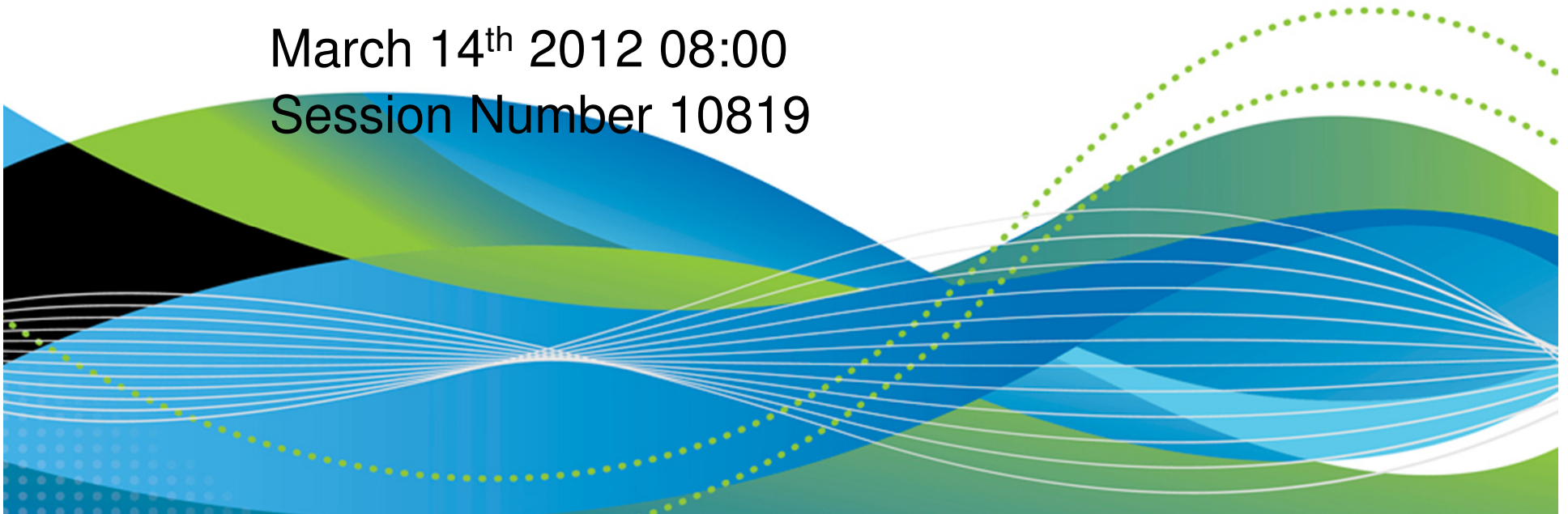


# zEnterprise Networking Lessons Learned

Thomas Cosenza [tcosenza@us.ibm.com](mailto:tcosenza@us.ibm.com)  
IBM STG Lab Services

March 14<sup>th</sup> 2012 08:00  
Session Number 10819



# Introduction

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

# zEnterprise

## Late 90s ~ Early 00's



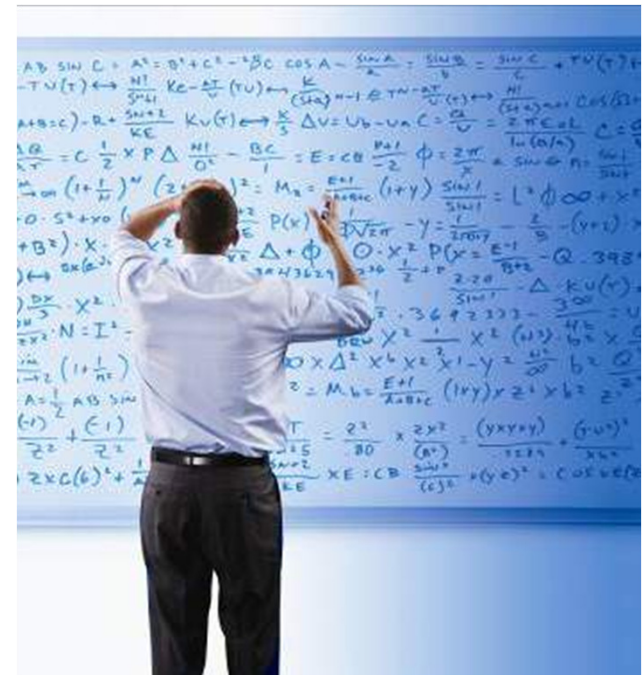
- Scaling drove performance
- Scaling drove down cost
- Performance constrained
- Active power dominates
- Focus on processor performance

