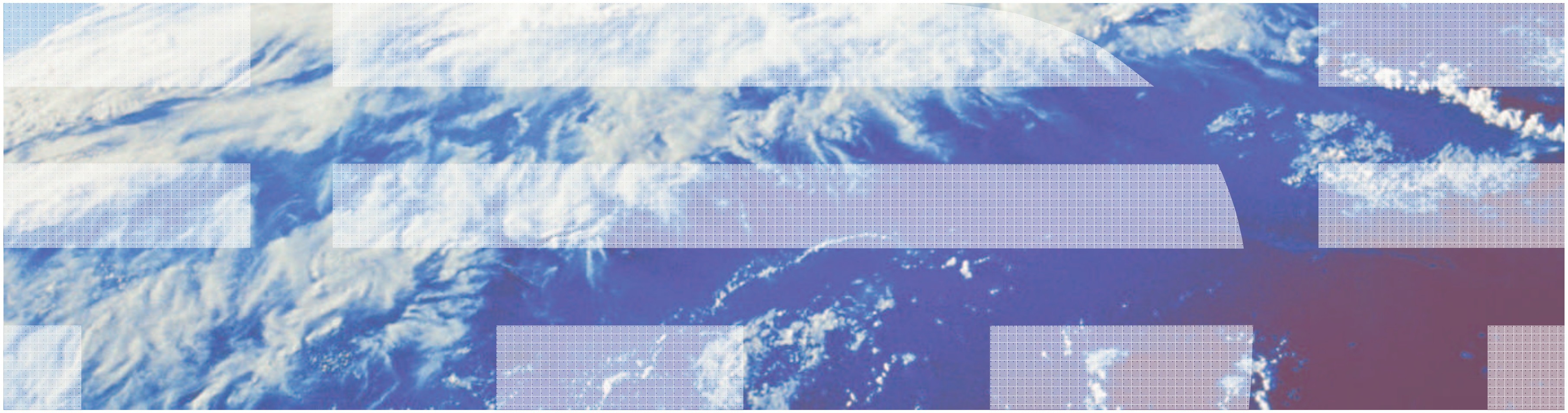
SHARE – Orlando – August 2011

Session 09563

Virtual Security Zones on z/VM

Alan Altmark
IBM Lab Services z/VM and Linux Consultant
Alan_Altmark@us.ibm.com



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

IBM*
IBM logo*
System Storage*
System z*
System z9*
System z10*
z9*
z10
z/OS*
z/VM*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

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

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.

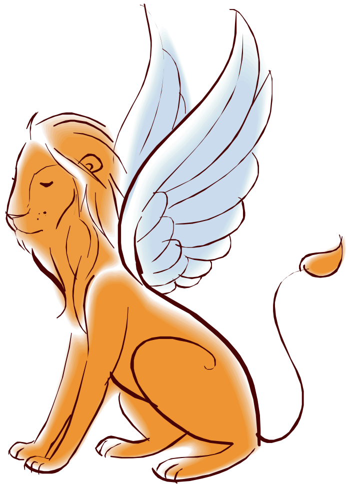
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

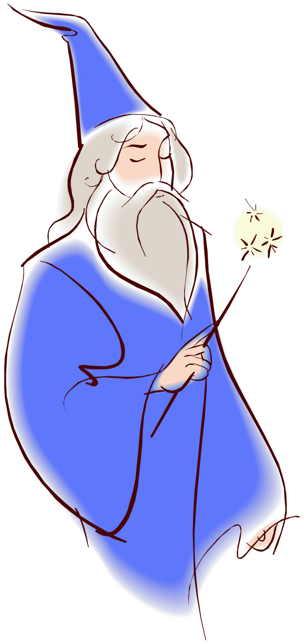
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

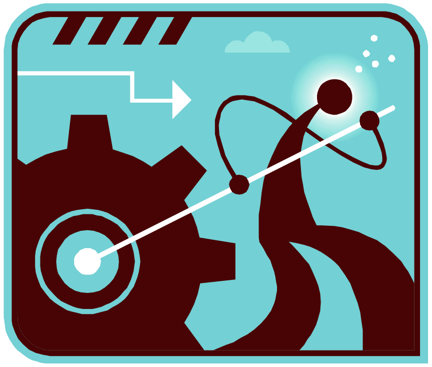
Agenda

- Introduction
- Securing System z hardware
- A multi-zone network
- VLANs and traffic separation
- Enforcing the rules

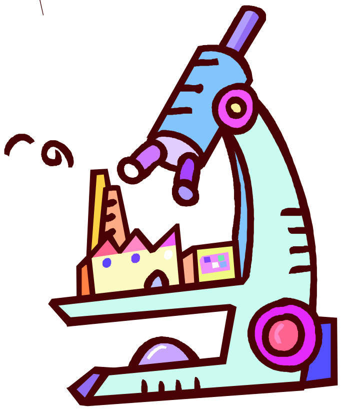
The Myth of Mainframe Security







The Reality of Mainframe Security



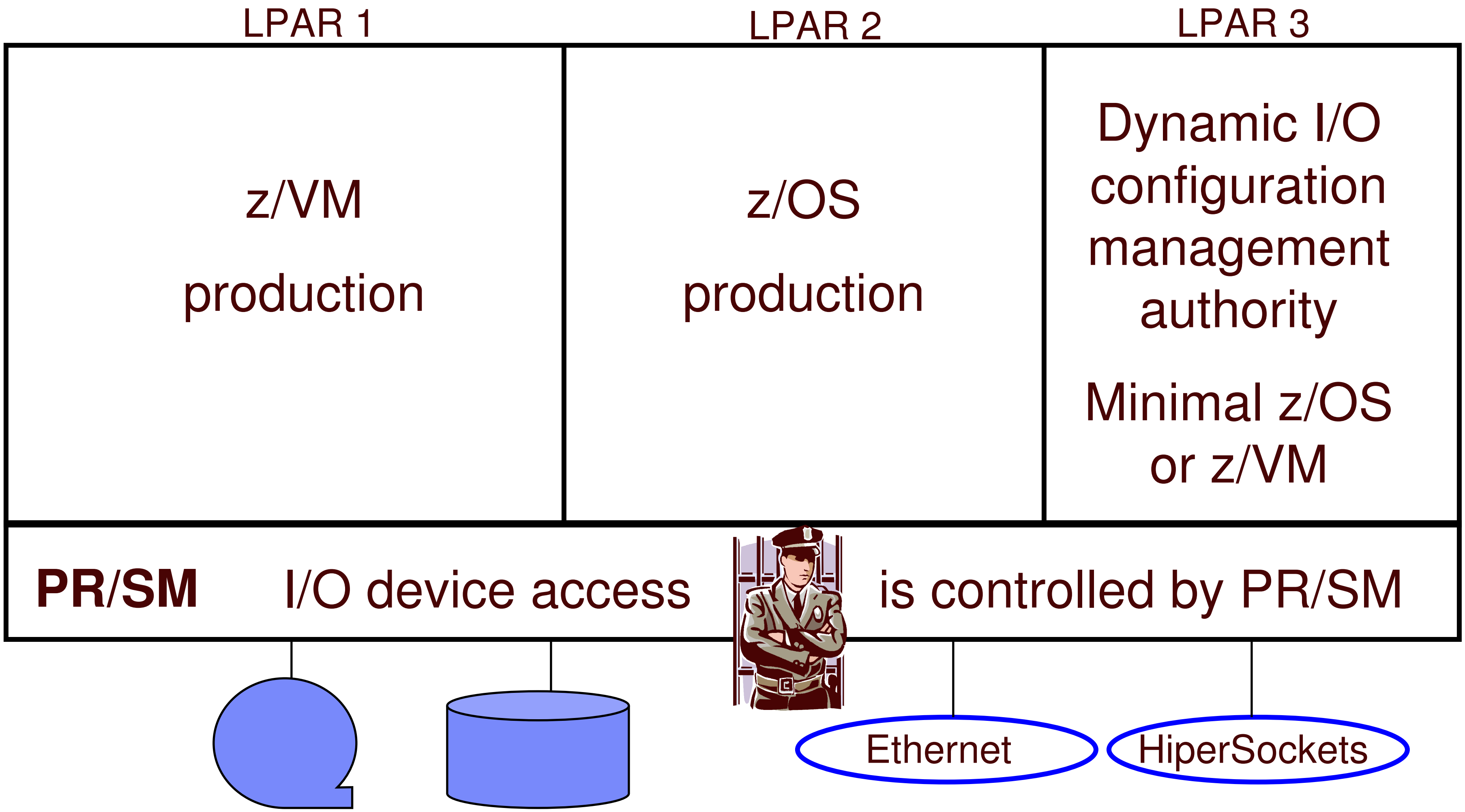
Securing the Hardware

z/VM Security begins with System z security

- Protect the HMC
  - Don’t share user IDs
  - …but don’t be afraid to connect it to your internal network
  - Limit span of control as appropriate; add roles

- Protect the I/O configuration
  - Create a separate LPAR that is authorized to modify the I/O config
  - Give partitions access only to devices they require

