#SHAREorg

SHARE

13401: Introduction to Mainframe Networking (Focus on z/OS)

Gwendolyn Dente (gdente@us.ibm.com)
IBM Advanced Technical Skills

Thursday, August 15, 2013: 1:30 PM-2:30 PM
Room 206 (Hynes Convention Center)
Session Number 13401

SHARE in Boston

#SHAREorg

SHARE

Abstract

- LPARs, Sysplex, TCP/IP, Enterprise Extender, VPN, are just some of the networking concepts associated with the mainframe. You attend meetings everyday where you hear these terms, but do you know what they mean? The speaker will provide you with the background to understand the basic concepts of mainframe networking and take you out of the 'fog'. She will show you where the similarities and differences are between mainframe networking and other forms. The focus is on z/OS even though other operating systems for the mainframe play a role in this presentation as well.

SHARE in Boston

Agenda

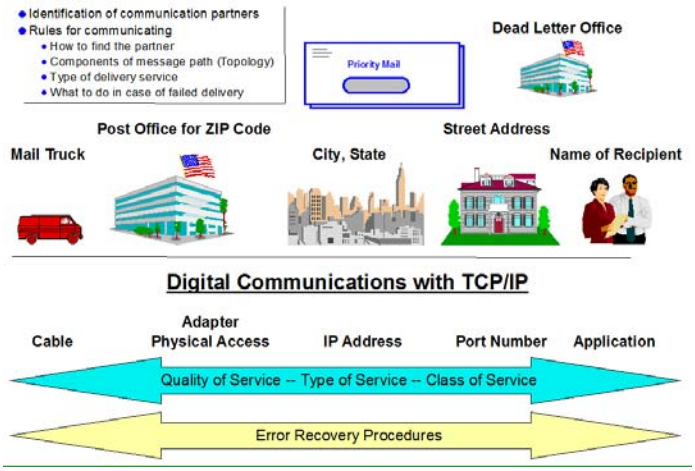
- Requirements for Communication
- What are Networking Architectures?
- Networking Architectures on System z
- Z Hardware Platform Support of Network Architectures
- Differences in Networking Applications
- Differences in Security Implementations
- Appendices:
  - References
  - Differences in Network Definition Processes
  - Differences in File Types
  - Differences in Resolving Names to IP Addresses

Requirements for Communication

A General Model for Sending Messages

- Format of a Destination address in the USA:
  - Name of Recipient
  - Street Address (Number + Name)
  - City, State
  - ZIP Code

A General Model for Sending Messages



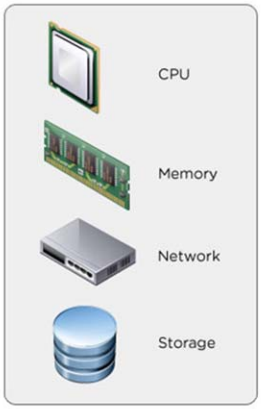
Requirements for Successful Communication

- *Connecting two entities in order to exchange information.*
  - ***How to identify and locate the opposite end?***
    Is there a name or address?
  - ***How to connect to the opposite end?***
    Can the message be sent directly or must it be transferred at intermediate stops along the way?
  - ***What are the rules to govern an orderly exchange of information?***
    What kind of service to provide to this piece of information?
    How to know that the data has been received?
    How much data should I send at once?
    How to end the communication?

- Communication Protocols
  - Naming and Addressing Conventions
  - Rules for organizing the network topology: nodes and links
  - Rules for connecting communication partners: communication setup and takedown
  - Rules for routing the information
  - Rules for managing performance on the connection

Basic Components of a Computing Platform

Laptop:	System z:
•CPU	•CPU
	•Speciality and Assist Processors
•Memory	•Main Storage
•Cache Memory	•Cache Storage
•Disk	•DASD
•Ethernet Port	•OSA Adapter with LAN Ports
•Serial Port	•Channels



And then there is the software:

- •Operating System Software
- •Communications Access Method Software
- •Application Software
- •File Management and Organization Software

Laptop:

- Memory
- Cache Memory
- Disk
- Ethernet Port
- Serial Port

System z

- Main Storage
- Cache Storage
- DASD
- OSA Adapter with LAN Ports
- Channels

What are Networking Architectures?

Foundations for Communications across a Network

- **Communication of messages**
  - **Requirements:**
    - Hardware components
    - Software components
  - **Guided by communication architectures**
    - **SNA (IBM Systems Network Architecture)**
      - *IBM Proprietary Architecture to allow sharing of communications devices and links (since 1974)*
    - **TCP/IP (Transmission Control Protocol / Internet Protocol) (formalized in 1982/1983)**
      - *Heir to ARPANET and DARPANET military and university communication projects*
      - *Governed by Requests for Comment (RFCs) regulated by the Internet Engineering Task Force (IETF)*
      - *Influenced by TCP/IP additions in the Berkeley Software Distribution (BSD) of UNIX*
- **Protocols (Controls or Rules) for Communication in General**
  - Roles of the **participants** (primary, sender, receiver, client, server, peers, etc.)
  - Rules for **starting and ending** communication
  - Rules for **identifying** hardware or software **participants** (names, network IDs, addresses, etc.)
  - Rules for **locating** participants (finding a route or path between them)
  - Rules for managing the **performance** characteristics of the networking path
  - Rules for **recovering** interrupted communications
- **Protocols for the Software Architecture**
- **Controls or Rules for Communication over the Hardware Components:**
  - **Engineering and Signalling over the Data Links**
    - Channel Cables
    - Serial Cables
    - SDLC
    - Token Ring
    - Ethernet

Identifying the Communication Partner

Identity depends on the Communications Architecture

Systems Network Architecture (SNA)

- **By NETID and LUNAME**
  - Could be a terminal
  - Could be an application on the terminal or server
- Can be a Virtualized LUname (“z/OS VTAM Generic Resources)

TCP/IP

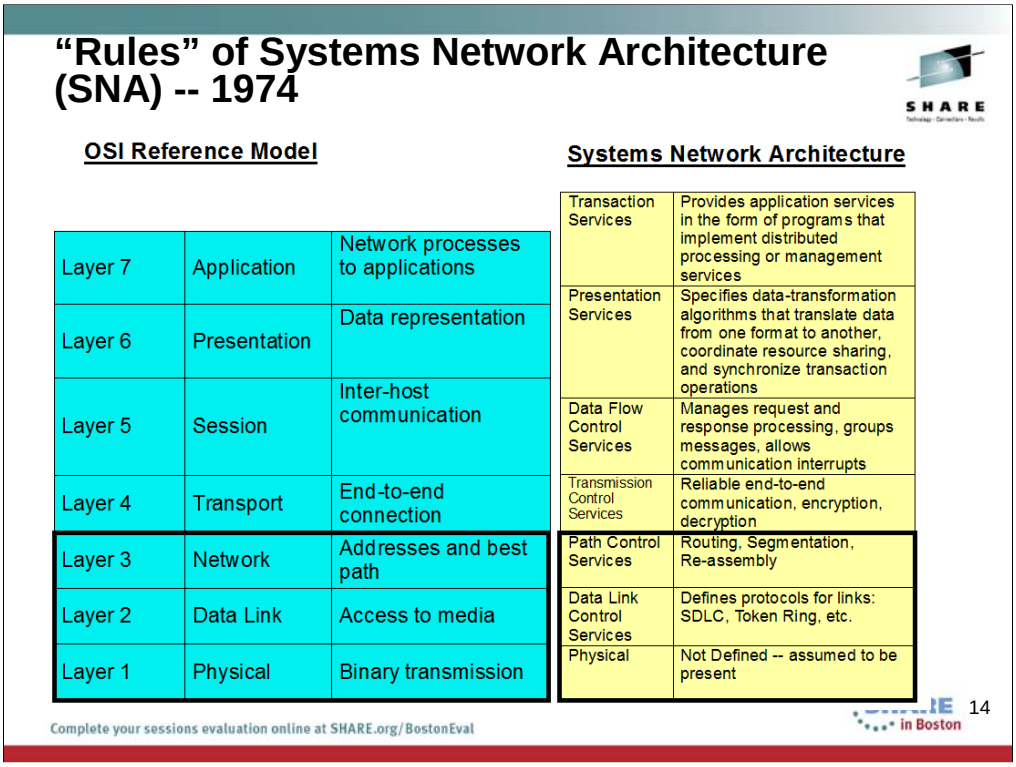
- **By IP Address (IPv4 or IPv6) and optionally Application Port Number**
  - Could be a terminal
  - Could be an application on a terminal or server
- Could be a Virtualized or “shared” IP address to represent multiples
  - Sysplex Distribution (z/OS TCP/IP)
- Exploiting a **Domain Name Server or a Host Local** file to map a NAME to the required IP Address

Locating the Communication Partner

- Identifying the Partner
- How to identify the LOCATION of the Partner in the Network
  - "Network Topology"
- Sending Data over Routes or Paths to the Partner
  - How to define routes or paths or maps to the partner
  - How to assign communication to various paths
    - Performance of Paths?
      - *High Priority?*
      - *Low Priority*
    - Availability of Paths for Recovery
      - *Primary paths or routes*
      - *Alternate paths or routes*

Managing the Data Flow between Partners

- How much data to send
- How to present the data to the end user
- When to reduce or increase amount of data to send



From Wikipedia, the "free encyclopedia"

"The **Open Systems Interconnection (OSI) model** (ISO/IEC 7498-1) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO)."

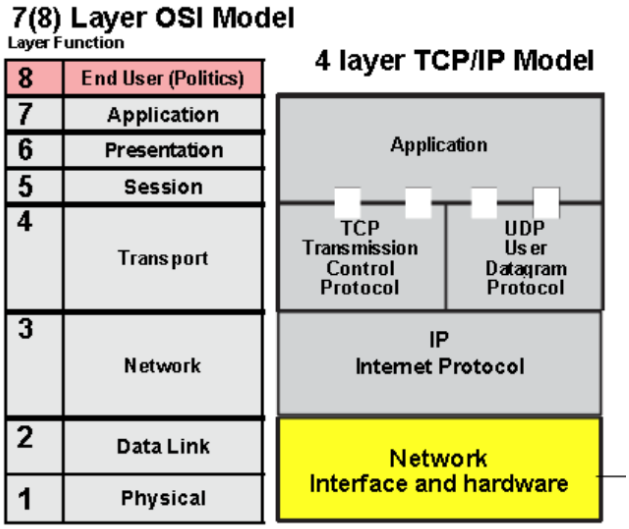
"The model groups similar communication functions into one of seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer."

Systems Network Architecture (SNA) also uses layers to describe networking functions.

From Wikipedia, the "free encyclopedia"

"Systems Network Architecture (**SNA**) is IBM's proprietary networking architecture created in 1974.[1] It is a complete protocol stack for interconnecting computers and their resources. SNA describes the protocol and is, in itself, not a single piece of software. The implementation of SNA takes the form of various communications packages, most notably Virtual telecommunications access method (VTAM) which is the mainframe package for SNA communications."

“Rules” of TCP/IP Network Architecture



From Wikipedia, the “free encyclopedia”

“The **Internet protocol suite** is the networking model and a set of communications protocols used for the Internet and similar networks. It is commonly known as **TCP/IP**, because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP) were the first networking protocols defined in this standard. It is occasionally known as the **DoD model** due to the foundational influence of the ARPANET in the 1970s (operated by DARPA, an agency of the United States Department of Defense).”

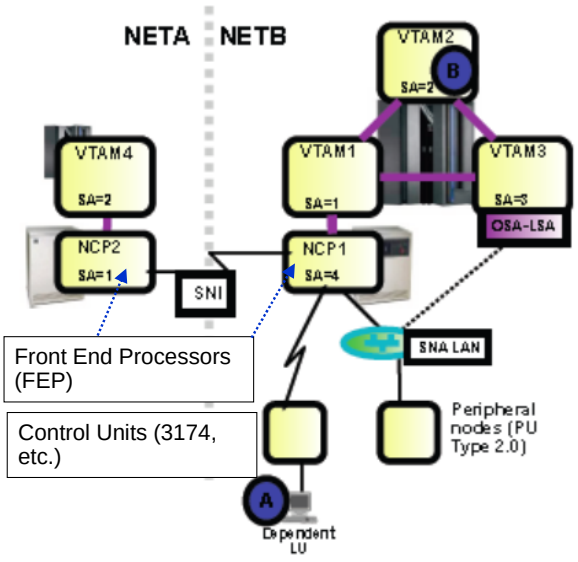
“TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. It has four abstraction layers which are used to sort all related protocols according to the scope of networking involved.[1][2] From lowest to highest, the layers are:

The TCP/IP model and related protocols are maintained by the Internet Engineering Task Force (IETF).”

SHARE

Architectures on System z

SNA Subarea Networking



❖**SNA nodes are Physical Units (PUs):**

- Subarea (SA) nodes (VTAM, NCP) (PU 4 or 5) or
- Peripheral nodes (PU 2 or PU 1)
  - •Reside in Control Units like a 3274 or 3174

❖**Communication Partners** reside in Subarea Nodes or Peripheral Nodes

- Are identified by their NETID and their Name
  - ✓ **System Services Control Point (SSCP name)**
  - ✓**Logical Unit (LU)**

❖They are found by their **location** in a NETID, a subarea, and an element in a subarea

VTAM = Virtual Telecommunications Access Method

NCP = Network Control Program (runs in a physical Front-End Processor (FEP) called a 3745/6 or an emulated 3745/6 called Communication Controller on Linux (CCL) in System z)

Offloads processing from the VTAM in a partition to the FEP.

SNI=SNA Network Interconnect (to establish connections between partners in different NETIDs)

Types of SNA Names for communication:

For Subareas:

SSCPs (a Physical Unit Type 5)

NCPs (a Physical Unit Type 4)

Peripheral Nodes

PU Type 2

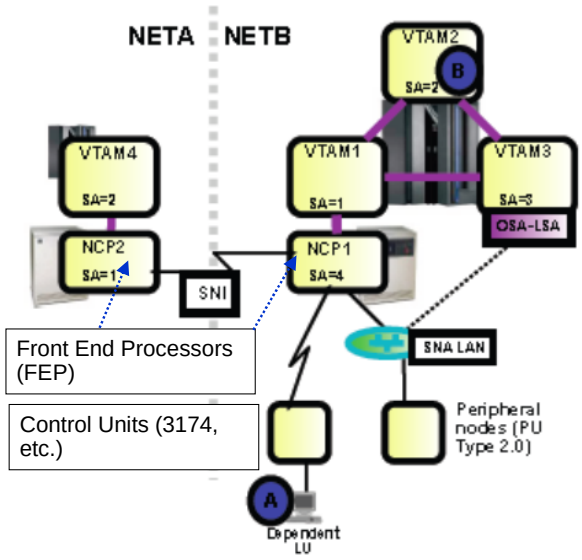
PU Type 1

LUs

Dependent LUs

Independent LUs

SNA Subarea Networking Definitions



- **DEFINITION REQUIRED:**
- **All resources (nodes, links, paths)** in an SNA network (a NETID) must be defined on each subarea node for it to be able to establish sessions through the SNA subarea network:
  - The dreaded **SNA path tables**
    - All possible session paths – **primary and alternate -- (routes** between subarea nodes) must be predefined on all the subarea nodes.

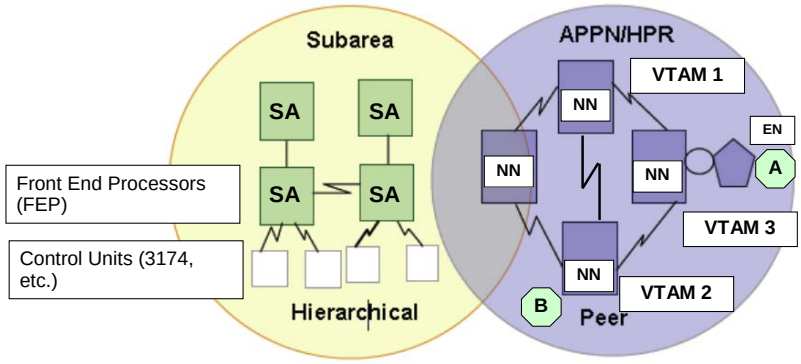
SHARE in Boston 18

VTAM = Virtual Telecommunications Access Method

NCP = Network Control Program (runs in a physical Front-End Processor (FEP) called a 3745/6 or an emulated 3745/6 called Communication Controller on Linux (CCL) in System z)

Offloads processing from the VTAM in a partition to the FEP.

SNA Networks and their Evolution



SNA originally consisted of subarea protocols

- •Advanced Peer to Peer networking (APPN) introduced mid 1980s
- •High Performance Routing (APN/HPR)introduced in 1990s
- •Enterprise Extender (EE; HPR over UDP) introduced in 1999

NN: Network Node

•EN: End Node

SNA Advanced Peer to Peer Networking (APPN)

If the business partner also enables APPN, then the interconnection between the two networks can be done using APPN Multiple Network

Connectivity and Extended Border Node(s) instead of the subarea-based SNI technology.

Peripheral node

•Non-subarea dependent LU access through an APPN network uses Dependent LU Requester/Server technology (DLUR/DLUS)

•Session paths are computed dynamically in an APPN network and need not be predefined.

HPR is an extension to APPN, so an HPR environment inherits all the characteristics of APPN.

•If A and B are in session with each other over the link between VTAM2 and VTAM3 and that link fails, the SNA session between A and B will no longer break as long as the links between VTAM2, VTAM1, and VTAM3 are HPR links, such as XCF or MPC+ channels.

• When the link breaks, HPR will make a non-disruptive path switch and switch the session to go between VTAM2, via VTAM1, to VTAM3 and

then further on to End Node 3 (EN3).

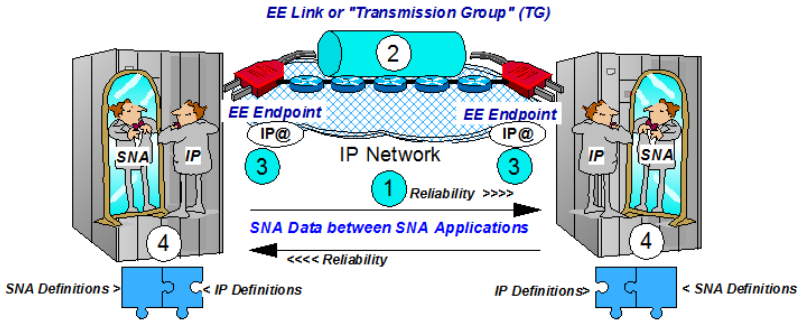
SNA High Performance Routing (HPR)

If the business partner also enables APPN and HPR then the interconnection between the two business partners can be done using APPN Multiple Network Connectivity, Extended Border Node(s), and HPR over IP - or in other words via the Internet instead of private lines

between NCPs.

•An extension to HPR is to use an IP network as an HPR link - this is known as HPR over IP (HPR/IP) or HPR over UDP (HPR/UDP) or more generally as Enterprise Extender (EE)

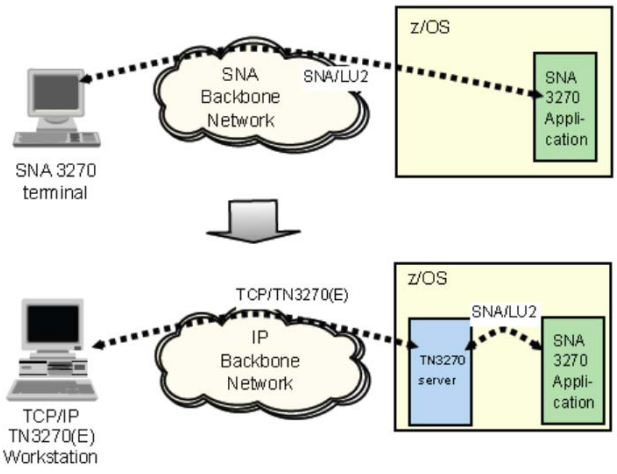
Enterprise Extender: SNA over UDP/IP



❖Enterprise Extender uses "unreliable, connectionless" UDP in the IP network, but it derives its reliability from APPN/HPR architecture, which provides:
- •Error detection and retransmission
- •Non-disruptive reroute
- •Congestion control
- •Prioritization

❖The single EE connection might comprise multiple IP links interconnected through multiple IP routers.
❖Availability of the IP network is provided by redundant paths and preferably dynamic routing protocols.
❖The IP network provides the packet forwarding.
❖EE Endpoint is identified by means of an IP address ('IP@') or a Hostname resolved to an IP address.
❖Platform-specific coding ties SNA to IP within the EE Endpoint node.