## Today's Enterprise

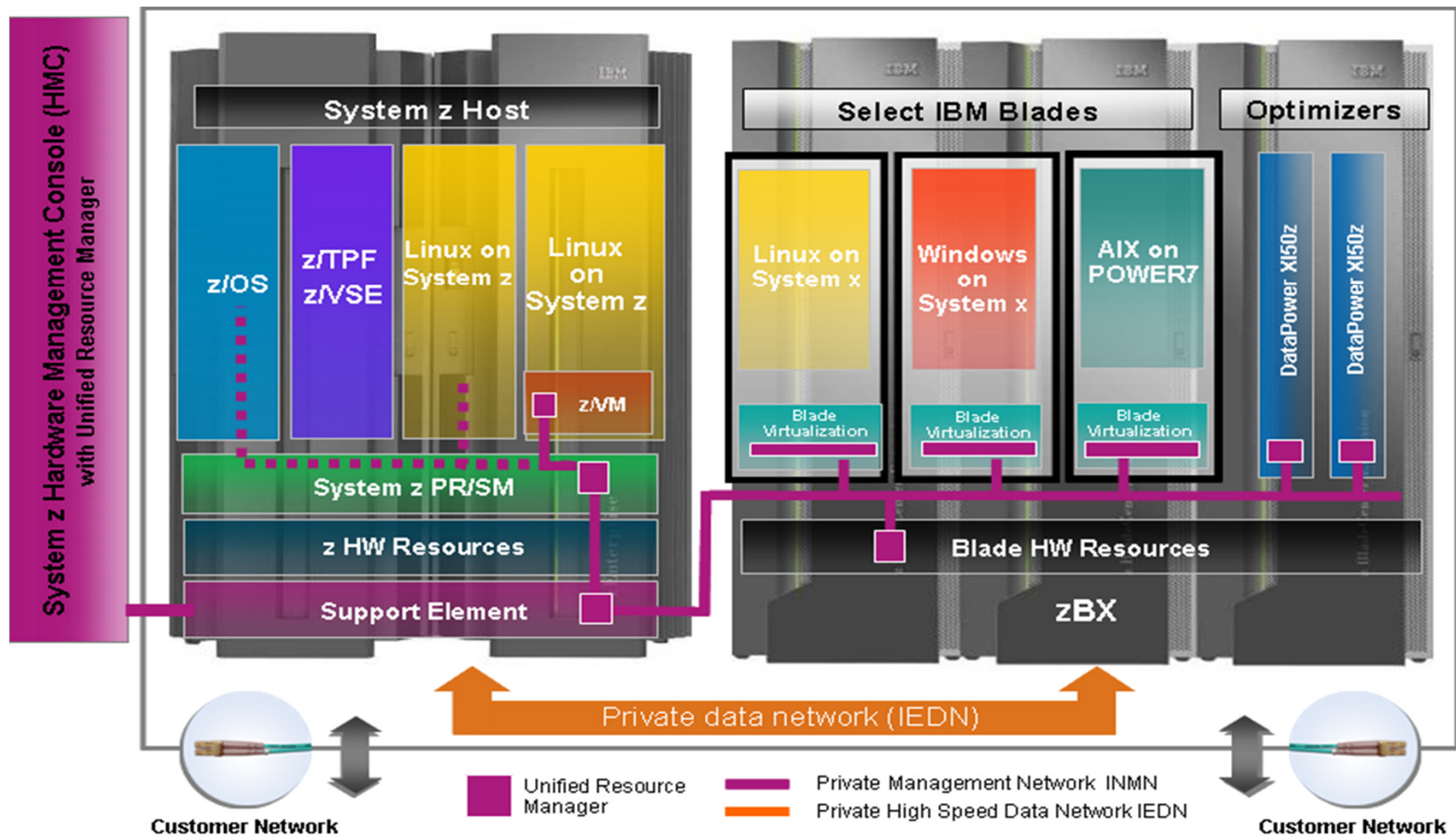
- INNOVATION drives performance
- Scaling drives down cost
- Power constrained
- Standby power dominates
- Focus on SYSTEM performance

