IBM Software Group
Enterprise Networking Solutions (ENS) and Transaction Processing Facility (TPF)

z/OS Communications Server V1R8 Technical Overview

Alfred B Christensen - alfredch@us.ibm.com
Sam Reynolds - samr@us.ibm.com

April 2007

IBM Systems

Trademarks and notices

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

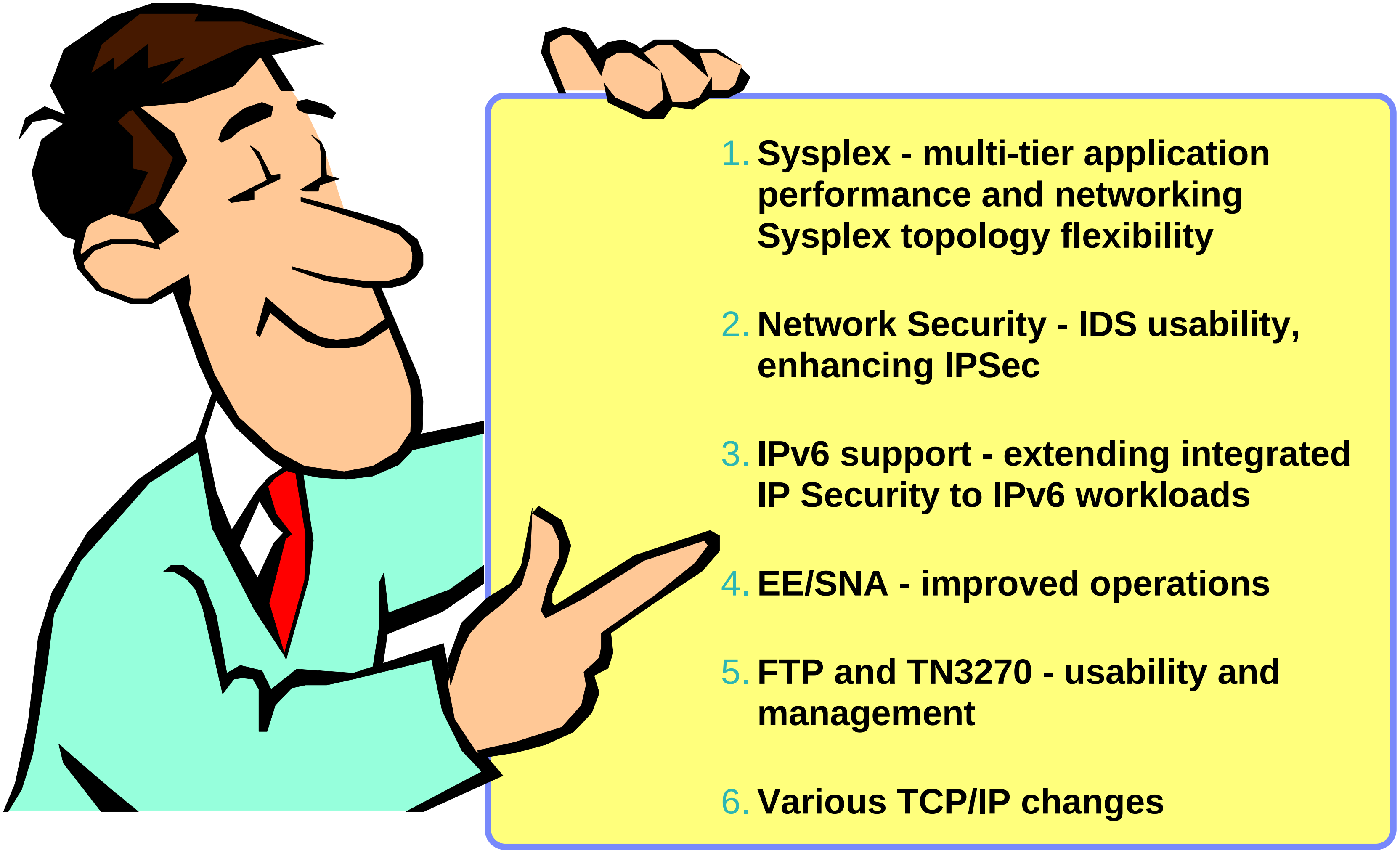
- AIX®
- AnyNet®
- AS/400®
- Candle®
- CICS®
- CICSPlex®
- CICS/ESA®
- DB2®
- DB2 Connect™
- DPI®
- DRDA®
- e business(logo)®
- ESCON®
- eServer™
- ECKD™
- FFST™
- GDDM®
- GDPS®
- HiperSockets™
- IBM®
- Infoprint®
- IMS™
- IP PrintWay™
- iSeries™
- Language Environment®
- MQSeries®
- MVS™
- MVS/ESA™
- NetView®
- OS/2®
- OS/390®
- Parallel Sysplex®
- PrintWay™
- PR/SM™
- pSeries®
- RACF®
- Redbooks™
- Redbooks (logo)™
- S/390®
- System/390®
- ThinkPad®
- Tivoli®
- Tivoli (logo)®
- VM/ESA®
- VSE/ESA™
- VTAM®
- WebSphere®
- xSeries®
- z/Architecture™
- z/OS®
- z/VM®
- zSeries®
- System z™

- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat is a trademark of Red Hat, Inc.
- SUSE® LINUX Professional 9.2 from Novell®
- Other company, product, or service names may be trademarks or service marks of others.
- This information is for planning purposes only. The information herein is subject to change before the products described become generally available.
- All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

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

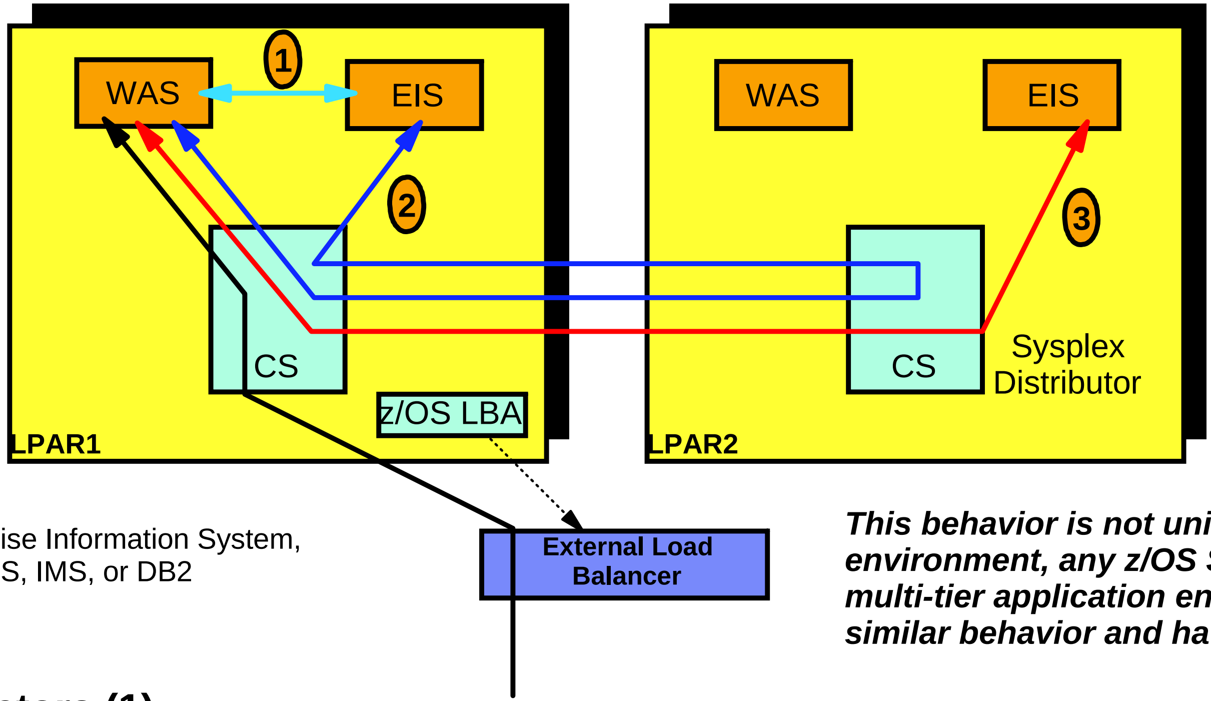
Agenda



1. **Sysplex - multi-tier application performance and networking Sysplex topology flexibility**
2. **Network Security - IDS usability, enhancing IPSec**
3. **IPv6 support - extending integrated IP Security to IPv6 workloads**
4. **EE/SNA - improved operations**
5. **FTP and TN3270 - usability and management**
6. **Various TCP/IP changes**

Sysplex - multi-tier application performance and networking Sysplex topology flexibility

Local vs. remote connector support in today's z/OS environment



Today, multi-tier subsystems and applications need to make a tradeoff between availability and performance objectives.

EIS: Enterprise Information System, such as CICS, IMS, or DB2

This behavior is not unique to a WAS environment, any z/OS Sysplex-resident multi-tier application environment may exhibit similar behavior and have similar issues.

- **Local connectors (1)**
  - Optimized high-speed path (based on local services, such as cross-memory services and RRS)
  - Availability of local target of concern (no automatic switch to target on other LPAR if local is unavailable)
  - If local target becomes unavailable, WAS transactions may complete fast and WLM may in that scenario consider the LPAR a good candidate for increased workload (storm-drain issue)
- **Remote connectors (2 and 3)**
  - Uses TCP/IP for communication
  - Sysplex Distributor (or other load balancer) selects a target among any available targets in the Sysplex
  - If target is local and Sysplex Distributor is remote, communication path is not efficient (2)
  - It is not today possible to favor a local target even if one exists and has capacity

Availability?

End-to-end performance?

Improved multi-tier application support by Sysplex Distributor - optimized for local performance without losing availability

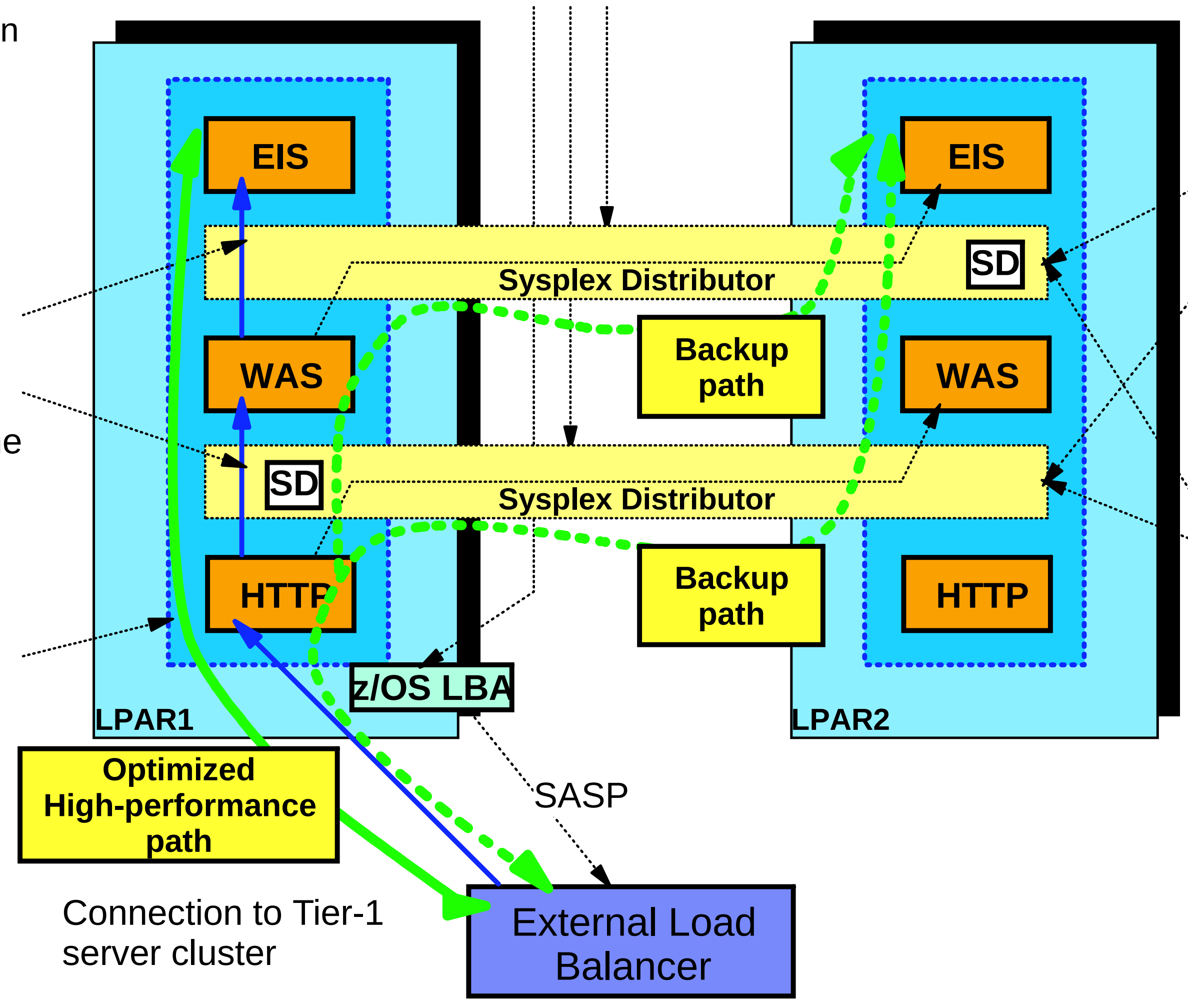
Application endpoint awareness via enhanced Sysplex sockets API processing

- Avoid authentication overhead
- Avoid data conversions

Fast direct local sockets path inside the same "tower" (inside the same TCP/IP stack)

Server instances within same "tower" are **preferred targets**

1. WLM LPAR and server-specific performance weights
2. TCP/IP stack server-specific health weights



Connection to Tier-1 server cluster

Level of **local favoritism** can be configured via new OPTLOCAL option on VIPADISTRIBUTE

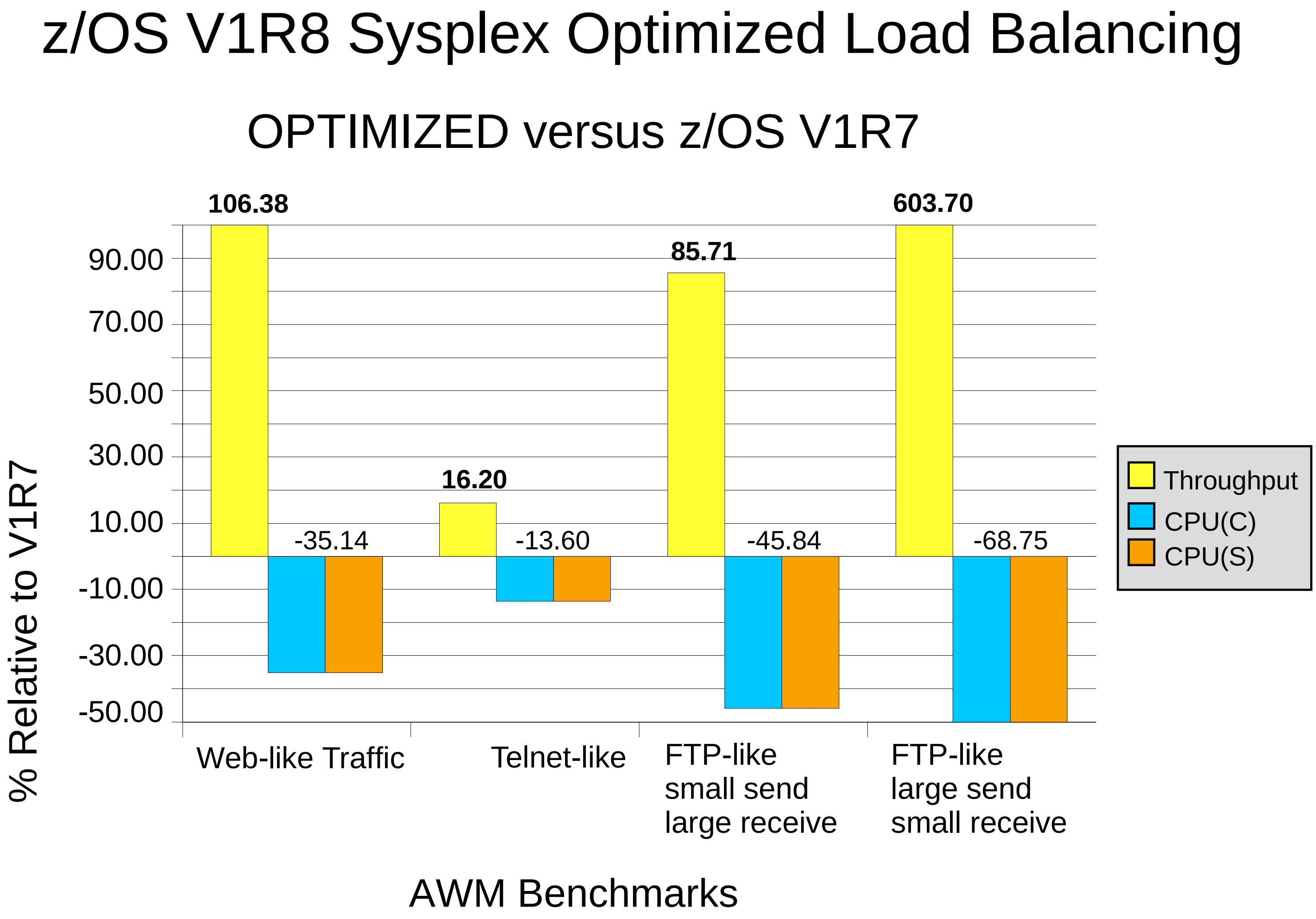
- Always choose local target if target is available and healthy
- Control level of WLM weight impact on target selection