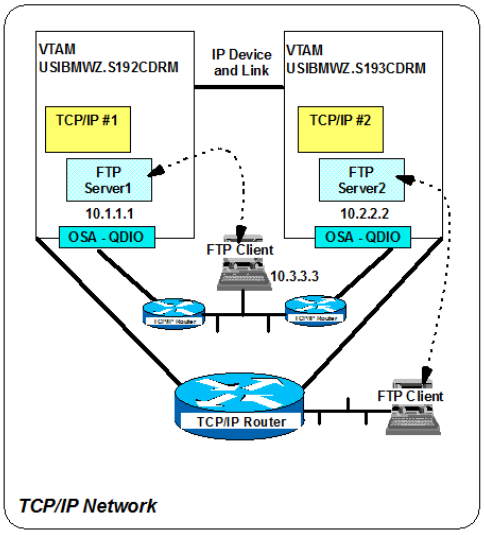
TN3270



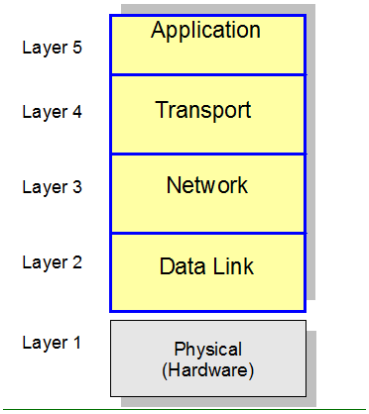
- There are hundreds of thousands of SNA LU2-based applications out there today that will not be migrated to native sockets (ever).

- Many OEM and IBM client products available
- IBM products include PCOMM and HOD (Host-On-Demand)

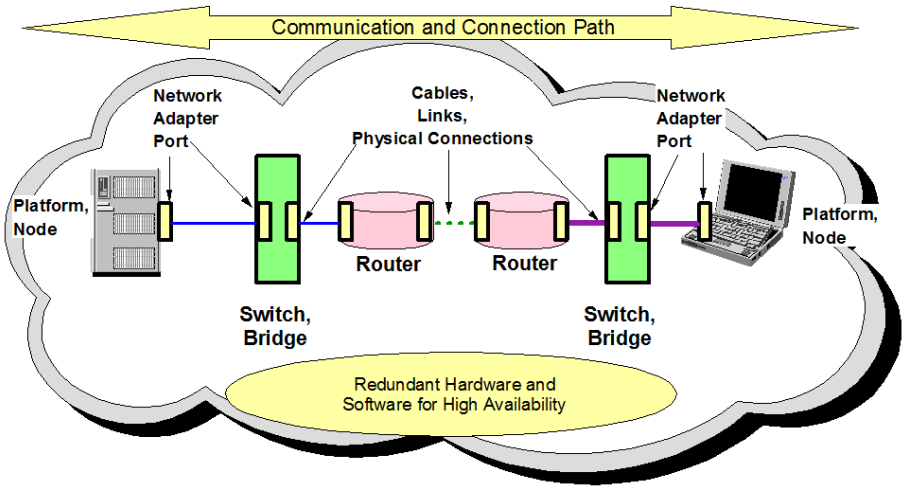
Networks on Z: TCP/IP



TCP/IP Network

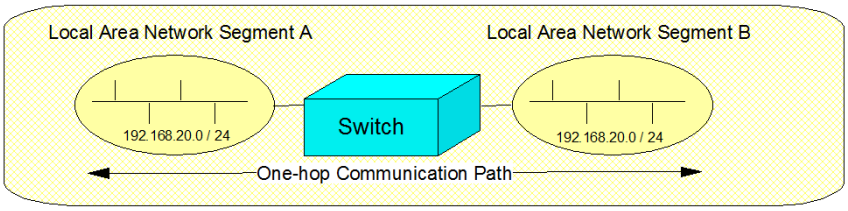


Network Topology Equipment

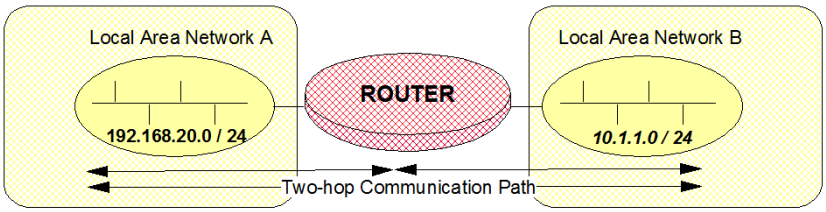


Switching vs. Routing

- **A Switch connects multiple LAN Segments into a single logical LAN.**
  - We have one LAN with network address of 192.168.20.0 / 24

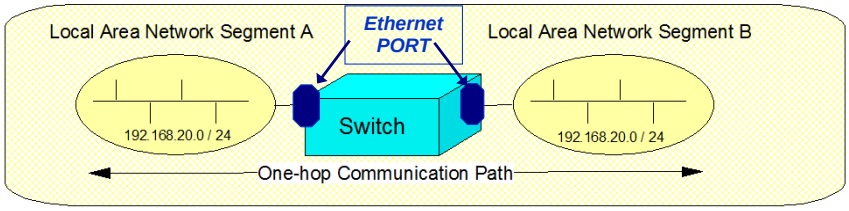


- **A Router connects multiple distinct LAN Segments to create a routing path.**
  - We have two LANs -- each with a separate network address. Nodes in LAN A can communicate over the router with Nodes in LAN B.

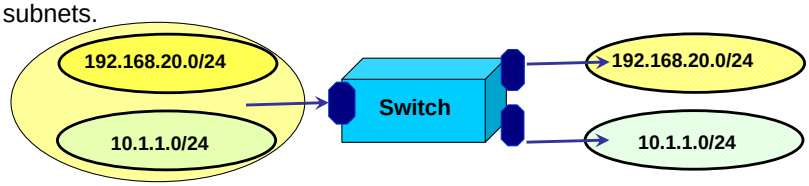


Virtual Local Area Networks (VLAN) with Switching

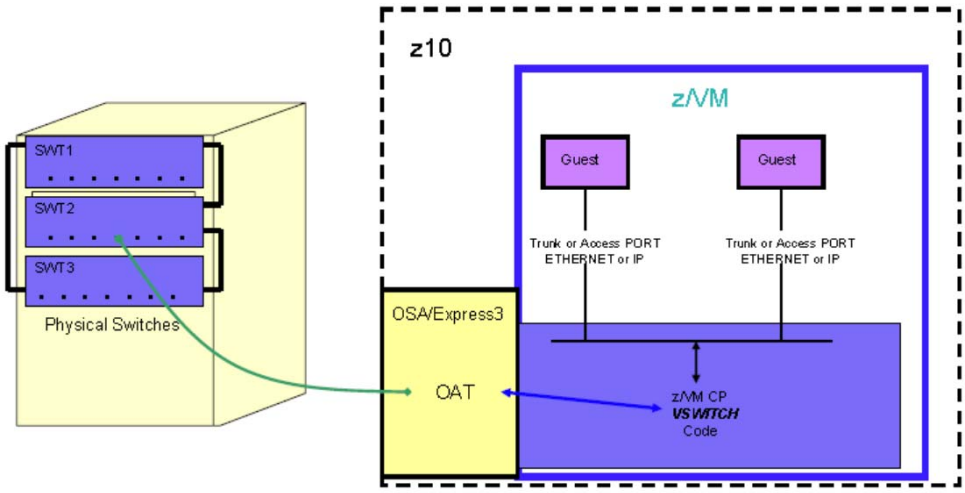
- **A Switch connects multiple LAN Segments into a single logical LAN.**
  - We have one LAN with network address of 192.168.20.0 / 24



A single physical Ethernet Cable on the left can be subdivided into multiple VIRTUAL LAN cables to produce multiple VLAN connections to different subnets.



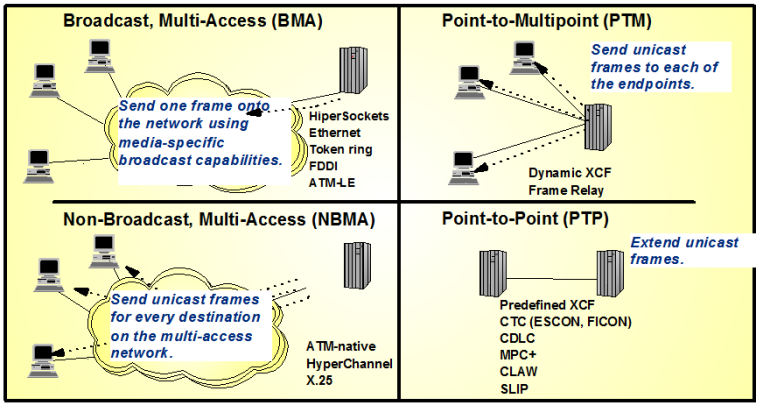
A Virtual Switch (VSwitch) in z/VM



Network Topology Types

Most Common:
Local Area Network (LAN)

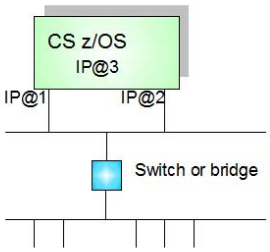
Sysplex Distributor:
Exploits XCF networks on System z



X.25 Packet Switching:
Still commonly in use in some countries

Channel-attached routers (ESCON, FICON)
Channel-attached Operating System Images

Flat Network – Static Routing



- **One IP network address space without any IP routing.**
  - All hosts are attached to the same shared media.
  - All addresses come from a single IP Subnet or network.
  - The media typically consist of many segments with various bridge/switch technologies to interconnect them, but the entire network looks like one Multi-Access Broadcast network from an IP perspective (be careful with such a design: broadcast storms, bridge hops, etc.)

- Outbound traffic will multipath over the two adapters (independent of use of any dynamic routing protocol).
- Each adapter will respond to ARP requests for its own IP address.
- Adapters must be LCS (OSA, 2216-LCS, 3172-LCS). MPCIPA implements similar functions in the adapter.
- If the IP@1 adapter fails, the other adapter will do a gratuitous ARP for IP@1 and begin responding to ARPs for IP@1 in addition to its own IP@2.
- If a VIPA address is defined (IP@3) and the VIPA address belongs to the same IP network as the two adapters (really a design violation!), then one of the adapters will respond to ARPs for that VIPA address (and move to the other, if the first adapter fails).
  - This function is also called "ARP Takeover"
- In a fully flat network environment, there is no need to use a dynamic routing protocol.

- ***Flat networks are not a recommended design approach for medium to large IP networks.***
- ***Flat networks do not provide the granularity you often want to be able to segregate network traffic for management or security purposes.***

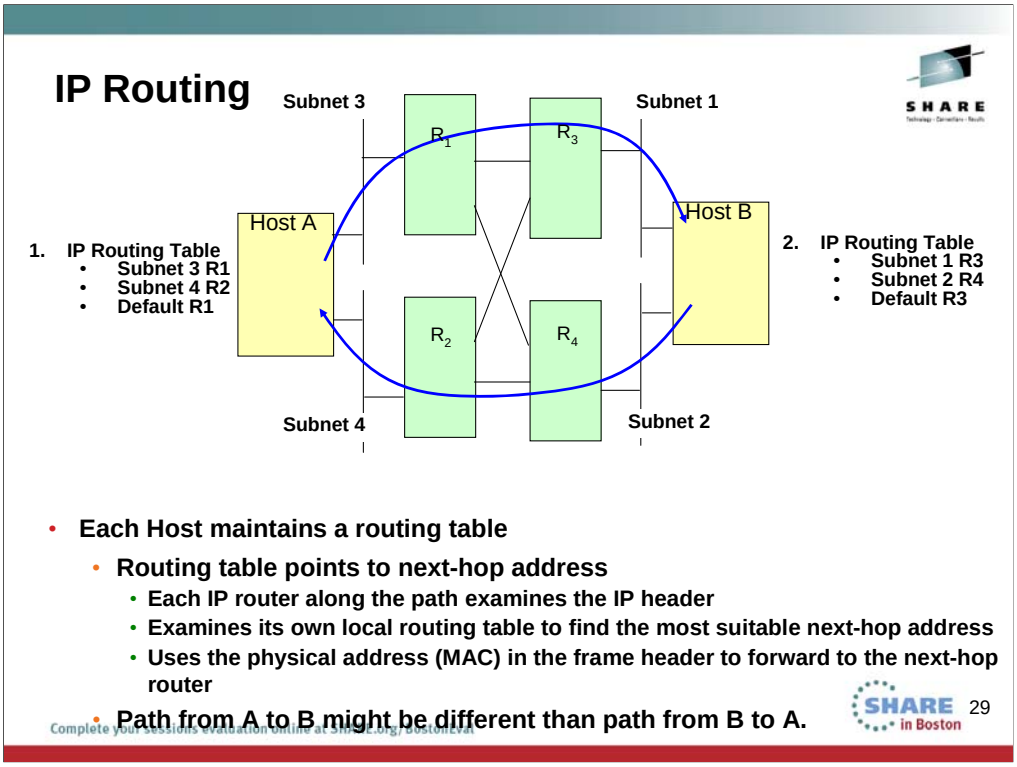
All z/OS operating systems and architectures have ways to statically define routes.

With Subarea SNA, this is through path tables.

With IP, this is through Static routing definitions.

With APPN and APPN/HPR, the routing tables are dynamically learned.

With IP and dynamic routing protocols, the routes are dynamically learned or computed.



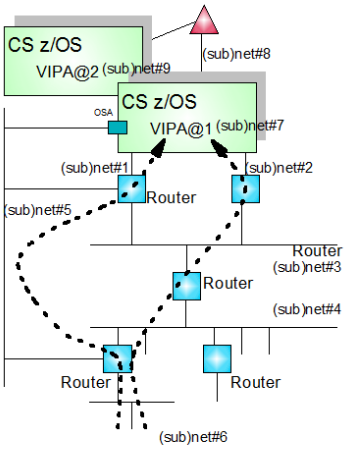
Host A only needs to know next hop IP address; it does not need to know the full network topology in order to reach any given IP network address.

Each IP router along the path must examine the IP header and look into its local routing table to decide the most suitable next hop address before forwarding the IP datagram.

Uses the physical address (Media access control address – MAC - or channel address)) in the frame header to determine where the next-hop router is

Path from A to B might be different than path from B to A.

Router-Based Network Design



- Outbound traffic will multipath over the two channel-attached routers (if static or OSPF routes are used).
- Channel-attached routers and OSAs combined.
- Back-end OS/390 systems can be connected through sysplex connectivity (XCF or CTC).
- If one channel-attached router fails, dynamic routing protocols will converge all inbound and outbound traffic over the other channel-attached router (NB: router cost/metrics).
- If VIPA addresses are used, traffic to/from the VIPA addresses can flow over any of the channel-attached routers.
- In a router-based network, network segments and routers can fail without impacting other users than those that were directly attached to the failing network segment. Dynamic routing protocols will re-route IP traffic via alternate paths between any two destinations in the network.

Router-based network design is the recommended design for medium to large networks.

- Multiple IP network address spaces using Routers to interconnect (sub)networks.
  - Hosts in different network segments are attached to the same shared media.
  - Each network segment is in its own IP Subnet or network.
    - Note: Within a subnet, multiple parts of a (sub)network may be bridged or switched together.

Static vs. Dynamic Routing (Both in System z)

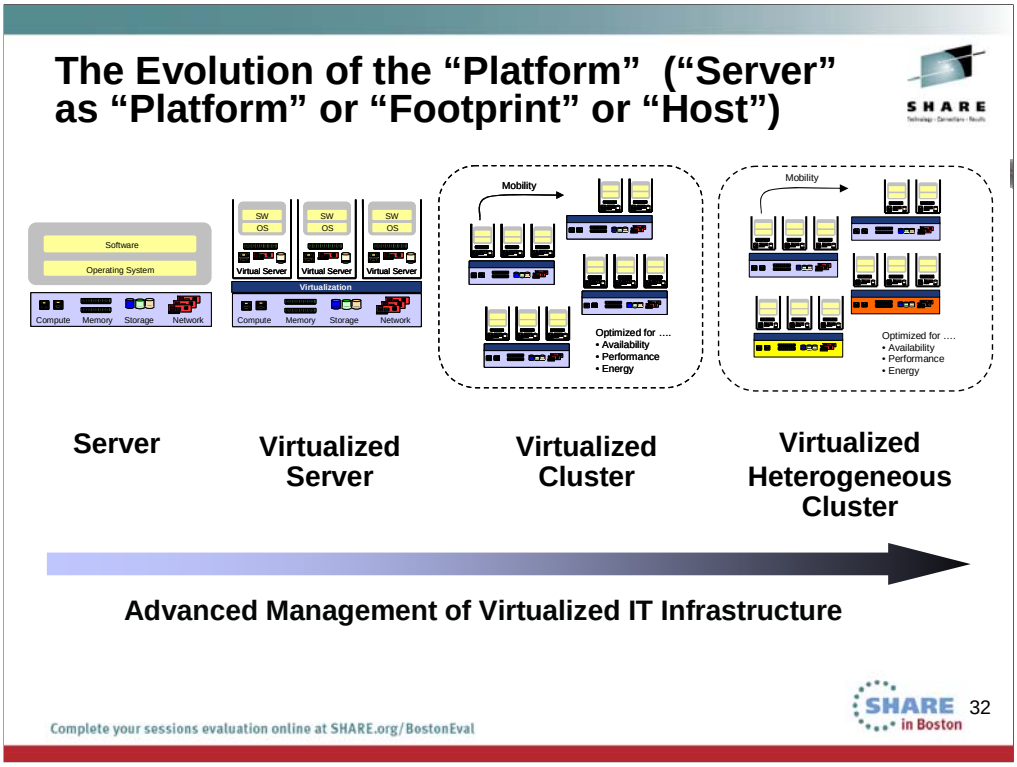
Static routes -- Manual Configuration

- Route definitions are configured manually and stay static until manually changed.
  - BEGINROUTES definitions in z/OS TCP/IP Profile (Preferred)
  - GATEWAY (to be discontinued)
  - In OMPROUTE: DEFAULT can be defined statically (and is not advertised)
- ICMP redirect messages may change statically defined routing tables.
- OSA ARP Takeover function provides route recovery over failed interfaces although the routing table itself does not change.

Dynamic routes -- Dynamically Learned

- Route definitions are updated dynamically by a dynamic route update server that uses a dynamic route update protocol to exchange route information with other dynamic route update servers on other IP hosts.