# 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

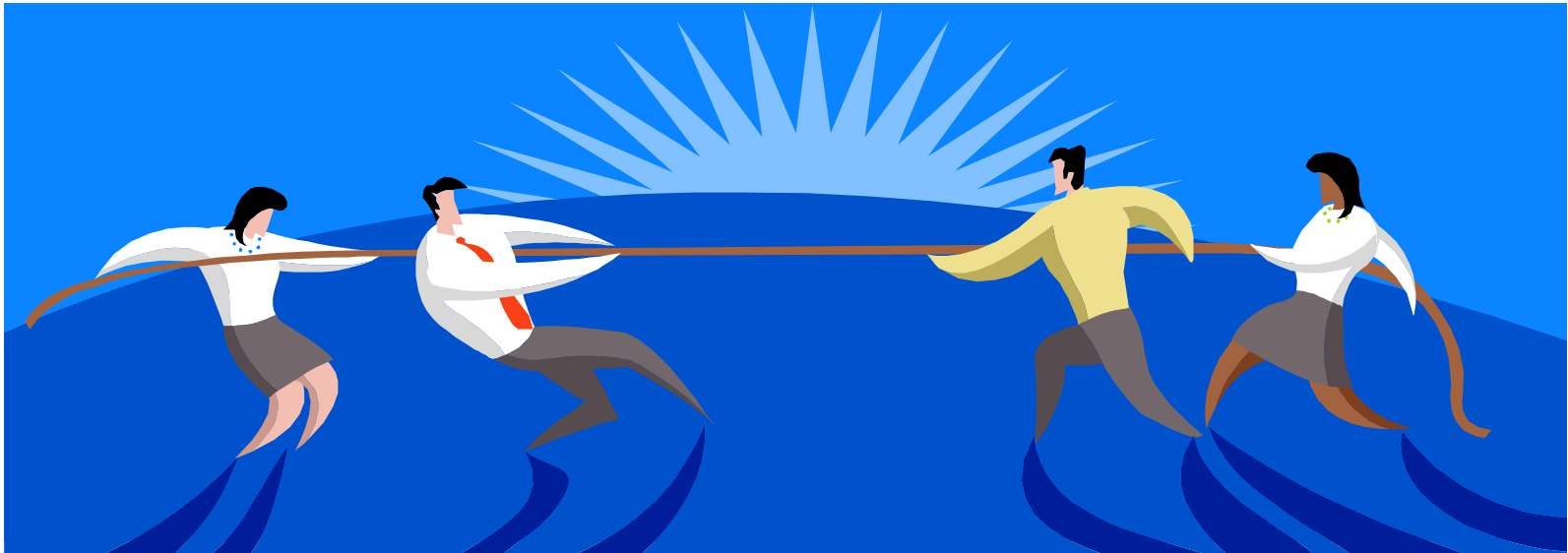




# The Only Constant is Change

- 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



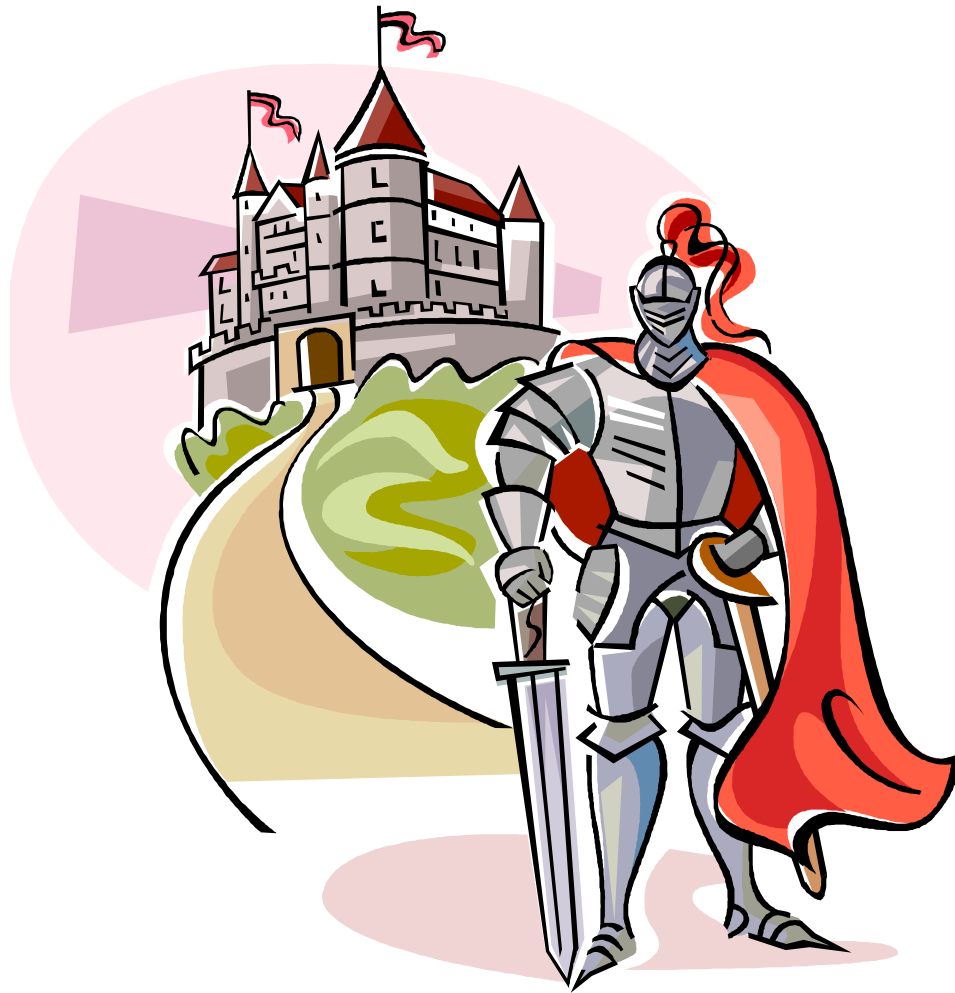
