New Function Summary

Version 1 Release 11
New Function Summary

Version 1  Release 11
Note:

Before using this information and the product it supports, be sure to read the general information under “Notices” on page 161.

Sixth Edition (September 2009)

This edition applies to Version 1 Release 11 of z/OS (5694-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

IBM welcomes your comments. You may send your comments to the following address.

International Business Machines Corporation
Attn: z/OS Communications Server Information Development
Department AKCA, Building 501
P.O. Box 12195, 3039 Cornwallis Road
Research Triangle Park, North Carolina 27709-2195

You can send us comments electronically by using one of the following methods:

Fax (USA and Canada):
1+919-254-1258
Send the fax to “Attn: z/OS Communications Server Information Development”

Internet e-mail:
comsvrcf@us.ibm.com

World Wide Web:

If you would like a reply, be sure to include your name, address, telephone number, or FAX number. Make sure to include the following in your comment or note:

• Title and order number of this document
• Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# Contents

**Figures** .............................. vii

**Tables** ............................... ix

**About this document** ........................ xi

- Who should read this document .............................. xi
- How this document is organized .............................. xi
- How to use this document ................................. xii
  - Determining whether a publication is current .............. xii
  - How to contact IBM service ............................... xiii
- Conventions and terminology that are used in this document ........... xiii
- Prerequisite and related information ...................... xiv
- How to send your comments ................................. xviii

**Summary of changes** ........................ xix

**Chapter 1. Planning to use new functions** ........................ 1

- Introduction to z/OS Communications Server .................. 1
- Determining which documents to use when migrating ............ 1
- IP encryption features ........................................ 2
- Planning checklist ............................................ 3
- TCP/IP packaging process ..................................... 4
  - MVS data sets ............................................... 4
  - File system files ........................................... 7
- Defining SNA data sets ......................................... 7
  - Data sets containing information for z/OS V1R11 Communications Server .......................... 10
  - Data sets containing information for NCP ................... 18

**Chapter 2. Roadmap to functions** ............................ 21

**Chapter 3. V1R11 new function summary** ........................ 25

- Support considerations in V1R11 ............................. 25
- General release considerations in V1R11 ...................... 25
- Application integration, data consolidation, and standards ... 25
  - New SMTP client for sending Internet mail .................. 26
  - FTP enhancements ............................................ 28
  - Customizable pre-logon banner for telnetd ................. 35
  - Remote execution server enhancements ..................... 35
  - TN3270 support of TSO logon reconnect .................... 36
  - IPv6 stateless address autoconfiguration enhancements .... 36
  - New API to obtain IPv4 network interface MTU ............ 38
  - RFC 5095 deprecation of IPv6 type 0 route header ........ 38
  - CICS sockets enhancements .................................. 39
- Availability and business resilience ............................ 39
  - Improved responsiveness to storage shortage conditions .... 39
  - Disable moving DVIPA as source IP address ................. 40
  - Support for enhanced WLM routing algorithms .............. 40
- Scalability, performance, constraint relief, and accelerators .......... 41
  - accept_and_receive API enhancements ....................... 41
  - TCP/IP support for system z10 hardware instrumentation .......... 42
  - TCP/IP pathlength improvements ................................ 42
  - TCP throughput improvements for high-latency networks .......... 43
  - Virtual storage constraint relief ......................... 43
  - NSS private key and certificate services for XML appliances .... 44
<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Extender IPSec performance improvements</td>
<td>44</td>
</tr>
<tr>
<td>Resolver DNS cache</td>
<td>45</td>
</tr>
<tr>
<td>Sysplex autonics improvements for FRCA</td>
<td>46</td>
</tr>
<tr>
<td>QDIO routing accelerator</td>
<td>46</td>
</tr>
<tr>
<td>Sysplex distributor enhancements</td>
<td>47</td>
</tr>
<tr>
<td>OSA-Express3 optimized latency mode</td>
<td>50</td>
</tr>
<tr>
<td>Security</td>
<td>51</td>
</tr>
<tr>
<td>IPSec enhancements</td>
<td>51</td>
</tr>
<tr>
<td>AT-TLS enhancements</td>
<td>52</td>
</tr>
<tr>
<td>Simplification and consumability</td>
<td>53</td>
</tr>
<tr>
<td>Configuration Assistant enhancements</td>
<td>53</td>
</tr>
<tr>
<td>syslogd enhancements</td>
<td>53</td>
</tr>
<tr>
<td>syslogd browser and search facilities</td>
<td>54</td>
</tr>
<tr>
<td>Policy infrastructure management enhancements</td>
<td>55</td>
</tr>
<tr>
<td>MVS console support for select TCP/IP commands</td>
<td>57</td>
</tr>
<tr>
<td>IBM Health Checker for z/OS DNS server check</td>
<td>57</td>
</tr>
<tr>
<td>SNA and Enterprise Extender</td>
<td>58</td>
</tr>
<tr>
<td>Display potential model application name</td>
<td>58</td>
</tr>
<tr>
<td>Include data space VIT with INOP dump</td>
<td>58</td>
</tr>
<tr>
<td>HPR performance enhancements</td>
<td>59</td>
</tr>
<tr>
<td>APPN topology database update enhancements</td>
<td>62</td>
</tr>
<tr>
<td>Provide ACF/TAP as part of z/OS Communications Server</td>
<td>63</td>
</tr>
<tr>
<td>System management and monitoring</td>
<td>64</td>
</tr>
<tr>
<td>IBM Health Checker for z/OS RFC 4301 compliance</td>
<td>64</td>
</tr>
<tr>
<td>Network management enhancements</td>
<td>64</td>
</tr>
<tr>
<td>Verbose Ping</td>
<td>68</td>
</tr>
<tr>
<td>Virtualization</td>
<td>68</td>
</tr>
<tr>
<td>QDIO enhancements for Workload Manager IO priority</td>
<td>68</td>
</tr>
<tr>
<td>QDIO support for OSA interface isolation</td>
<td>69</td>
</tr>
</tbody>
</table>

### Chapter 4. V1R10 new function summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support considerations in V1R10</td>
<td>71</td>
</tr>
<tr>
<td>Performance improvements for IP in V1R10</td>
<td>71</td>
</tr>
<tr>
<td>TCP/IP performance improvements</td>
<td>72</td>
</tr>
<tr>
<td>IPSec cryptography performance improvements</td>
<td>72</td>
</tr>
<tr>
<td>TN3270E Telnet server ECDSA reduction</td>
<td>72</td>
</tr>
<tr>
<td>Security</td>
<td>72</td>
</tr>
<tr>
<td>DataPower integration with NSS SAF access service</td>
<td>73</td>
</tr>
<tr>
<td>Defensive filtering</td>
<td>74</td>
</tr>
<tr>
<td>Allow routed traffic in default filter policy</td>
<td>75</td>
</tr>
<tr>
<td>IPSec RFC currency</td>
<td>75</td>
</tr>
<tr>
<td>Enhanced port access control</td>
<td>77</td>
</tr>
<tr>
<td>Enhanced rpcbind application registration control</td>
<td>77</td>
</tr>
<tr>
<td>FTP security enhancements</td>
<td>81</td>
</tr>
<tr>
<td>TLS/SSL enablement for Load Balancing Advisor</td>
<td>83</td>
</tr>
<tr>
<td>Remove support of traffic regulation policy in Policy Agent</td>
<td>87</td>
</tr>
<tr>
<td>Security options for centralized policy server connections</td>
<td>87</td>
</tr>
<tr>
<td>Autolog support for AT-TLS dependent applications</td>
<td>88</td>
</tr>
<tr>
<td>Business resiliency</td>
<td>89</td>
</tr>
<tr>
<td>TN3270E Telnet server LU name coordination in a sysplex</td>
<td>89</td>
</tr>
<tr>
<td>Subplex support for Load Balancing Advisor</td>
<td>92</td>
</tr>
<tr>
<td>Hardware-related enhancements</td>
<td>94</td>
</tr>
<tr>
<td>INTERFACE statement support for QDIO</td>
<td>94</td>
</tr>
<tr>
<td>Multiple VLAN support</td>
<td>95</td>
</tr>
<tr>
<td>HiperSockets multiple write facility</td>
<td>96</td>
</tr>
<tr>
<td>OSA-Express3 multi-port support for IP</td>
<td>98</td>
</tr>
<tr>
<td>Consumability</td>
<td>99</td>
</tr>
<tr>
<td>Configuration Assistant: Import of policy configuration data</td>
<td>99</td>
</tr>
<tr>
<td>Configuration Assistant: IP address groups</td>
<td>100</td>
</tr>
<tr>
<td>Middleware enablement</td>
<td>101</td>
</tr>
<tr>
<td>Network management interface enhancements</td>
<td>101</td>
</tr>
</tbody>
</table>
Communicating Your Comments to IBM
Figures

1. Correlation between DD statement and NCP definition statement ............... 19
Tables

1. Comparing documents used in migration ........................................ 2
2. Distribution library data sets ...................................................... 4
3. Target library data sets ............................................................. 5
4. Shared distribution and target library data sets .............................. 6
5. z/OS data sets containing information for z/OS Communications Server .... 7
6. z/OS data sets containing information for both VTAM and NCP ............... 9
7. IBM-supplied default values for CSM buffer pools .......................... 15
8. Roadmap to functions ............................................................... 21
9. New SMTP client for sending Internet mail .................................... 27
10. FTP access to UNIX named pipes ................................................ 29
11. FTP large-volume access ............................................................ 33
12. FTP passive mode enhancements ................................................ 34
13. Customizable pre-logon banner for otelnetd ................................ 35
14. Remote execution server enhancements ...................................... 36
15. IPv6 stateless address autoconfiguration enhancements .................... 37
16. New API to obtain IPv4 network interface MTU ............................... 38
17. Improved responsiveness to storage shortage conditions ................... 39
18. Support for enhanced WLM routing algorithms .............................. 41
19. TCP throughput improvements for high-latency networks .................. 43
20. Virtual storage constraint relief .................................................. 44
21. NSS private key and certificate services for XML appliances ............... 44
22. Resolver DNS cache ................................................................. 45
23. QDIO routing accelerator .......................................................... 47
24. Sysplex distributor connection routing accelerator ........................... 48
25. OSA-Express3 optimized latency mode ........................................ 50
26. AT-TLS enhancements ............................................................. 52
27. Configuration Assistant enhancements ...................................... 53
28. syslogd enhancements ............................................................. 54
29. syslogd browser and search facilities ......................................... 55
30. Policy infrastructure management enhancements ............................ 55
31. MVS console support for select TCP/IP commands ........................... 57
32. IBM Health Checker for z/OS DNS server check ............................... 58
33. Display potential model application name ................................... 58
34. Include data space VIT with INOP dump .................................... 59
35. HPR performance enhancements coexistence PTF APARs ................... 60
36. HPR performance enhancements ................................................ 60
37. APPN topology database update enhancements ................................ 63
38. Provide ACF/TAP as part of z/OS Communications Server ................ 63
39. IBM Health Checker for z/OS RFC 4301 compliance ........................ 64
40. NMI stack configuration data ..................................................... 65
41. Network management interface enhancements - detailed CSM usage ........ 66
42. OSA network traffic analyzer data .............................................. 67
43. NMI sysplex networking data ..................................................... 68
44. Verbose Ping ............................................................................. 68
45. QDIO enhancements for WLM IO priority ..................................... 69
46. QDIO support for OSA interface isolation .................................... 70
47. DataPower integration with NSS SAF access service ........................ 73
48. Defensive filtering ....................................................................... 74
49. Allow routed traffic in default filter policy ................................... 75
50. IPSec RFC currency .................................................................... 76
51. Enhanced port access control ...................................................... 77
52. Enhanced rpcbind application registration control - Registry updates ...... 79
53. Enhanced rpcbind application registration control - Target assistance requests 80
54. FTP enhancements: Restrict users that can log in to the FTP server ....... 82
55. FTP enhancements: Configure the FTP server to support non-z/OS FTP clients that connect to the protected port.

56. TLS/SSL enablement for Load Balancing Advisor.

57. Remove support of traffic regulation policy in Policy Agent.


59. Autolog support for AT-TLS dependent applications.

60. TN3270E Telnet server LU name coordination in a sysplex.

61. Subplex support for Load Balancing Advisor.

62. INTERFACE statement support for QDIO.

63. Multiple VLAN support.

64. HiperSockets multiple write facility with zIIPs configured.

65. HiperSockets multiple write facility with zIIPs not configured.

66. Configuration Assistant: Import of policy configuration data.

67. Configuration Assistant: IP address groups.

68. NMI: IP security enhancements.

69. NMI: Timestamps collection enhancement.

70. FRCA cache enhancements for WebSphere Application Server.

71. SNMP enhancements.

72. Socket API timeout support.

73. Optimize asynchronous socket receive use of 64-bit shared memory.

74. Path MTU discovery for Enterprise Extender for IP.

75. IBM Health Checker for z/OS enhancements.

76. Netstat enhancements.

77. OMPROUTE enhancements.

78. Diagnostic enhancements for TCP/IP host name configuration problems.

79. IPCS formatter enhancements.

80. Data trace enhancements.

81. Packet trace enhancements.

82. TCP/IP SMF record enhancements.

83. Allow DNS BIND 9 server to run with BPX.SUPERUSER authorization function.

84. ASID reuse for TCP/IP, TN3270E, and resolver.

85. Resolver support for EDNS0.

86. FTP application data enhancements.

87. FTP client API for Java.

88. FTP JES enhancements.

89. FTP enhancements: Configure the FTP server to support writing to a batch pipe subsystem.

90. FTP and MVS data set contention enhancements.

91. FTP keepalive enhancements.

92. Path MTU discovery for Enterprise Extender.

93. Extended border node searching enhancement.

94. TGN parameter for EE model PUs.

95. Stalled HPR pipe termination.

96. RTP pipe session limit control.

97. Display RTP enhancements.

98. MAXLOCAT enhancement.

99. Start option for CSDUMP triggers.

100. TCP/IP performance improvements for SNA.

101. IPCS support of VTAM display commands.

102. OSA-Express3 multi-port support.
About this document

The purpose of this document is to describe the exploitation considerations of the new functions for the TCP/IP and SNA components of z/OS® Version 1 Release 11 Communications Server (z/OS Communications Server). It also includes the exploitation considerations of z/OS V1R10 Communications Server.

The information in this document supports both IPv6 and IPv4. Unless explicitly noted, information describes IPv4 networking protocol. IPv6 support is qualified within the text.

z/OS Communications Server exploits z/OS UNIX® services even for traditional MVS™ environments and applications. Therefore, before using TCP/IP services, your installation must establish a full-function mode z/OS UNIX environment—including a Data Facility Storage Management Subsystem (DFSMStpd™), a Hierarchical File System (HFS), and a security product (such as Resource Access Control Facility, or RACF®)—before z/OS Communications Server can be started successfully. Refer to z/OS UNIX System Services Planning for more information.

Throughout this document when the term RACF is used, it means RACF or an SAF-compliant security product.

This document refers to Communications Server data sets by their default SMP/E distribution library name. Your installation might, however, have different names for these data sets where allowed by SMP/E, your installation personnel, or administration staff. For instance, this document refers to samples in SEZAINST library as simply in SEZAINST. Your installation might choose a data set name of SYS1.SEZAINST, CS390.SEZAINST or other high level qualifiers for the data set name.

Who should read this document

This document is designed for planners, system programmers, and network administrators who are planning to install z/OS Communications Server and who want to learn more about its new and enhanced features.

To use the IP functions described in this document, you need to be familiar with Transmission Control Protocol/Internet Protocol (TCP/IP) and the z/OS platform.

To use the SNA functions described in this document, you need to be familiar with the basic concepts of telecommunication, SNA, VTAM®, and the z/OS platform.

How this document is organized

This document contains these topics:

- Chapter 1, “Planning to use new functions,” on page 1 includes a brief introduction to z/OS Communications Server, information about hardware requirements, references to documents that will help you if you are migrating, information about the IP encryption features, a planning checklist, and data set information.
How to use this document

Use this document as a brief introduction to z/OS Communications Server and as an introduction to every function and enhancement of the current and most recent releases of z/OS Communications Server.

The roadmap topics show you a list of the functions of the current and most recent releases. Use the roadmaps to see a release at a glance and to determine which functions have tasks that are necessary to exploit the functions.

Use the function summary topics to learn about this information:

• A brief description of the function or enhancement
• Identification of the area that the function is designed to improve, such as customization or diagnosis
• Restrictions of the function, if any
• A task table identifying the actions necessary to use the function
• References to the documents that contain more detailed information

Determining whether a publication is current

As needed, IBM updates its publications with new and changed information. For a given publication, updates to the hardcopy and associated BookManager softcopy are usually available at the same time. Sometimes, however, the updates to hardcopy and softcopy are available at different times. The following information describes how to determine if you are looking at the most current copy of a publication:

• At the end of a publication’s order number there is a dash followed by two digits, often referred to as the dash level. A publication with a higher dash level is more current than one with a lower dash level. For example, in the publication order number GC28-1747-07, the dash level 07 means that the publication is more current than previous levels, such as 05 or 04.

• If a hardcopy publication and a softcopy publication have the same dash level, it is possible that the softcopy publication is more current than the hardcopy.
publication. Check the dates shown in the Summary of Changes. The softcopy publication might have a more recently dated Summary of Changes than the hardcopy publication.

- To compare softcopy publications, you can check the last two characters of the publication’s file name (also called the book name). The higher the number, the more recent the publication. Also, next to the publication titles in the CD-ROM booklet and the readme files, there is an asterisk (*) that indicates whether a publication is new or changed.

**How to contact IBM service**


Most problems can be resolved at this Web site, where you can submit questions and problem reports electronically, as well as access a variety of diagnosis information.

For telephone assistance in problem diagnosis and resolution (in the United States or Puerto Rico), call the IBM Software Support Center anytime (1-800-IBM-SERV). You will receive a return call within 8 business hours (Monday – Friday, 8:00 a.m. – 5:00 p.m., local customer time).

Outside the United States or Puerto Rico, contact your local IBM representative or your authorized IBM supplier.

If you would like to provide feedback on this publication, see “Communicating Your Comments to IBM” on page 181.

---

**Conventions and terminology that are used in this document**

Commands in this book that can be used in both TSO and z/OS UNIX environments use the following conventions:

- When describing how to use the command in a TSO environment, the command is presented in uppercase (for example, NETSTAT).
- When describing how to use the command in a z/OS UNIX environment, the command is presented in bold lowercase (for example, netstat).
- When referring to the command in a general way in text, the command is presented with an initial capital letter (for example, Netstat).

All of the exit routines described in this document are installation-wide exit routines. You will see the installation-wide exit routines also called installation-wide exits, exit routines, and exits throughout this document.

The TPF logon manager, although shipped with VTAM, is an application program. Therefore, the logon manager is documented separately from VTAM.

Samples used in this book might not be updated for each release. Evaluate a sample carefully before applying it to your system.