System z Hardware Security



LPAR 1

z/VM

production

LPAR 2

z/OS

production

LPAR 3

Dynamic I/O configuration management authority

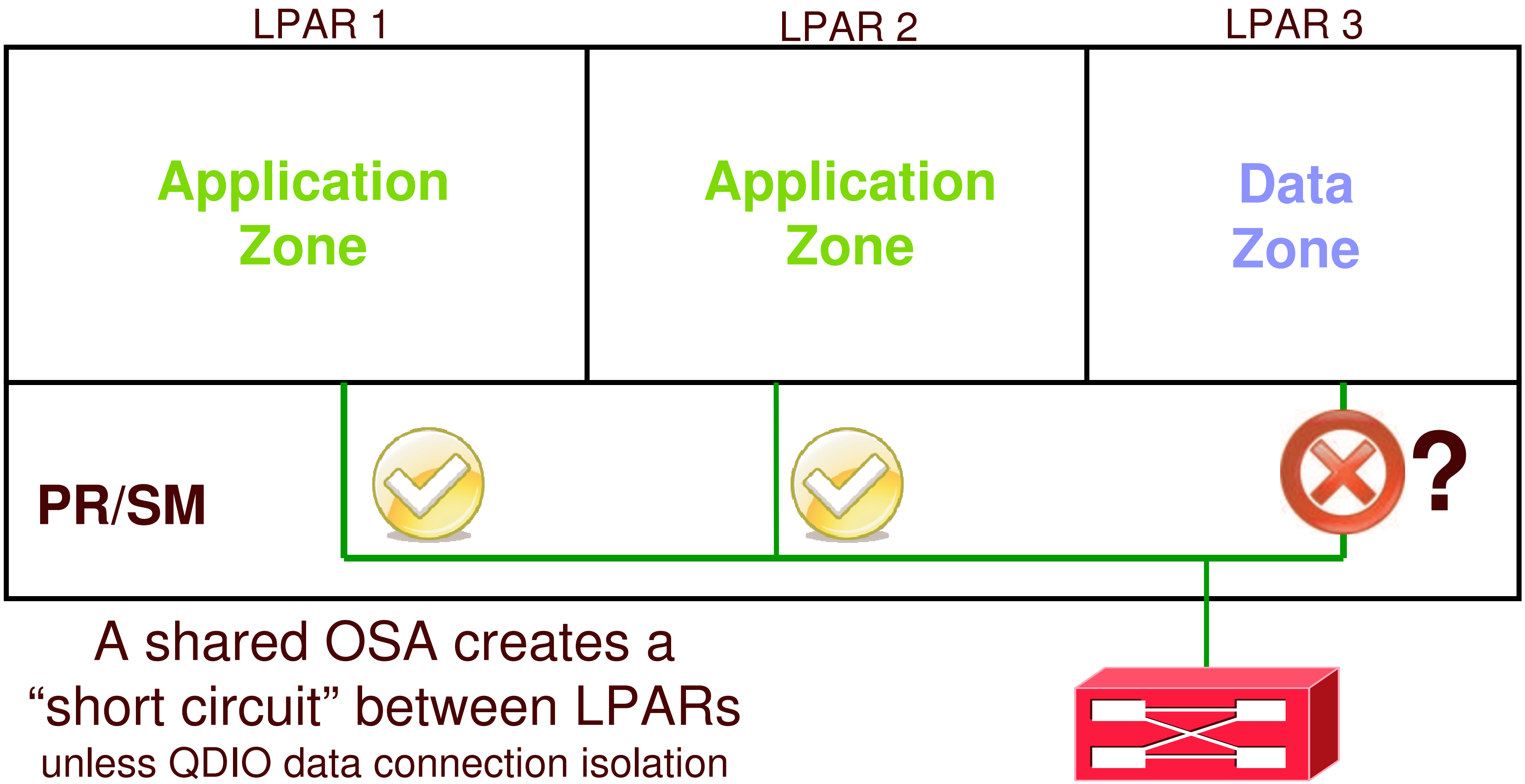
Minimal z/OS or z/VM

PR/SM I/O device access is controlled by PR/SM

Ethernet

HiperSockets

WARNING: Shared Open Systems Adapters

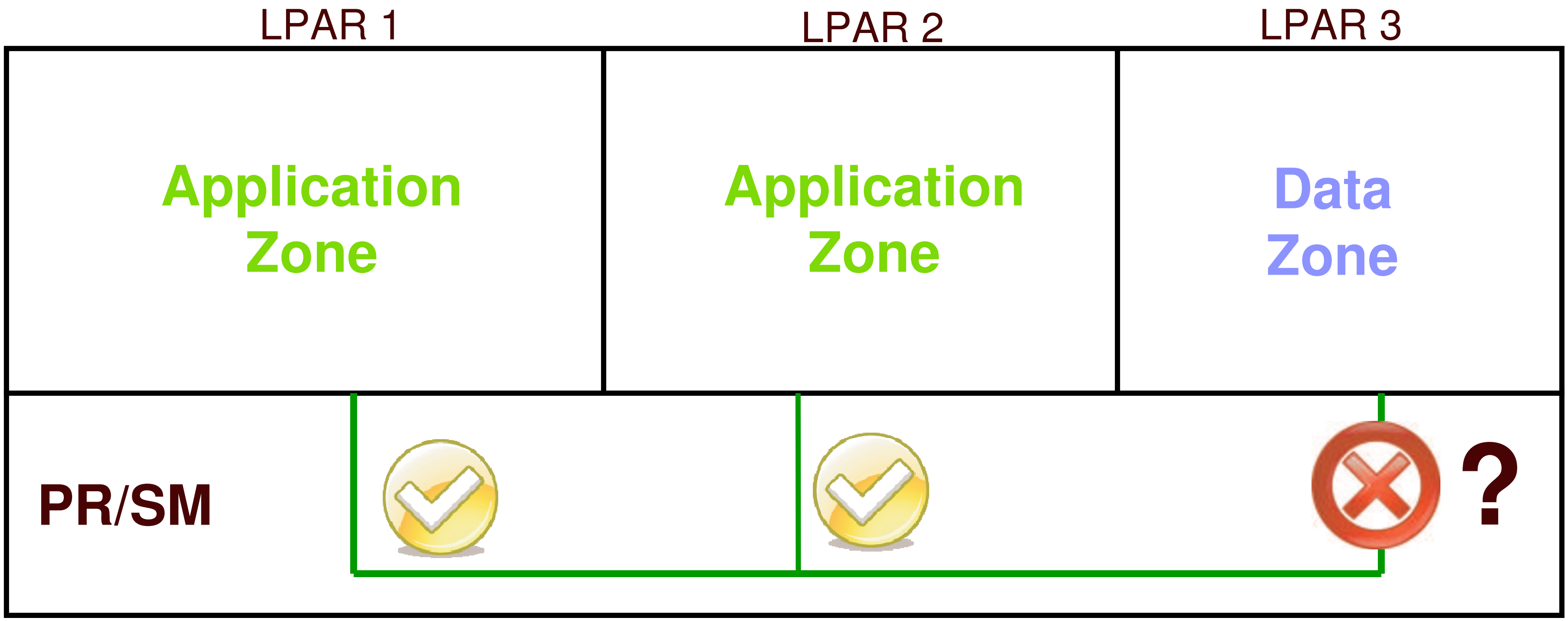


A shared OSA creates a "short circuit" between LPARs

unless QDIO data connection isolation is used on z10 or z196

IBM

WARNING: HiperSockets

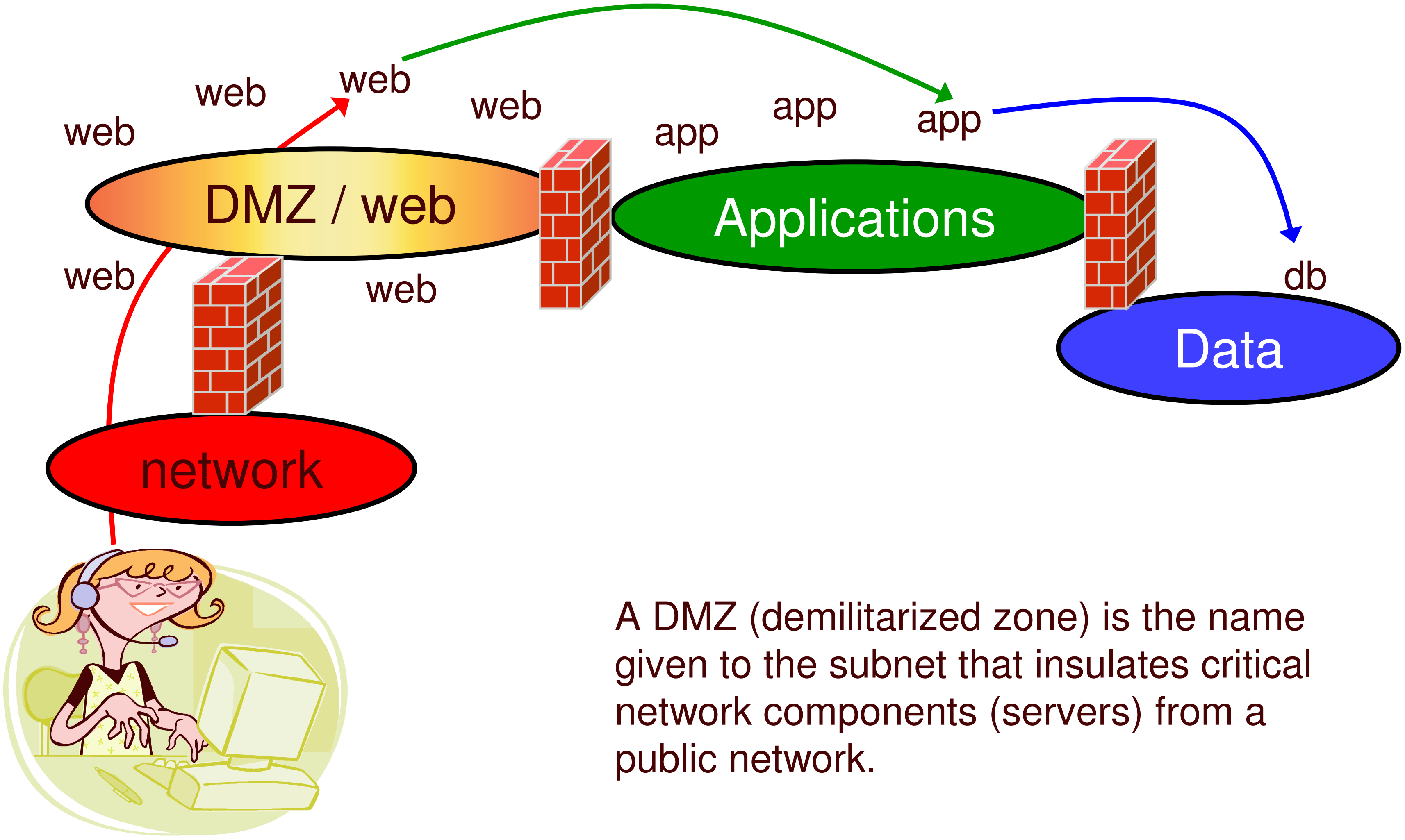


A HiperSocket is a LAN segment.

