



SHARE
Session 6864

Boston

Treasure Hunt:

**Buried Gems in z/OS Communications
Server V1R8, V1R9, V1R10, V1R11**

Gwen Dente (gdente@us.ibm.com)

Tuesday, August 3, 4:30 PM - 6:00 PM

Room 109
(Hynes)



IBM Advanced Technical Skills



Abstract

- Well, a lot has happened with Communications Server since z/OS V1R8. And z/OS V1R8 is already out of service. Of course, z/OS V1R9 is almost out of service (September 2010).
- But ... if you were like the rest of us, you were just scrambling to keep your head above water while simply trying to migrate to a supported release. In the process you probably heard or read a lot about all the enhancements in V1R8, V1R9, V1R10, and V1R11 -- but did any of this news really register?? Well, probably the really big items did stick with you -- but did you know there were a lot of hidden gems in these releases that could make your life easier?
- This session presents practical examples of a pot-pourri of pearls for your Communications Server z/OS implementation. With this knowledge under your belt, you can stop feeling overwhelmed about the impending V1R11 (or even V1R12) upgrade and feel that playing "catch up" with the previous releases will be a "snap."
- Disclaimer: There are no IPv6 and very few Enterprise Extender or Sysplex/VIPA topics in this presentation, as these two subjects have been on the radar screen for quite a while now and are covered extensively in many other presentations. Therefore, you will find some of these items documented in the appendices of this presentation.
- Therefore, this session tends to focus on subjects that have been "under the radar" and that have escaped many an implementer's attention.
- **NOTE: Although V1R8 items are included in the handout, only a few of these will be presented during the session, since this release is out of service.**

Acknowledgments: Many visuals are modified from presentations produced by Alfred Christensen, Mike Fox, Dave Herr, and Tom McSweeney of z/OS Communications Server Development.

© Copyright IBM 2010

Why Make Plans to Move to z/OS V1R10 or V1R11 Now?

- z/OS V1R9 has "end-of-service" date of September 30, 2010! Time to move to z/OS V1R10 or V1R11!
- The tables below indicate the end-of-service dates for z/OS releases.
 - An asterisk (*) indicates projected date. Actual end of marketing or end of service date has not been announced yet.
 - http://www-03.ibm.com/servers/eserver/zseries/zos/support/zos_eos_dates.html

Program Number	Version Release Modification	Announced	Available	Withdrawn from Marketing	Service Discontinued
5694-A01	1.11.0	2009/08/18	2009/09/25	2010/09*	2012/09*
5694-A01	1.10.0	2008/08/05	2008/09/26	2009/10/26	2011/09*
5694-A01	1.09.0	2007/08/08	2007/09/28	2008/10/27	2010/09/30 ←
5694-A01	1.08.0	2006/08/08	2006/09/29	2007/10/22	2009/09/30** ←
5694-A01	1.07.0	2005/07/27	2005/09/30	2006/10/23	2008/09/30**
5694-A01	1.06.0	2005/08/10	2004/09/24	2005/10/24	2007/09/30
5694-A01	1.05.0	2004/02/10	2004/03/26	2004/09/09	2007/03/31
5694-A01	1.04.0	2002/08/13	2002/09/27	2004/09/09	2007/03/31
5694-A01	1.03.0	2002/02/19	2002/03/29	2002/09/12	2005/03/31
5694-A01	1.02.0	2001/09/11	2001/10/26	2002/03/14	2004/10/31
5694-A01	1.01.0	2000/10/03	2001/03/30	2001/10/11 or 2002/06/25	2004/03/31

** Support for z/OS V1.7 was withdrawn on September 30, 2008 and support for z/OS V1.8 is planned to be withdrawn on September 30, 2009. The IBM Lifecycle Extension for z/OS V1.7 (5637-A01) and the IBM Lifecycle Extension for z/OS V1.8 (5638-A01) provide fee-based corrective service (a fix, bypass, or restriction to a problem) for up to two years beyond the withdrawal of service dates for z/OS V1.7 and z/OS V1.8 listed above.

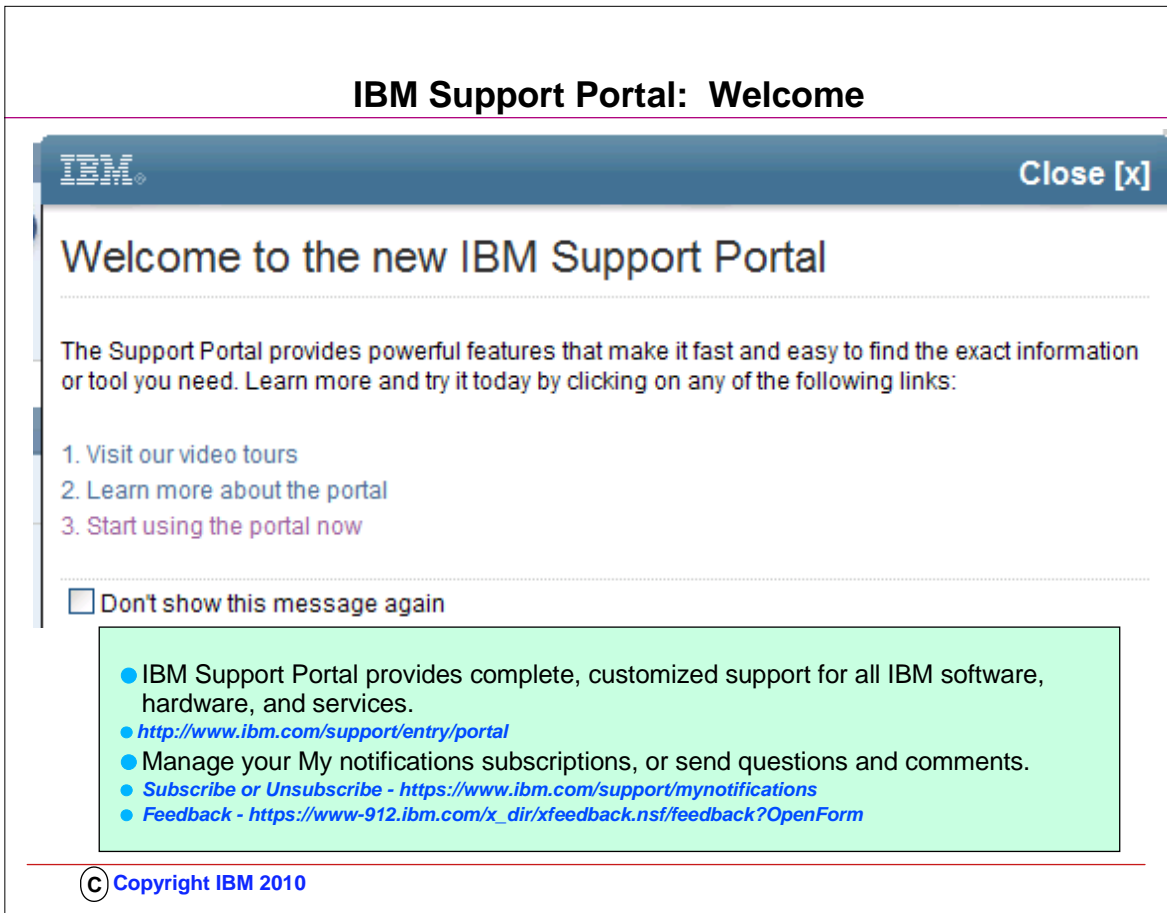
© Copyright IBM 2010

Gems: Migration Planning Improvements



© Copyright IBM 2010

IBM Support Portal: Welcome



The screenshot shows a web browser window titled "IBM Support Portal: Welcome". The window has a blue header bar with the IBM logo on the left and a "Close [x]" button on the right. The main content area has a heading "Welcome to the new IBM Support Portal" followed by a paragraph: "The Support Portal provides powerful features that make it fast and easy to find the exact information or tool you need. Learn more and try it today by clicking on any of the following links:". Below this are three numbered links: "1. Visit our video tours", "2. Learn more about the portal", and "3. Start using the portal now". There is a checkbox labeled "Don't show this message again" which is currently unchecked. A light green box contains a bulleted list of features and links: "● IBM Support Portal provides complete, customized support for all IBM software, hardware, and services.", "● <http://www.ibm.com/support/entry/portal>", "● Manage your My notifications subscriptions, or send questions and comments.", "● [Subscribe or Unsubscribe - https://www.ibm.com/support/mynotifications](https://www.ibm.com/support/mynotifications)", and "● [Feedback - https://www-912.ibm.com/x_dir/xfeedback.nsf/feedback?OpenForm](https://www-912.ibm.com/x_dir/xfeedback.nsf/feedback?OpenForm)". At the bottom left of the window, there is a copyright notice: "© Copyright IBM 2010".

1. NEW and ready for you! The new IBM Support Portal provides complete, customized support for all IBM software, hardware, and services.
2. Start using the IBM Support Portal today!
 1. <http://www.ibm.com/support/entry/portal>
3. Manage your My notifications subscriptions, or send questions and comments.
 1. [Subscribe or Unsubscribe - https://www.ibm.com/support/mynotifications](https://www.ibm.com/support/mynotifications)
 2. [Feedback - https://www-912.ibm.com/x_dir/xfeedback.nsf/feedback?OpenForm](https://www-912.ibm.com/x_dir/xfeedback.nsf/feedback?OpenForm)
4. To ensure proper delivery please add mynotify@stg.events.ihost.com to your address book. You received this e-mail because you are subscribed to IBM My notifications as: <userid>@xxx.yyy.zzz

IBM Support Portal: Overview & Product List

Support overview
Support for my selected products

Search support
Within my selected products
All support & downloads

Choose your products
Manage my product list
Your selected products
z/OS Communications Server
Enter a product name to add it to this product list:

Choose your task
Overview
Downloads
Troubleshooting
Documentation
Forums & communities

Featured links
z/OS Communications Server
Support Technical Exchange
z/OS Communications Server Performance Data
RSS feeds of support content
Request e-mail updates

Notifications
My Notifications
z/OS Communications Server
Create or update your subscription for this product

Flashes & alerts
Alerts: Get the most up to date alerts for your product(s)
IBM Support Portal
z/OS Communications Server
24 Feb 2010: DEFAULT route usage changed in z/OS 1.11 for...
22 May 2009: Abend0c4 in VTAM module ISTPUCCA during...
12 Mar 2009: z/OS Communications Server and OSA...
02 Sep 2008: Storage Display Command Not Accepted by the...
04 Apr 2008: Migration Issue for Custom

Support resources
IBM Education Assistant
Passport Advantage
Software Electronic Support brochure
Software Subscription and Support
Software Support Offerings
Support phone numbers & contacts
Support RSS feeds
Support subscriptions
Upgrades, accessories and parts
Why renew your Software Support?

Product related links
Overview

System availability
Last updated: March 9, 2010 5:34:28 PM
All applications are available
View details

<http://www.ibm.com/support/entry/portal>
<https://www.ibm.com/support/mynotifications>
https://www-912.ibm.com/x_dir/xfeedback.nsf/feedback?OpenForm

© Copyright IBM 2010

Notice how you can customize your IBM Support Panel View.

(1) The panel here is customized to view only z/OS Communications Server.

(2) The z/OS Communications Server selection provides you with the opportunity to select an Overview, to select the Downloads for z/OS Communications Server (like Configuration Assistant for building policies), to select Troubleshooting, Documentation, and even subscribe to Forums and communities.

(3) The featured links on the z/OS Communications Server page can connect you to the Performance data that will help you determine the contrasting performance of SSL/TLS and no SSL/TLS, the contrasting performance of TCP/IP applications from release to release.

(4) "My Notifications" are particularly important here if you want to be advised of any additions to the z/OS Communications Server site by email.

This is how you can learn about new APARs, technical notes, and so on.

(5) For example, through a subscription to "My Notifications" an email would have advised you in February 2010 about the change in the DEFAULT route usage.

Help for the Novice User

- **z/Basic Skills Information Center**

- Directed to new hires and inexperienced users
- Contains documentation and learning modules
- Includes links to existing library
 - <http://publib.boulder.ibm.com/infocenter/zoslnctr/v1r7/index.jsp>

- **New books available at following location:**

- <http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/>
 - z/OS Basics - describes the z/OS operating system
 - z/OS Networking Basics - describes IP and SNA basics
 - z/OS Security

- **IBM Education Assistant:**

- <http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r1/index.jsp>

Help for the Novice User

Home
Mainframe concepts
z/OS concepts
Application programming on z/OS
Networking on z/OS
z/OS problem management
Security on z/OS
z/OS system installation and maintenance
Data and storage management on z/OS
Online workloads for z/OS
Reusable JCL collection
30-minute courses on z/OS
Glossary of z/OS terms and abbreviations
Notices and accessibility
Help for the information center
Contact z/OS
ibm.com: About IBM - Privacy - Contact

z/OS basic skills information center

New to z/OS?
New to z/OS? You've come to the right place! The z/OS basic skills information center is the fastest way to learn and become productive on z/OS.
Once you've learned the basic z/OS concepts and skills presented here, you can find the z/OS product documentation at the [z/OS Internet Library Web site](#).

- **Mainframe concepts**
[HTML](#) | [PDF](#)
Get started with the mainframe.
- **z/OS concepts**
[HTML](#) | [PDF](#)
Get started with the fundamental concepts of z/OS.
- **Application programming on z/OS**
[HTML](#) | [PDF](#)
Learn about the application development environment on z/OS.
- **Networking on z/OS**
[HTML](#) | [PDF](#)
Learn the fundamentals of TCP/IP and SNA networks on z/OS.
- **Problem management on z/OS**
[HTML](#) | [PDF](#)
Get the jump on handling problems.
- **Security on z/OS**
[HTML](#) | [PDF](#)
Understand why z/OS is the most secure system around.
- **Help for the information center**
Get help using the information center.
- **z/OS system installation and maintenance**
[HTML](#) | [PDF](#)
What the system programmer does.
- **Data and storage management on z/OS**
[HTML](#) | [PDF](#)
All about storing and managing data on z/OS.
- **Online workloads for z/OS**
[HTML](#) | [PDF](#)
Find out about z/OS middleware.
- **Reusable JCL collection**
[HTML](#) | [PDF](#)
JCL samples for the taking.
- **30-minute courses on z/OS**
[Mainframe hardware](#), [ISPF](#), and [JCL](#) courses available.
- **Glossary of z/OS terms**
[HTML](#) | [PDF](#)
Learn to speak z/OS.

What's new
→ Find out what's new in the z/OS basic skills IC

Related links
→ z/OS Internet Library

IBM Academic Initiative
→ Mainframe education opportunities

Podcast
→ Who uses mainframe computers? podcast

© Copyright IBM 2010

1. New to z/OS? You've come to the right place! The z/OS basic skills information center is the fastest way to learn and become productive on z/OS.
2. Once you've learned the basic z/OS concepts and skills presented here, you can find the z/OS product documentation at the z/OS Internet Library Web site.
3. z/Basic Skills Information Center
 1. Directed to new hires and inexperienced users
 2. Contains documentation and learning modules
 3. Includes links to existing library
 1. <http://publib.boulder.ibm.com/infocenter/zoslnctr/v1r7/index.jsp>
4. New books available at following location:
 1. <http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/>
 2. z/OS Basics - describes the z/OS operating system
 3. z/OS Networking Basics - describes IP and SNA basics

Customer Connect for z/OS Communications Server V1R11

- <http://www.ibm.com/technologyconnect/index.jsp>

IBM Customer Connect - Mozilla Firefox: IBM Edition

File Edit View History Bookmarks Tools Help

ibm.com https://www-309.ibm.com/technologyconnect/index.jsp

Getting Started Latest Headlines Customize Links Free Hotmail IBM Business Transfor... IBM Business Transfor... IBM Internal H

IBM Customer Connect

United States [change] Terms of use

Home Products Services & solutions Support & downloads My account

IBM Customer Connect

IBM Customer Connect

Online customer tools

IBM Customer Connect provides IBM customers and Business Partners with access to a comprehensive suite of e-business Tools™, design solutions, supply chain information and online education.

Access to the tools requires an IBM ID and proper user permission. If you are a current customer of the IBM Technology Group and wish to request access, please see your account manager for more information.

Due to scheduled maintenance, the IBM Customer Connect (ICC) Web portal services will be unavailable from 11:00 PM US ET on Friday, July 23, 2010 to 5:00 AM US ET on Sunday, July 25, 2010. We sincerely regret the inconvenience. Thank you.

The IBM Customer Connect Help Desk is available 24x7 by phone or e-mail.

US/Canada: 1-888-220-3343
International: +91 80 4193 0239
E-mail: eConnect@us.ibm.com

New Users
→ Registration
Registration Help & FAQ

Connectivity
Browser support

Need more help?
IBM Customer Connect contact info.

About IBM | Privacy | Contact

© Copyright IBM 2010

1. For external customers:
2. ... IBM Customer Connect at
 1. ... <https://www.ibm.com/technologyconnect/index.jsp>
 1. – Sign in
 2. – Select Product Introduction
 3. – Select On Demand Publications
 4. – Select V1R11
3. IBM Education Assistant:
 1. <http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r1/index.jsp>

Resources for Migration to z/OS V1R11

● <http://www-03.ibm.com/systems/z/os/zos/installation/>

The screenshot shows the IBM website interface. At the top, there is a navigation bar with the IBM logo, a search box, and a language selector set to "United States". Below the navigation bar, there are tabs for "Home", "Solutions", "Services", "Products", "Support & downloads", and "My IBM". A user is logged in as "Ms. Gwendolyn Dente". The main content area is titled "z/OS V1R11.0 migration and installation". A left sidebar contains a menu with categories like "z/OS", "About z/OS", "Software", "How to Buy", "Migration & Installation", "News", "Support", "Downloads", "Education", "Library", and "Contact z/OS". The main content includes a breadcrumb trail "IBM Systems > System z > Operating systems >", a list of installation information topics, a section for "IBM fee offerings" with a link to "Worldwide CustomPac Offerings", and a "z/OS migration & installation resources" sidebar with links to various version pages. A "New z/OS V1.9 migration teleconference" sidebar is also present.

IBM Systems > System z > Operating systems >

z/OS V1R11.0 migration and installation

You can find the following installation information topics on this Web page:

- [z/OS V1R11.0 installation planning](#)
- [Ordering z/OS and related products](#)
- [z/OS installation-related publications](#)
[V1.11](#) | [V1.10](#) | [V1.9](#) | [V1.8](#) | [V1.7](#) | [V1.6](#)
[V1.5](#) | [V1.4](#) | [V1.3](#) | [V1.2](#) | [V1.1](#)
- [Other useful resources](#)

IBM fee offerings

[Worldwide CustomPac Offerings](#)
Find out about customized software packages to install z/OS and related products and services.

z/OS migration & installation resources

→ z/OS migration & installation Web pages
[V1.11](#) | [V1.10](#) | [V1.9](#)
[V1.8](#) | [V1.7](#) | [V1.6](#)
[V1.5](#) | [V1.4](#) | [V1.3](#)
[V1.2](#) | [V1.1](#)

New z/OS V1.9 migration teleconference - Your questions answered

→ Replay now available for this June 12th Webcast/open discussion

Related links

- Resources for business partners
- Resources for developers

© Copyright IBM 2010

First Things First: 4 Manuals to Get You Started with Migration

z/OS Comm Server information in system books

● **z/OS Migration**

- Lists Comm Server function that requires you to take action to migrate to V1R10
- This information is not provided in this format in the Communications Server library

● **z/OS Summary of Message and Interface Changes**

- 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

● **z/OS Introduction and Release Guide**

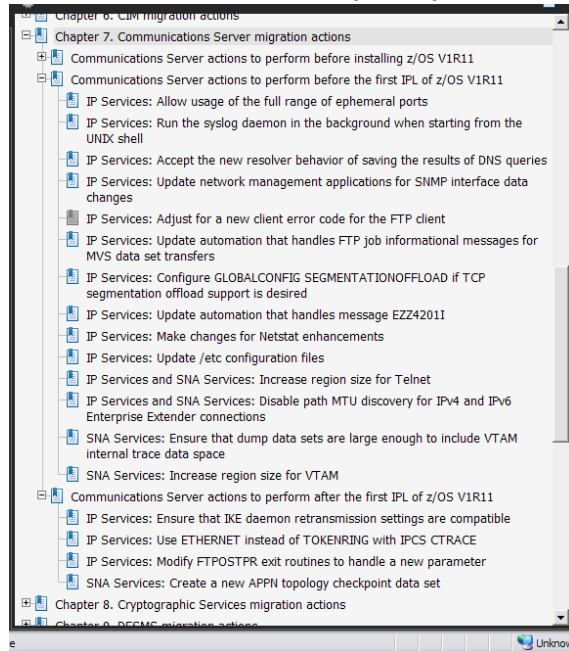
- Presents high-level function descriptions with pointers to the detailed descriptions in New Function Summary

● **z/OS Communications Server New Function Summary**

- Detailed descriptions of new CS functions

Resources for Migration to z/OS V1R11

- Z/OS Migration Guide
- <http://publibz.boulder.ibm.com/epubs/pdf/e0z2m171.pdf>



© Copyright IBM 2010

1. z/OS Migration
2. • Lists Comm Server function that requires you to take action to migrate to V1R9, V1R10, V1R11
3. • This information is not provided in this format in the Comm Server library

Resources for Migration to z/OS V1R11

● <http://publibz.boulder.ibm.com/epubs/pdf/e0z2m171.pdf>

Chapter 7. Communications Server migration actions	
Communications Server actions to perform before installing z/OS V1R11	131
IP Services: Modify applications to no longer add IPv6-type IP routing headers to outgoing packets	132
IP Services: Update automation to accommodate FTP output that is changed for extended address volumes	132
IP Services: Update procedures that use the syslogd job name	133
IP Services: Accept the new behavior of TCP receive buffer size	134
IP Services: Migrate from NDB function	135
IP Services: Migrate from BIND DNS 4.9.3 function	136
IP Services: Migrate from BIND function	137
IP Services: Migrate from DHCP server function	137
IP Services: Remove customization of SNMP sysObjectID MIB object in OSNMPD.DATA file	138
IP Services: Update IP filter policy to filter IP fragments correctly for RFC 4301 compliance	139
IP Services: Migrate FTP servers sharing FTPDATA with FTP clients	142
IP Services: Update network management applications for SNMP support of the RFC versions of networking MIB modules	144
IP Services: Specify at least one valid ZIIP subparameter on GLOBALCONFIG ZIIP statements	145
IP Services: Migrate from QoS TR policy to IDS TR policy	146
SNA Services: Ensure compatible levels of VTAM for HPR sessions	148
SNA Services: Update applications and user exits that use the VTAM version and release level in algebraic expressions	149
Communications Server actions to perform before the first IPL of z/OS V1R11	150
IP Services: Allow usage of the full range of ephemeral ports	150
IP Services: Run the syslog daemon in the background when starting from the UNIX shell	151
IP Services: Accept the new resolver behavior of saving the results of DNS queries	152
IP Services: Update network management applications for SNMP interface data changes	153
IP Services: Adjust for a new client error code for the FTP client	155
IP Services: Update automation that handles FTP job informational messages for MVS data set transfers	155
IP Services: Configure GLOBALCONFIG SEGMENTATIONOFFLOAD if TCP segmentation offload support is desired	157
IP Services: Update automation that handles message EZZI201L	157
IP Services: Make changes for Netstat enhancements	158
IP Services: Update /etc configuration files	159
IP Services and SNA Services: Increase region size for Telnet	161
IP Services and SNA Services: Disable path MTU discovery for IPv4 and IPv6 Enterprise Extender connections	162
SNA Services: Ensure that dump data sets are large enough to include VTAM internal trace data space	163
SNA Services: Increase region size for VTAM	164
Communications Server actions to perform after the first IPL of z/OS V1R11	165
IP Services: Ensure that IKE daemon retransmission settings are compatible	165
IP Services: Use ETHERNET instead of TOKENRING with IPCS CTRACE	166
IP Services: Modify FTPOSTPR exit routines to handle a new parameter	167
SNA Services: Create a new APTN topology checkpoint data set	168

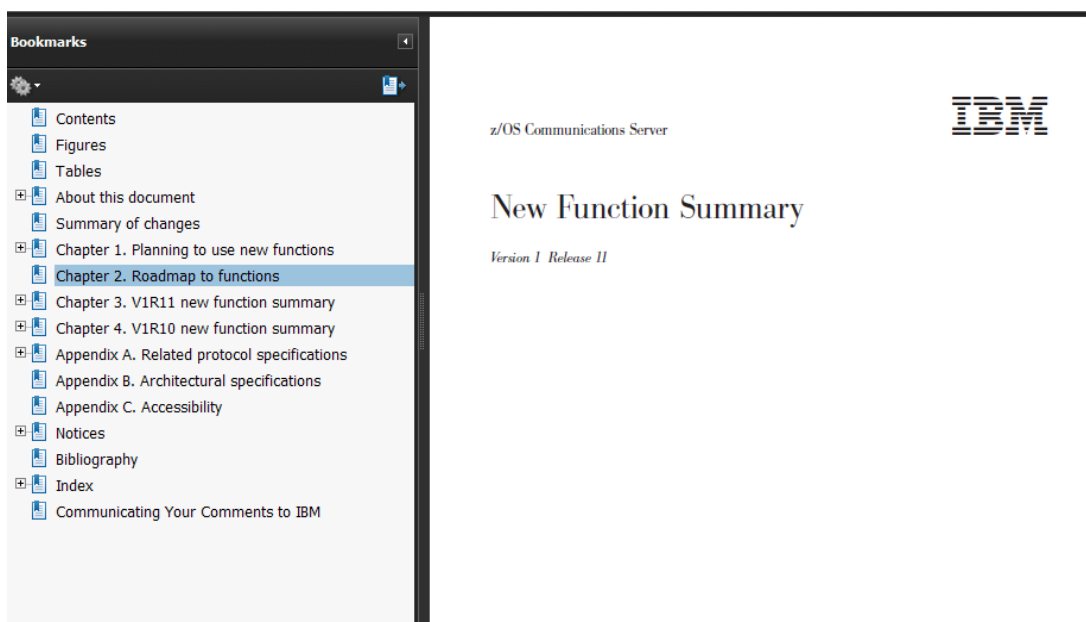
This topic describes migration actions for base element Communications Server.