For definitions of the terms and abbreviations that are used in this document, you can view the latest IBM terminology at [the IBM Terminology Web site](http://www.software.ibm.com/network/comms/server/support/)
Clarification of notes

Information traditionally qualified as Notes is further qualified as follows:

Note  Supplemental detail
Tip   Offers shortcuts or alternative ways of performing an action; a hint
Guideline
     Customary way to perform a procedure
Rule  Something you must do; limitations on your actions
Restriction
     Indicates certain conditions are not supported; limitations on a product or facility
Requirement
     Dependencies, prerequisites
Result  Indicates the outcome

Prerequisite and related information

z/OS Communications Server function is described in the z/OS Communications Server library. Descriptions of those documents are listed in "Bibliography" on page 171, in the back of this document.

Required information

Before using this product, you should be familiar with TCP/IP, VTAM, MVS, and UNIX System Services.

Softcopy information

Softcopy publications are available in the following collections.

<table>
<thead>
<tr>
<th>Titles</th>
<th>Order Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS V1R11 Collection</td>
<td>SK3T-4269</td>
<td>This is the CD collection shipped with the z/OS product. It includes the libraries for z/OS V1R11, in both BookManager and PDF formats.</td>
</tr>
<tr>
<td>z/OS Software Products Collection</td>
<td>SK3T-4270</td>
<td>This CD includes, in both BookManager and PDF formats, the libraries of z/OS software products that run on z/OS but are not elements and features, as well as the Getting Started with Parallel Sysplex® bookshelf.</td>
</tr>
<tr>
<td>z/OS V1R11 and Software Products DVD Collection</td>
<td>SK3T-4271</td>
<td>This collection includes the libraries of z/OS (the element and feature libraries) and the libraries for z/OS software products in both BookManager and PDF format. This collection combines SK3T-4269 and SK3T-4270.</td>
</tr>
<tr>
<td>z/OS Licensed Product Library</td>
<td>SK3T-4307</td>
<td>This CD includes the licensed documents in both BookManager and PDF format.</td>
</tr>
</tbody>
</table>
IBM System z Redbooks Collection

SK3T-7876

The Redbooks selected for this CD series are taken from the IBM Redbooks inventory of over 800 books. All the Redbooks that are of interest to the zSeries platform professional are identified by their authors and are included in this collection. The zSeries subject areas range from e-business application development and enablement to hardware, networking, Linux*, solutions, security, parallel sysplex, and many others.

Other documents

For information about z/OS products, refer to z/OS Information Roadmap (SA22-7500). The Roadmap describes what level of documents are supplied with each release of z/OS Communications Server, as well as describing each z/OS publication.

Relevant RFCs are listed in an appendix of the IP documents. Architectural specifications for the SNA protocol are listed in an appendix of the SNA documents.

The following table lists documents that might be helpful to readers.

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNA Formats</td>
<td>GA27-3136</td>
</tr>
<tr>
<td>TCP/IP Tutorial and Technical Overview</td>
<td>GG24-3376</td>
</tr>
<tr>
<td>Understanding LDAP</td>
<td>SG24-4986</td>
</tr>
<tr>
<td>z/OS Cryptographic Services System SSL Programming</td>
<td>SC24-5901</td>
</tr>
<tr>
<td>z/OS Integrated Security Services LDAP Server Administration and Use</td>
<td>SC24-5923</td>
</tr>
<tr>
<td>z/OS JES2 Initialization and Tuning Guide</td>
<td>SA22-7532</td>
</tr>
<tr>
<td>z/OS Problem Management</td>
<td>G325-2564</td>
</tr>
<tr>
<td>z/OS MVS Diagnosis: Reference</td>
<td>GA22-7588</td>
</tr>
<tr>
<td>z/OS MVS Diagnosis: Tools and Service Aids</td>
<td>GA22-7589</td>
</tr>
<tr>
<td>z/OS MVS Using the Subsystem Interface</td>
<td>SA22-7642</td>
</tr>
<tr>
<td>z/OS Program Directory</td>
<td>G110-0670</td>
</tr>
<tr>
<td>z/OS UNIX System Services Command Reference</td>
<td>SA22-7802</td>
</tr>
<tr>
<td>z/OS UNIX System Services Planning</td>
<td>GA22-7800</td>
</tr>
<tr>
<td>z/OS UNIX System Services Programming: Assembler Callable Services Reference</td>
<td>SA22-7803</td>
</tr>
<tr>
<td>z/OS UNIX System Services User’s Guide</td>
<td>SA22-7801</td>
</tr>
<tr>
<td>z/OS XL C/C++ Run-Time Library Reference</td>
<td>SA22-7821</td>
</tr>
</tbody>
</table>
Redbooks

The following Redbooks might help you as you implement z/OS Communications Server.

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications Server for z/OS V1R10 TCP/IP Implementation, Volume 1: Base Functions, Connectivity, and Routing</td>
<td>SG24-7696</td>
</tr>
<tr>
<td>Communications Server for z/OS V1R10 TCP/IP Implementation, Volume 2: Standard Applications</td>
<td>SG24-7697</td>
</tr>
<tr>
<td>Communications Server for z/OS V1R10 TCP/IP Implementation, Volume 3: High Availability, Scalability, and Performance</td>
<td>SG24-7698</td>
</tr>
<tr>
<td>Communications Server for z/OS V1R10 TCP/IP Implementation, Volume 4: Security and Policy-Based Networking</td>
<td>SG24-7699</td>
</tr>
<tr>
<td>IBM Communication Controller Migration Guide</td>
<td>SG24-6298</td>
</tr>
<tr>
<td>IP Network Design Guide</td>
<td>SG24-2580</td>
</tr>
<tr>
<td>Managing OS/390 TCP/IP with SNMP</td>
<td>SG24-5866</td>
</tr>
<tr>
<td>Migrating Subarea Networks to an IP Infrastructure Using Enterprise Extender</td>
<td>SG24-5957</td>
</tr>
<tr>
<td>SecureWay™ Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements</td>
<td>SG24-5631</td>
</tr>
<tr>
<td>SNA and TCP/IP Integration</td>
<td>SG24-5291</td>
</tr>
<tr>
<td>TCP/IP in a Sysplex</td>
<td>SG24-5235</td>
</tr>
<tr>
<td>TCP/IP Tutorial and Technical Overview</td>
<td>GG24-3376</td>
</tr>
<tr>
<td>Threadsafe Considerations for CICS</td>
<td>SG24-6351</td>
</tr>
</tbody>
</table>

Where to find related information on the Internet

z/OS

This site provides information about z/OS Communications Server release availability, migration information, downloads, and links to information about z/OS technology

http://www.ibm.com/systems/z/os/zos/

z/OS Internet Library

Use this site to view and download z/OS Communications Server documentation

www.ibm.com/systems/z/os/zos/bkserv/

IBM Communications Server product

The primary home page for information about z/OS Communications Server

http://www.software.ibm.com/network/commsserver/

IBM Communications Server product support
Use this site to submit and track problems and search the z/OS Communications Server knowledge base for Technotes, FAQs, white papers, and other z/OS Communications Server information


IBM Communications Server performance information

This site contains links to the most recent Communications Server performance reports.

http://www.ibm.com/support/docview.wss?uid=swg27005524

IBM Systems Center publications

Use this site to view and order Redbooks, Redpapers, and Technotes

http://www.redbooks.ibm.com/

IBM Systems Center flashes

Search the Technical Sales Library for Techdocs (including Flashes, presentations, Technotes, FAQs, white papers, Customer Support Plans, and Skills Transfer information)

http://www.ibm.com/support/techdocs/atsmastr.nsf

RFCs

Search for and view Request for Comments documents in this section of the Internet Engineering Task Force Web site, with links to the RFC repository and the IETF Working Groups Web page

http://www.ietf.org/rfc.html

Internet drafts

View Internet-Drafts, which are working documents of the Internet Engineering Task Force (IETF) and other groups, in this section of the Internet Engineering Task Force Web site

http://www.ietf.org/ID.html

Information about Web addresses can also be found in information APAR III11334.

Note: Any pointers in this publication to Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

DNS Web sites

For more information about DNS, see the following USENET news groups and mailing addresses:

USENET news groups
comp.protocols.dns.bind

BIND mailing lists
http://www.isc.org/ml-archives/

BIND Users

- Subscribe by sending mail to bind-users-request@isc.org.
- Submit questions or answers to this forum by sending mail to bind-users@isc.org.

BIND 9 Users (This list might not be maintained indefinitely.)
The z/OS Basic Skills Information Center

The z/OS Basic Skills Information Center is a Web-based information resource intended to help users learn the basic concepts of z/OS, the operating system that runs most of the IBM mainframe computers in use today. The Information Center is designed to introduce a new generation of Information Technology professionals to basic concepts and help them prepare for a career as a z/OS professional, such as a z/OS system programmer.

Specifically, the z/OS Basic Skills Information Center is intended to achieve the following objectives:

- Provide basic education and information about z/OS without charge
- Shorten the time it takes for people to become productive on the mainframe
- Make it easier for new people to learn z/OS

To access the z/OS Basic Skills Information Center, open your Web browser to the following Web site, which is available to all users (no login required):

http://publib.boulder.ibm.com/infocenter/zoslnctr/v1r7/index.jsp

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this document or any other z/OS Communications Server documentation, do one of the following:

- Go to the z/OS contact page at http://www.ibm.com/systems/z/os/zos/webqs.html. You can enter and submit your comments in the form provided at this Web site.
- Send your comments by e-mail to comsvrcf@us.ibm.com. Be sure to include the name of the document, the part number of the document, the version of z/OS Communications Server, and, if applicable, the specific location of the text that you are commenting on (for example, a section number, a page number or a table number).
Summary of changes

Summary of changes
for GC31-8771-05
z/OS Version 1 Release 11

This document contains information previously presented in GC31-8771-04, which supports z/OS Version 1 Release 10.

New information

Chapter 3, “V1R11 new function summary,” on page 25 includes descriptions for the new functions and enhancements introduced in this release and explains how to use them. Entries for the new functions and enhancements are added to Chapter 2, “Roadmap to functions,” on page 21.

Changed information

The IP and SNA sections are combined in chapters by release; they are no longer presented separately.

Deleted information

- The release summary chapters for z/OS V1R9 are deleted and the V1R9 entries are deleted from Chapter 2, “Roadmap to functions,” on page 21.

You can still access the old release summary documentation at this Web site: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/.

This document includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

You might notice changes in the style and structure of some content in this document—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

Summary of changes
for GC31-8771-04
z/OS Version 1 Release 10

This document contains information previously presented in GC31-8771-03, which supports z/OS Version 1 Release 9.

New information

- Chapter 3. V1R10 IP new function summary includes descriptions and exploitation procedures for the new IP functions and enhancements introduced in this release. Entries for the new functions and enhancements are added to Chapter 2. Roadmap to IP functions.
- Chapter 6. V1R10 SNA new function summary includes descriptions and exploitation procedures for the new SNA functions and enhancements
introduced in this release. Entries for the new functions and enhancements are added to Chapter 5. Roadmap to SNA functions.

**Deleted information**

- The release summary chapters for z/OS V1R8 are deleted. Likewise, the entries related to those releases are deleted from Chapter 2. Roadmap to IP functions and Chapter 5. Roadmap to SNA functions.


This document includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

You might notice changes in the style and structure of some content in this document—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.
Chapter 1. Planning to use new functions

These topics help you plan to use new functions:
- “Introduction to z/OS Communications Server”
- “Determining which documents to use when migrating”
- “IP encryption features” on page 2
- “Planning checklist” on page 3
- “TCP/IP packaging process” on page 4
- “Defining SNA data sets” on page 7

Introduction to z/OS Communications Server

z/OS Communications Server is a network communication access method. It provides both Systems Network Architecture (SNA) and Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocols for z/OS.

The TCP/IP protocol suite (also called stack), includes associated applications, transport- and network-protocol layers, and connectivity and gateway functions. See z/OS Communications Server: IP Configuration Guide for more information about z/OS Communications Server IP protocols.

The SNA protocols are provided by VTAM and include Subarea, Advanced Peer-to-Peer Networking® (APPN), and High Performance Routing protocols. z/OS Communications Server provides the interface between application programs residing in a host processor, and resources residing in an SNA network; it also links peer users in the network. See z/OS Communications Server: SNA Network Implementation Guide for more information about z/OS Communications Server SNA protocols.

For the purposes of this library, the following descriptions apply:

- The IBM System z10™ product line includes IBM System z10™ Enterprise Class (z10 EC™) and the IBM System z10 Business Class™ (z10 BC™).
- The IBM System z9® product line includes IBM System z9 Enterprise Class (z9® EC) (formerly known as the IBM System z9 109 [z9-109]), and the IBM System z9 Business Class (z9 BC).
- The IBM eServer™ zSeries product line includes the IBM eServer zSeries 990 (z990), 890 (z890), 900 (z900) and 800 (z800).
- The IBM System 390 (S/390®) product line includes the IBM S/390 Parallel Enterprise Server™ Generation 5 (G5) and Generation 6 (G6), and the IBM S/390 Multiprise® 3000 Enterprise Server.

The z10 EC, z10 BC, z9 EC (formerly z9-109), z9 BC, z990, z890, z900, and z800 servers are also known as z/Architecture® servers. z/OS V1R11 Communications Server runs only in z/Architecture mode on z/Architecture servers. The G5, G6, and Multiprise 3000 servers are not supported for z/OS V1R11 Communications Server.

Determining which documents to use when migrating

This table will help you determine which documents to use as you migrate.
Table 1. Comparing documents used in migration

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| z/OS Planning for Installation       | This document helps you prepare to install z/OS or z/OS.e by giving you information you need to write an installation plan. To install means to perform the tasks necessary to make the system operational, starting with a decision to either install for the first time or upgrade, and ending when the system is ready for production. An installation plan is a record of the actions you need to take to install z/OS or z/OS.e.  
**Recommendation:** It is strongly recommended that you read this document.  
Use this document as you prepare to install z/OS or z/OS.e. |
| z/OS Migration                       | This document describes how to migrate (convert) from release to release. After a successful migration, the applications and resources on your new z/OS system will function the same way they did previously.  
Use this document as a reference in keeping all z/OS applications working as they did in previous releases. |
| z/OS Introduction and Release Guide  | This document provides an overview of z/OS and lists the enhancements in each release.  
Use this document to determine whether to obtain a new release and to decide which new functions to implement. |
| z/OS Summary of Message and Interface Changes | This document describes the changes to interfaces for individual elements and features of z/OS.  
Use this document as a reference to the new and changed commands, macros, panels, exit routines, data areas, messages, and other interfaces of individual elements and features of z/OS. |
| z/OS Communications Server: New Function Summary | This document includes function summary topics to describe all the functional enhancements for the IP and SNA components of Communications Server, including task tables that identify the actions necessary to exploit new function.  
Use this document as a reference to using all the enhancements of z/OS Communications Server. |

For an overview and map of the documentation available for z/OS, see the [z/OS Information Roadmap](#).

**IP encryption features**

Encryption features are available for IP at no additional cost. Communications Server Security Level 3 is an optional unpriced feature and must be ordered.

The encryption features include these capabilities:

**Level 1**  
This level of encryption is included in the base of z/OS V1R11 Communications Server.

**Level 2**  
This level of encryption is included in the base of z/OS V1R11 Communications Server and offers IP security protocol (IPSec) DES and SNMPv3 56-bit DES.

**Level 3**  
This level of encryption is included in the Communications Server Security Level 3 optional unpriced feature and offers IPSec Triple DES and AES.
Planning checklist

Migrating a z/OS Communications Server system from a previous release involves considerable planning. To familiarize yourself with the migration process, review this checklist. Tailor the checklist to meet the specific requirements of your installation.

__ 1. Understand your network topology, including the hardware and software in your network and your network configuration.

__ 2. Understand that z/OS V1R11 Communications Server is a base element of z/OS. Use the appropriate documents as you plan, migrate, and install:
   For information about migration and writing an installation plan, see "Determining which documents to use when migrating" on page 1.
   For information about installation, see these documents:
   • [z/OS Program Directory](#)
   • Preventative Service Planning (PSP) bucket (available by using IBMLINK)
   • Softcopy Installation Memo (for Bookmanager publications)
   • [ServerPac: Installing Your Order](#), if you use the ServerPac method to install z/OS
   For information about storage requirements, see the [z/OS Program Directory](#), IBMLINK, or [z/OS Communications Server Support](#). You can also see the storage estimate worksheets in [z/OS Communications Server: SNA Network Implementation Guide](#).

__ 3. Develop your education plan:
   • Evaluate the z/OS V1R11 Communications Server features and enhancements by reading the new function summary topics in this document. Plan which new functions will be incorporated into your system.

__ 4. Review and apply the Program Temporary Fixes (PTFs), including Recommended Service Upgrades (RSUs), for the current-minus-3 month plus all hipers and PEs. The PTFs are available monthly through the period for which the release is current and can be obtained by using IBMLINK.
   RSU integration testing for a release will be performed for five quarters after the general availability date for that release.

__ 5. Get acquainted with the helpful information found at [z/OS Communications Server Support](#).

__ 6. In writing a test plan for z/OS, include test cases for these items:
   • TCP/IP applications
   • Key or critical SNA applications and Original Equipment Manufacturer (OEM) software products.
   • User-written applications such as: Customer Information Control System (CICS®) sockets, Information Management System (IMS™) sockets, REXX™ sockets, Sockets Extended, UNIX System Services sockets, and Macro Sockets
   • Operator commands
   • Your terminal and printer types

__ 7. Back up your user exits and user modifications for later restore.

__ 8. Install z/OS Communications Server with the other elements and features of z/OS. IBM has defined the appropriate product enablement settings in the IFAPRD00 member of SYS1.IBM.PARMLIB. For information about dynamic enablement, see [z/OS Planning for Installation](#).

__ 9. Complete post-installation activities:
• Use **z/OS Communications Server: IP Configuration Guide** to customize your TCP/IP system.

• Use the following to customize your SNA system:
  - **z/OS Communications Server: SNA Customization**
  - **z/OS Communications Server: SNA Network Implementation Guide**
  - **z/OS Communications Server: SNA Resource Definition Reference**

• Use **z/OS Migration** to determine migration actions.

• Reinstall user exits.

• Reinstall user modifications.

• Update operating procedures and automation routines.

• Activate new functions.


---

**TCP/IP packaging process**

As a result of the installation process for **z/OS V1R11 Communications Server**, the product is installed in both traditional MVS data sets and in files in the z/OS UNIX HFS. For details on changes in the MVS data sets, see "MVS data sets." For details on requirements for HFS files, see "File system files" on page 7.

---

**MVS data sets**

*Table 2* lists the distribution library data sets required by **z/OS V1R11 Communications Server**.