Treat is like one.

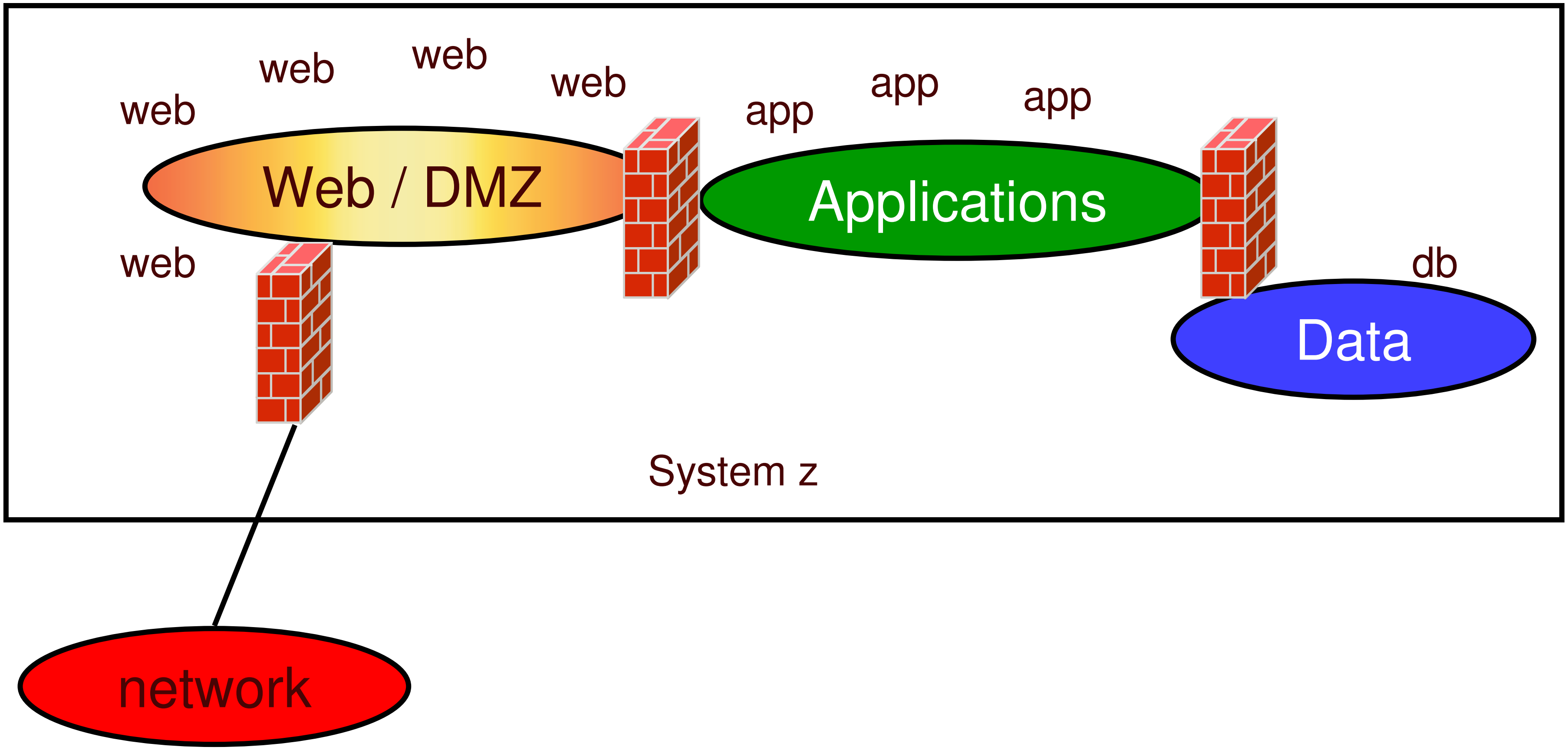
Multi-zone networks

Multi-zone Network



A DMZ (demilitarized zone) is the name given to the subnet that insulates critical network components (servers) from a public network.