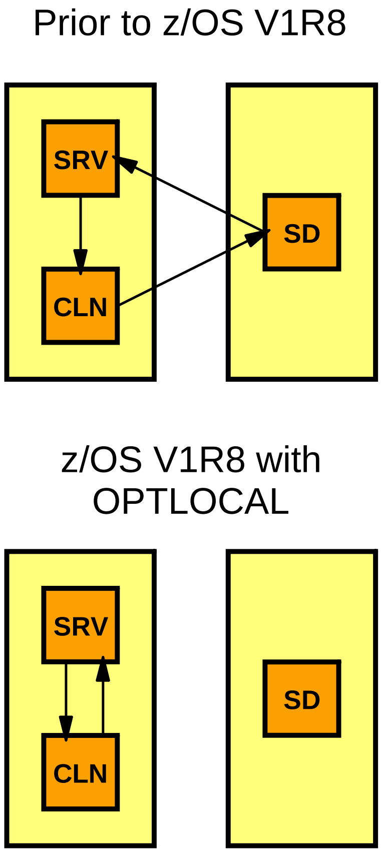
Optimized traffic flow:

- "Distributed" Sysplex Distributor logic in each stack avoids cross-LPAR flows for connection setup when local target is chosen.
- Avoids traffic routing via SD-owning LPAR for local targets

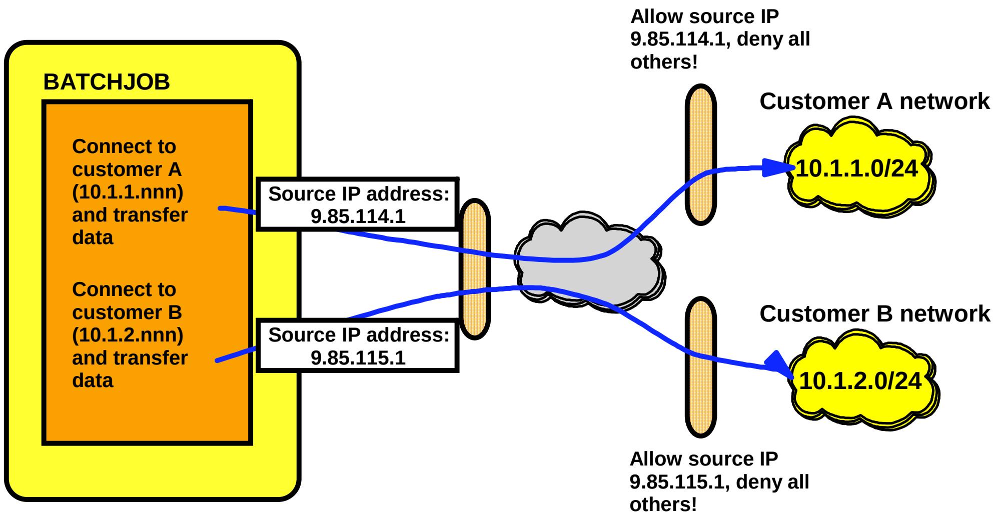
Benchmark comparison - local optimization

With OPTLOCAL, multi-tier subsystems and applications can have both performance and availability within a z/OS Sysplex





Adding support for yet another popular requirement: destination-based source IP address selection


Allow source IP 9.85.114.1, deny all others!
BATCHJOB
Connect to customer A (10.1.1.nnn) and transfer data
Connect to customer B (10.1.2.nnn) and transfer data
Source IP address: 9.85.114.1
Source IP address: 9.85.115.1
Customer A network
10.1.1.0/24
Customer B network
10.1.2.0/24
Allow source IP 9.85.115.1, deny all others!

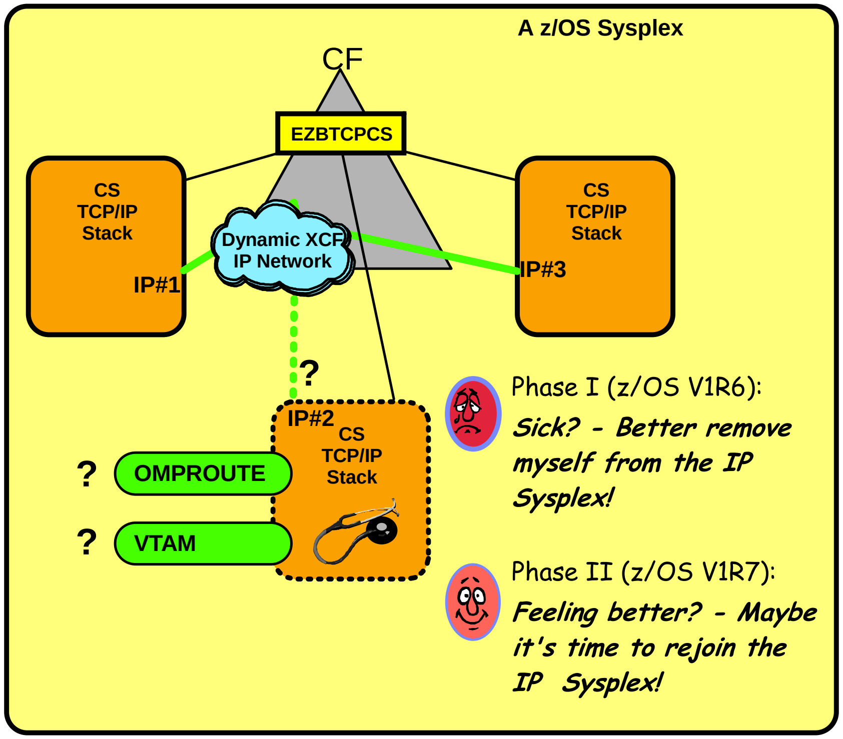
```
SRCIP
      Jobname CUSTAJOB   9.85.112.1
      Jobname CUSTBJOB   9.85.113.1
      Jobname User1*     888:555::222
      DESTIP             10.1.1.0/24 9.85.114.1
      DESTIP             10.1.2.0/24 9.85.115.1
ENDSRCIP
```

Increased flexibility to meet business partner firewall requirements.

Extending configuration control over which local IP address to use for outbound connections from z/OS

- ✓ Outbound connections can use same IP addresses as inbound connections to same application without application change:
  - Easier for accounting and management
  - Easier for security (firewall admin)
  - Permits source IP address selection controls for applications even when application doesn't provide for this programmatically (most don't, but some do!)
- ✓ Introduced job-specific source IP addressing in z/OS V1R6
  - A new TCPIP.Profile statement SRCIP/ENDSRCIP allows the selection of a source IP address for outbound TCP connections by job name
  - Overrides TCPSTACKSOURCEVIPA and SOURCEVIPA specifications
- ✓ **Introduces destination-based source IP address selection in z/OS V1R8**
  - **Extends the SRCIP/ENDSRCIP block with destination IP address-based rules**
  - **The source IP address used by a DESTIP rule cannot in CS z/OS V1R8 be a distributed DVIPA**
  - **Useful if jobnames are unpredictable or if the same jobname establishes connections to multiple business partners**

TCP/IP Sysplex autonomics in z/OS V1R6 and V1R7 reacts to and recovers dynamically from a range of error conditions



Phase I (z/OS V1R6):
Sick? - Better remove myself from the IP Sysplex!

Phase II (z/OS V1R7):
Feeling better? - Maybe it's time to rejoin the IP Sysplex!

The assumption is that if a TCP/IP stack determines it can no longer perform its Sysplex functions correctly, it is better for it to leave the TCP/IP XCF group and by doing so, signal the other TCP/IP stacks in the Sysplex that they are to initiate whatever recovery actions have been defined, such as moving dynamic VIPA addresses or removing application instances from distributed application groups.

- Autonomic functions to reduce single point of failure for distributed applications in a Sysplex
  - Monitor CS health indicators
    - Storage usage - CSM, TCPIP Private & ECSA
  - Monitor dependent networking functions
    - OMPROUTE availability
    - VTAM availability
    - XCF links available
  - Monitor Communications Server component-specific functions

- Monitors determine if this TCPIP stack will remove itself from the Sysplex and allow a healthy backup to take ownership of the Sysplex duties (own DVIPAs, distribute workload)

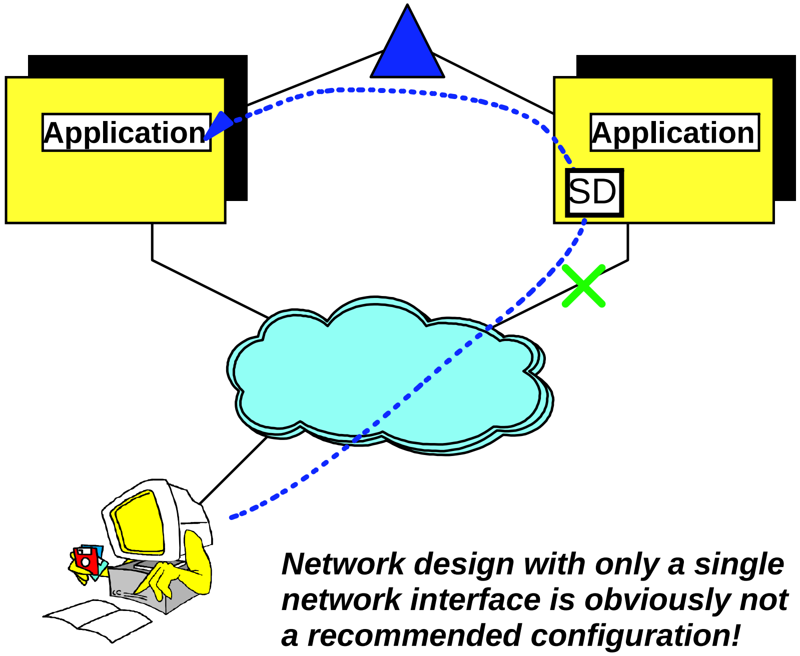
- Monitoring is always done, but configuration controls in the TCPIP Profile determine if the TCPIP stack removes itself from the Sysplex.

```
GLOBALCONFIG SYSPLEXMONITOR TIMERSECS
seconds RECOVERY|NORECOVERY
DELAYJOIN|NODELAYJOIN
AUTOREJOIN|NOAUTOREJOIN
```

You really should enable SYSPLEXMONITOR!

- *Timersecs* - used to determine duration of the troubling condition before issuing messages or leaving the Sysplex (if Recovery)
- *RECOVERY* - TCPIP removes itself from the Sysplex.
- *NORECOVERY* - TCPIP does not remove itself from the Sysplex.
- *DELAYJOIN* - Delay joining Sysplex until OMPROUTE is up
- *NODELAYJOIN* - Join Sysplex immediately
- *AUTOREJOIN* - Rejoin when condition is cleared
- *NOAUTOPREJOIN* - Let an operator decide when to rejoin

TCP/IP Sysplex autonomics adds automated recovery from outages of selected network interfaces



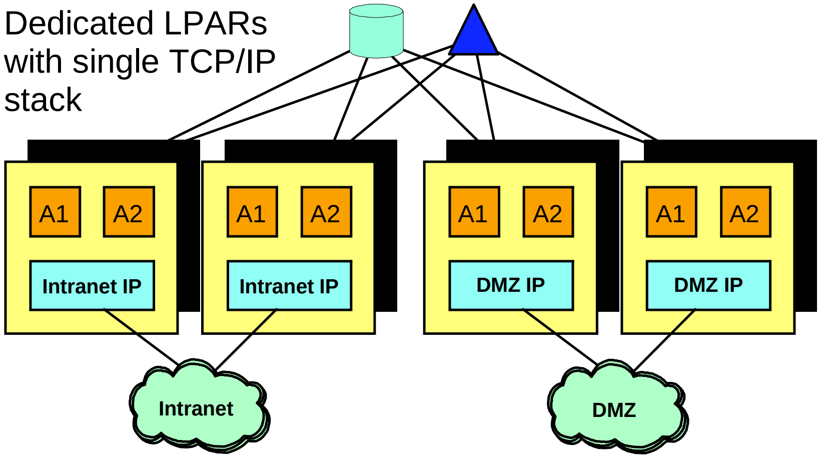
Network design with only a single network interface is obviously not a recommended configuration!