*Table 2. Distribution library data sets*

<table>
<thead>
<tr>
<th>Data set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEZADBR1</td>
<td>Database Request Module (DBRM) members</td>
</tr>
<tr>
<td>AHELP</td>
<td>TSO help files</td>
</tr>
<tr>
<td>AEZAMAC1</td>
<td>Assembler macros</td>
</tr>
<tr>
<td>AEZAMAC2</td>
<td>C header files</td>
</tr>
<tr>
<td>AEZAMAC3</td>
<td>Pascal include files</td>
</tr>
<tr>
<td>AEZAMODS</td>
<td>Distribution library for base link-edit modules</td>
</tr>
<tr>
<td>AEZARNT1</td>
<td>Reentrant object module for SEZAX11L, SEZAXTLB, SEZAOLDX, and SOCKETS</td>
</tr>
<tr>
<td>AEZARNT2</td>
<td>Reentrant object module for SEZAXAWL</td>
</tr>
<tr>
<td>AEZARNT3</td>
<td>Reentrant object module for SEZAXMLB</td>
</tr>
<tr>
<td>AEZAROE2</td>
<td>Reentrant object module for SEZAXAWL (z/OS UNIX support)</td>
</tr>
<tr>
<td>AEZAROE3</td>
<td>Reentrant object module for SEZAXMLB (z/OS UNIX support)</td>
</tr>
<tr>
<td>AEZARNT4</td>
<td>Reentrant object modules for RPC</td>
</tr>
<tr>
<td>AEZAROE1</td>
<td>Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)</td>
</tr>
<tr>
<td>AEZASMP1</td>
<td>Sample source programs, catalog procedures, CLIST, and installation jobs</td>
</tr>
<tr>
<td>AEZAXLTD</td>
<td>Translated default tables</td>
</tr>
<tr>
<td>AEZAXLTK</td>
<td>Translated Kanji, Hangeul, and Traditional Chinese DBCS tables and codefiles</td>
</tr>
</tbody>
</table>
### Table 2. Distribution library data sets (continued)

<table>
<thead>
<tr>
<th>Data set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEZAXLT1</td>
<td>Translation table SBCS source and DBCS source for Hangeul and Traditional Chinese</td>
</tr>
<tr>
<td>AEZAXLT2</td>
<td>TELNET client translation tables</td>
</tr>
<tr>
<td>AEZAXLT3</td>
<td>Kanji DBCS translation table source</td>
</tr>
<tr>
<td>ABLSCLI0</td>
<td>clists, execs, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables</td>
</tr>
<tr>
<td>ABLSMMSG0</td>
<td>messages, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables</td>
</tr>
<tr>
<td>ABLSPNL0</td>
<td>panels, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables</td>
</tr>
<tr>
<td>ABLSTBL0</td>
<td>tables, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables</td>
</tr>
</tbody>
</table>

Table 3 lists the target library data sets required by z/OS V1R11 Communications Server.

### Table 3. Target library data sets

<table>
<thead>
<tr>
<th>Data set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEZACMAC</td>
<td>Client Pascal macros, C headers, and assembler macros</td>
</tr>
<tr>
<td>SEZACMTX</td>
<td>Load library for linking user modules and programs</td>
</tr>
<tr>
<td>SEZADBCX</td>
<td>Source for the Kanji, Hangeul, and Traditional Chinese DBCS translation tables</td>
</tr>
<tr>
<td>SEZADBRM</td>
<td>DBRM members</td>
</tr>
<tr>
<td>SEZADPIL</td>
<td>SNMP Distributed Programming Interface library</td>
</tr>
<tr>
<td>SEZADSIL</td>
<td>SNMP command processor and SNMP/IUCV subtask for the NetView® program, and the SQESERV module for the SNMP query engine</td>
</tr>
<tr>
<td>SEZADSIM</td>
<td>SNMP messages for the NetView program</td>
</tr>
<tr>
<td>SEZADSIP</td>
<td>SNMP/IUCV initialization parameters for the NetView program</td>
</tr>
<tr>
<td>SEZAEEXEC</td>
<td>CLISTs and REXX programs</td>
</tr>
<tr>
<td>SEZAINST</td>
<td>Installation samples and related members</td>
</tr>
<tr>
<td>SEZALIBN</td>
<td>NCS library system library</td>
</tr>
<tr>
<td>SEZALOAD</td>
<td>Executable load modules for concatenation to LINKLIB</td>
</tr>
<tr>
<td>SEZALNK2</td>
<td>LB@ADMIN for the NCS administrator</td>
</tr>
<tr>
<td>SEZALPA</td>
<td>Executable load modules for concatenation to LPALST</td>
</tr>
<tr>
<td>SEZAMENU</td>
<td>ISPF messages</td>
</tr>
<tr>
<td>SEZANCLS</td>
<td>NetView SNMP CLISTs</td>
</tr>
<tr>
<td>SEZANMAC</td>
<td>C headers and assembler macros for z/OS UNIX and TCP/IP Services APIs</td>
</tr>
<tr>
<td>SEZANPNL</td>
<td>NetView SNMP panels</td>
</tr>
<tr>
<td>SEZAOLDX</td>
<td>X Window System library (X10 compatibility routines)</td>
</tr>
<tr>
<td>SEZAPENU</td>
<td>ISPF panels</td>
</tr>
<tr>
<td>SEZARNT1</td>
<td>Reentrant object module for SEZAX11L, SEZAXTLB, SEZAOLDX, and SOCKETS</td>
</tr>
<tr>
<td>SEZARNT2</td>
<td>Reentrant object module for SEZAXawl</td>
</tr>
</tbody>
</table>
Table 3. Target library data sets (continued)

<table>
<thead>
<tr>
<th>Data set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEZARNT3</td>
<td>Reentrant object module for SEZAXMLB</td>
</tr>
<tr>
<td>SEZARNT4</td>
<td>Reentrant object modules for RPC</td>
</tr>
<tr>
<td>SEZAROE1</td>
<td>Reentrant object module for SEZAXI1L, SEZAXTLB, and SEZAOLODX (z/OS UNIX support)</td>
</tr>
<tr>
<td>SEZAROE2</td>
<td>Reentrant object module for SEZAXAWL (z/OS UNIX support)</td>
</tr>
<tr>
<td>SEZAROE3</td>
<td>Reentrant object module for SEZAXMLB (z/OS UNIX support)</td>
</tr>
<tr>
<td>SEZARPCL</td>
<td>Remote procedure call library</td>
</tr>
<tr>
<td>SEZATCP</td>
<td>Executable load modules for STEPLIB or LNKLIST concatenation</td>
</tr>
<tr>
<td>SEZATCPX</td>
<td>Source for the country SBCS translation tables</td>
</tr>
<tr>
<td>SEZATELX</td>
<td>Source for the TELNET country translation tables</td>
</tr>
<tr>
<td>SEZAXAWL</td>
<td>Athena widget set</td>
</tr>
<tr>
<td>SEZAXLD1</td>
<td>Translated default tables</td>
</tr>
<tr>
<td>SEZAXLD2</td>
<td>Translated Kanji, Hangeul, and Traditional Chinese DBCS default tables and DBCS codefiles for TELNET transform mode</td>
</tr>
<tr>
<td>SEZAXMLB</td>
<td>Motif widget set</td>
</tr>
<tr>
<td>SEZAXTLB</td>
<td>X Window System Toolkit library</td>
</tr>
<tr>
<td>SEZAXI11L</td>
<td>X Window System library</td>
</tr>
</tbody>
</table>

Table 4 lists the shared distribution and target library data sets required by z/OS V1R11 Communications Server.

Table 4. Shared distribution and target library data sets

<table>
<thead>
<tr>
<th>Data set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS1.CSSLIB</td>
<td>Interface routines for accessing callable services</td>
</tr>
<tr>
<td>SYS1.HELP</td>
<td>TSO help files</td>
</tr>
<tr>
<td>SYS1.MIGLIB</td>
<td>z/OS Communications Server formatted dump routines for the interactive problem control system (IPCS) and the z/OS Communications Server VIT Analysis Tool module, ISTRAFT1, which is used for problem diagnosis</td>
</tr>
<tr>
<td>SYS1.MSGENU / SYS1.AMSGENU</td>
<td>English-language message tables used by the MVS message service (MMS)</td>
</tr>
<tr>
<td>SYS1.NUCLEUS</td>
<td>Resident SVCs, callable services tables, and abnormal termination modules</td>
</tr>
<tr>
<td>SYS1.PARMLIB / SYS1.APARMLIB</td>
<td>IBM-supplied and installation-created members, which contain lists of system parameter values</td>
</tr>
<tr>
<td>SYS1.SAXREXEC</td>
<td>Contains system REXX programs</td>
</tr>
<tr>
<td>SYS1.SBLSQLCLI0</td>
<td>IPCS REXX execs and CListS</td>
</tr>
<tr>
<td>SYS1.SBLSKEL0</td>
<td>ISPF skeletons for the IPS Dialog</td>
</tr>
<tr>
<td>SYS1.SBLMESSAGE</td>
<td>ISPF messages for the IPS Dialog</td>
</tr>
<tr>
<td>SYS1.SBLSPNL0</td>
<td>ISPF panels for the IPS Dialog</td>
</tr>
<tr>
<td>SYS1.SBLSTBL0</td>
<td>ISPF tables for the IPS Dialog</td>
</tr>
</tbody>
</table>
File system files

See z/OS UNIX System Services Planning and z/OS UNIX System Services User’s Guide for a description of the file system files.

Defining SNA data sets

This section describes z/OS data sets that you need to define or modify for z/OS V1R11 Communications Server. Table 5 shows the z/OS data sets that contain information for z/OS V1R11 Communications Server, and Table 6 on page 9 shows the z/OS data sets that contain information for both VTAM and NCP.

Enterprise Extender requires IP dataset definitions in addition to the SNA data sets. See z/OS Communications Server: IP Configuration Guide for more information.

These tables show the data sets and the approximate storage requirements for any new data sets and for any existing data sets whose requirements might have changed since your last installation.

Table 5. z/OS data sets containing information for z/OS Communications Server

<table>
<thead>
<tr>
<th>Name of data set</th>
<th>Contents</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS1.DSDB1</td>
<td>Data files of APPN directory information</td>
<td>Required for APPN directory checkpointing function; must be allocated before z/OS Communications Server initialization. This data set cannot be allowed to span multiple volumes.</td>
</tr>
<tr>
<td>SYS1.DSDB2</td>
<td>Data files of APPN directory information</td>
<td>Required for APPN directory checkpointing function; must be allocated before z/OS Communications Server initialization. This data set cannot be allowed to span multiple volumes.</td>
</tr>
<tr>
<td>SYS1.DSDBCTRL</td>
<td>Current status of SYS1.DSDB1 and SYS1.DSDB2</td>
<td>Required for APPN directory checkpointing function; must be allocated before z/OS Communications Server initialization. This data set cannot be allowed to span multiple volumes.</td>
</tr>
<tr>
<td>SYS1.DUMPxx</td>
<td>Records of SVC DUMP</td>
<td>Required for diagnosis.</td>
</tr>
<tr>
<td>SYS1.LINKLIB</td>
<td>z/OS Communications Server initialization module, ISTINM01, which is used when z/OS Communications Server is started</td>
<td>Required.</td>
</tr>
<tr>
<td>SYS1.LPALIB</td>
<td>z/OS Communications Server load modules and user-written exit routines to be loaded into the shared link pack area</td>
<td>Required.</td>
</tr>
<tr>
<td>SYS1.MACLIB</td>
<td>z/OS Communications Server application program interface macros</td>
<td>Required.</td>
</tr>
<tr>
<td>Name of data set</td>
<td>Contents</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SYS1.MIGLIB</td>
<td>z/OS Communications Server formatted dump routines for the interactive problem control system (IPCS) and the z/OS Communications Server VIT Analysis Tool module, ISTRAFT1, which is used for problem diagnosis</td>
<td>Required.</td>
</tr>
<tr>
<td>SYS1.NUCLEUS</td>
<td>z/OS Communications Server resident SVCs and abnormal termination modules</td>
<td>Required.</td>
</tr>
<tr>
<td>SYS1.PARMLIB</td>
<td>IBM-supplied and installation-created members, which contain lists of system parameter values</td>
<td>Required. This may also be a data set in the logical parmlib concatenation.</td>
</tr>
<tr>
<td>SYS1.PROCLIB</td>
<td>JCL for started tasks</td>
<td>Required for logon manager.</td>
</tr>
<tr>
<td>SYS1.SBLSCLI0</td>
<td>IPCS REXX execs and CLISTs</td>
<td>Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See <a href="http://www.ibm.com">z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures</a> for more information.</td>
</tr>
<tr>
<td>SYS1.SBLSKEL0</td>
<td>ISPF skeletons for the IPCS dialog</td>
<td>Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See <a href="http://www.ibm.com">z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures</a> for more information.</td>
</tr>
<tr>
<td>SYS1.SBLSMSG0</td>
<td>ISPF messages for the IPCS dialog</td>
<td>Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See <a href="http://www.ibm.com">z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures</a> for more information.</td>
</tr>
<tr>
<td>SYS1.SBLSPNL0</td>
<td>ISPF panels for the IPCS dialog</td>
<td>Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See <a href="http://www.ibm.com">z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures</a> for more information.</td>
</tr>
<tr>
<td>SYS1.SBLSTBL0</td>
<td>ISPF tables for the IPCS dialog</td>
<td>Required for z/OS Communications Server dump analysis enhancements and VIT analysis.</td>
</tr>
<tr>
<td>SYS1.SISTASGD</td>
<td>ASN.1 and GDMO syntax data sets</td>
<td>Included for reference by CMIP services application programmers.</td>
</tr>
</tbody>
</table>
| SYS1.SISTASN1    | Contains two categories of data set members:  
  • ACYPRES: List of abstract syntax notation 1 (ASN.1) definition data sets. This is a member of a partitioned data set.  
  • The members listed in ACYPRES.  
 | Required for CMIP services. See [“SYS1.SISTASN1” on page 11](#) for a description. |
| SYS1.SISTCLIB    | z/OS Communications Server load modules to be loaded into common service area and extended common service area (CSA/ECSA) storage | Required. |
| SYS1.SISTCMIP    | Directory definition file. The member name of the directory definition file is ACYDDF. | Required for CMIP services. See [“SYS1.SISTCMIP” on page 11](#) for a description. |
### Table 5. z/OS data sets containing information for z/OS Communications Server (continued)

<table>
<thead>
<tr>
<th>Name of data set</th>
<th>Contents</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS1.SISTDAT1</td>
<td>Online tools</td>
<td>Optional. Use this library only if you intend to use the online information tools included with z/OS Communications Server.</td>
</tr>
<tr>
<td>SYS1.SISTDAT2</td>
<td>Message skeleton file for translation</td>
<td>Required. See <a href="https://www.ibm.com">z/OS Communications Server: SNA Network Implementation Guide</a></td>
</tr>
<tr>
<td>SYS1.SISTGDMO</td>
<td>Compiled definitions for the ISO standard, Guidelines for the Definition of Managed Objects (GDMO). This is a partitioned data set consisting of one member, ACYGDMO.</td>
<td>Required for CMIP services. Member name ACYGDMO must be included on the DD statement for SISTGDMO in the VTAM start procedure: //ACYGDMO DD SYS1.SISTGDMO(ACYGDMO),DISP=SHR.</td>
</tr>
<tr>
<td>SYS1.SISTMAC1</td>
<td>z/OS Communications Server macros used to build user tables and parameter lists to build installation exits</td>
<td>Required.</td>
</tr>
<tr>
<td>SYS1.TRACE</td>
<td>GTF trace records</td>
<td>Required to run external trace. <strong>Note:</strong> For information about using multiple SYS1.TRACE data sets, see the <a href="https://www.ibm.com">z/OS MVS Diagnosis: Tools and Service Aids</a>.</td>
</tr>
<tr>
<td>SYS1.TRSDB</td>
<td>Network topology database</td>
<td>Required for APPN topology database checkpointing function; must be allocated before initialization. This data set cannot be allowed to span multiple volumes.</td>
</tr>
<tr>
<td>Dynamic I/O configuration data sets</td>
<td>Dynamically created definitions of devices with all associated LUs</td>
<td>Optional; includes USER1.AUTO.VTAMLST and a catalog entry checkpoint data set. Required for dynamic I/O configuration.</td>
</tr>
</tbody>
</table>

Table 6 shows the z/OS data sets that contain VTAM information and NCP information if there is an NCP owned by that VTAM.

### Table 6. z/OS data sets containing information for both VTAM and NCP

<table>
<thead>
<tr>
<th>Name of data set</th>
<th>Contents</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS1.ASAMPLIB</td>
<td>Sample of network operator command table and sample JCL for installation</td>
<td>Required for installation. Provided by IBM.</td>
</tr>
<tr>
<td>SYS1.SAMPLIB</td>
<td>Alterable copy of sample network operator command table, sample JCL for installation, and command lists for dynamic I/O</td>
<td>Required for installation. Provided by IBM.</td>
</tr>
<tr>
<td>SYS1.SSPLIB</td>
<td>NCP loader utility program</td>
<td>Required; added when NCP is installed. See &quot;SYS1.SSPLIB&quot; on page 19 for information on SYS1.SSPLIB requirements.</td>
</tr>
<tr>
<td></td>
<td>NCP dump utility program</td>
<td>Required; added when NCP is installed. See &quot;SYS1.SSPLIB&quot; on page 19 for information on SYS1.SSPLIB requirements.</td>
</tr>
<tr>
<td></td>
<td>NCP dump bootstrap program</td>
<td>Required; added when NCP is installed. See &quot;SYS1.SSPLIB&quot; on page 19 for information on SYS1.SSPLIB requirements.</td>
</tr>
<tr>
<td>Name of data set</td>
<td>Contents</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SYS1.VTAMLIB</td>
<td>Load modules for z/OS Communications Server</td>
<td>Only z/OS Communications Server load modules are required. Created during system generation. Must be listed in an IEAAPFxx parmlib member.</td>
</tr>
<tr>
<td></td>
<td>User-defined tables, default tables, and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit routines</td>
<td></td>
</tr>
<tr>
<td>SYS1.VTAMLST</td>
<td>z/OS Communications Server definition</td>
<td>Required; created by user before starting z/OS Communications Server. You can modify this data set, but you need to be very careful about the relationship between z/OS Communications Server and NCP definition statements. For example, changing a VTAMLST member without changing a corresponding NCP definition statement can cause serious errors that are difficult to diagnose.</td>
</tr>
<tr>
<td></td>
<td>statements and start options</td>
<td></td>
</tr>
<tr>
<td>Configuration restart data sets</td>
<td>z/OS Communications Server status of minor nodes for each major node</td>
<td>Required if a warm restart is to be used. Created by user before starting z/OS Communications Server.</td>
</tr>
<tr>
<td>SYS1.NODELST</td>
<td>z/OS Communications Server status of major</td>
<td>Required if restart of all previously active major nodes is desired.</td>
</tr>
<tr>
<td></td>
<td>nodes</td>
<td></td>
</tr>
<tr>
<td>NCP load library</td>
<td>NCP load modules</td>
<td>Each NCP stored as a separate member of library. Created during NCP generation. Must be an APF-authorized library.</td>
</tr>
<tr>
<td>NCP dump data set</td>
<td>Dump records for NCP</td>
<td>Required if z/OS Communications Server is requested to provide a dump of NCP. Created by user before starting z/OS Communications Server.</td>
</tr>
<tr>
<td>SYS1.LDRIOTAB</td>
<td>Dump records for loader channel I/O trace</td>
<td>Required to hold loader channel I/O trace dumps. Created by user before starting z/OS Communications Server.</td>
</tr>
<tr>
<td>CSP and MOSS dump data set</td>
<td>Dump records for CSP and MOSS</td>
<td>Required if z/OS Communications Server is requested to provide a dump of CSP or MOSS and if the user wants to store the CSP or MOSS dump in a unique data set. Created by user before starting z/OS Communications Server.</td>
</tr>
</tbody>
</table>

**Data sets containing information for z/OS V1R11 Communications Server**

This section describes data sets that contain information for z/OS V1R11 Communications Server.