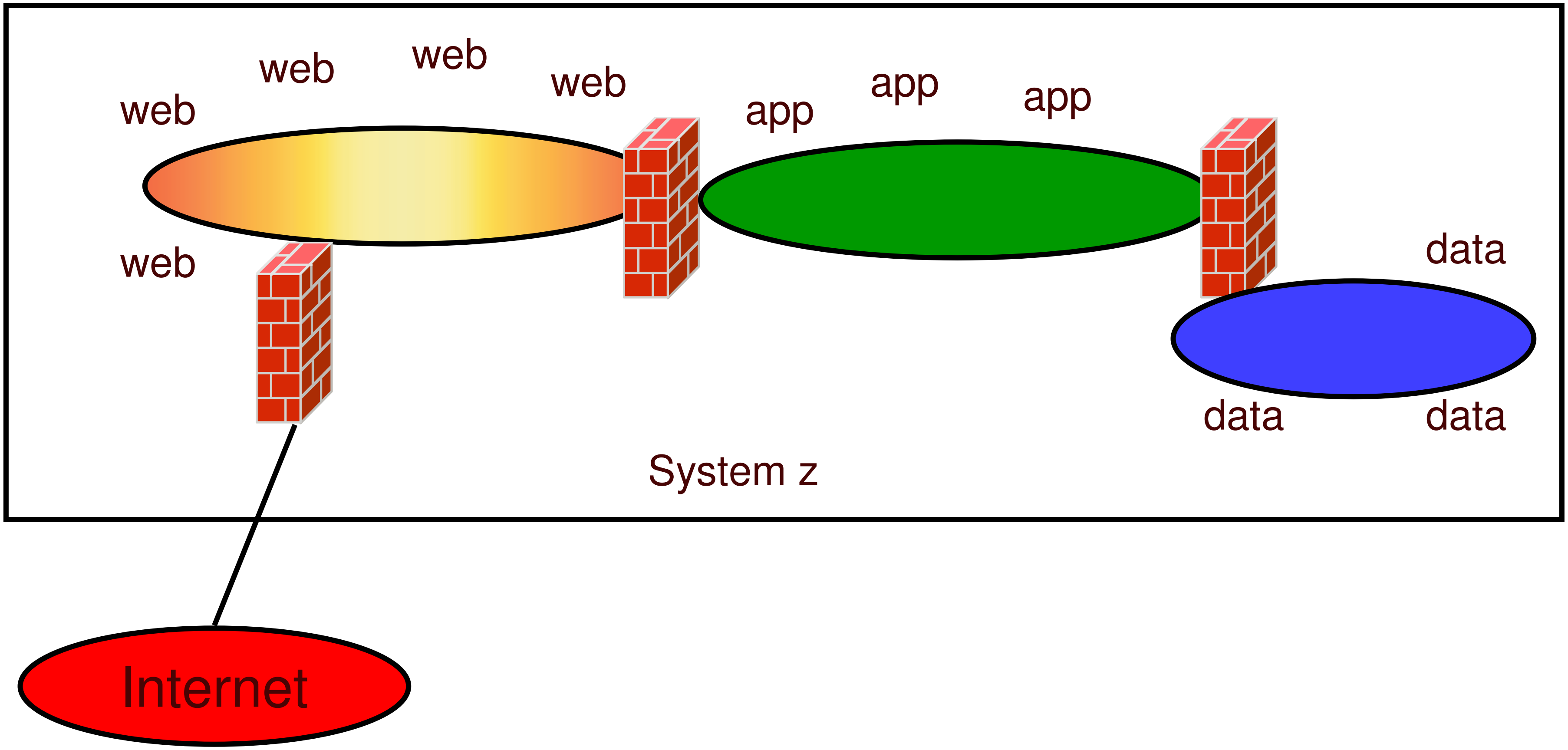
Multi-zone Network on System z



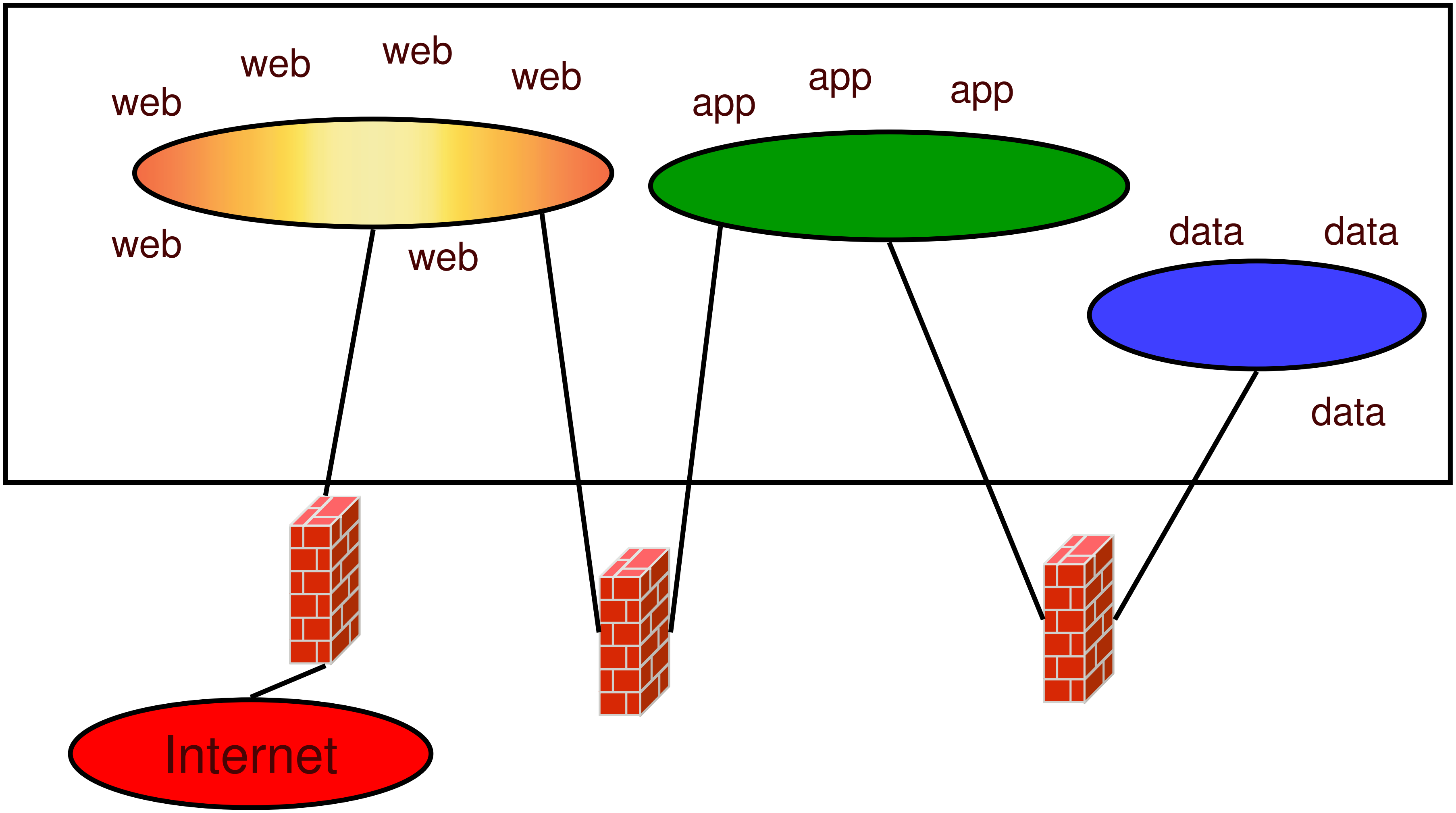
Firewalls

“Where, oh, where has my firewall gone?”