Communications Server actions to perform before installing z/OS V1R11

This topic describes Communications Server migration actions that you can perform on your current (old) system. You do not need the z/OS V1R11 level of

© Copyright IBM 2010

z/OS Communications Server New Function Summary (V1R11: 1.11 and 1.10)



● <http://publibz.boulder.ibm.com/epubs/pdf/f1a1f250.pdf>

● Reached through: <http://www-03.ibm.com/systems/z/os/zos/bkserv/r11pdf/#commserv>

© Copyright IBM 2010

1. The starting place to learn about new functions is the New Function Summary.
2. This visual shows you that the V1R11 edition includes a roadmap of all the functions in the last two releases; details about each function are in Chapter 3 (R11) and in Chapter 4 (R10).
3. Each of the two chapters contains a list of both IP and SNA functions in the V1R11 edition. The V1R10 and V1R9 editions are laid out a bit differently, with SNA and IP functions being in separate sections of the various chapters.

"Roadmap to functions" in z/OS Communications Server New Function Summary (V1R11: 1.11 and 1.10)

Bookmarks

- About this document
- Summary of changes
- Chapter 1. Planning to use new functions
- Chapter 2. Roadmap to functions**
- Chapter 3. V1R11 new function summary
 - Support considerations in V1R11
 - General release considerations in V1R11
- Application integration, data consolidation, and standards
- Availability and business resilience
- Scalability, performance, constraint relief, and accelerators
- Security
- Simplification and consumability
- SNA and Enterprise Extender
- System management and monitoring
- Virtualization
- Chapter 4. V1R10 new function summary
 - Support considerations in V1R10
 - Performance improvements for IP in V1R10

Chapter 2. Roadmap to functions

This topic includes a roadmap table to all of the functions and enhancements that were introduced in z/OS V1R11 Communications Server and z/OS V1R10 Communications Server.

The **Exploitation actions** column indicates whether tasks are required to either use the functional enhancement or to satisfy incompatibilities or dependencies.

Table 8. Roadmap to functions

Functional enhancement	Exploitation actions
Enhancements introduced in z/OS V1R11 Communications Server	
"New SMTP client for sending Internet mail" on page 26	Yes
"FTP access to UNIX named pipes" on page 29	Yes
"FTP large-volume access" on page 33	Yes
"FTP passive mode enhancements" on page 33	Yes
"Customizable pre-logout banner for csh/ssh" on page 35	Yes
"Remote execution server enhancements" on page 35	Yes
"rXN32ti support of TSO logon reconnect" on page 36	No
"IPv6 stateless address autoconfiguration enhancements" on page 36	Yes
"New API to obtain IPv4 network interface MTU" on page 38	Yes
"RPC 5065 deprecation of IPv6 type 0 route header" on page 38	No
"CICS sockets enhancements" on page 39	No
"Improved responsiveness to storage shortage conditions" on page 39	Yes
"Disable moving DVIWA as source IP address" on page 40	No
"Support for enhanced WLM routing algorithms" on page 41	Yes
"accept_and_receive API enhancements" on page 41	No
"rCPI/IP support for system z10 hardware instrumentation" on page 42	No
"rCPI/IP pathlength improvements" on page 42	No
"rCPI throughput improvements for high-latency networks" on page 42	Yes
"Virtual storage constraint relief" on page 43	Yes

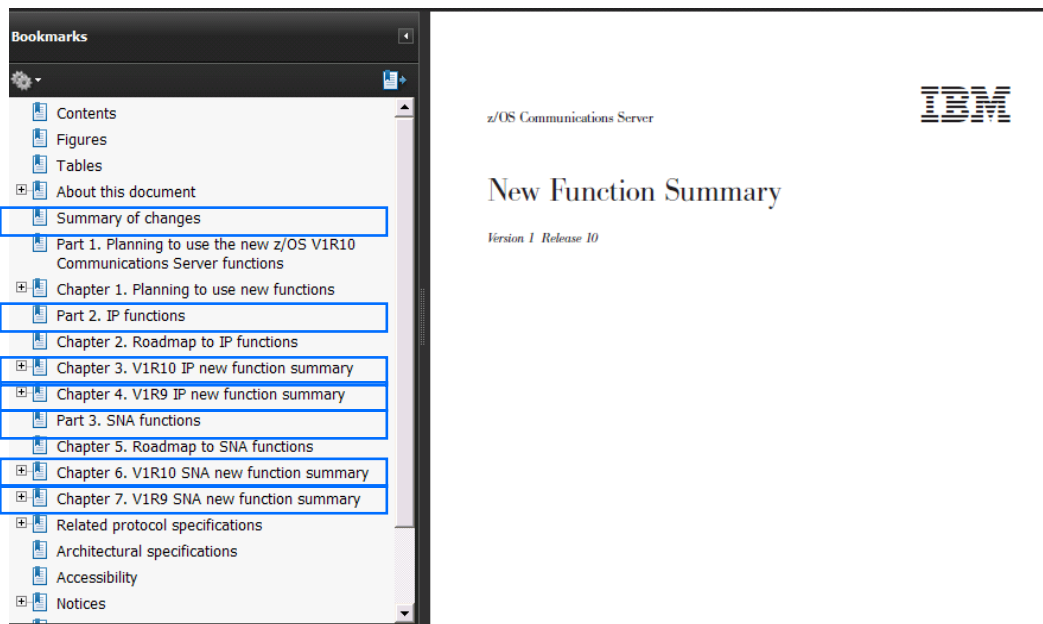
● <http://publibz.boulder.ibm.com/epubs/pdf/f1a1f250.pdf>

● Reached through: <http://www-03.ibm.com/systems/z/os/zos/bkserv/r11pdf/#commserv>

© Copyright IBM 2010

1. The starting place to learn about new functions is the New Function Summary.
2. This visual shows you that the V1R11 edition includes a roadmap of all the functions in the last two releases; details about each function are in Chapter 3 (R11) and in Chapter 4 (R10).

"Roadmap to functions" in z/OS Communications Server New Function Summary (V1R10: 1.10 and 1.9)



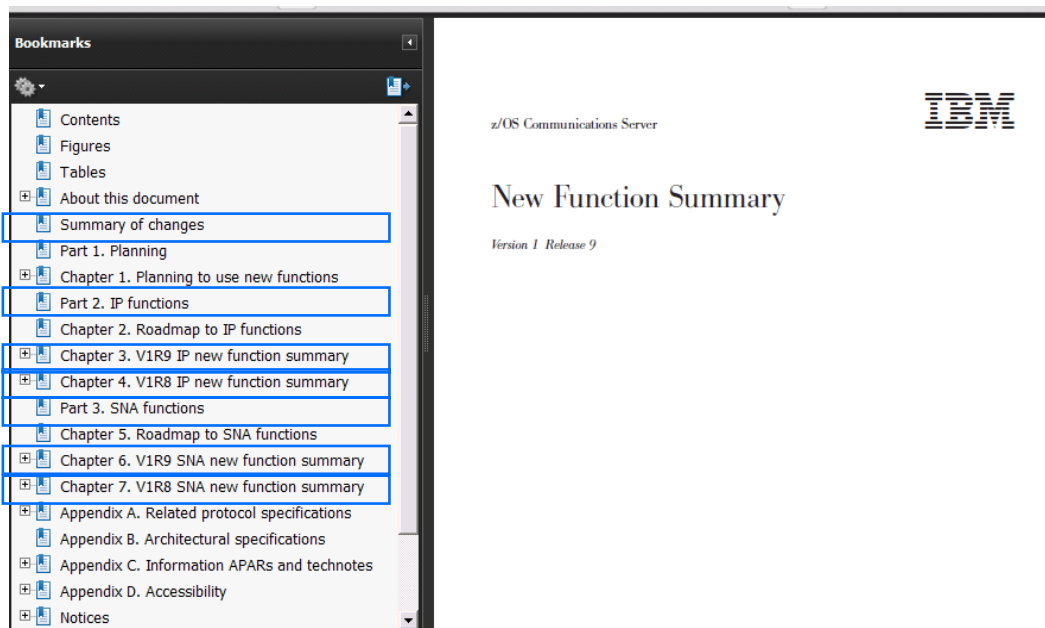
● <http://publibz.boulder.ibm.com/epubs/pdf/f1a1f250.pdf>

● Reached through: <http://www-03.ibm.com/systems/z/os/zos/bkserv/r11pdf/#commserv>

© Copyright IBM 2010

1. This visual shows you that the V1R10 edition includes a roadmap of all the functions in the last two releases.
2. The organization is a bit different from that of the V1R11 manual, in that the IP functions for each of the last two releases are listed in one part, and the SNA functions are listed in another.
3. Nevertheless, you can see that this manual is also a wonderful starting point, and does contain the changes in V1R9 that are not included in the V1R11 manual.

"Roadmap to functions" in z/OS Communications Server New Function Summary (V1R9: 1.9 and 1.8)



● <http://publibz.boulder.ibm.com/epubs/pdf/f1a1f250.pdf>

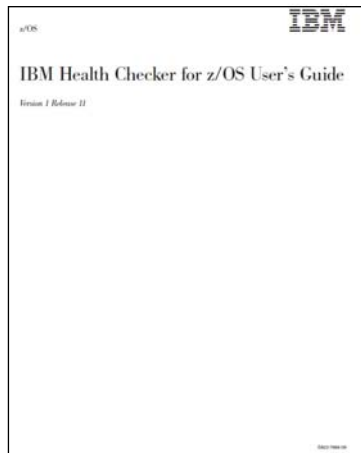
● Reached through: <http://www-03.ibm.com/systems/z/os/zos/bkserv/r11pdf/#commserv>

© Copyright IBM 2010

1. This visual shows you that the V1R9 edition includes a roadmap of all the functions in the last two releases.
2. The organization is a bit different from that of the V1R11 manual, in that the IP functions for each of the last two releases are listed in one part, and the SNA functions are listed in another. It has the same organization as the V1R10 manual.
3. Nevertheless, you can see that this manual is also a wonderful starting point, and does contain the changes in V1R8 that are not included in the V1R10 manual.

Health Checks Available for z/OS Communications Server

http://www-03.ibm.com/systems/z/os/zos/hchecker/check_table.html



IBM Health Checker for z/OS User's Guide (GA22-7994)

IBM Systems > System z > Operating systems > z/OS

Checks available for IBM Health Checker for z/OS

The following table lists currently available IBM checks by check owning component or product and the APAR or z/OS release in which they were introduced.

For complete check descriptions, see the [IBM Health Checker for z/OS checks](#) topic in the [IBM Health Checker for z/OS User's Guide](#).

Check owner	Check name	APAR number and/or z/OS release
IBMASH ASH	ASH_LOCAL_SLOT_USAGE	Integrated in z/OS V1R8.
	ASH_NUMBER_LOCAL_DATASETS	
	ASH_PAGE_ADD	
	ASH_PLPA_COMMON_SIZE	
IBMCATALOG Catalog	CATALOG_IMBED_REPLICATE	Integrated in z/OS V1R11.
	CETCP_SVSLEXHON_RECOV_TCFIPstackname CVTAN_T18UP_T28UP_EE CVTAN_T18UP_T28UP_NOBE CVTAN_VIT_DSPSIZE CVTAN_VIT_OPT_ALL CVTAN_VIT_OPT_PSSMS CVTAN_VIT_SIZE	Integrated in z/OS V1R9.
IBMC65 Communications Server	CETCP_TCPMAXCVDUPR_SIZE_TCFIPstackname	Integrated in z/OS V1R8.
	CVTAN_CSM_STG_LIMIT	
	CSTCP_CINET_PORTING_RSV_TCFIPstackname	Integrated in z/OS V1R10.
	ZOSHGV1R10_CS_BIND4	GA22593 and P668135 contain checks for z/OS V1R8 and V1R9 and is integrated into V1R10.
	ZOSHGV1R11_CS_DNSBIND9	Integrated in z/OS V1R11.
	ZOSHGV1R11_CS_RFC4301	GA22605 and P684362 contain check for z/OS V1R10 and V1R11.
IBMCNZ Consoles	CNZ_CONSOLE_MSCORE_AND_ROUTCOD	GA02005 contains checks for z/OS V1R6-V1R7 and is integrated in z/OS V1R8.
	CNZ_AHNF_EVENTUAL_ACTION_MSGS	
	CNZ_CONSOLE_MASTERAUTH_CMDSYS	
	CNZ_CONSOLE_F_ROUTCODE_11	
	CNZ_BMCS_HARDCOPY_MSCORE	
	CNZ_BMCS_INACTIVE_CONSOLES	
	CNZ_SYSCONS_MSCORE	
	CNZ_SYSCONS_PD_MODE	
	CNZ_SYSCONS_ROUTCODE	
	CNZ_TASK_TABLE	
	CNZ_SYSCONS_MASTER (z/OS V1R6-V1R7 only)	
CNZ_OBSOLETE_MSGFIELD_AUTOMATION	Integrated in z/OS V1R11.	

© Copyright IBM 2010

1. You will probably want to download the IBM Health Checker for z/OS User's Guide to investigate how to implement Health Checker and to understand the various types of health checks that are available to you, including those in IBM Communications Server.
2. The User's Guide points you to a web page that is kept updated for all currently available health checks:
 1. http://www-03.ibm.com/systems/z/os/zos/hchecker/check_table.html
3. The web page provides you the name of the RFC4301 health check that you will want your z/OS Systems Programmer to implement for you.

Resources for Migration to z/OS V1R11: Health Checker

```
F HEALTHCK,DISPLAY,CHECKS
HZS0200I 10.25.57 CHECK SUMMARY
```

CHECK	OWNER	CHECK NAME	STATE	STATUS
IBMCS		CSTCP_CINET_PORTRNG_RSV_TCPCS1	AE	SUCCESSFUL
IBMCS		CSTCP_SYSPLEXMON_RECOV_TCPCS1	AE	EXCEPTION-LOW
IBMCS		CSTCP_TCPMAXRCVBUFRSIZE_TCPCS1	AE	SUCCESSFUL
IBMCS		CSTCP_SYSTCPIP_CTRACE_TCPCS1	AE	EXCEPTION-LOW
IBMCS		CSVTAM_T1BUF_T2BUF_NOEE	AE	SUCCESSFUL
IBMCS		CSVTAM_T1BUF_T2BUF_EE	AD	ENV N/A
IBMCS		CSVTAM_VIT_OPT_ALL	AE	EXCEPTION-LOW
IBMCS		CSVTAM_VIT_DSPSIZE	AE	EXCEPTION-LOW
IBMCS		CSVTAM_VIT_OPT_PSSSMS	AE	SUCCESSFUL
IBMCS		CSVTAM_VIT_SIZE	AE	EXCEPTION-LOW
IBMCS		CSVTAM_CSM_STG_LIMIT	AE	SUCCESSFUL
IBMUSS		USS_MAXSOCKETS_MAXFILEPROC	AD	UNEXP ERROR
IBMUSS		USS_AUTOMOUNT_DELAY	AD	ENV N/A
IBMUSS		USS_FILESYS_CONFIG	AE	EXCEPTION-MED
IBMXGLOGR		IXGLOGR_ENTRYTHRESHOLD	AE	SUCCESSFUL

- *No check for TCPRCVBUFRSIZE --but verify anyway that it is at least 64K so that you can take advantage of "Dynamic Right Sizing" in z/OS V1R11*

© Copyright IBM 2010

- To setup Health Checker to run, you must:
 - 1.1 Allocate the HZSPDATA data set to save check data between restarts
 - 2.2 Set up the HZSPRINT utility
 - 3.3 Define log streams
- If you want to maintain an historical record of your check output
 - 1.4 Create security definitions
 - Give the Health Checker proc update access to the HZSPDATA data set
 - Give the Health Checker proc read access to the HZSPRMxx parmlib members
 - Give the Health Checker proc read access to each Health Checker logstream
 - Authorize HZSPRINT users to QUERY and MESSAGES services
 - Authorize SDSF support for Health Checker message output
 - 7.5 Create multilevel security definitions, if necessary
 - 8.6 Create HZSPRMxx from the HZSPRM00 parmlib member
- If you want to make permanent changes to check values & parameters
- If you want to deactivate a check
 - 1.7 Start the IBM Health Checker for z/OS proc
- ..Step-by-Step details for setting up Health Checker can be found in .. IBM Health Checker for z/OS User's Guide and at http://www-03.ibm.com/systems/z/os/zos/hchecker/check_table.html
- Setting the TCP Buffer size to a minimum of 64K is important if you want to take advantage of "DYNAMIC RIGHTSIZING" in z/OS V1R11.
 - Streaming workload over large bandwidth and high latency networks (such as satellite links) is in general constrained by the TCP window size. The problem is that it takes time to send data over such a network. At any given point in time data filling the full window size is 'in-transit' and cannot be acknowledged until it starts arriving at the receiver side. The sender can send up to the window size and then must wait for an ACK to advance the window size before the next chunk can be sent.
 - If it were possible to dynamically adjust the window size to what it takes to fill the network in-between the sender and the receiver, higher throughput might be achieved.
 - This support will, on the receiver side, dynamically adjust the window size upward (beyond 180K if so needed) in an attempt to 'fill' the pipe between the sender and the receiver. The aim is that as soon as the sender has sent the end of its window, the sender receives an ACK from the receiver. That ACK allows the sender to advance the window and send another chunk onto the network.
 - The dynamic right sizing (DRS) algorithm is based on a paper that was published by Los Alamos National Laboratory. The goal of DRS is to keep the pipe full and prevent sender from being constrained by the advertised window. The window size may grow as high as 2 Mbytes. The TCP/IP stack will disable the function if the application doesn't keep up. A netstat all report will show the DRS-adjusted receive buffer size.
 - NOTE: Be sure to check the size of your TCPRCVBUFRSIZE and adjust to 64K or higher; otherwise the Dynamic Right Sizing function in V1R11 may not work for you; the receive buffer must be equal to or larger than 64K. There is no healthchecker available to verify the size of the TCPRCVBUFRSIZE ... there is only one for TCPMAXRCVBUFRSIZE.

How to Use the Migration Health Checker

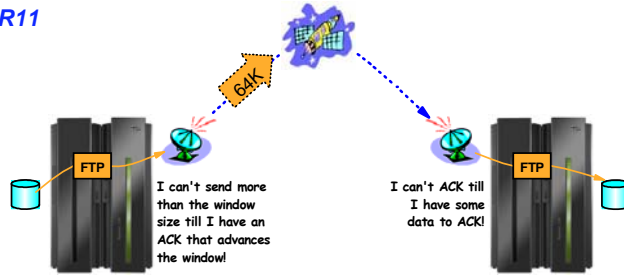
- Activate the Migration Health Checks appropriate for the migration plan, specifying releases you are migrating through and to.
- For example:
 - F HZSPROC,ACTIVATE,CHECK=(IBMCS,ZOSMIGV1R10*)
 - Migration Health Checks will run on the system.
 - Review output for exceptions to create planning items for the migration plan.
 - Can deactivate Migration Health Checks after reviewing output
For example:
 - F HZSPROC,DEACTIVATE,CHECK=(IBMCS,ZOSMIGV1R10*)
- No automatic correction of exceptions is done by IBM Health Checker for z/OS.

© Copyright IBM 2010

1. Exception messages from Health Checker are an indication of a potential availability or performance problem
2. .. Just because you get an exception, it doesn't mean that there is a problem to report to IBM
3. .. You need to look over the exception message and decide whether the suggested change is appropriate for your system.
Either
 1. .. Implement the suggested change
 2. .. Change the parameters of the check
 3. .. Inactivate the check
 4. .. Delete the check

Resources for Migration to z/OS V1R8: Health Checker

- **z/OS CS V1R8 implemented initial support for and use of the z/OS Health-checker infrastructure:**
 - 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**)
 - The default size of the TCP maximum receive buffer size (the **TCPMAXRCVBUFRSIZE** option in the TCP/IP Profile)
 - **DYNAMIC RIGHT SIZING in V1R11**
 - **TCPRCVBUFRSIZE>= 64K**



- Improves performance for inbound streaming TCP connections over networks with large bandwidth and high latency by automatically tuning the ideal window size for such TCP connections.
- This function does not take effect for applications which use a TCP receive buffer size smaller than 64K.
 - The enhancement implements an algorithm known as "DYNAMIC RIGHT SIZING"

© Copyright IBM 2010

1. What is Health Checker?
2. ..IBM Health Checker for z/OS is a component of MVS. It consists of:
 1. •The framework - The interface that allows the customer to run and manage checks
 2. •The individual checks - specific settings or values checked for potential problems
 3. -Individual checks are owned by a component or element
 4. ..It identifies potential problems before they impact availability or cause outages.
 1. •Configuration is complicated:
 1. ..Many outages or performance bottlenecks are caused by configuration problems
 2. ..Sometimes, default values are best guesses
 3. ..Best practices may not become known until exposure in many environments
 4. ..It checks the current active z/OS and sysplex settings and definitions for a system and compares the values to those suggested by IBM or defined by the customer.
3. ..IBM Health Checker for z/OS produces output in the form of detailed messages to let the customer know of both potential problems and suggested actions to take.
 1. •Can be viewed via: SDSF, HZSPRINT utility, or log stream
 2. •Exceptions produce WTO messages
 3. •Use the information in the check message to resolve possible configuration problems
4. Setting the TCP Buffer size to a minimum of 64K is important if you want to take advantage of "DYNAMIC RIGHTSIZING" in z/OS V1R11.
 1. Streaming workload over large bandwidth and high latency networks (such as satellite links) is in general constrained by the TCP window size. The problem is that it takes time to send data over such a network. At any given point in time data filling the full window size is 'in-transit' and cannot be acknowledged until it starts arriving at the receiver side. The sender can send up to the window size and then must wait for an ACK to advance the window size before the next chunk can be sent.
 2. If it were possible to dynamically adjust the window size to what it takes to fill the network in-between the sender and the receiver, higher throughput might be achieved.
 3. This support will, on the receiver side, dynamically adjust the window size upward (beyond 180K if so needed) in an attempt to 'fill' the pipe between the sender and the receiver. The aim is that as soon as the sender has sent the end of its window, the sender receives an ACK from the receiver. That ACK allows the sender to advance the window and send another chunk onto the network.
 4. The dynamic right sizing (DRS) algorithm is based on a paper that was published by Los Alamos National Laboratory. The goal of DRS is to keep the pipe full and prevent sender from being constrained by the advertised window. The window size may grow as high as 2 Mbytes. The TCP/IP stack will disable the function if the application doesn't keep up. A netstat all report will show the DRS-adjusted receive buffer size.
5. NOTE: Be sure to check the size of your TCPRCVBUFRSIZE and adjust to 64K or higher; otherwise the Dynamic Right Sizing function in V1R11 may not work for you; the receive buffer must be equal to or larger than 64K. There is no healthchecker available to verify the size of the TCPRCVBUFRSIZE ... there is only one for TCPMAXRCVBUFRSIZE.