**SYS1.SISTCLIB**

SYS1.SISTCLIB contains the z/OS Communications Server modules to be loaded into common service area and extended common service area (CSA/ECSA) storage.

To prepare the SYS1.SISTCLIB data set, do these steps:

1. Allocate the SYS1.SISTCLIB data set using a utility program, and catalog the data set before SMP/E installation. See the installation JCL sample ISTJEXAL in the z/OS Program Directory for a sample job using the IEFBR14 program to allocate SYS1.SISTCLIB.
2. Add a DD card for SYS1.SISTCLIB in the VTAM NET procedure as follows:
   */SISTCLIB DD DSN=SYS1.SISTCLIB,DISP=SHR

3. Define SYS1.SISTCLIB as an authorized library (a library listed in the currently
   used IEAAPFx).

**SYS1.SISTCMIP**

SYS1.SISTCMIP contains the IBM-supplied CMIP directory definition file (with the
DD name ISTCMIP), which you can edit to restrict access to CMIP services.

The LRECL and BLKSIZE for this file are both 80.

The file is loaded when CMIP services is started and can be reloaded using the
**MODIFY TABLE** command. Start CMIP services using one of these methods:
- Issue the **MODIFY VTAMOPTS** command with the **OSIMGMT=YES** operand.
- Start z/OS Communications Server with the **OSIMGMT=YES** start option.
If CMIP services is active, edit the directory definition file and then load it by
issuing the **MODIFY TABLE** command:
   MODIFY proc,TABLE,OPT=LOAD,TYPE=CMIPDDF

**SYS1.SISTASN1**

The LRECL and BLKSIZE for this file are both 1024.

**SYS1.VTAMLST**

SYS1.VTAMLST is the z/OS Communications Server definition library, which
consists of files containing the definitions for network resources and start options.
It is a required partitioned data set, and you need to allocate it on a direct-access
volume before you file z/OS Communications Server network definitions.

This data set can be allocated and cataloged at either of these times:
- Any time before its initial use. Run the IEHPROGM utility program or the
  IEBUPDTE utility program.
- When the data set is first used. Code the appropriate job control language (JCL).

To prepare the SYS1.VTAMLST data set, do these steps:

1. Allocate space to accommodate the filing of definitions for major nodes and
   anticipated sets of start options. The amount needed depends on the number
   of nodes and operands used and on the number of start options. See z/OS
   Communications Server: SNA Network Implementation Guide for more information
   about start options.

2. Specify the DD name for SYS1.VTAMLST as VTAMLST. You should specify
   these DCB subparameters:
   RECFM=FB,LRECL=80,BLKSIZE=any multiple of 80

3. Code **LABEL=RETBP=0** on all DD statements for SYS1.VTAMLST. If you do
   not, an operator awareness message requiring a reply might be generated.

4. If you generate a NEWDEFN data set as part of NCP generation processing,
   ensure that it is loaded into SYS1.VTAMLST prior to activating the NCP. Failure
   to do so can cause serious problems. z/OS Communications Server uses the
   NCP source, in addition to the NCP load module and RRT, when loading and
   activating communication controllers. SYS1.VTAMLST must contain either the
   source used as input to the NCP generation process, if a NEWDEFN data set
   was not created, or the NEWDEFN data set, if one was created. For more
   information about NEWDEFN, see NCP, SSP, and EP Generation and Loading
   Guide.
5. If you are configuring z/OS Communications Server as an APPN node (or plan to do so in the future), copy the IBM-supplied APPN class of service (COS) definitions and APPN transmission group (TG) profiles from ASAMPLIB into SYS1.VTAMLST. Three sets of IBM-supplied COS definitions are available to enable z/OS Communications Server to select an optimal route for a session:
   • COSAPPN
     The definitions in COSAPPN are appropriate for most sessions.
   • ISTACST2
     The definitions in ISTACST2 are most useful for multiple types of connections with different TG characteristics. For example, the definitions are useful when channel-to-channel, token ring network, FDDI LAN, or ATM are used in the network.
   • ISTACST3
     The definitions in ISTACST3 are designed to enable z/OS Communications Server to select an optimal route for a session when connections used in the network include those with high speed link characteristics such as FICON®, Gigabit Ethernet, and HiperSockets™.

One of these three sets of APPN COS definitions is required if z/OS Communications Server is configured as an APPN node. To use COSAPPN, ISTACST2, or ISTACST3, you must copy the appropriate set of definitions into SYS1.VTAMLST at z/OS Communications Server installation, and then activate the member in which the definitions reside. You can copy more than one set of definitions into SYS1.VTAMLST, but you can have only one set active at any time. For additional information about selecting and activating the best APPN COS definitions for your network, see the discussion about the IBM-supplied default classes of service in z/OS Communications Server: SNA Network Implementation Guide.

The IBM-supplied TG profiles are in IBMTGPS in ASAMPLIB. IBMTGPS is not required, but you should include it. You can copy IBMTGPS into SYS1.VTAMLST; it is automatically activated when z/OS Communications Server is initialized.

Guidelines:
1. Because CP-CP session paths might include subarea VRs, it is also strongly recommended that you update your logon mode tables (including the IBM-supplied logon mode table, ISTINCLM) to include an appropriate COS= value on the CPSVCMG and CPSVRMGR mode table entries. Otherwise, a blank COS name will be used to determine the subarea VR and transmission priority that will be used for the VR portion of the CP-CP session path.
2. You can modify SYS1.VTAMLST, but you need to be very careful about the relationship between z/OS Communications Server and NCP definition statements. For example, changing a VTAMLST member without changing a corresponding NCP definition statement can cause serious errors that are difficult to diagnose.

SYS1.VTAMLIB
SYS1.VTAMLIB is the z/OS Communications Server load module library, which consists of files containing the user tables, exit routines, and replaceable constants. It is a required partitioned data set.

To prepare the SYS1.VTAMLIB data set, do these steps:
1. Allocate the SYS1.VTAMLIB data set using the IEHPROGM utility program, and catalog the data set before SMP/E installation.
2. Define the data set on a direct-access volume (which can be the system residence volume), and secondary space can be allocated. Space requirements are described in the 
[/z/OS Program Directory](#) that is included with the z/OS Communications Server distribution tape.

SYS1.VTAMLIB is used to store these user tables:

- Class of service (COS) table
- Communication network management (CNM) routing table

**Note:** SYS1.LPALIB can no longer be used to store the CNM routing table.

- Interpret table containing logon descriptions and any installation-coded logon routines in this table
- Logon mode table
- Session awareness (SAW) data filter table
- Unformatted system services table

3. Code the DD name for SYS1.VTAMLIB as VTAMLIB. You should specify these subparameters on the DCB parameter, with BLKSIZE specified as full-track blocking relative to the capacity of your direct access storage device (DASD):

   ```
   RECFM=U,BLKSIZE=
   ```

4. Define SYS1.VTAMLIB as an authorized library (a library listed in the currently used IEAAPFxx).

**Parmlib member for Communication Storage Manager (CSM)**

The IVTPRM00 parmlib member sets parameters for CSM storage. IVTPRM00 is read during CSM initialization as a result of the first issuance of the IVTCSM REQUEST=CREATE_POOL macro. (z/OS Communications Server issues this macro when started.) These definitions can also be changed without requiring a re-IPL by editing the IVTPRM00 member and issuing the MODIFY CSM command without specifying the parameters on the command.

The parameter member IVTPRM00 can be found in:

- A data set defined by the PARMLIB DD statement in the TSO start procedure
- A data set in the logical parmlib concatenation
- SYS1.PARMLIB

IVTPRM00 has this format:

```
column |...+....1....+....2....+....3....+....4....+...

 FIXED MAX(maxfixK|M)
 ECSA MAX(maxecsaK|M)

[POOL(bufsize, bufsource, initbuf, minfree, expbuf)]
```

**Rules:**

1. Each line in IVTPRM00 must start in column one.
2. FIXED and MAX or ECSA and MAX keywords must be separated by one or more spaces. It must be completed with its values on the same line.

The first two lines in the CSM parmlib member define the maximum amount of storage to be dedicated to fixed and ECSA buffers in CSM. Note that the fixed maximum represents the total fixed storage above and below the 2-gigabyte bar.
You can also specify one POOL definition for each CSM buffer pool of a particular bufsize and bufsource combination. If parameters are not provided for a given CSM buffer pool, the IBM-supplied default values are used unless a program has provided these values on an IVTCSM REQUEST=CREATE_POOL macro.

This describe the variable fields in the CSM parmlib member:

**maxfix**
A decimal integer specifying the maximum bytes of fixed storage to be dedicated for use by CSM. The range is from 1024K to 30720M. The default is 100M.

**maxecsa**
A decimal integer specifying the maximum bytes of ECSA storage to be dedicated for use by CSM. The range is from 1024K to 2048M. The default is 100M.

Note: The maxecsa value should be less than 90% of the ECSA available on the z/OS system. CSM adjusts the maxecsa value to 90% of the system ECSA value and issues the message IVT5590I when the maxecsa value configured is larger than 90% of the ECSA available on the system.

K
Denotes size in kilobytes

M
Denotes size in megabytes.

**bufsize**
Specifies the size of the buffers in the pool to be created. Valid pool sizes are 4K, 16K, 32K, 60K and 180K. bufsize is required for each POOL definition.

**bufsource**
Specifies the storage source from which buffers are allocated. The values for bufsource are:

ECSA Buffers are allocated from ECSA storage.

DSpace Buffers are allocated from data space storage.

The bufsource variable is required for each POOL definition.

**expbuf**
Specifies the number of buffers by which the pool is expanded when the number of free buffers falls below the minfree value. The valid ranges for each CSM buffer pool size are as follows:

<table>
<thead>
<tr>
<th>Bufsize</th>
<th>Range for Expbuf</th>
</tr>
</thead>
<tbody>
<tr>
<td>4K</td>
<td>1–256</td>
</tr>
<tr>
<td>16K</td>
<td>1–256</td>
</tr>
<tr>
<td>32K</td>
<td>1–128</td>
</tr>
<tr>
<td>60K</td>
<td>1–68</td>
</tr>
<tr>
<td>180K</td>
<td>1–22</td>
</tr>
</tbody>
</table>

The expbuf variable is required for each POOL definition.

**initbuf**
Specifies the initial number of buffers to be created in the pool when the first IVTCM REQUEST=CREATE_POOL macro is issued by an application. If this value is specified as 0, only the base pool structure is created. In this case, the pool will be expanded on the first IVTCSM REQUEST=GET_BUFFER based on the specification for expbuf. The pool will not contract below the level specified by either initbuf or expbuf, whichever is higher.
The range for initbuf is 0–9999. If initbuf is omitted, the IBM-supplied default value is used unless overridden by an application’s CREATE_POOL request.

**minfree**

Specifies the minimum number of buffers to be free in the pool at any time. The storage pool will be expanded if the number of free buffers falls below this limit. The range for minfree is 0–9999. If minfree is omitted, the IBM-supplied default value is used unless overridden by an application’s CREATE_POOL request.

Table 7 shows the IBM-supplied default values for expbuf, initbuf, and minfree for the CSM buffer pools.

<table>
<thead>
<tr>
<th>Bufsize</th>
<th>4 KB</th>
<th>16 KB</th>
<th>32 KB</th>
<th>60 KB</th>
<th>180 KB</th>
</tr>
</thead>
<tbody>
<tr>
<td>INITBUF</td>
<td>64</td>
<td>32</td>
<td>16</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>MINFOREE</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>EXPBUF</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

z/OS system symbols can be used in IVTPRM00. See z/OS Communications Server: SNA Network Implementation Guide for more information about this function.

IBM Health Checker for z/OS can be used to check whether appropriate values are defined for the maximum amount of storage to be dedicated to fixed buffers and ECSA buffers in CSM. For more details about IBM Health Checker for z/OS, see IBM Health Checker for z/OS in z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures.

**APPN checkpointing data sets**

These data sets are used when z/OS Communications Server is defined as a network node or interchange node, and are required for the APPN checkpointing function. These data sets cannot be allowed to span multiple volumes.

- SYS1.DSDB1
- SYS1.DSDB2
- SYS1.DSDBCTRL
- SYS1.TRSDB

SYS1.DSDB1 and SYS1.DSDB2 contain APPN directory information that is used to initialize the directory database when z/OS Communications Server is restarted.

Directory database information is stored alternately between SYS1.DSDB1 and SYS1.DSDB2. The directory database information is written to one of the data sets whenever a MODIFY CHKPT TYPE=ALL or TYPE=DIR, HALT, or HALT QUICK command is issued.

Not all of the resources from the directory database are written to the data sets when there is a checkpoint. The resources that are written to the data sets are those that satisfy these requirements:

- Targeted by a search
- Have a dynamic entry type that is not registered
- Updated within a period of time specified by the DIRTIME start option
The resources that are registered to the database at startup through resource registration and definition are not included in the checkpointed information.

SYS1.DSDBCTRL contains the current status of SYS1.DSDB1 and SYS1.DSDB2. It is read by z/OS Communications Server during initialization to determine whether SYS1.DSDB1 or SYS1.DSDB2 will be used to load the APPN directory database.

SYS1.TRSDB is required for checkpointing the network topology database. The information in this data set is used to initialize the network topology database whenever z/OS V1R11 Communications Server is restarted. The network topology database is written to this file whenever a MODIFY CHKPT TYPE=TOPO or TYPE=ALL, HALT, or HALT QUICK command is issued.

The APPN checkpointing data sets should be allocated and cataloged prior to z/OS Communications Server initialization. To prepare the APPN checkpointing data sets, do these tasks:

- Specify the DD name for SYS1.DSDB1 as DSDB1, for SYS1.DSDB2 as DSDB2, for SYS1.DSDBCTRL as DSBCTRL, and SYS1.TRSDB as TRSDB.
- Specify these DCB subparameters for SYS1.DSDB1, SYS1.DSDB2, and SYS1.DSDBCTRL:
  
  ```
  RECFM=FB,LRECL=1000,BLKSIZE=any multiple of 1000,DSORG=PS
  ```

- Specify these DCB subparameters for SYS1.DSDBCTRL:
  
  ```
  RECFM=FB,LRECL=20,BLKSIZE=20,DSORG=PS
  ```

Notes:

1. It is recommended that you not modify any of the foregoing data sets.
2. The DSDBCTRL is a fixed, 20-byte file; it requires a 20-byte block.

   Regarding DSDB1 and DSDB2: Every thousand resources to be checkpointed occupies 35 logical records, or six 6KB blocks of space; the only resources to be checkpointed are the cache DLU entries found during the search.
3. z/OS Communications Server fails the initial load of the network topology database if the checkpointed data set of another node is used, or the SSCPNAME operand is changed between the two IPLs. Should the initial load fail, z/OS Communications Server can acquire the information dynamically using TDUs.

**Configuration restart data sets**

If you want to use the z/OS Communications Server configuration restart facility, define configuration restart Virtual Storage Access Method (VSAM) data sets. See z/OS Communications Server: SNA Network Implementation Guide for a description of the configuration restart support.

To set up data sets for the major nodes that you will be using with configuration restart, do these steps:

1. Use a DD statement to define a configuration restart VSAM data set for each major node. The ddname must match the ddname on the CONFIGDS operand of either the PCCU definition statement for the associated NCP or the VBUILD definition statement for the associated major node. There are no z/OS Communications Server restrictions on this data set name.

   This example defines a catalog entry to allocate space for a VSAM data set to contain the configuration restart data:
   
   ```
   DEFINE
   CLUSTER(NAME(RESTART) -
   VOL(PUBLIC) -
   ```

   ```
   ```
KEYS(18 0)
DATA(NAME(RESTART.DATA) -
RECORDS(200 20) -
RECORDSIZE(46 158)) -
INDEX(NAME(RESTARTI.INDEX) -
TRACKS(1))

2. Code the INDEX operand on the DEFINE command, or let it default. (See the sample DEFINE command.) The data set must be indexed.
3. Code KEYS (18 0). A key length of 18 bytes and an offset of 0 bytes are required.
4. Code RECORDSIZE (46 158). The average record size must be 46 bytes, and the maximum record size must be 158 bytes.
5. Make sure that the number of records in the file is equal to the number of minor nodes defined in the major node. When you choose the number of records for a switched major node, include each PATH definition statement. Therefore, the primary allocation should be the number of minor nodes in the major node, and the secondary allocation should be about 0.1 times the number of minor nodes.
6. When you change a major node definition in SYS1.VTAMLST, do not use the WARM start option when activating the new definition for the first time.

Dynamic configuration data sets for channel-attached devices

You can dynamically configure channel-attached devices in your network. See z/OS Communications Server: SNA Network Implementation Guide for a full description of this support.

To prepare your system to support dynamic configuration of channel-attached devices, complete these steps during your installation:

1. Define USER1.AUTO.VTAMLST as a partitioned data set. You can customize the name of the data set by altering its name in the ISTDEFIN command list. A sample of ISTDEFIN is found in SYS1.SAMPLIB.
2. Concatenate the USER1.AUTO.VTAMLST data set to the SYS1.VTAMLST data set as defined on the VTAMLST DD statement in the z/OS Communications Server start procedure. You also need to code the AUTO.VTAMLST data set as shared (DISP=SHR).

```
//VTAMLST DD DSN=SYS1.VTAMLST,DISP=SHR
DD DSN=USER1.AUTO.VTAMLST,DISP=SHR
...
USER1.AUTO.VTAMLST is used by ISTDEFIN for storing automatically generated major nodes. Each member of USER1.AUTO.VTAMLST representing a data host will then contain the definition for just one device. A local SNA major node will also include any of its associated LUs.
3. Set the data set control block (DCB) information for this data set with the same values as for the other VTAMLST data sets.
4. Define a catalog entry checkpoint data set (AUTOCKPT) for dynamic configuration support:

DEFINE
   CLUSTER(NAME('VSAM.AUTOCKPT') -
   VOL(PUBLIC) -
   KEYS(4 0) -
   DATA(NAME('VSAM.AUTOCKPT.DATA')-
   RECORDS(200 20) -
   RECORDSIZE(24 136)) -
   INDEX(NAME(VSAM.AUTOCKPT.INDEX) -
   TRACKS(1))
```
5. Add this data set using the AUTOCKPT DD statement in the z/OS Communications Server start procedure:

```plaintext
//AUTOCKPT DD DSN=VSAM.AUTOCKPT,AMP=AMORG,DISP=OLD
```

First Failure Support Technology
First Failure Support Technology™ (FFST™) helps you diagnose software problems by capturing information about a potential problem when it occurs.