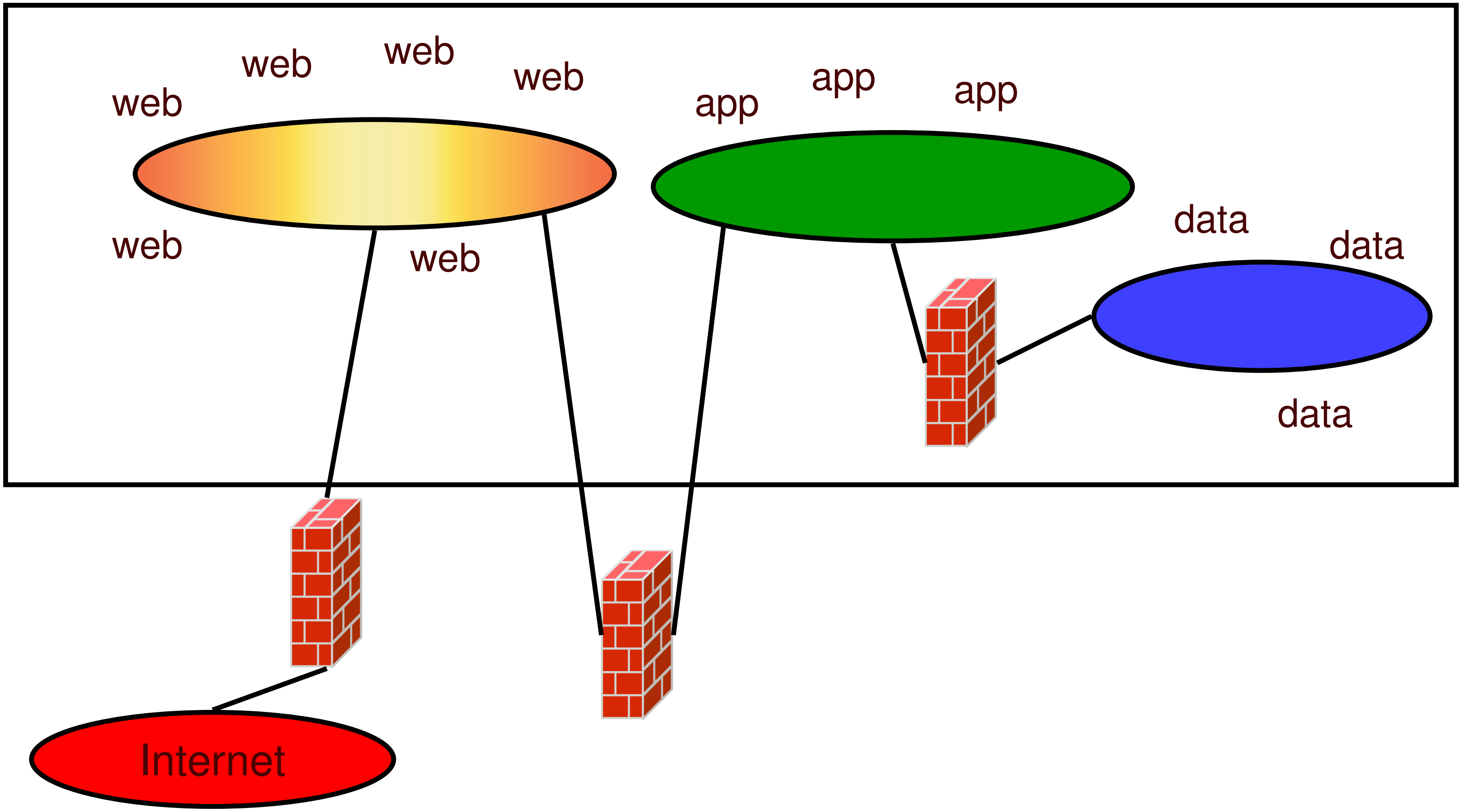
Inboard (internal) firewalls



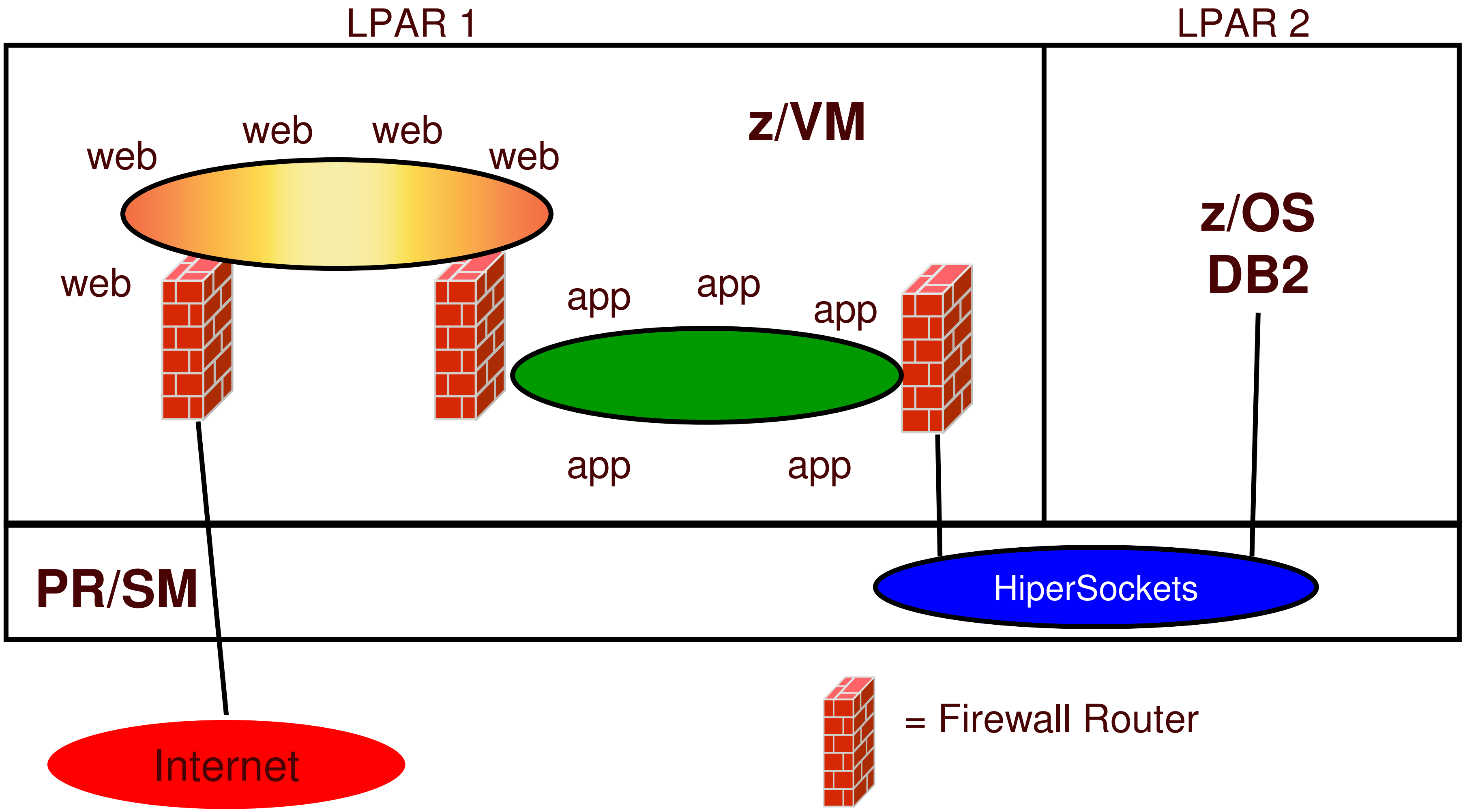
Outboard (external) firewalls



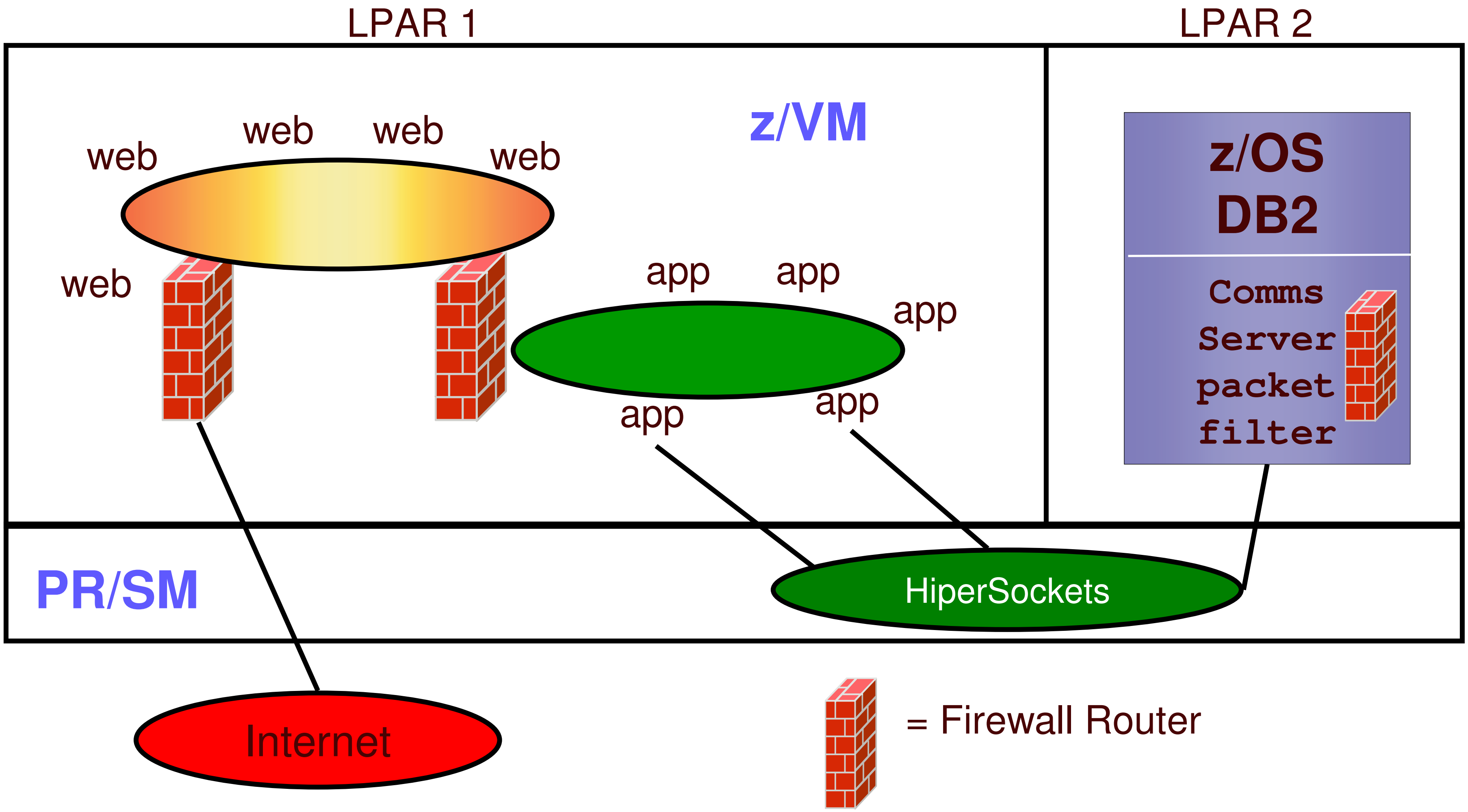
Combination firewalls



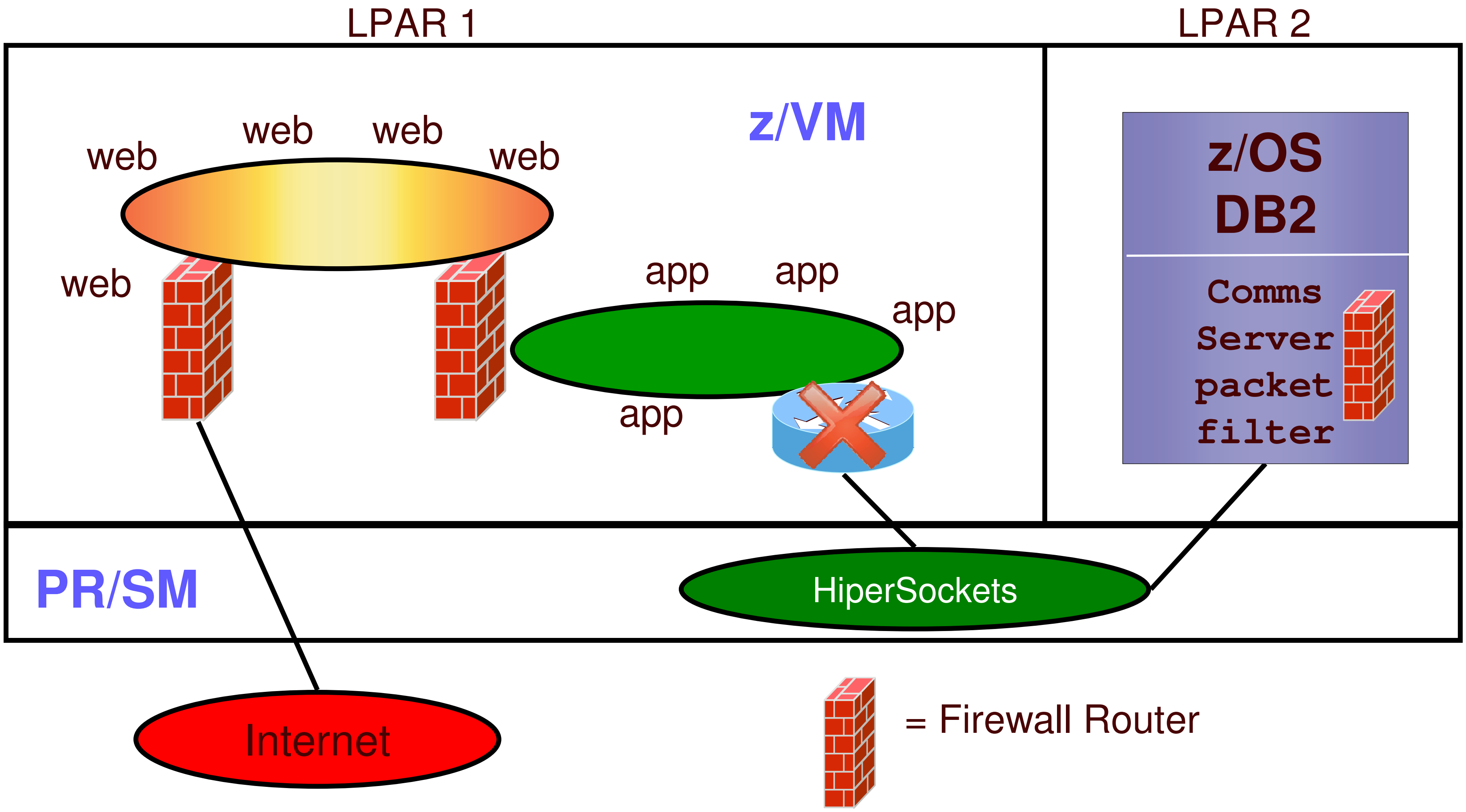
Guest LANs with HiperSockets



HiperSockets & z/OS packet filters

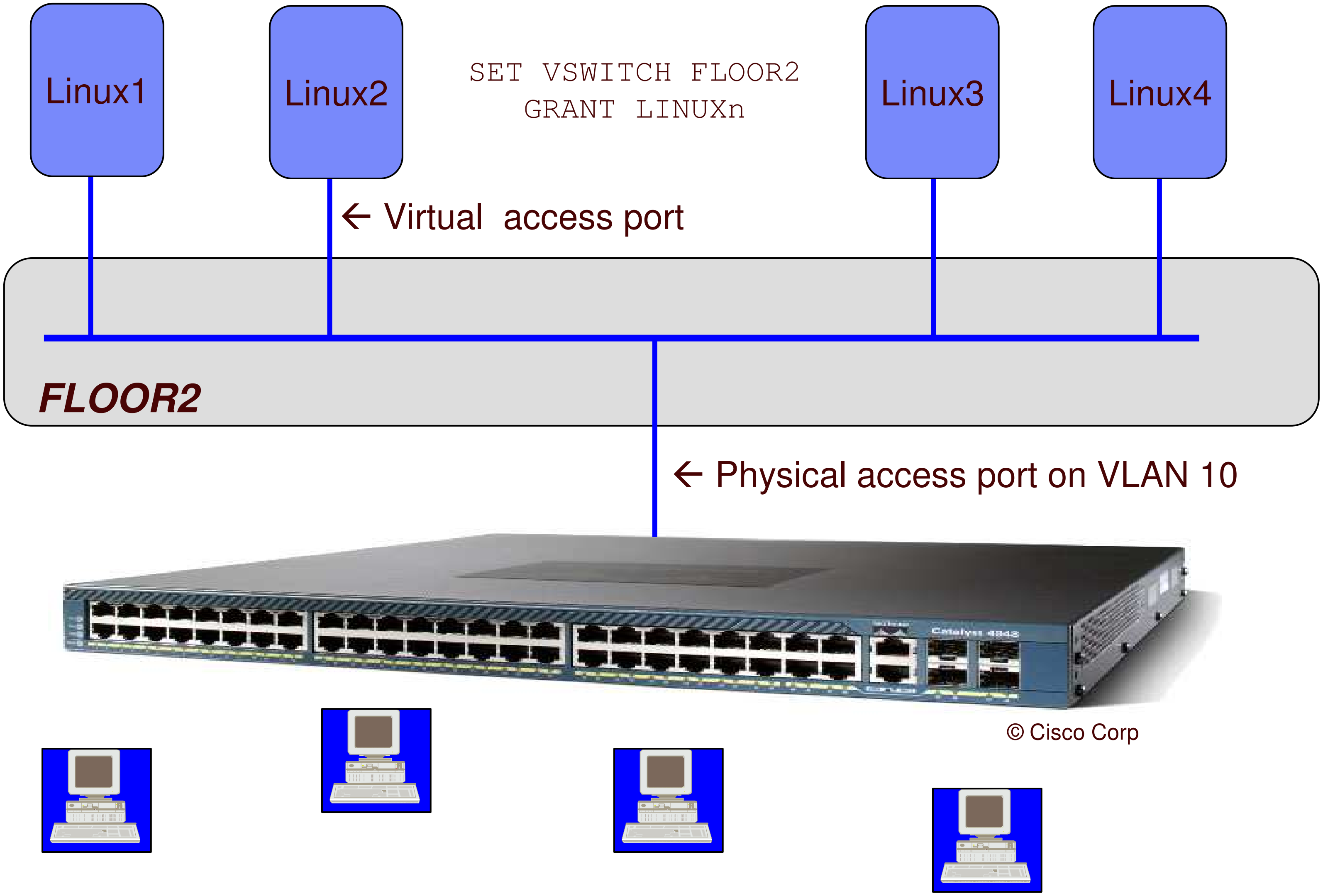


"Tempting, but no…"