Resources for Migration to z/OS V1R9: Health Checker

● z/OS CS V1R9 extends support for and use of the z/OS Health-checker infrastructure:

- If a TCP/IP stack has **DYNAMICXCF** defined in combination with **GLOBALCONFIG SYSPLEXMONITOR** without the RECOVERY option, a warning will be issued since this is not a recommend best practice combination. In this case, the automated **RECOVERY** option should be used.
- Various VTAM checks are being added:
- Check that the **VIT SIZE** is not lower than the default value of 999
- Check that the **VIT** options **PSS** (VTAM's Process Scheduling Services) and **SMS** (VTAM's Storage Management Services) are turned on - they are always needed to service a problem
- Check that **DSPSIZE** is at least 5 (50 Megabytes)
- Check to see if someone has **OPT=ALL** specified (requesting all VIT trace options be turned on) - this may not be optimal, unless requested by VTAM services personnel
- Check that the Enterprise Extender QDIO/iQDIO buffer pools (**T1Buf and T2Buf pools**) are of reasonable sizes

© Copyright IBM 2010

1. What is Health Checker?

1. ..IBM Health Checker for z/OS is a component of MVS. It consists of:
 1. •The framework - The interface that allows the customer to run and manage checks
 1. •The individual checks - specific settings or values checked for potential problems
 2. –Individual checks are owned by a component or element
 3. ..It identifies potential problems before they impact availability or cause outages.
 1. •Configuration is complicated:
 2. ..Many outages or performance bottlenecks are caused by configuration problems
 3. ..Sometimes, default values are best guesses
 4. ..Best practices may not become known until exposure in many environments
 5. ..It checks the current active z/OS and sysplex settings and definitions for a system and compares the values to those suggested by IBM or defined by the customer.
 2. ..IBM Health Checker for z/OS produces output in the form of detailed messages to let the customer know of both potential problems and suggested actions to take.
 1. •Can be viewed via: SDSF, HZSPRINT utility, or log stream
 2. •Exceptions produce WTO messages
 3. •Use the information in the check message to resolve possible configuration problems

Resources for Migration to z/OS V1R10: Health Checker

● z/OS CS "Best Practice" Health Check

- Check that the *BPXPRMxx INADDRANYPORT and INADDRANYCOUNT* specifications match correct *TCP/IP PORT/PORTRANGE* definitions
- These ports must be reserved to OMVS - if not, an abend EC6 may occur when Common INET tries to use one of them

● z/OS CS now implements migration checks within the z/OS Healthchecker "Best Practice" infrastructure

- A check to determine if Boot Information Negotiation Layer (BINL) server function is in use on the system.
- A check to determine if Berkeley Internet Name Domain 4.9.3 (BIND 4.9.3) DNS server function is in use on the system.
- A check to determine if Dynamic Host Configuration Protocol (DHCP) server function is in use on the system.
- A check to determine if Network Database (NDB) server function is in use on the system.

● The migration health checks that are delivered as part of z/OS V1R10 CS, will be rolled back to z/OS V1R8 and V1R9

```
HZS0001I CHECK(IBMCS,ZOSMIGV1R10_CS_BIND4):  
ISTM004E BIND 4.9.3 DNS server function is in use on this  
system during this IP.
```

© Copyright IBM 2010

1. The V1R10 Migration Health Checks:

1. Objective is to provide programmatic migration checks that can give you an early warning if you are using functions that will be significantly changed or removed in future releases

2. Traffic Regulation Policies

1. z/OS V1.9 is the last release of z/OS Communications Server which will support the configuration of Traffic Regulation (TR) policy as part of the Quality of Service discipline. The TR configuration function remains supported, but IBM recommends that you implement it as part of the Intrusion Detection Services (IDS) policy configuration made available in z/OS V1.8. This change is only for the TR policy configuration. The TR policy functions themselves remain unaffected. For more information, please refer to z/OS V1.8 Communications Server's IP Configuration Guide, chapter 16, "Intrusion Detection Services", and IP Configuration Reference, chapter 23, "Intrusion Detection Services policy".

2. z/OS CS Network Data Base (NDB) server removal

1. In a future release of z/OS, the Network Database (NDB) function will be removed from the z/OS Communications Server component. Customers who currently use or plan to use the NDB function should investigate the distributed data facility (DDF) provided by z/OS DB2, and the DB2 Run-Time Client. DDF allows client applications running in an environment that supports DRDA to access data at DB2 servers.

3. z/OS CS Dynamic Host Configuration Protocol (DHCP) server removal

1. In a future release of z/OS, the Dynamic Host Configuration Protocol (DHCP) server function will be removed from the z/OS Communications Server component. Customers who currently use or plan to use the z/OS DHCP server should investigate using a DHCP server on Linux for System z.

4. z/OS CS Boot Information Negotiation Layer (BINL) removal

1. In a future release of z/OS, the Boot Information Negotiation Layer (BINL) function will be removed from the z/OS Communications Server component. Customers using this function should investigate the use of IBM Tivoli Provisioning Manager for OS Deployment for network-based operating system installation services.

5. NOTE: All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice.

Manuals in Communications Server V1R11

Book	Number
*** New Function Summary	GC31-8771-05
** Communications Server ACF/TAP Trace Analysis Handbook	GC23-8588-00
IPv6 Network and Design Guide	SC31-8885-07
IP Configuration Guide	SC31-8775-15
IP Configuration Reference	SC31-8776-16
SNA Network Implementation	SC31-8777-09
SNA Resource Definition	SC31-8778-10
SNA Operation	SC31-8779-09
Quick Reference	SX75-0124-09
IP User's Guide and Commands	SC31-8780-09
IP System Administrator's Commands	SC31-8781-09
SNA Diagnosis, Vol 1: Techniques and Procedures	GC31-6850-04
SNA Diagnosis, Vol 2: FFST Dumps and the VIT	GC31-6851-04
IP Diagnosis	GC31-8782-10
SNA Messages	SC31-8790-09

Not all manuals are listed; Some of the manuals are valid for both V1R10 and V1R11.

Beginning with z/OS V1R7.0, there are no longer any z/OS elements and features licensed manuals. z/OS elements and features manuals that were licensed in previous z/OS releases have been declassified for z/OS V1R7.0 and you can find them with the rest of the z/OS V1R7.0 unlicensed manuals.

© Copyright IBM 2010

1. Link to manuals is at:

1. <http://www-03.ibm.com/systems/z/os/zos/bkserv/r11pdf/#commserv>
2. <http://www-03.ibm.com/systems/z/os/zos/bkserv/r11pdf/>

Manuals in Communications Server V1R11

Book	Number
IP Messages: Volume 1 (EZA)	SC31-8783-10
IP Messages: Volume 2 (EZB, EZD)	SC31-8784-09
IP Messages: Volume 3 (EZY)	SC31-8785-09
IP Messages: Volume 4 (EZZ, SNM)	SC31-8786-11
IP and SNA Codes	SC31-8791-09
IP Programmer's Guide and Reference	SC31-8787-11
SNA Customization	SC31-6854-03
CSM Guide	SC31-8801-02
SNA Data Areas, 1	GC31-6852-03
SNA Data Areas, 2	GC31-6853-03
SNA Resource Definition Samples	SC31-8836-05
...	
...	

Not all manuals are listed; Some of the manuals are valid for both V1R10 and V1R11.

Beginning with z/OS V1R7.0, there are no longer any z/OS elements and features licensed manuals. z/OS elements and features manuals that were licensed in previous z/OS releases have been declassified for z/OS V1R7.0 and you can find them with the rest of the z/OS V1R7.0 unlicensed manuals.

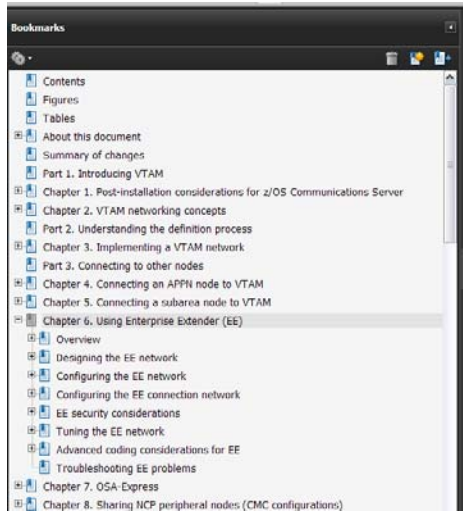
© Copyright IBM 2010

1. Link to manuals for downloading is at:

1. <http://www-03.ibm.com/systems/z/os/zos/bkserv/r11pdf/#commserv>
2. <http://www-03.ibm.com/systems/z/os/zos/bkserv/r11pdf/>

Are You Looking for Tutorials on Enterprise Extender?

● SNA Network Implementation Guide (SC31-8777-09)



Chapter 6. Using Enterprise Extender (EE)

Companies continue to rely on older applications that require access to these applications was through SNA. Today, applications are generally based on TCP/IP. Initially, companies supported SNA applications separately, but are now seeking ways to consolidate SNA applications to TCP/IP and, in many cases, it is technically impractical because of the lack of source code.

With Enterprise Extender (EE) you can extend the reach of SNA data to include TCP/IP networks and IP-attached devices, providing scalability, and control similar to those that SNA uses. EE uses standard IP technology and does not require any changes in the IP backbone.

You can use an IP network for SNA sessions with Enterprise Extender (EE) provides enablement of IP applications and convergence of SNA and IP transport while preserving SNA application and end-to-end connection. Conceptually, an IP connection that represents an APPN/HPR transmission group (TG) in a session.

● Share presentations

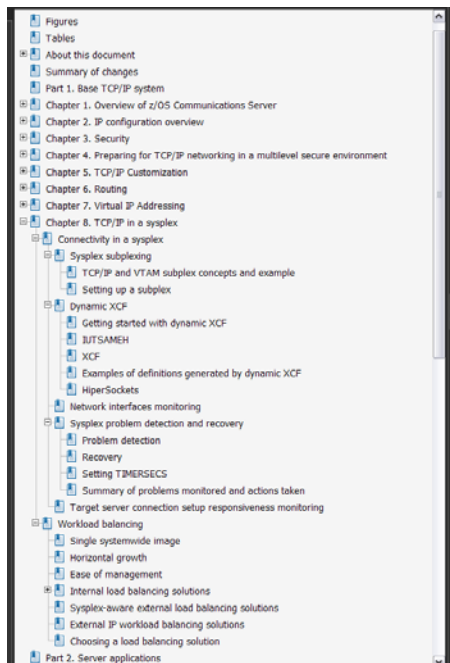
● www.ibm.com/support/techdocs/

© Copyright IBM 2010

1. Implementers may be aware of the many EE presentations on the SHARE website (www.share.org) and on the IBM Techdocs website (www.ibm.com/support/techdocs), but too many people are overlooking the comprehensive Tutorials available in the SNA Network Implementation Guide. Since z/OS V1R6, the Enterprise Extender chapter has been available.
2. Notice the sections in the EE Chapter (Chapter 6) of the z/OS V1R11 Communications Server edition of the manual:
 1. Overview
 2. Designing the EE Network
 3. Configuring the EE Network
 4. Configuring the EE Connection Network
 5. EE Security Considerations
 6. Tuning the EE Network
 7. Advanced Coding considerations for EE
 8. Troubleshooting EE problems

Are You Looking for Tutorials on Sysplex Distributor?

● IP Configuration Guide (SC31-8777-09)



The screenshot shows a table of contents for the IP Configuration Guide. The items listed are:

- Figures
- Tables
- About this document
- Summary of changes
- Part 1. Base TCP/IP system
 - Chapter 1. Overview of z/OS Communications Server
 - Chapter 2. IP configuration overview
 - Chapter 3. Security
 - Chapter 4. Preparing for TCP/IP networking in a multilevel secure environment
 - Chapter 5. TCP/IP Customization
 - Chapter 6. Routing
 - Chapter 7. Virtual IP Addressing
 - Chapter 8. TCP/IP in a sysplex
- Connectivity in a sysplex
 - Sysplex subplexing
 - TCP/IP and VTAM subplex concepts and example
 - Setting up a subplex
 - Dynamic XCF
 - Getting started with dynamic XCF
 - JUTSAMEH
 - XCF
 - Examples of definitions generated by dynamic XCF
 - HiperSockets
 - Network interfaces monitoring
 - Sysplex problem detection and recovery
 - Problem detection
 - Recovery
 - Setting TMERSECS
 - Summary of problems monitored and actions taken
 - Target server connection setup responsiveness monitoring
- Workload balancing
 - Single systemwide image
 - Horizontal growth
 - Ease of management
 - Internal load balancing solutions
 - Sysplex-aware external load balancing solutions
 - External IP workload balancing solutions
 - Choosing a load balancing solution
- Part 2. Server applications

z/OS Communications Server



IP Configuration Guide

Version 1 Release 10

© Copyright IBM 2010

1. Implementers may be aware of the many Traffic Distribution presentations on the SHARE website (www.share.org) and on the IBM Techdocs website (www.ibm.com/support/techdocs), but too many people are overlooking the Tutorials available in the IP Configuration Guide.
2. Notice the sections in the Chapter on "TCP/IP in a Sysplex" (Chapter 8) of the z/OS V1R11 Communications Server edition of the manual:
 1. Connectivity in a Sysplex
 1. Sysplex Subplexing
 2. Dynamic XCF
 3. Network Interfaces Monitoring
 4. Sysplex Problem Detection and recovery
 5. Target Server connection setup responsiveness monitoring
 2. Workload Balancing
 1. Single Systemwide Image
 2. Horizontal Growth
 3. Ease of management
 4. Internal load balancing solutions
 5. Sysplex-aware external load balancing solutions
 6. Choosing a load balancing Solution

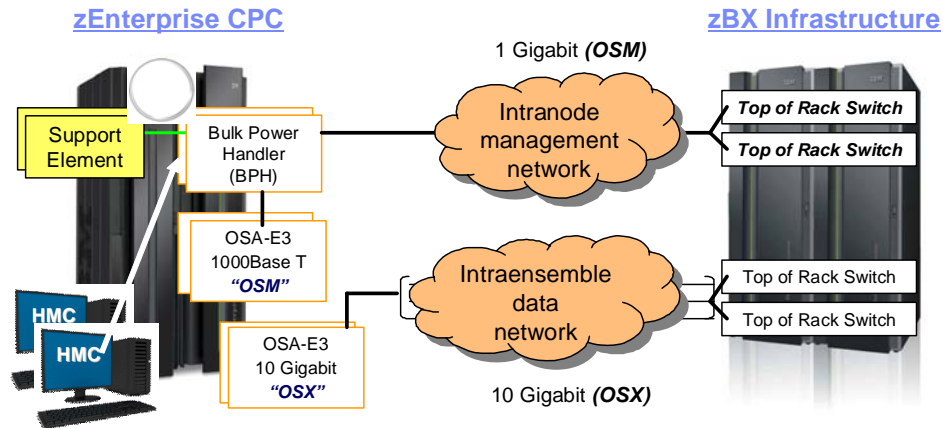
Gem Available Since V1R4 to Prepare
you for zEnterprise™ System and
z/OS V1R12



© Copyright IBM 2010

Overview of zEnterprise System and Ensemble Networking

Management Network: IPv6 only
 Implement it and then forget about it!
 Data Network: IPv4 or IPv6



- Intranode management network (INMN)
 - 1000Base-T OSA-Express3 (copper) --- QDIO (*CHPID Type OSM*) – Cables are 3.2 meters long from OSM to BPH in CEC and 26 meters from BPH to TOR
 - HMC security is implemented with standard practices **PLUS** additional security mechanisms:
 - > Isolated IPv6 network with “*link-local*” addresses only; authentication and authorization and access control, etc.
- Intraensemble data network (IEDN)
 - 10 Gigabit OSA-Express3 --- QDIO (*CHPID Type OSX*) – Cables are maximum of 26 meters long to TOR & 10km long-range
 - Security is implemented with standard practices **PLUS** additional security mechanisms: access control, authentication, authorization, application security, routing table restrictions, IP Filtering, etc.
 - Networks can be further isolated using VLAN and VMAC segmentation of the network connections

© Copyright IBM 2010

Since V1R4: Implement IPv6 Without Exploiting It!!

Effect of the IPv6 Addressing on a Participating z/OS Stack

1. Change to BPXPRMxx (UNIX member in PARMLIB)
2. Change to NETSTAT output
 - LONG for IPv6 (or mixed) output (SHORT not supported when IPv6 enabled.)
 - Must use NETSTAT ROUTE to see an IPv6 route
 - and not NETSTAT GATE, which sees only IPv4
 - No Message Identifiers in the LONG Format of TSO NETSTAT

LONG Format =
IPv6 or IPv4

```
D TCPIP,TCPIPT,N,HOME,FORMAT=LONG
EZZ0101I NETSTAT CS V1R10 TCPIPT 034
HOME ADDRESS LIST:
LINKNAME:  VLINK1
ADDRESS:   192.168.20.102
FLAGS:    PRIMARY
LINKNAME:  LGIG1F
ADDRESS:   192.168.20.92
FLAGS:
...
LINKNAME:  LOOPBACK
ADDRESS:   127.0.0.1
FLAGS:
LINKNAME:  LOOPBACK6
ADDRESS:   ::1
FLAGS:
7 OF 7 RECORDS DISPLAYED
END OF THE REPORT
```

SHORT Format
= IPv4 only

```
D TCPIP,TCPIPT,N,HOME
EZZ2500I NETSTAT CS V1R10 TCPIPT 021
HOME ADDRESS LIST:
ADDRESS          LINK          FLG
192.168.20.102  VLINK1        P
192.168.20.92   LGIG1F
10.1.1.2         EZASAMEMVS
...
127.0.0.1       LOOPBACK
6 OF 6 RECORDS DISPLAYED
END OF THE REPORT
```

Otherwise: IPv6 Usage is
Transparent



© Copyright IBM 2010

1. Even if you are not yet thinking of implementing an Ensemble Network, you should think about starting to use the LONG FORMAT of the NETSTAT OUTPUT in z/OS. You can define this as a default in the IPCONFIG statement of the TCP/IP Profile.
 1. The benefit is that you are positioning yourself for the change in the z/OS NETSTAT output displays which will occur once you enable the z/OS stack for dual-mode (i.e., IPv4 and IPv6). Once you implement IPv6 in z/OS, the LONG format of the display is the only one available.
2. Although INMN uses IPv6, the IPv6 usage in the INMN network is virtually transparent. IPv6 exploitation is unnecessary to create the Ensemble Environment.
3. You do not have to “learn” IPv6 to participate in an Ensemble. You only have to enable the stack to use IPv6, and there are only two changes you must make to do so: Implement IPv6 using definitions in SYS1.PARMLIB(BPXPRMnn) and then optionally change any automated processes you may have to issue and interpret NETSTAT commands to utilize the LONG format of the command. The FORMAT LONG is used to support longer IPv6 addresses. Therefore, LONG FORMAT is always used when IPv6 is enabled. FORMAT SHORT is not supported when IPv6 is enabled. FORMAT can be defined in the IPCONFIG statement of a z/OS TCP/IP stack and thus cause all netstat commands to adopt the LONG format in an IPv4-enabled implementation.
4. Most Netstat Output in a TCP/IP Stack on z/OS that is not enabled for IPv6 can be displayed with either the LONG or the SHORT format. If you have automated operations that are triggered by NETSTAT Short Format messages under TSO (and TSO only), be aware of the fact that NETSTAT in LONG format does not produce Message Identifiers. Under TSO, Netstat output displays in IPv4 can contain messages with the Prefix “EZZ” as with EZZ2761I. These “EZZ” messages do not appear with other forms of the Netstat output, as under UNIX or with the MVS “D TCPIP” variants of the Netstat command. Note that the Message Identifiers under TSO are displayed if the TSO user ID profiles are set to the value PROFILE MSGID and if the TCP/IP stack not enabled for IPv6 processing.
5. Note that “NETSTAT” is not regulated by standards; as a result each vendor platform can have a different implementation of the output displays for any of the netstat commands and options. Although you may have written shell scripts or Rexx programs to reformat output displays from a netstat command, every release of software or upgrade of an operating system can introduce changes that cause you to revisit your installation’s customized scripts to process netstat output. In other words, you are already familiar with this process of testing and possibly changing your customized scripts with every new release; the enablement of IPv6 is just another change that you must anticipate as usual. One of the benefits of the netstat display output on z/OS is that, even with an IPv4 network, you can still choose to begin displaying netstat output using the LONG format. This means, that even before a migration to ensemble networking (which will require IPv6 enablement), you can begin the process of modifying your customized scripts and your automated operations that may have been relying on message identifiers. If you have developed REXX programs that issue Netstat commands under TSO and parse the output lines based on message identifiers, you may need to change those REXX programs to use some other token in the output lines to decide the format of the line you are trying to parse.
6. NOTE on z/VM: z/VM handles the INMN requirement for IPv6 differently. VM only supports IPv6 on a layer 2 mode Virtual Switch. The main TCP/IP stack does not have to talk IPv6 to be part of an ensemble. Z/VM has another internal z/VM Stack that is used for OSM connectivity. The customer does not use this stack. The netstat output for the IEDN is thus either IPv4 or IPv6, depending on whether the main stack is communicating using IPv6 or not. The customer will not have to configure this stack when Ensemble Managed.

Gems in Netstat



© Copyright IBM 2010

Configurable Maximum for D TCPIP,,NETSTAT MVS (V1R10)

- Provide a configurable maximum for records displayed by a D TCPIP,,NETSTAT MVS console command

- Remember that the maximum value denotes number of records, not number of lines written to the console - these six lines count as two records:

```
SNTPD      0000001B UDP
LOCAL SOCKET:  0.0.0.0..123
FOREIGN SOCKET: *.*
SNTPD      0000001C UDP
LOCAL SOCKET:  :::123 (IPV6_ONLY)
FOREIGN SOCKET: *.*
```

- Default maximum remains 100
- Can be changed via new GLOBALCONFIG MAXRECS statement
 - Maximum can either be * - no maximum
 - Any value between 1 and 65535
- If the number of lines displayed as the result of a D TCPIP,,NETSTAT console command exceeds 65535 before MAXRECS is hit, an error message will be issued (instead of an abend D23)

NETSTAT ALL Is Available on MVS Console (V1R10)

- **With this new configuration support available, we add**
 - **D TCPIP,,NETSTAT,ALL** MVS console command support for the NETSTAT ALL report
 - This report can produce significant amounts of output if it is used without filters

```
                .--MAXRECS 100 -----.  
>>-GLOBALCONFig-----+-----+-----<<  
                '-+-MAXRECS * -----+-'  
                '-MAXRECS recs -'
```

- **Provide a configurable maximum for records displayed by a D TCPIP,,NETSTAT MVS console command**
 - Can be changed via new GLOBALCONFIG MAXRECS statement
 - Maximum can either be * - no maximum
 - Any value between 1 and 65535
 - If the number of lines displayed as the result of a D TCPIP,,NETSTAT console command exceeds 65535 before MAXRECS it hit, an error message will be issued (instead of an abend D23)

© Copyright IBM 2010

1. If you use automation programs which process MVS operator command output, and you want these programs to process detailed TCP connection and UDP endpoint data, you can update the programs to invoke the DISPLAY TCPIP,,NETSTAT command with the ALL option.
2. You should also update the programs to detect the new report output line which indicates that the report has been truncated:
 1. REPORT TRUNCATED DUE TO GREATER THAN 65533 LINES OF OUTPUT
3. By checking for this output line, the program will know when the report output is incomplete.