**NODELST data set**
You can define a NODELST data set to maintain a list of major nodes that are active at one time. If you use the NODELST facility, you need to define VSAM data sets. See [z/OS Communications Server: SNA Network Implementation Guide](#) for more information on how NODELST is used.

To define a NODELST data set, perform these steps:
1. Use the DEFINE command to define a catalog entry and allocate space for an indexed cluster:

   ```plaintext
   DEFINE CLUSTER(NAME(NODLST1) -
   VOL(PUBLIC) -
   KEYS(2 0) -
   DATA(NAME(NODLST1.DATA) -
   RECORDS(120 20) -
   RECORDSIZE(10 10)) -
   INDEX(NAME(NODLST1.INDEX) -
   TRACKS(1))
   ```

2. Code the INDEX operand on the DEFINE command, or let it default. (See the preceding sample DEFINE command.) The data set must be indexed.
3. Code KEYS (2 0). A key length of 2 bytes and an offset of 0 bytes are required.
4. Code RECORDSIZE (10 10). The average record and the maximum record must each have a length of 10 bytes.
5. Make sure that the number of records in the file is equal to the number of major node and dynamic reconfiguration data set (DRDS) file activations that occur from the time z/OS Communications Server is started until it is halted. This includes major nodes that are reactivated. The primary allocation should be about 1.2 times the total number of major nodes and DRDS files in the network, and the secondary allocation should be about 0.2 times the total number.

You can use defaults for all other data characteristics.

**Data sets containing information for NCP**
This section describes some of the data sets that contain information for NCP. You might need to define these data sets for your communication controller.

**NCP load library**
The NCP load library contains the NCP and the resource resolution table (RRT) load modules.

To load NCP, create an NCP load module data set to allocate space. Cataloging the data set is optional. To activate the NCP, the NCP load library must also be available so that the RRT can be accessed.
Figure 1 shows the correlation between the DD statement for the NCP load module data set and the NCP BUILD definition statement.

**DD Statement for NCP Load Module Data Set in VTAM Start Procedure**

```
/NCPLOAD DD DSN=SYS1.NCPLOAD,DISP=.
```

**NCP Definition Statement**

```
BUILD DD name, lowest level qualifier of data set name, and value of LOADLIB operand must match (in this example, these three are NCPLOAD).
LOADLIB=NCPLOAD.
```

---

**Figure 1. Correlation between DD statement and NCP definition statement**

NCP load module data sets must be in an authorized program facility (APF) library. Since z/OS Communications Server must be loaded from an authorized library, the system verifies that all modules subsequently loaded by z/OS Communications Server be contained in authorized libraries. If the NCP load library is not APF authorized, an ABEND306 may occur when z/OS Communications Server attempts to load the NCP RRT during an NCP activation. An NCP load module data set can contain more than one NCP.

**SYS1.SSPLIB**

SYS1.SSPLIB contains the System Support Program (SSP) utilities used by NCP. SYS1.SSPLIB is a required partitioned data set and is added when NCP is installed. It must be in one of these places:

- SYS1.LINKLIB
- A concatenation of SYS1.LINKLIB (a library listed in the currently used LNKLSTxx parmlib member)
- A STEPLIB in the start procedure, to specify an authorized program facility (APF) library

**NCP dump**

The NCP dump data set receives the NCP dump output (one data set for each host z/OS Communications Server). To dump NCP, you need to allocate space for this data set. You can also catalog this data set. The name of the NCP dump data set is defined when NCP is coded.

This dump data set must accommodate a dump of the entire communication controller storage. The size of communication controller storage depends on the model number.

The DD statement defines the dump data set for the communication controller. The `ddname` must match the `ddname` on the DUMPDS operand of the PCCU definition statement for the associated NCP. z/OS Communications Server has no restrictions on the data set name.

Chapter 1. Planning to use new functions 19
z/OS Communications Server dump processing fails if the SSP modules that need to be loaded to process the dump are not accessible to z/OS Communications Server. See “SYS1.SSPLIB” on page 19 for information on SYS1.SSPLIB requirements.

For more information about the NCP dump data set, see the *NCP, SSP, and EP Diagnosis Guide*.

**Loader channel I/O trace**

The loader channel I/O trace data set (LDRIOTAB) receives communication controller channel information if a load of an NCP fails. The information collected includes channel control words, channel status words, and the first 20 bytes of any data associated with a *WRITE*, *WRITEIPL*, or *WRITEBRK* channel command.

The DD statement defines the trace data set for the SSP load utility. The *ddname* must be LDRIOTAB, but there are no restrictions on the data set name. The data requires only one track of DASD storage and should have a blocksize and logical record length of 121. The data set must be allocated before it is defined in the z/OS Communications Server start procedure.

Set the disposition of the data set as share, pass, and keep in the z/OS Communications Server start procedure.

See *NCP, SSP, and EP Trace Analysis Handbook* for more information about the loader channel I/O trace data set.

**CSP and MOSS dump (IBM 3720, 3725, and 3745 only)**

The communication scanner processor (CSP) and maintenance and operator subsystem (MOSS) dump data sets, which apply only to the IBM 3720, 3725, and 3745 Communication Controllers, are used for traces of the CSP and MOSS. To dump the CSP and MOSS microcode for problem determination, create one data set for the dump of each component. These data sets can be cataloged. The names of these data sets are defined to z/OS Communications Server in the start procedure.

The DD statement for each dump data set defines it for the NCP utility used to dump the communication controller. The *ddname* must match the *ddname* on the CDUMPDS (for a CSP dump) or MDUMPDS (for a MOSS dump) operand of the PCCU definition statement for the appropriate NCP. z/OS Communications Server has no restrictions on the data set name.
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

<table>
<thead>
<tr>
<th>Functional enhancement</th>
<th>Exploitation actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhancements introduced in z/OS V1R11 Communications Server</td>
<td></td>
</tr>
<tr>
<td>“New SMTP client for sending Internet mail” on page 26</td>
<td>Yes</td>
</tr>
<tr>
<td>“FTP access to UNIX named pipes” on page 28</td>
<td>Yes</td>
</tr>
<tr>
<td>“FTP large-volume access” on page 33</td>
<td>Yes</td>
</tr>
<tr>
<td>“FTP passive mode enhancements” on page 33</td>
<td>Yes</td>
</tr>
<tr>
<td>“Customizable pre-logon banner for otelnetd” on page 35</td>
<td>Yes</td>
</tr>
<tr>
<td>“Remote execution server enhancements” on page 35</td>
<td>Yes</td>
</tr>
<tr>
<td>“TN3270 support of TSO logon reconnect” on page 36</td>
<td>No</td>
</tr>
<tr>
<td>“IPv6 stateless address autoconfiguration enhancements” on page 36</td>
<td>Yes</td>
</tr>
<tr>
<td>“New API to obtain IPv4 network interface MTU” on page 38</td>
<td>Yes</td>
</tr>
<tr>
<td>“RFC 5095 deprecation of IPv6 type 0 route header” on page 38</td>
<td>No</td>
</tr>
<tr>
<td>“CICS sockets enhancements” on page 39</td>
<td>No</td>
</tr>
<tr>
<td>“Improved responsiveness to storage shortage conditions” on page 39</td>
<td>Yes</td>
</tr>
<tr>
<td>“Disable moving DVIPA as source IP address” on page 40</td>
<td>No</td>
</tr>
<tr>
<td>“Support for enhanced WLM routing algorithms” on page 40</td>
<td>Yes</td>
</tr>
<tr>
<td>“accept_and_receive API enhancements” on page 41</td>
<td>No</td>
</tr>
<tr>
<td>“TCP/IP support for system z10 hardware instrumentation” on page 42</td>
<td>No</td>
</tr>
<tr>
<td>“TCP/IP pathlength improvements” on page 42</td>
<td>No</td>
</tr>
<tr>
<td>“TCP throughput improvements for high-latency networks” on page 43</td>
<td>Yes</td>
</tr>
<tr>
<td>“Virtual storage constraint relief” on page 43</td>
<td>Yes</td>
</tr>
<tr>
<td>“NSS private key and certificate services for XML appliances” on page 44</td>
<td>Yes</td>
</tr>
<tr>
<td>“Enterprise Extender IPSec performance improvements” on page 44</td>
<td>No</td>
</tr>
<tr>
<td>“Resolver DNS cache” on page 45</td>
<td>Yes</td>
</tr>
<tr>
<td>“Sysplex autonomies improvements for FRCA” on page 46</td>
<td>No</td>
</tr>
<tr>
<td>“QDIO routing accelerator” on page 46</td>
<td>Yes</td>
</tr>
<tr>
<td>“Sysplex distributor connection routing accelerator” on page 48</td>
<td>Yes</td>
</tr>
<tr>
<td>“Sysplex distributor optimization for multi-tier z/OS workloads” on page 48</td>
<td>No</td>
</tr>
<tr>
<td>“Sysplex distributor support for DataPower” on page 49</td>
<td>Yes</td>
</tr>
<tr>
<td>“OSA-Express3 optimized latency mode” on page 50</td>
<td>Yes</td>
</tr>
<tr>
<td>“IPSec enhancements” on page 51</td>
<td>No</td>
</tr>
<tr>
<td>“AT-TLS enhancements” on page 52</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 8. Roadmap to functions (continued)

<table>
<thead>
<tr>
<th>Functional enhancement</th>
<th>Exploitation actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Configuration Assistant enhancements” on page 53</td>
<td>Yes</td>
</tr>
<tr>
<td>“syslogd enhancements” on page 53</td>
<td>Yes</td>
</tr>
<tr>
<td>“syslogd browser and search facilities” on page 54</td>
<td>Yes</td>
</tr>
<tr>
<td>“Policy infrastructure management enhancements” on page 55</td>
<td>Yes</td>
</tr>
<tr>
<td>“MVS console support for select TCP/IP commands” on page 57</td>
<td>Yes</td>
</tr>
<tr>
<td>“IBM Health Checker for z/OS DNS server check” on page 57</td>
<td>Yes</td>
</tr>
<tr>
<td>“Display potential model application name” on page 58</td>
<td>Yes</td>
</tr>
<tr>
<td>“Include data space VIT with INOP dump” on page 58</td>
<td>Yes</td>
</tr>
<tr>
<td>“HPR performance enhancements” on page 59</td>
<td>Yes</td>
</tr>
<tr>
<td>“APPN topology database update enhancements” on page 62</td>
<td>Yes</td>
</tr>
<tr>
<td>“Provide ACF/TAP as part of z/OS Communications Server” on page 63</td>
<td>Yes</td>
</tr>
<tr>
<td>“IBM Health Checker for z/OS RFC 4301 compliance” on page 64</td>
<td>Yes</td>
</tr>
<tr>
<td>Network management enhancements - “Stack configuration data” on page 64</td>
<td>Yes</td>
</tr>
<tr>
<td>Network management enhancements - “Detailed CSM usage” on page 65</td>
<td>Yes</td>
</tr>
<tr>
<td>Network management enhancements - “OSA network traffic analyzer data” on page 66</td>
<td>Yes</td>
</tr>
<tr>
<td>Network management enhancements - “Sysplex networking data” on page 67</td>
<td>Yes</td>
</tr>
<tr>
<td>“Verbose Ping” on page 68</td>
<td>Yes</td>
</tr>
<tr>
<td>“QDIO enhancements for Workload Manager IO priority” on page 68</td>
<td>Yes</td>
</tr>
<tr>
<td>“QDIO support for OSA interface isolation” on page 69</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Enhancements introduced in z/OS V1R10 Communications Server

<table>
<thead>
<tr>
<th>Functional enhancement</th>
<th>Exploitation actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>“TCP/IP performance improvements” on page 72</td>
<td>No</td>
</tr>
<tr>
<td>“IPSec cryptography performance improvements” on page 72</td>
<td>No</td>
</tr>
<tr>
<td>“TN3270E Telnet server ECSA reduction” on page 72</td>
<td>No</td>
</tr>
<tr>
<td>“DataPower integration with NSS SAF access service” on page 73</td>
<td>Yes</td>
</tr>
<tr>
<td>“Defensive filtering” on page 74</td>
<td>Yes</td>
</tr>
<tr>
<td>“Allow routed traffic in default filter policy” on page 75</td>
<td>Yes</td>
</tr>
<tr>
<td>“IPSec RFC currency” on page 75</td>
<td>Yes</td>
</tr>
<tr>
<td>“Enhanced port access control” on page 77</td>
<td>Yes</td>
</tr>
<tr>
<td>“Enhanced rpcbind application registration control” on page 77</td>
<td>Yes</td>
</tr>
<tr>
<td>“TCP security enhancements” on page 81</td>
<td>Yes</td>
</tr>
<tr>
<td>“TLS/SSL enablement for Load Balancing Advisor” on page 83</td>
<td>Yes</td>
</tr>
<tr>
<td>“Remove support of traffic regulation policy in Policy Agent” on page 87</td>
<td>Yes</td>
</tr>
<tr>
<td>“Security options for centralized policy server connections” on page 87</td>
<td>Yes</td>
</tr>
<tr>
<td>“Autolog support for AT-TLS dependent applications” on page 88</td>
<td>Yes</td>
</tr>
<tr>
<td>“TN3270E Telnet server LU name coordination in a sysplex” on page 89</td>
<td>Yes</td>
</tr>
<tr>
<td>“Subplex support for Load Balancing Advisor” on page 92</td>
<td>Yes</td>
</tr>
<tr>
<td>“INTERFACE statement support for QDIO” on page 94</td>
<td>Yes</td>
</tr>
<tr>
<td>“Multiple VLAN support” on page 95</td>
<td>Yes</td>
</tr>
<tr>
<td>“HiperSockets multiple write facility” on page 96</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Table 8. Roadmap to functions (continued)

<table>
<thead>
<tr>
<th>Functional enhancement</th>
<th>Exploitation actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>“OSA-Express3 multi-port support for IP” on page 98</td>
<td>Yes</td>
</tr>
<tr>
<td>“Configuration Assistant: Import of policy configuration data” on page 99</td>
<td>Yes</td>
</tr>
<tr>
<td>“Configuration Assistant: IP address groups” on page 100</td>
<td>Yes</td>
</tr>
<tr>
<td>“Network management interface enhancements” on page 101</td>
<td>Yes</td>
</tr>
<tr>
<td>“FRCA cache enhancements for WebSphere Application Server” on page 103</td>
<td>Yes</td>
</tr>
<tr>
<td>“SNMP enhancements” on page 104</td>
<td>Yes</td>
</tr>
<tr>
<td>“Socket API timeout support” on page 105</td>
<td>Yes</td>
</tr>
<tr>
<td>“Optimize asynchronous socket receive use of 64-bit shared memory” on page 107</td>
<td>Yes</td>
</tr>
<tr>
<td>“Path MTU discovery for Enterprise Extender for IP” on page 108</td>
<td>Yes</td>
</tr>
<tr>
<td>“IBM Health Checker for z/OS enhancements” on page 109</td>
<td>Yes</td>
</tr>
<tr>
<td>“Netstat enhancements” on page 110</td>
<td>Yes</td>
</tr>
<tr>
<td>“OMPROUTE enhancements” on page 111</td>
<td>Yes</td>
</tr>
<tr>
<td>“Diagnostic enhancements for TCP/IP host name configuration problems” on page 113</td>
<td>Yes</td>
</tr>
<tr>
<td>“IPCS formatter enhancements” on page 113</td>
<td>Yes</td>
</tr>
<tr>
<td>“Data trace enhancements” on page 114</td>
<td>Yes</td>
</tr>
<tr>
<td>“Packet trace enhancements” on page 115</td>
<td>Yes</td>
</tr>
<tr>
<td>“TCP/IP SMF record enhancements” on page 116</td>
<td>Yes</td>
</tr>
<tr>
<td>“Allow DNS BIND 9 server to run with BPX.SUPERUSER authorization” on page 117</td>
<td>Yes</td>
</tr>
<tr>
<td>“ASID reuse for TCP/IP, TN3270E, and resolver” on page 118</td>
<td>Yes</td>
</tr>
<tr>
<td>“Resolver support for EDNS0” on page 120</td>
<td>No</td>
</tr>
<tr>
<td>“FTP application data enhancements” on page 120</td>
<td>Yes</td>
</tr>
<tr>
<td>“FTP client API for Java” on page 121</td>
<td>Yes</td>
</tr>
<tr>
<td>“FTP JES enhancements” on page 122</td>
<td>Yes</td>
</tr>
<tr>
<td>“FTP batch pipe subsystem enhancements” on page 123</td>
<td>Yes</td>
</tr>
<tr>
<td>“FTP and MVS data set contention enhancements” on page 124</td>
<td>Yes</td>
</tr>
<tr>
<td>“FTP keepalive enhancements” on page 125</td>
<td>Yes</td>
</tr>
<tr>
<td>“Path MTU discovery for Enterprise Extender for SNA” on page 128</td>
<td>Yes</td>
</tr>
<tr>
<td>“TN3270E Telnet server ECSA reduction” on page 129</td>
<td>No</td>
</tr>
<tr>
<td>“Extended border node searching enhancement” on page 129</td>
<td>Yes</td>
</tr>
<tr>
<td>“TGN parameter for EE model PUs” on page 130</td>
<td>Yes</td>
</tr>
<tr>
<td>“Stalled HPR pipe termination” on page 131</td>
<td>Yes</td>
</tr>
<tr>
<td>“RTP pipe session limit control” on page 132</td>
<td>Yes</td>
</tr>
<tr>
<td>“Display RTP enhancements” on page 133</td>
<td>Yes</td>
</tr>
<tr>
<td>“MAXLOCAT enhancement” on page 134</td>
<td>Yes</td>
</tr>
<tr>
<td>“Start option for CSDUMP triggers” on page 135</td>
<td>Yes</td>
</tr>
<tr>
<td>“TCP/IP performance improvements for SNA” on page 135</td>
<td>Yes</td>
</tr>
<tr>
<td>“IPCS support of VTAM display commands” on page 136</td>
<td>Yes</td>
</tr>
<tr>
<td>“OSA-Express3 multi-port support for SNA” on page 137</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Chapter 3. V1R11 new function summary

This information contains topics about every function or enhancement introduced in z/OS V1R11 Communications Server. Each function is described and the following information is presented if applicable:

- Restrictions, dependencies, and coexistence considerations of the function
- A task table that identifies the actions necessary to use the function
- References to the documents that contain more detailed information

See Table 8 on page 21 for a complete list of the functional enhancements.