Typical UNIX Daemons	Hello	RIP	OSPF	EGP	BGP
RouteD		V1			
GateD, V2	Yes	V1		Yes	V1
GateD, V3	Yes	V1, V2	V2	Yes	V2, V3



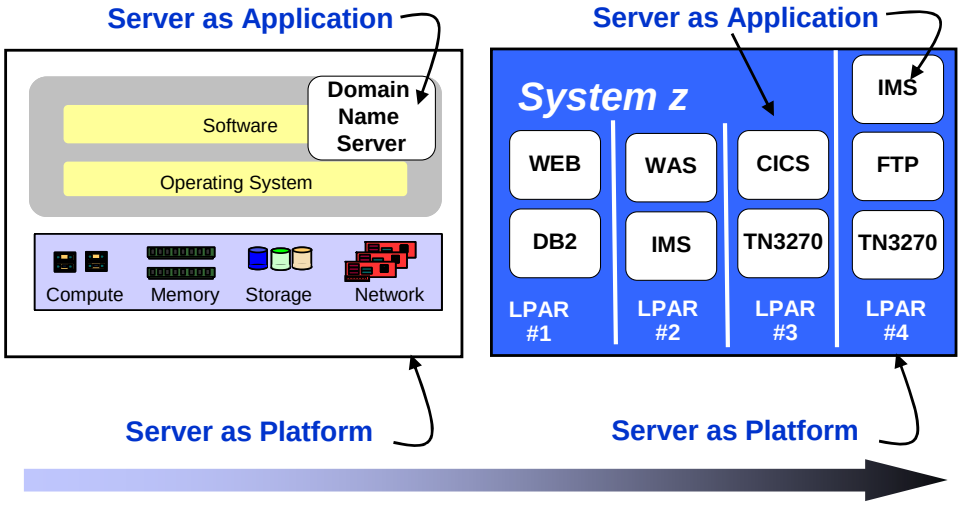
First there were individual operating systems on individual server platforms. The platforms were also known as a physical Server or a computing footprint or even a physical Host. All resources on the platform were dedicated to a single operating system.

Then virtualization of this physical server environment took over. A single physical server could emulate or be virtualized into multiple "physical" servers running separate hosts on a single physical platform. All these virtual servers could share the system resources through the controls provided by a specialized operating system known as a Hypervisor. A user desiring to reach one of these hosts or virtual servers directed his connection or session request to one of the virtual servers and the user's operations would be carried out on that one virtual server using shared resources.

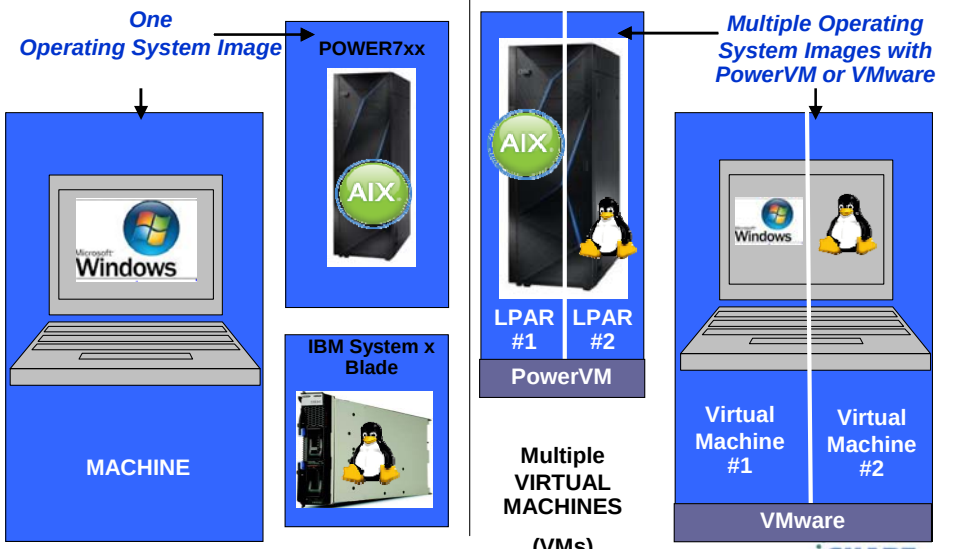
Then several virtual servers could be clustered together to give the appearance of a single system image. With the assistance of certain types of software, the user directed his connection to what he thought was a single target. In reality, his connection request could land at any of virtual servers in the virtualized cluster. Such clusters shared software applications and disk storage among them so that any single one of them could satisfy a user request. This type of single system image was built from homogeneous platform types.

Finally the concept of heterogeneous computing allowed heterogeneous platform types to cooperate with each other to satisfy user requests.

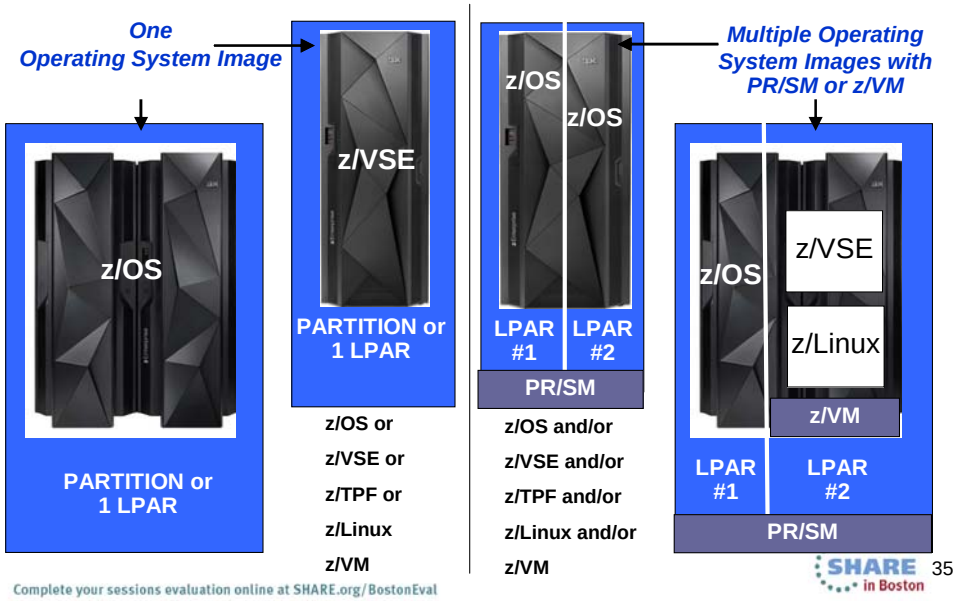
The Evolution of the "Server" ("Server" as "Application" or "Application Server")



On Personal Workstation, x86, or Power: Single Operating System vs. Multiple Operating Systems with Hypervisor of VMware, xHyp, PowerVM

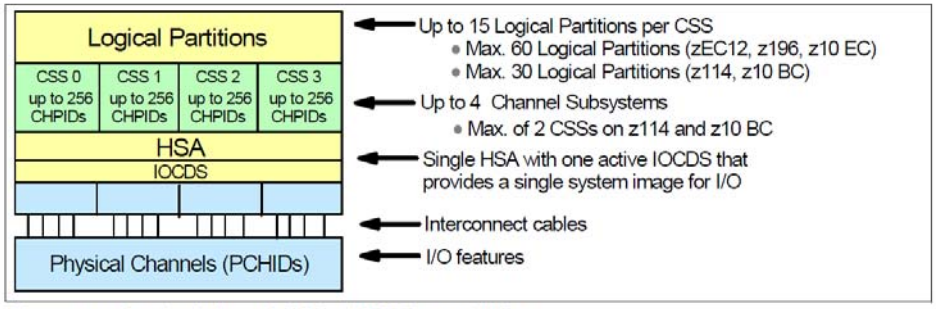


On z: Single Partition vs. Multiple Logical Partitions (LPARs) through Hypervisors of PR/SM and/or z/VM



Hardware Platform Support of the Network Architectures on System z

General Hardware Layout of System z



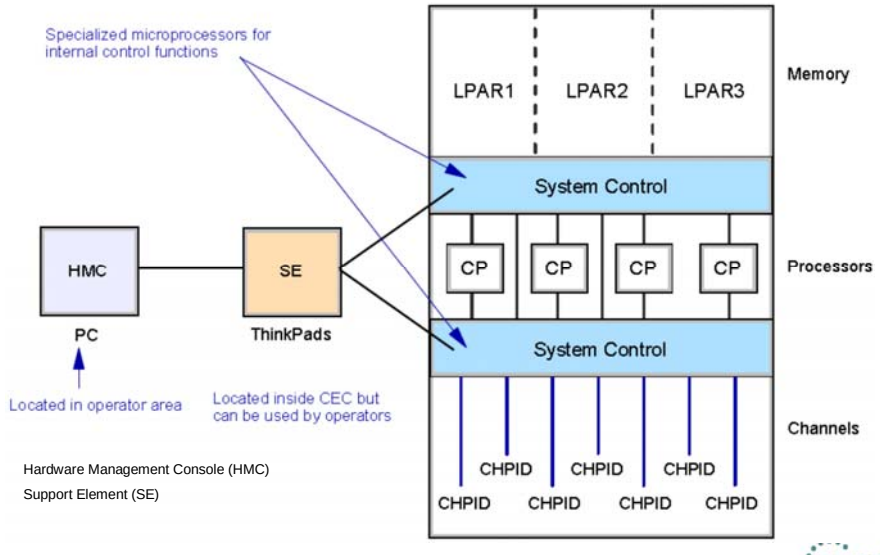
CHPID – Channel Path ID (logical)

PCHID – Physical Channel ID

IOCDS – Input Output Control Data Set translates physical I/O addresses (composed of CHPID numbers, switch port numbers, control unit addresses, and unit addresses) into *device numbers* that are used by the operating system software to access devices.

HSA - Hardware Save Area which holds the I/O configuration data for the server

Controlling the Hardware from Consoles



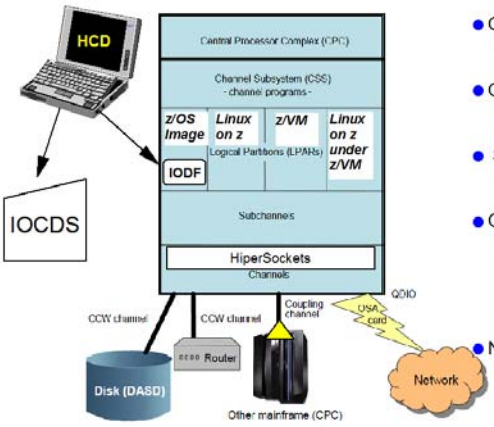
Hardware Management Console (HMC)

Support Element (SE)

Specialty Processors for Offload from CP

- **Users of System z pay Licensing Costs based on the processing time they use on General Purpose Processors (CP – Control Processor)**
- **Specialty Processors have a lower licensing fee structure**
- **Users can reduce Licensing Costs by offloading from CPs to Speciality Processors like:**
  - **IFLs (Integrated Facility for Linux):**
    - The Integrated Facility for Linux (IFL) is a processor dedicated to Linux workloads on IBM System z servers. The IFL is supported by the z/VM virtualization software and the Linux operating system; it cannot run other IBM operating systems.
  - **zIIP Engines:**
    - The IBM System z Integrated Information Processor (zIIP) is available on all IBM zEnterprise (zEnterprise™), System z10, and System z9 servers. It is designed to help free-up general computing capacity and lower overall total cost of computing for select data and transaction processing workloads for business intelligence (BI), ERP and CRM, and select network encryption workloads on the mainframe. Eligible workloads include DB2, HiperSockets large messages, XML, IPSec (VPNs) with z/OS Communications Server, and other.
  - **zAAP Engines:**
    - The IBM System z Application Assist Processors (zAAPs) is available on all IBM zEnterprise EC12, IBM zEnterprise, IBM System z10, and IBM System z9 servers. The zAAP specialty engine provides an attractively priced execution environment for web-based applications and SOA-based technologies, such as JAVA and XML.

Channel & Network Interface Structure on System z



- Central Processor Complex (CPC):
  - passes input/output (I/O) Request to CSS
- Channel Subsystem (CSS):
  - moves data asynchronously to its input/outpt devices
- Subchannel:
  - the individual input/output devices in the CSS that are assigned to the LPARs
- Channel:
  - represented by a channel path ID or CHPID and represents the actual communication path.
  - CHPID is mapped to the PCHID in the HCD and the IOCDS.
- Network Interfaces:
  - identified to TCP/IP by the CHPID and the Subchannel address that are defined in the IOCDS.

The I/O configuration of the central processor complex is defined in a data set called the I/O Configuration Data Set, or IOCDS.

Connections to to devices or networks outside of the System z complex are defined on hardware adapters or interfaces called channels. For system z there are several ways to assign hardware addresses to these channels:

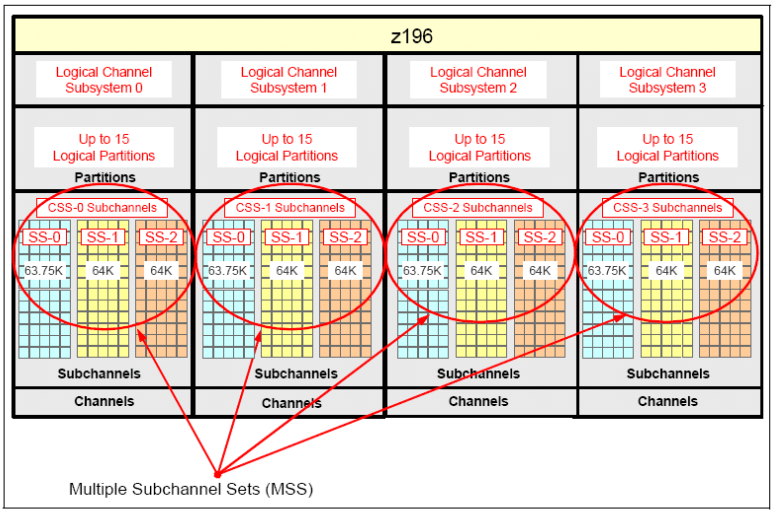
Note: The I/O configuration of the central processor complex is defined in a data set called the I/O Configuration Data Set, or IOCDS. The I/O configuration is normally done using a tool called the Hardware Configuration Dialog, or HCD. HCD also creates a data set called an I/O definition file, or IODF. The IODF is read by the z/OS operating system.

A central processor complex can also be configured using a less easy-to-use statement syntax called IOCP statements. IOCP stands for I/O Configuration Program (IOCP). The IOCP creates an I/O configuration data set (IOCDS).

IOCP statements can be migrated to IODF statements using HCD.

Multiple subchannel sets on zEC12 and z196

Note: z114 supports only LCSS 0 and 1, 15 LPARs each, and had only two subchannel sets in each LCSS



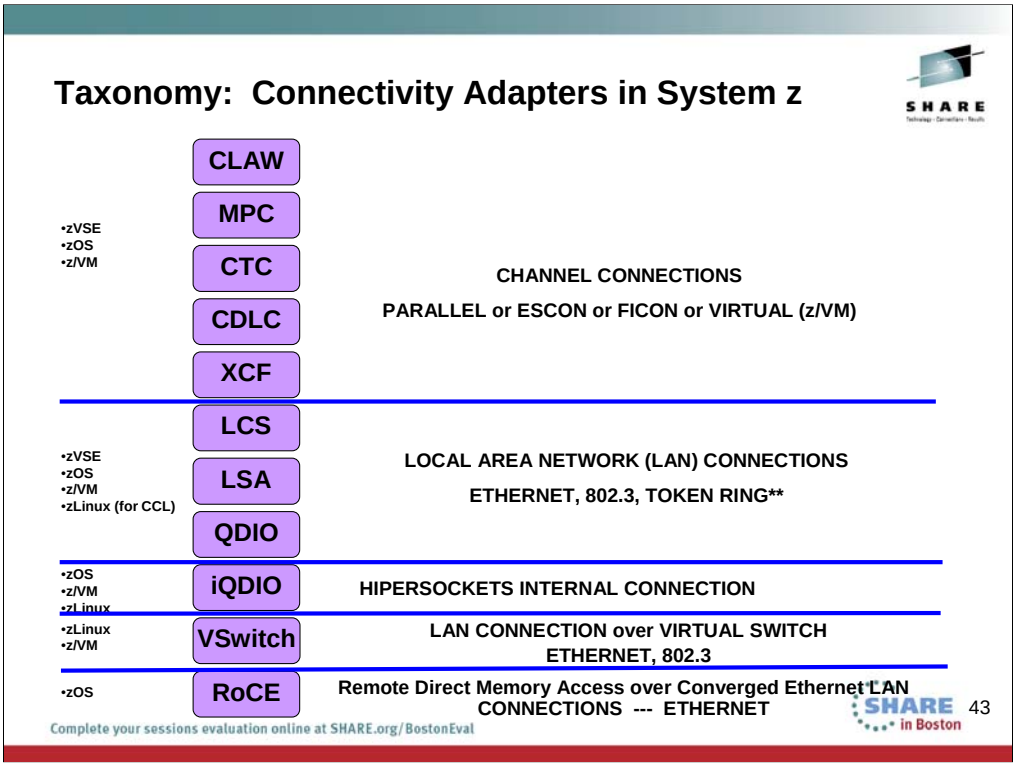
MIF – Multi Image Facility can share a channel within a LCSS
Span channel – Can share a channel with other LCSS

Sharing Channels across LPARs and LCSSs

- **IOCDS** – Input Output Control Data Set translates physical I/O addresses (composed of CHPID numbers, switch port numbers, control unit addresses, and unit addresses) into *device numbers* that are used by the operating system software to access devices.
- **It defines which Physical I/O addresses are shared.**
- **Hardware Console Definitions and the IOCDS map the Hardware Channel Positions (PCHIDs) to the Channel Path ID (CHPID) numbers.**
  - The operating systems use the IOCDS to define the Device Numbers in their Operating Systems.
  - **If you migrate to a new hardware platform, the Operating system definitions can remain the same because they rely on CHPID, Control Unit, and Device numbers; only the mapping of the PCHIDs to the CHPIDs needs to change!**

Sharing channels within a LCSS is call MIF multi-image facility

Sharing channel across multiple LCSS is called "SPAN channel" or spanning a channel



z/Architecture Channel

Input/output (I/O) channels are components of the zEC12 and System z CSS and IBM z/Architecture®. They provide a pipeline through which data is exchanged between systems, or between a system and external devices. z/Architecture channel connections are referred to as *channel paths*.

The most common attachment to a z/Architecture channel is a control unit (CU) accessed via an Enterprise Systems Connection (IBM ESCON®) or Fibre connection (FICON) channel. The CU controls I/O devices such as disk and tape drives.

Alternate Taxonomy: Types of Network Connectivity

- **Physical Network Adapters**
  - Channels
    - ESCON, FICON, XCF
  - RoCE (RDMA over Converged Ethernet)
  - Local Area Network (LAN) Adapters
    - Open System Adapters (OSA) with OSA LAN Ports
- **Virtual Network Adapters**
  - HiperSockets
  - Virtual LAN Adapters over LAN or HiperSockets or VSwitch
  - Virtual Channel-to-Channel Adapters (under z/VM)

Channels and CHPID types

Table 1-1 Channel and CHPID types

Channel type	CHPID type	Description
ESCON[a]	CVC	Conversion Channel (ESCON to Parallel BL).
	CBY	Conversion Channel (ESCON to Parallel BY).
	CNC	Connection Channel (ESCON Architecture).
	CTC	Channel-to-Channel (communicates with ESCON CNC).
FICON	FC	Fibre Connection (FICON) architecture - native FICON.
	FCV[b]	FICON converted (FICON to ESCON).
	FCP	Fibre Channel Protocol (full fabric attachment of Small Computer System Interface devices).
HiperSockets	IQD	Internal Queued Direct I/O.

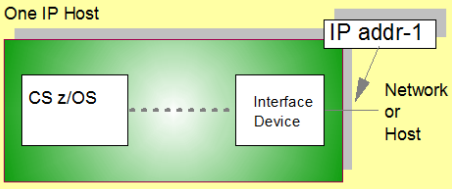
a. Not supported on IBM zEnterprise EC12
b. Only supported with FICON Express LX feature

Important: The IBM ESCON Director (9032-005 including all features) was withdrawn from the market on December 31, 2004. There is no IBM replacement for the 9032-005.