Virtual Switches
VLANs and traffic separation

VLAN-unaware VSWITCH



Linux1

Linux2

```
SET VSWITCH FLOOR2
GRANT LINUXn
```

Linux3

Linux4

← Virtual access port

FLOOR2

← Physical access port on VLAN 10

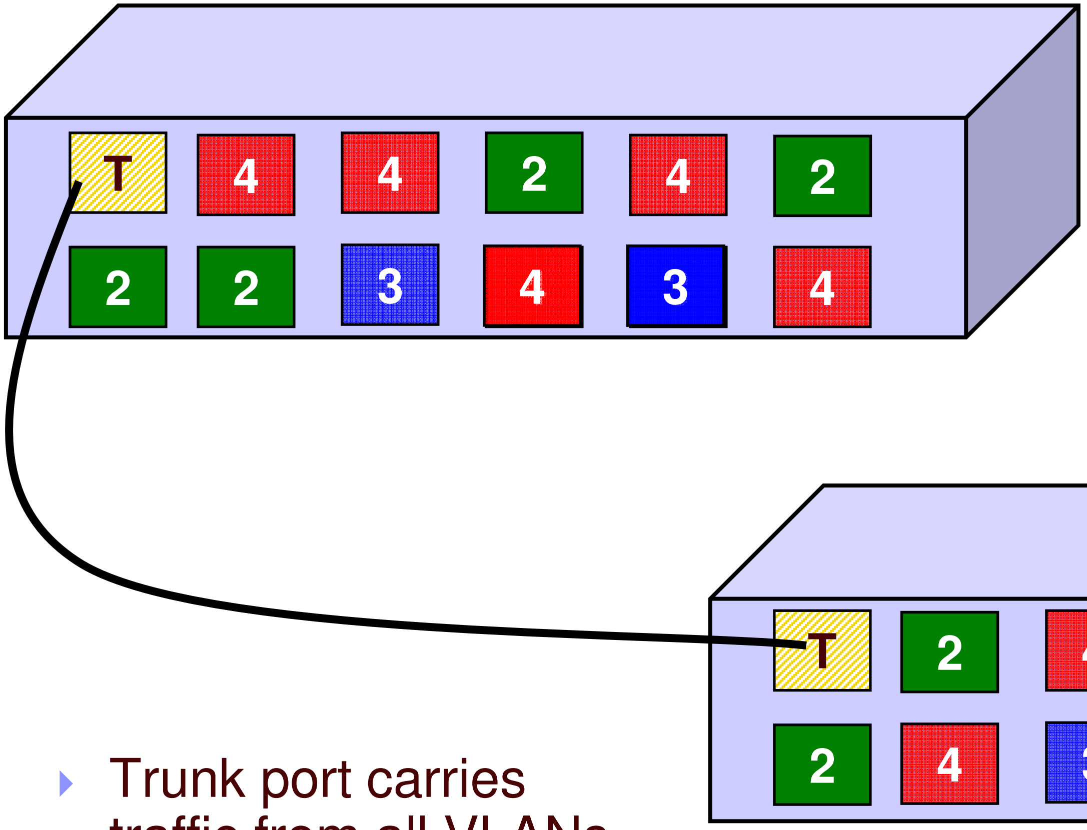
© Cisco Corp

IEEE VLANs

© Cisco Corp

- If you run out of ports, you don’t throw it away, you daisy chain (“trunk”) it to another switch.

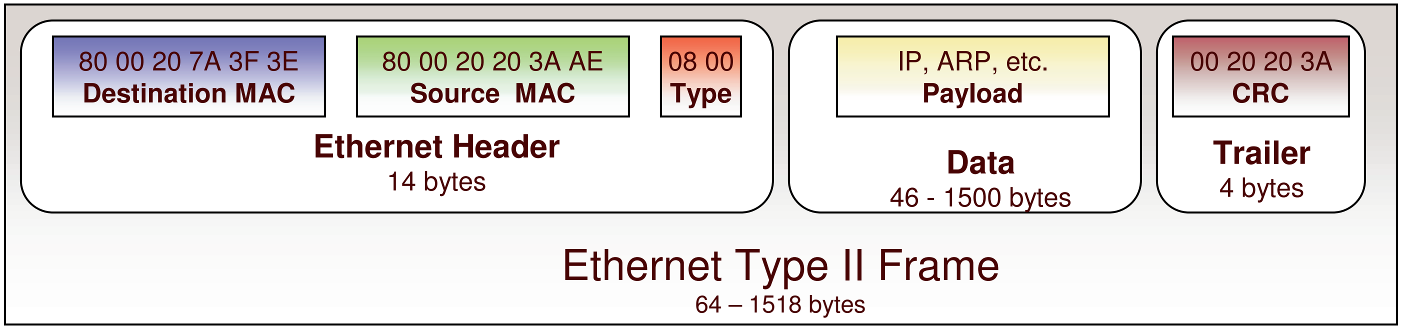
Trunk Port vs. Access Port



- Access port carries traffic for a single VLAN
- Host not aware of VLANs

- Trunk port carries traffic from all VLANs
- Every frame is tagged with the VLAN id

Access vs. Trunk



80 00 20 7A 3F 3E
Destination MAC

80 00 20 20 3A AE
Source MAC

08 00
Type

Ethernet Header
14 bytes

IP, ARP, etc.
Payload

Data
46 - 1500 bytes

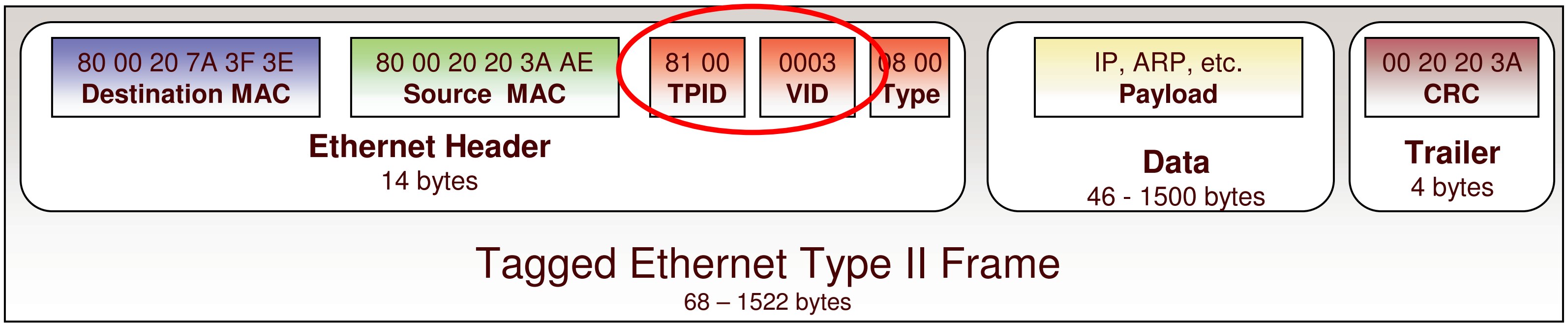
00 20 20 3A
CRC

Trailer
4 bytes

Ethernet Type II Frame
64 – 1518 bytes

Access port and Trunk port

When used on a trunk port, the switch will associate (but not tag) it with the **native** VID