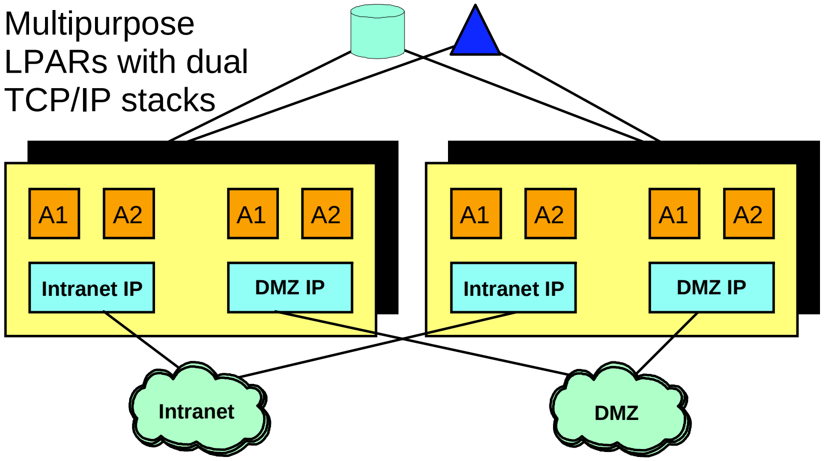
- **Assume that DYNAMICXCF is not an OSPF interface or that we have disabled routing through z/OS in general (NODATAGRAMFWD):**
  - Assume the downstream nodes cannot reach the SD node
    - OSA failure
    - First hop router (downstream) problems
  - All Sysplex health monitors indicate a healthy environment
    - Dynamic XCF connectivity is working
    - No storage issues
    - VTAM is operational
    - OMPROUTE is operational
    - Target Server Responsiveness Fraction indicates no SD environment health problems
  - But since there is no route from the client into the SD node, the SD functions appear unavailable

- **Network outage detection added to the Sysplex autonomics of TCP/IP**
  - Specify which network interfaces to be monitored and if dynamic routing monitoring is to be included or not
  - Monitor network interface itself (active or inactive)
    - To detect interface hardware issues
  - If dynamic routing is used, monitor if dynamic routes exist over the interface
    - To detect first-hop router issues
  - DELAYJOIN extended to monitor for interfaces up and dynamic routes detected

If a network outage condition is detected, the stack may remove itself from the Sysplex if requested by the configuration - allowing backup stacks in the Sysplex to take over its Sysplex responsibilities.

z/OS Sysplex connectivity to multiple security areas has been a challenge ever since CS began using Sysplex capabilities


Dedicated LPARs with single TCP/IP stack

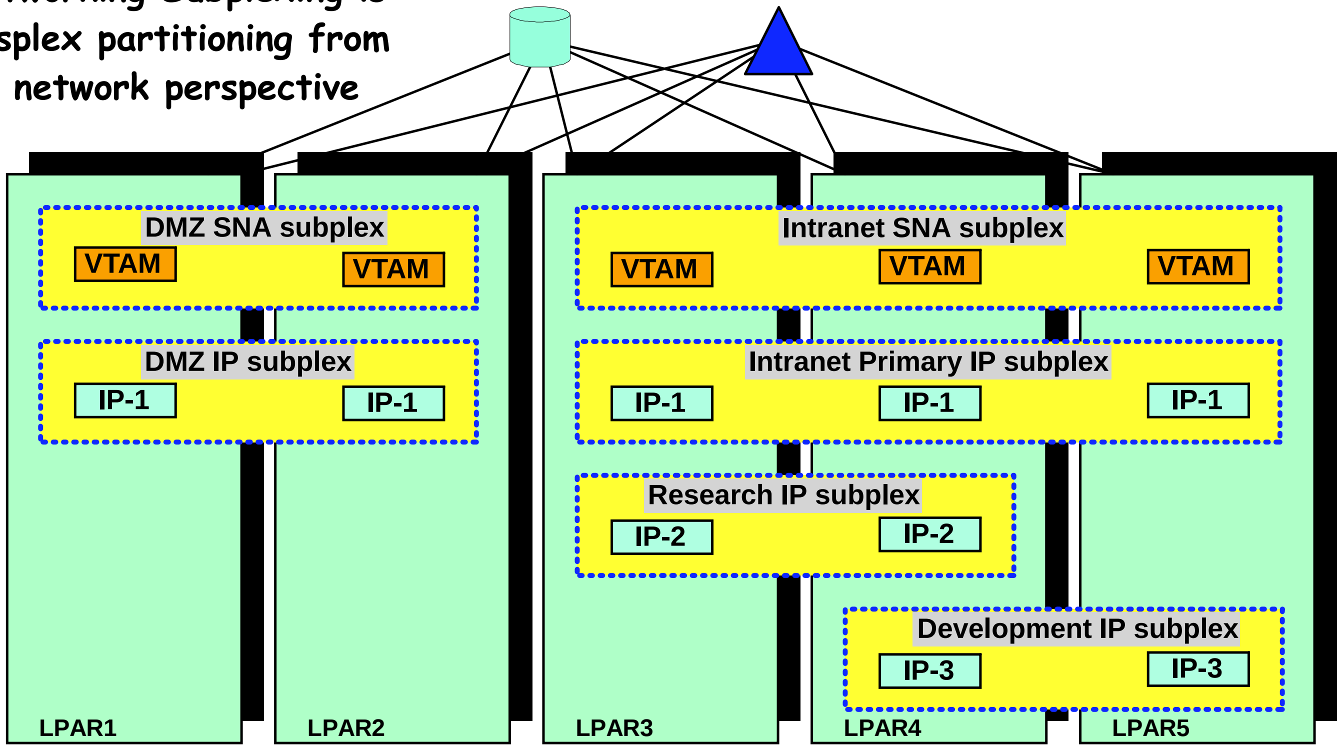

Multipurpose LPARs with dual TCP/IP stacks

- **How to control level of automatic connectivity?**
  - XCF signaling (group name) - both IP and SNA
  - IUTSAMEH (same host IP links inside an LPAR)
  - HiperSockets (as enabled via IQDCHPID in VTAM)
- **How to control level of IP and SNA resource awareness?**
  - Dynamic IP address discovery across the Sysplex
  - VTAM generic resource and MNPS resource scope spans the full Sysplex
- **How to control scope of IP workload balancing using Sysplex Distributor?**
  - SD requires Dynamic XCF to be enabled, and Dynamic XCF will establish automatic IP connectivity to all stacks in the Sysplex that also have Dynamic XCF enabled

To support environments such as these, installations typically end up implementing complex resource controls and disabling many of the dynamic networking functions that are provided by TCP/IP and VTAM.

Enable use of networking Sysplex functions in a Sysplex that is connected to multiple security areas

Networking Subplexing is Sysplex partitioning from a network perspective



Formalized technologies to support multiple network communities within a single z/OS Sysplex - with each community being able to benefit from the networking Sysplex availability and single-system image capabilities.

- **One SNA subplex per LPAR**
- **An IP subplex cannot span multiple SNA subplexes**
- **Different IP stacks in an LPAR may belong to different IP subplexes**
- **Standard RACF controls for stack access and application access to z/OS resources need to be in place.**

- **Networking subplex scope:**
  - VTAM Generic Resources (GR) and Multi-Node Persistent Session (MNPS) resources
  - Automatic connectivity - IP connectivity and VTAM connectivity over XCF (including dynamic IUTSAMEH and dynamic HiperSockets based on Dynamic XCF for IP)
  - IP stack IP address (including dynamic VIPA) awareness and visibility
  - Dynamic VIPA movement candidates
  - Sysplex Distributor target candidates

Subplexing configuration overview

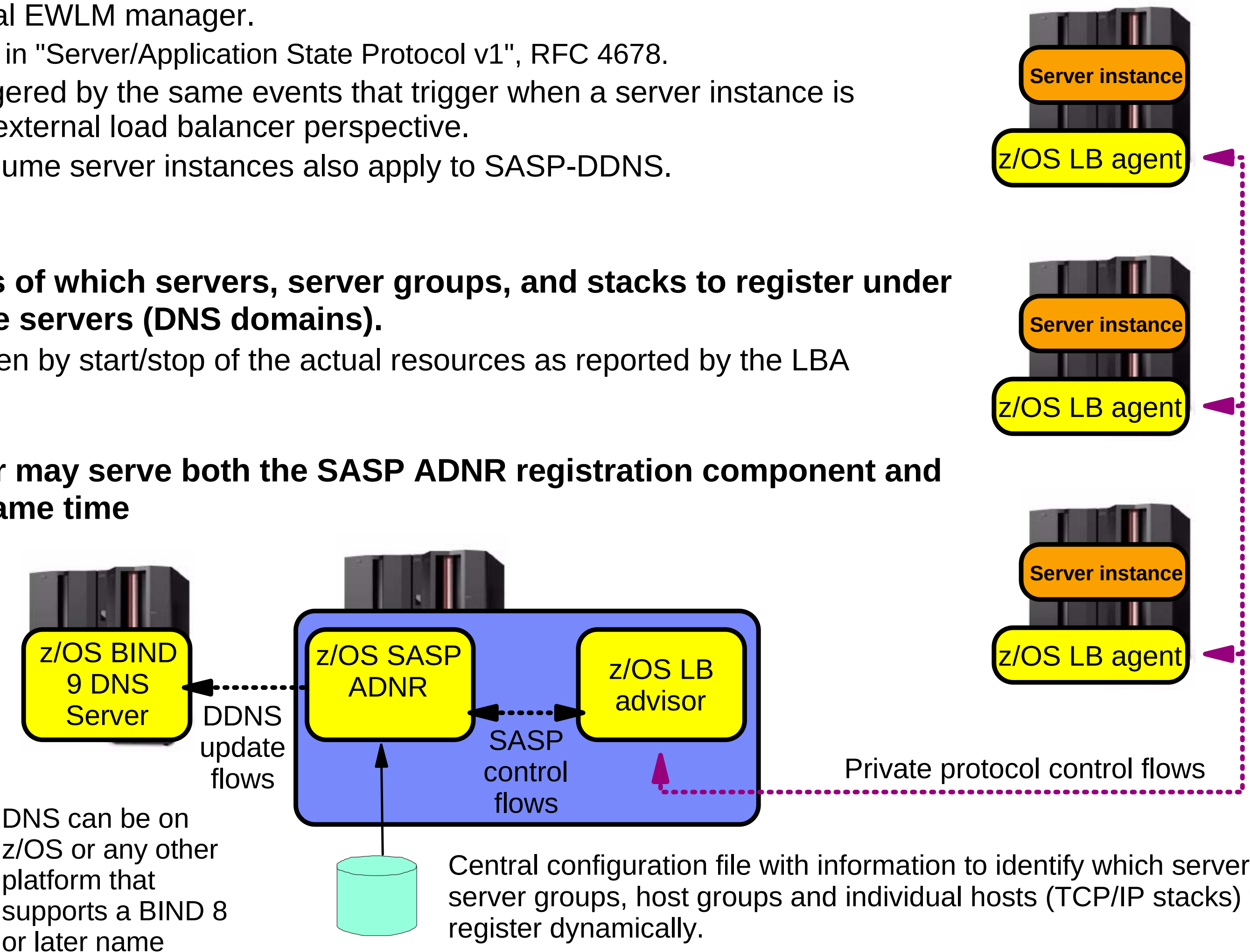
If you do not define the new options, all XCF group names and structure names default to the pre-z/OS V1R8 values

- **New VTAM Start Option:**
  - XCFGRPID vv
    - where vv is a number between 02 and 31
- **VTAM joins ISTXCFvv and ISTCFSvv Sysplex groups**
  - If no XCFGRPID is specified, VTAM will join ISTXCF and ISTCFS01 - as before
- **STRGR and STRMNPS CF structure names are suffixed with vv**
  - For example, if STRGR=ISTMYGR, VTAM will attempt to connect to structure ISTMYGRvv.
  - If no XCFGRPID is specified, VTAM will connect to the names specified in STRGR and STRMNPS without any suffix - as before.
- **New TCP/IP Profile parameters on the GLOBALCONFIG statement:**
  - XCFGRPID tt - used to partition the TCP/IP Sysplex groups into subplexes
    - tt is a numeric value between 02 and 31
  - IQDVLANID nn - used to partition HiperSockets for Dynamic XCF connectivity into subplexes
    - nn is a numeric value between 1 and 4094
    - IQDVLANID support for HiperSockets requires a z890 GA2 or z990 GA2 hardware level.
  - These values cannot be modified through Vary Obeyfile processing
- **TCP/IP will join Sysplex group EZBTvvtt, where vv is the VTAM subplex number from above**
- **SWSA and Sysplexports structure names will be suffixed with vvtt - EZBDVIPAvvtt and EZBEPORTvvtt**
  - For example, if the TCP/IP GLOBALCONFIG specified an XCFGRPID of 05 and the supporting VTAM was started with XCFGRPID=23, this stack would connect to EZBEPORT2305

Replacing the dynamic DNS registration part of the DNS/WLM component with a dynamic DNS solution

Dynamic DNS registration when servers start and stop in the z/OS Sysplex

- **Automated Domain Name Registration (ADNR) component will use existing z/OS load balancing advisor infrastructure and appear to the load balancing advisor as an external load balancer**
  - Potentially possible to extend the dynamic registration capabilities to any SASP-server based implementation, such as a global EWLM manager.
    - The SASP protocol is defined in "Server/Application State Protocol v1", RFC 4678.
  - Registration/de-registration triggered by the same events that trigger when a server instance is available/not available from an external load balancer perspective.
  - LBA controls to quiesce and resume server instances also apply to SASP-DDNS.
  - Sysplex-wide scope.
- **Central Sysplex-wide definitions of which servers, server groups, and stacks to register under which names and in which name servers (DNS domains).**
  - Registration/de-registration driven by start/stop of the actual resources as reported by the LBA infrastructure.
- **The z/OS load balancing advisor may serve both the SASP ADNR registration component and external load balancers at the same time**



Even though ADNR connects to the z/OS LBA as a load-balancer, it doesn't do any load balancing (it ignores the weights that are returned from the z/OS LBA)

DNS can be on z/OS or any other platform that supports a BIND 8 or later name server

Central configuration file with information to identify which servers, server groups, host groups and individual hosts (TCP/IP stacks) to register dynamically.

- No requirements to have applications register themselves

OSA-Express2 segmentation offload configuration control via APAR PK21685 and PK26905

- **OSA-E2, 1 GbE (versus no segmentation offload):**

AWM Workload	Trans/Sec Delta %	CPU/Tran Delta %
RR 60	+ 1.3 %	- 0.7 %
CRR 9	+ 2 %	- 0.1 %
STR (1/20M):		
64K(send)/32K(recv)	Equal	- 28.9 %
180K(send)/64K(recv)	Equal	- 36.3 %
256K(send)/64K(recv)	Equal	- 39.2 %

- **OSA-E2, 10 GbE (versus no segmentation offload):**

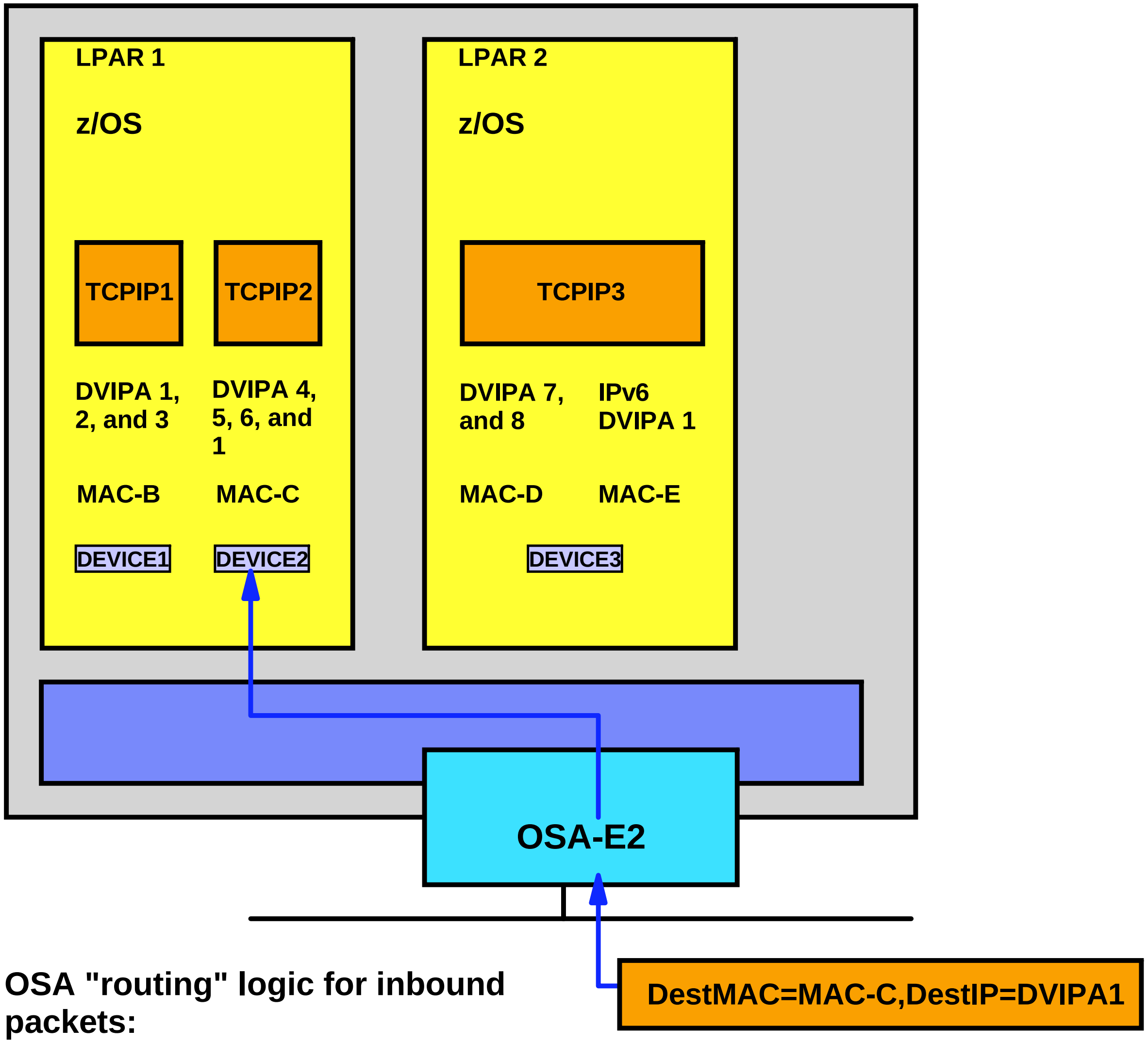
AWM Workload	Trans/Sec Delta %	CPU/Tran Delta %
RR 60	+ 1.7 %	- 2 %
CRR 60	+ 5.2 %	- 1 %
STR (1/20M):		
64K(send)/32K(recv)	+ 1.1 %	- 33.4 %
180K(send)/64K(recv)	+ 1.5 %	- 41.5 %
256K(send)/64K(recv)	+ 0.4 %	- 44.9 %