## Groups to add in

- 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

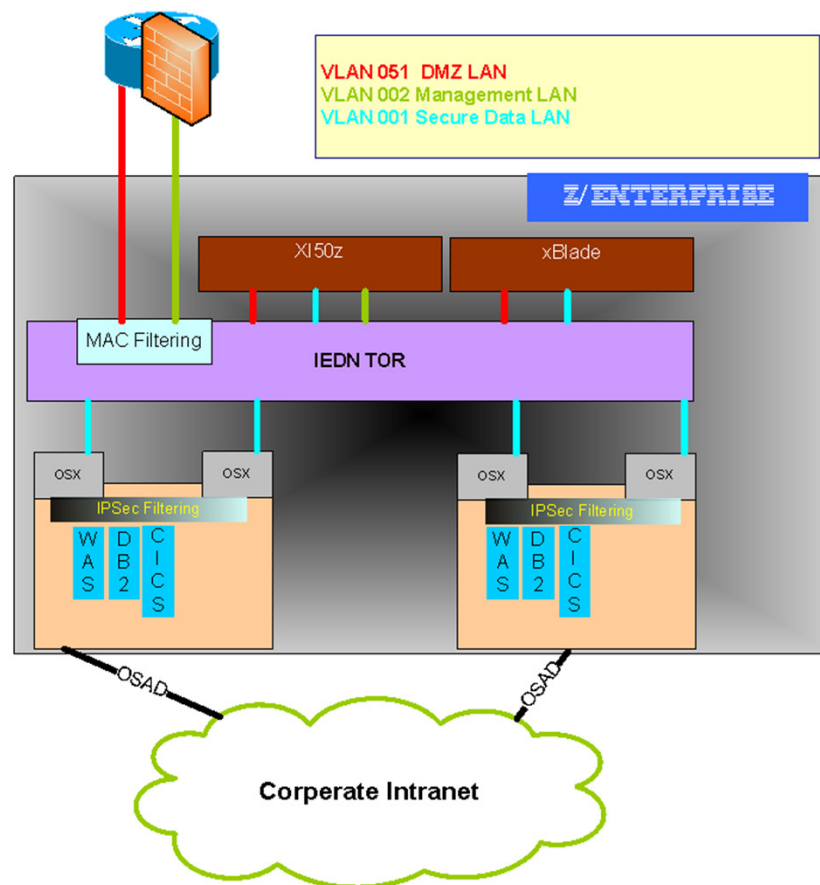
# Moving the Castle Wall



# 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



# Keeping the Heart Beat Going





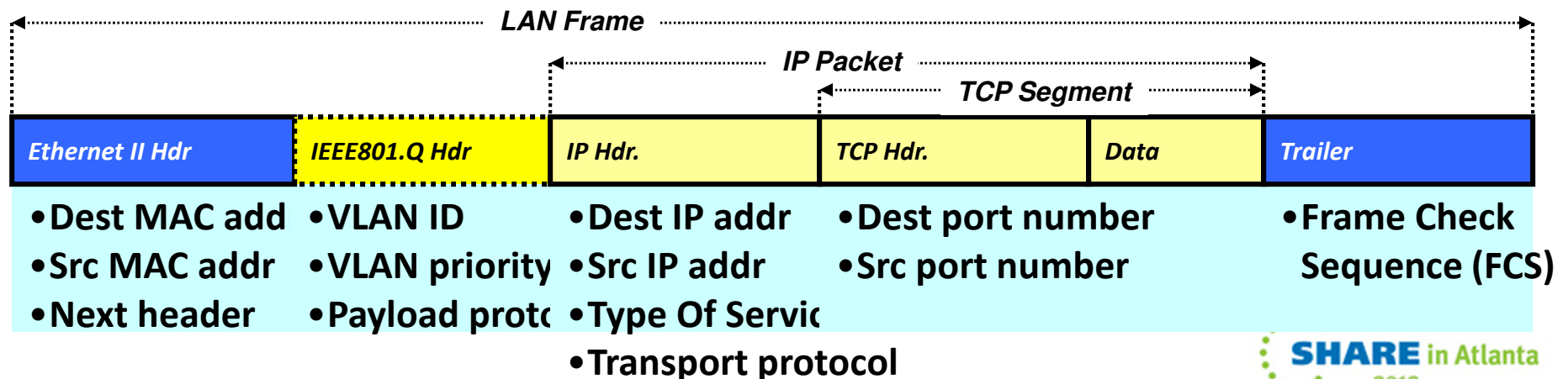