APPLDATA on the NETSTAT Command (V1R9, V1R10)

From MVS Console, TSO, UNIX

- Display TCPIP,,Netstat,ALLConn,APPLDATA<,filter>
- Display TCPIP,,Netstat,Conn,APPLDATA<,filter>
 - Includes APPLDATA in report if present
- Display TCPIP,,Netstat,ALLConn,APPLD=xx?xx*
- Display TCPIP,,Netstat,Conn,APPLD=xx?xx*
 - Includes APPLDATA in report
 - Limited to connections with matching APPLDATA
 - Case insensitive search
 - Wildcards are supported:
 - ? Exactly one arbitrary character
 - * Zero or more arbitrary characters

V1R9: Exploited by CICS Sockets and TN3270

V1R10: Exploited by FTP Client and Server

© Copyright IBM 2010

1. APPLDATA is available for TCP applications if they are instrumented to exploit it. Network Management Interface applications may also choose to exploit this capability.
2. Applications may place non-printable characters in the string. Netstat will display them as '.'. Only printable characters may be entered in Netstat filters. Nonprintable characters must be skipped over with wild card characters in the filter.
3. This support was rolled back to V1R7 and V1R8 at the request of other IBM applications that are interested in exploiting it.
4. For CICS, the support provides the ability to:
 1. identify TCP connections for IP CICS Socket applications:
 1. Listener, child server, and client transactions
5. IOCTL or ioctl()
6. z/OS TCP APIs supported
 1. Macro – EZASMI
 1. Assembler programs
 2. CALL instruction – EZASOKET
 1. Assembler, COBOL or PL/1 programs
 1. – Batch, CICS or IMS applications
 3. IP CICS C socket library stubs
 1. C programs
 4. IP REXX Socket library
 1. EXECs

Netstat ALL: Displaying Sockets Storage Usage (V1R9)

```
Client Name: TCPCS Client Id: 0000000C
Local Socket: 9.67.115.5..23 Foreign Socket: 9.27.11.182..4665
Last Touched: 16:46:15 State: Establish
BytesIn: 0000001062 BytesOut: 0000000480
...
ReceiveDataQueued: 000000002C
OldQDate: 09/15/06 OldQTime: 03:36:32
SendDataQueued: 000002C000
OldQDate: 09/15/06 OldQTime: 03:36:32
```

- CSM Storage:
 - Held in ECSA/Dataspace and is used to store data waiting to be read by an Application.
- ECSA:
 - TCP control blocks reference the data stored in CSM
 - An application (local or remote) may have a problem reading its data causing CSM and ECSA storage growth

© Copyright IBM 2010

1. For each TCP connection TCPIP maintains a send and receive buffer. The size used is specified on the TCPCONFIG parameters TCPCVBufSize and TCPSENDBfrsize or overridden by the application by using the SO_SNDBUF and SO_RCVBUF options in a SetSocketopt command.
2. If TCPIP is unable to immediately send the data when asked by the application (usually because the remote side has lowered their window size) then TCPIP will hold the data on the send queue. Once the queue reaches the send buffer size then TCPIP will not honor any additional send requests from the application on that connection until TCPIP is able to send some of the data already waiting on the send queue.
3. For each UDP socket TCPIP does not queue send data but will queue up received data waiting for the application to read it. The only limit on how much received data can be queued is by specifying UDPQUEUELIMIT on the UDPCONFIG statement, otherwise there is no limit on how much can be queued.
4. For both UDP sockets and TCP connections the message data is stored in CSM buffers. These may be in either ECSA or dataspace. Each message also has a control block structure that points to the message and contains information about the message and queue pointers. This control block is stored in ECSA.
5. TCPIP related ECSA and CSM storage growth may be attributed to application problems. A problem application may have stopped issuing reads for data for some reason or may be running too slowly to keep up with the speed that data is being received from it's remote partner. This can occur on either side of the connection and either can affect storage build up on z/OS TCPIP.
6. NETSTAT ALL: Additional messages have been added to the TCP connection and UDP socket information to specifically list receive and send queue data byte counts and the date and time of the oldest messages on these queues. For UDP sockets TCPIP maintains a count of the number of messages on the receive queue and this data is also now displayed.
7. If there is no data on a specific queue then the OldQDate and OldQTime message will not be displayed for that queue.
8. EXPLANATION OF SELECTED FIELDS FOR TCP CONNECTIONS:
9. FOR TCP CONNECTIONS:
 1. ReceiveDataQueued
 1. The number of bytes of data on the receive queue from the remote application yet to be read. The amount of data queued can be up to 2 times the ReceiveBufferSize. When it is not zero, the following information is displayed:
 1. OldQDate: The date of the oldest data on the receive queue.
 2. OldQTime: The time of the oldest data on the receive queue.
 2. The ReceiveDataQueued information is not displayed for a connection that is in LISTEN state.

Netstat Dev or Netstat Home: INTFNAME Filter (V1R10)

```
Home address list:
Address          Link           Flg
-----          ----           ---
192.168.115.5   OSAQDIOLINK   P
192.168.113.11 TR1
201.2.10.31     VIPLC9020A1F I
127.0.0.1       LOOPBACK

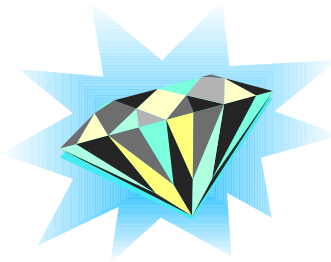
Address          Interface      Flg
-----          -
192.168.125.5   OSAQDIOINTF
```

- INTFNAME may specify the OSA Portname!
- You can see all associated INTERFACES connected to the same PORT.

© Copyright IBM 2010

1. This is an example of the Netstat H0me/-h report from an IPv4-only TCP/IP stack.
2. This report displays the IPv4 home addresses defined with an INTERFACE statement separately from the others.

Gems with Interfaces and LANs



© Copyright IBM 2010

Convert DEVICE/LINK Definitions of QDIO to INTERFACE Statement

```
>>_INTERFace_intf_name_DEFINE_IPAQENET_ Interface Definition |____><
|_DELETE_
Interface Definition:
|_PORTNAME portname_ IPADDR_ ipv4_address_ /0_>
|_NONRouter_ READSTORAGE GLOBAL_ _INBPERF BALANCED_>
>|_PRIRouter_ |_MTU num_|_VLANID id_|_READSTORAGE_MAX_|_INBPERF_DYNAMIC_|_IPBCAST_|
|_SECRouter_ |_AVG_|_MINCPU_|
|_MIN_|_MINLATENCY_|
>|_SECCLASS 255_|_NOMONSYSPLEX_|_NODYNVLANREG_|
|_SECCLASS security_class_|_MONSYSPLEX_|_DYNVLANREG_|_ROUTEALL_|
|_VMAC_|_macaddr_|_ROUTECL_|
```

- **Complete definition in one statement**
 - No Home entry required because includes IP Address
 - No errors with subnet mask, because it is included
 - No errors with MTU, because it is included
- **SourceVIPA is directly tied to the interface if desirable**
- **Unnecessary gratuitous ARPs for VIPAs eliminated**
- **New messages for MTU conflicts with OMPROUTE configuration file**
- **Provides VIRTUALIZATION of the OSA Port into multiples with VLAN and VMAC**
- **No multiple VLAN with DEVICE/LINK**

© Copyright IBM 2010

1. ...OMPROUTE checks for mismatches with INTERFACE statement in stack profile
2. ... Issues new message
3. ... Uses value configured to OMPROUTE
4. EZZ8163I stack_name MTU value stack_val for interface differs from omproute_procname MTU value omproute_val
5. EZZ8164I stack_name subnet mask value stack_val for interface differs from omproute_procname subnet mask value omproute_val
6. If you define the OSA using DEVICE/LINK statements, then the stack will inform OSA to perform ARP processing for all VIPAs in the home list which can result in numerous unnecessary gratuitous ARPs for VIPAs in an interface takeover scenario.
7. However, if you use the IPv4 INTERFACE statement for IPAQENET, you can control this VIPA ARP processing by configuring a subnet mask for the OSA. If you specify a non-0 num_mask_bits value on the IPADDR parameter of the INTERFACE statement, then the stack will inform OSA to only perform ARP processing for a VIPA if the VIPA is configured in the same subnet as the OSA (as defined by the resulting subnet mask).

Example: INTERFACE for IPv4 (V1R10)

```
INTERFACE NSQDIO411 DEFINE IPAQENET
IPADDR 172.16.11.1/24
PORTNAME NSQDIO1
VLANID 411
MTU 1492
VMAC
SOURCEVIPAINTERFACE LVIPA1
;
; LVIPA1 is the name of a static VIPA
; from a previous LINK statement
;
INTERFACE NSQDIO412 DEFINE IPAQENET
IPADDR 172.16.12.1/24
PORTNAME NSQDIO1
VLANID 412
MTU 1492
VMAC
SOURCEVIPAINTERFACE LVIPA2
```

- **HOME eliminated:**
 - IPADDR
- **Subnet Mask in definition**
 - OMPROUTE conflicts detected
- **MTU in definition**
 - OMPROUTE conflicts detected
- **SOURCEVIPAINTERFACE in definition**
- **At V1R11, Optimized Latency Mode on an OSA-E3 takes effect only if coded with**
 - INTERFACE
- **At V1R12, OSX device is defined only with INTERFACE statement.**

© Copyright IBM 2010

1. This is an example of multiple VLAN definitions with two INTERFACE statements for IPAQENET. Each statement defines an IPv4 interface associated with the same OSA-Express port NSQDIO1. Each specifies a subnet mask of 24 bits ('FFFFFF00'x) and defines a unique subnet.
2. The statements contain different VLAN IDs, and each requests that OSA generate a virtual MAC address (and defaults to ROUTEALL). Each statement specifies the link_name of a static VIPA for the source VIPA function.
3. Because so many definitions that used to reside in the HOME list and in BSDROUTINGPARMS are now included in the INTERFACE definition, it is easier to add and delete interfaces dynamically without having to modify the HOME LIST>
 1. EZZ8163I stack_name MTU value stack_val for interface differs from omproute_procname MTU value omproute_val
 2. EZZ8164I stack_name subnet mask value stack_val for interface differs from omproute_procname subnet mask value omproute_val

Adjusting for Throughput & Latency on OSA Interfaces (1.11)

```
>>--LINK--link_name--IPAQENET--device_name-->>----->
                                         '-IPBCAST-'
--READSTORAGE GLOBAL---
>>----->
  '-VLANID --id-'   '-READSTORAGE--MAX--+'
                                     '+AVG+'
                                     '-MIN-'

--INBPERF BALANCED-----,   '-IFSPEED 100000000-'
>>----->
  '-INBPERF--DYNAMIC-----+'   '+IFSPEED ifspeed---+'
    '+MINCPU-----+'         '-IFHSPEED ifhspeed-'
    '-MINLATENCY-'

--SECCLASS 255-----,   --NOMONSYSPLEX-.
>>----->
  '-SECCLASS security_class-'   '-MONSYSPLEX---'

--NODYNVLANREG-.
>>----->
  '-DYNVLANREG---'
                                     |
                                     |   '-ROUTEALL-. |
                                     |   '-VMAC-----+'
                                     |   '-macaddr-'   '-ROUTECL-'
```

- On Device/Link
- On INTERFACE
- Recommend:
- "Dynamic"

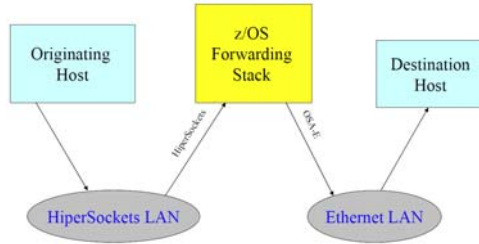
**Should see a significant throughput improvement for a single-session interactive workload
Some throughput improvement for multiplesession interactive workload
For streaming workloads the operating characteristics should be similar to the INBPERF
parameter value of BALANCED**

© Copyright IBM 2010

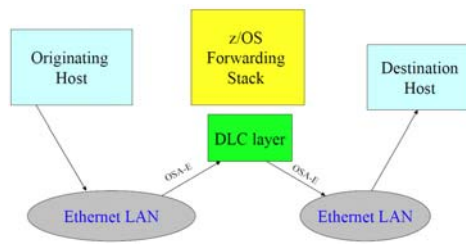
- LAN idle timer settings have contributed to network latency on zSeries
 - Even when the INBPERF parameter is specified with a value of MINLATENCY the permitted inter-packet gap is set to 20 microseconds
 - LAN idle timer settings are static and can not be changed unless the connection to OSA connection is terminated and reestablished.
- Performance studies have shown network latency improvements in environments where the CEC is under low utilization of up to 35% by tuning the Lan Idle timer within the OSA Express2 using a dynamic algorithm that takes workload characteristics. This dynamic algorithm involves taking the current default interpacket gap of 40 microseconds to as low as 1 microsecond.
- A new INBPERF parameter option of DYNAMIC will now be permitted. This new configurable setting allows the TCP/IP stack to dynamically calculate the best values for the LAN idle timer settings. These settings will indirectly determine how frequently the OSA adapter will interrupt the host for inbound traffic.
- New DYNAMIC option for the existing INBPERF parameter.
- INBPERF parameter can be specified on the OSAExpress QDIO LINK or INTERFACE statement.
- New option is valid for OSA-Express2 on an IBM System z9 EC or z9 BC with the corresponding Dynamic LAN Idle functional support
- When specified for an OSA-Express device that does not support this new function then the option of BALANCED will be used for INBPERF parameter.
- INBPERF
- An optional parameter indicating how frequently the adapter should interrupt the host for inbound traffic. There are three supported static settings (MINCPU, MINLATENCY, and BALANCED). The static settings use static interrupt timing values. The static values are not always optimal for all workload types or traffic patterns, and cannot account for changes in traffic patterns.
- There is also one supported dynamic (DYNAMIC) setting. This setting causes the host (stack) to dynamically adjust the timer-interrupt value while the device is active and in use. This function exploits an OSA hardware function called Dynamic LAN Idle. Unlike the static settings, the DYNAMIC setting reacts to changes in traffic patterns, and sets the interrupt-timing values at the point where throughput is maximized. The dynamic setting does not incur additional CPU consumption which might have been produced by using any of the static settings.
- Valid settings include:
 - DYNAMIC: The host to dynamically signals OSA to change the timer-interrupt value based on current inbound workload conditions. The DYNAMIC setting is effective only for Open Systems Adapter-Express2 on an IBM System z9 EC or z9 BC with the corresponding Dynamic LAN Idle functional support. See the 2094DEVICE Preventive Service Planning (PSP) and the 2096DEVICE Preventive Service Planning (PSP) buckets for further information about the level of Open Systems Adapter-Express2 that supports this function. When this setting is specified for a older Open Systems Adapter-Express, the stack reverts to using the BALANCED setting. The DYNAMIC setting should outperform the other three static settings for most workload mixes.
- MINCPU
- This setting uses a static interrupt-timing value, selected to minimize host interrupts without regard to throughput. This mode of operation might result in minor queueing delays (latency) for packets into the host, which is not optimal for workloads with demanding latency requirements.
- MINLATENCY
- This setting uses a static interrupt-timing value, selected to minimize latency (delay), by more aggressively presenting received packets to the host. This mode of operation generally results in higher CPU consumption than the other three settings. Use this setting only if host CPU consumption is not an issue.
- BALANCED
- This setting uses a static interrupt-timing value, selected to achieve reasonably high throughput and reasonably low CPU consumption. This is currently the default value.

"Fast Path" Routing: QDIO Acceleration (V1R11)

Without Fast Path QDIO Acceleration



With Fast Path QDIO Acceleration

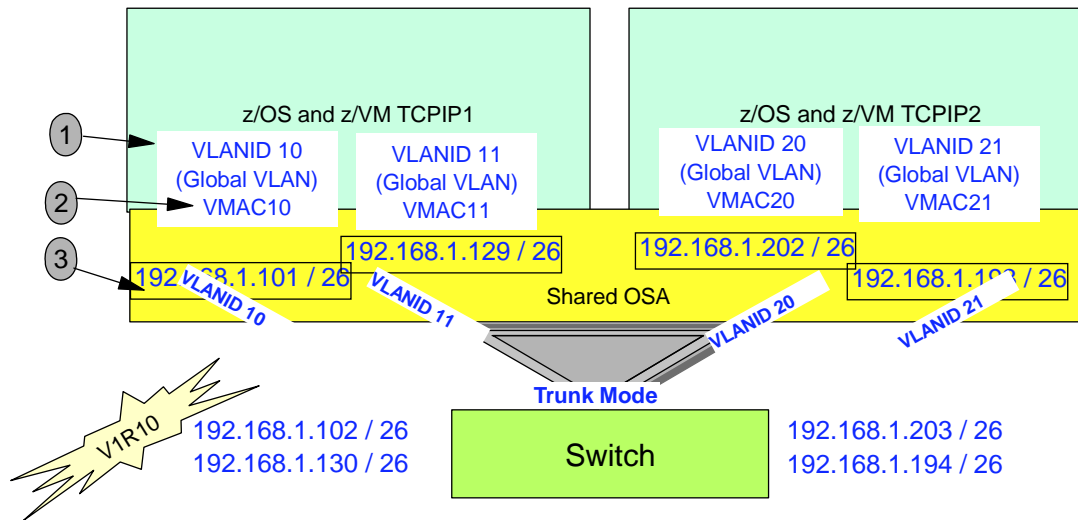


Function	IQDIOROUTING	QDIOACCELERATOR
OSA-E → HiperSockets	Yes	Yes
HiperSockets → OSA-E	Yes	Yes
OSA-E → OSA-E	No	Yes
HiperSockets → HiperSockets	No	Yes
Sysplex Distributor	No	Yes

© Copyright IBM 2010

1. A function called "IQDIORouting" was introduced in an earlier release of z/OS to provide a fast path for HiperSockets routing of packets. The new function introduced in V1R11 enhances the "fast path" architecture and has fewer restrictions than IQDIORouting.
2. QDIO Acceleration is a function that allows forwarding of IP Packets from one interface to another interface without having to pass through the upper layers of the TCP/IP protocol stack. It provides "fast path" IP forwarding.
 1. See the visuals to understand how routing looks without and then with QDIO Acceleration.
 2. See the table to understand to which interface flows QDIO Acceleration applies.
3. Requirement:
 1. IPConfig QDIOACCELERATOR is mutually exclusive with IQDIOROUTING
 2. Works with Unfragmented packets only
 3. IP Security cannot be enabled
 4. IP Forwarding should be enabled unless you want this function only for SD

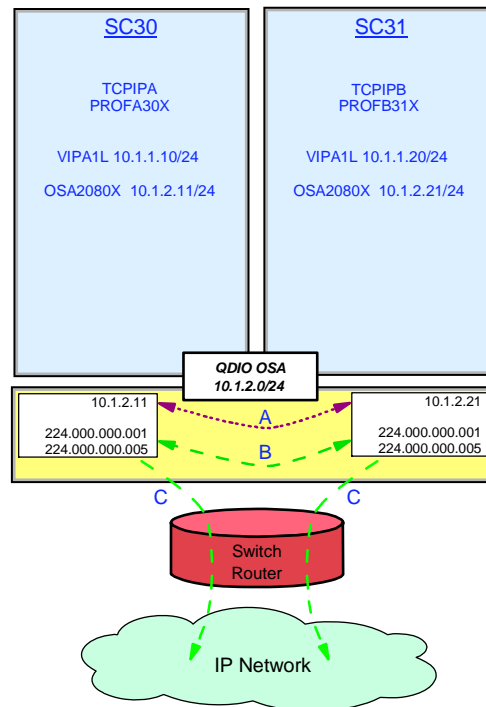
Multiple VLAN Support in z/OS CS V1R10: Shared OSA



- 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.

© Copyright IBM 2010

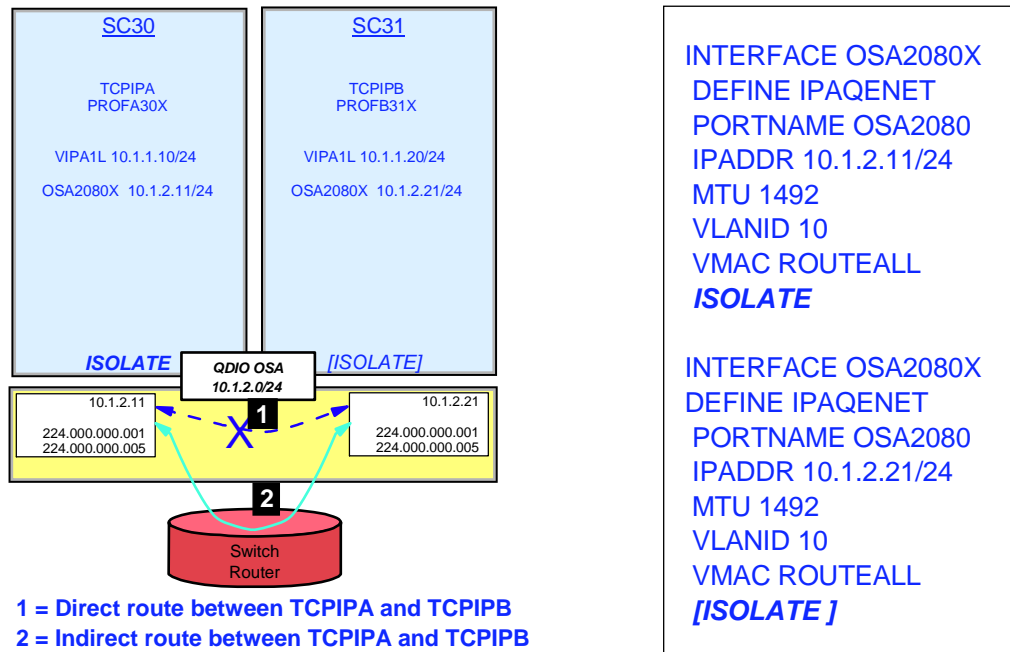
OSA Connection Isolation (1.11)



© Copyright IBM 2010

1. Another method available to isolate traffic across a shared OSA port is OSA Connection Isolation. This method can be deployed with or without out assigning a VLAN ID or a VMAC to the OSA port.
2. Many customers share OSA-Express ports across logical partitions, especially if capacity is not an issue. Each stack sharing the OSA port registers certain IP addresses and multicast groups with the OSA.
3. For performance reasons, the OSA-Express bypasses the LAN and routes packets directly between the stacks when possible.
4. For unicast packets, OSA internally routes the packet when the next-hop IP address is registered on the same LAN or VLAN by another stack sharing the OSA port.
 1. A: You see how TCPIPA routes a packet to 10.1.2.21 in TCPIPB over the OSA port without exiting out onto the LAN because the next hop to reach the destination is registered in the OSA Address Table (OAT); the TCPIPA routing table indicates that the destination can be reached by hopping through the direct connection to the 10.1.2.0/24 network.
 2. B For multicast (e.g., OSPF protocol packets), OSA internally routes the packet to all sharing stacks on the same LAN or VLAN which registered the multicast group. Note how TCPIPA and TCPIPB have each registered multicast addresses for OSP (224.000.000.00n) in the OSA port.
 3. C OSA also sends the multicast/broadcast packet to the LAN. For broadcast (not depicted), OSA internally routes the packet to all sharing stacks on the same LAN or VLAN.
5. Some customers express concerns about this efficient communication path and wish to disable it; they may wish to disable the function because traffic flowing internally through the OSA adapter bypasses any security features implemented on the external LAN

OSA Connection Isolation (1.11)



© Copyright IBM 2010

- Some environments require strict controls for routing data traffic between servers or nodes. In certain cases, the LPAR-to-LPAR capability of a shared OSA port can prevent such controls from being enforced. For example, you may need to ensure that traffic flowing through the OSA adapter does not bypass firewalls or intrusion detection systems implemented on the external LAN. We have described several ways to isolate traffic from different LPARs on a shared OSA port, with one of these methods being OSA Connection Isolation.
- The feature is called OSA Connection Isolation in z/OS, but it is also available in z/VM, where it is called QDIO data connection isolation or VSWITCH port isolation. It allows you to disable the internal routing on a QDIO connection basis, providing a means for creating security zones and preventing network traffic between the zones. It also provides extra assurance against a misconfiguration that might otherwise allow such traffic to flow as in the case of an incorrectly defined IP filter. With interface isolation, internal routing can be controlled on an LPAR basis. When interface isolation is enabled, the OSA will discard any packets destined for a z/OS LPAR that is registered in the OAT as isolated.
- QDIO interface isolation is supported by Communications Server for z/OS V1R11 and all OSA-Express3 and OSA-Express2 features on System z10, and by all OSA-Express2 features on System z9, with an MCL update. Refer to the appropriate Preventive Service Planning bucket for details regarding your System z server.
- Coding ISOLATE on your INTERFACE statement enables the function. It tells the OSA-Express not to allow communications to this stack other than over the LAN.
 - As the visual depicts, the ISOLATE parameter is available only on the INTERFACE statement. To eliminate the direct path through the OSA between the two depicted LPARs, you need code ISOLATE on only one of the two INTERFACES. We have coded it on both in order to assure, that if any other LPAR starts sharing the OSA port, that other LPAR cannot use the direct path to communicate even with TCPIPB..
- If you attempt to code ISOLATE on an INTERFACE that does not support the ISOLATE function, you receive a message:
 - EZD0022I INTERFACE OSA2080X DOES NOT SUPPORT THE ISOLATE FUNCTION
- Dynamic routing protocol implementations with RIP or OSPF require careful planning on LANs where OSA-Express connection isolation is in effect; the dynamic routing protocol learns of the existence of the direct path but is unaware of the isolated configuration, which renders the direct path across the OSA port to the registered target unusable. If the direct path that is operating as ISOLATED is selected, you will experience routing failures.
- If the visibility of such errors is undesirable, you can take other measures to avoid the failure messages. If you are simply attempting to bypass the direct route in favor of another, indirect route, you can accomplish this as well with some thoughtful design.
- For example, you might purposely bypass the direct path by using Policy Based Routing (PBR) or by coding static routes that supersede the routes learned by the dynamic routing protocol. You might adjust the weights of connections to favor alternate interfaces over the interfaces that have been coded with ISOLATE.
- If, however, TCPIPA and TCPIPB do need to exchange information, you will need to deploy an effective route that bypasses the direct route between them. Therefore, at TCPIPA you might add a non-replaceable static route to an IP address in TCPIPB; the static route in the BEGINROUTES block points to the next-hop router on the path indicated with (2) in the visual.