- **TCP segmentation offload with OSA-Express 2 on z890, z990, or System z9 provides attractive performance for outbound streaming workload (file transfer type of workload)**

- **Initially, support was implemented in TCP/IP to dynamically determine if the OSA microcode supported segmentation offload and, if so, then always enable it.**

- **APAR PK21685 (z/OS V1R6 and V1R7) and APAR PK26905 (z/OS V1R8) implement a GLOBALCONFIG option to specify if TCP/IP should or should not enable segmentation offload.**
  - GLOBALCONFIG [NO]SEGMENTATIONOFFLOAD

OSA Express2 virtual MAC addressing when operating in layer-3 mode - making a z/OS LPAR look like a "normal" TCP/IP host



OSA "routing" logic for inbound packets:

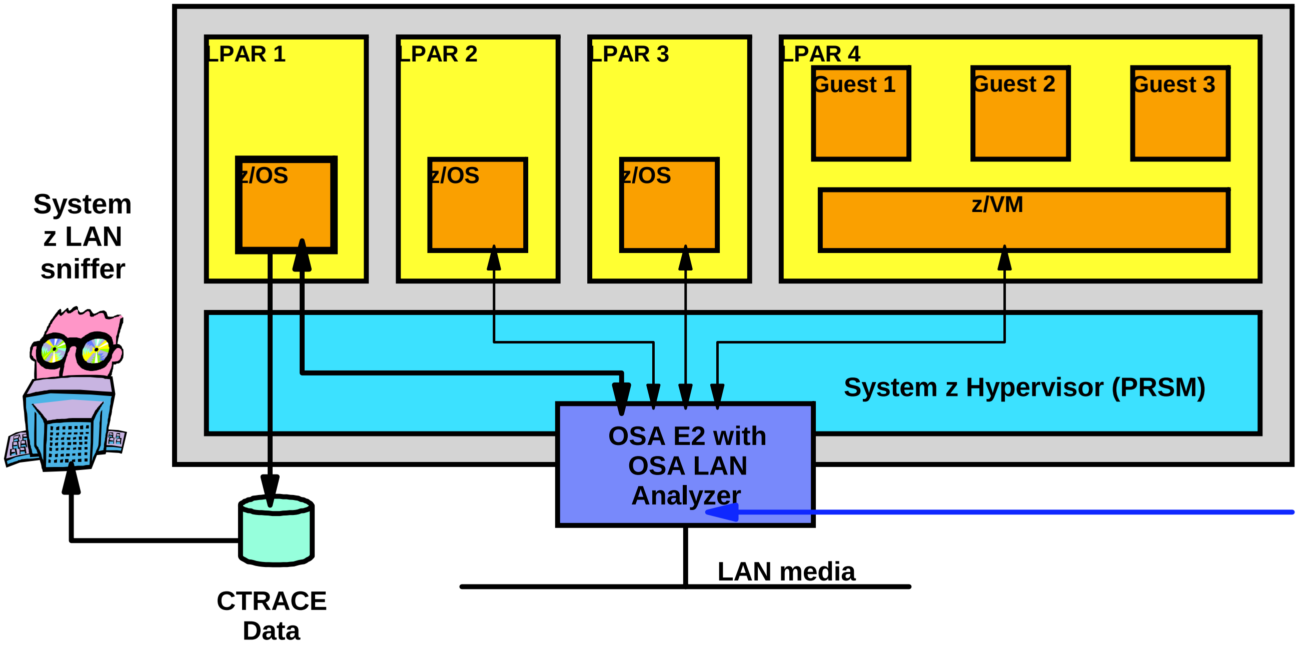
1. **Destination MAC address**
2. **VLAN ID**
3. **IPv4 or IPv6 address**

- **Enables first hop routers and load balancers to use dispatch mode (MAC-level) forwarding**
  - Avoids use of GRE
  - Enables use of dispatch mode by devices that do not support GRE (Cisco CSM and CSS)
  - Enables use of dispatch mode for IPv6 for which GRE isn't defined
  - Removes the need for using NAT instead of dispatch mode forwarding
    - NAT requires strict control of outbound path to handle NAT on outbound flows
- **Makes System z LPARs look more like "normal" TCP/IP nodes on a LAN**
  - Simplifies network infrastructure
  - Avoids the whole PRIROUTER/SECROUTER setup issue when sharing a port between multiple LPARs

OSA Express2 network traffic analyzer (NTA) overview

- **TCP/IP commands to enable an OSA Express Network Traffic Analyzer (OSAENTA) function**
  - New VARY TCPIP,,OSAENTA command
  - New OSAENTA TCP/IP profile statement
- **Filters to OSA to identify which data to capture**
  - LLC type, IP addresses, port, etc.
- **Let OSA capture the data using the LAN analyzer trace collection functions**
- **Transmit the captured trace data to TCP/IP over a QDIO data device**
- **TCP/IP will then save the trace data and provide tools that format the data using existing TCP/IP CTRACE facilities**
  - Trace data for packets to/from all LPARs that share the adapter is available

System z resident hardware LAN sniffer to enable LAN problem determination on the platform.

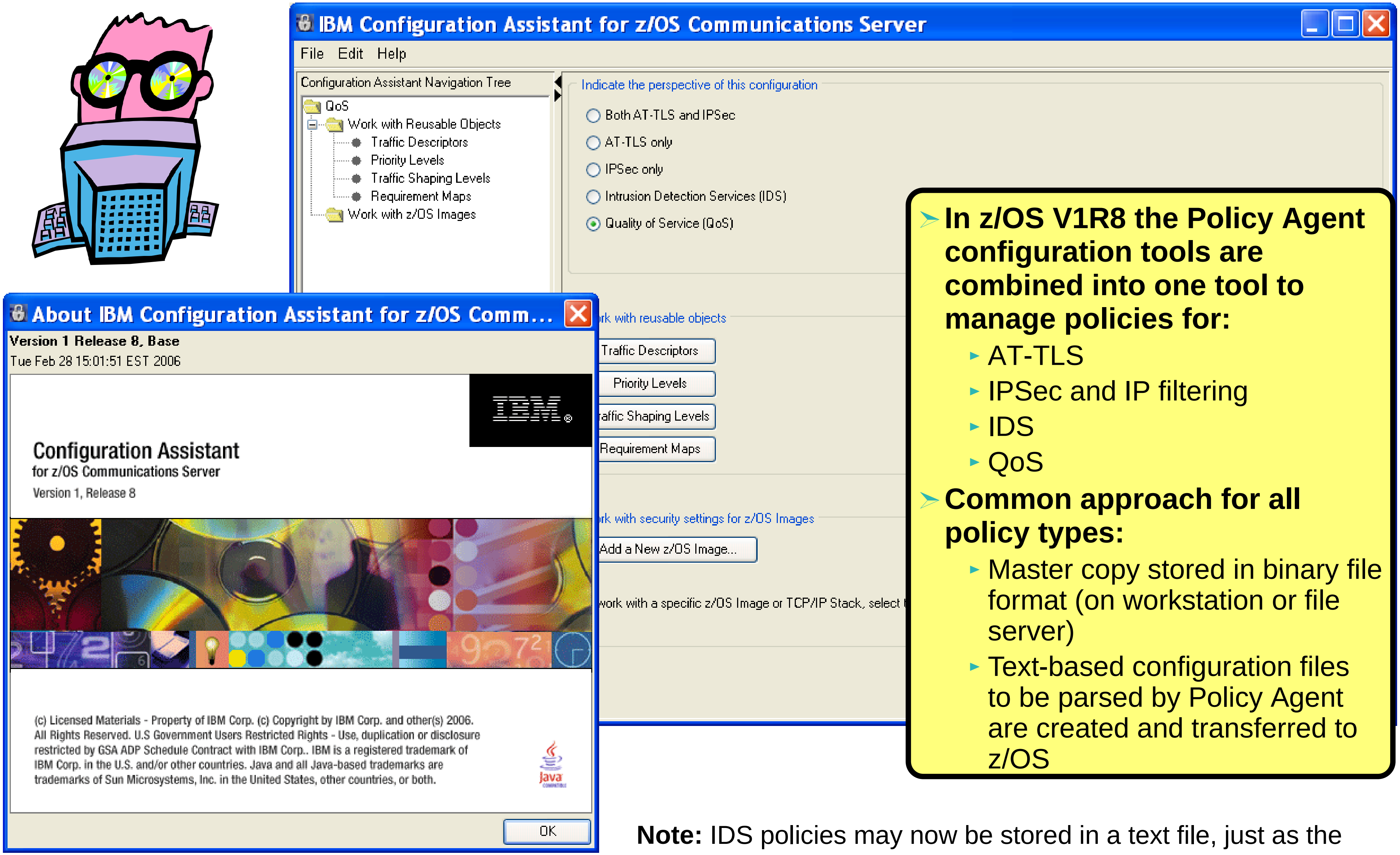


OSA LAN traffic analyzer captures packets as close as possible to the point of transmission to or receipt from the LAN.

- Functions similar to sniffer products, such as Ethereal

Network security - IDS usability, enhancing IPSec, removal of Firewall Technologies

IBM Configuration Assistant for z/OS Communications Server



Configuration Assistant Navigation Tree

- QoS
  - Work with Reusable Objects
    - Traffic Descriptors
    - Priority Levels
    - Traffic Shaping Levels
    - Requirement Maps
  - Work with z/OS Images

Indicate the perspective of this configuration

○ Both AT-TLS and IPSec

○ AT-TLS only

○ IPSec only

○ Intrusion Detection Services (IDS)

● Quality of Service (QoS)

rk with reusable objects

rk with security settings for z/OS Images

work with a specific z/OS Image or TCP/IP Stack, select

About IBM Configuration Assistant for z/OS Comm...

Version 1 Release 8, Base

Tue Feb 28 15:01:51 EST 2006

Configuration Assistant
for z/OS Communications Server
Version 1, Release 8

(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006. All Rights Reserved. U.S Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.. IBM is a registered trademark of IBM Corp. in the U.S. and/or other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

- **In z/OS V1R8 the Policy Agent configuration tools are combined into one tool to manage policies for:**
  - AT-TLS
  - IPSec and IP filtering
  - IDS
  - QoS
- **Common approach for all policy types:**
  - Master copy stored in binary file format (on workstation or file server)
  - Text-based configuration files to be parsed by Policy Agent are created and transferred to z/OS

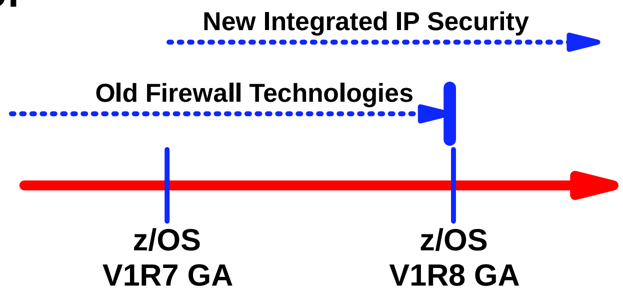
Note: IDS policies may now be stored in a text file, just as the other policy types. There is no requirement for LDAP.

Security standards update

- **AES - Advanced Encryption Standard**
  - AES is an official US. Government standard. The Secretary of Commerce approved the adoption of the AES as an official government standard, effective May 26, 2002
    - Federal Information Processing Standard
      - FIPS publication 197
  - AES is stronger than the Data Encryption Standard (DES) and therefore should be a popular standard both inside and outside the United States.
  - AES is a bulk encryption algorithm
    - Suitable for TLS and IPSec
    - More secure than DES (Data Encryption Standard)
- **Supported by System SSL element of z/OS since z/OS V1R4**
- **Support for use of AES was added to SSL-enabled CS components (TN3270, FTP, and Sendmail) and to Application Transparent TLS in z/OS V1R7**
- **z/OS V1R8 adds support of AES 128-bit encryption for IPSec workload**

z/OS IPSec and VPN support

- **New in z/OS V1R7, complete IPSec, filtering, and IKE solution part of z/OS Communications Server**
  - Alternative to Firewall Technologies
- **z/OS Communications Server IPSec features**
  - Simplified configuration, infrastructure, administrative controls
  - Improved serviceability, messages
  - Base for enhancements - NAT traversal, IPv6, etc.
- **Starting in z/OS V1R8, Firewall Technologies is no longer available**



- **Announced Feb 15th, 2005**
  - z/OS V1.7 is the last z/OS release to include the Firewall Technologies component of the Integrated Security Services element.
  - Many Firewall Technologies functions have been stabilized for some time and can be replaced using comparable or better functions provided by or planned for Communications Server, notably,
    - IPSec
    - IP packet filtering
    - In addition, a functionally rich downloadable tool is planned to replace the IP Security and IP Filtering configuration GUI support.
  - The following functions will be removed without replacement:
    - FTP Proxy services
    - Socks V4 services
    - Network Address Translation (NAT)
    - RealAudio support

Migrating from Firewall Technologies to z/OS Communications Server IP Security:

- **http://www.ibm.com/support/docview.wss?rs=852&context=SSSN3L&dc=DA400&uid=swg27008603&loc=en_US&cs=UTF-8&lang=en&rss=ct852other**

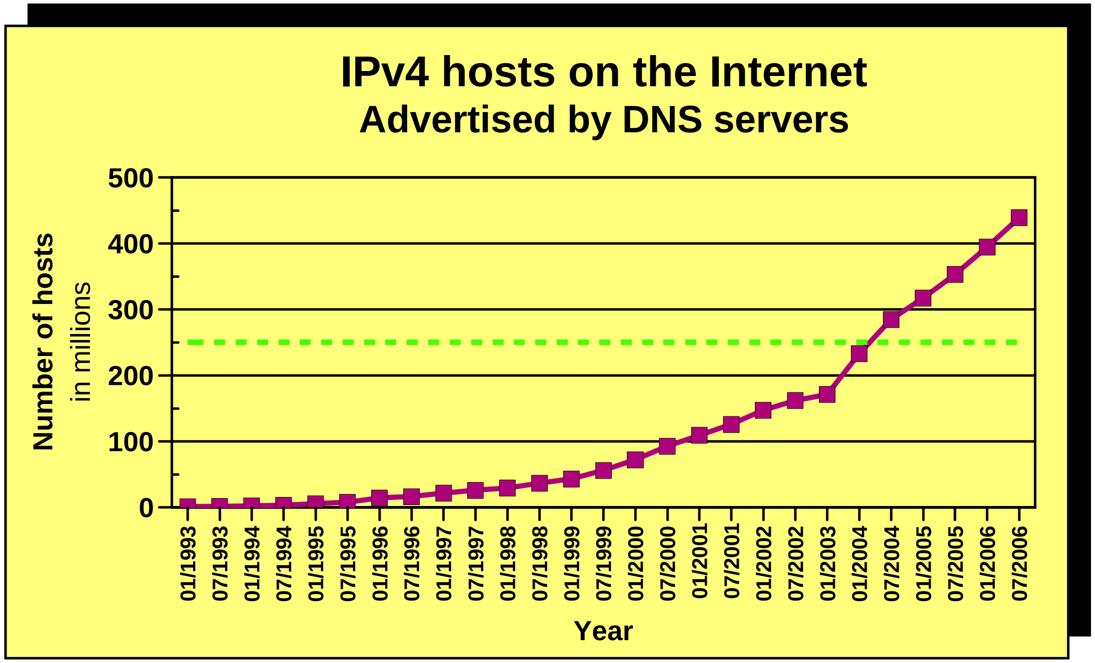
IPv6 support - extending integrated IP Security to IPv6 workloads