See z/OS Migration for information about how to migrate and maintain the functional behavior of previous releases.

See z/OS Summary of Message and Interface Changes for information about new and changed messages and interfaces.

Support considerations in V1R11

z/OS V1R11 Communications Server removes support for the following functions:

- Boot Information Negotiation Layer (BINL) server function
- Berkeley Internet Name Domain 4.9.3 (BIND 4.9.3) DNS server, including the Connection Optimization (DNS/WLM) function
- Dynamic Host Configuration Protocol (DHCP) server function
- Network Database (NDB) server function

See z/OS Migration for detailed information about all the z/OS V1R11 Communications Server support considerations.

General release considerations in V1R11

In addition to the function-specific updates, z/OS V1R11 Communications Server introduces the following changes:

- Each router using OSPF has a 32-bit router ID that uniquely identifies it within an OSPF autonomous system. If multiple routers use the same router ID, routing problems including adjacency failures and packet loss can occur. OMPROUTE issues message EZZ8165I when it detects another OSPF router that is using the same router ID as OMPROUTE.
- The trace resolver output includes additional time stamps when communicating with a Domain Name System (DNS) server. You can use this information to identify domain name servers that are responding slowly or not at all to resolver queries.
- Netstat connection reports include TCP connections in SynRcvd state.

Application integration, data consolidation, and standards

The following topics enhance application integration, data consolidation, and standards:

- "New SMTP client for sending Internet mail" on page 26
- "FTP enhancements" on page 28
New SMTP client for sending Internet mail

z/OS V1R11 Communications Server introduces a new mail-forwarding SMTP client application called Communications Server SMTP (CSSMTP). CSSMTP processes spool files on the JES spool data set that contain mail messages and forwards the mail messages to target message transfer agents (MTAs) without resolving each recipient.

If you currently use MVS batch jobs to send bulk mail by way of SMTPD, you can use CSSMTP to offload this mail. CSSMTP can improve the performance, scalability, and availability for the client function of SMTPD, but it does not act as a listening MTA server like SMTPD; CSSMTP can send mail to the Internet from z/OS, but it cannot receive mail from the Internet into z/OS.

CSSMTP can coexist with SMTPD and multiple instances of CSSMTP can run on a single host.

CSSMTP implements RFC 2821 and RFC 2822 for interacting with server MTAs, and it supports additional RFCs for message size (RFC 1870) and security (RFC 3207).

If you are currently using Communications Server SMTPD on z/OS, you should consider using CSSMTP. See the information about differences between CSSMTP and SMTPD in z/OS Communications Server: IP Configuration Guide for more information about moving from the SMTPD to the CSSMTP application.

Dependencies: If you are using Transport Layer Security (TLS) to provide private, authenticated communication over the Internet, you need to configure TLS on the CSSMTP application and the target server. See RFC 3207 SMTP Service Extension for Security SMTP over TLS for details. Ensure that the CSSMTP application and the target server are configured the same way for secure mail. See the information about enabling the SMTP server and client to use Transport Layer Security (TLS) in z/OS Communications Server: IP Configuration Guide for details.

Using the new SMTP client for sending Internet mail

If you want to use this function, perform the appropriate tasks in Table 9 on page 27.
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Configure the CSSMTP application. | Create the file manually using a text editor or copy and modify the sample provided in CSSMTPCF in SEZAINST. | • Communications Server SMTP application statement in [z/OS Communications Server: IP Configuration Reference](#)  
• Configuring the CSSMTP application in [z/OS Communications Server: IP Configuration Guide](#)  
• The CSSMTPCF configuration sample included in SEZAINST |
| Configure JES2 or JES3. | Perform the following steps:  
1. Ensure that CSSMTP interfaces with JES APIs to create, read, write, and purge data from the JES spool data set.  
2. Set JES initialization parameters correctly so that mail can be sent to CSSMTP. | [Steps for JES setup in z/OS Communications Server: IP Configuration Guide](#) |
| Optionally, set up security authorization to control who can start, stop, or issue the modify commands for the CSSMTP application. | See [z/OS Communications Server: IP Configuration Guide](#) for information on setting up this security authorization. | • If the security product being used is RACF, see [z/OS Security Server RACF Security Administrator’s Guide](#) for information regarding RACF controls for the start, stop, and modify commands.  
• Steps for granting authority to start CSSMTP in [z/OS Communications Server: IP Configuration Guide](#) |
| Optionally, control access to CSSMTP by defining the necessary SERVAUTH profiles and permitting authorized users to these profiles for an external writer name. | See [z/OS Communications Server: IP Configuration Guide](#) and the EZARACF sample in SEZAINST for information on setting RACF for CSSMTP. | • See the information about controlling which users can send mail by way of CSSMTP by restricting the user IDs in [Security for CSSMTP (optional) in z/OS Communications Server: IP Configuration Guide](#)  
• ExtWrtName statement in [z/OS Communications Server: IP Configuration Reference](#) |
| If you want to check and subsequently accept or reject mail outbound from the JES spool file, write and activate the CSSMTP user exit program. | Use the sample VERSION3 user exit CSSMTPV3 in SEZAINST. | [CSSMTP exit in z/OS Communications Server: IP Configuration Reference](#) |
Table 9. New SMTP client for sending Internet mail (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Create mail on the spool file. | Examples:  
  - Use the SMTPNOTE CLIST to prepare mail using the Time Sharing Option (TSO) EDIT command or to send mail that is created with another system editor.  
  - Issue an XMIT command, which sends a previously constructed mail file containing SMTP commands for one or more mail messages. The mail file is sent to the spool file to be processed by CSSMTP.  
  - Use the IEBGENER utility to copy a mail file to a JES syout file. | Sending electronic mail using the Communications Server SMTP application in z/OS Communications Server: IP User’s Guide and Commands |
| Customize the SMTPNOTE CLIST. | Copy and customize the SMTPNOTE CLIST on every system on which users will be able to send mail with the SMTPNOTE CLIST.  
  Tips:  
  - SMTPNOTE uses the TSO transmit (XMIT) command to interface with CSSMTP.  
  - There is a sample for SMTPNOTE in SEZAINST member SMTPNOTE. | Steps for customizing the SMTPNOTE CLIST (optional) in z/OS Communications Server: IP Configuration Guide |
| Depending on your network design, determine whether AT-TLS will be used to secure some or all of the connections for mail between CSSMTP clients and servers. | Determine which CSSMTP target servers (if used) will have TLS to provide private, authenticated communication over the Internet. See RFC 3207 SMTP Service Extension for Security SMTP over TLS for details. | See the following topics in z/OS Communications Server: IP Configuration Guide  
  - Application Transparent Transport Layer Security data protection  
  - Steps for using Transport Layer Security for CSSMTP |
| Start CSSMTP if not already started. | Create a new data set member in your procedure library for the CSSMTP JCL. | Steps for configuring and starting CSSMTP in z/OS Communications Server: IP Configuration Guide  
  - The CSSMTPCF configuration sample included in SEZAINST |

FTP enhancements

The FTP enhancements include the following topics:

- “FTP access to UNIX named pipes”
- “FTP large-volume access” on page 33
- “FTP passive mode enhancements” on page 33

FTP access to UNIX named pipes

In z/OS V1R11 Communications Server, FTP can transfer files to and from z/OS UNIX System Services named pipes.

Applications that support reading from named pipes can process data that is transferred into a named pipe while FTP is still writing data into the named pipe. Likewise, FTP can initiate the transfer of data that is written to or from a named
pipe while an application is still writing to or from the named pipe. Applications that support reading from and writing to named pipes benefit because of the following reasons:

- An I/O transfer to a named pipe is faster than an I/O transfer to a regular z/OS UNIX System Services file.
- Applications can run simultaneously with file transfers.

Restrictions:

- Anonymous users cannot create, rename, delete, read from, or write to named pipes in the FTP server z/OS UNIX System Services file system.
- You can append to but not replace the contents of a named pipe.
- The operating system provides no serialization for z/OS UNIX named pipes. Multiple processes can read from or write to a named pipe.

Using the FTP access to UNIX named pipes: If you want to use this function, perform the appropriate tasks in Table 10.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Determine whether a named pipe exists in the FTP server UNIX file system. | From the z/OS FTP client, issue one of the following subcommands to list the contents of the directory where you expect the named pipe:  
- Dir  
- LS | See the following topics in z/OS Communications Server: IP User’s Guide and Commands:  
- Dir subcommand—Obtain a list of directory entries  
- LS subcommand—Obtain a list of file names  
Also see Displaying file and directory permissions in z/OS UNIX System Services User’s Guide |
| Use an FTP client to create a named pipe on a z/OS FTP server host for later use. | Do one of the following:  
- From the z/OS FTP client, issue the MKFifo subcommand.  
- From any FTP client, issue the QUOte subcommand to send an XFIF<pathname> command to the server.  
This named pipe will not contain any data. | See the following topics in z/OS Communications Server: IP User’s Guide and Commands:  
- MKFifo subcommand  
- Using z/OS UNIX System Services named pipes |
| Control the file permissions that are assigned to named pipes created by z/OS FTP in the server file system. | Do one of the following to configure the server UMASK value:  
- Code the UMASK statement in the FTP.DATA file before starting the server.  
- From the z/OS FTP client, issue the SIte subcommand to set the server UMASK value for the current session.  
- From any FTP client, issue the QUOte subcommand to send a SITE command with the UMASK parameter to the server. | UMASK (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference  
Also see the following topics in z/OS Communications Server: IP User’s Guide and Commands:  
- SIte subcommand—Send site-specific information to a host  
- QUOte subcommand—Send an uninterpreted string of data |
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Change the file permissions that are assigned to a named pipe while you are logged into the z/OS FTP server on the target host. | Do one of the following:  
- From the z/OS FTP client, issue the SITE subcommand with the CHMOD parameter.  
- From any FTP client, issue the QUOTE subcommand to send a SITE command with the CHMOD parameter to the server. | See the following topics in z/OS Communications Server: IP User's Guide and Commands:  
- SITE subcommand—Send site-specific information to a host  
- QUOTE subcommand—Send an uninterpreted string of data |
| Transfer data into a named pipe on a z/OS FTP server host. | Perform the following steps:  
1. Configure the server for named pipe transfer.  
2. If you are using the z/OS FTP client, use the SUnique subcommand to toggle the SUnique value to off.  
3. Start a process at the FTP server host to read from the named pipe.  
4. Store or append a file to the named pipe on the server host. | See the following topics in z/OS Communications Server: IP User's Guide and Commands:  
- SUnique subcommand—Changes the storage method  
- Using z/OS UNIX System Services named pipes Also see the following topics in z/OS Communications Server: IP Configuration Reference:  
- UNIXFILETYPE (FTP client and server) statement  
- FIFOOPENTIME (FTP client and server) statement  
- FIFOIOTIME (FTP client and server) statement |
| Retrieve data from a named pipe on a z/OS FTP server host. | Perform the following steps:  
1. Configure the server for named pipe transfer.  
2. Start a process on the FTP server host to write to the named pipe.  
3. From the FTP client, issue the GET subcommand to start the file transfer. | Using z/OS UNIX System Services named pipes in z/OS Communications Server: IP User's Guide and Commands:  
- UNIXFILETYPE (FTP client and server) statement  
- FIFOOPENTIME (FTP client and server) statement  
- FIFOIOTIME (FTP client and server) statement Also see the following topics in z/OS Communications Server: IP Configuration Reference:  
- UNIXFILETYPE (FTP client and server) statement  
- FIFOOPENTIME (FTP client and server) statement  
- FIFOIOTIME (FTP client and server) statement |
Table 10. FTP access to UNIX named pipes (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Configure the server for named pipe transfer. | Configure these values at the FTP server:  
- UNIXFILETYPE FIFO  
- FIFOOPENTIME  
- FIFOIOTIME  
Do one of the following to configure these values:  
- Code the following statements in FTP.DATA before starting the server:  
  - UNIXFILETYPE FIFO  
  - FIFOIOTIME  
  - FIFOOPENTIME  
- From the z/OS FTP client, issue the SITE subcommand with the UNIXFILETYPE, FIFOIOTIME, and FIFOOPENTIME parameters.  
- From any FTP client, issue the QUOte subcommand to send SITE commands to the server with the UNIXFILETYPE, FIFOIOTIME, and FIFOOPENTIME parameters. | See the following topics in z/OS Communications Server: IP Configuration Reference:  
- UNIXFILETYPE (FTP client and server) statement  
- FIFOOPENTIME (FTP client and server) statement  
- FIFOIOTIME (FTP client and server) statement  
See the following topics in z/OS Communications Server: IP User's Guide and Commands:  
- SITE subcommand—Send site-specific information to a host  
- QUOte subcommand—Send an uninterpreted string of data  
- Using z/OS UNIX System Services named pipes |
| Display the server settings for the following configuration options:  
- UNIXFILETYPE  
- FIFOOPENTIME  
- FIFOIOTIME | Do one of the following:  
- From the z/OS FTP client, issue one of the following subcommands:  
  - STAT  
  - STAT (UNIXFILETYPE)  
  - STAT (FIFOOPENTIME)  
  - STAT (FIFOIOTIME)  
- From any FTP client, issue the QUOte subcommand to send SITE commands to the FTP server:  
  - STAT  
  - XSTA (UNIXFILETYPE) | STAtus subcommand—Retrieve status information from a remote host in z/OS Communications Server: IP User's Guide and Commands |
| Control the file permissions that are assigned to named pipes that are created by z/OS FTP on the client host. | Do one of the following to configure the server UMASK value:  
- Code the UMASK statement in the client FTP.DATA before starting the client.  
- From the z/OS FTP client, issue the LOCSite subcommand to set the client UMASK value for the current session. | UMASK (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference  
LOCSite subcommand—Specify site information to the local host in z/OS Communications Server: IP User’s Guide and Commands |
<p>| Change the file permissions that are assigned to a named pipe on the FTP client host. | Issue the LOCSite subcommand with the CHMOD parameter. | LOCSite subcommand—Specify site information to the local host in z/OS Communications Server: IP User’s Guide and Commands |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Transfer data into a named pipe on a z/OS FTP client host. | Perform the following steps:  
1. Configure the client for named pipe transfer.  
2. Start a process at the FTP client host to read from the named pipe.  
3. From the FTP client, issue the Get or MGet subcommand | Using z/OS UNIX System Services named pipes in z/OS Communications Server: IP User’s Guide and Commands  
Also see the following topics in z/OS Communications Server: IP Configuration Reference  
• UNIXFILETYPE (FTP client and server) statement  
• FIFOOPENTIME (FTP client and server) statement  
• FIFOIOTIME (FTP client and server) statement |
| Send data from a named pipe on a z/OS FTP client host. | Perform the following steps:  
1. Configure the client for named pipe transfer.  
2. Start a process on the FTP client host to write to the named pipe.  
3. From the FTP client, issue the Put, MPut, or APPEnd subcommand to start the file transfer. | Using z/OS UNIX System Services named pipes in z/OS Communications Server: IP User’s Guide and Commands  
Also see the following topics in z/OS Communications Server: IP Configuration Reference  
• UNIXFILETYPE (FTP client and server) statement  
• FIFOOPENTIME (FTP client and server) statement  
• FIFOIOTIME (FTP client and server) statement |
| Configure the client for named pipe transfer. | Configure the following values at the FTP client:  
• UNIXFILETYPE FIFO  
• FIFOOPENTIME  
• FIFOIOTIME  
Do one of the following to configure these values:  
• Code the following statements in FTP.DATA before starting the client:  
  – UNIXFILETYPE FIFO  
  – FIFOIOTIME  
  – FIFOOPENTIME  
• From the z/OS FTP client, issue the LOCStie subcommand with the UNIXFILETYPE, FIFOIOTIME, and FIFOOPENTIME parameters. | See the following topics in z/OS Communications Server: IP Configuration Reference  
• UNIXFILETYPE (FTP client and server) statement  
• FIFOOPENTIME (FTP client and server) statement  
• FIFOIOTIME (FTP client and server) statement  
Also see the following topics in z/OS Communications Server: IP User’s Guide and Commands  
• LOCStie subcommand—Specify site information to the local host  
• Using z/OS UNIX System Services named pipes |
| Display the client settings for the following configuration options:  
• UNIXFILETYPE  
• FIFOOPENTIME  
• FIFOIOTIME | From the z/OS FTP client, issue one of the following subcommands:  
• LOCStat  
• LOCStat UNIXFILETYPE  
• LOCStat FIFOOPENTIME  
• LOCStat FIFOIOTIME | LOCStat subcommand—Display local status information in z/OS Communications Server: IP User’s Guide and Commands |
FTP large-volume access
In z/OS V1R11 Communications Server, FTP reports can display space statistics for volumes. The reports are generated by using the QDISK parameter on the following subcommands and command:
- The FTP client LOCSIte and SIte subcommands with the QDISK parameter now use an enhanced format to report space statistics for volumes.
- The FTP server SITE command with the QDISK parameter now uses an enhanced format to report space statistics for volumes.

Using the FTP large-volume access: If you want to use this function, perform the appropriate tasks in Table 11.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display space statistics for one or more volumes on the z/OS FTP client host.</td>
<td>From the z/OS FTP client, issue the LOCSIte subcommand with the QDISK parameter.</td>
<td>LOCSIte subcommand—Specify site information to the local host in z/OS Communications Server: IP User’s Guide and Commands</td>
</tr>
<tr>
<td>Interpreting the output by issuing the LOCSIte subcommand with the QDISK parameter.</td>
<td>See z/OS Communications Server: IP Messages Volume 1 (EZA) for an explanation of the following messages: EZA2192I, EZA2193I, and EZA2194I in z/OS Communications Server: IP User’s Guide and Commands</td>
<td></td>
</tr>
<tr>
<td>Display space statistics for one or more volumes on the z/OS FTP server host.</td>
<td>After logging into the z/OS FTP server, do one of the following: From the z/OS FTP client, issue the SIte subcommand with the QDISK parameter. From any FTP client, issue the QUOte subcommand in one of the following ways: QUOte SITE QDISK QUOte SITE QDISK=volume serial where volume serial is the volume serial number of a volume on the FTP server host.</td>
<td>SIte subcommand—Send site-specific information to a host and QUOte subcommand—Send an uninterpreted string of data in z/OS Communications Server: IP User’s Guide and Commands</td>
</tr>
<tr>
<td>Interpreting the server reply to the SITE command when the QDISK parameter is specified.</td>
<td>See z/OS Communications Server: IP and SNA Codes for an explanation of the following codes: 200- Percent Free Largest Free 200- Volume Free Cyls Trks Cyls-Trks Ext Use Attr 200- Percent Free Free Largest Free and 200- Volume Free Cyls Trks Cyls-Trks Ext Use Attr FTP replies in z/OS Communications Server: IP and SNA Codes</td>
<td></td>
</tr>
</tbody>
</table>

FTP passive mode enhancements
In z/OS V1R11 Communications Server, the FTP client supports a new configuration option, PASSIVEIGNOREADDR. This option causes the z/OS FTP client to ignore the IP address in the PASV reply when it is establishing a data connection to the FTP server. Instead, the z/OS FTP client uses the IP address it used to log into the FTP server and the port number from the PASV reply to establish the data connection.
The option enables passive mode data connections to succeed when the server is behind Network Address Translation (NAT) processing and might not advertise its correct external IP address to the client.