## .High Availability and Blades

- 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

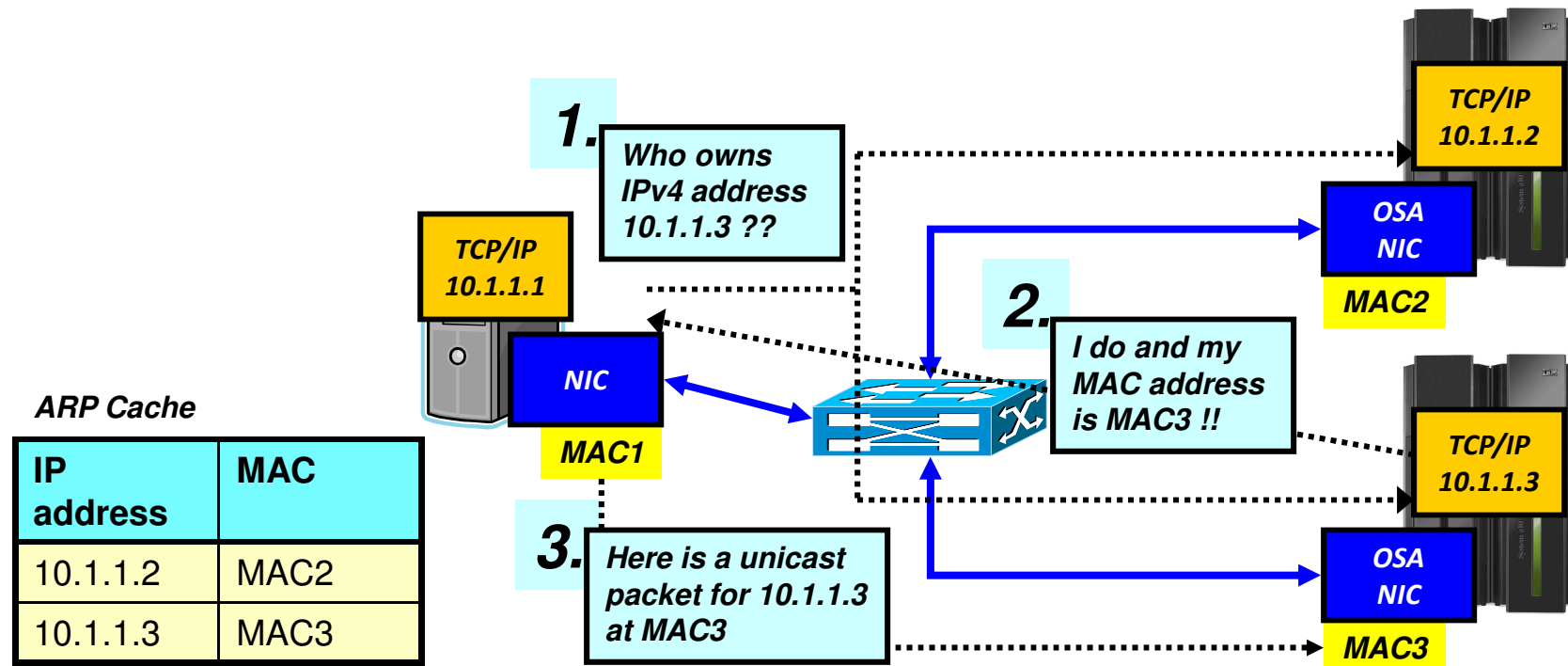


# .What is Layer 2 Routing

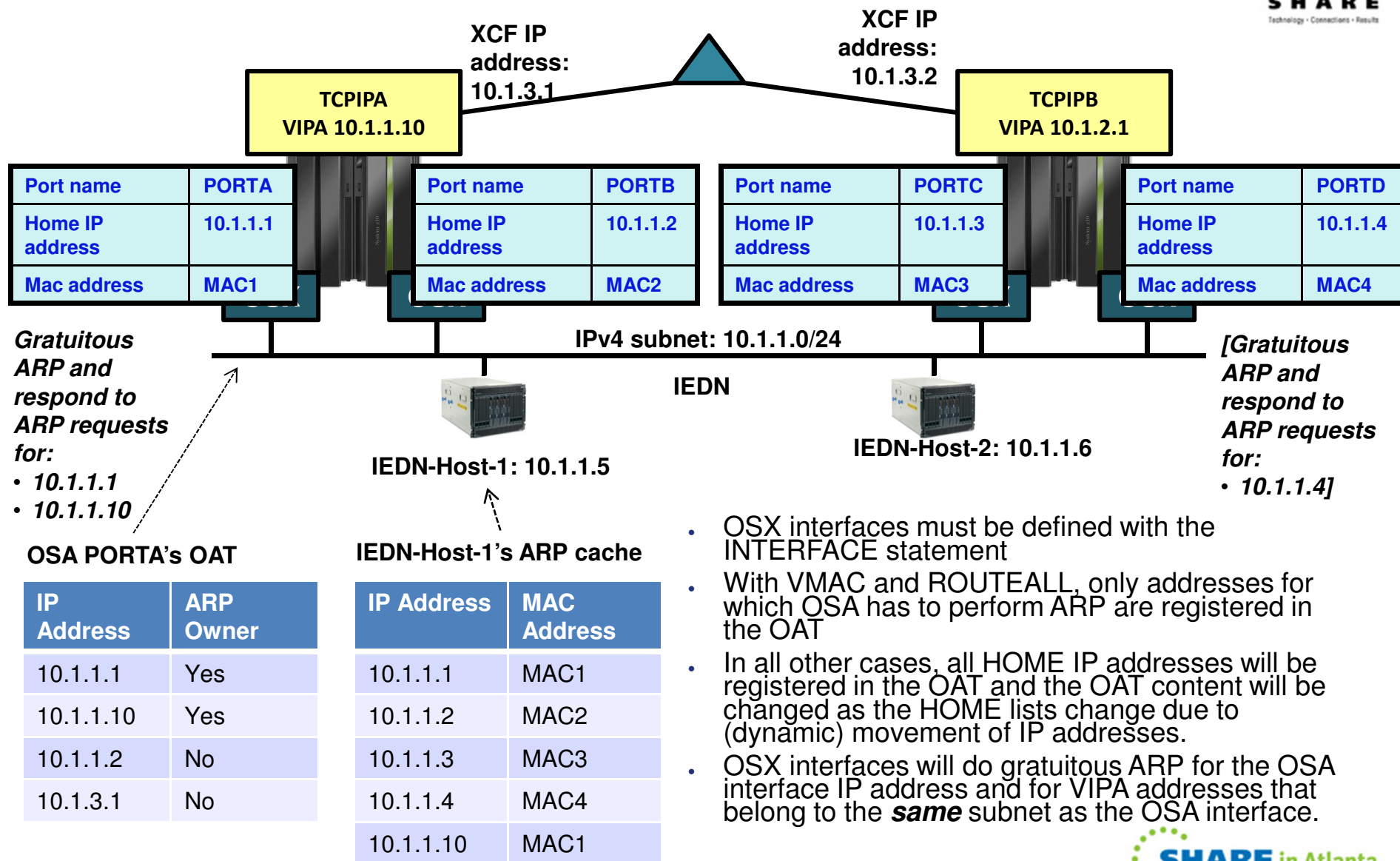
- The LAN infrastructure transports “Frames” between Network Interface Cards (NICs)
- Each NIC has a physical hardware address –called Media Access Control (MAC)
- Every frame comes from a MAC and goes to a MAC
- A frame carries a payload of a specified protocol type, such as ARP, IPv4, IPv6, SNA LLC2,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