80 00 20 7A 3F 3E
Destination MAC

80 00 20 20 3A AE
Source MAC

81 00
TPID

0003
VID

08 00
Type

Ethernet Header
14 bytes

IP, ARP, etc.
Payload

Data
46 - 1500 bytes

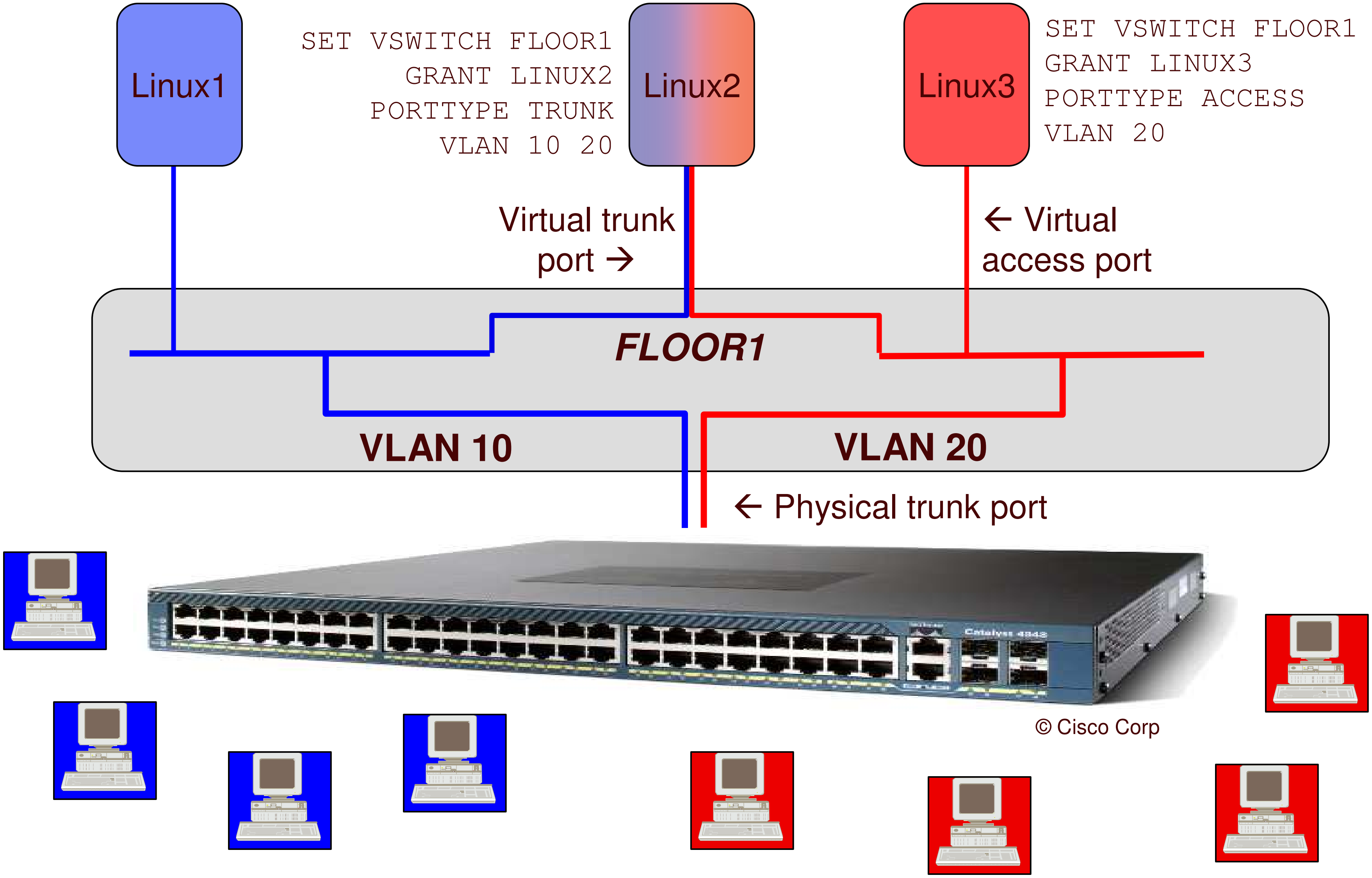
00 20 20 3A
CRC

Trailer
4 bytes

Tagged Ethernet Type II Frame
68 – 1522 bytes

Trunk port

VLAN-aware VSWITCH

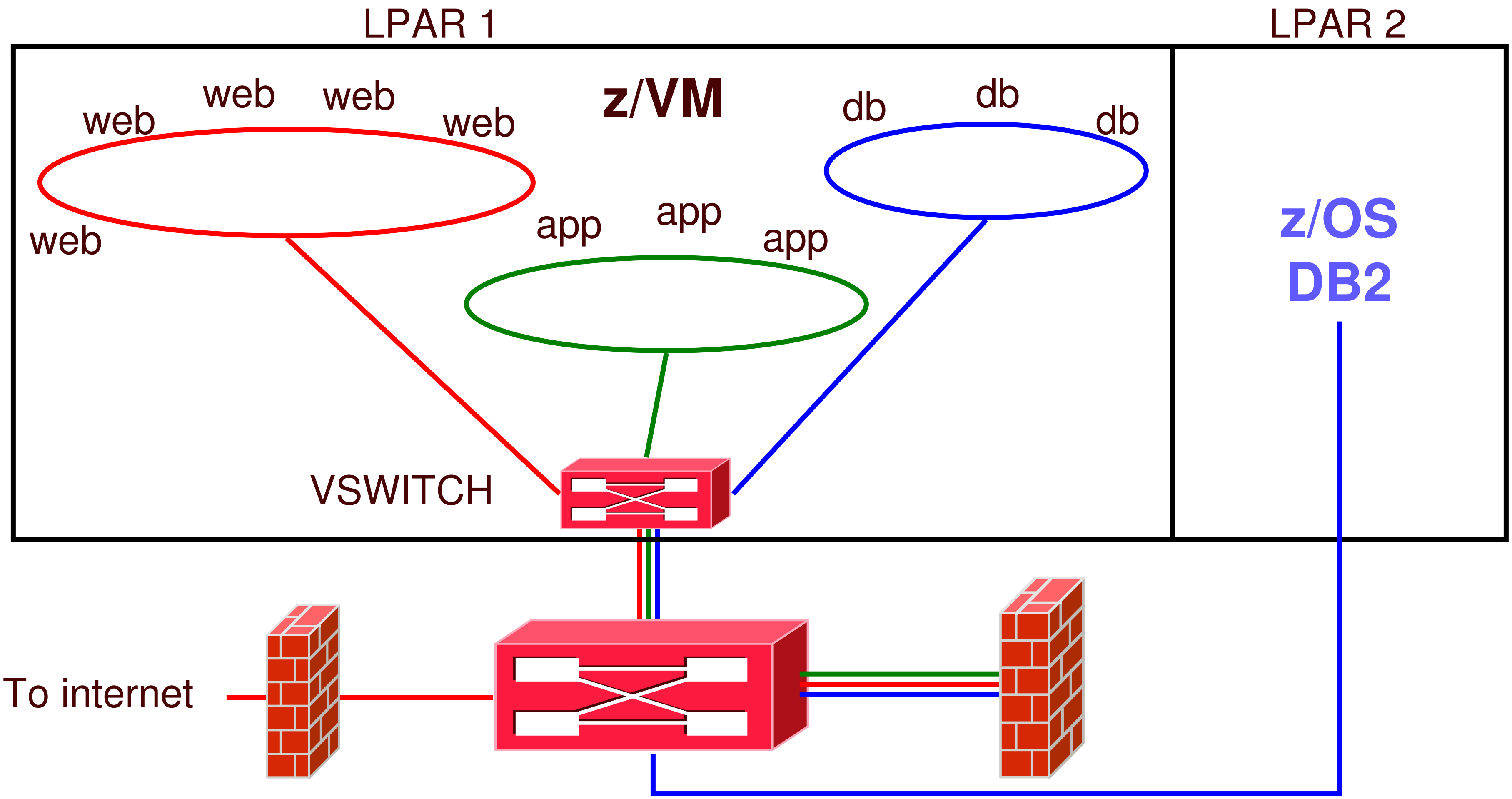


```
SET VSWITCH FLOOR1
      GRANT LINUX2
   PORTTYPE TRUNK
     VLAN 10 20
```

```
SET VSWITCH FLOOR1
GRANT LINUX3
PORTTYPE ACCESS
VLAN 20
```

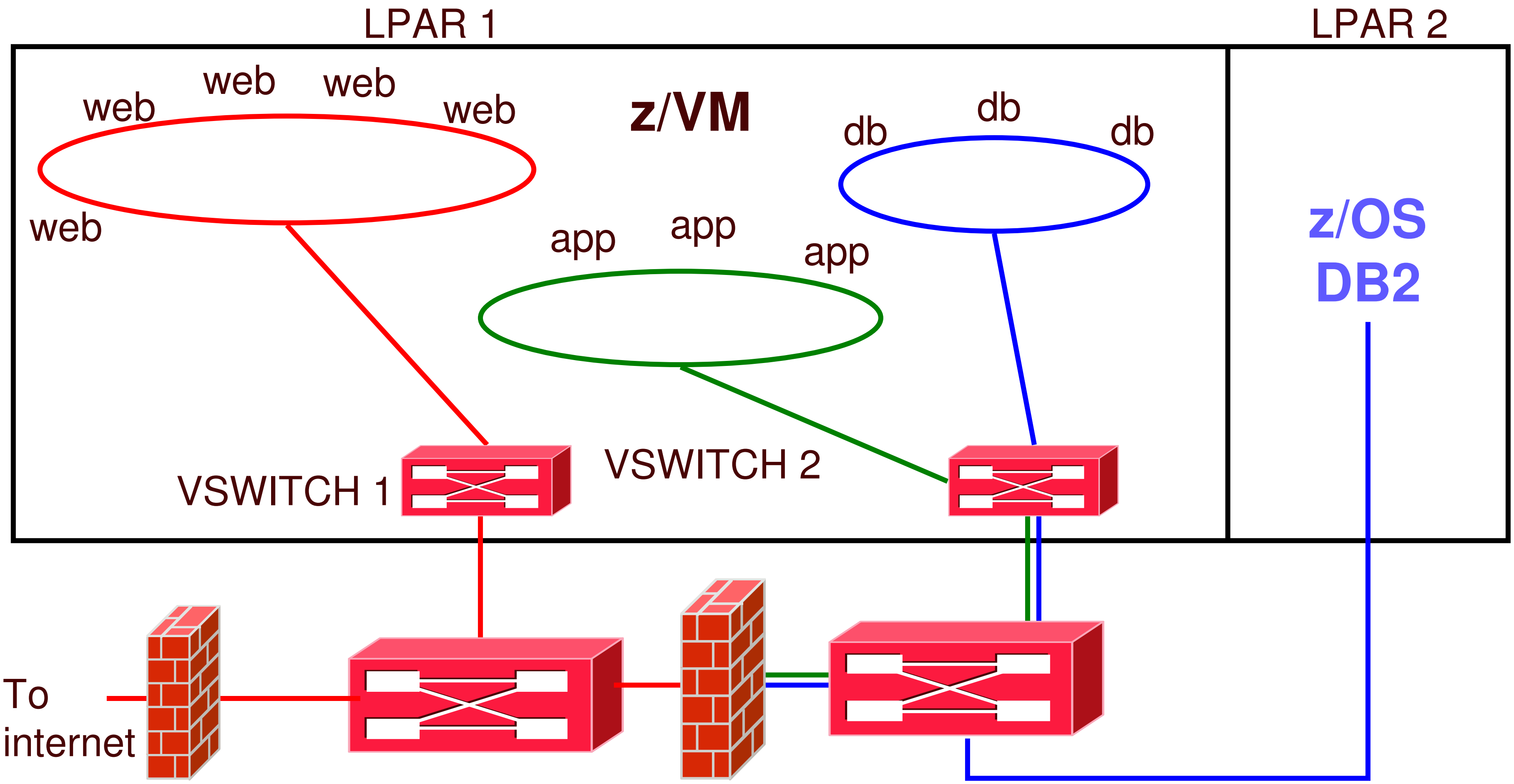
© Cisco Corp

Network with VSWITCH (fully shared)



With 1 VSWITCH, 3 VLANs, and a multi-domain firewall

Multi-zone Network with VSWITCH (red zone physical isolation)



With 2 VSWITCHes, 3 VLANs, and a multi-domain firewall

Enforcing the Separation

Turn off backchannel communications

- No user-defined Guest LANs
  - VMLAN LIMIT TRANSIENT 0
- No virtual CTC
  - MODIFY COMMAND DEFINE IBMCLASS G PRIVCLASS M
- No IUCV
  - Use explicit IUCV authorization in the directory, not IUCV ALLOW or IUCV ANY
- No secondary consoles
  - MODIFY COMMAND SET SUBCMD SECUSER IBMCLASS G PRIVCLASS M

- But what else might there be?

