must enable IPv6 in the BPX PARM
  - You must change the VTAMOPT as Ensomble=YES

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.youtube.com/user/zOSCommServer	IBM Communications Server YouTube Channel
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

Thank You!

IBM Comm Server

Find us on Facebook at
http://www.facebook.com/IBMCommserver

Follow us on Twitter at
http://www.twitter.com/IBM_Commserver

Visit the z/OS CS YouTube channel at
http://www.youtube.com/user/zOSCommServer

Questions?

Thomas Cosenza

System z I/T Specialist

IBM STG Lab Services

XI50z Team Lead

3031 N Rocky Point DR
Tampa, FL 33607-5878

Tel 720-395-7392

Mobile 813-270-9911

Email:
tcosenza@us.ibm.com