Extending integrated IP Security functions to include IPv6 traffic

- **z/OS V1R5 and V1R6 have both been IPv6 Ready Logo Phase-1 certified**
- **IPv6 Ready Logo Phase-2 has now been defined and the main addition is required support for IPv6 IP Security (IPSec)**
  - Standard requirement for all IPv6 platforms
  - Replace application-specific security, such as OSPFv3
  - Opportunity for end-to-end IPSec security between all IPv6 hosts

Phase-1

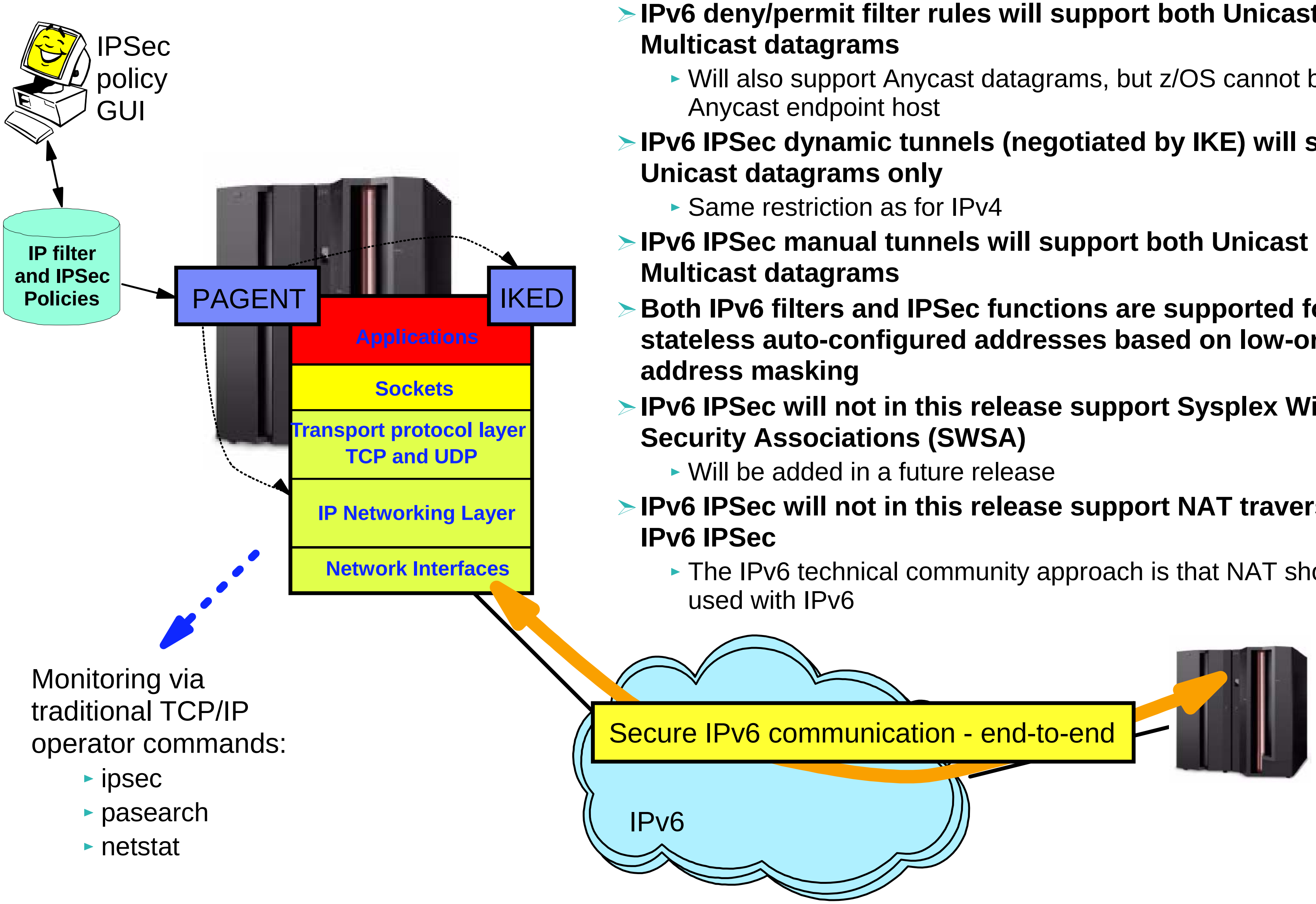
Phase-2



- **Source: http://www.isc.org/index.pl?/ops/ds**

- **z/OS V1R7 re-implemented IPSec support for IPv4:**
  - Fully integrated into Communications Server
  - IP filtering
  - Static IPSec tunnels
  - Dynamic IPSec tunnels (IKE)
  - IPv4 NAT traversal support
  - Simplified configuration and operation
  - Improved scalability and performance
- **z/OS V1R8 extends IPSec support to IPv6**

IPv6 IPSec support details


IPSec policy GUI
IP filter and IPSec Policies
PAGENT
IKED
Applications
Sockets
Transport protocol layer TCP and UDP
IP Networking Layer
Network Interfaces
Secure IPv6 communication - end-to-end
IPv6

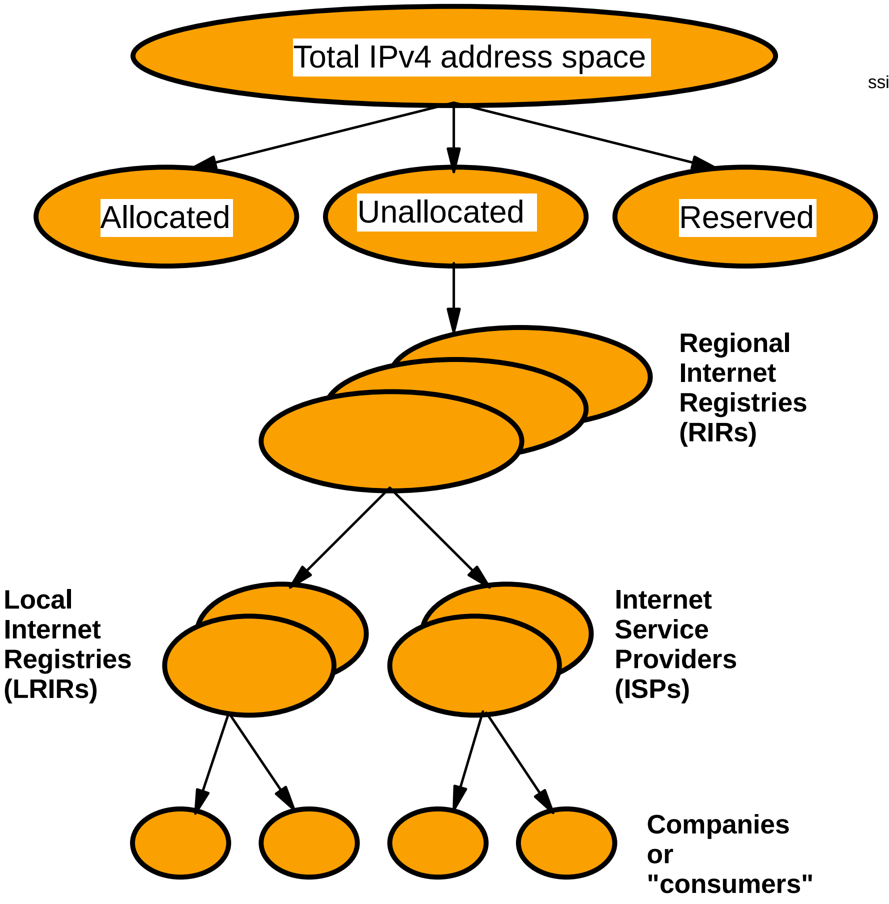
- **IPv6 deny/permit filter rules will support both Unicast and Multicast datagrams**
  - Will also support Anycast datagrams, but z/OS cannot be an Anycast endpoint host
- **IPv6 IPSec dynamic tunnels (negotiated by IKE) will support Unicast datagrams only**
  - Same restriction as for IPv4
- **IPv6 IPSec manual tunnels will support both Unicast and Multicast datagrams**
- **Both IPv6 filters and IPSec functions are supported for stateless auto-configured addresses based on low-order address masking**
- **IPv6 IPSec will not in this release support Sysplex Wide Security Associations (SWSA)**
  - Will be added in a future release
- **IPv6 IPSec will not in this release support NAT traversal for IPv6 IPSec**
  - The IPv6 technical community approach is that NAT should not be used with IPv6

Monitoring via traditional TCP/IP operator commands:

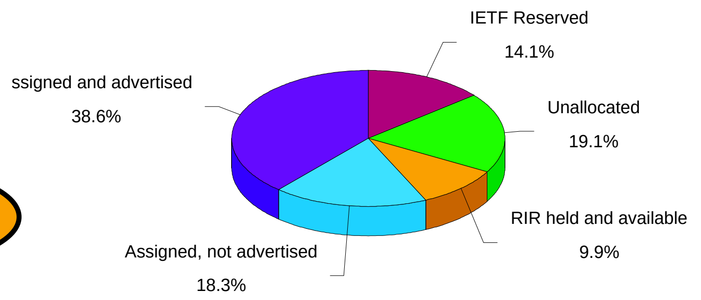
- ipsec
- pasearch
- netstat

IPv4 address space data as of January 2007

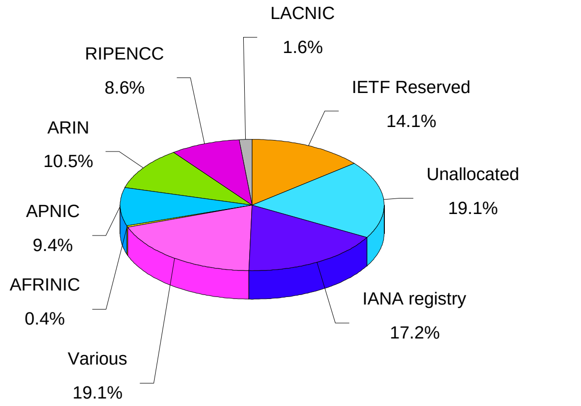
How the IPv4 address space is managed:


Total IPv4 address space
Allocated
Unallocated
Reserved
Regional Internet Registries (RIRs)
Local Internet Registries (LRIRs)
Internet Service Providers (ISPs)
Companies or "consumers"

IPv4 Address Space



IPv4 Address Space by RIR



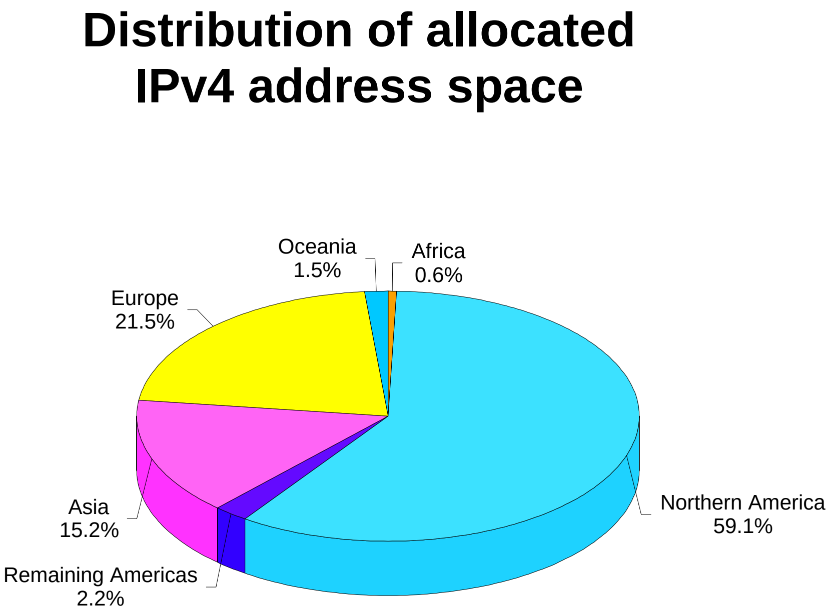
The most current predictions estimate that the unallocated pool will be exhausted around 2011/2012.

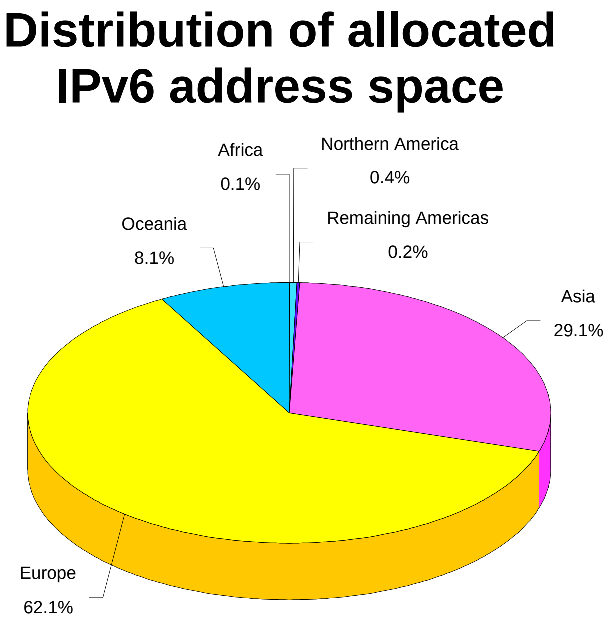
Some of the assigned but not advertised space may potentially be reused to prolong the life of IPv4.

RIR: Regional Internet Registry
IANA Registry: Space assigned directly by IANA (before regional registries were introduced)
Various: Space allocated to various registries (before regional registries were introduced)
AFRINIC: Africa, portions of the Indian Ocean
APNIC: Portions of Asia, portions of Oceania (includes Australia, China, India)
ARIN: Canada, United States, islands in the Caribbean Sea and North Atlantic Ocean
RIPENCC: Europe, the Middle East, Central Asia
LACNIC: Latin America, portions of the Caribbean

Source: "IPv4 Address Report" - http://www.potaroo.net/tools/ipv4/

Which geography use the allocated IP addresses as of January 2007?