# .So lets look at this process

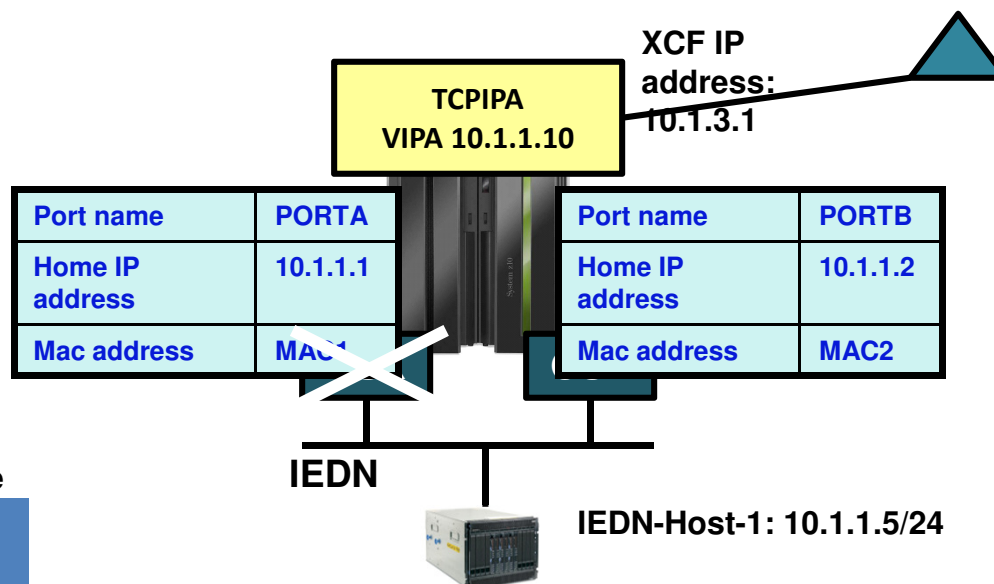


# .z/OS VIPA address visibility on the IEDN



# 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).



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        |

IEDN-Host-1's ARP cache

| 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        |

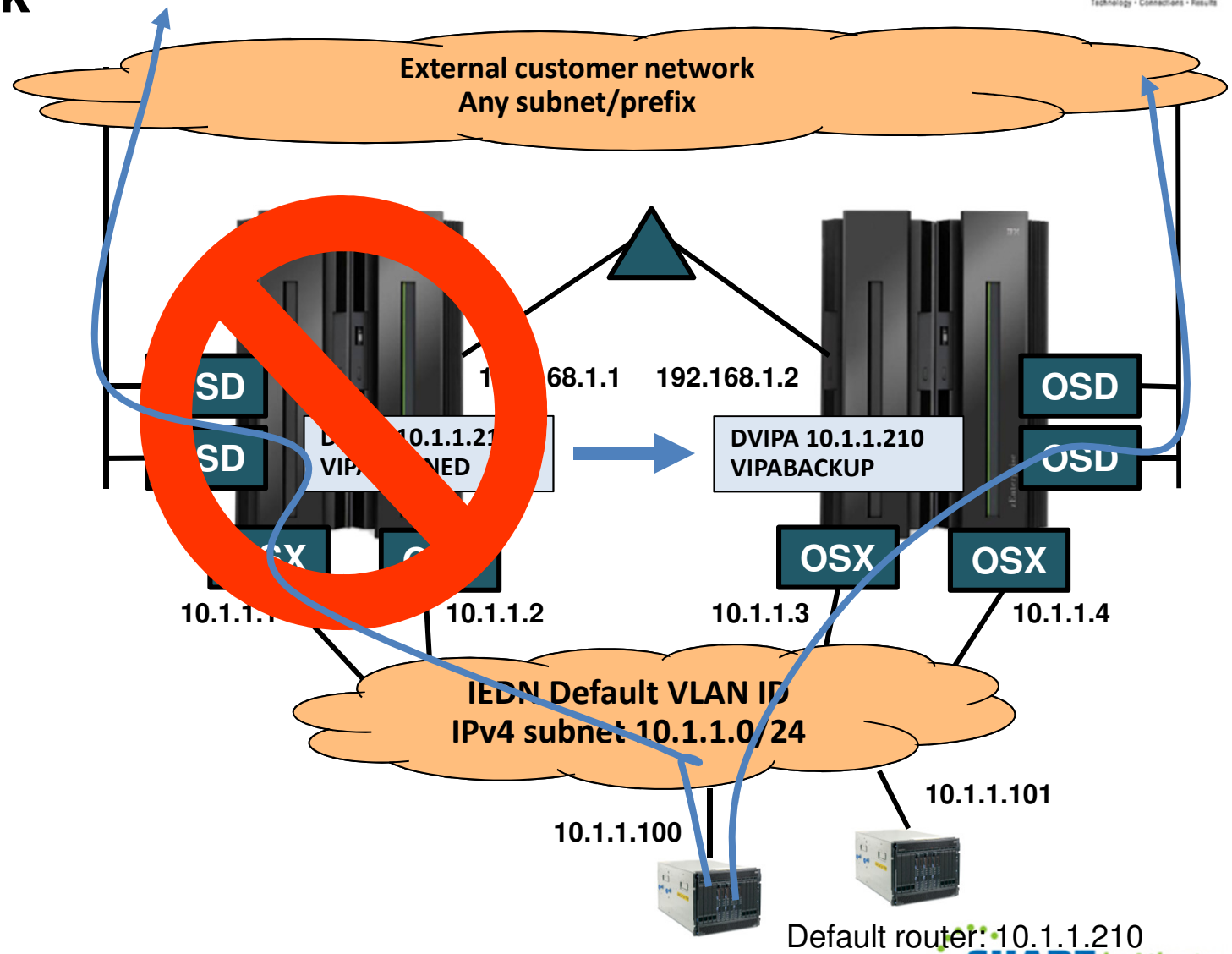
~~OSA PORTA's OAT~~

| <del>IP Address</del> | <del>ARP Owner</del> |
|-----------------------|----------------------|
| <del>10.1.1.1</del>   | <del>Yes</del>       |
| <del>10.1.1.10</del>  | <del>Yes</del>       |
| <del>10.1.1.2</del>   | <del>No</del>        |
| <del>10.1.3.1</del>   | <del>No</del>        |

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





# Iron Hand



# Isolating traffic




- You may have multiple systems within your ensemble
- 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

# .For more information



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



# .Thank You!



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



Follow us on Twitter at  
[http://www.twitter.com/IBM\\_Commserver](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*

**IBM**

*3031 N Rocky Point DR*

*Tampa, FL 33607-5878*

*Tel 720-395-7392*

*Mobile 813-270-9911*

*Email: [tcosenza@us.ibm.com](mailto:tcosenza@us.ibm.com)*