Turn off backchannel communication

- VMCF
  - MODIFY DIAGNOSE DIAG068 IBMCLASS G PRIVCLASS M

- ESA/XC mode address space sharing (ADRSPACE PERMIT)

- DCSS

- And we can add new interfaces in an APAR

- Google “less than class g” by Rob van der Heij

- Too hard for some folks

- Consider RACF Mandatory Access Controls instead
  - AppArmor and SELinux provide the same capabilities for Linux

Multi-Zoning with RACF

- Mandatory access controls override end user controls
  - Users are assigned to one or more named projects

  - Minidisks, guest LANs, VSWITCHes, and VLAN IDs, NSSes, DCSSes, spool files
    - all represent data in those same projects

  - Users can only access data in their assigned projects

  - Overrides user- or admin-given permissions

Multi-Zoning with RACF

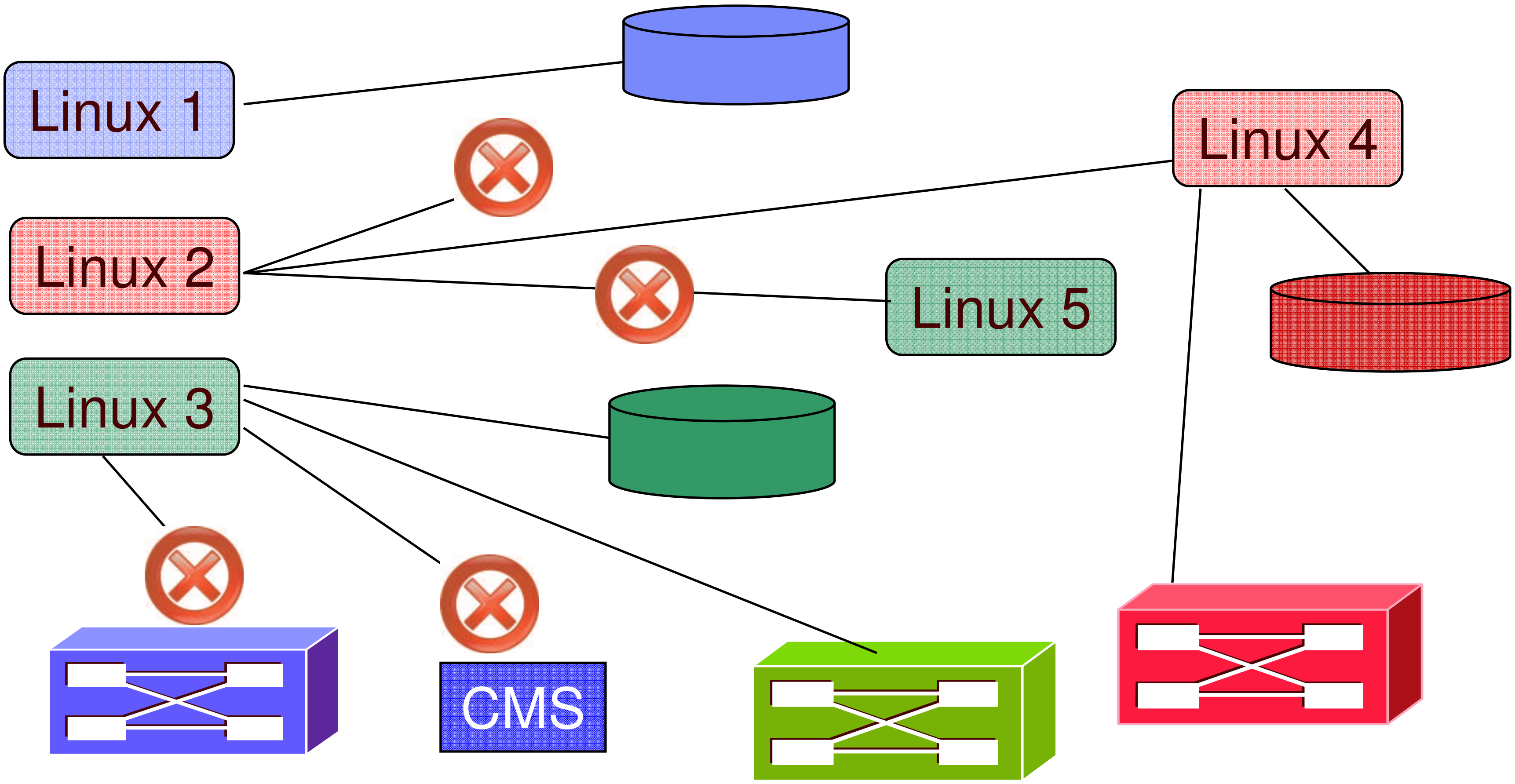
- A **Security Label** combines the concepts of
  - Security clearance (secret, top secret, eyes only)
  - Information zones

- Information zones apply to any place data may exist
  - disks, networks, and other users

- Security clearance
  - Ensures servers cannot see extra-sensitive data in their information zone
  - Prevents copying of data to medium that is readable by servers with lower security clearance (“No write down”)
  - Not prevalent since there is no equivalent in distributed networking solutions

- Label “dominance” is established based on intersection of zones and security clearance
  - Not just a simple string comparison

Multi-zone z/VM LPAR with RACF Security Label Enforcement



Multi-Zoning with RACF

Create security levels and data partitions

```
RDEFINE SECDATA SECLEVEL ADDMEM(DEFAULT/100)

RDEFINE SECDATA CATEGORY ADDMEM(INTERNET DMZ APPS DATA COMMON)

RDEFINE SECLABEL PUBLIC SECLEVEL(DEFAULT)ADDCATEGORY(COMMON)
    UACC(NONE)

RDEFINE SECLABEL RED SECLEVEL(DEFAULT)ADDCATEGORY(DMZ COMMON)
    UACC(NONE)

RDEFINE SECLABEL GREEN SECLEVEL(DEFAULT) ADDCATEGORY(APPS COMMON)
    UACC(NONE)

RDEFINE SECLABEL BLUE SECLEVEL(DEFAULT) ADDCATEGORY(DATA COMMON)
    UACC(NONE)
```

Multi-Zoning with RACF

Assign virtual machines their SECLABELs

```
PERMIT RED CLASS(SECLABEL) ID(LXHTTP01) ACCESS(READ)
ALTUSER LXHTTP01 SECLABEL(RED)

PERMIT GREEN CLASS(SECLABEL) ID(LXWAS001) ACCESS(READ)
ALTUSER LXWAS001 SECLABEL(GREEN)
```

Multi-Zoning with RACF

- But sometimes a server serves the Greater Good, providing services to all users

- Exempt server from label checking

- Assign system servers label SYSNONE

```
PERMIT SYSNONE CLASS(SECLABEL) ID(TCPIP) ACCESS(READ)

ALTUSER TCPIP SECLABEL(SYSNONE)
```

Multi-Zoning with RACF

- Assign labels to resources
  - VMMDISK – Minidisk
  - VMLAN – Guest LANs and Virtual Switches

```
–RALTER VMMDISK LXHTTP01.201 SECLABEL(RED)

–RALTER VMLAN SYSTEM.NET1 SECLABEL(RED)

–RALTER VMLAN SYSTEM.NET2.0307 SECLABEL(GREEN)
–RALTER VMLAN SYSTEM.NET2.0410 SECLABEL(BLUE)
```

- If you intend to activate TERMINAL or VMSEGMT classes, those resources all need SECLABELs

Multi-Zoning with RACF

- Activate RACF protection
  - SETROPTS CLASSACT(SECLABEL VMMDISK VMLAN)
  - SETROPTS RACLIST(SECLABEL)
  - SETROPTS MLACTIVE(WARNINGS)
    - If resource doesn’t have a seclabel, message is issued and seclabels are ignored.

  Or

  - SETROPTS MLACTIVE(FAILURES)
    - If resource doesn’t have a seclabel, command fails.
      - This is more secure!

Summary

- Check network design with network architect

- Place firewalls where the network security team wants them to go

- Use common sense
  - Protect the hardware
  - Protect your data
  - Protect your servers
  - Protect your company
  - Protect yourself!!

Reference Information

- This presentation
  - – http://www.VM.ibm.com/devpages/altmarka/present.html
- z/VM Security resources
  - – http://www.VM.ibm.com/security
- z/VM Secure Configuration Guide
  - – http://publibz.boulder.ibm.com/epubs/pdf/hcss0b30.pdf
- System z Security
  - – http://www.ibm.com/systems/z/advantages/security/
- z/VM Home Page
  - – http://www.VM.ibm.com

Dank u
Dutch

Merci
French

Спасибо
Russian

Gracias
Spanish

شكراً
Arabic

감사합니다
Korean

Tack så mycket
Swedish

धन्यवाद
Hindi

תודה רבה
Hebrew

Obrigado
Brazilian
Portuguese

谢谢
Chinese

Dankon
Esperanto

Thank You

ありがとうございます
Japanese

Trugarez
Breton

Tak
Danish

Danke
German

Grazie
Italian

நன்றி
Tamil

děkuji
Czech

ขอบคุณ
Thai

go raibh maith agat
Gaelic