It is clearly Northern America that managed to grab IPv4 addresses

And it is clearly Europe, Asia, and Oceania that lead the migration to IPv6

Source: "IPv4 Address Report" - http://www.potaroo.net/tools/ipv4/

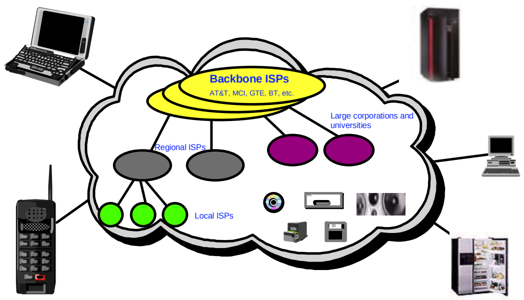
The Journey to IPv6 for z/OS Communications Server

- **The first phase (z/OS V1R4)**
  - Stack support for IPv6 base functions - (APIs, Protocol layers)
  - Resolver
  - High speed attach (OSA Express QDIO))
  - Service tools (Trace, Dump, etc.)
  - Configuration and netstat, ping, traceroute, SMF
  - Static Routing
  - FTP, otelnetd, UNIX rexec, UNIX rshd/rexecd
- **The second phase (z/OS V1R5)**
  - Network Management
    - Applications and DPI
    - Version-neutral TCP/IP Standard MIBs
    - Additional SMF records
  - Applications/Clients/APIs
    - TN3270 server, CICS sockets, Sendmail, ntp, dcas, rxserve, rsh client
  - Enterprise Extender
  - Point to Point - type DLCS
  - Dynamic Routing Protocol w/ OMPROUTE (only RIPng)
- **The third phase (z/OS V1R6)**
  - Sysplex Exploitation (Dynamic VIPA, Sysplex Distributor functions)
  - Dynamic Routing Protocol w/ OMPROUTE (OSPFv3)
  - Additional Network Management MIBs
- **The fourth phase (z/OS V1R7)**
  - SNMP UDP standard MIB (RFC2013) and IBM MVS TCP/IP Enterprise-specific MIB for UDP
  - Advanced Socket API support - RFC3542
  - IPv6 Two Default Routers - required for IPv6 compliance
  - HiperSockets
- **The fifth phase (z/OS V1R8)**
  - Integrated IPSec for IPv6
  - RPCBIND (RPC over IPv6)
- **After z/OS V1R8**
  - Complete Advanced Socket APIs
  - Extended Stats MIB, OSPFv3 MIB
  - Intrusion Detection Services
  - IPv6 mobility support
  - FRCA support for IPv6

Latest predictions talk about running out of IPv4 addresses in the 2011/2012 time frame.

Objective is to have IPv6 production ready on the platform when you need it!

The Internet - a worldwide digital utility.



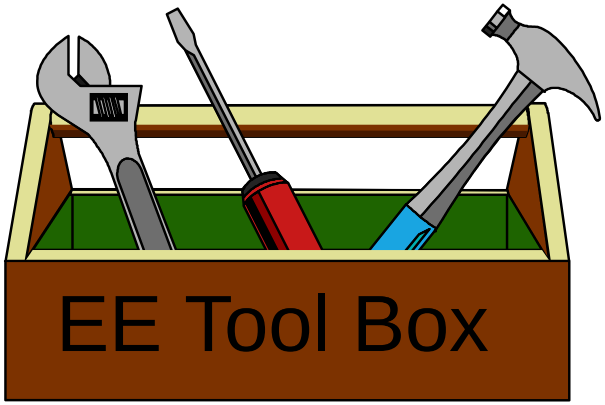
Connectivity for ***anyone*** from ***anywhere*** (car, home, office) to ***anything***!

EE/SNA - improved operations

Enterprise Extender Connectivity Test Command

- **The Enterprise Extender connectivity test command is useful in debugging various network problems. This command can be used to test an existing Enterprise Extender connection, or it can be used to assist in diagnosing why an EE connection cannot be established.**

- **The EE connectivity test will verify:**
  - EE line availability
  - Address resolution capability
  - EE partner reachability
    - UDP requests with varying TTL (time-to-live) or hop count values are sent to the EE partner host
    - The command then waits for the routers between the local and remote hosts to send TTL-exceeded messages.
      - In the case where TTL-exceeded message are not received, the command allows for maximum number of retry attempts for that particular hop in the route.
    - The output generated from this request will show the reachability to the remote EE endpoint over all five UDP ports reserved for EE.
    - When MULTIPATH function is enabled in the Enterprise Extender capable TCP/IP stack, the EE connectivity test is repeated for each valid TCP/IP interface which routes EE traffic.



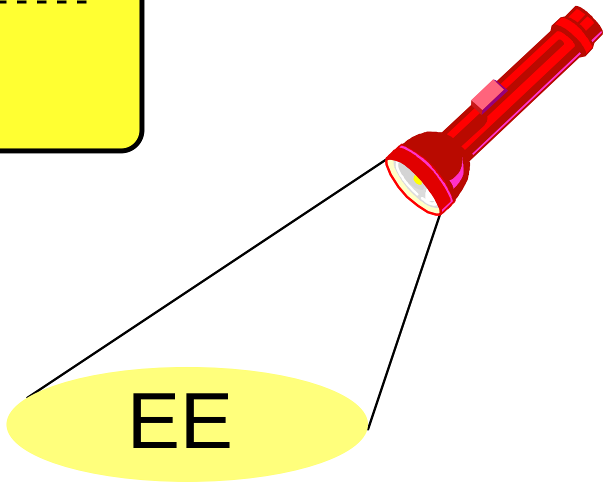
Enterprise Extender Connectivity Test Command...

```
D NET,EEDIAG,TEST=YES,IPADDR=(10.81.1.1,10.81.2.2),LIST=DETAIL
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = EEDIAG
IST2119I ENTERPRISE EXTENDER DISPLAY CORRELATOR:  EE00001C
IST2067I EEDIAG DISPLAY ISSUED ON 09/22/05 AT 14:54:20
IST1680I LOCAL IP ADDRESS 10.81.1.1
IST1680I REMOTE IP ADDRESS 10.81.2.2
IST2023I CONNECTED TO LINE LNEE4001
IST2126I CONNECTIVITY TEST IN PROGRESS
IST314I END
IST350I DISPLAY TYPE = EEDIAG
IST2119I ENTERPRISE EXTENDER DISPLAY CORRELATOR: EE00001C
IST2131I EEDIAG DISPLAY COMPLETED ON 09/22/05 AT 14:54:21
IST2132I LDLC PROBE VERSIONS: VTAM = V1           PARTNER = UNKNOWN
IST1680I LOCAL IP ADDRESS 10.81.1.1
IST1680I REMOTE IP ADDRESS 10.81.2.2
IST924I -------------------------------------------------------------
IST2133I INTFNAME: MPC4121L                INTFTYPE: MPCPTP
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12000
IST2137I     1  10.81.2.2                   RTT:     2
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12001
IST2137I     1  10.81.2.2                   RTT:     4
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12002
IST2137I     1  10.81.2.2                   RTT:     4
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12003
IST2137I     1  10.81.2.2                   RTT:     4
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12004
IST2137I     1  10.81.2.2                   RTT:     4
  ...
```

Enterprise Extender Connectivity Test Command...

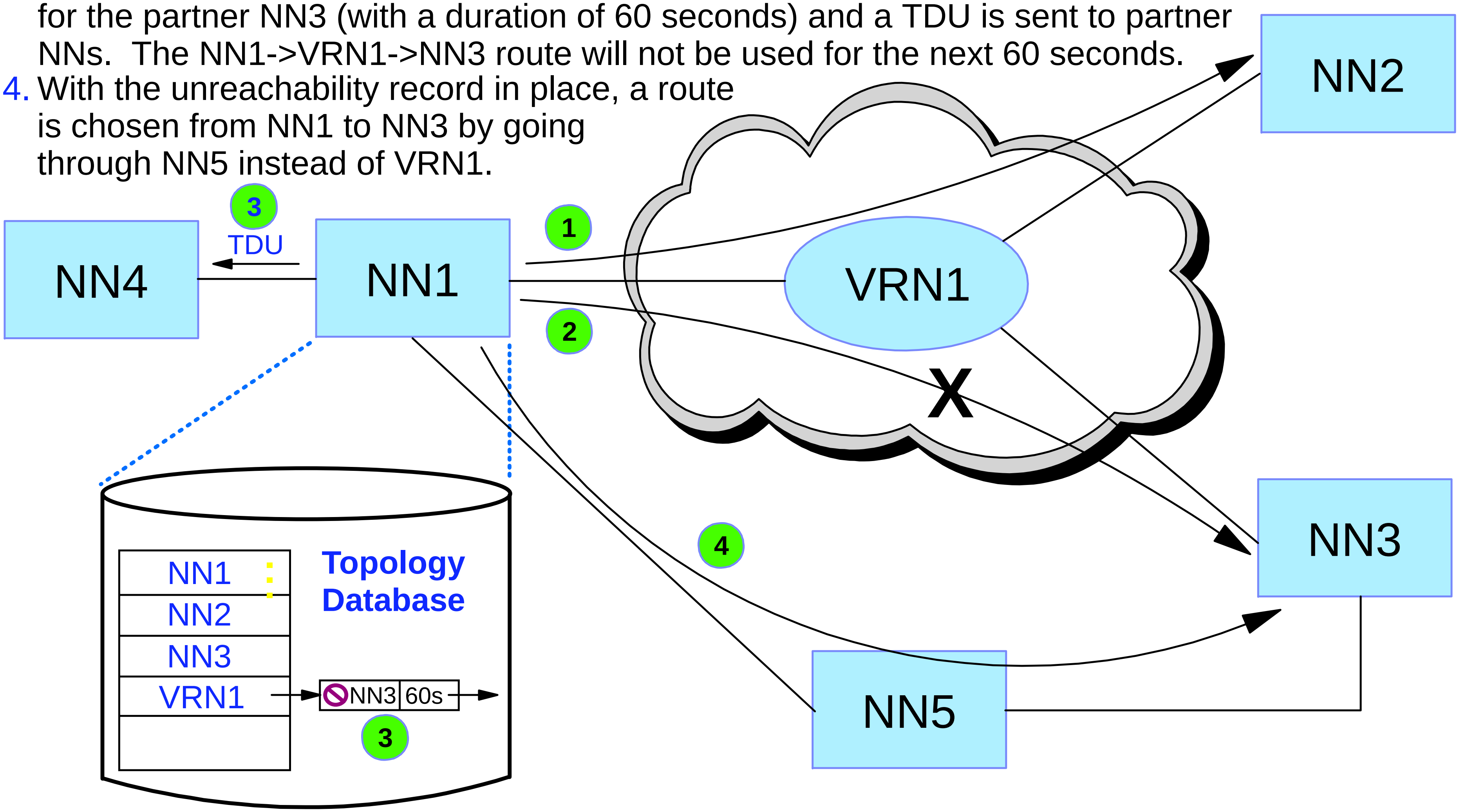
```
 ...

IST924I -------------------------------------------------------------
IST2133I INTFNAME: MPC4221L                INTFTYPE: MPCPTP
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12000
IST2137I     1  10.81.2.2                   RTT:     3
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12001
IST2137I     1  10.81.2.2                   RTT:     3
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12002
IST2137I     1  10.81.2.2                   RTT:     3
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12003
IST2137I     1  10.81.2.2                   RTT:     3
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12004
IST2137I     1  10.81.2.2                   RTT:     3
IST924I -------------------------------------------------------------
IST2139I CONNECTIVITY TEST RESULTS DISPLAYED FOR 2 INTERFACES
IST314I END
```



EE Connection Network Reachability Awareness (V1R6)

1. NN1 successfully contacts NN2 across VRN1.
2. NN1's attempt to contact NN3 across VRN1 fails.
3. In NN1's topology database, an "unreachability record" is associated with VRN1 for the partner NN3 (with a duration of 60 seconds) and a TDU is sent to partner NNs. The NN1->VRN1->NN3 route will not be used for the next 60 seconds.
4. With the unreachability record in place, a route is chosen from NN1 to NN3 by going through NN5 instead of VRN1.



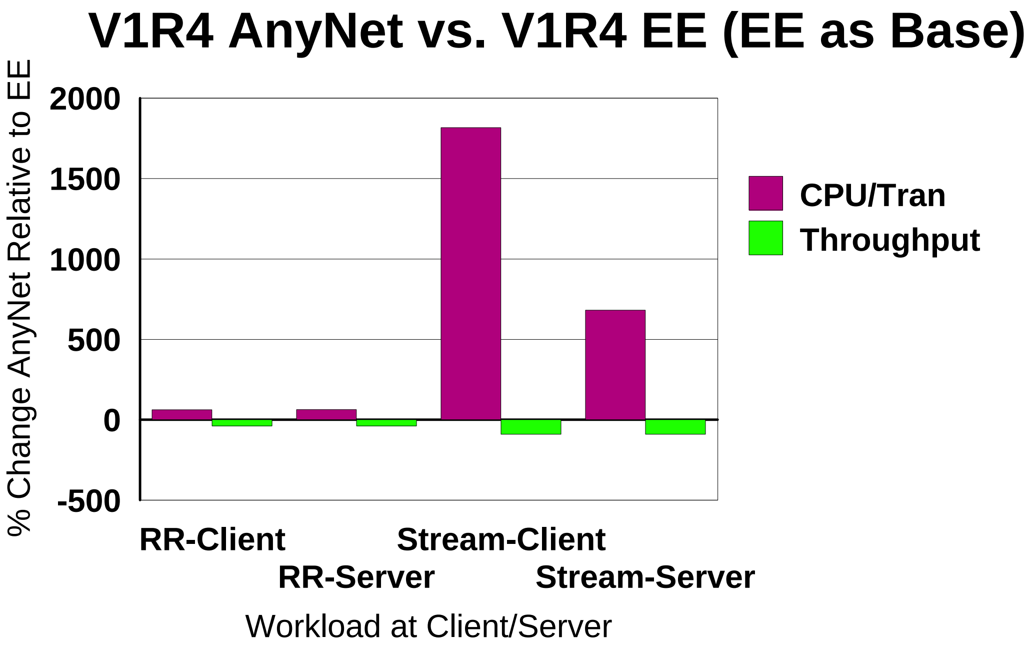
Connection Network Reachability Awareness Enhancements

- **In V1R8, the maintenance of unreachable partner information is centralized under the virtual routing node records. (Prior to V1R8, unreachable partner information associated with end nodes was associated with end node records.) This centralization allows for improvements in serviceabilty and usability. In particular:**
  - DISPLAY TOPO, LIST=UNRCHTIM now uses a VRN= operand instead of the ID operand (that previously specified either a VRN or EN name, sometimes requiring the issuance of multiple display commands to retrieve the full set of unreachable partner information).
  - DISPLAY TOPO, LIST=UNRCHTIM now allows ORIG and DEST operands for additional granularity
  - MODIFY TOPO,FUNCTION=CLRUNRCH provides similar improvements, including the VRN operand, and support for ORIG and DEST operands.

```
d net,topo,list=unrchtim,orig=neta.sscp1a,vrn=vrn1
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = TOPOLOGY
IST2057I UNREACHABLE PARTNER INFORMATION:
IST924I -------------------------------------------------------------
IST2051I VIRTUAL NODE NETA.VRN1 - 6 UNREACHABLE PARTNERS
IST2052I   ORIGIN NODE        PARTNER NODE    UNRCHTIM  EXPIRES
IST2055I NETA.SSCP1A        NETA.SSCPAA          300S   00:15:42
IST2055I NETA.SSCP1A        NETWORKB.SSCP7B       45S   23:18:19
IST924I -------------------------------------------------------------
IST314I END
```

Removal of AnyNet

- **Enterprise Extender, TN3270, and distributed Communications Server Remote API functions are the strategic protocols for SNA/IP integration**
  - AnyNet has not been enhanced in years
- **EE is functionally superior, but also significantly outperforms AnyNet by all measures:**
  - AnyNet exhibits lower throughput and higher CPU utilization relative to EE:
    - Interactive workloads
      - Throughput down 39%
      - CPU utilization up 63%
    - Stream workloads
      - Throughput down 89%
      - CPU utilization up 682-1817%



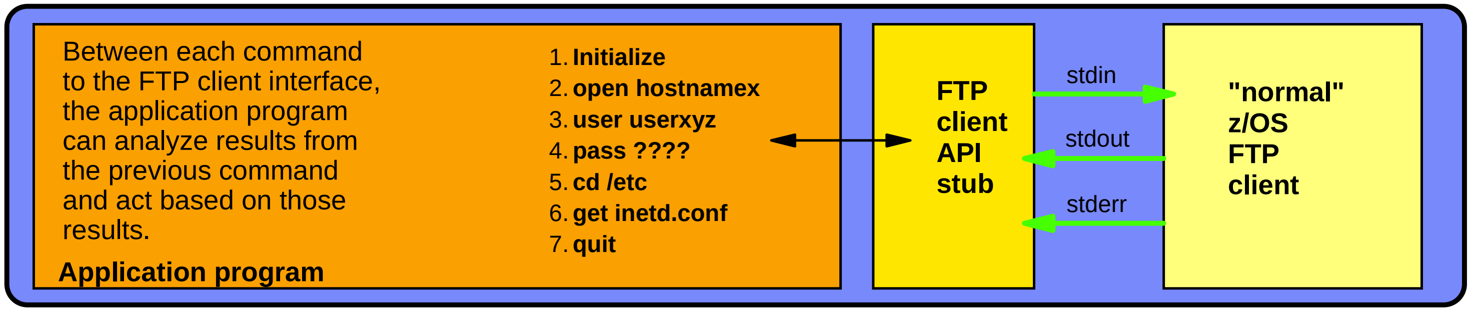
- **As of z/OS V1R8, AnyNet will no longer be included as a component of Communications Server**

FTP and TN3270 - usability and management

FTP client API in REXX

- **z/OS V1R6 provided the initial callable FTP client programming interface**
  - This initial version was provided as a callable program interface to be used from Assembler, Cobol, or PL/I application programs
- **z/OS V1R7 extends that FTP client programming interface with a C library interface**
  - To be used by C or C++ application programmers
- **z/OS V1R8 will further extend the FTP client programming interface support by providing a REXX API**
  - To be used by REXX application programmers

```
/* Create FTP client control information     */
if ftp('create','fcai.', TRACEID) < 0 then do
   Say 'Unable to create the FCAI'
   exit
end
/* Enable trace                              */
if ftp('fcai.', 'set_trace', 'ON') < 0 then do
   call ftp_error 'fcai.'
end
/* Open a connection                         */
if ftp('fcai.', 'init', OPENSTRING, VAR1, VAR2) then do
   call ftp_error 'fcai.'
end
/* Send USER command                         */
if ftp('fcai.', 'scmd', USER_COMMAND, 'W') < 0 then do
   call ftp_error 'fcai.'
end
/* Send password                             */
if ftp('fcai.', 'scmd', PASS_COMMAND, 'W') < 0 then do
   call ftp_error 'fcai.'
end
```



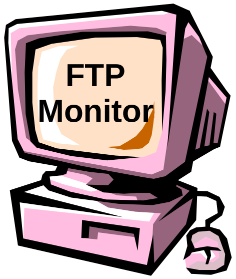
Between each command to the FTP client interface, the application program can analyze results from the previous command and act based on those results.