OSA Connection Isolation (1.11)

```
*****
*** OSA/SF Get OAT output created 10:46:14 on 09/23/2009 ***
*** IOACMD APAR level - OA26486 ***
*** Host APAR level - OA26486 ***
*****
*** Start of OSA address table for CHPID 02 ***
*****
* UA(Dev) Mode Port Entry specific information Entry Valid
*****
Image 2.3 (A23 ) CULA 0
80(2080)* MPC N/A OSA2080 (QDIO control) SIU ALL
82(2082) MPC 00 No4 No6 OSA2080 (QDIO data) Isolated SIU ALL
VLAN 10 (IPv4)

Group Address Multicast Address
01005E000001 224.000.000.001
01005E000005 224.000.000.005

VMAC IP address
HOME 020010749925 010.001.002.011

83(2083) MPC 00 No4 No6 OSA2080 (QDIO data) S ALL

...

```

© Copyright IBM 2010

1. Even the OSA/SF display shows where ISOLATE is enabled, as you can see from the display.

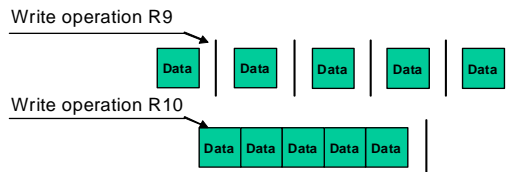
HiperSockets Multiple Write and zIIP Offload (V1R10)

TCP/IP Profile

GLOBALCONFIG IQDMULTIWRITE ZIIP IQDIOMULTIWRITE

IBM System z10 EC Hipersockets Multiple Write Facility

- Hipersockets can now move multiple output data buffers in one write operation
 - Reduces CPU utilization
 - For large outbound messages
 - Used when message spans Hipersocket frame size




© Copyright IBM 2010

1. The newly announced IBM System z10 includes a new function called HiperSockets Multiple Write. This allows multiple data buffers to be moved from one system image to another across HiperSockets with one operation. This can reduce CPU utilization.
2. When enabled, HiperSockets Multiple Write will be used anytime a message spans the HiperSockets frame size, thus requiring multiple output buffers to transfer the message. Therefore, it will only be used for larger outbound messages. Spanning multiple output data buffers can be affected by a number of factors including:
 1. Hipersocket frame size
 2. Application socket send size
 3. TCP send size
 4. MTU size
3. SUMMARY: HiperSockets Multiple Write
 1. Requirements
 1. • IBM System z10
 2. Restrictions
 1. • Unsupported if z/OS is running as a guest in a z/VM environment.
 2. • Supported for large outbound messages only
4. SUMMARY: .. zIIP-Assisted HiperSockets Multiple Write
 1. Requirements
 1. • HiperSockets Multiple Write must be enabled
 2. Restrictions
 1. • Will only be used for large outbound TCP messages (that originate in this host).

Enabling HiperSockets Multiple Write and zIIP Offload (V1R10)

● Enabling HiperSockets Multiple Write on Globalconfig:

```
>>-GLOBALCONFig----->
>--+-----+-----><
| +-NOIQDMULTIWRITE----- |
+-|-----+-----+
+--IQDMULTIWRITE-----+
```



● Enabling HiperSockets Multiple Write with zIIP Offload:

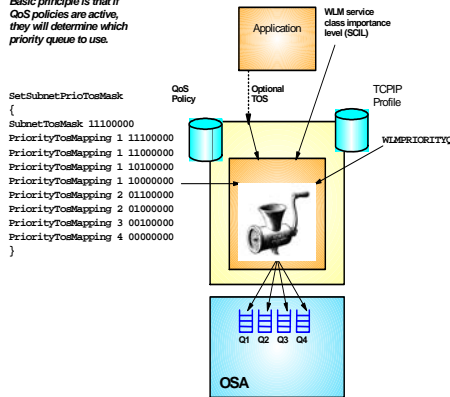
```
>>-GLOBALCONFig----->
.
.
>--+-----+-----><
| .NOIPSECURITY-. |
+ZIIP+-----+-----+
| 'IPSECURITY---' |
| .NOIQDIOMULTIWRITE-. |
+-----+
'IQDIOMULTIWRITE---'
..
```

© Copyright IBM 2010

1. With HiperSockets Multiple Write enabled you should see a performance improvement and reduction in CPU utilization for large outbound messages.
2. .. zIIP assist will also help reduce costs associated with general CPU utilization.
3. .. Both HiperSockets Multiple Write and zIIP-Assisted HiperSockets
4. Multiple Write are disabled by default. Enable them using the new options on the GLOBALCONFIG statement.
5. .. There are no WLM (enclave) configuration changes required.
6. .. The PROJECTCPU function in z/OS Workload Manager can be used to project zIIP effectiveness.

Exploiting QDIO Priority Queueing with WLM Service Classes (V1R11)

Basic principle is that if QoS policies are active, they will determine which priority queue to use.



```

policyRule telnetd # telnet traffic
{
  protocolNumberRange 6
  SourcePortRange 23
  policyActionReference interactive1
}

policyAction interactive1
{
  policyScope DataTraffic
  OutgoingTOS 10000000
}
    
```

10000000 Send on QDIO Q1

Disregarding SYSTEM (to which WLM PRIORITYQ will ALWAYS assign QDIO priority 1) these service classes are assigned control values

0. SYSSTC service class^r
1. User defined services classes with Importance level 1
2. User defined services classes with Importance level 2
3. User defined services classes with Importance level 3
4. User defined services classes with Importance level 4
5. User defined services classes with Importance level 5
6. User defined service classes associated with a Discretionary goal

WLM PRIORITYQ: YES
 IOPRI1 0
 IOPRI2 1
 IOPRI3 2 3
 IOPRI4 4 5 6 FWD

© Copyright IBM 2010

1. The QDIO OSAs are implemented with four internal queues. Outbound Data traffic is distributed over these four queues based upon a Quality of Service (QoS) definition that established Types of Service in the "Precedence Bits" of the IP Header. Most applications fail to establish these precedence bits; Enterprise Extender is an exception to this. Other applications are assigned precedence bits based upon a QoS policy that you may have defined with z/OSMF or with z/OS Configuration Assistant GUI and then installed with Policy Agent into the TCP/IP stack.
2. The first visual in the upper left shows you the four QDIO queues and shows you how different Types of Service are mapped within Policy Agent to distributed traffic outbound over each of the four queues.
3. The visual below the aforementioned visual shows you a sample policy that might be used to assign a high priority (TOS of 10000000) to Telnet traffic and therefore cause it to be dispatched on QDIO OSA Queue #1.
4. In general most shops do little to nothing to prioritize their OSA-Express outbound data, missing any benefits the prioritization provides
5. Beginning with V1R11, it is now possible to allow outbound traffic to be assigned precedence bits based upon WLM priorities and "Service Class Importance Levels."
 1. Since the WLM service classes should already be assigned to the jobs, all that needs to be done is to give the stack 'permission' to use it for prioritization.
 2. Defaults are provided that should give a good distribution of work across the priority queues.
 3. If QoS or the application has assigned an IPv4 ToS/IPv6 Traffic Class then enabling this function will only affect those packets assigned a ToS/Traffic Class value of zeros.
 4. Enterprise Extender always assigns a non-zero ToS/Traffic Class so unless it is changed to zero by QoS, Enterprise Extender traffic is not affected.
6. Therefore, with V1R11, all you need to do is enable the use of WLM Service Class important Level as a means of assigning traffic to the QDIO queues. You do this by enabling:
 1. IPCONFIG WLM PRIORITYQ (WLM PRIORITYQ: YES on a Netstat Config indicates WLM PRIORITYQ is enabled)
 1. If you do not want to accept the default queueing, you may override it with a parameter of IOPRI n. Below you see the default settings for IOPRI n when you specify WLM: PRIORITYQ by itself on the IPCONFIG statement.
 2. IOPRI1 0 OSA-Express priority queue 1 is used for packets from jobs with a control value 0 (SYSSTC)
 3. IOPRI2 1 OSA-Express priority queue 2 is used for packets from jobs with a control value 1 (services classes with Importance level 1)
 4. IOPRI3 2 3 OSA-Express priority queue 3 is used for packets from jobs with control values 2 and 3 (services classes with Importance levels 2 and 3)
 5. IOPRI4 4 5 6 FWD OSA-Express priority queue 4 is used for packets from jobs with control values 4, 5, and 6 (services classes with Importance levels 4 and 5 and discretionary) as are all non-accelerated forwarded packets
7. Points to remember:
 1. WLM PRIORITYQ has little effect unless there is enough traffic to cause contention for the OSA-Express resources
 2. WLM PRIORITYQ has no effect unless packet IPv4 ToS/IPv6 Traffic Class is zeros. This is typically the case if you have not defined a network QoS policy
 3. WLM PRIORITYQ does not affect accelerated packet priority.

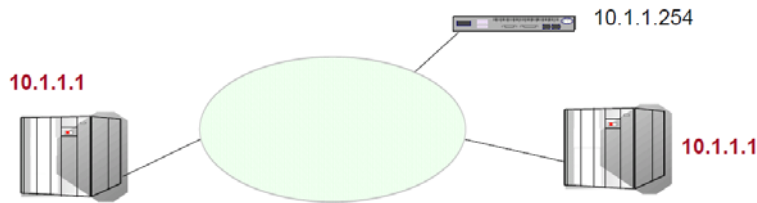
Gems with Routing



© Copyright IBM 2010

OSPF Detection of Duplicate RouterID (V1R11)

EZZ8165I DUPLICATE IPV4 OSPF ROUTER ID 10.2.3.4 DETECTED

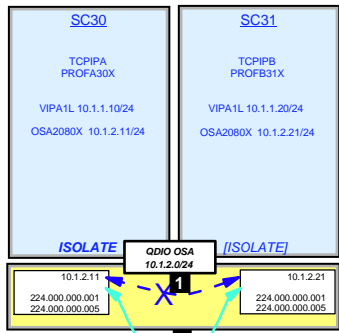


- If multiple OSPF routers use the same router ID, routing problems will occur:
 - Routes are continuously added and deleted by neighboring routers
 - Increased OSPF traffic as designated router floods new LSAs
 - Packet loss or connectivity loss depending upon routing environment
 - Problem can be difficult to diagnose due to varied symptoms
- New Console Message to identify the situation, allowing for correction by System z Networking System Programmer.

© Copyright IBM 2010

1. Although router IDs should be unique, sometimes multiple OSPF routers are configured with the same router ID. This will cause routing problems.
2. The designated router is getting router LSAs from each router with different information. The router will update its routing table and then flood the updated LSAs to other routers in the area.
3. This will cause routes to cycle from active to non-active states, or be constantly added then deleted from the network topography, causing excessive network disruption. Packets can be lost in a routing loop or dropped as these routes consistently change. This can cause intermittent ping timeouts or poor performance on connections. The symptoms will stop if the duplicate router is stopped. This type of problem can be difficult to diagnose.
4. The picture shows three OSPF routers, however two of them are using the same router ID.
5. In V1R11 OMPROUTE will issue message EZZ8165I when OSPF packets are received from a adjacent router with the same router ID OMPROUTE is using. EZZ8165I is issued to the console once every 10 minutes per OSPF version. So, if a router is using the same router ID for both IPv4 and IPv6 OSPF, message EZZ8165I is issued twice.
6. Message EZZ8165I only detects this situation has occurred. Unfortunately, OMPROUTE can't resolve this problem dynamically. The first step is to verify the router ID being used by this OMPROUTE is correct. If the router ID in message EZZ8165I is not the expected router ID, the configuration needs to be verified. OMPROUTE should be configured with a router ID, so the same router ID is used by this OMPROUTE instance. The router ID should not be a DVIPA address, as this address can be active on multiple TCPIP stacks. Message EZZ8134I should have been issue when OMPROUTE started if a DVIPA address had been used. If the router ID in message EZZ8165I is correct for OMPROUTE, someone else in the OSPF autonomous system is incorrectly using the router ID. The designated router should be checked first, using neighbor displays. You are trying to correlate the router ID with an interface address to determine which router is incorrectly using the router ID. A packet trace or sniffer trace can also be used to find the IP address. Once the router has been identified, the router can be configured with the correct router ID.

OSA Connection Isolation: Dynamic Routing Considerations (1.11)



1 = Direct route between TCPIPA and TCPIPB
2 = Indirect route between TCPIPA and TCPIPB

- Combine OMPROUTE with Static Routes to bypass direct routing through OSA port.

```

;TCPIPA.TCPPARMS(ROUTA30X)
;AUTOLOG LIST: INITIALIZE OMPROUTE
...
BEGINRoutes
; Direct Routes - Routes directly connected to my interfaces
; Destination Subnet Mask First Hop Link Name Packet Size
ROUTE 10.1.2.0/24 10.1.2.240 OSA2080X mtu 1492
ROUTE 10.1.1.0/24 10.1.2.240 OSA2080X mtu 1492
ROUTE 10.1.1.20/32 10.1.2.240 OSA2080X mtu 1492
ENDRoutes
    
```

```

;TCPIPB.TCPPARMS(ROUTB31X)
;AUTOLOG LIST: INITIALIZE OMPROUTE
...
BEGINRoutes
; Direct Routes - Routes directly connected to my interfaces
; Destination Subnet Mask First Hop Link Name Packet Size
;
ROUTE 10.1.2.0/24 10.1.2.240 OSA2080X mtu 1492
ROUTE 10.1.1.0/24 10.1.2.240 OSA2080X mtu 1492
ROUTE 10.1.1.10/32 10.1.2.240 OSA2080X mtu 1492
ENDRoutes
    
```

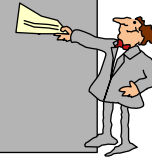
© Copyright IBM 2010

1. Some environments require strict controls for routing data traffic between servers or nodes. In certain cases, the LPAR-to-LPAR capability of a shared OSA port can prevent such controls from being enforced. For example, you may need to ensure that traffic flowing through the OSA adapter does not bypass firewalls or intrusion detection systems implemented on the external LAN. We have described several ways to isolate traffic from different LPARs on a shared OSA port, with one of these methods being OSA Connection Isolation.
2. The feature is called OSA Connection Isolation in z/OS, but it is also available in z/VM, where it is called QDIO data connection isolation or VSWITCH port isolation. It allows you to disable the internal routing on a QDIO connection basis, providing a means for creating security zones and preventing network traffic between the zones. It also provides extra assurance against a misconfiguration that might otherwise allow such traffic to flow as in the case of an incorrectly defined IP filter. With interface isolation, internal routing can be controlled on an LPAR basis. When interface isolation is enabled, the OSA will discard any packets destined for a z/OS LPAR that is registered in the OAT as isolated.
3. QDIO interface isolation is supported by Communications Server for z/OS V1R11 and all OSA-Express3 and OSA-Express2 features on System z10, and by all OSA-Express2 features on System z9, with an MCL update. Refer to the appropriate Preventive Service Planning bucket for details regarding your System z server.
4. Coding ISOLATE on your INTERFACE statement enables the function. It tells the OSA-Express not to allow communications to this stack other than over the LAN.
 1. As the visual depicts, the ISOLATE parameter is available only on the INTERFACE statement. To eliminate the direct path through the OSA between the two eepcited LPARs, you need code ISOLATE on only one of the two INTERFACES. We have coded it on both in order to assure, that if any other LPAR starts sharing the OSA port, that other LPAR cannot use the direct path to communicate even with TCPIPB..
5. If you attempt to code ISOLATE on an INTERFACE that does not support the ISOLATE function, you receive a message:
 1. EZD0022I INTERFACE OSA2080X DOES NOT SUPPORT THE ISOLATE FUNCTION
6. Dynamic routing protocol implementations with RIP or OSPF require careful planning on LANs where OSA-Express connection isolation is in effect; the dynamic routing protocol learns of the existence of the direct path but is unaware of the isolated configuration, which renders the direct path across the OSA port to the registered target unusable. If the direct path that is operating as ISOLATED is selected, you will experience routing failures.
7. If the visibility of such errors is undesirable, you can take other measures to avoid the failure messages. If you are simply attempting to bypass the direct route in favor of another, indirect route, you can accomplish this as well with some thoughtful design.
8. For example, you might purposely bypass the direct path by using Policy Based Routing (PBR) or by coding static routes that supersede the routes learned by the dynamic routing protocol. You might adjust the weights of connections to favor alternate interfaces over the interfaces that have been coded with ISOLATE.
9. If, however, TCPIPA and TCPIPB do need to exchange information, you will need to deploy an effective route that bypasses the direct route between them. Therefore, at TCPIPA you might add a non-replaceable static route to an IP address in TCPIPB; the static route in the BEGINROUTES block points to the next-hop router on the path indicated with (2) in the visual.
10. The effect of ICMP redirect packets: To avoid the override of the ICMP redirect packets that would most likely occur from the router to the originating host, you need to disable the receipt of ICMP redirects in the IP stacks or disable ICMP redirects at the router. If you are using OMPROUTE, ICMP redirects are automatically disabled, as evidenced by the message that appears during OMPROUTE initialization:
 1. EZZ7475I ICMP WILL IGNORE REDIRECTS DUE TO ROUTING APPLICATION BEING ACTIVE
11. The visual shows the coding for Static non-replaceable routes at TCPIPA and TCPIPB to override direct route through OSA port

OMPROUTE Initialization: Configuration DD Statement (V1R9)

```
//OMPROUTE PROC
//OMPROUTE EXEC PGM=OMPROUTE,REGION=4096K,TIME=NOLIMIT,
// PARM=('POSIX(ON)',
//   'ENVAR("_CEE_ENVFILE=DD:STDENV")/-t2 -d1') ★
★//OMPCFG DD DSN=USER1.OMPROUTE(&OMPCFG),DISP=SHR
★//STDENV DD DSN=USER1.OMPROUTE(OMPENV1),DISP=SHR
//SYSPRINT DD SYSOUT=*
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
//*SYSMDUMP DD
DSN=(USER1.OMPROUTE.DUMP),DISP=(NEW,DELETE,CATLG),
//* DCB=(RECFM=FBS,LRECL=4096,BLKSIZE=4096),
//* UNIT=SYSDA,SPACE=(CYL,(100,100),RLSE),VOL=SER=IPCS08
```

- ★ Be careful about leaving tracing and debugging on.
- ★ STDENV files must be VB
- ★ Specify OMPCFG DD card to identify the Configuration



© Copyright IBM 2010

1. Prior to z/OS V1R9 it was necessary for individual started procedures to be maintained for each OMPROUTE instance.
2. Both internal and external users have requested a way to specify an OMPROUTE configuration file name which includes an MVS system symbol in the started procedure for OMPROUTE, so that one started procedure could be shared by multiple OMPROUTE instances.
3. OMPROUTE now supports a DD:OMPCFG statement in its started procedure. This allows for MVS system symbols to be used in the name of the OMPROUTE configuration file, eliminating the necessity to maintain multiple OMPROUTE started procedures
4. As was the case prior to V1R9, beware of leaving Tracing and Debugging options active in a running OMPROUTE address space.
5. As was the case prior to V1R9, beware of specifying an OMPROUTE Environment file that is not a VB or HFS (zFS) file.
6. search order remains the same:
 1. a. DD:OMPCFG
 2. b. OMPROUTE_FILE environment variable
 3. c. /etc/omproute.conf
 4. d. hlq.ETC.OMPROUTE.CONF

System Symbols in OMPROUTE Configuration File (V1R9)

```
Routerid=1.1.1.&VIP A1
```

```
;  
OSPF_Interface  
IP_ADDRESS=10.10.10.&VIP A1  
SUBNET_MASK=255.255.255.0  
;  
; Where &VIP A1=1 in the IEASYMxx PARMLIB  
; member, the above translates to:  
; Routerid=1.1.1.1  
;  
OSPF_Interface  
IP_ADDRESS=10.10.10.1  
SUBNET_MASK=255.255.255.0
```

hlq.PARMLIB(IEASYMxx)

&VIP A1=1

- OMPROUTE supports MVS system symbols in its configuration files.
- To confirm correct parsing, use OMPROUTE output commands or enable -t2 -d1 in OMPROUTE initialization.

© Copyright IBM 2010

1. The ability to use the MVS system symbols in the OMPROUTE configuration file is nice in and of itself because now OMPROUTE configuration files can be shared
2. between OMPROUTE instances. It was possible to share configuration files between OMPROUTE configuration files between OMPROUTE instances prior to V1R9 by using wildcarding; however in an OSPF environment there was no way to wildcard the Routerid, so if you did share configuration files, there was no way to specify a unique routerid for each OMPROUTE instance.
3. If you need to see how a symbol was translated, turn on -t2 -d1 OMPROUTE trace and look for the text "Translated to". For each line that contained an MVS system symbol there will be a line in the trace file which shows to what the symbol was translated.

INCLUDE Statement for OMPROUTE Configuration File (V1R10)

```
AREA
AREA_NUMBER=1.1.1.1
STUB_AREA=NO;

INCLUDE /u/user1/omproute.conf
INCLUDE //'USER1.INC10'
Include //'USER1.&SYSNAME..OMP'

OSPF_INTERFACE
IP_ADDRESS=10.9.128.128
NAME=DUMMY_SASRVA2
SUBNET_MASK=255.255.255.240
ROUTER_PRIORITY=0
ATTACHES_TO_AREA=1.1.1.1;
```

● OMPROUTE "Include file":

- Easier to share common OMPROUTE definitions within a Sysplex

```
>> _____ <<
|_Include_ _//'fully qualified MVS dataset name' _ _|
|_/_file system absolute pathname_____|
```

© Copyright IBM 2010

1. Common configuration statements can be grouped into separate files and specified in the OMPROUTE configuration via the INCLUDE statement
2. Single, multiple, and nested INCLUDE statements can be used in configuring OMPROUTE
3. Rules:
 1. INCLUDE statement must be the only configuration statement on the line.
 2. INCLUDE statement must not end with semicolon.
 3. There must be no more than 10 nested INCLUDE statements.
 4. Static system symbols can be specified as part of the data set name.
 5. Only 1 INCLUDE statement can be specified per line, anything else that follows the statement will be ignored.
4. If a syntax error is encountered in the final version of the configuration file after INCLUDE file(s) were processed, use debug level d1 to print a copy of the expanded configuration file to your OMPROUTE trace.

Deleted Routes: D TCPIP,,OMP,RTTABLE,DELETED (V1R9)

- Display TCPIP,,OMP,RTTABLE,DELETED to see all deleted routes in OMPROUTE's main routing table

```
D TCPIP,TCPCS1,OMP,RTTABLE,DELETED
EZZ8137I IPV4 DELETED ROUTES 816
TYPE  DEST NET      MASK      COST    AGE    NEXT HOP
-----
DEL   10.11.0.0      FFFF0000  16      6      NONE
DEL   10.11.2.1      FFFFFFFF  16      5      NONE
DEL   10.61.0.2      FFFFFFFF  16      6      NONE
...
...
15 NETS DELETED, 2 NETS INACTIVE
```

© Copyright IBM 2010

1. This is an example of the output of the D TCPIP,OMP,RTTABLE,DELETED display.
2. The same information can be seen also in the F OMP,RTTABLE,DELETED display
3. In order to investigate deleted networks as indicated in OSPF RTTABLE display, it used to be necessary to run an OMPROUTE debug trace and analyze the EZZ8061I and EZZ7943I messages indicating each network as it is deleted, or to take a dump of the OMPROUTE address space and send it to support.

Locating Path MTU Bottleneck with "Ping" (V1R9)

```
>> _ping_ host_name_ ><
  [ Option ]
  -h
  -?
Option:
  <
  -A_ ipv4_
    | ipv6_ |
    | 1 |
  -c_
    | echo_ |
  -i interface_
    | 256 |
  -l_
    | bytes_ |
  -n
  -P_ yes_
    | ignore_ |
  -p tcpname_
  -s srcip_
  -t_ 10_
    | seconds_ |

>> _PING_ host_name_ ><
  [ Option ]
  Help
  ?
Option:
  <
  Addrtype_ ipv4_
    | ipv6_ |
  Count_ 1
  Intf interface_
  Length_ 256
  | bytes_ |
  NOName
  PMTU_ yes_
    | ignore_ |
  Srcip srcip_
  TCP tcpname_
  Timeout_ 10
    | seconds_ |
```

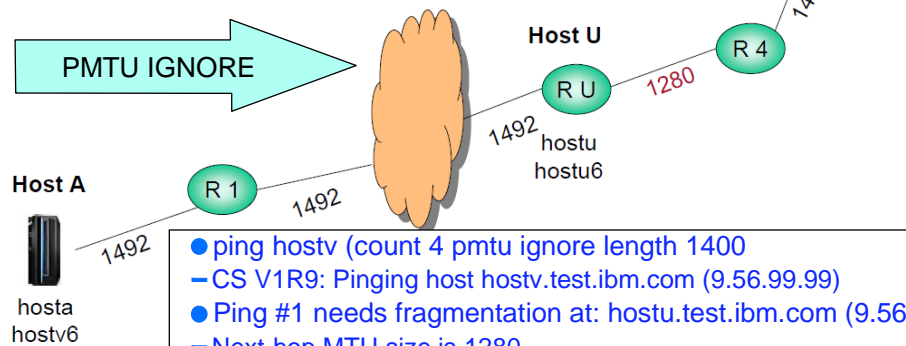
- **PMTU/-P ignore:** ignore the current cached path MTU discovery value for the destination host
 - Display of MTU problem location (even if PATH MTU in effect)
 - Displays host name and IP address where the outbound packet needs to be fragmented
 - Ping displays the next-hop MTU value
 - For IPv4, only available if detecting host supports RFC1191
- **NONAME/-n:** Specifies that the Ping command should not resolve IP addresses to host names. This saves a name server lookup.