Restrictions:
- These enhancements generally allow passive mode FTP data connections to be established through NAT firewalls in cases in which EPSV (extended passive mode support) would have done so. If the FTP control connection is secured with SSL/TLS and if the NAT firewalls (in addition to performing NAT) also implement dynamic filters based on the content of the PASV (or EPSV) reply, these enhancements might not be sufficient to allow the connections to be established through the NAT firewalls. In these cases, use the FTP CCC command (clear command channel).
- FTP ignores the PASSIVEIGNOREADDR option during proxy file transfer.

Dependency: The FWFRIENDLY parameter must be set to TRUE for the PASSIVEIGNOREADDR option to have an effect.

Using the FTP passive mode enhancements: If you want to use this function, perform the tasks in Table 12.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Enable the FTP client to ignore the IP address in the PASV reply from the server. | Do one of the following:  
  - Code the PASSIVEIGNOREADDR TRUE statement in the FTP client FTP.DATA file.  
  - Issue the LOCSite subcommand with the PASSIVEIGNOREADDR parameter. |  
| Configure the client to use the PASV command to establish data connections for file transfer. | Do one of the following:  
  - Code the FWFRIENDLY TRUE statement in the FTP client FTP.DATA file.  
  - Issue the LOCSite subcommand with the FWFRIENDLY parameter. |  
| Determine whether the FTP client uses or ignores the IP address in the PASV reply. | Issue the LOCSTat subcommand. You can use the PASSIVEIGNOREADDR option to limit the display to the PASSIVEIGNOREADDR configuration only. | LOCSTat subcommand—Display local status information in [z/OS Communications Server: IP User’s Guide and Commands](https://www.ibm.com/support/knowledgecenter/en/SSGUGG_11.0.0/com.ibm.zos.v1r11.cmp_iprc.doc/ )  |
| Determine whether the FTP client issues the EPSV command. | Issue the LOCSTat subcommand. You can use the EPSV4 option to limit the display to information about the EPSV4 command only. | LOCSTat subcommand—Display local status information in [z/OS Communications Server: IP User’s Guide and Commands](https://www.ibm.com/support/knowledgecenter/en/SSGUGG_11.0.0/com.ibm.zos.v1r11.cmp_iprc.doc/ )  |
Table 12. FTP passive mode enhancements (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Enable file transfer through a NAT firewall when the control connection is encrypted and the FTP server does not support the EPSV command. | Perform the following steps: 1. Use the procedure for enabling the FTP client to ignore the IP address in the server's PASV reply. 2. Use the procedure for configuring the client to use the PASV command to establish data connections for file transfer. | See the following topics in z/OS Communications Server: IP Configuration Reference  
• PASSIVEIGNOREADDR (FTP client) statement  
• FWFRIENDLY (FTP client) statement  
Also see LOCSIte subcommand—Specify site information to the local host in z/OS Communications Server, IP User's Guide and Commands |

Customizable pre-logon banner for otelnetd

In z/OS V1R11 Communications Server, the z/OS UNIX Telnet server (otelnetd) provides a new banner page that can be displayed prior to the login prompt when a user connects to the server. This new banner page is in addition to the banner page that can be displayed after a user successfully logs into the server.

Restrictions:

• The banner page must be stored in the /etc/otelnetd.banner directory.
• The existing -h parameter disables the display of the new banner page as well as the post-login banner page.

Using the customizable pre-logon banner for otelnetd

If you want to use this function, perform the task in Table 13.

Table 13. Customizable pre-logon banner for otelnetd

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the z/OS UNIX Telnet server (otelnetd) to display a banner page before the login prompt is displayed</td>
<td>Perform the following steps: 1. Create the /etc/otelnetd.banner directory. 2. Edit the /etc/otelnetd.banner file to contain your banner page message.</td>
<td>Installation information in z/OS Communications Server: IP Configuration Guide</td>
</tr>
</tbody>
</table>

Remote execution server enhancements

When the purge parameter of the MVS remote execution server is set to N (PURGE=N), the server leaves jobs on the JES spool; however, there are other conditions that can cause a job to remain on the spool. z/OS V1R11 Communications Server improves the availability of the MVS remote execution server by polling JES for the status of jobs that are flagged as residing on the spool when the internal job name table is almost full. Job names that represent jobs that have been purged become available for reuse. The polling function is not related to the setting of the PURGE parameter.

The server issues new messages to the console when the server detects that the job name table is getting full. Automation can detect this condition and restart the server if necessary.
Restriction: The remote execution server must be running on an IBM stack.

**Using the remote execution server enhancements**

If you want to use this function, perform the tasks in Table 14.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect remote execution server resource shortage problems.</td>
<td>Update your operating procedures or your automation product to monitor the new messages EZA4434I and EZA4434E.</td>
<td>Z/OS Communications Server: IP Messages Volume 1 (EZA)</td>
</tr>
<tr>
<td></td>
<td>• Message EZA4434I is issued when approximately 85% of the resources are exhausted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Message EZA4435E is issued when all the resources are exhausted.</td>
<td></td>
</tr>
<tr>
<td>Handle remote execution server resource shortage problems.</td>
<td>Perform the appropriate steps:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If message EZA4434I is displayed on the console and if the remote execution server is running with the PURGE=N option specified, do the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Verify that the server was started with the PURGE=N parameter.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Issue the MODIFY command to change the parameter to PURGE=Y.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If message EZA4434I is displayed on the console, check the JES spool and keep purging any accumulated RSH jobs that can be removed from the spool. RSH and REXEC requests will continue to be processed. You should recycle the server as soon as possible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If message EZA4435E is displayed on the console, check the JES spool and keep purging any accumulated RSH jobs that can be removed from the spool. Stop the RSH server and then start it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Result:</strong> RSH and REXEC requests will be able to be processed.</td>
<td></td>
</tr>
</tbody>
</table>

**TN3270 support of TSO logon reconnect**

z/OS V1R11 Communications Server, in conjunction with TSO/E, provides support for logon reconnect when the LOGONHERE parameter is correctly defined in SYS1.PARMLIB member IKJTSOxx. The logon reconnect will takeover the original TSO session even when the original TSO session is not disconnected. See the following for coding details:

- Z/OS MVS Initialization and Tuning Reference
- Z/OS TSO/E Customization

There are no tasks to enable this function; it is automatically enabled.

**IPv6 stateless address autoconfiguration enhancements**

In z/OS V1R11 Communications Server, a client application can use IPv6 temporary addresses that were automatically configured and that were generated from a random interface ID to address security and privacy concerns identified by RFC 4941, Privacy Extensions for Stateless Address Autoconfiguration in IPv6. The use of temporary addresses with random and changing interface IDs embedded in the address makes it more difficult for eavesdropping software to correlate...
independent transactions that use different IPv6 addresses that were automatically configured but that involve the same z/OS system.

Restriction: The use of IPv6 temporary addresses that are automatically configured is restricted to IPAQENET6 interfaces.

Incompatibility: IPv6 temporary addresses that are automatically configured are not generated for an interface that has manually configured IP addresses or prefixes.

Using the IPv6 stateless address autoconfiguration enhancements

If you want to use this function, perform the appropriate tasks in Table 15.

Table 15. IPv6 stateless address autoconfiguration enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the generation of IPv6 temporary addresses for a TCP/IP stack.</td>
<td>Specify the TEMPADDRS parameter on the IPCONFIG6 statement.</td>
<td>See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in z/OS Communications Server: IPv6 Network and Application Design Guide.</td>
</tr>
<tr>
<td>Specify the IPv6 prefixes for which IPv6 temporary addresses can be generated for a specific interface (if you need to limit the prefixes for which temporary addresses are generated).</td>
<td>Specify the TEMPPREFIX parameter on the INTERFACE statement.</td>
<td>See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in z/OS Communications Server: IPv6 Network and Application Design Guide.</td>
</tr>
<tr>
<td>Enable a client application to use IPv6 temporary addresses.</td>
<td>Specify a JOBNAME jobname TEMPADDRS entry in the SRCIP statement block.</td>
<td>See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in z/OS Communications Server: IPv6 Network and Application Design Guide.</td>
</tr>
<tr>
<td>Display stack-level IPv6 temporary address information.</td>
<td>Issue the Netstat CONFIG/-f command to display the stack-level IPv6 temporary address information.</td>
<td>See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in z/OS Communications Server: IPv6 Network and Application Design Guide.</td>
</tr>
<tr>
<td>Display the IPv6 prefixes for which IPv6 temporary addresses can be generated for an interface.</td>
<td>Issue the Netstat DEVLINKS/-d command to display the IPv6 prefixes for which temporary addresses can be generated for an interface.</td>
<td>See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in z/OS Communications Server: IPv6 Network and Application Design Guide.</td>
</tr>
</tbody>
</table>
Table 15. IPv6 stateless address autoconfiguration enhancements (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the configured SRCIP entries.</td>
<td>Issue the Netstat SRCIP/-J command to display the SRCIP entries.</td>
<td>• See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in z/OS Communications Server: IPv6 Network and Application Design Guide.</td>
</tr>
<tr>
<td>Display IPv6 temporary addresses that are generated.</td>
<td>Issue the Netstat HOME/-h command to display any temporary addresses that are generated.</td>
<td>• See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in z/OS Communications Server: IPv6 Network and Application Design Guide.</td>
</tr>
</tbody>
</table>

New API to obtain IPv4 network interface MTU

In z/OS V1R11 Communications Server, applications can determine the MTU (maximum transmission unit) for a TCP/IP stack IPv4 interface using a new programming interface ioctl. This support is similar to existing support for IPv6 interfaces.

**Restriction:** This function does not support applications that are using the Pascal application programming interface or the C application programming interface that is provided by TCP/IP.

**Using the new API to obtain IPv4 network interface MTU**

If you want to use this function, perform the task in Table 16.

Table 16. New API to obtain IPv4 network interface MTU

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine the MTU for a TCP/IP stack IPv4 interface.</td>
<td>Issue the SIOCGIFMTU ioctl.</td>
<td>• z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• z/OS Communications Server: IP CICS Sockets Guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• z/OS Communications Server: IP IMS Sockets Guide.</td>
</tr>
</tbody>
</table>

RFC 5095 deprecation of IPv6 type 0 route header

In z/OS V1R11 Communications Server, TCP/IP is modified to deprecate support for IPv6 type 0 routing headers. The reason for this deprecation is described in RFC 5095.

There are no tasks to enable this change; it is automatically enabled.

**Incompatibility:** Any application that uses the IPV6_RTHDR option to build type 0 routing headers in the IPv6 packets that it sends now receives an error when it attempts to do this.
CICS sockets enhancements
The z/OS Communication Server IP CICS socket interface and listener use the latest version of the CICS/TS macros. This version of the macros provides load module addressability relief in IP CICS socket load modules and the ability to run on all available releases of CICS/TS.

There are no tasks to enable this function; it is automatically enabled.

Availability and business resilience
z/OS V1R11 Communications Server includes enhancements to availability and business resilience in the following areas:

• “Improved responsiveness to storage shortage conditions” on page 40
• “Disable moving DVIPA as source IP address” on page 40
• “Support for enhanced WLM routing algorithms” on page 40

Improved responsiveness to storage shortage conditions
In z/OS V1R11 Communications Server, TCP/IP and OMPROUTE processing is improved to do the following:

• Provide CSM extended common service area (ECSA) storage relief in response to excessive storage on the send queue for a TCP connection
• Issue messages to syslogd when excessive or old data is accumulating on the receive or send queue for a TCP connection
• Increase the likelihood that OMPROUTE will continue to function through a temporary storage shortage, such as experiencing CSM ECSA or CSM data space conditions or reaching the TCP/IP defined limits for ECSA or private storage

In addition, z/OS Communications Server inbound processing for OSA-Express in QDIO mode and HiperSockets devices monitors the amount of ECSA storage buffered on the inbound data path. When ECSA storage usage for a particular device is excessive or when ECSA limits become constrained or critical, packets might be intentionally discarded to minimize impacts to system performance and system integrity.

Restriction: Packets will only be intentionally discarded for OSA-Express in QDIO mode and HiperSockets devices.

Incompatibility: If the CIA VTAM internal trace option is not enabled, discarded packets are not traced.

Using the improved responsiveness to storage shortage conditions
There are no tasks to provide CSM ECSA storage relief, to increase the likelihood that OMPROUTE will continue to function through a temporary storage shortage, or to use the improvements associated with discarding packets. Those functions are automatically enabled. The tasks in Table 17 are optional.

Table 17. Improved responsiveness to storage shortage conditions

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the issuing of messages to syslogd when excessive or old data is accumulating on the receive or send queue for a TCP connection.</td>
<td>Configure and start syslogd and TRMD.</td>
<td>Configuring the syslog daemon (syslogd) and TRMD in z/OS Communications Server: IP Configuration Guide</td>
</tr>
</tbody>
</table>
Table 17. Improved responsiveness to storage shortage conditions (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnose storage problems with TCP applications.</td>
<td>Complete the storage problem steps described in <a href="#">z/OS Communications Server: IP Diagnosis Guide</a></td>
<td><a href="#">Diagnosing storage abends and storage growth in z/OS Communications Server: IP Diagnosis Guide</a></td>
</tr>
</tbody>
</table>

Disable moving DVIPA as source IP address

The TCPSTACKSOURCEVIPA function is enhanced in z/OS V1R11 Communications Server to prevent the stack from using dynamic virtual IP addresses (DVIPAs) in MOVING state as source IP addresses. New TCP outbound connections that are established after the DVIPA has transitioned to the MOVING state no longer use the DVIPA as a source IP address. This enables DVIPAs in the MOVING state to return to their original state in a timely manner.

There are no tasks to enable this function; it is automatically enabled.

Support for enhanced WLM routing algorithms

z/OS V1R11 Communications Server enhances server-specific workload manager (WLM) recommendations that are used by the sysplex distributor to balance workload when DISTMETHOD SERVERWLM is configured on the VIPADISTRIBUTE statement. Two new configuration parameters enable WLM to do the following:

- Direct more workload targeted for zIIP or zAAP specialty processors to systems that have these more affordable processor cycles available, thereby reducing the overall cost of running those workloads
- Consider the different importance levels of displaceable capacity when determining server-specific recommendations

Restriction: The new configuration parameters can be used by WLM for server-specific recommendations only when all systems in the sysplex are V1R11 or later. In a mixed-release environment, the new crossover costs and importance level weighting parameters are ignored by WLM when it determines a server-specific weight.

Dependency: At a minimum, an IBM System z® Integrated Information Processor (IBM zIIP) or IBM System z Application Assist Processor (zAAP) is required for workloads that are targeted to a zIIP or zAAP

Using the support for enhanced WLM routing algorithms

If you want to use this function, perform the appropriate tasks in Table 18 on page 41.
Table 18. Support for enhanced WLM routing algorithms

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify crossover costs for running a server’s zIIP or zAAP targeted workload on a conventional processor. These costs are used by WLM when it determines a server-specific recommendation.</td>
<td>Perform the following steps: 1. Add or change the PROCXCOST parameter on a VIPADISTRIBUTE statement that has a DISTMETHOD parameter that has a value of SERVERWLM. 2. Issue a VARY TCPIP,OBEYFILE command for the modified profile.</td>
<td>VIPADYNAMIC statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Specify how aggressively WLM should favor displaceable capacity at lower importance levels over capacity at higher importance levels when it determines a server-specific recommendation.</td>
<td>Perform the following steps: 1. Add or change the ILWEIGHTING parameter on a VIPADISTRIBUTE statement that has a DISTMETHOD parameter that has a value of SERVERWLM. 2. Issue a VARY TCPIP,OBEYFILE command for the modified profile.</td>
<td>VIPADYNAMIC statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Verify the configured crossover costs for running workloads targeted to zIIP or zAAP.</td>
<td>Use the Netstat VIPADCFG/-F DETAIL command to determine the configured crossover costs that will be passed to WLM by sysplex distributor.</td>
<td>Netstat VIPADCFG/-F report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Verify the configured ILWEIGHTING value.</td>
<td>Use the Netstat VIPADCFG/-F DETAIL command to determine the configured ILWEIGHTING value that will be passed to WLM by sysplex distributor.</td>
<td>Netstat VIPADCFG/-F report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
</tbody>
</table>

Scalability, performance, constraint relief, and accelerators

z/OS V1R11 Communications Server includes enhancements to scalability, performance, constraint relief, and accelerators in the following areas:

- “accept_and_recv API enhancements”
- “TCP/IP support for system z10 hardware instrumentation” on page 42
- “TCP/IP pathlength improvements” on page 42
- “TCP throughput improvements for high-latency networks” on page 43
- “Virtual storage constraint relief” on page 43
- “NSS private key and certificate services for XML appliances” on page 44
- “Enterprise Extender IPSec performance improvements” on page 44
- “Resolver DNS cache” on page 45
- “Sysplex autonomic improvements for FRCA” on page 46
- “QDIO routing accelerator” on page 46
- “Sysplex distributor enhancements” on page 47
- “OSA-Express3 optimized latency mode” on page 50

accept_and_recv API enhancements

The accept_and_recv socket API enables z/OS applications and middleware to process short-lived client TCP connections more efficiently by combining the functions of multiple socket calls into one call. Although the accept_and_recv API has been available for several releases, z/OS V1R11 Communications Server contains significant enhancements:
• accept_and_recv socket calls can be issued asynchronously using the UNIX System Services Async I/O (BPX1AIO or BPX4AIO) callable services.
• The accept_and_recv processing is implemented natively in the Communications Server TCP/IP protocol stack. This reduces the overhead associated with communications between the UNIX System Services layer and TCP/IP.
• Incoming TCP connections that might incur delays in receiving data are processed more efficiently. The accept_and_recv processing can now logically separate these connections from connections that are functioning optimally so that they do not impact the performance of accept_and_recv API requests.

There are no tasks to enable this function; it is automatically enabled.

Restrictions:
• The accept_and_receive API does not support the msg_waitall option.
• Asynchronous accept_and_recv() calls cannot be mixed with asynchronous accept() calls.

TCP/IP support for system z10 hardware instrumentation

In z/OS V1R11 Communications Server, TCP/IP uses the z/OS MVS CSVDYLPA service to load its load modules. Using CSVDYLPA gives the z/OS MVS Contents Supervisor awareness of the location and attributes of z/OS Communication Server load modules and entry points. Vendor utility functions that intend to map z/OS Communication Server code can use the z/OS MVS services CSVQUERY or CSVINFO to obtain the location of z/OS Communications Server load modules and entry points.