FCV was supported with z10's and earlier servers

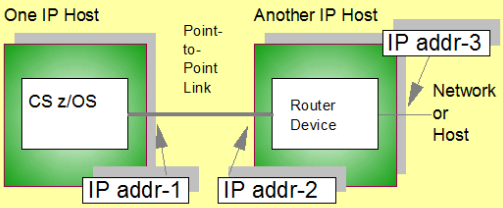
Z Network Interfaces to Attach to a Network

- Directly Attached Network Interfaces



Device may be inboard (OSA adapter) or outboard (3172 LCS or 2216-LCS)

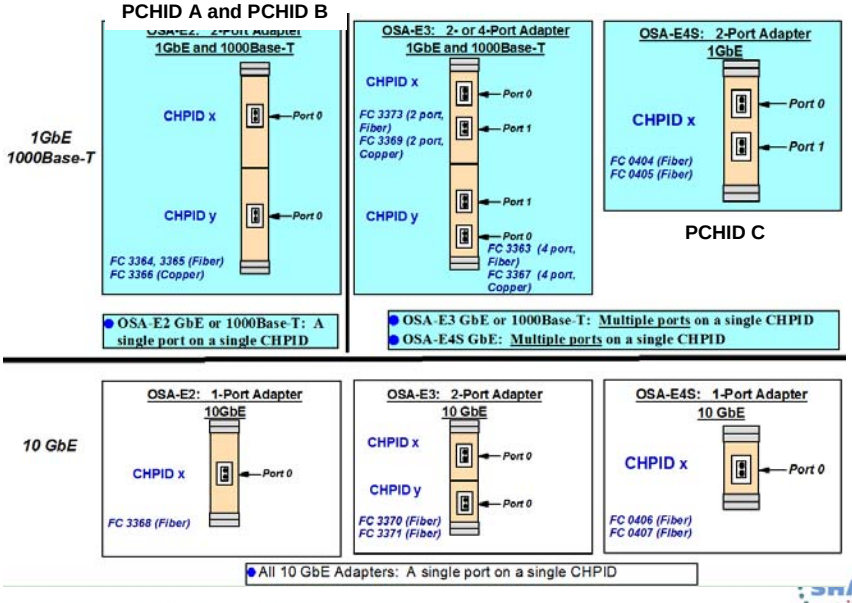
- Channel-Attached Routers



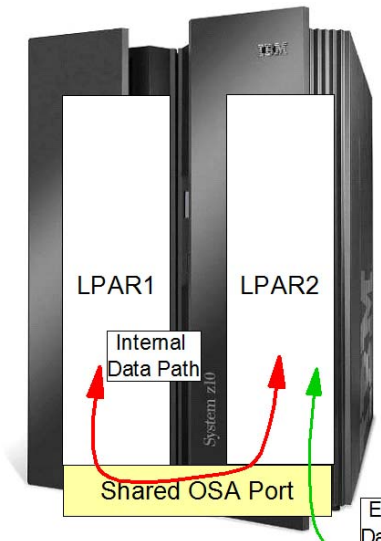
- ✓LCS - Token-ring, Ethernet, and FDDI (3172, OSA, 2216)
- ✓MPCIPA - 10 Gigabit or Gigabit Ethernet and Fast Ethernet (OSA-Express w. QDIO)
- ✓HiperSockets (a form of MPCIPA)
- ✓X.25 PSDN
- ✓CTC (Virtual Channel to Channel)
- ✓XCF
- ✓SAMEHOST
- ✓SNALINK
- ✓HyperChannel
- ✓ATM (LE or Native)

- ✓Cisco CIP
  - CLAW
  - ESCON
  - FICON
- ✓NCP (SNALINK or CDLC)

PCHID Mapped to CHPID; OSA Adapter/Port

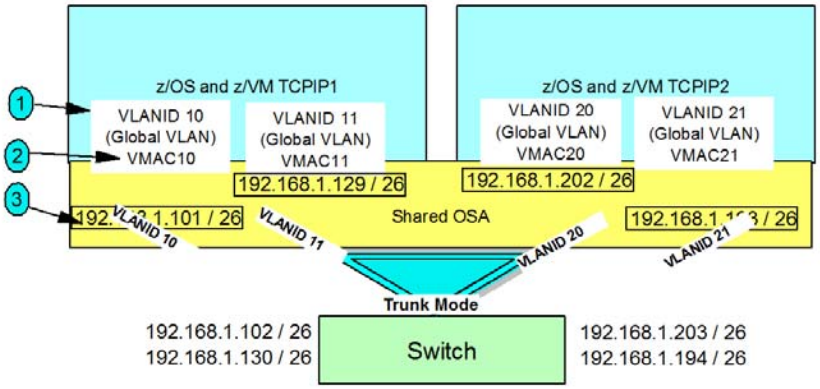


Sharing OSA Ports

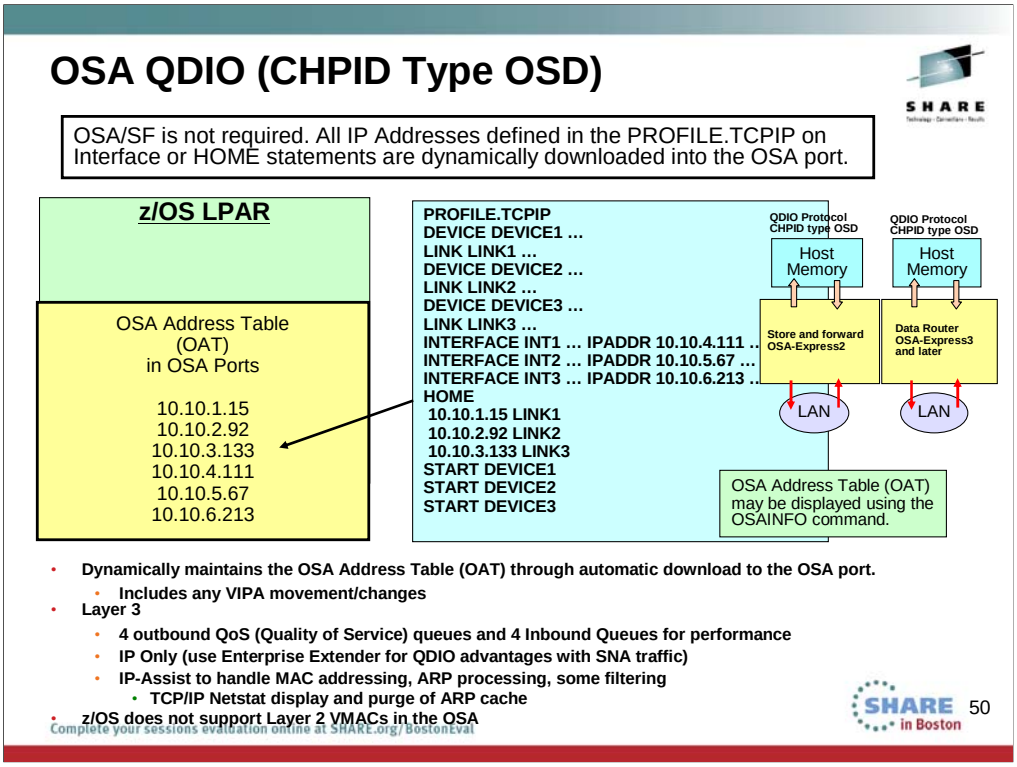


- A shared OSA Port permits communication through the OSA path without exiting onto the network if the routing table identifies the OSA as the next hop in the path.
- Which LPAR is inbound data from the Network sent to? Depends on:
  - OSA Address Table (OAT) Entry, or
  - Primary/Secondary Router designation, or
  - Virtual MAC address
  - To a certain extent: VLAN ID

Multiple VLAN Support over [Shared] OSA



- Starting at V1R10 you can have up to 8 VLANs per stack, per OSA port, per IP version.
  1. With multiple VLAN IDs per stack on an OSA port, you must assign a VLAN ID to every one of the multiple Interfaces on that OSA port and
  2. You must assign or default to separate VMACs on each VLAN ID.
  3. As usual, each VLAN ID must be on a separate subnet.



Supports high-speed LPAR-to-LPAR communication

OSA microprocessor communicates directly with System z using data queues in memory

Continuous direct data exchanges

Communications remain active

Utilizes Direct Memory Access (DMA) protocol

Reduced I/O interrupts

Reduced Latency

Dynamically maintains the OSA Address Table (OAT).

Does not require OSA/SF.

All addresses are dynamically downloaded to the OSA.

Any VIPA movement/changes are dynamically downloaded to the OSA from the TCP/IP stack.

Layer 3

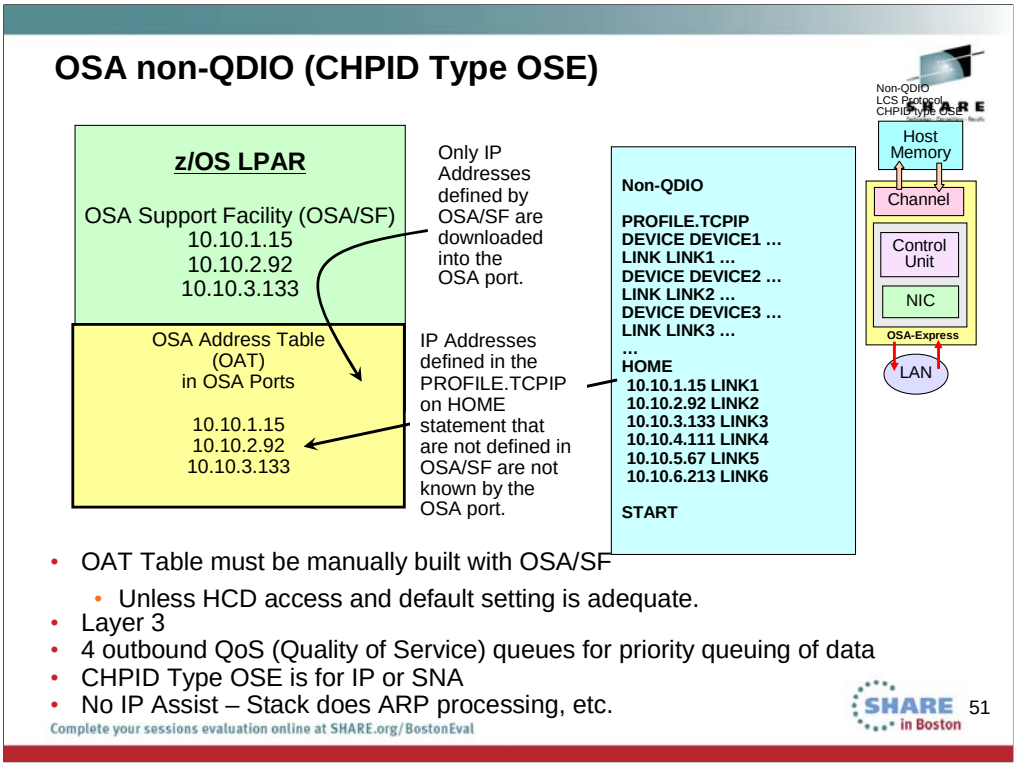
4 outbound QoS (Quality of Service) queues for priority queuing of data

IP Only (use Enterprise Extender for QDIO advantages with SNA traffic)

IP-Assist to handle MAC addressing, ARP processing, some filtering

TCP/IP Netstat display and purge of ARP cache

Layer 2 (not supported by z/OS)



OAT=OSA Address Table

For OSA-E3S and prior in non-QDIO mode, OSA/SF as a host program is required for SNA definition and for non-default TCP/IP definition.

For OSA-E4S on the second generation of the zEC12 or the first generation of the zBC12 and higher can be configured for non-QDIO with the OSA/SF host program. Optionally the OSA/SF on HMC is available for the configuration.

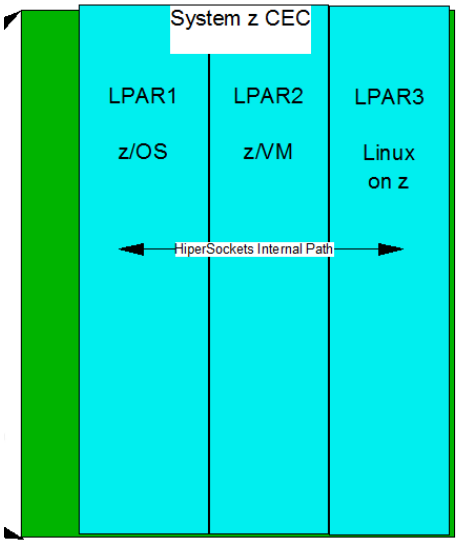
For OSA=E5S and higher in non-QDIO mode, OSA/SF on HMC is required for SNA definition and for non-default TCP/IP definition.

HiperSockets: Internal Communication Path

CEC = Central Electronics Complex

HiperSockets = aka “iQDIO” or Internal QDIO

Available to TCP/IP only

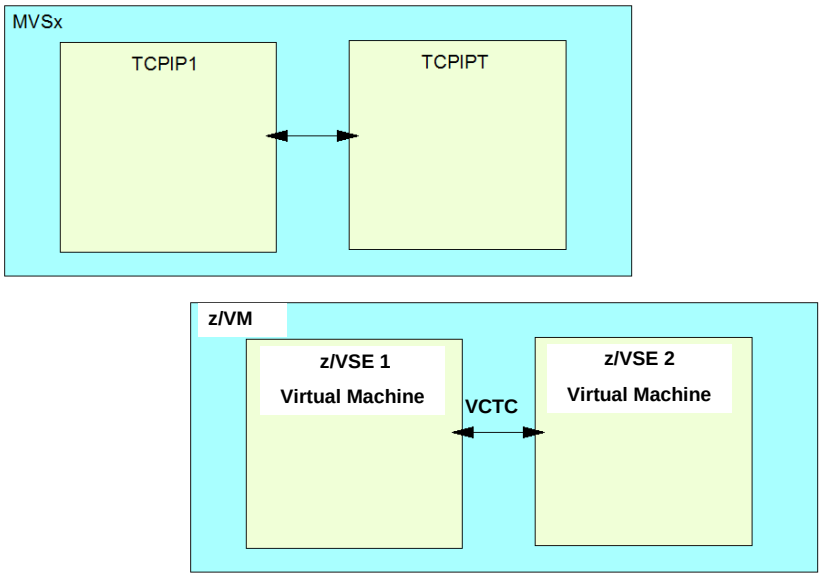


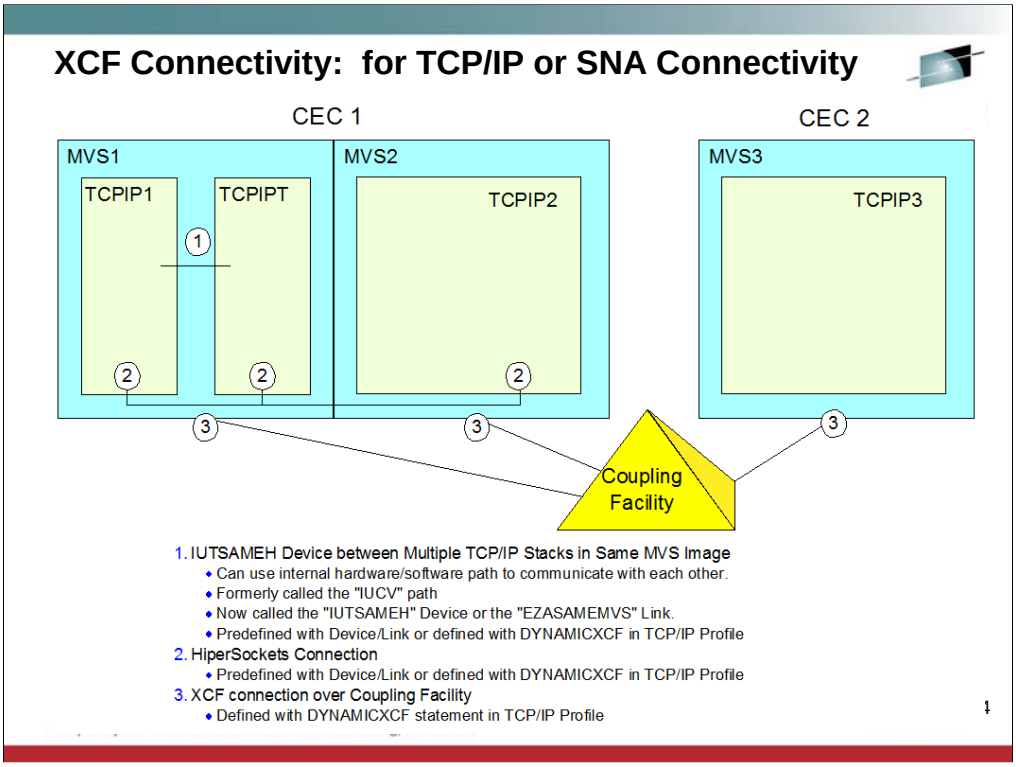
HiperSockets is an internal communication path through hardware and software on a single Central Electronics Complex.

Mainframe HiperSockets is a technology that provides high-speed TCP/IP connectivity within a central processor complex. It eliminates the need for any physical cabling or external networking connection between servers running in different LPARs.

The communication is through the system memory of the processor, so servers are connected to form a "internal LAN."

IUTSAMEH or Virtual Channel-to-Channel



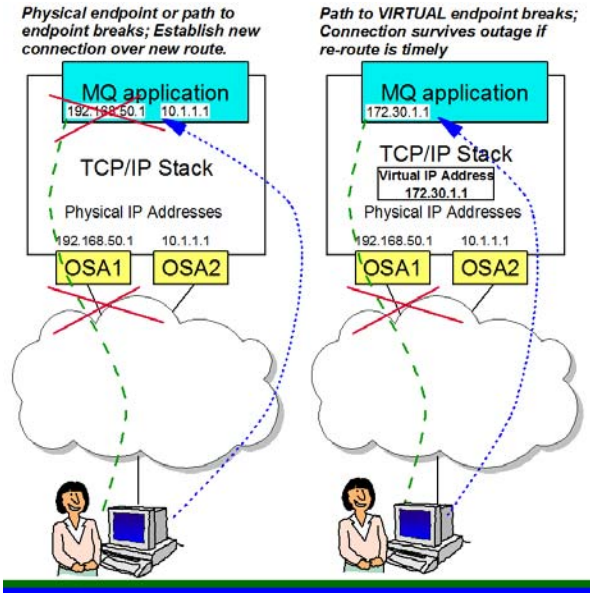


XCF = Cross System Coupling Facility

Types of IP Addresses

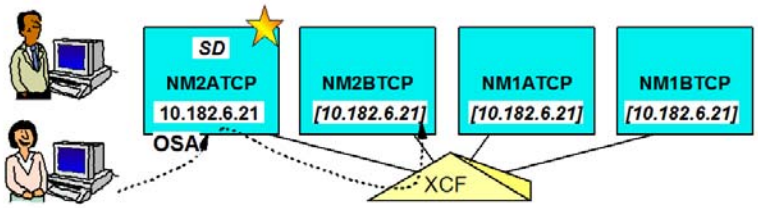
- **Real Addresses**
  - Associated with Physical Adapter types
- **Virtual IP Addresses (VIPAs)**
  - Not associated with Physical Adapter types (represented with address control blocks in software only)
    - Static VIPAs (statically defined)
    - Dynamic VIPAs (designed for high availability: mobility from one system to another)
      - *Predefined with VIPADEFINE and VIPABACKUP*
      - *Dynamically allocated through definition of VIPARANGE*
    - Dynamic VIPAs (designed for high availability and performance: to provide traffic distribution
      - *Predefined with VIPADISTRIBUTE*

Virtual IP Address: Basic Concepts for Static VIPA



A timely reroute usually requires a Dynamic Routing Protocol like OSPF in z/OS.