1. **Initialize**
2. **open hostnamex**
3. **user userxyz**
4. **pass ????**
5. **cd /etc**
6. **get inetd.conf**
7. **quit**

Significantly improved automation capabilities for file transfer operations that are initiated on z/OS

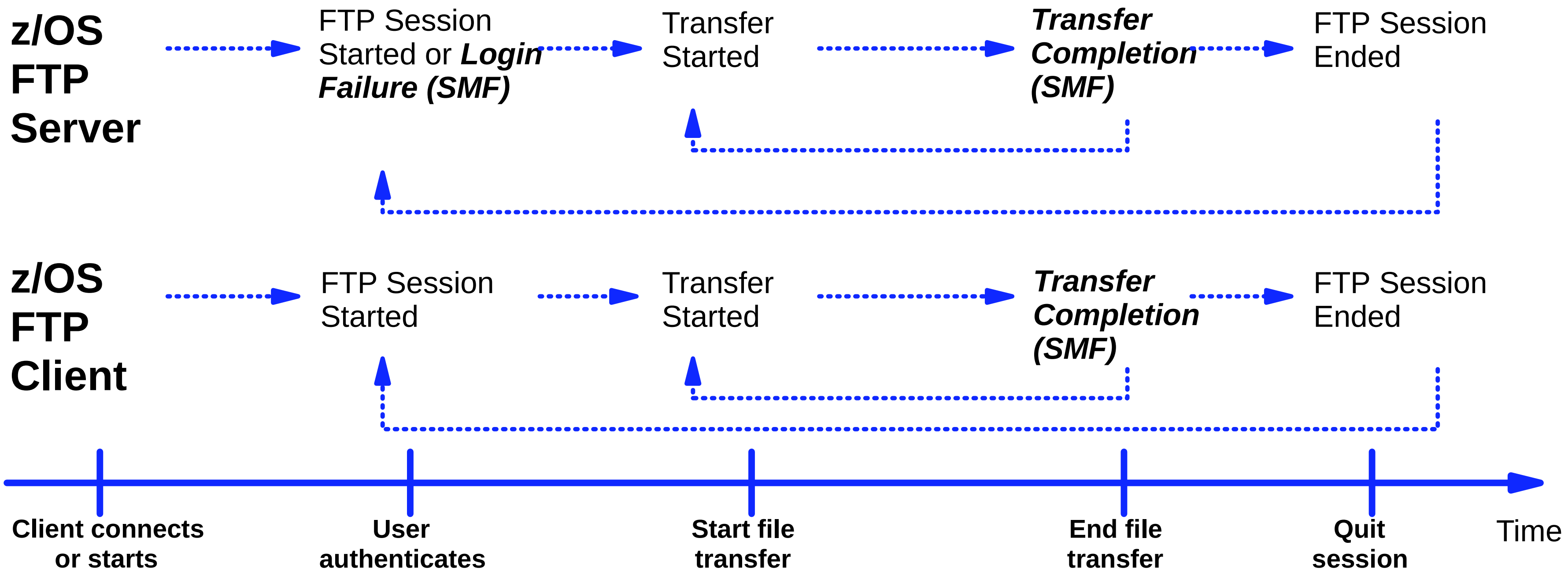
Enhanced real-time FTP monitoring capabilities through new NMI application event reporting

- **Which FTP client or server sessions are currently active?**
- **Which FTP server sessions did USERXYZ have during the last two hours?**
- **Which file transfers did not complete successfully since last night?**
- **For active file transfers, status monitoring is possible by combining information from other NMI real-time interfaces to query transfer progress**



Real-time z/OS FTP activity monitor (such as OMEGAMON XE)

Network Management Interface (NMI) - Application Event Monitoring



z/OS FTP Server

FTP Session Started or ***Login Failure (SMF)***

Transfer Started

Transfer Completion (SMF)

FTP Session Ended

z/OS FTP Client

FTP Session Started

Transfer Started

Transfer Completion (SMF)

FTP Session Ended

Client connects or starts

User authenticates

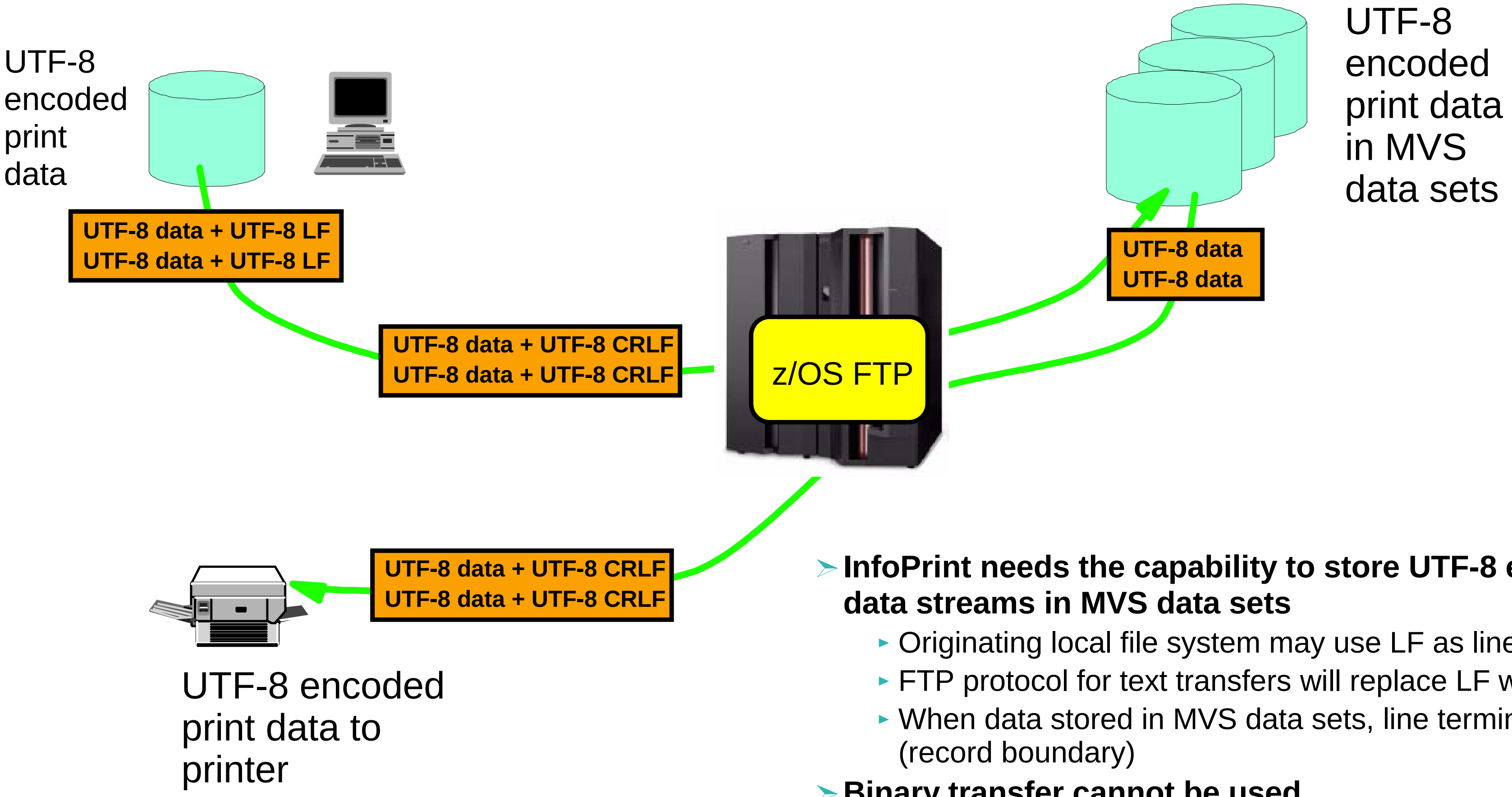
Start file transfer

End file transfer

Quit session

Time

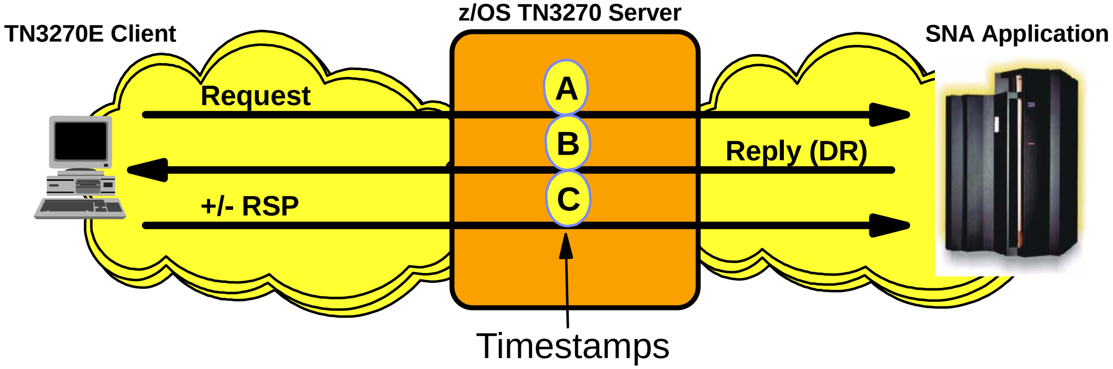
FTP support of UTF-8 encoded InfoPrint print data sets



- **InfoPrint needs the capability to store UTF-8 encoded print data streams in MVS data sets**
  - Originating local file system may use LF as line termination
  - FTP protocol for text transfers will replace LF with CRLF
  - When data stored in MVS data sets, line termination is implicit (record boundary)
- **Binary transfer cannot be used**
  - Would preserve the LF character in the MVS data set
- **Traditional text transfer cannot be used either**
  - Would require unwanted code page conversion
- **New specific UNICODE support is needed:**
  - Apply text transfer processing in terms of line termination handling
  - Process data as-is (without code page conversion)

- **z/OS FTP still needs a few modifications to fully support all UNICODE code pages and conversions**
  - To be addressed in future release

TN3270 response time monitor results via the NMI interface and via SMF recording



Response times

```
Round-trip time = Time C - Time A
IP time         = Time C - Time B
SNA time        = Round trip time -
                  IP time
```

Life-of-connection data for life-of-connection averages

- Transaction count
- Round trip & IP response time totals
- Averages for round trip, IP, and SNA response times

Life-of-SNA session data for life-of-SNA session averages *(to be added in z/OS V1R8)*

- Transaction count
- Round trip & IP response time totals
- Averages for round trip, IP, and SNA response times

Sliding window data for sliding window averages

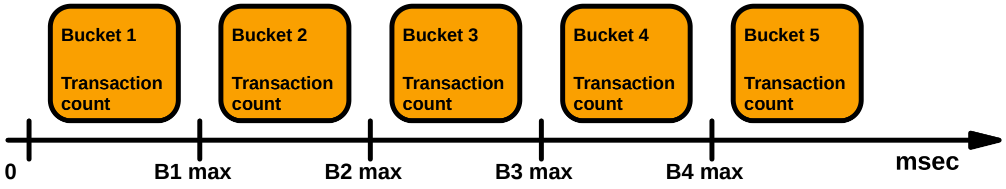
- Period transaction count
- Period round trip & IP response time totals
- Sliding window transaction count
- Sliding window round trip & IP response time totals

Sum of squares for variance and standard deviation

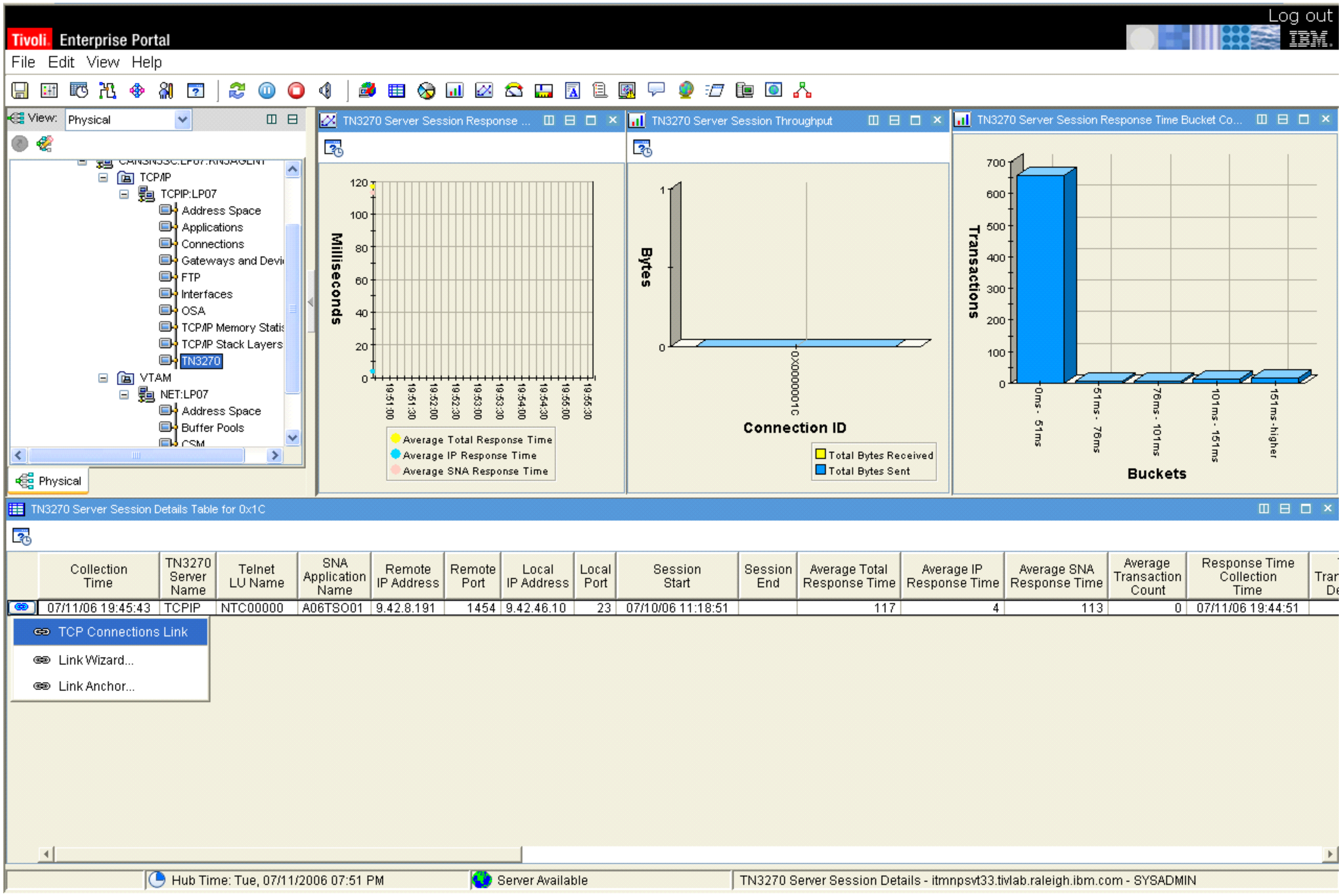
- Round trip, IP, and SNA sum of squares