© Copyright IBM 2010

1. MTU problems can exist in large networks. The problem occurs where the MTU for a segment of the network is smaller than the network segments to which it is connected.
2. Detecting MTU problems is difficult because, when the problem occurs, the IPv4 packets are normally fragmented. And z/OS CS currently does not provide any command to detect MTU problems.
3. Path MTU discovery support can help avoid fragmentation by determining the smallest MTU value for the path to a destination host. But it does not provide information about where the problem is located in the network.
4. IPv4
 1. Packets can be fragmented by any host
 2. Setting the "don't fragment" bit in the IP header prevents packet from being fragmented.
5. IPv6
 1. Packets only fragmented at sending host. Will not be fragmented by any intermediate hosts.
 2. Setting the IPV6_DONTFRAG socket option in the sending socket prevents the packet from being fragmented.
6. When an IPSec tunnel exists on the path to the destination host, you may need to issue the Ping command more than once to determine the network MTU value.
 1. If a network segment within the tunnel has a smaller MTU size than the Ping packet, the initial Ping commands will time out.
 2. The sending TCP/IP stack will fail the send of a later Ping echo request, and the Ping command will display the next-hop MTU size, based on the tunnel's MTU.
7. PMTU IGNORE is described in the visual.
8. PMTU YES means to honor the cached PMTU value. If path MTU discovery is enabled and has already determined an MTU value for the destination, and the length of the Ping echo request packet is larger than this MTU size, then the local TCP/IP stack does not send out the packet. In this case, The Ping command displays one of the local stack's IP addresses as the host address where fragmentation is needed, and the next-hop MTU value displayed by the Ping command is the current path MTU value to the destination.

Locating Path MTU Bottleneck with "Ping" (V1R9)

- For Ping from Host A to Host V, with a length of 1400,
 - Host U will send an ICMP "Needs Fragmentation" message, or ICMPv6 "Too Big" message to Host A
 - Ping on Host A will display Host U's host name, IP address, and the next-hop MTU size of 1280



- ping hostv (count 4 pmtu ignore length 1400)
 - CS V1R9: Pinging host hostv.test.ibm.com (9.56.99.99)
- Ping #1 needs fragmentation at: hostu.test.ibm.com (9.56.22.22)
 - Next-hop MTU size is 1280
- Ping #2 needs fragmentation at: hostu.test.ibm.com (9.56.22.22)
 - Next-hop MTU size is 1280
- Ping #3 needs fragmentation at: hostu.test.ibm.com (9.56.22.22)
 - Next-hop MTU size is 1280
- Ping #4 needs fragmentation at: hostu.test.ibm.com (9.56.22.22)
 - Next-hop MTU size is 1280

© Copyright IBM 2010

1. In this network, there is an MTU problem. To determine where the problem is, we can use the Ping command with the PMTU/-P parameter, so the outbound packets will not be fragmented. And since we suspect the problem is somewhere out in the network, we would specify IGNORE for the PMTU/-P parameter so that any path MTU value cached at Host A for destination Host V, would be ignored.
2. Since the packet data length is 1400, Host U could only forward the packet if it could fragment the packet. Instead Host U sends an ICMP or ICMPv6 error message back to Host A to indicate that the packet is too big and needs to be fragmented.
3. This example shows the output of the Ping command which was used to detect the network MTU problem in the network on the previous slide. We invoked the Ping command on Host A, with a destination host of Host V. Since we suspected that the problem was out in the network somewhere, we specified PMTU IGNORE so that the packet would be sent out, even if path MTU discovery had determined that the path MTU size was smaller than the length of 1400.
 1. The Ping responses show that the MTU problem is at Host U. And the next-hop MTU size from Host U to the network segment which leads to Host V is 1280.
4. Ping command times out or output appears incorrect: Remember MULTIPATH PERPACKET support uses smallest MTU of all equal-cost routes to destination

Gems with FTP



© Copyright IBM 2010

Restrict Non-TLS User Access to FTP Server 1.10

```
RDEFINE SERVAUTH EZB.FTP.MVS*.FTP*.PORT21 UACC(NONE)
PERMIT EZB.FTP.MVS*.FTP*.PORT21 CLASS(SERVAUTH) ACCESS(READ) ID(MARCELLO,SUSAN)
```

FTPROME

```
; FTP Server FTP.DATA (NO TLS)
```

```
VERIFYUSER TRUE
```



Sophia



Marcello

V1R10: SERVAUTH
for non-TLS

FTPMIAMI

```
; FTP Server FTP.DATA (TLS)
```

```
TLSMECHANISM      ATTLS
EXTENSIONS        AUTH_TLS
SECURE_CTRLCONN   PRIVATE
SECURE_DATACONN   CLEAR
SECURE_FTP        ALLOWED
SECURE_LOGIN      VERIFY_USER
SECURE_PASSWORD   REQUIRED
```



Susan



Fred

© Copyright IBM 2010

- By default, any user ID that is valid on the z/OS host can log into FTP. For security purposes, a customer may want to allow only certain user IDs to log into FTP on a certain host. z/OS FTP currently provides two ways to do this:
 - you can code and install the FTCHKPWD exit routine, or
 - you can configure TLS level 3 client authentication.
- The FTCHKPWD exit routine is code written by you which is invoked by the FTP server as part of validating the user ID used to log into FTP. The sample FTCHKPWD in SEZAINST shows one method of using an exit routine to control which user IDs are allowed to log into the FTP server.
- TLS level 3 client authentication adds a Security Access Facility (SAF) profile check to TLS level 2 client authentication. After configuring TLS level 2 client authentication, you can define a server port profile in the SERVAUTH class, and grant READ access to those user IDs you want to allow to log into the FTP server. FTP will verify each user ID logging in with TLS has at least READ access to the profile.
- If users log on using SSL/TLS with Client Authentication and the SECURE_LOGIN option is set to VERIFY_USER, the FTP server will check if the user has READ access to EZB.FTP.<systemname>.<ftpdaemonname>.PORTxxxx SERVAUTH resource. Client Authentication requires that the user present an x.509 client certificate.
- If users do not use SSL/TLS or the VERIFY_USER option isn't set as above, no checking of the SERVAUTH resource is done prior to V1R10
- Now with V1R10 we are giving installations an easy way to limit use of the FTP server functions in general without requiring TLS with Client Authentication:
 - Define the EZB.FTP.<systemname>.<ftpdaemonname>.PORTxxxx SERVAUTH SERVAUTH resource with universal access set to NONE
 - Permit those users who are allowed to use the FTP server with READ access to the SERVAUTH resource
- Note that if you code this statement in the server FTP.DATA: SECURE_LOGIN VERIFY_USER
 - And the session is TLS secured, FTP ignores the VERIFYUSER value and checks the server port profile before allowing the login.
- In the examples shown, Sophia is not allowed access to the non-TLS FTP server because of the SERVAUTH definitions depicted. Fred is not allowed access to the FTP server even if he has a client certificate, because he is also not authorized through the SERVAUTH definitions.

FTP Enhancements: Connection APPLDATA (V1R10)

```

/u/user1 netstat -G EZAFTP*
MVS TCP/IP NETSTAT CS V1R10 TCPIP Name: TCPCS 01:50:14
User Id Conn Local Socket Foreign Socket State
FTPD1 000000BC 1.2.5.36..20 1.2.5.36..1026 Establish
Application Data: EZAFTP0S D USER2 C PSSS
    
```

Offset	Description
1 – 8	The string "EZAFTP0S"
9	Blank
10	C for a control connection socket D for a data connection socket
11	Blank
12-20	User ID used to log into FTP
21	Blank
22	Security protection C for Clear; S for Safe; P for private; L for Clear but previously safe or private
...	More fields (see <i>IP Configuration Reference</i> for details)

- **z/OS CS V1R9: APPLDATA of 40 characters for a TCP sockets**
 - exploited by CICS, TN3270
- **V1R10: APPLDATA**
 - exploited by FTP Client and Server

© Copyright IBM 2010

1. This data is kept in the APPLDATA field of the socket. It can be set or updated by a TCP application using an IOCTL sockets call and can be included in NETSTAT ALL, ALLCONN, and CONN reports and used as a filter. This data also can be included in the NMI network monitor interface. The suggested syntax for the field is to use an eight-character application identifier in the first 8 characters of the 40-character APPLDATA field
2. In V1R9, this support is used by CICS Sockets to associate CICS-specific information with CICS sockets endpoints
3. For example: EZACICSO SRV1 0000123 USER1234 CICA
4. Also in V1R9, it is used by the TN3270 server to associate TN3270-specific information with TN3270 sockets endpoints
5. For example: EZBTNSRV TCPABC80 TSO10001 ET B
6. Now in V1R10, both the FTP client and the FTP server will associate FTP-specific information with the FTP sockets endpoints:
 1. FTP component (Client, Server, Daemon)
 2. Type of connection (Control or Data)
 3. User ID
 4. Security characteristics (SSL/TLS, GSSAPI, Ciphers, etc.)
 5. Info about file being transferred (direction, type, location)
7. z/OS V1R9 CS implemented support for TCP applications to associate up to 40 characters of application-specific data with a TCP socket:
 1. Can be set or updated by a TCP application using an IOCTL sockets call
 2. Is included in NETSTAT ALL, ALLCONN, and CONN reports and used as a filter
 3. Is included in the NMI network monitor interface
 4. Suggested format for the field is to use an eight-byte application identifier in the first 8 characters of the 40-character APPLDATA field
8. The string 'PSSS' for the server data socket is part of the other fields mentioned in the table. It indicates a PORT command established the connection; the transfer was inbound to the server, the file type was SEQ, and the file location was a sequential MVS data set.

FTP Batch, REXX, JAVA Client: API for FTP Return Codes (V1R8, V1R10)

In z/OS Communications Server V1R6 an Assembler, COBOL, and PL/I API was made available for the FTP client. It allows customers great flexibility in programming the FTP Client to transfer files. Batch files and REXX scripts could not retrieve return codes for conditional execution. So programs could not be made to logically change actions or tasks depending on the return values or data.

In V1R7, C and C++ were added. A sample is shipped in /usr/lpp/tcpip/samples/ftpcapic.c. Devised to be copied as a starting point for customer development. It shows compile options and linkage editor options to produce an actual program. The actual task of the sample program is to do a LIST subcommand of the /tmp directory and find the largest file in that directory. The hostname, userid and password are all defines at the top of the program. A return code check routine (check_interface_result) is provided which can be expanded by a customer. Provides a routine (print_output_lines) to print the data in the buffer provided by the FTP Client API.

In V1R8, REXX API was added. In V1R10, JAVA API was added.

© Copyright IBM 2010

Client FTP Data Specified at Client Invocation (V1R7-8)

```
ftp -r TLS -f "//sys1.cs.tcparms(ftpclsec)" -p TCPIPT -s 192.168.20.101 192.168.20.105
```

```
<_____>
>>_ftp_____>
|_ -a_ NEVER_ | | _21_ | | | |
| | GSSAPI_| | | foreign_host_| |
| | TLS_| | | port_number_|
|_ -d_ |
|_ -e_ |
|_ -f_ftpdata_|
|_ ...
```

"-f" Specifies the client FTP.DATA file. The parameter can be an HFS file, an MVS data set, or a DD name.

Provide command line parameter to specify FTP.DATA

No need to back up file or data set in search order

No need to back off file or data set to restore prior FTP.DATA

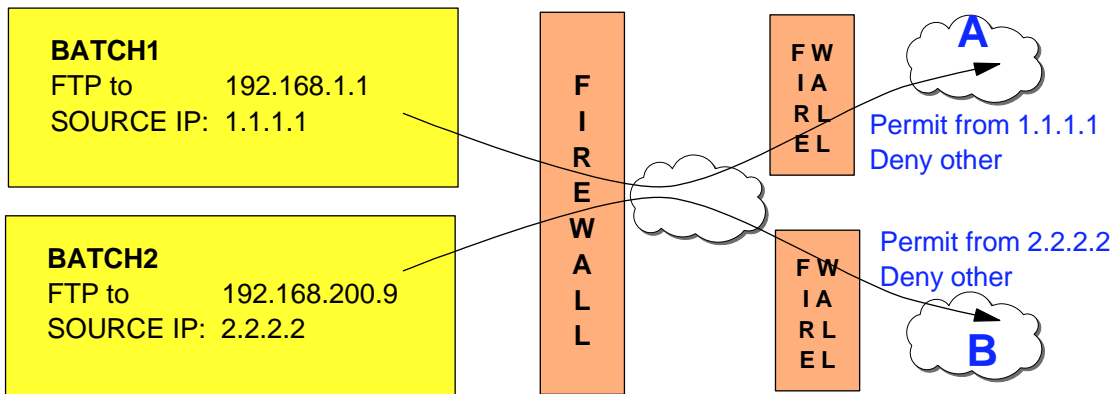
Easier to test changes to client FTP.DATA

© Copyright IBM 2010

Search Order for Client FTP Data

TSO Environment	z/OS Unix shell
0. -f parameter	0. -f parameter
1. SYSFTPD DD statement	1. \$HOME/ftp.data
2. tso_prefix.FTP.DATA	2. userid.FTP.DATA
3. userid.FTP.DATA	3. /etc/ftp.data
4. /etc/ftp.data	4. SYS1.TCPPARMS(FTPDATA) dataset
5. SYS1.TCPPARMS(FTPDATA) dataset	5. tcpip_hlq.FTP.DATA
6. tcpip_hlq.FTP.DATA	

Choosing FTP Client Source IP Address (V1R10)



```
>ftp -s 1.1.1.1 192.168.1.1
Using 'USER1.FTP.DATA' for local site configuration parameters.
IBM FTP CS V1R9
FTP: using TCP1A
Connecting to: mvs1.tcp.labs.ibm.com 192.168.1.1 port: 21.
220-FTPD1 IBM FTP CS V1R9 at mvs1.tcp.labs.ibm.com, 21:02:48 ...
220 Connection will not time out.
NAME (mvs1:USER1):
```

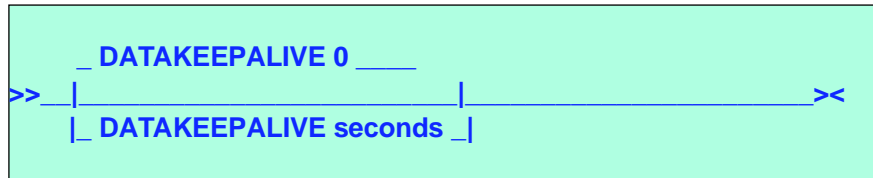
© Copyright IBM 2010

1. The TCP/IP stack determines the source IP address. This can be based on TCP/IP configuration options such as Job-Specific Source IP or it may be determined when the route to the FTP server is found.
2. In some situations the FTP client may want to use a different source IP address when connecting to different FTP servers.
3. In firewall configurations, it may be necessary to use a specific source IP address for the firewall to allow the connection.
4. But, there is no way for the FTP client, itself, to specify the source IP address that should be used.
5. This diagram shows an example of when the FTP client may want to specify the source IP address.
6. In the diagram, the customer has a network setup where the z/OS system running the FTP client has two interfaces into the network.
7. The customer needs to be able to FTP into two other networks which are protected by firewalls. The firewalls are configured to only allow connections from specific IP addresses.
8. So the only way to successfully FTP into "Customer A network", is to use a source IP address of 1.1.1.1 or into Customer B network is to use a source IP address of 2.2.2.2.
9. Since there is no way for the FTP client to specify a source IP address without this V1R9 improvement, there is no guarantee that the TCP/IP stack would choose the correct interface UNLESS you implement the SRCIP block in an appropriate manner.
10. Since there are two interfaces into the network the TCP/IP stack may choose either interface.

FTP KeepAlive (V1R10)

● FTP.DATA for both server and client

- Use the DATAKEEPALIVE statement to define the data connection keepalive timer.



SITE DATAKEEPALIVE=xxx

LOCSITE DATAKEEPALIVE=xxx

● DATAKEEPALIVE Parameters

- seconds The number of seconds of inactivity before a keepalive packet is sent out on the FTP data connection. The valid range is 0 (not used) through 86400 (24 hours). The default is 0.

● Usage Notes

- Specify 0 to use the keepalive interval specified in the TCP/IP stack.
- Specify 86400 to prevent any keepalive packet from being sent

© Copyright IBM 2010

1. Any TCP/IP connection is subject to monitoring by the network. The session may be canceled if no activity on the session is detected within a defined period of time as determined by the network device. Cancelling the session prevents any further communication between the session partners. In cancelling the session, the session partners may not be notified of this cancellation which can result in a hung session if the session partners do not provide for this situation.
2. To prevent cancellation, TCP/IP sends keepalive packets. A keepalive packet contains one byte of data and uses a sequence number of a packet that was already sent.
3. The remote session partner discards the data packet because they have already received the packet.
4. The benefit is that any device monitoring the session will detect that the session is active.
5. The FTP control connection is the connection over which FTP commands are sent from the client to the server. The keepalive interval can be customized by the KEEPALIVE statement in the FTP.DATA configuration file instead of utilizing the TCP/IP stack's keepalive interval.
6. The FTP data connection, over which file data flows during a file transfer between the client and server, does not support any customization of the keepalive interval.
7. This session is susceptible to being cancelled if the connection stays idle too long. A long running DB/2 query or a job submitted to JES that has not completed can cause this to occur.
8. While the TCP/IP stack provides the ability to configure when keepalive packets are generated, this interval may exceed that needed by FTP.
9. Without the ability to customize a keepalive interval on the FTP data connection, FTP must rely on the keepalive interval defined to the stack.
10. The FTP connection may be monitored by a device whose cancellation timer is less than the stack keepalive timer.
11. Each network has its specific needs and a single stack keepalive interval may not be able to cover all of these networks.
12. The value may be set through the SITE and LOCSITE commands as well.
13. **PASSIVE MODE:** When logging in from a non-z/OS FTP client to a z/OS FTP server and using passive mode, the SITE command is not supported by a non-z/OS client. Use the QUOTE SITE subcommand to have the z/OS FTP server initiate keepalive packets to keep the data connection from being cancelled because of inactivity.

Gems with TN3270 and Telnet ("otelneta")



© Copyright IBM 2010

System Symbolics in USS MSG 10 in V1R8

USSMSG10 - Initial logon panel.

Most other USSMSGxx are used to report errors back to the end user.

Symbolic substitution for certain variables known to Telnet exist for messages already.

LU name	@@LUNAME
IP Address	@...@IPADDR
IP Port	@@PRT
Hostname	@...@IPHOSTNAME
Date/Time	@@@@DATE/@@@@TIME

☛ Telnet will now also check for System Symbolics in the message string.
&SYSNAME. &SYSR1.

```
USSMSG10: Enter: LOGON APPLID() LOGMODE() DATA()
Port: 01648        Date: 01/18/06
IPADDR: 9.94.103.223    Time: 15:14:41
System Name: MVS023    Release: MVS018
```

☛ Specify LUNAME or SCAN on the message as you would for @@ string substitution.

© Copyright IBM 2010

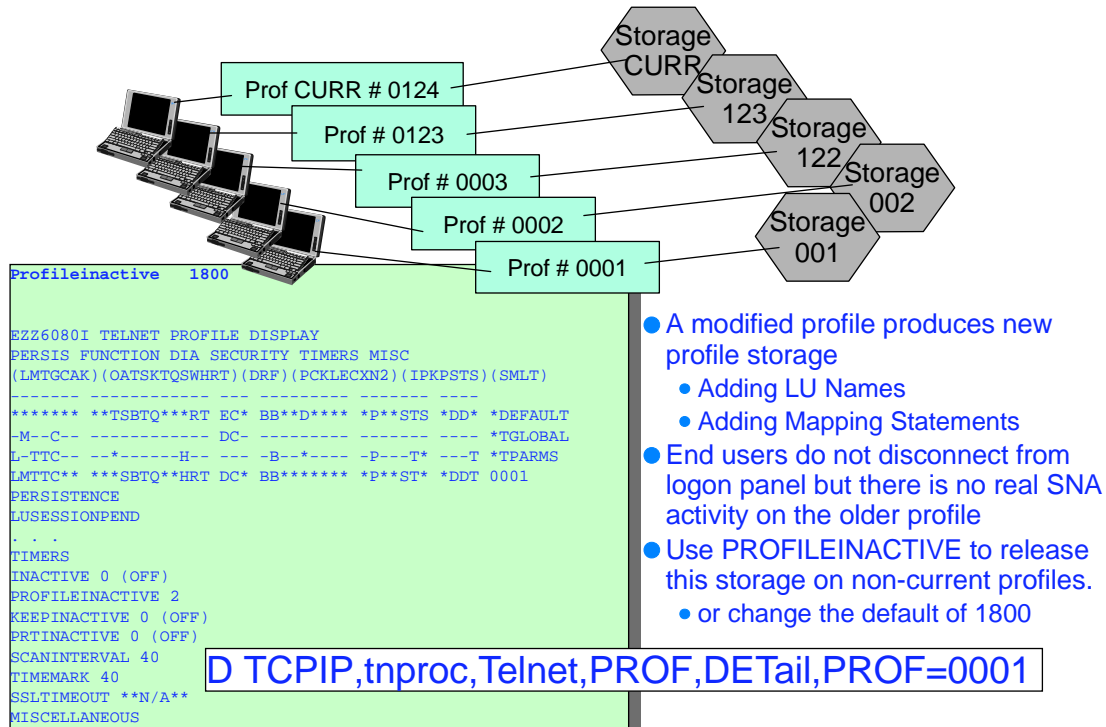
System Symbolics in USS MSG 10 in V1R8

Sample section to generate the MSG10 Screen

```
DC X'11'          SET BUFFER ADDRESS ORDER
DC X'C2E0'        ROW 5 COLUMN 2
DC X'1D'          START FIELD
DC X'F0'          PROTECT SKIP NORMAL
DC C'System Name: &&SYSNAME.  '
DC C'Release: &&SYSR1.  '
*
```

➤ Note the extra '&' on the symbolic name. This is necessary for the compiler to produce the right symbolic.