Sysplex Distributor on z/OS TCP/IP: Basic Operation - VIPA presents Single System Image



Sysplex Workload Distribution On System z with z/OS TCP/IP
- •All Sysplex Nodes Communicate via XCF
- •XCF used for Signalling/Messaging but also for Data Transport

One Stack Performs Routing Functions
- •Owns Sysplex-Wide VIPA And Advertises To Routers
- •Routes Connection Requests To Application Hosts
- •With Real-Time Consultation With WLM And Policy Agent
- •If WLM Not Available, target stack selection is random or other distribution algorithm may be defined.

Other Network-Connected Stack Is Backup
- •Takes Over From Primary In Case Of Failure

Dynamic Routing Protocols, OSPF Or RIP, Recommended

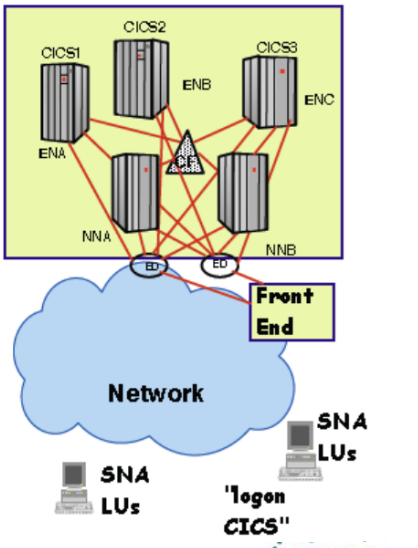
Presenting a Single System Image (SSI) to the world for traffic distribution with z/OS.

Virtual IP Address (VIPA)

Distributed Dynamic VIPA (DRVIPA)

SNA Sysplex Functions

- **VTAM Generic Resources**
  - Provides session balancing and availability
  - Users logon to a generic name - VTAM decides which application to use
  - Requires APPN in the Sysplex
- **Multinode Persistent Sessions (MNPS)**
  - Sessions can continue with application started on another image if current image fails
  - Builds on HPR's path switch technology
  - Only recommended for LU6.2 applications where the availability requirements justify the added CPU cost
- **XCF**
  - Cross system coupling facility
  - Dynamic APPN links automatically activated between all VTAM's in sysplex specifying XCFINIT=YES



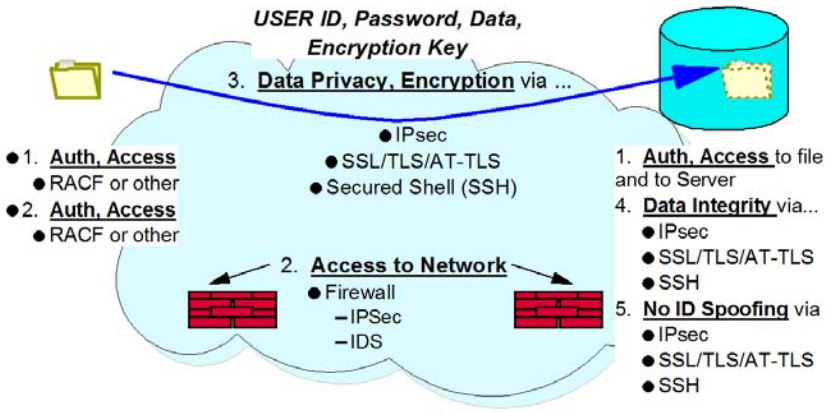
Members of a Sysplex share messages with each other over XCF links.

Members of a Parallel Sysplex share data and policies with each other that are stored in a Coupling Facility.

Operating Systems may avail themselves of Coupling Facility Links to send payload/production data to each other.

Differences in Applications in z Networking

Securely Transferring Files over the Network



1. Authentication & Access Control to file and to file transfer command.
2. Authentication & Access Control to the Network.
3. Data Privacy for USER ID, Password, Payload Data, Encryption Key.
4. Data Integrity: Proof that data was not altered in flight.
5. Non-Repudiation: Proof that the data was sent by the declared sender.

Confusing Acronyms for File Transfer

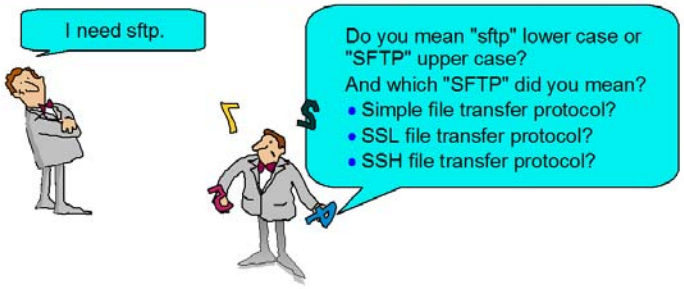
Acronym & Meaning	RFC #	Function
Punched Paper Tape Punched Cards	N/A	
Exchanging Tapes	N/A	
SFTP Simple File Transfer Protocol	913 (now historic)	unsecured, unathenticated transfer of files - - **TCP Port 115**
TFTP Trivial File Transfer Protocol	1350	unsecured, unauthenticated, and functionally limited transfer of files in a small private intranet (usually boot files for routers) - **UDP Port 69**
SCP Secure Copy Program	BSD Remote Copy Protocol	secured, authenticated transfer of files over SSH - **TCP Port 22 (SSH)**
FTP File Transfer Protocol	959 2428 (EPSV)	File transfer providing optional RACF or application password authentication, directory searches, file deletes, and more. ***TCP Ports 21 and 20***

Confusing Acronyms for File Transfer …

Acronym & Meaning	RFC #	Function
SFTP SSL File Transfer Protocol	959 2428 (EPSV) 4217	Original Acronym used for SSL FTP: security provided with x.509 certificates together with SSL/TLS procotocols ***TCP Ports 21 and 20***
FTPS File Transfer Protocol Secure or File Transfer Protocol SSL/TLS/ AT-TLS	959 2228 4217	Secured transfer of files relying optionally on RACF and/or application password authentication, certificate authentication and encryption through SSL/TLS or AT-TLS protocols ***TCP Ports 21 and 20*** **Deprecated: TCP Port 990**
ftpd and **ftps** file transfer protocol daemon file transfer protocol server (z/OS forked address space for remote client)	959 or 959, 2228, 4217	Address spaces and processes used by both FTP and FTPS ***TCP Ports 21 and 20***
SFTP SSH File Transfer Protocol Runs under SSH		Secured transfer of files using authentication and encryption facilities of Secured Shell; password authentication is optional ***TCP Port 22***
SSH Secured Shell	4251 (Version 2)	Secured tunnel for communication for: file transfer, terminal command interaction, and other
sftp and sftpd secure file transfer protocol client and daemon		sftp = SSH client command for SSH File Transfer sftpd = SSH server listening for client connect requests ***TCP Port 22***

Confusing Acronyms for File Transfer …

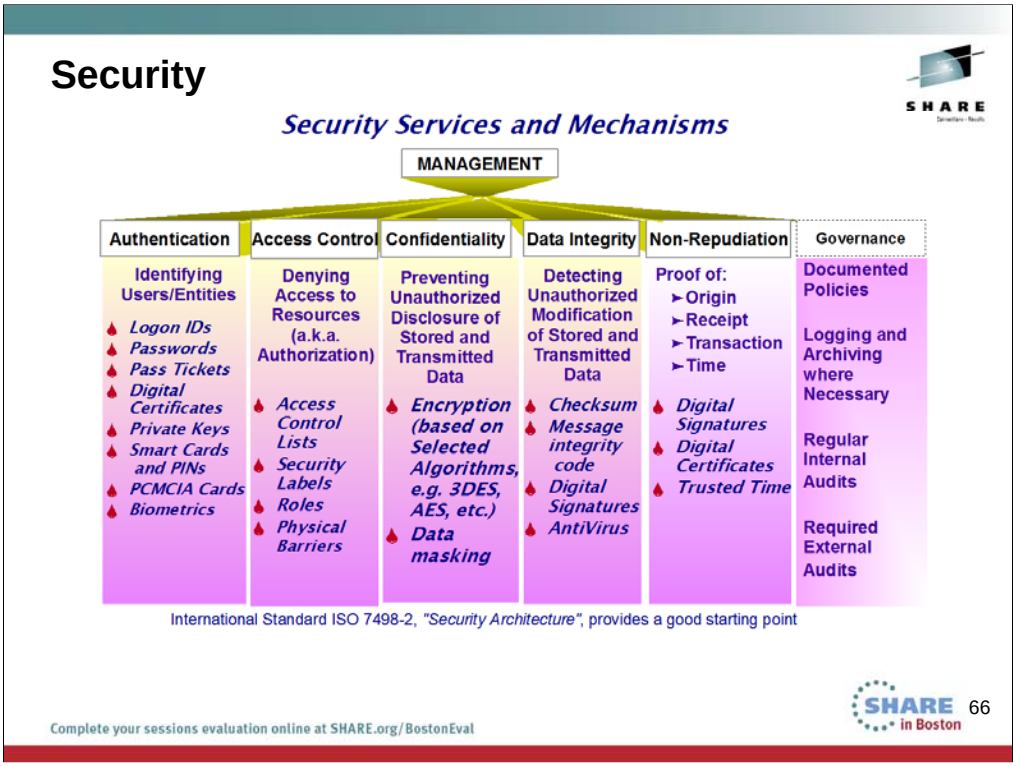
Acronym & Meaning	RFC #	Function
FTP over SSH File Transfer Protocol over an SSH Tunnel	959 2428 (EPSV) 4251	File transfer per RFC959 secured by tunnelling it through SSH
Managed File Transfer Protocols	Proprietary Implementations	File transfer for DB2, with automated recovery of failed file transmissions



Solution to the Alphabet Soup of Acronyms

- **Do not use the terms or acronyms without explanation:**
  - **"Secured FTP"**
  - **"SFTP" or "sftp"**
- **If someone else does use these expressions, ask him to ...**
  - **Identify what technology is being used to secure the File Transfer:**
    - With SSH?
    - With SSL or TLS or AT-TLS?
    - With a VPN (IPSec Virtual Private Network)?
    - Proprietary coding?
    - Other?
- **Explain the requirements for the File Transfer:**
  - **Security Service that is required?**
    - Authentication
    - Access Control
    - Confidentiality (Encryption, Data Masking
    - Data Integrity Preservation
    - Non-repudiation
    - FIPS 140 dependencies?
  - **Recovery/Restart Capability**
  - **Platforms that are involved?**
  - **Types of files needing to be transferred?**
    - File Organization: Record (e.g., MVS organization), Stream, VSAM, DB2, etc.?
  - **Cost?**
  - **Other?**

Differences in Security Implementations



Legacy Security Needs as depicted still exist. However, the tools or mechanisms used to provide the security have had to become increasingly sophisticated to meet current demands. Some of the security technologies above are no longer as powerful as they once appeared, and new technologies have had to arise to meet advances in security infringements.

Identification of Users

Authentication of Users with Passwords

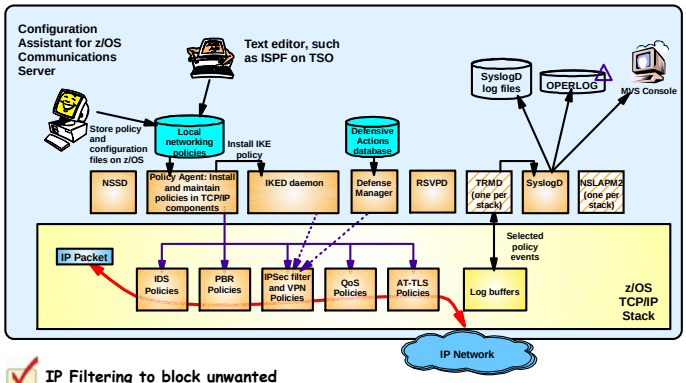
Access Control of Users to

- Building
- Room
- Data Access
- Networks (Firewalls and IP Filtering)
- Intrusion Detection and Services

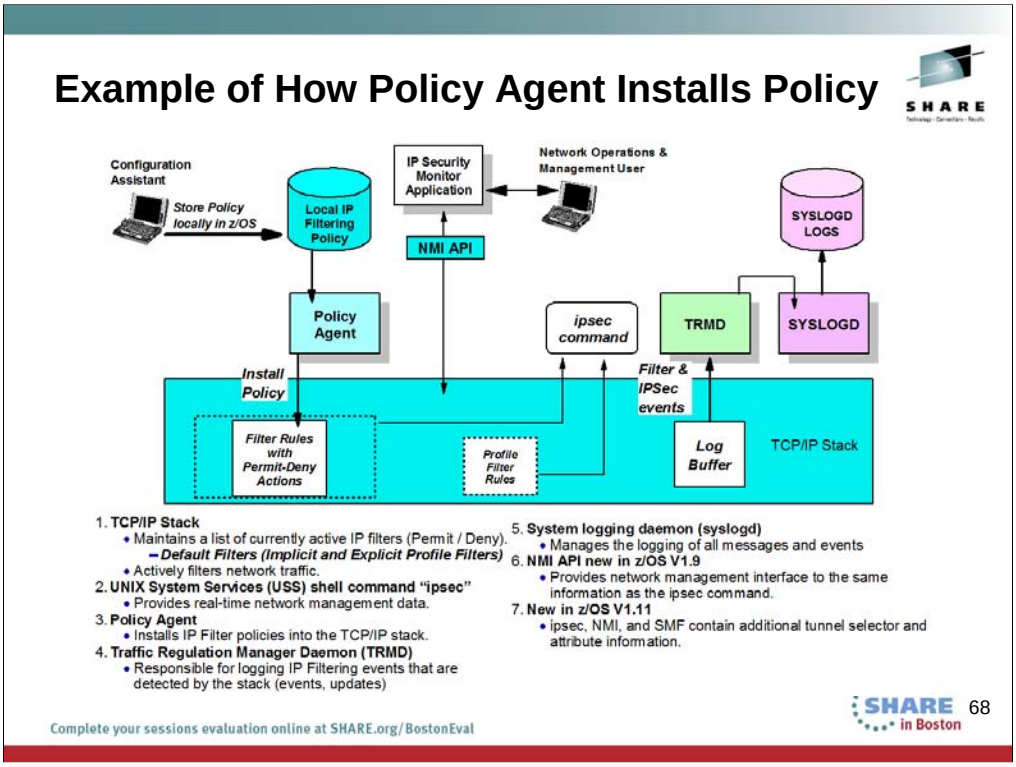
Data Privacy or Confidentiality

Data Integrity – Trust in the sent or received data

Security Policies with z/OS CS Policy Agent



- IP Filtering to block unwanted traffic from entering or leaving your z/OS system
- Application-specific selection of outbound interface and route (Policy-based routing PBR)
- Connection-level security for TCP applications without application changes
- Providing secure end-to-end IPSec VPN tunnels on z/OS
- Making sure high-priority applications also get high-priority processing by the network
- Protection against "bad guys" trying to attack your z/OS system



Internet Key Exchange daemon (IKED)

- •Responsible for retrieving IPsec policies from the Policy Agent.
- •Used for dynamic VPNs.
- •Allows for secret keys and other protection-related parameters to be exchanged prior to a communication without the intervention of the user.

TCP/IP Stack

- •Maintains a list of currently active IP filters and IPsec security associations.
- •Actively filters network traffic.
- •Controls encryption and decryption of network data.
- •Maintains counters associated with an IPsec security association lifetime.

UNIX System Services (USS) shell command "ipsec"

- •Provides real-time network management data.

NMI API new in z/OS V1.9

- •Provides network management interface to the same information as the ipsec command.

New in z/OS V1.11

- •ipsec, NMI, and SMF contain additional tunnel selector and attribute information.

Policy Agent

- •Used to configure IPsec policies.
- •Installs IPsec policies into the IKED and the TCP/IP stack.

Traffic Regulation Manager Daemon (TRMD)

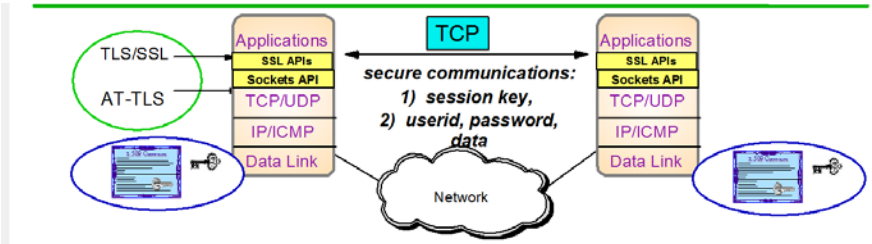
- •Responsible for logging IPsec events that are detected by the stack, including:
  - •IP Filter events
  - •Updates to IPsec policy
  - •Creation, deletion, and refresh of IPsec security associations

System logging daemon (syslogd)

- •Manages the logging of all messages and events

Secured Sockets Layer for Protecting Traffic

Provides security through authentication, encryption, and data integrity checking over an entire network path from application or application-owning node to remote application or application-owning node.



AT-TLS vs. SSL or TLS

- Application Transparent TLS vs. Secured Sockets Layer vs. Transport Layer Security Protocols

	Stands for:	Designed by:	Main Features:	CS Applications
SSL V2	Secure Sockets Layer	NetScape	Server Authentication	TN3270 Server
SSL V3	Secure Sockets Layer	NetScape	Client Authentication	TN3270 Server, FTP
TLS-enabled Telnet (SSL V3.1)	Transport Layer Security -Enabled Telnet	IETF Draft RFC	Single port for SSL Negotiation or non-SSL	TN3270 Server
TLS 1.0	Transport Layer Security	IETF RFC 2246	Standards-Based; Negotiable TLS or SSL port	FTP Server & Client, TN3270 Server, AT-TLS
TLS 1.1	Transport Layer Security	IETF RFC 4346	Standards-Based; New notes, error handling, notes ...	Any applications with AT-TLS -- ***At V1R11 it is AT-TLS default***
AT-TLS	Application-Transparent TLS	IBM; complies with previous standards, incl. de facto	Foundation based on Standards; Application Transparency	Any application; some applications enjoy additional options

This chart explains the evolution of Secure Sockets Layer in Communications Server.

The SSL V2.0 protocol is described within the documentation for SSL V3.0, because even SSL V3.0 can negotiate down to SSL V2.0.

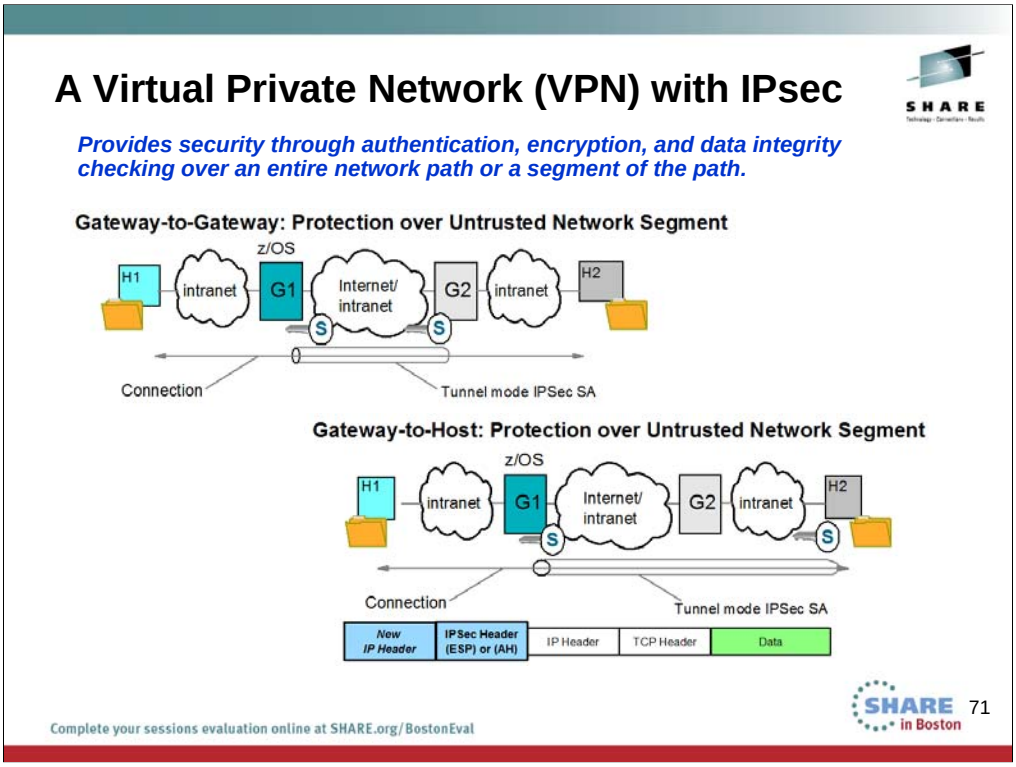
The SSL V3.0 protocol is described at http://home.netscape.com/eng/ssl3/draft302.txt

Note the unfortunate name applied to SSL V3.1: "TLS-enabled ...."