Round trip response time counts by time bucket

- **Reporting:**
  - z/OS V1R5
    - Reporting via SNMP MIB data
    - Reporting via MVS console display commands
  - z/OS V1R8 to add
    - Real-time reporting via the Network Management Interface
      - SNA session termination event
      - OMEGAMON XE for Mainframe Networks Version 4.1 uses this support.
    - Reporting via TN3270 server SMF records
      - SNA session termination record (subtype 21)



OMEGAMON XE for Mainframe Networks - TN3270 detail response time data



	Collection Time	TN3270 Server Name	Telnet LU Name	SNA Application Name	Remote IP Address	Remote Port	Local IP Address	Local Port	Session Start	Session End	Average Total Response Time	Average IP Response Time	Average SNA Response Time	Average Transaction Count	Response Time Collection Time	Trar De
	07/11/06 19:45:43	TCPIP	NTC00000	A06TSO01	9.42.8.191	1454	9.42.46.10	23	07/10/06 11:18:51		117	4	113	0	07/11/06 19:44:51	

Hub Time: Tue, 07/11/2006 07:51 PM

Server Available

TN3270 Server Session Details - itmnpsvt33.tivlab.raleigh.ibm.com - SYSADMIN

TN3270 server enhancements

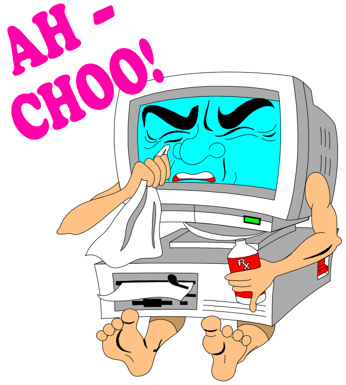
- **Improved recovery when a client is running multiple TN3270 sessions**
  - If the z/OS CS TN3270 server receives a new connection from a client IP address that already has one or more existing connections, the server will "poke" the existing connections to make sure they are still up.
  - If not, they will be cleaned up immediately
  - This improves the case where a client has TN3270 sessions which go down, so he starts a new session and reconnects.
    - helps avoid the "connect connect, already connected" error scenario
- **Support for MVS system symbolics in the USS message table**
  - for example, would enable the USS logon screen to report which LPAR is serving the client.
- **Allow the LU Exit to specify the USS table and/or Interpret table names**
- **Support removed for obsolete statements:**
  - QUEUESESSION statement no longer supported
    - Use QSESSion parameter on the RESTRICTAPPL or ALLOWAPPL statement instead
  - LUSESSIONPEND, MSG07, TELNETDEVICE statements no longer supported in the BEGINVTAM block
    - Code statement in TelnetGlobals, TelnetParms, or ParmsGroup instead

Various TCP/IP changes

Communications Server initial support for the z/OS health-checker

- **CS z/OS will in this release implement its initial support for the IBM Health Checker for z/OS and Sysplex component.**

- **Initial focus will be on the Communications Server health checker infrastructure and a few selected configuration options that are known to have caused problems in the past:**
  - The default size of the TCP receive buffer size (the TCPMAXRCVBUFRSIZE option in the TCP/IP Profile)
  - The default set of options for CTRACE
  - Maximum amount of fixed CSM storage (the MAXFIX option in IVTPRMxx)
  - Maximum amount of ECSA CSM storage (the MAXECSA option in IVTPRMxx)



Various network management enhancements

- **EE NMI selection filter enhancements**
  - Support wild card names on the CP name filter

- **Connection termination reason code in TCP connection termination SMF record**
  - Request from various network management vendors to have the exact TCP connection termination reason code recorded in the TCP connection termination SMF record
  - There are many reasons why a TCP connection may be terminated - apart from normal termination

- **Ability to drop socket endpoint through the NMI interface**
  - Function similar to the current netstat command interface to drop a connection endpoint
  - Will require that the NMI process userID is permitted to the MVS.VARY.TCPIP.DROP SAF resource

Better tracking of DVIPA creation and deletion

- **Netstat VDPT display enhancements for current number of active connections**

- **Issue MVS console messages with more details when application-specific DVIPAs are created or deleted**

```
EZD1204I - DYNAMIC VIPA dvipa WAS CREATED USING IOCTL BY jobname ON tcpstackname
EZD1205I - DYNAMIC VIPA dvipa WAS CREATED USING BIND BY jobname ON tcpstackname
EZD1206I - DYNAMIC VIPA dvipa WAS DELETED USING IOCTL BY jobname ON tcpstackname
EZD1207I - DYNAMIC VIPA dvipa WAS DELETED USING CLOSE BY jobname ON tcpstackname
```

- **Include additional information regarding the creation of a DVIPA in the** *netstat vipadyn* **report:**

```
MVS TCP/IP NETSTAT CS V1R8       TCPIP Name: TCPCS           18:28:50
Dynamic VIPA:
  IP Address      AddressMask     Status    Origination     DistStat
  ----------      -----------     ------    -----------     --------
  201.2.10.11     255.255.255.192 Active    VIPADefine      Dist
    ActTime:      03/02/2005 16:45:20
  201.2.10.12     255.255.255.192 Active    VIPADefine      Dist/Dest
    ActTime:      03/02/2005 16:45:20
  201.2.10.14     255.255.255.192 Backup    VIPABackup
    ActTime:      n/a
  201.2.10.32     <None>          Backup    VIPABackup
    ActTime:      n/a
  199.199.199.8   255.255.255.0   ACTIVE    VIPARANGE IOCTL
    ActTime:      03/02/2005 16:45:20       JobName:        JOBTST1A
  199.199.199.9   255.255.255.0   ACTIVE    VIPARANGE BIND
    ActTime:      03/02/2005 16:45:20       JobName:        JOBTST1B
```

Additional netstat command enhancements

- **Various Netstat enhancements**
  - Enhanced ability to select only the listening socket of a server with many active connections - netstat all and netstat conn reports
    - New modifier called SERVER
  - Add information about autolog configuration to the existing netstat config report

```
Autolog Configuration Information:     Wait time 5
Proc Name: xxxxxxxxx  Job Name: yyyyyyyy
  Parmstring: zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
              zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
```

  - Add new ipaddress+port selection filter to connection-oriented netstat reports
    - IPPORT filter: ipaddress+port
  - Add new modifier to the netstat slap report to select only active policies
    - New modifier called ACTIVE

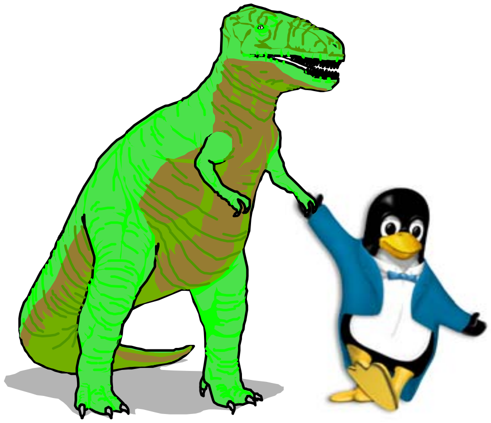
Retired TCP/IP Profile parameters

- **Support for the ASSORTEDPARMS and KEEPALIVEOPTIONS statements in the TCP/IP profile has been removed.**
- **These statements have been deprecated since z/OS V1R2 with warning messages issued.**
- **The parameters on these statements have equivalent parameters on the GLOBALCONFIG, IPCONFIG, IPCONFIG6, TCPCONFIG, and UDPCONFIG statements.**

Linux Message Integration

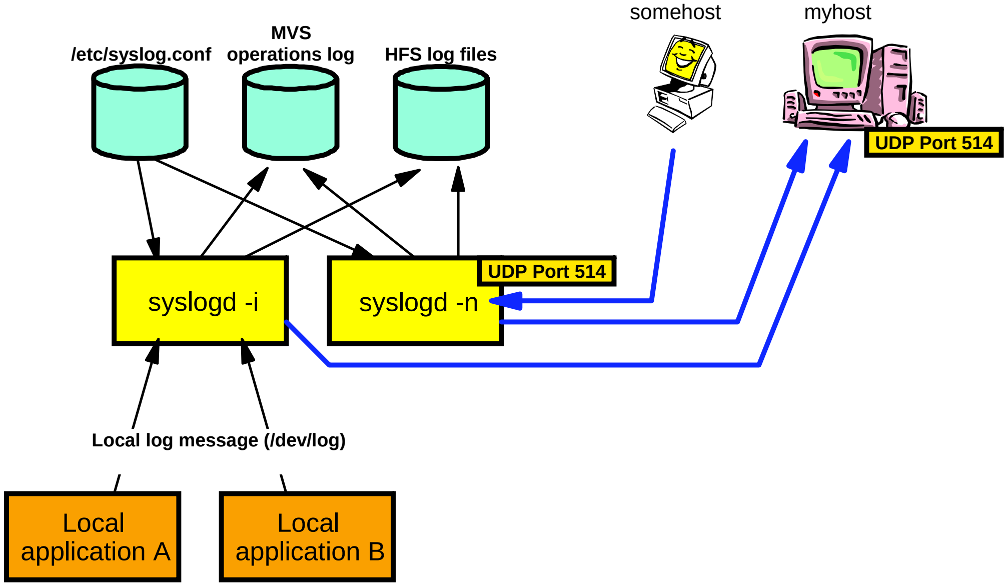
- **Allow SyslogD to receive syslog messages from System z Linux systems over the UDP/IP network and write these messages to a new destination: /dev/operlog**

- **Two instances of SyslogD will be supported, one each in "local" mode and "network" mode:**
  - Local mode will exclusively monitor internal syslog() API activity
  - Network mode will exclusively monitor UDP port 514 for AF_INET/AF_INET6 incoming datagrams



- **Add support for Hostname or IP address filters in SyslogD rules:**
  - Current filters allow facility, priority, userid, and jobname
  - New support will allow filter to specify source hostname or source IP address (IPv4 or IPv6)
  - IP address in rule filter can include a prefix length to cover a range of IP addresses

- **Support added for new SyslogD destination: /dev/operlog**
  - Messages sent to the z/OS OPERLOG logstream
  - May be a DASD-only logstream per LPAR
  - May be a consolidated Sysplex-wide logstream



Statements of Direction

Statements of direction

- **z/OS V1R6 Communications Server and subsequent releases include support for a standalone TN3270 Server. This standalone TN3270 server provides increased flexibility, improved reliability, and simplified problem diagnosis as compared to the in-stack version of the TN3270 Server. z/OS V1.8 is planned to be the last release of z/OS Communications Server which will support the in-stack version of the TN3270 Server. After z/OS V1.8, this capability will be removed from the product. In preparation for that change, customers should consider implementing the standalone TN3270 Server. For more information please refer to http://www.ibm.com/software/network/commserver/zos/**

- **The APPC Application Suite is a set of common applications originally designed to enhance the value of SNA networks for end users. Since more full-featured alternative applications exist in modern integrated SNA/IP networks, z/OS V1.8 is planned to be the last release of z/OS Communications Server which will include the APPC Application Suite. After z/OS V1.8 the APPC Application Suite will no longer be shipped with the product, and will not be supported. However, note that APPC itself remains an integral part of z/OS Communications Server's SNA functions, and there are no plans to remove APPC from z/OS. For more information please refer to http://www.ibm.com/software/network/commserver/zos/**

z/OS CS V1R8
Quick Overview

z/OS CS V1R8 overview - part 1 of 2

- **Sysplex support - multi-tier application performance and networking Sysplex topology flexibility**
  - Automated DNS registration of application-specific hostnames
  - XCF group name for VTAM and TCP/IP (or network Sysplex partitioning)
  - Enhanced Netstat VIPADyn/-v display
  - New messages for DVIPA activation/deactivation
  - Netstat VDPT display - include current number of active connections
  - Serialization of DVIPA (BIND/IOCTL) adds and deletes
  - Dynamic detection and recovery for DVIPA unreachability
  - Optimize Sysplex Distributor intra-Sysplex load balancing
  - Bypass distributing host for client to server Sysplex Distributor traffic when client and assigned server are on same Sysplex member host
  - Source IP address selection based on destination IP address

- **Network security - IDS usability, enhancing IPSec**
  - Support IDS policy in flat file format
  - Support AES cryptographic algorithm for IPSec
  - Complete NAT traversal for IPSec protected traffic - NAT port traversal (NAPT)

- **SNA and EE - improved operations**
  - EE connection network reachability awareness enhancements
  - Remove AnyNet functions from Communications Server (SOD)
  - Retire multiple SAP support for EE parallel connections (SOD)
  - EE connectivity test command

- **IPv6 support - extending integrated IP Security to IPv6 workloads**
  - IPv6 IPSec support

z/OS CS V1R8 overview - part 2 of 2

- **FTP server and client - client usability and management**
  - FTP client API in REXX
  - FTP SMF record enhancements
  - FTP UNICODE without EBCDIC translation

- **TN3270 server - management enhancements**
  - TN3270 performance MIB data on TN3270 SMF record
  - TN3270 performance MIB data via the NMI callable management interface
  - Miscellaneous TN3270 Enhancements

- **Other TCP/IP changes**
  - Remove Assortedparms and Keepaliveoptions statements from TCP/IP profile configuration
  - Provide relief for constrained ECSA storage
  - Pre-Router enhancements

- **Network management**
  - Netstat enhancements
  - Add the ability to drop a list of socket endpoints using the NMI callable management interface
  - NMI enhancements for EE
  - Add connection termination reason code to TCP connection termination SMF record
  - Remove support for Version 1 networking SLA MIB
  - Communications Server support for Health Checker
  - SNMP Enhancements
  - Linux Message Integration

For more information....

URL	Content
http://www.ibm.com/servers/eserver/zseries	IBM eServer zSeries Mainframe Servers
http://www.ibm.com/servers/eserver/zseries/networking	Networking: IBM zSeries Servers
http://www.ibm.com/servers/eserver/zseries/networking/technology.html	IBM Enterprise Servers: Networking Technologies
http://www.ibm.com/software/network/commserver	Communications Server product overview
http://www.ibm.com/software/network/commserver/zos/	z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	Communications Server for Linux on zSeries
http://www.ibm.com/software/network/ccl	Communication Controller for Linux on zSeries
http://www.ibm.com/software/network/commserver/library	Communications Server products - white papers, product documentation, etc.
http://www.redbooks.ibm.com	ITSO Redbooks
http://www.ibm.com/software/network/commserver/support	Communications Server technical Support
http://www.ibm.com/support/techdocs/	Technical support documentation (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)