PROFILEINACTIVE: Releasing TN3270 Profile Storage (V1R9)



- A modified profile produces new profile storage
 - Adding LU Names
 - Adding Mapping Statements
- End users do not disconnect from logon panel but there is no real SNA activity on the older profile
- Use PROFILEINACTIVE to release this storage on non-current profiles.
 - or change the default of 1800

© Copyright IBM 2010

1. When a V TCPIP,tnproc,Obeyfile command is issued, new private storage is obtained from the address space to create completely new profile structures from the Telnet statements in the profile dataset. The new profile becomes the current profile and the previously current profile is considered non-current. Each profile, by port, is assigned a number in ascending order when created starting with 1. The current profile has been assigned a number but is referred to as the CURR profile until it is replaced.
2. New connections are always associated with the CURR profile. Once a connection is associated with a profile, it stays associated with that profile until the connection is dropped. The connection will never access another profile. Telnet profile storage is never completely released. A small block is used to anchor the larger parameter and mapping structures. When a profile is no longer current and there are no connections associated with the profile, all parameter and mapping structure storage is released leaving only the small anchor block that is used for profile displays.
3. The solution to this storage problem is to more actively manage the non-Current profiles. Instead of waiting for all connections to end, periodically check all connections associated with the non-current profile. If the connection does not have a Systems Network Architecture, SNA, session and the connection has not been in a SNA session for at least a configurable period of time, drop the connection. Most end users have auto-reconnect specified on their emulators causing the emulator to immediately re-establish a TCP connection with the new current profile. Without auto-reconnect, the end user will need to manually reconnect.
4. When the connection is dropped, that is one less connection associated with the old profile. When the connection count goes to zero, the profile parameter and mapping structures can be released, freeing potentially large amounts of storage.
5. A potential storage shortage problem is avoided by cleaning up these unnecessary connections and non-current profiles.
6. Profileinactive is a new parameter used to control how long a connection can stay connected without a SNA session when associated with a non-current profile. The time specified is in seconds. Telnet is initialized with a value of 1800 seconds (or 30 minutes). The function can be turned off by coding a time value of zero.
7. Like most other parameters, Profileinactive can be specified in TelnetGlobals, TelnetParms, or ParmsGroup depending on the level of granularity desired.
8. If the default is used, connections associated with non-current profiles will be dropped after being without a SNA session for at least 30 minutes. Because the timer is shared with Inactive,PrtnInactive, and KeepInactive, the connection will be dropped sometime soon after 30 minutes, but probably not at precisely 30 minutes.
9. There is a new connection drop message:
 1. A new connection drop reason for EZZ6034I
 2. 1 INACT-PF
 3. EZZ6034I TELNET CONN 00000183 LU **N/A** CONN DROP INACT-PF IP..PORT: ::FFFF:9.65.224.165..1643
 4. You can display the profile with: Display TCPIP,tnproc,Telnet,PROF,DETail,PROF=0001

Displaying APPLDATA for TN3270 (V1R9)

netstat tcp all

```
Client Name: TELNET                      Client Id: 00000021
Local Socket: ::ffff:9.42.104.171..6001
Foreign Socket: ::ffff:9.37.215.144..2395
BytesIn: 000000000000000000405
. . .
```

```
Application Data:  EZBTNSRV TCPM1001 TSO10002 ET ST14S
```

Eyecatcher
LU name
Application name
Connection & Emulator type
Security Level Protocol Cipher

- 1. Connection negotiation complete
 - Security Level / (Protocol) / (Cipher), Connection mode & Emulator Type (LU name – If TN3270E connection)
- 2. SNA session established
 - LU name, Application name
- 3. SNA session ends and TCP connection remains (If connection drops, data clear is not done)
 - Clear application name (Clear LU name – If not TN3270E connection)

© Copyright IBM 2010

1. The APPLDATA section is updated at three different key events for a Telnet connection.
2. The first update to APPLDATA occurs when Telnet protocol negotiation is complete.
 1. By this time we have completed System SSL handshake and Telnet negotiations: We know what the security level, protocol, and cipher are and we know what the connection mode and emulator type are. If the connection mode is TN3270E we also know the LU name assigned to the connection. This information will not change over the life of the connection.
3. The second update to APPLDATA occurs when a SNA session is established. If an LU name was not associated with the connection during Telnet protocol negotiation, an LU name is assigned during SNA session setup. The LU name and application name are added to the APPLDATA section.
4. The third update to APPLDATA occurs if the LUSESSIONPEND statement is mapped to the Telnet connection which keeps the TCP connection active after logoff from the application. In this case the application name is cleared and the LU name may be cleared depending on connection mode. If the connection is dropped when the session logoff is received, the application name and LU name remain in the APPLDATA section and will be present in the TCP connection termination SMF record.
5. APPLDATA is presented in several netstat commands. This slide shows sample output from a netstat all command. Connection mode and emulator type values ET indicate a TN3270E connection mode with a terminal emulator. Security values ST14S indicate a secure connection using TLSv1 and cipher 4S. The connection is represented by LU name TCPM1001 and the end user is in session with application TSO10002.

Formerly UNIX-only Commands Now at MVS Console (V1R11)

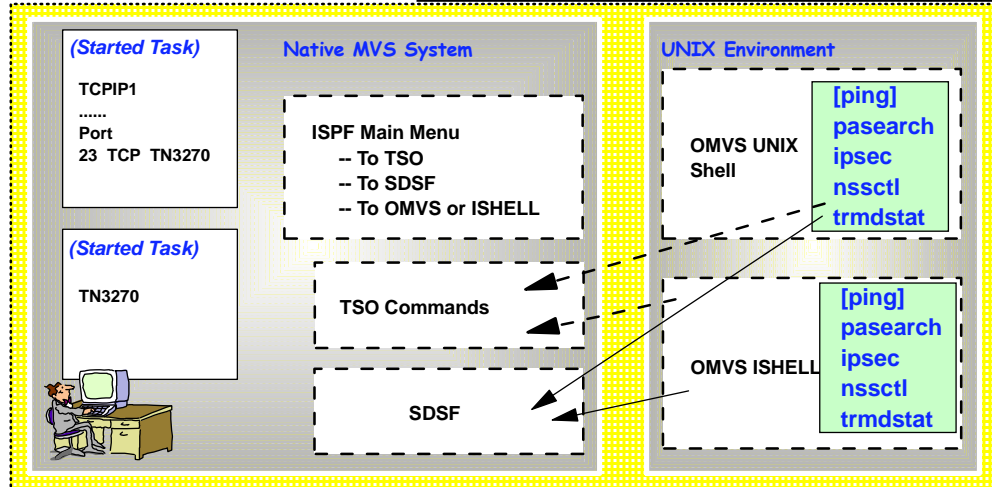
- Following Commands that were formerly UNIX-only, may now be executed at the MVS Console, from NetView, and from TSO using the EZACMD interface:

- ping (NOTE: At TSO continue to use the TSO version of "ping.")
- pasearch
- ipsec
- nssctl
- trmdstat

```
%%ezacmd 'ping -v w3.ibm.com'
```

```
netvasis ezacmd ping -v w3.ibm.com max=20
```

```
ezacmd ipsec -f display max=10
```



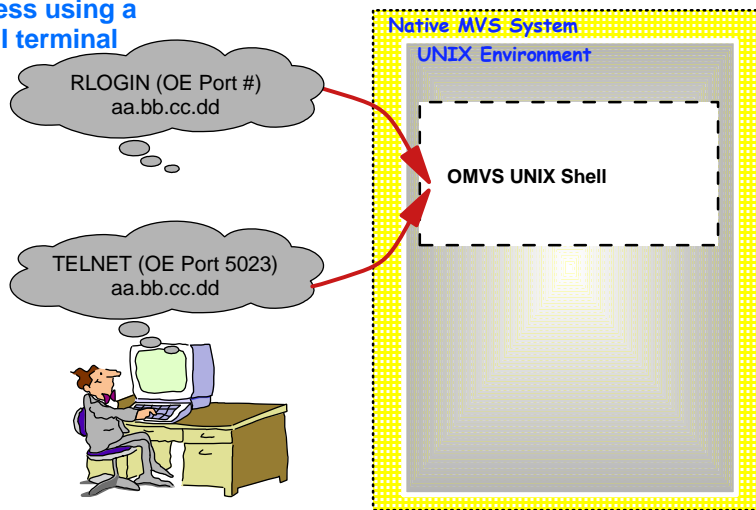
REFERENCE: UNIX System Services Command Reference

© Copyright IBM 2010

- z/OS V1R11 makes the z/OS UNIX commands listed above available in the three new command environments:
 - z/OS console, NetView, and TSO. Only the z/OS UNIX commands listed above are made available in these environments.
- Ping is not a policy-related command, but customers have asked for ping from the z/OS console for many years.
- The infrastructure that was built for the policy-related commands was very easily expanded to also support ping.
- Since TSO has a native TSO ping command already, the z/OS UNIX ping was not made available in TSO.
- The command examples for PING show you, in sequence, the syntax for: MVS Console, NetView, TSO.
- EZACMD is a generalized interface to the selected set of z/OS UNIX commands. The same EZACMD command is used from TSO, the z/OS console, and NetView. Each environment has specific requirements and characteristics, which you should read about in the IP Configuration Guide. For setting up z/OS System REXX in general for the MVS Console and for TSO, refer to the z/OS publication "MVS Programming: Authorized Assembler Services Guide", chapter 31 "System REXX" and z/OS "MVS Initialization and Tuning Reference", Chapter 8 "AXR00 (default System REXX data set concatenation)".
 - EZACMD should be copied into the REXX libraries used by TSO and by NetView for its use there.
- The EZACMD supports UNIX commands. Command options are case sensitive and must be entered exactly as documented for the z/OS UNIX command in question.
 - The MAX keyword can be entered in any case and it may be present anywhere after the command-name.
 - Output from the commands is displayed as-is. Some commands in some of the supported environments will produce output lines that are too long for the display environment. Such long output lines will be folded onto the following line. No attempt is made to re-format the output from the existing z/OS UNIX commands.
- EZACMD is delivered as a compiled REXX program in two different system libraries. One library is SYS1.SAXREXEC, which is the system REXX system library. This is a VB, LRECL=255 library. The second library is tcpip.SEZAEXEC, which is the z/OS Communications Server REXX library. This is an FB, LRECL=80 library.
- SYS1.SAXREXEC is used from the z/OS console by means of the system REXX infrastructure, which requires a VB, 255 library.
 - tcpip.SEZAEXEC is used from TSO and NetView.
- Remember System REXX requires that all REXX libraries used by System REXX are VB, LRECL=255
 - TSO and NetView might have been set up to use either FB, LRECL=80 or VB, LRECL=255
 - SYS1.SAXREXEC is VB, 255
 - tcpip.SEZAEXEC is FB, 80
 - EZACMD is delivered in both libraries
 - Consider SERVAUTH profiles for especially the ipsec command usage

Accessing UNIX Shell with UNIX Telnet (Port 23): Banners ...

Telnet process using a VT100 ASCII terminal



```
#=====
# service | socket | protocol | wait/ | user | server | server program
# name   | type   |         | nowait|     | program | arguments
#=====
login    stream tcp nowait OMVSKERN /usr/lpp/tcpip/rlogind rlogind -m
#
otelnet  stream tcp nowait OMVSKERN /usr/lpp/tcpip/sbin/otelnetd -l
# telnet stream tcp nowait OMVS /usr/sbin/otelnetd otelnetd -l -n -h
```

© Copyright IBM 2010

1. You may also implement an ASCII version of TELNET that operates only in a UNIX environment; Telnet (sometimes called "otelnet") also defaults to using Port 23, but many people assign a different port to it, for example we have used Port 5023 here. You use an ASCII terminal or terminal emulator (like the the VT100 emulator) to work in this UNIX environment.
 1. Telnet does not have its own "listener" and so it uses the services of INETD, which listens for connections to Telnet.
 2. UNIX Telnet is implemented by defining it to INETD and then starting INETD as a UNIX process from /etc/rc.
2. You can enter UNIX commands once you have entered the UNIX environment.
3. This visual shows you two methods to enter the UNIX environment:
 1. Use RLOGIN to arrive at the UNIX shell, or
 2. Use OTELNET (TELNET) to the OTELNETD port to arrive at the shell.

Two Telnet Banners: Before and After Login (V1R11)

UNIX Telnet Shell Screen: Display banners or suppress with "-h" initialization

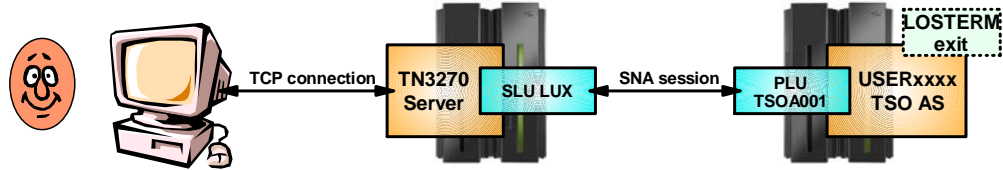


```
-----  
here is the test banner before login from /etc/otelnetd.banner  
-----  
EZYTE27I login: gdente  
EZYTE28I gdente Password:  
IBM  
Licensed Material - Property of IBM  
5647-A01 (C) Copyright IBM Corp.  
(C) Copyright Mortice Kern Systems, Inc.  
(C) Copyright Software Development Group, University of Waterloo  
  
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 the IBM Corp.  
  
-----  
here is the test banner after login from /etc/banner  
-----  
#
```

© Copyright IBM 2010

1. This is the type of UNIX shell screen you would see if you used either TELNET or RLOGIN to the UNIX telnet port.
2. The z/OS UNIX Telnet server (otelnetd) provides access to z/OS UNIX shell applications on the host using the Telnet protocol. The z/OS UNIX Telnet server lets hosts in an IP network log on to the z/OS shell environment directly, without going through TSO.
3. Otelnetd provides a customizable banner that is presented to a user after a user logs in. This banner is located in /etc/banner.
4. Customers want the ability to have a banner page presented before a user logs in to otelnetd. They wanted to be able to provide information in this banner, such as which system a user is about to log in to and possibly other information. A new banner to accommodate this requirement was introduced with z/OS V1R11 Communications Server.
 1. The new banner is called /etc/otelnetd.banner. **If the existing -h parameter is specified for otelnetd in /etc/inetd.conf, it now disables the display of both /etc/banner and /etc/otelnetd.banner. An example of how to code this is shown.**

LOGONHERE (V1R11)



If old SNA session exists, when user attempts reconnect, disconnect old SNA session and proceed with TSO logon reconnect.

- Combined effort by TSO and CS development
- New LOGONHERE option in IKJTSoxx member to enable new support
- Enables reconnecting TSO user from a new SNA session
- Helps further reduce number of "USERID already in use" errors

TSO Reconnect Possible	Single session	Multiple sessions	NATed connectivity
TKOGENLU[RECON]	✓		
CheckClientConn	✓	✓	
TKOSPECLU[RECON]	✓	✓	✓
TSO LOGONHERE	✓	✓	✓
TIMEMARK/SCANINTERVAL	✓	✓	✓

© Copyright IBM 2010

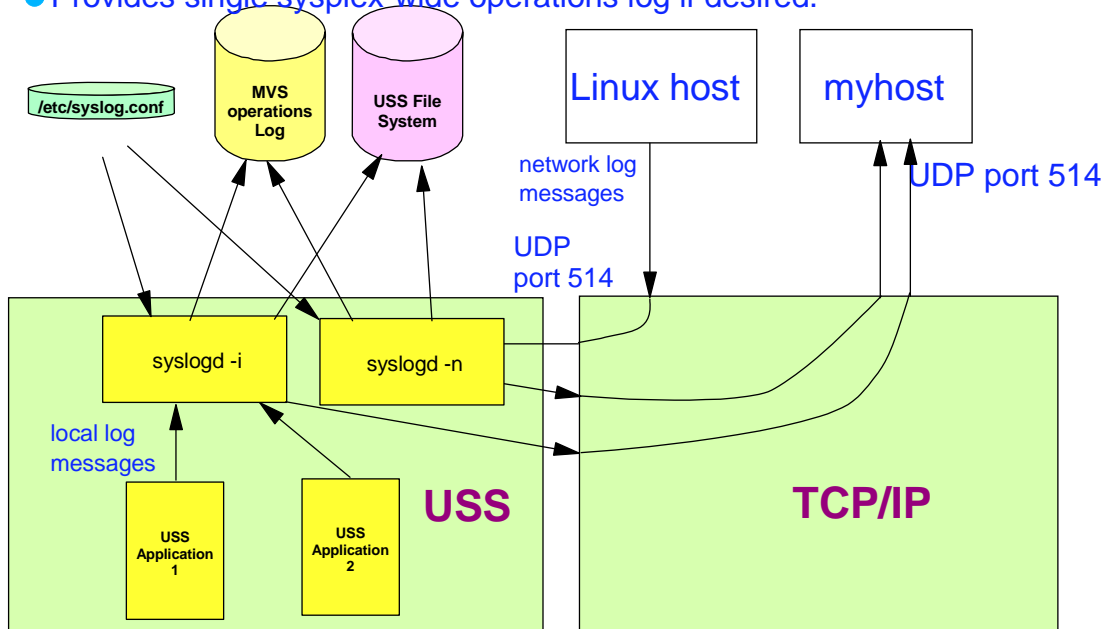
1. TSO reconnect has so far been supported in the case where the original SNA session had been disconnected. If an SNA session was still active, it was not possible to use reconnect. In the case where a TN3270 client lost a TCP connection with the TN3270 server, but the SNA session remained active, you could not use reconnect.
2. A modification has been made to TSO. The modification is governed by a new option in IKJTSoxx – a LOGONHERE option. With that option enabled, users can reconnect even when an old SNA session exists. The old SNA session is being disrupted (LOSTERM exit), and reconnect for the new session is processed.
3. This function is an alternative to other TN3270 server options for cleaning up old TCP connections and or SNA session.

Gems with SYSLOGD

© Copyright IBM 2010

Linux Message Integration with SYSLOGD V1R8

- 2 SYSLOGDs: one Local Mode (-i) and one Network Mode (-n)
- Provides single sysplex-wide operations log if desired.



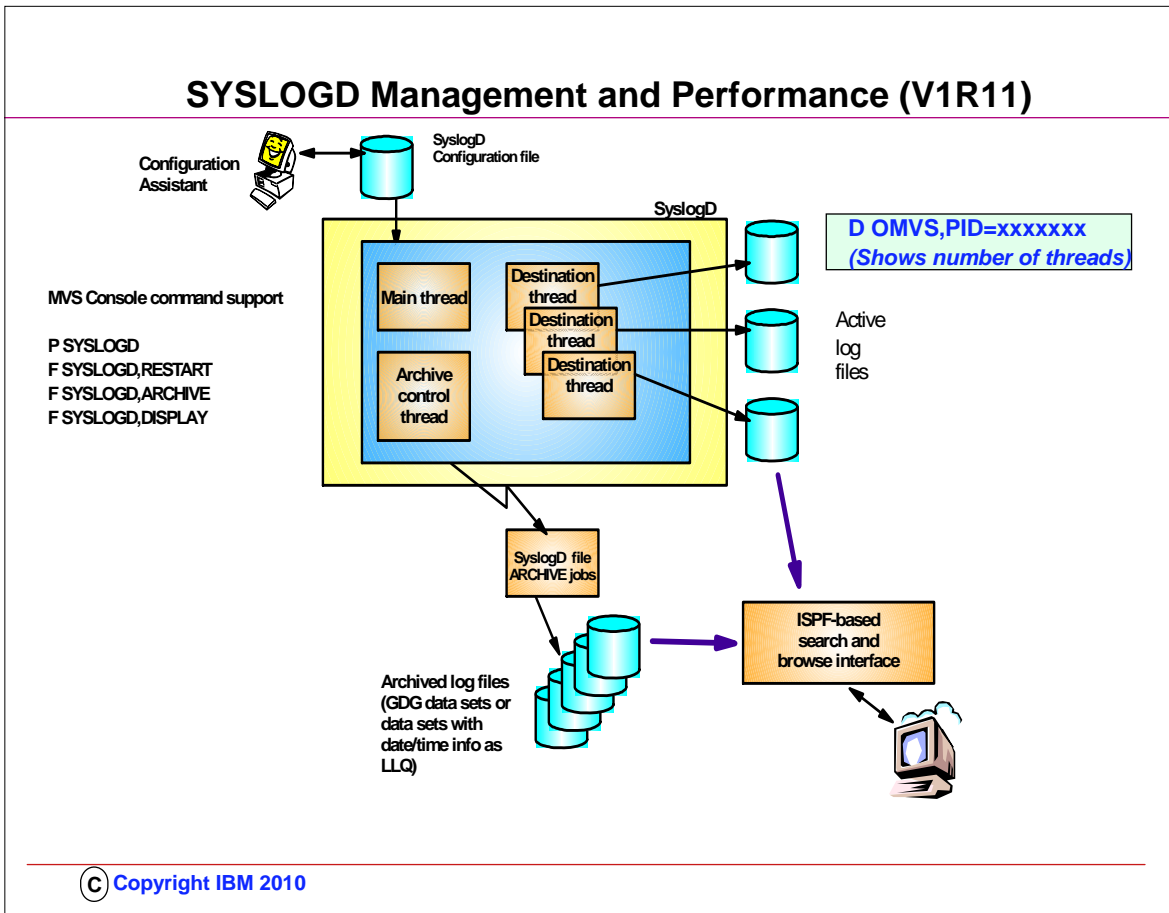
© Copyright IBM 2010

Linux Message Integration with SYSLOGD V1R8

- SYSLOGD log messages can now be collected from numerous network sources including Linux hosts and can be filtered to log to the desired destination based on the source IP address or hostname
 - log messages from network hosts can be written to the MVS operations log (operlog)
 - operlog can be used in place of or in addition to MVS syslog (console log)
 - in a sysplex environment operlog can be configured as a log stream in the coupling facility
 - provides a single sysplex-wide consolidated message log that contains z/OS generated messages and syslogd messages
 - better performance than writing to /dev/console
- Performance of syslogd is improved
 - a local-only and a network-only instance may be run concurrently (i.e., TWO instances of Syslogd!)
 - One instance in local only mode (-i option)
 - One instance in network only mode (-n option)
 - new command option (-x) improves performance by avoiding IP address-to-hostname resolution for network log messages
- If you use both local and network logging, IBM recommends that you use two instances of syslogd
 - helps ensure that local syslogd logging is not adversely affected by the amount of remote messages being forwarded to z/OS

© Copyright IBM 2010

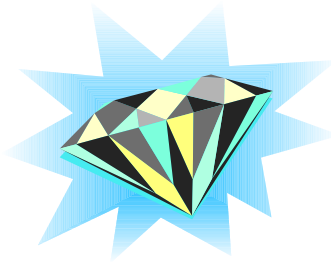
SYSLOGD Management and Performance (V1R11)



© Copyright IBM 2010

1. This slide shows a high-level overview of the new and improved syslogd components.
2. Syslogd is now a multi-threaded implementation allowing for more parallel processing in peak periods. Syslogd continues to write log messages to z/OS UNIX files. A new archive function will archive the content of a z/OS UNIX log file to an MVS data set. The MVS data set can either be a sequential data set (low level qualifiers specify date and time) or a new generation of a generation data group (GDG). The archive operation can be initiated by an operator. At a specific point in time (for example, shortly after midnight). Or when the utilization of one of the file systems the z/OS UNIX log files are written to exceeds a configurable threshold.
3. Command support includes the ability to shut syslogd down using a P command. Syslogd will in R11 not change address space name after it has started. If you start a procedure by the name of SYSLOGD – the resulting address space name remains SYSLOGD.
4. The ISPF browser starts by reading the syslogd configuration file, locates the active z/OS UNIX files, and all available MVS archives. It supports browsing individual files or data sets, in addition to performing extensive searches in one or a series of files or data sets.

Gems with Security



© Copyright IBM 2010

IPsec Standards Compliance (V1R10)

RFC	Department of Defense Advanced UNIX Server Profile	National Institute of Standards and Technology Host Profile	z/OS CS V1R10
2407 ISAKMP DOI	MUST	MUST	✓ (already supported)
2408 ISAKMP	MUST	MUST	✓ (already supported)
2409 IKE	MUST	MUST	✓ (already supported)
3948 UDP-encap ESP	N/A	MAY	✓ (already supported)
4109 IKE algorithms	MUST	MUST	✓ (already supported)
4301 IPsec	MUST	SHOULD+	✓ (new in V1R10)
4302 IP AH	MUST	MAY	✓ (already supported)
4303 IP ESP	MUST	MUST	✓ (already supported)
4304 ESN	SHOULD	MUST	✓ (new in V1R10)
4305 IPsec algorithms	SHOULD+	SHOULD+	✓ (already supported)
4308 Crypto suites	MUST	MAY	✓ (new in V1R10)

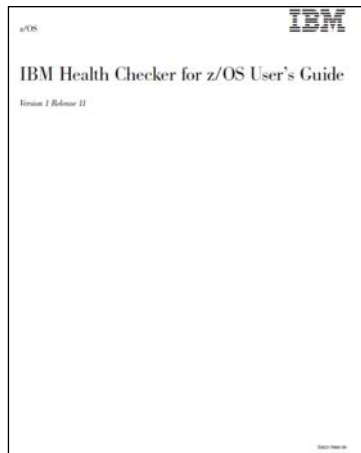
Security mandates can require compliance with standards.
Auditors must check for these on all platforms.

© Copyright IBM 2010

1. z/OS Communications Server V1R10 supports all IPsec RFCs at levels currently required by DOD and NIST profiles.
2. Note that some elements of RFC 4301 require the use of IKEv2; for example, support for dynamic tunnels that cover a range of ports. Since z/OS Communications Server does not support IKEv2, these elements are not supported on z/OS Communications Server.
3. Note that the z/OS Communications Server support for RFC 4304 extends to recognition of ESN proposals during the negotiation of security associations, but not to supporting the use of ESN. z/OS Communications Server IKED will reject an SA proposal that includes ESN. If there are SA acceptable proposals without ESN then z/OS Communications Server IKED will accept them.

Health Checks Available for z/OS Communications Server

http://www-03.ibm.com/systems/z/os/zos/hchecker/check_table.html



IBM Health Checker for z/OS User's Guide (GA22-7994)

IBM Systems > System z > Operating systems > z/OS

Checks available for IBM Health Checker for z/OS

The following table lists currently available IBM checks by check owning component or product and the APAR or z/OS release in which they were introduced.

For complete check descriptions, see the [IBM Health Checker for z/OS checks](#) topic in the [IBM Health Checker for z/OS User's Guide](#).