The only piece of TLS that is represented in TN3270 at V2R10 is the ability to negotiate either TLS-enabled or to use a single port for both SSL and basic (i.e., non-SSL) connections. The current draft (as of 09/00) is draft4, whose URL is http://search.ietf.org/internet-drafts/draft-ietf-tn3270e-telnet-tls-04.txt.

The TLS 1.0 protocol is defined in RFC 2246 at www.ietf.org/rfc.html.

The TLS 1.1 protocol is defined in RFC 2246 at www.ietf.org/rfc.html. The updates for TLSv1.1 implement protection against security attacks and other minor changes. TLSv1.1 is compatible with previous TLS versions. AT-TLS can now be configured to enable or disable TLSv1.1. TLSv1.1 is enabled by default.



These are two of several examples for building a Virtual Private Network.

Gateway to Gateway:

- The Data and Security Endpoints are different.
- We need an IP Header to identify the Security Endpoints;
- We need a different IP Header to identify the Data Endpoints.
- In this way we can TUNNEL the Data Endpoint IP Header inside the Security Endpoint IP Header.

Gateway-to-Host:

- The Data and Secxurity Endpoints on the left are different
- The Data and Security Endpoints on the right are the same
- We need an IP Header to identify the Security Endpoints;
- We need a different IP Header to identify the Data Endpoints.
- In this way we can TUNNEL the Data Endpoint IP Header inside the Security Endpoint IP Header.

Appendix: References

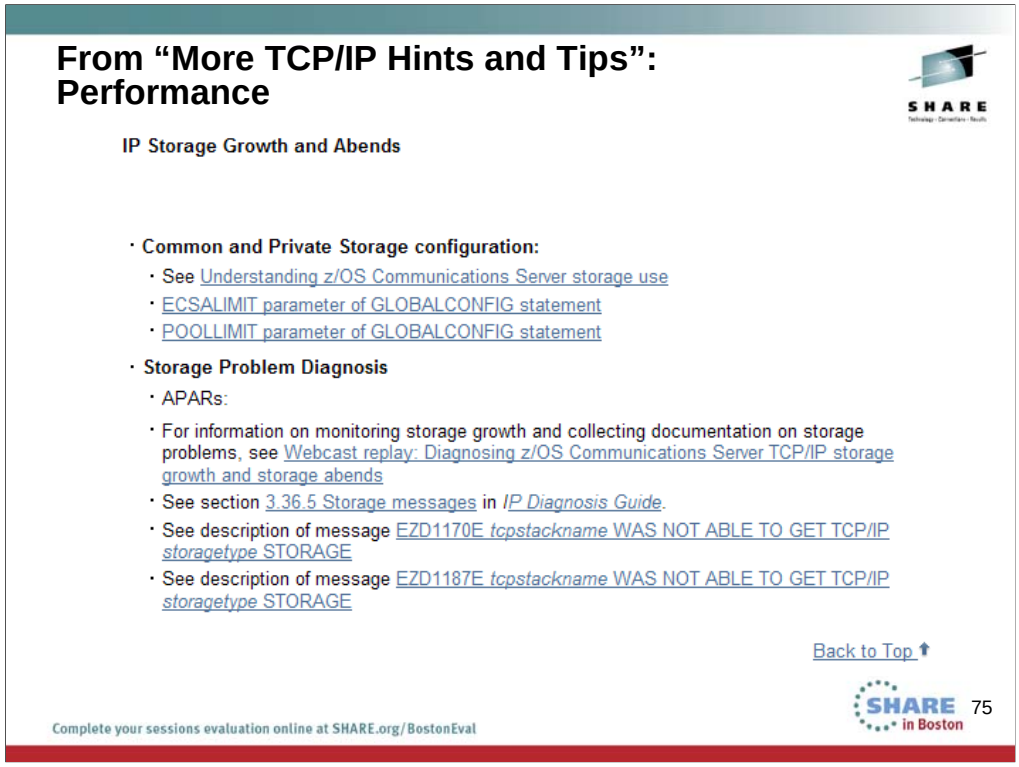
For More Information

- IBM z/OS Communications Server Product Manuals
  - Resource Link
- IBM Redbooks on http://www.redbooks.ibm.com/
  - z/OS Communications Server
  - OSA-Express
  - IBM System z Connectivity Handbook
- Web Document ***z/OS V1R11 Communications Server Scalability, performance, constraint relief, and accelerator***
  - http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/topic/com.ibm.iea.commserv_v1/commserv/1.11z/hardware/perf.pdf
- Web Documents on ATS TechDocs web site http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/Techdocs
  - FLASH10744 QDIO OSA Definition Migration: Device/Link to Interface
  - WP101327 Performance and Capacity Planning Information for z/OS Communications Server
  - PRS1707 z/OS OMPROUTE Hints and Tips -- Focus on OSPF
  - PRS4927 Ordering OSA Adapters with Multiple Ports per CHPID? Don't Make these Mistakes!!
  - PRS3950 Avoiding the Pitfalls of an OSA-E3 or OSA-E4S Migration (z/OS Examples)
  - PRS3296 Understanding VLANs when Sharing OSA Ports on System z
  - FLASH10706 OSA-E3 Multiport and Portname Conflicts
  - PRS789 z/OS Communications Server TCP/IP VIPA (Virtual IP Address)

Documents, URLs for Performance & Tuning

- http://www-01.ibm.com/support/docview.wss?uid=swg27020466&aid=3
  - OSA Performance Improvements
- http://www-01.ibm.com/support/docview.wss?uid=swg27005524
  - **z/OS Communications Server Performance Index**
- http://www-947.ibm.com/support/entry/portal/
  - http://www-947.ibm.com/support/entry/portal/overview//software/other_software/z~os_communications_server
    - **IBM Support Assistant**
- **http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp**
  - **IBM Education Assistant**

See the appendix of this document to find out about Web portals like the IBM Support Assistant and IBM Education Assistant, which will help you navigate to performance and tuning sites for various components, including z/OS Communications Server.

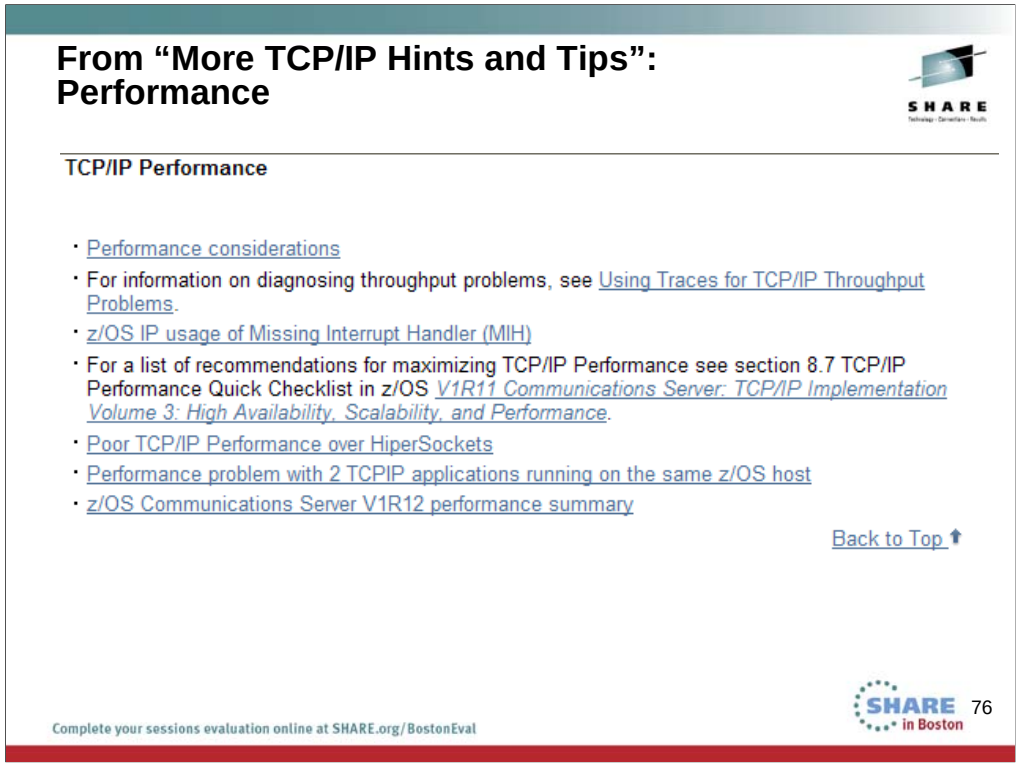


The web page for this information is http://www-01.ibm.com/support/docview.wss?uid=swg27019687

You reach this page by going to …

http://www-01.ibm.com/software/network/commserver/zos/ and then selecting “Technical Articles”.

http://www-01.ibm.com/support/docview.wss?rs=852&uid=swg27006776



The web page for this information is http://www-01.ibm.com/support/docview.wss?uid=swg27019687

You reach this page by going to …

http://www-01.ibm.com/software/network/commserver/zos/ and then selecting “Technical Articles”.

http://www-01.ibm.com/support/docview.wss?rs=852&uid=swg27006776

Manuals to Get You Started with CS Migration

- **z/OS Introduction and Release Guide (GA22-7502-nn)**
  - Presents high-level function descriptions with pointers to the detailed descriptions in New Function Summary
- **z/OS Migration (GA22-7499-nn)**
  - Lists Communications Server function that requires you to take action to migrate to V1R12 or V1R13
  - This information is not provided in this format in the Communications Server library
- **z/OS Communications Server New Function Summary (GC31-8771-nn)**
  - Detailed descriptions of new CS functions
- **z/OS Summary of Message and Interface Changes (SA22-7505-nn)**
  - Lists all new and changed Comm Server commands, parameters, socket API changes, FTP and Telnet changes, etc.
  - This information is not provided in this format in the Communications Server library
- **IBM Health Checker for z/OS: User's Guide (SA22-7994-nn)**
  - Install Health Checker on current release to review migration warnings for new release

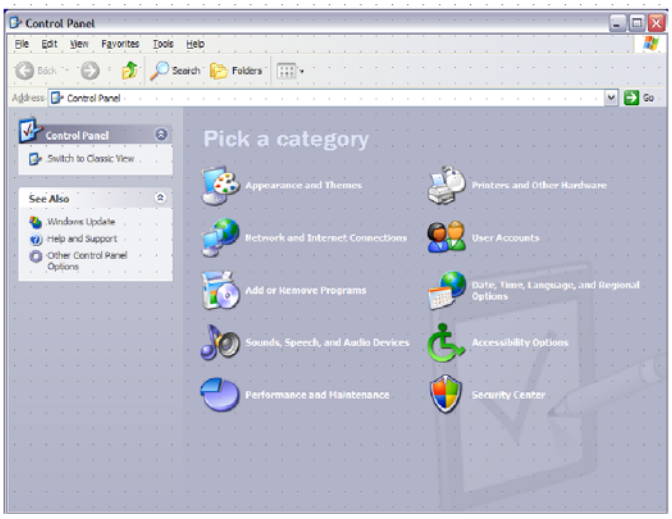
Appendix:
Operating Systems Supporting the Different Architectures and Networks

Operating Systems: Single vs. Multiple-User Operating Systems

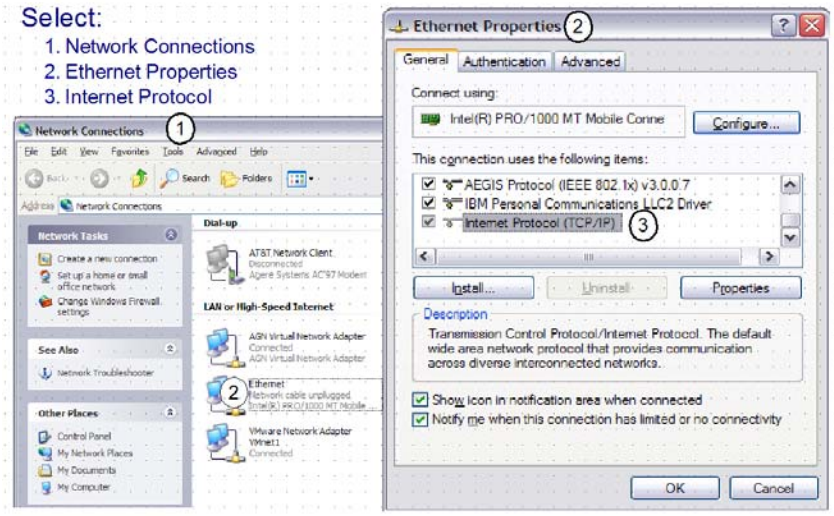
- **Windows**
  - Typically a “Single-user system”
  - Typically Security mechanisms need not be as robust as what is on a z platform
- **z/OS (MVS), z/VM, Linux on z, z/VSE, z/TPF.**
  - Typically “Multi-user systems”
  - Strong security mechanisms
    - In Hardware and Microcode (Firmware)
    - In Software applications
    - In centralized Security Access Facility (SAF) like RACF or ACF2 or Top Secret

You have learned that MVS is an operating system that typically hosts many users at a time. This is unlike your windows operating system on your workstation or laptop, that tends to host only one user at a time. As a result, MVS requires very strong security measures to ensure that users do not interfere with each other and cannot access resources for which they have not been authorized. Some of these security measures are anchored in the hardware and microcode of the System z. Other security measures are anchored in security definitions available in applications and in security access facilities like RACF. The security in z/OS Communications Server is thus tightly controlled through a multitude of mechanisms.

Windows Operating System Example (XP)



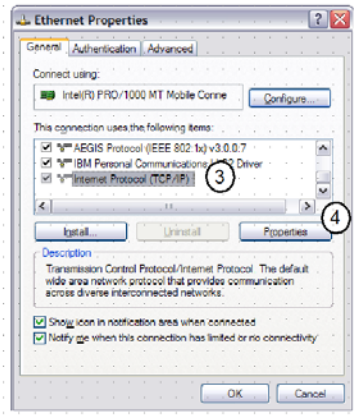
Configuring through a GUI

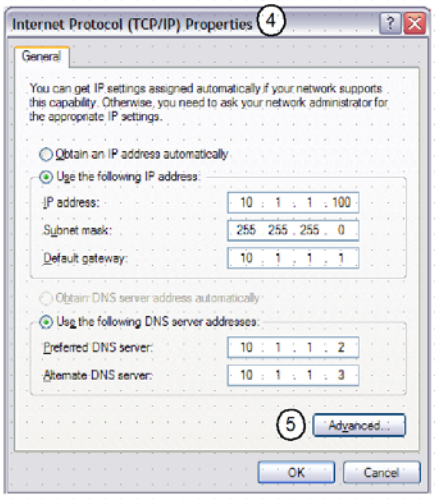


Configuring through a GUI …

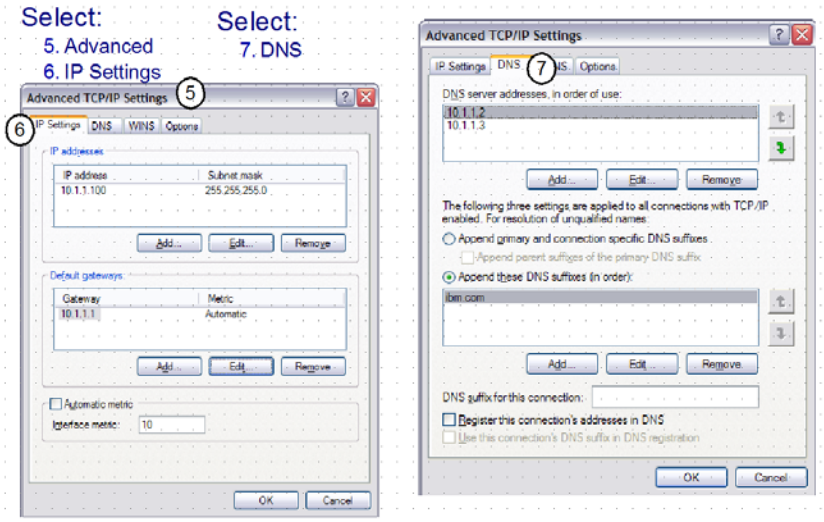
Select:

3. Ethernet Protocol (TCP/IP)
4. Properties
5. Advanced





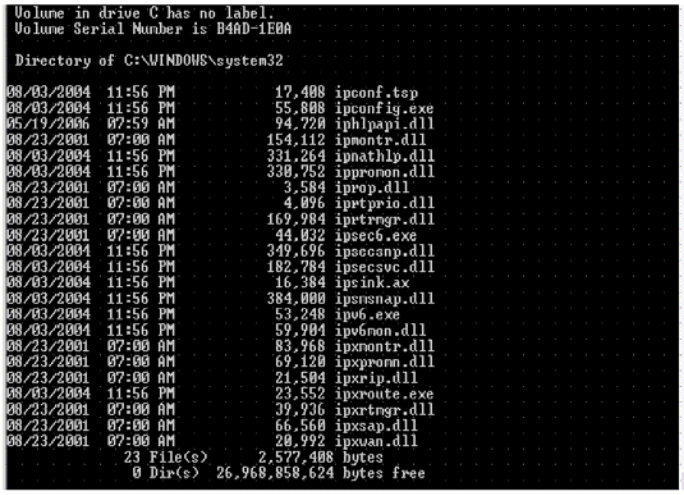
Configuring through a GUI …



TCP/IP Execution Environment in Windows

Windows uses an ASCII keyboard and ASCII character set for interpreting data.

File Structure for IP Definition in Windows



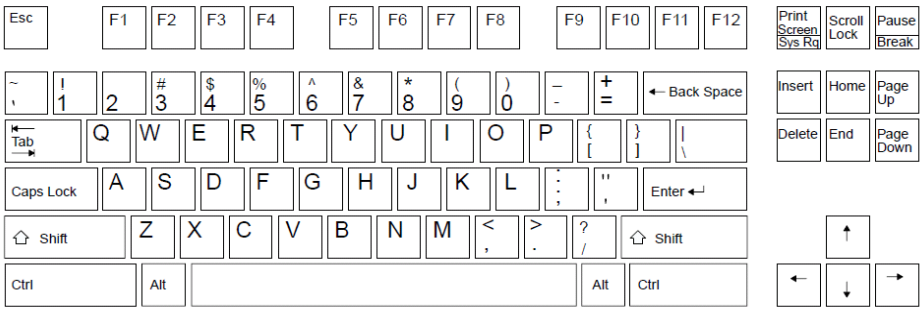
```
 Volume in drive C has no label.
 Volume Serial Number is B4AD-1E0A

 Directory of C:\WINDOWS\system32

08/03/2004  11:56 PM            17,408 ipconf.tsp
08/03/2004  11:56 PM            55,808 ipconfig.exe
05/19/2006  07:59 AM            94,720 iphlpapi.dll
08/23/2001  07:00 AM           154,112 ipmontr.dll
08/03/2004  11:56 PM           331,264 ipnathlp.dll
08/03/2004  11:56 PM           330,752 ippromon.dll
08/23/2001  07:00 AM             3,584 iprop.dll
08/23/2001  07:00 AM             4,096 iprtprio.dll
08/23/2001  07:00 AM           169,984 iprtrmgr.dll
08/23/2001  07:00 AM            44,032 ipsec6.exe
08/03/2004  11:56 PM           349,696 ipsecsnp.dll
08/03/2004  11:56 PM           182,784 ipsecsvc.dll
08/03/2004  11:56 PM            16,384 ipsink.ax
08/03/2004  11:56 PM           384,000 ipsmsnap.dll
08/03/2004  11:56 PM            53,248 ipv6.exe
08/03/2004  11:56 PM            59,904 ipv6mon.dll
08/23/2001  07:00 AM            83,968 ipxmontr.dll
08/23/2001  07:00 AM            69,120 ipxpromn.dll
08/23/2001  07:00 AM            21,504 ipxrip.dll
08/03/2004  11:56 PM            23,552 ipxroute.exe
08/23/2001  07:00 AM            39,936 ipxrtmgr.dll
08/23/2001  07:00 AM            66,560 ipxsap.dll
08/23/2001  07:00 AM            20,992 ipxwan.dll
              23 File(s)      2,577,408 bytes
               0 Dir(s)  26,968,858,624 bytes free
```

Comparison of ASCII and EBCDIC Character Sets

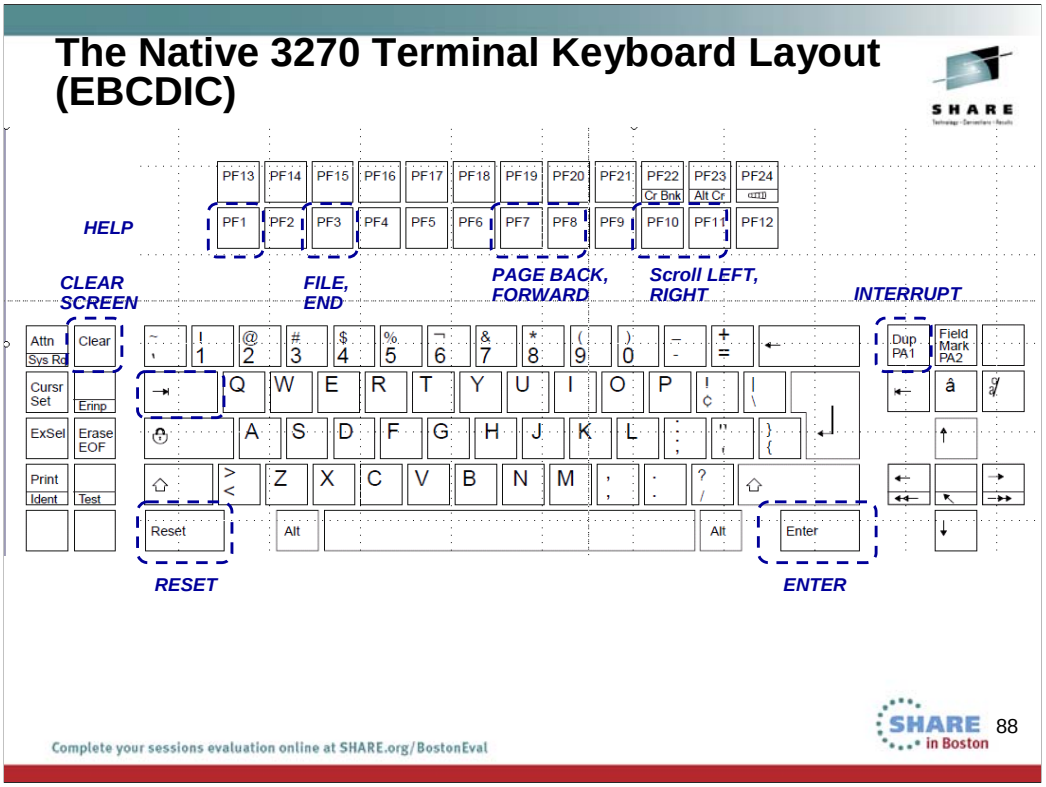
Character	EBCDIC	ASCII
A	11000001 (x'C1')	01000001 (x'41')
B	11000010 (x'C2')	01000010 (x'42')
a	10000001 (x'81')	01100001 (x'61')
1	11110001 (x'F1')	00110001 (x'31')
space	01000000 (x'40')	00100000 (x'20')

Many control characters in ASCII and EBCDIC are the same, but some do vary. The control characters mapped to video terminal display keyboards tend to be in different locations if you are using a keyboard that is attached to an ASCII application vs. one that is attached to an EBCDIC application. See the keyboard layouts on the following pages.

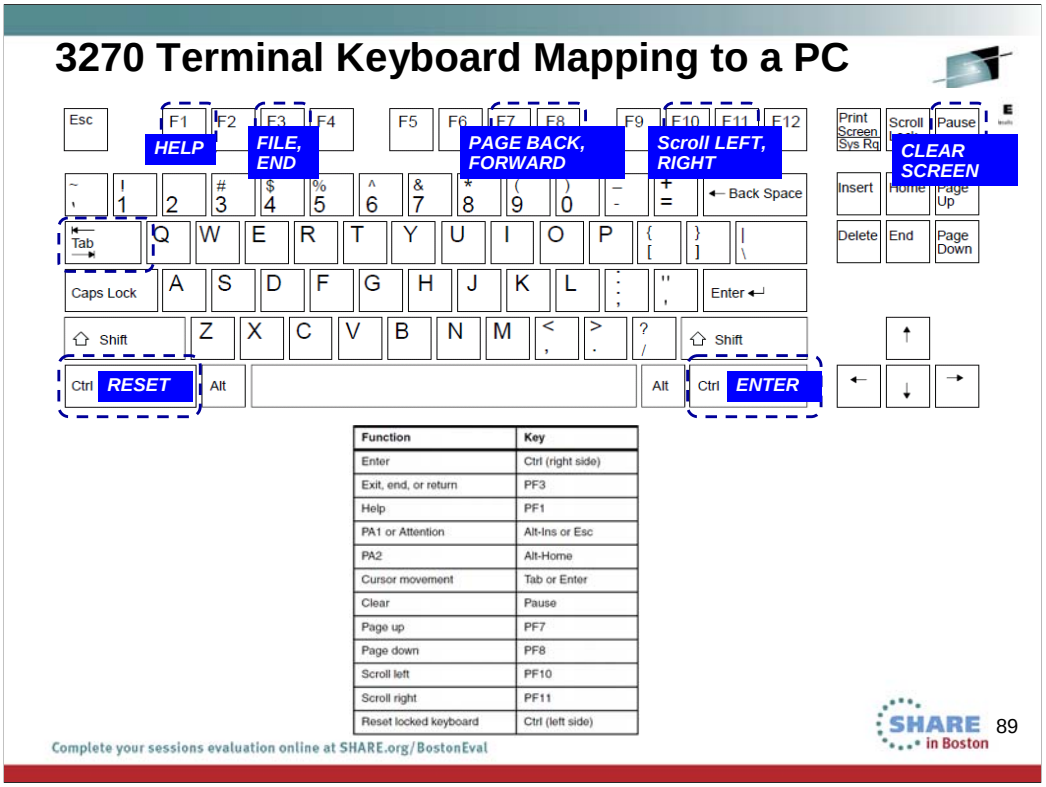
An ASCII Laptop or Workstation Terminal Keyboard Mapping



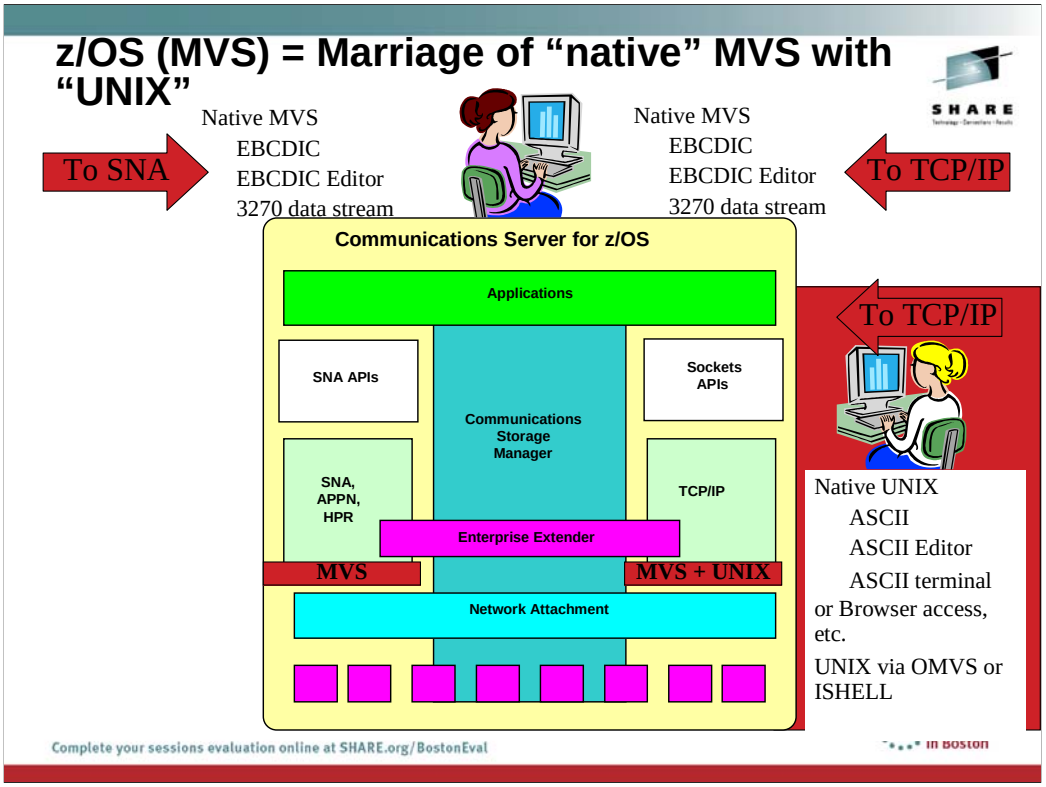
The visual shows you the layout of a subset of an English-language, native 3270 datastream keyboard. The keys that are “highlighted” represent frequently used keys that occupy different positions and have different functions on a workstation (or PC, or laptop) keyboard. A 3270 terminal emulator running on a workstation initializes a keyboard mapping function, which changes the standard PC keyboard’s keys to correspond to a 3270 terminal session.



The visual shows you the layout of a subset of an English-language, native 3270 datastream keyboard. The keys that are “highlighted” represent frequently used keys that occupy different positions and have different functions on a workstation (or PC, or laptop) keyboard. A 3270 terminal emulator running on a workstation initializes a keyboard mapping function, which changes the standard PC keyboard’s keys to correspond to a 3270 terminal session.



The visual shows you the layout of a subset of an English-language, native 3270 datastream keyboard. The keys that are “highlighted” represent frequently used keys that occupy different positions and have different functions on a workstation (or PC, or laptop) keyboard. A 3270 terminal emulator running on a workstation initializes a keyboard mapping function, which changes the standard PC keyboard’s keys to correspond to a 3270 terminal session.

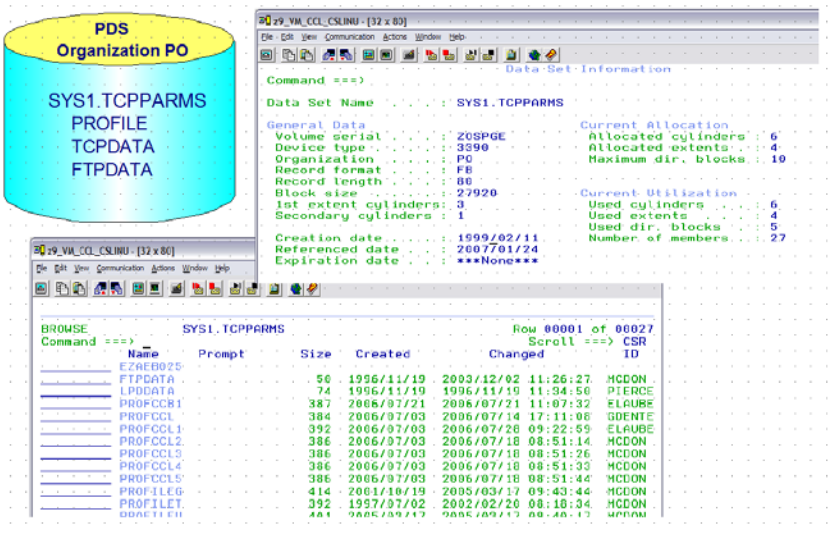


You have also heard from previous speakers, including Linda that MVS or z/OS has evolved from what originally was a purely mainframe operating system with an MVS identity to what is now a combination operating system that can run both MVS applications and UNIX applications. It thus has a dual personality: part MVS and part UNIX. You have heard that the original name for UNIX on z/OS was "Open Edition" or "OMVS" or even "UNIX System Services." We also reference UNIX System Services with the acronym "USS." The SNA component of CS -- VTAM-- does not exploit UNIX System Services in z/OS, but TCP/IP does.

UNIX tends to use ASCII character sets and ASCII terminal emulation; MVS tends to use EBCDIC character sets and 3270 terminal emulation.

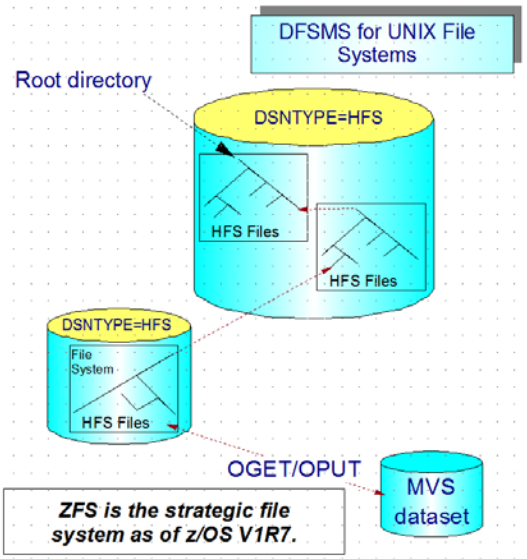
You can reach UNIX files and processes in two fashions: natively using ASCII emulators including browsers, or via 3270 data streams entering into the OMVS shell or the ISHELL which enables the use of the ISPF EBCDIC editor.

MVS Datasets for TCP/IP: Sequential File Systems and PDS(E)s



Unix System Services File Structures: zFS or HFS (zSeries or Hierarchical File System)

- Organized into "Directories" and "Files."
- HFS is hierarchically organized file system
- zFS is linearly organized; it is strategic and is the better performing file system of the two
- All data treated as byte streams
- Concurrent write to file from multiple address space
- Permission control
- Byte range locking (voluntary)
- Special files
  - a. Pipes; FIFOs; Character special files
- Import/Export to MVS data sets
- Mountable
- ADSM or Tivoli Storage Manager for file-level backup/restore
- DFSMS/HSM for HFS-level backup/restore
- HFSs can since OS/390 V2R9 be shared in write mode between multiple MVS images in a sysplex



ZFS is the strategic file system as of z/OS V1R7.

Starting and Configuring z/OS TCP/IP Applications

```
//RESOLVER PROC PARMS='CTRACE(CTIRES00)'
//EZBREINI EXEC PGM=EZBREINI,REGION=0M,TIME=1440,PARM=&PARMS   1
//*SETUP   DD  DSN=TCPIP.TCPPARMS(SETUPRES),DISP=SHR,FREE=CLOSE   2
//*SETUP   DD  DSN=TCPIP.SETUP.RESOLVER,DISP=SHR,FREE=CLOSE
//*SETUP   DD  PATH='/etc/setup.resolver',PATHOPTS=(ORDONLY)   2
...
```

```
/etc/rc
_BPX_JOBNAME='syslogd'   /usr/sbin/syslogd -f /etc/syslog.conf &
                  1                          2
```

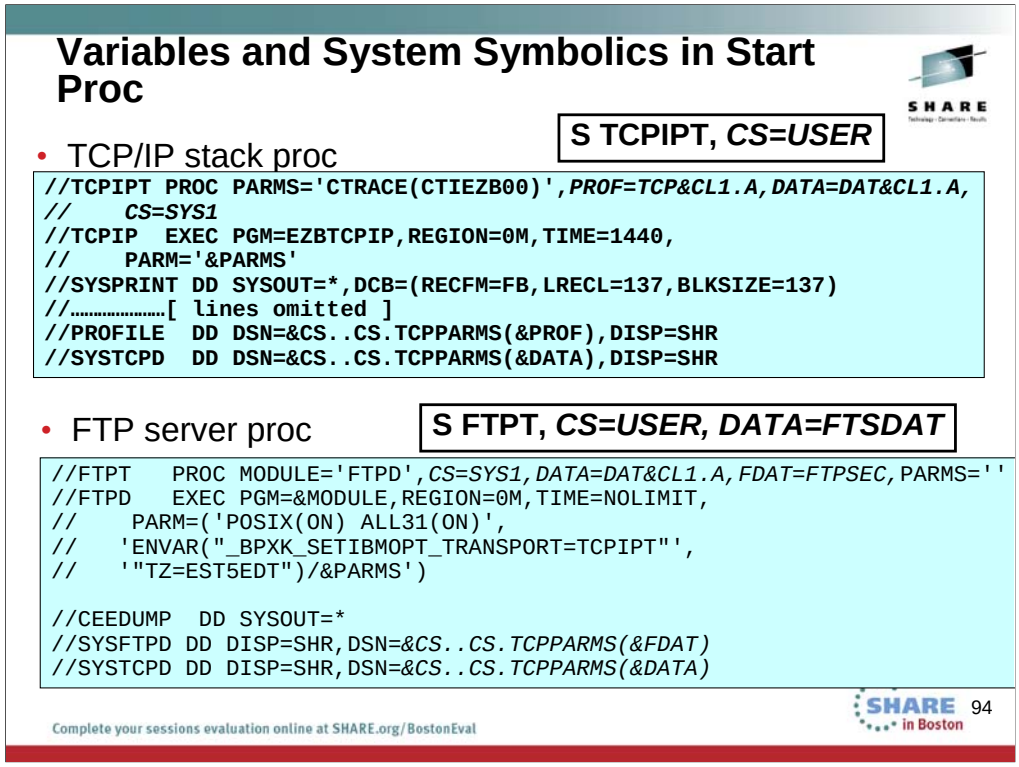
1. TCP/IP Jobs & Applications can be started with ...
   - JCL invoking MVS programs or UNIX processes
   - From /etc/rc in UNIX System Services
     - Some from within /etc/inetd
   - From the z/OS Unix Shell

NOTE: Not all applications can be started either way.