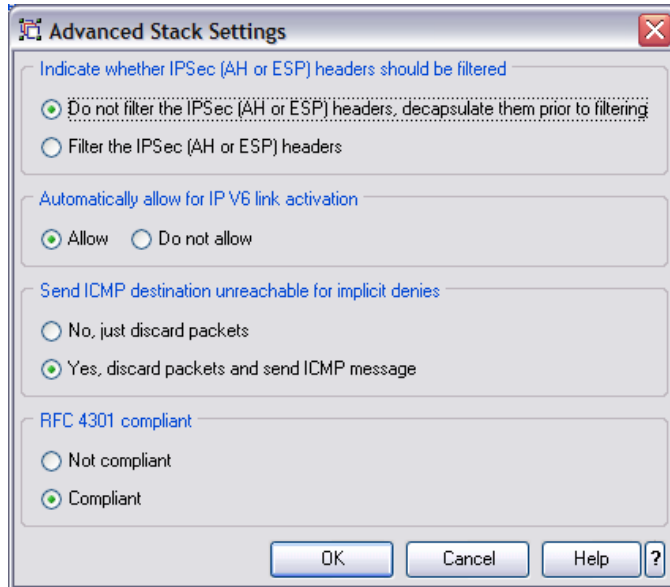
Check owner	Check name	APAR number and/or z/OS release
IBMASH ASH	ASH_LOCAL_SLOT_USAGE	Integrated in z/OS V1R8.
	ASH_NUMBER_LOCAL_DATASETS	
	ASH_PAGE_ADD	
	ASH_PLPA_COMMON_SIZE	
IBM-CATALOG Catalog	CATALOG_IMBED_REPLICATE	Integrated in z/OS V1R11.
	IBM-CSE Communications Server	CETCP_SVTCTCPF_TRACE_TCPFstackname
CETCP_TCPMAXCVDUPRFSIZE_TCPFstackname		Integrated in z/OS V1R9.
CEVTAM_CSM_STG_LIMIT		
CSTCP_SVSPLEXNON_RECOV_TCPFstackname		Integrated in z/OS V1R10.
CEVTAM_T18UP_T28UP_EE		
CEVTAM_T18UP_T28UP_NOBE		
CEVTAM_VIT_DSPSIZE		
CEVTAM_VIT_OPT_ALL		
CEVTAM_VIT_OPT_PSSMS		
CSTCP_CINET_PORTING_RSV_TCPFstackname		Integrated in z/OS V1R10.
ZOSHGV1R10_CS_BIND4	GA22593 and P668135 contain checks for z/OS V1R8 and V1R9 and is integrated into V1R10.	
ZOSHGV1R10_CS_BINL	Integrated in z/OS V1R11.	
ZOSHGV1R10_CS_DNCP		
ZOSHGV1R10_CS_NDB		
ZOSHGV1R11_CS_DNSBIND9	GA22605 and P684362 contain check for z/OS V1R10 and V1R11.	
ZOSHGV1R11_CS_RFC4301	GA22605 and P684362 contain check for z/OS V1R10 and V1R11.	
CNZ	CNZ_CONSOLE_MSCORE_AND_ROUTCOD	GA00205 contains checks for z/OS V1R8-V1R7 and is integrated in z/OS V1R8.
	CNZ_AHNI_EVENTUAL_ACTION_MSGS	
	CNZ_CONSOLE_MASTERAUTH_CMDSYS	
	CNZ_CONSOLE_MASTERAUTH_CMDSYS	
	CNZ_CONSOLE_SOUTCODE.11	
	CNZ_BMCS_INACTIVE_CONSOLES	
	CNZ_BMCS_HARDCOPY_MSCORE	
	CNZ_SYSCONS_MSCORE	
	CNZ_SYSCONS_PD_MODE	
	CNZ_SYSCONS_SOUTCODE	
CNZ_TASK_TABLE		
CNZ_SYSCONS_MASTER (z/OS V1R6-V1R7 only)	Integrated in z/OS V1R11.	
CNZ_OBSOLETE_MSGFIELD_AUTOMATION		

RFC4301 Compliance

© Copyright IBM 2010

1. You will probably want to download the IBM Health Checker for z/OS User's Guide to investigate how to implement Health Checker and to understand the various types of health checks that are available to you, including those in IBM Communications Server.
2. The User's Guide points you to a web page that is kept updated for all currently available health checks:
 1. http://www-03.ibm.com/systems/z/os/zos/hchecker/check_table.html
3. The web page provides you the name of the RFC4301 health check that you will want your z/OS Systems Programmer to implement for you.

RFC4301 Compliance: IP Filtering and IPsec VPNs



● Routed Traffic Rules must not contain:

- Port Numbers
- ICMP(v6) Code Types
- OSPF Types

● For Migration:

- Use the z/OS Migration Manual
- Use the GUI
- Use the z/OS V1R11 HealthChecker (available at V1R10)

- When given a choice, always try to configure IPsec with RFC4301 compliance. After V1R11 you must configure RFC4301 compliance and will not want to be forced to reconfigure your policies!

© Copyright IBM 2010

1. RFC4301 "Security Architecture for the Internet Protocol" specifies the base architecture for IPsec compliant systems
 1. – Includes restrictions on the routing of fragmented packets
 2. ... In z/OS V1R10 and V1R11, RFC4301 compliance enforcement is an optional setting in the z/OS IPsec policy
 3. – Changing an IPsec policy from non-compliant to compliant might require minor changes to IP filters for IP traffic that is routed through z/OS
2. RFC4301 - "Security Architecture for the Internet Protocol"
 1. Prior to RFC 4301 support, IPsec filters all routed IP fragments using a policy of first possible filter match (RFC4301 compliance=no)
 1. port, type, or code specifications are allowed on routed traffic rules
 2. filter all IP fragments by first possible filter match - except: non-initial IP fragments only match rules covering All ports, types, or codes
 2. RFC 4301 introduces rules and restrictions to ensure proper classification of fragments (RFC4301 compliance=yes)
 1. Use and enforce the RFC 4301 restrictions on IP filter rules: no port, type, or code specifications on routed traffic rules
 2. RFC4301Compliance parameter on the IpFilterPolicy statement
3. To be RFC4301-compliant, you should not filter on ports/type/code for routed traffic
 1. You can have the GUI enforce this or just issue a GUI health check warning
 1. A z/OS migration health check in z/OS V1R11 will determine if you have such filter rules:
 1. – ISTM010E IPsec filter rules that violate RFC4301 compliance are in use on this system during this IPL
4. This restriction can be temporarily suspended up through z/OS V1R11 until you update your policy to comply with the restriction. As an interim measure, you can configure the stack as Not compliant as indicated by one of the radio buttons in this GUI panel.
5. You may choose to relax the restriction until you have updated your configuration. If you choose to relax the restriction, you should be aware that the vulnerabilities cited in RFC 4301 concerning routed traffic and fragmented packets will apply to you.
6. At V1R12, you are no longer given a choice to be non-RFC4301-compliant.

Miscellaneous Gems



© Copyright IBM 2010

Verbose Ping (V1R11)

- z/OS ping has been made to look more like ping on other platforms.
 - A new verbose (or `-v`) option

```
USER1:/u/user1: >ping -v w3.ibm.com
CS V1R11: Pinging host w3.ibm.com (9.17.137.11)
with 256 bytes of ICMP data
ping #1 from 9.17.137.11: bytes=264 seq=1 ttl=242 time=56.64 ms
ping #2 from 9.17.137.11: bytes=264 seq=2 ttl=242 time=56.90 ms
ping #3 from 9.17.137.11: bytes=264 seq=3 ttl=242 time=57.96 ms
Ping statistics for w3.ibm.com (9.17.137.11)
    Packets: Sent=3, Received=3, Lost=0 (0% loss)
    Approximate round trip times in milliseconds:
    Minimum=56.64 ms, Maximum=57.96 ms, Average=57.17 ms, StdDev=0.70 ms
USER1:/u/user1: >
```

© Copyright IBM 2010

1. z/OS ping has been made to look like ping on most other platforms.
2. The new verbose or `-v` option will by default send three echo requests, calculate statistics for those three requests, and display the statistical summary as the response.

Do You Know Your TCP/IP Stack's Hostname? (V1R10)

**EZZ0162I HOSTNAME FOR tcpstackname IS
hostname**

- Some applications issue: `GETHOSTBYNAME`
- If your resolver file is not set up correctly, you could be providing an unintended hostname!
 - Need to understand Global Resolver processing - which changed radically way back at V1R2!
- An IPL is required to change a hostname.
- Verify at startup what the hostname of your running TCP/IP job is!

© Copyright IBM 2010

1. TCPIP learns its hostname at startup.
2. ..Applications can issue a `gethostname` call to get the hostname TCPIP learned at startup.
3. ..Applications may fail if `gethostname` returns an unexpected hostname.
4. ..TCPIP needs to be recycled to learn a new hostname.
5. Search Order for Hostname:
 1. The name on the stack's `TCPIP.DATA HOSTNAME` statement is used.
 1. The z/OS UNIX search order is used to find the stack's `TCPIP.DATA` statements unless you use the Global Resolver. Refer to "Search orders used in the z/OS UNIX environment" in the z/OS Communications Server IP Configuration Guide for more information on the search order
 2. If there is no valid `HOSTNAME` statement, the VMCF node name with which VMCF was started is used.
 3. If VMCF was not active when the stack was started, the `CVTSNAME` value (the `SYSNAME=value` in `IEASYSxx` that was IPLed) is used.
6. To see where TCPIP is finding the hostname, you can add a `SYSTCPT DD` to the TCPIP proc. This will provide a resolver trace that will tell you what `tcpip.data` files are being used by TCPIP to find the hostname.
7. Applications can get hostnames to use in different ways. One way is to issue a `gethostname` call to get the hostname TCPIP learned at startup. If an unexpected hostname is returned, this can cause the application to not run properly.
8. Since TCPIP needs to be recycled to learn a new hostname, this can be an outage for the user – with the application not working until TCPIP is recycled to pick up the correct hostname.
9. With this enhancement in V1R10, you can find out the first time you initialize your TCP/IP stack what hostname it is using and make any corrections before things turn critical.

Specifying Port Ranges for VIPADistribute (V1R9)

```
VIPADYNAMIC
...
VIPADefINE MOVE IMMED 255.255.0.0 203.1.1.94
1 VIPADISTRIBUTE 203.1.1.94 PORT 3006 3008-3010 DESTIP ALL
2 VIPADISTRIBUTE 203.1.1.94 PORT 3015-3018 3020-3021 3024 DESTIP ALL
VIPADefINE MOVE IMMED 255.255.0.0 203.1.1.95
3 VIPADISTRIBUTE 203.1.1.95 PORT 2001-2064 DESTIP ALL
ENVIPADYNAMIC
```

1. Single Port and Port Range
2. Two Port Ranges and Single Port
3. Port Range

© Copyright IBM 2010

1. With V1R9, the VIPADISTRIBUTE statement syntax is more flexible. It will now accept individual port numbers, a range of port numbers, or a combination of individual ports and ranges for the PORT keyword. The maximum number of ports that can be specified on a VIPADISTRIBUTE statement or for a DVIPA over multiple statements remains 64.
2. As previously you can still completely omit the port numbers.

Selecting the Source IP Address - 1.8, 1.9

SRCIP

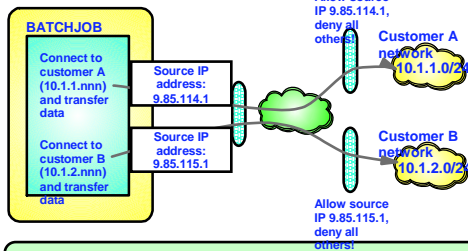
```

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

- 1.8: based on DESTIP
- 1.9: based on DESTIP with DRVIPA
- To use a DRVIPA as a source IP Address:

- GLOBALCONFIG
EXPLICITBINDPORTRANGE
- SYSPLEXPORTS and CF Structure
- SRCIP Rules



CINET: Supported if only one stack configured - or multiple stacks configured but all applications have stack affinity

- **Reminder: In 1.9 FTP client can request specific SOURCEIP.**

© Copyright IBM 2010

1. In z/OS V1R8, we introduced an option to select source IP address based on the destination IP address a connection was directed towards.
2. But we specifically excluded support for that source IP address to be a Sysplex-wide source IP address (a distributed DVIPA)
3. If installations need to be able to submit multiple jobs, that all need to connect to business partners and the jobs may execute in parallel on multiple LPARs in the Sysplex - we need a distributed DVIPA as source IP address!
4. z/OS CS V1R9 extended the destination-based source IP address selection to include a distributed DVIPA:
5. Participating stacks will reserve a coordinated range of port numbers for this use - new option on GLOBALCONFIG
6. If an application issues an explicit bind to INADDR_ANY or INADDR6_ANY and port 0, the stack has SYSPLEXPORTS enabled, and the stack has SRCIP rules - a port from this new range will be requested

Security: Limiting Access to Unreserved Ports - (1.10)

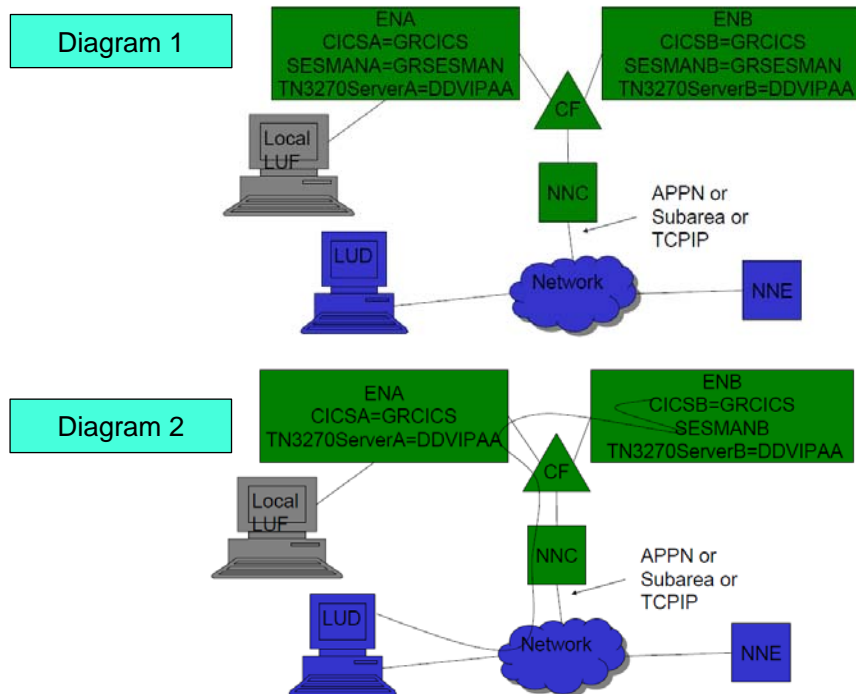
PORT	UNRSV	TCP	MYAPP1		
PORT	UNRSV	TCP	*	SAF	RES2
PORT	UNRSV	TCP	*	SAF	GENERIC WHENLISTEN
PORT	UNRSV	UDP	*	SAF	GENERIC EPHEMERAL

- Controls TCP listens on unreserved ports
 1. Denies all TCP listens on an unreserved port,
– **except for application MYAPP1**
 2. Denies all TCP listens on an unreserved port, except for all users permitted to the specified SAF resource:
– **EZB.PORTACCESS.sysname.stackname.RES2**
 3. Prevents all users from opening any unreserved TCP ports as servers, unless they have access to the SAF resource:
– **EZB.PORTACCESS.sysname.stackname.GENERIC**
 4. Prevents all users from explicitly binding to any unreserved UDP ports, unless they have access to the SAF resource:
– **EZB.PORTACCESS.sysname.stackname.EPHEMERAL**

© Copyright IBM 2010

1. UDP and TCP port usage by server programs can be controlled via port reservations in the TCP/IP profile
2. If there is no port reservation for a given port number, then any application can use it as a server port
3. Prior to V1R10, you could use RESTRICTLOWPORTS to prevent users and jobs that are not authorized or UID(0) from choosing ports below 1024.
4. Port access can be controlled by server jobname or server userID access authorization to a SAF resource that is associated with the port.
5. This new function only controls application-specified ports. It does not affect generic binds or use of ephemeral ports (meaning, port number chosen by the stack).
6. **Caution:** PORT UNRSV controls could have broad and unexpected consequences
 1. .. For example: Client programs may execute under many different user IDs, so all address spaces where the client program can execute may need to be authorized.
7. POSSIBLE IMPLEMENTATION APPROACH:
 1. Determine unreserved ports used by your applications
 1. Define following: .. PORT UNRSV protocol * SAF xyz WHENBIND
 2. Create.. SERVAUTH profile with UACC(READ)
 1. .. Audit the successes to determine the names of the applications
 3. Reserve ports for your discovered applications
 1. .. PORT or PORTRANGE profile statements
 2. .. Enable PORT UNRSV control by DENY or SAF UACC(NONE)
 1. .. Monitor failures and reserve ports as appropriate

Simplify Generic Resource Selection (V1R9)



© Copyright IBM 2010

1. These are Generic Resource configurations in a sysplex connected to a broader network. CICSA and CICSB are known by generic resource name GRCICS.
2. **DIAGRAM 1:**
3. Session managers SESMANA and SESMANB are known by generic resource name GRSESMAN. The TN3270 servers are half tcpip and half SNA and imply there is TCPIP connectivity to these hosts.
4. The TN3270 servers are also known by their TCPIP DDVIPA address DDVIPAA. The connection from NNC to the network could be through APPN, subarea, or TCPIP (Enterprise Extender or TN3270). A session from LUF to GRCICS would be influenced by the generic resource exit flag
5. GRRFNPLL during generic resource resolution at End Node A. A session from TN3270 Server or through GRSESMAN (in relay mode) to GRCICS would be influenced by the generic resource exit flag GRRFNPLA during generic resource resolution at ENA or ENB. Generic resource resolution at all nodes in the sysplex is influenced by the generic resource exit flags GRRFWLMX and GRRFUVX.
6. **DIAGRAM 2:**
7. This shows a TCPIP connection that has been distributed to the TN3270 server A using DDVIPA workload distribution. In turn a SNA session is started from TN3270 server A to session manager SESMANB. A target generic resource application GRCICS is then selected at the session manager and it does a CLSDST-PASS to generic resource GRCICS. Generic resource resolution selects generic resource instance CICSB. Given that load balancing was done once for the connection to TN3270 server A it may be beneficial for the generic resource resolution done during CLSDST PASS processing at ENB to prefer a generic resource instance on the Origin Logical Unit host: that is CICSA on ENA. There is no way to do this today, unless you make substantial changes to the generic resource exit.
8. **HOW GENERIC RESOURCE SELECTION WORKS:**
9. The default generic resource resolution process is to first use an affinity to direct sessions from the same LU to the same generic resource instance. An affinity is created when the first session between an LU and a generic resource is started. An affinity maps the LU name and generic resource name to a specific instance of the generic resource.
10. If no affinity has been created yet, then the MVS Work Load Manager is called to identify the best generic resource instance.
11. If the generic resource exit (ISTEXCGR) is active then it is called to potentially select a different generic resource instance than was selected by the MVS Work Load Manager and set generic resource resolution flags affecting the next generic resource resolution.
12. Session distribution is determined during session initiation in a process called generic resource resolution. It is performed at the first VTAM APPN node in the sysplex that receives the session initiation request and has access to the generic resource Coupling Facility structure.
 1. Typical generic resource applications are CICS, IMS, DB2, TSO, and session managers.
13. Generic Resources purpose is to provide high availability and load balancing.
14. Generic Resource resolution is the process of identifying a specific generic resource instance. Generic Resources is an expansion of the older VTAM USERVAR function.
15. For those of you familiar with TCPIP, Generic Resources is analogous to the Distributed Dynamic Virtual Internet Protocol Address (DDVIPA) function in TCPIP.

Simplify Generic Resource Selection (V1R9)

GRHOST01 VBUILD TYPE=GRPREFS

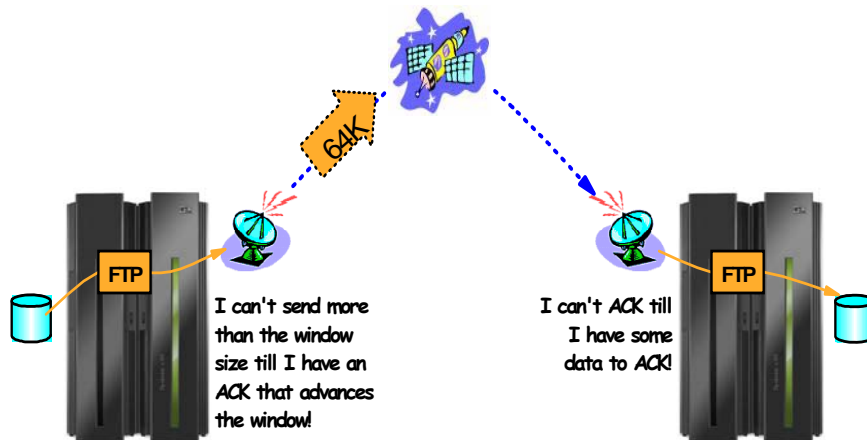
GRPREF GREXIT=NO,WLM=YES,LOCAPPL=YES,LOCLU=YES,PASSOLU=NO
 GRCICS GRPREF GREXIT=NO,WLM=NO,LOCAPPL=YES,LOCLU=YES,PASSOLU=YES
 GRTSO GRPREF GREXIT=YES,WLM=YES,LOCAPPL=YES,LOCLU=YES,PASSOLU=NO

OPERAND	VALUES	DEFAULT	MEANING
GREXIT	Yes No	No	
LOCAPPL	Yes No	Yes	
LOCLU	Yes No	Yes	
PASSOLU	Yes No	No	
WLM	Yes No	Yes	

© Copyright IBM 2010

1. The only control available prior to V1R9 over how the Generic Resources are selected was through the Generic Resources exit routine (ISTEXCGR). Many customers dislike writing or making changes to this exit, and so a VBUILD TYPE=GRPREFS options has been introduced to simplify GR selection.
2. The new VBUILD type is GRPREFS. The new definition statement GRPREF can be used to identify the generic resource preferences of each generic name. A nameless GRPREF can be defined to identify default generic resource preferences.
3. Five operands can be defined on the GRPREF definition statement.
 1. GREXIT=YES|NO (DEFAULT=NO)
 2. LOCAPPL=YES|NO (DEFAULT=YES)
 3. LOCLU=YES|NO (DEFAULT=YES)
 4. PASSOLU=YES|NO (DEFAULT=NO)
 5. WLM=YES|NO (DEFAULT=YES)
4. Except for the new function of PASSOLU these operands default to the same behavior as the corresponding GR EXIT flags.
5. You can activate a GRPREFS table using the VARY NET,ACT,ID= command where the name of the table is the VTAMLST member name that contains the generic resource preferences definitions.
6. You can also start the GRPREFS table using the VTAM Config List using the same name. Since a table cannot be inactivated, to effectively inactivate a table activate a generic resource preferences table with a nameless entry and no operands.

Dynamic Right Sizing (V1R11)



- Improves performance for inbound streaming TCP connections over networks with large bandwidth and high latency by automatically tuning the ideal window size for such TCP connections.
- This function does not take effect for applications which use a TCP receive buffer size smaller than 64K.
 - The enhancement implements an algorithm known as "DYNAMIC RIGHT SIZING"

© Copyright IBM 2010

1. Setting the TCP Buffer size to a minimum of 64K is important if you want to take advantage of "DYNAMIC RIGHTSIZING" in z/OS V1R11.
2. Streaming workload over large bandwidth and high latency networks (such as satellite links) is in general constrained by the TCP window size. The problem is that it takes time to send data over such a network. At any given point in time data filling the full window size is 'in-transit' and cannot be acknowledged until it starts arriving at the receiver side. The sender can send up to the window size and then must wait for an ACK to advance the window size before the next chunk can be sent.
3. If it were possible to dynamically adjust the window size to what it takes to fill the network in-between the sender and the receiver, higher throughput might be achieved.
4. This support will, on the receiver side, dynamically adjust the window size upward (beyond 180K if so needed) in an attempt to 'fill' the pipe between the sender and the receiver. The aim is that as soon as the sender has sent the end of its window, the sender receives an ACK from the receiver. That ACK allows the sender to advance the window and send another chunk onto the network.
5. NOTE: Be sure to check the size of your TCPRCVBUFRSIZE and adjust to 64K or higher; otherwise the Dynamic Right Sizing function in V1R11 may not work for you; the receive buffer must be equal to or larger than 64K. There is no healthchecker available to verify the size of the TCPRCVBUFRSIZE ... there is only one for TCPMAXRCVBUFRSIZE.

End of Topic

© Copyright IBM 2010