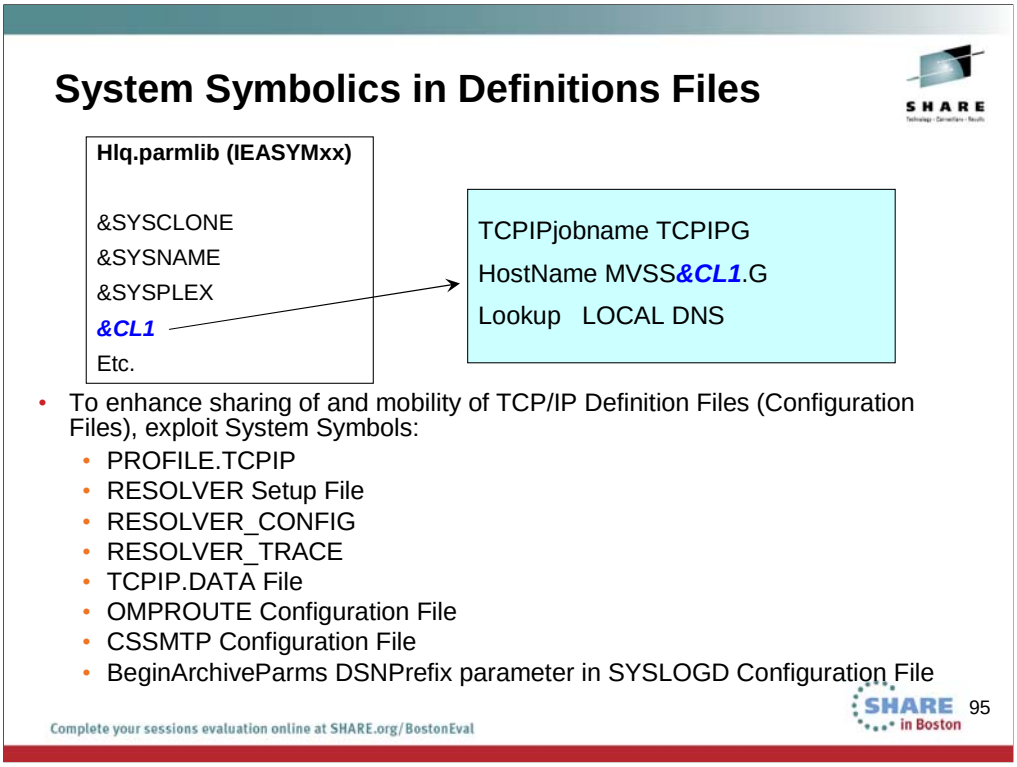
2. TCP/IP Applications can be configured with ...
   - MVS Dataset Member Configuration Definitions (Symbolics often supported)
   - UNIX ZFS or HFS Configuration

Consult IP Configuration Guide for the instructions!

Variables and System Symbolics in Start Proc



By exploiting MVS System Symbols and/or Variables in JCL, we can enhance the usability and flexibility of procedures. For example, in our classes we use the same procedures, but, without having to redefine statements in the procedures, we can override certain values as is depicted in our TCPIP stack JCL and our JCL for starting FTP.



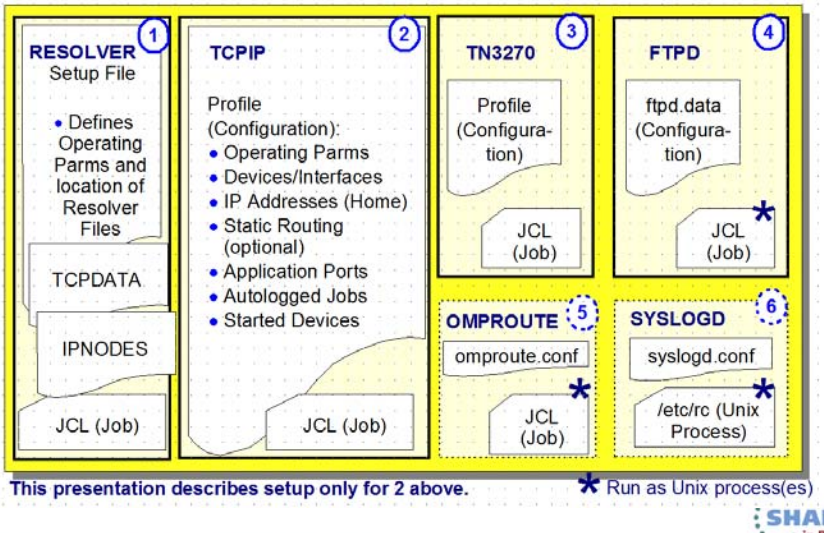
MVS system symbols

Use of MVS system symbols in the PROFILE.TCPIP data set, and data sets referenced by VARY TCPIP,,OBEYFILE commands, is automatically supported. This automatic support first tries to use hiperspace memory files to perform the symbol translation, but if an error occurs, a temporary file is used. The temporary file is created in either the directory specified by the TMPDIR environment variable or, if the TMPDIR environment variable is not defined, in the /tmp directory. Use of MVS system symbols in the resolver setup file and the TCPIP.DATA file is also automatically supported. The resolver reads and processes the TCPIP.DATA file on behalf of TCP/IP applications that invoke resolver services. System symbols are resolved as file records are read. Use of MVS system symbols is also supported in the following cases:

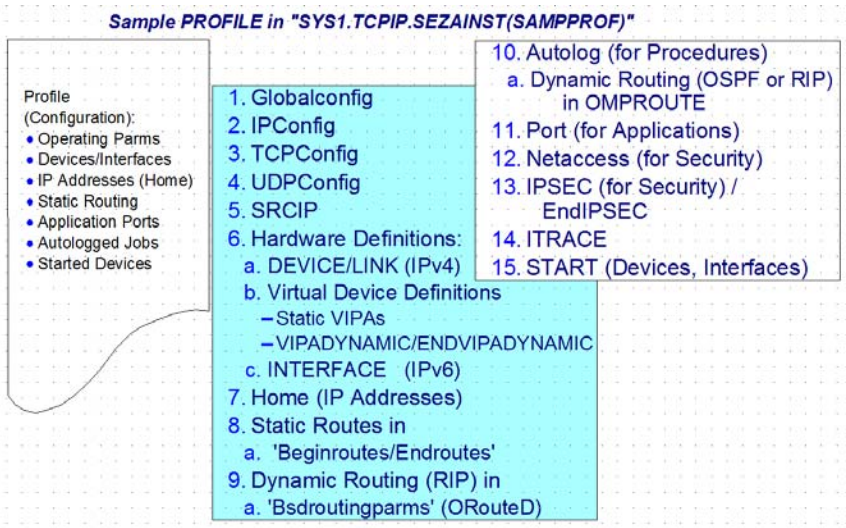
- Values of resolver environment variables, like RESOLVER_CONFIG and RESOLVER_TRACE
- OMPROUTE configuration file
- Communications Server SMTP (CSSMTP) configuration file
- BeginArchiveParms DSNPrefix parameter in the syslogd configuration file

For MVS system symbols in other configuration files, use the symbol translator utility, EZACFSM1, to translate the symbols before the files are read by TCP/IP. EZACFSM1 reads an input file and writes to an output file, translating any symbols in the process. For lists of the static system symbols and dynamic system symbols supported by EZACFSM1, see *z/OS MVS Initialization and Tuning Reference*.

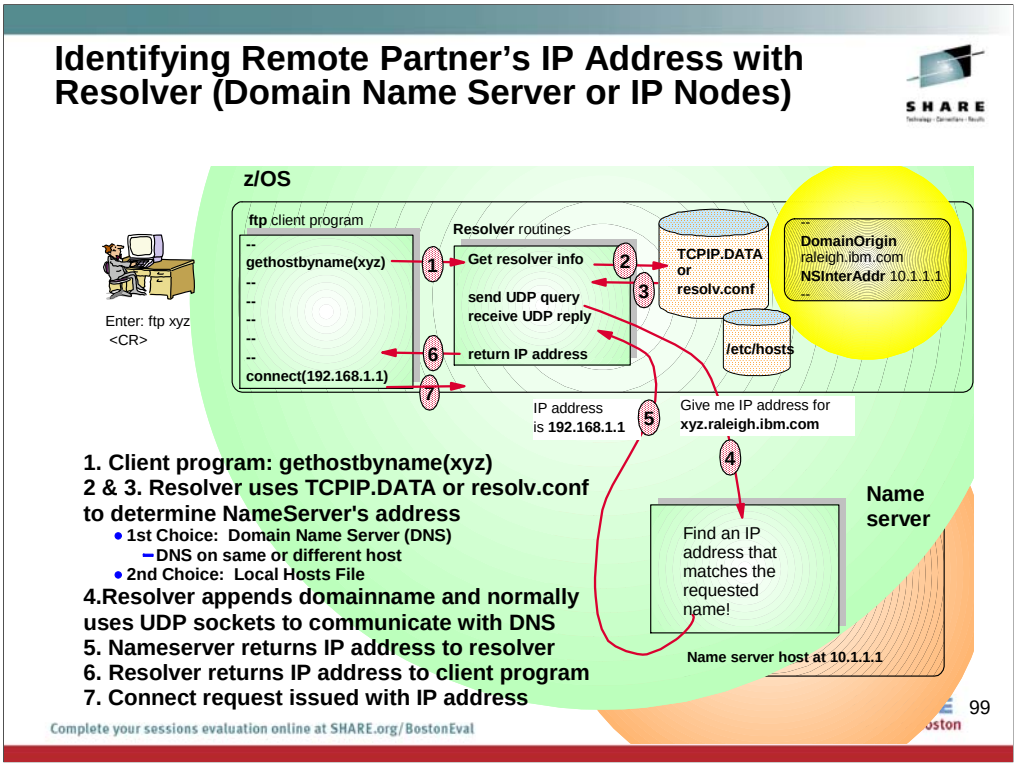
Typical Address Spaces for a Basic z/OS TCP/IP Implementation



Selected Statements in the z/OS TCP/IP Profile



Appendix:
The Resolver in z/OS TCP/IP



Step 1: Here, a user on z/OS or OS/390 enters a request to FTP to a host named xyz. The z/OS FTP client program issues a gethostbyname(xyz) call to the resolver.

Steps 2 & 3: The resolver routines get control and access information from the resolver configuration file to determine how to go about resolving this hostname. Resolver uses Resolver Setup File to determine whether to use a LOCAL name resolution file or a Domain Name Server to determine the IP Address; then it uses either the IPNODES file or the TCPIP.DATA or resolv.conf to determine NameServer's address or.

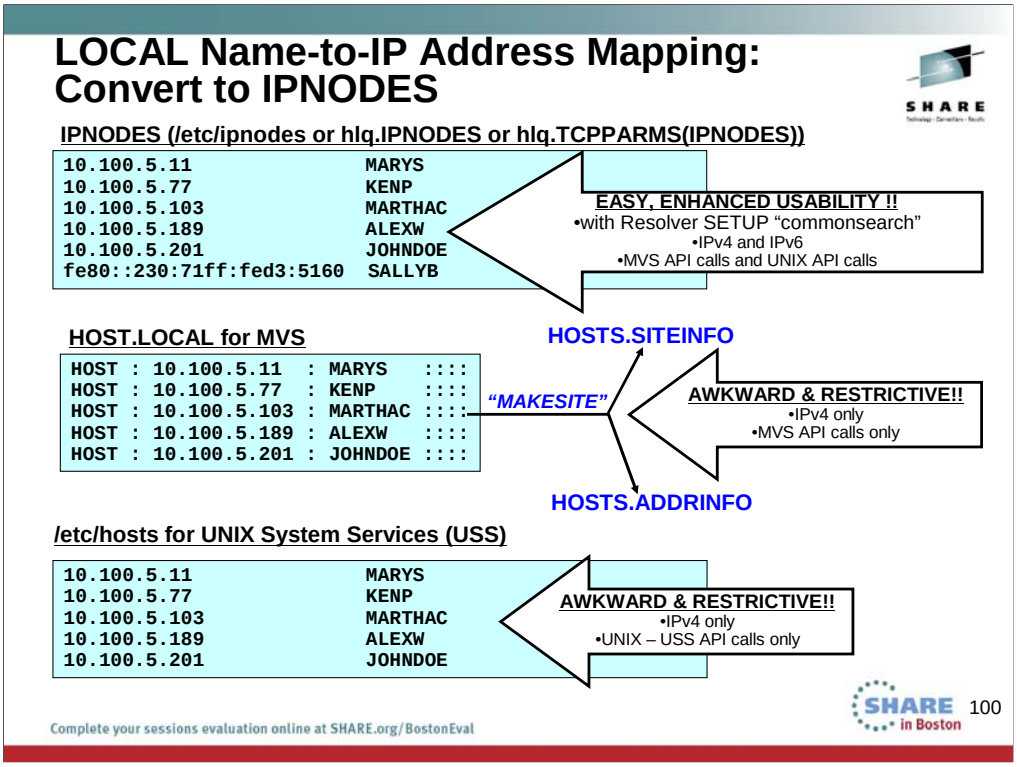
If there is no name server IP address in the resolver configuration file, the resolver looks for a local hosts file (typically /etc/hosts) for locally configured mappings between host names and IP addresses. This default sequence can be changed to look in the Local file first (either etc/hosts or IPNODES).

The name server may run on the same host as the one from which the query comes from (typically configured by specifying NSInterAddr as 127.0.0.1), or it may run on another host in the network.

Step 4: The resolver appends the domainname it learned from the resolver configuration file to the hostname (if no fully qualified hostname was used in the "gethostbyname(xyz)" request) and it generally uses UDP sockets to communicate with the name server.

In this example, the resolver finds that it is to use the DNS at address 10.1.1.1 to resolve the hostname and that it is to append the domain name raleigh.ibm.com to the hostname when requesting the resolution from the DNS.

Step 5: The bottom right box shows the DNS resolving the name xyz.raleigh.ibm.com to IP address 192.168.1.1 and returning this address to the resolver.



Guidelines: Use ETC.IPNODES (in the style of etc/ipnodes) as the preferred alternative to the generated local hosts tables from MAKESITE for the following reasons:

•No imposed 24 character restriction on host names.

•No imposed restriction on the first eight characters of the host names having to be unique. However, there are certain applications that require the first eight characters to be unique, such as Network Job Entry (NJE).

•Closely resembles that of other TCP/IP platforms, and eliminates the MAKESITE requirement of file post-processing.

•Allows configuration of both IPv4 and IPv6 addresses.

•Only one file is managed for the system, and that all the APIs can utilize the same single file. The COMMONSEARCH statement in the resolver setup file can be used to reduce IPv6 and IPv4 searching to a single search order, as well as to reduce the z/OS UNIX and native MVS environments to a single search order.

SYSTCPD DD or Global Resolver

- MVS JCL identifies PROFILE.TCPIP and Resolver

JCL Job

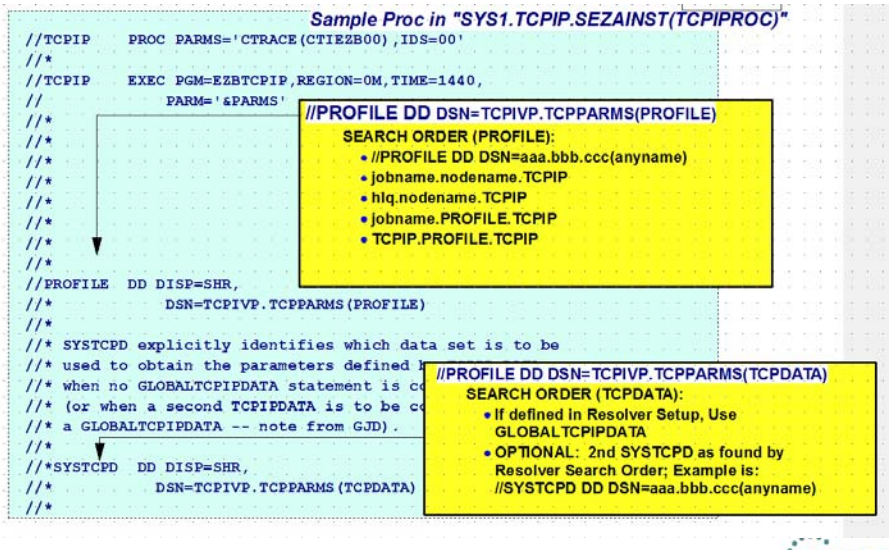
Sample Proc in "SYS1.TCPIP.SEZAINST(TCPIPROC)"

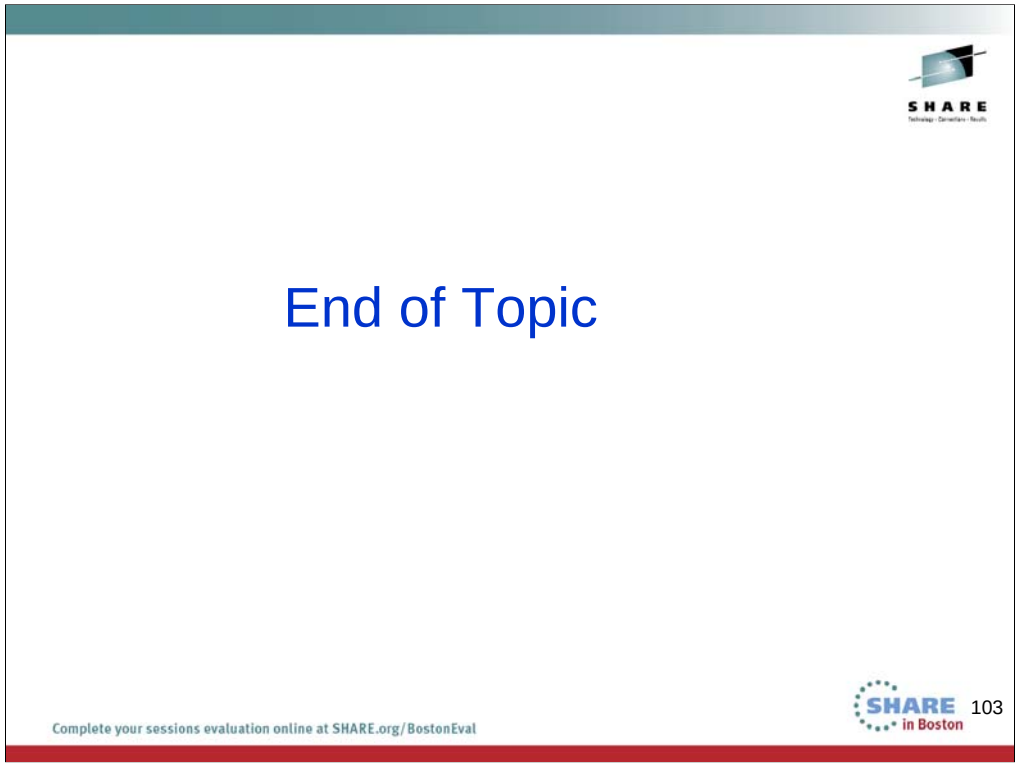
```
//TCPIP    PROC PARMS='CTRACE(CTIEZB00),IDS=00'
//*
//TCPIP    EXEC PGM=EZBTCPIP,REGION=0M,TIME=1440,
//             PARM='&PARMS'
//*
//*
//*
//*
//*
//*
//*
//*
//PROFILE  DD DISP=SHR,
//*            DSN=TCPIVP.TCPPARMS(PROFILE)
//*
//* SYSTCPD explicitly
//* used to obtain the
//* when no GLOBALTCPIP
//* (or when a second T
//* a GLOBALTCPIPDATA
//*
//*SYSTCPD  DD DISP=SHR,
//*           DSN=TCPIVP.TCPPARMS(TCPDATA)
//*
```

//PROFILE DD DSN=TCPIVP.TCPPARMS(PROFILE)
SEARCH ORDER (PROFILE):
//PROFILE DD DSN=aaa.bbb.ccc(anyname)
jobname.nodename.TCPIP
hlq.nodename.TCPIP
jobname.PROFILE.TCPIP
TCPIP.PROFILE.TCPIP

//SYSTCPD DD DSN=TCPIVP.TCPPARMS(TCPDATA)
SEARCH ORDER (TCPDATA):
•If defined in Resolver Setup, Use GLOBALTCPIPDATA
•OPTIONAL: 2nd SYSTCPD as found by Resolver Search Order; Example is: //SYSTCPD DD DSN=aaa.bbb.ccc(anyname)

MVS JCL Points to Configuration PROFILE & to Resolver




SHARE
End of Topic
Complete your sessions evaluation online at SHARE.org/BostonEval
SHARE in Boston
103