There are no tasks for this function; CSVDYLPA is used unconditionally.

TCP/IP pathlength improvements

In z/OS V1R11 Communications Server, the TCP layer is updated to detect and react transparently to two common sockets programming errors:
• Traffic stalls caused by Nagle algorithms and delayed TCP acknowledgements
• Deadlock caused by insufficient TCP receive buffer size

Traffic stalls caused by Nagle algorithms and delayed TCP acknowledgements

Certain transactional workloads tend to perform back-to-back socket send() calls that contain small amounts of data, with no intervening inbound activity. If the application has not disabled the Nagle algorithm by means of the TCP_NODELAY SetSockOpt call, the second send() call will queue until the data of the first send call() is acknowledged by the other side of the TCP connection. A problem can arise because most TCP stacks try to acknowledge every other packet. When the Nagle algorithm in the side of the TCP connection that sent the packet allows only a single packet to flow, the receiver becomes dependent upon its Delay Ack Timer (typically 200 milliseconds) before an ACK to the first segment is generated. The result is that traffic slows to fewer than five round trips per second. In z/OS V1R11 Communications Server, the send-side Nagle algorithm avoids such traffic stalls caused by delayed TCP acknowledgements from the receiver side of the TCP connection.

Deadlock caused by insufficient TCP receive buffer size

The msg_waitall flag on the read() call instructs the TCP layer not to post completion of the socket read() call until all of the requested data is present. This flag makes receive processing very efficient because it minimizes the number of
socket receive API crossings. Using this flag can cause a deadlock to occur if an insufficient TCP receive buffer size has been configured. The socket read() call is never posted in such a case. This scenario occurs when an application issues a msg_waitall socket read() call with a specific number of bytes, but configures a TCP receive buffer size of fewer bytes. In this case, TCP flow control stops the data flow before the full number of bytes of data can accumulate. z/OS V1R11 Communications Server detects this deadlock situation and it transparently increases the TCP receive buffer size so that the connection can flow for the full number of bytes.

There are no tasks for TCP/IP pathlength improvements; they are automatically enabled.

**TCP throughput improvements for high-latency networks**

z/OS V1R11 Communications Server 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.

**Restriction:** This function does not take effect for applications that request a TCP receive buffer size smaller than 64 K on the the SO_RCVBUF socket option on SETSOCKOPT() call. Also, if the TCPRCVBUFSIZE value is less than 64 K, then this function does not take effect for applications that do not use the SO_RCVBUF socket option on the SETSOCKOPT() call.

**Using TCP throughput improvements for high-latency networks**

If you want to use this function, perform the appropriate tasks in Table 19.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the TCP stack to automatically tune the ideal window size for inbound streaming TCP connections over networks that have large bandwidth and high latency.</td>
<td>Specify a TCP receive buffer size value of at least 64 K on the TCPRCVBUFSIZE parameter of the TCPCONFIG statement.</td>
<td>TCPCONFIG in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Determine whether the stack is automatically tuning the ideal window size for a TCP connection.</td>
<td>Issue the Netstat ALL/-A command.</td>
<td>Netstat ALL/-A report in z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
</tbody>
</table>

**Virtual storage constraint relief**

z/OS V1R11 Communications Server moves some data areas that map socket connections from ECSA to storage that is above the 2-gigabyte threshold. This change can provide additional common storage (ECSA) constraint relief; the ECSA storage reduction is directly proportional to the number of open sockets.

**Using the virtual storage constraint relief**

There are no tasks to enable this function; it is automatically enabled. To see the storage usage, perform the task in Table 20 on page 44.
Table 20. Virtual storage constraint relief

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Display the ECSA and 64-bit common TCP/IP storage usage information.</td>
<td>Specify the DISPLAY TCPIP, proname,STOR command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DISPLAY TCPIP,STOR in z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
</tbody>
</table>
No tasks are necessary; these enhancements are automatically enabled.

**Resolver DNS cache**

In z/OS V1R11 Communications Server, the resolver can use system-wide caching of Domain Name System (DNS) responses. The system resolver cache can be used to eliminate redundant network flows to DNS servers, which can provide significant performance improvements for z/OS workloads that perform repetitive resolver queries. The resolver cache is enabled by default and is shared across the entire z/OS system image. If you are currently running a caching-only DNS name server, you might be able to use the resolver DNS cache instead; the resolver DNS cache provides the same function with better system performance.

**Using the resolver DNS cache**

You do not have to perform any steps to enable the resolver DNS caching function; it is automatically enabled. The tasks in Table 22 are optional.

**Table 22. Resolver DNS cache**

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine whether caching is in effect on a system-wide basis.</td>
<td>Issue the MODIFY RESOLVER,DISPLAY command and look for the EZZ9304I CACHE message.</td>
<td>MODIFY command -- Resolver address space in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Determine whether caching is in effect for a specific application or resolver query.</td>
<td>Perform the following steps: 1. Enable the trace resolver function. 2. Start the application. 3. Issue the resolver query. 4. Examine the trace resolver res_init( ) information to determine whether the Cache or NoCache value is specified.</td>
<td>TRACE RESOLVER in z/OS Communications Server: IP Diagnosis Guide</td>
</tr>
<tr>
<td>Disable resolver DNS caching on a system-wide or application basis.</td>
<td>To disable system-wide caching, perform the following steps: 1. Specify the NOCACHE resolver setup statement in the resolver setup file data set. 2. Issue the MODIFY RESOLVER,REFRESH,SETUP=&lt;resolver setup file name&gt; command.</td>
<td>See the following topics in z/OS Communications Server: IP Configuration Reference:  - CACHE NOCACHE statements  - NOCACHE statement (TCPIP.DATA statement)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To disable caching on an application basis, perform the following steps: 1. Specify the NOCACHE statement in the TCPIP.DATA file used by this application. 2. Issue the MODIFY RESOLVER,REFRESH command or restart the application.
Table 22. Resolver DNS cache (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-enable resolver DNS caching on a system-wide or application basis.</td>
<td>To re-enable system-wide caching, perform the following steps: &lt;br&gt;1. Specify the CACHE resolver setup statement in the resolver setup file data set, or remove the NOCACHE resolver setup statement from the resolver setup file data set. &lt;br&gt;2. Issue the MODIFY RESOLVER,REFRESH,SETUP=resolver setup file name&gt; command.</td>
<td>See the following topics in z/OS Communications Server: IP Configuration Reference: &lt;br&gt;• CACHE NOCACHE statements &lt;br&gt;• NOCACHE statement (TCPIP.DATA statement)</td>
</tr>
<tr>
<td>Increase the maximum amount of storage that can be allocated for the resolver DNS cache.</td>
<td>Perform the following steps: &lt;br&gt;1. Specify the CACHESIZE resolver setup statement in the resolver setup file data set. &lt;br&gt;2. Issue the MODIFY RESOLVER,REFRESH,SETUP=resolver setup file name&gt; command.</td>
<td>CACHESIZE statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Delete all the resolver cache data.</td>
<td>Issue the MODIFY RESOLVER,FLUSH,ALL command.</td>
<td>MODIFY command -- Resolver address space in z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
<tr>
<td>Display information about the resolver cache.</td>
<td>Use the Netstat RESCache/-q command to display resolver cache statistics and detailed cache entry information.</td>
<td>Netstat RESCache/-q report in z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
</tbody>
</table>

Sysplex autonometrics improvements for FRCA

z/OS V1R11 Communications Server improves the accuracy of the server efficiency factor (SEF) for server applications using the Fast Response Cache Accelerator (FRCA) function with persistent HTTP connections. The SEF is one of the measures of the health of a particular server on a particular target stack. The higher the value, the healthier the application is. It generally measures how well a server application is processing established connections on its backlog queue.

There are no tasks for this function; it is automatically enabled.

QDIO routing accelerator

In z/OS V1R11 Communications Server, the QDIO routing accelerator function provides accelerated forwarding at the DLC layer for the following inbound packets:

- Inbound packets that are routed over HiperSockets and that are being forwarded outbound over OSA-Express QDIO or HiperSockets
- Inbound packets that are routed over OSA-Express QDIO and that are being forwarded outbound over OSA-Express QDIO or HiperSockets

Similar to HiperSockets accelerator, QDIO routing accelerator can improve latency and decrease CPU consumption for all accelerated traffic when routing forwarded...
traffic early during inbound processing. The QDIO routing accelerator function also provides accelerated forwarding of packets that the sysplex distributor forwards to a target stack when the packets are flowing over one of the above inbound and outbound DLC combinations.

Restrictions:
- The QDIO accelerator is limited to IPv4.
- The QDIO accelerator cannot be enabled if IP security is enabled on the stack.
- If IP forwarding is disabled on the stack, then the QDIO accelerator is limited to sysplex distributor forwarding.
- When the outbound interface is HiperSockets, packets from the sysplex distributor to the target are not accelerated with the VIPAROUTE destination.

Incompatibilities: Packets that are accelerated by the QDIO accelerator are not traced by the packet trace function on the forwarding stack; however, you can use the OSA-Express network traffic analyzer (OSAENTA) function to trace the packets that are accelerated to or from OSA-Express QDIO interfaces. For more information about OSAENTA, see OSA-Express network traffic analyzer trace in z/OS Communications Server: IP Configuration Guide

Using the QDIO routing accelerator
If you want to use this function, perform the appropriate tasks in Table 23.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the QDIO accelerator function to provide accelerated forwarding of packets.</td>
<td>Specify the QDIOACCELERATOR parameter on the IPCONFIG statement in the TCP/IP profile.</td>
<td>IPCONFIG statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Display whether the QDIO accelerator is enabled.</td>
<td>Issue the Netstat CONFIG/-f command.</td>
<td>Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Display the QDIO accelerator routes.</td>
<td>Issue the Netstat ROUTe/-r command with the QDIOACCEL parameter.</td>
<td>Netstat ROUTe/-r report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Display whether a sysplex distributor connection is eligible for acceleration.</td>
<td>Issue the Netstat VCRT/-V command with the DETAIL modifier.</td>
<td>Netstat VCRT/-V report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Display information about the number of packets and bytes that are accelerated after they are received over a specific interface.</td>
<td>Initiate VTAM tuning statistics for the OSA-Express QDIO or HiperSockets interface.</td>
<td>MODIFY TNSTAT command in z/OS Communications Server: SNA Operation</td>
</tr>
<tr>
<td>See information similar to packet trace information for packets that are accelerated either from or to an OSA-Express QDIO interface.</td>
<td>Use the OSAENTA function.</td>
<td>OSA-Express network traffic analyzer trace in z/OS Communications Server: IP Configuration Guide</td>
</tr>
</tbody>
</table>

Sysplex distributor enhancements
z/OS V1R11 Communications Server enhances sysplex distributor in the following areas:
- “Sysplex distributor connection routing accelerator” on page 48
Sysplex distributor connection routing accelerator

In z/OS V1R11 Communications Server, the QDIO accelerator provides accelerated forwarding of packets that the sysplex distributor forwards to a target stack when the packets are flowing over one of the following inbound and outbound DLC combinations:

- Inbound packets that are routed over HiperSockets and that are being forwarded outbound over OSA-Express QDIO or HiperSockets
- Inbound packets that are routed over OSA-Express QDIO and that are being forwarded outbound over OSA-Express QDIO or HiperSockets

Similar to HiperSockets accelerator, QDIO routing accelerator can improve latency and decrease CPU consumption for all accelerated traffic when routing forwarded traffic early during inbound processing.

See “QDIO routing accelerator” on page 46 for more information about QDIO acceleration.

**Using the sysplex distributor connection routing accelerator**: If you want to use this function, perform the appropriate tasks in Table 24.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the QDIO accelerator function to provide accelerated forwarding of packets.</td>
<td>Specify the QDIOACCELERATOR parameter on the IPCONFIG statement in the TCP/IP profile.</td>
<td>IPCONFIG statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Display whether the QDIO accelerator is enabled.</td>
<td>Issue the Netstat CONFIG/-f command.</td>
<td>Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
<tr>
<td>Display whether a sysplex distributor connection is eligible for acceleration.</td>
<td>Issue the Netstat VCRT/-V command with the DETAIL modifier.</td>
<td>Netstat VCRT/-V report in z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
<tr>
<td>Display information about the number of packets and bytes that are accelerated after being received over a specific interface.</td>
<td>Initiate VTAM tuning statistics for the OSA-Express QDIO or HiperSockets interface.</td>
<td>MODIFY TNSTAT command in z/OS Communications Server: SNA Operation</td>
</tr>
<tr>
<td>See information similar to packet trace information for packets that are accelerated either from or to an OSA-Express QDIO interface.</td>
<td>Use the OSAENTA function.</td>
<td>OSA-Express network traffic analyzer trace in z/OS Communications Server: IP Configuration Guide</td>
</tr>
</tbody>
</table>

**Sysplex distributor optimization for multi-tier z/OS workloads**

Prior to z/OS V1R11 Communications Server, you could configure sysplex distributor with OPTLOCAL to optimize connections when both connection endpoints potentially reside on the same TCP/IP stack within the sysplex. This feature can be useful in environments where multi-tier server applications are all located within the same z/OS system images in a single sysplex. In this type of environment, OPTLOCAL is deployed on the tier 2 sysplex distributor to optimize the connections between tier 1 and tier 2 server applications.
z/OS V1R11 allows a further optimization if sysplex distributor is also being used as the load balancer for the tier 1 server applications. This optimization allows the tier 1 sysplex distributor to have visibility into both tiers of the z/OS server applications on a given system when making a load balancing decision on an incoming tier 1 connection request. When using WLM based recommendations, this optimization allows sysplex distributor to compute a composite WLM weight for each system that includes the capacity, performance, and health characteristics of both the tier 1 server applications and the tier 2 server applications.

For a step-by-step description of how to use this function, see the information about sysplex distribution optimization for multi-tier z/OS workloads in z/OS Communications Server: IP Configuration Guide.

Restriction: All TCP/IP stacks that participate in the sysplex distribution as distributing, backup, or target stacks must be at V1R11 or later.

Sysplex distributor support for DataPower

The sysplex distributor feature of Communications Server provides workload balancing capabilities for TCP applications in a z/OS sysplex environment. These capabilities can significantly enhance the availability, performance, and scalability characteristics of z/OS TCP/IP-based applications. In z/OS V1R11, Communications Server, sysplex distributor is enhanced to provide similar workload balancing capabilities for IBM WebSphere® DataPower® appliances.

DataPower appliances are often deployed as a front-end processing tier to z/OS applications, which provides for transparent web services enablement of z/OS applications or accelerated and more efficient handling of web services security protocols, XML schema validation, and additional functions. In many of these environments, multiple DataPower instances are deployed in a cluster to provide higher availability and scalability, requiring an external, network-based load balancer to load balance incoming requests across the DataPower appliance instances.

When the DataPower tier finishes handling a request, it typically routes a request to a tier 2 application that is hosted within the z/OS environment, such as a CICS TM, IMS TM, or WebSphere application. These tier 2 requests might also require load balancing, especially when the applications are deployed in a sysplex environment. Prior to z/OS V1R11 Communications Server, sysplex distributor could be used to load balance the tier 2 requests into the z/OS sysplex. With this V1R11 enhancement, you can use sysplex distributor to load balance requests to both the DataPower and z/OS tiers, eliminating the need for deploying an external, network-based load balancer for the DataPower tier.

This enhancement also includes new support in the IBM WebSphere DataPower appliance, which enables sysplex distributor to optimize the load balancing support in several ways:

- Routing is optimized so that outbound traffic (from the tier 1 DataPower target server towards the client) does not need to traverse the sysplex distributor.
- Connection information provided by the DataPower appliances allows nondisruptive tier 1 takeover of existing connections between clients and DataPower targets.
- CPU usage information provided by the DataPower appliance allows sysplex distributor to optimize its load balancing decisions.
For more information and for step-by-step lists of tasks describing how to use sysplex distribution with DataPower, see the information about sysplex distribution with DataPower in z/OS Communications Server: IP Configuration Guide.

Restriction: All TCP/IP stacks that participate in the sysplex distributor support with DataPower must be V1R11 or later.

Coexistence requirements: An IBM WebSphere DataPower appliance with support for these optimizations is required in this environment.

**OSA-Express3 optimized latency mode**

z/OS V1R11 Communications Server improves performance for workloads that have demanding latency requirements because it provides a way for an OSA-Express3 device to run in optimized latency mode. Optimized latency mode optimizes interrupt processing for both inbound and outbound data. When an OSA-Express3 device is operating in optimized latency mode, latency is decreased and throughput is increased, particularly for interactive, non-streaming workloads.

Restriction: The number of concurrent network interfaces sharing an OSA-Express3 device is limited to four when one or more of the network interfaces is operating in optimized latency mode.

Incompatibilities:
- Traffic directed to OSA-Express3 write priority queue 4 will not benefit from optimized latency mode for outbound interrupt optimization.
- Traffic that is either inbound over or being forwarded to an OSA-Express3 device configured in optimized latency mode is not eligible for the accelerated routing function provided by HiperSockets Accelerator and QDIO Accelerator.
- Optimized latency mode can be configured only for an OSA-Express3 device that is configured with an INTERFACE statement, not with DEVICE and LINK statements.
- The optimized latency mode function targets a specific z/OS environment that has high-volume interactive workloads. Although optimized latency mode can compensate for some mixing of workloads, an excessive amount of high volume, streaming workloads, such as bulk data or file transfer, can result in higher CPU consumption.

Dependencies: This function is limited to OSA-Express3 ethernet features in QDIO mode (CHPID type OSD) running on an IBM System z10. See the 2097DEVICE and the 2098DEVICE Preventive Service Planning (PSP) buckets for further information.

**Using the OSA-Express3 optimized latency mode**

If you want to use this function, perform the tasks in Table 25.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable an OSA-Express3 device for optimized latency mode.</td>
<td>Specify the OLM parameter on the INTERFACE statement in the TCP/IP profile.</td>
<td>INTERFACE — IPAQENET OSP-Express QDIO interfaces and INTERFACE — IPAQENET6 OSA-Express QDIO interfaces in z/OS Communications Server: IP Configuration Reference</td>
</tr>
</tbody>
</table>
Table 25. OSA-Express3 optimized latency mode (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct traffic to OSA-Express3 write priority queues 1, 2, or 3.</td>
<td>Specify the WLMPRIORITYQ parameter on the GLOBALCONFIG statement in the TCP/IP profile.</td>
<td>GLOBALCONFIG in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Display OSA-Express3 performance options.</td>
<td>Issue the Netstat DEvlinks/-d command.</td>
<td>Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
<tr>
<td>Determine the effectiveness of optimizing interrupts by using optimized latency mode.</td>
<td>Issue the MODIFY TNSTAT command to display the tuning statistics for an OSA-Express3 device.</td>
<td>MODIFY TNSTAT command in z/OS Communications Server: SNA Operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Message IST1230I in z/OS Communications Server: SNA Messages</td>
</tr>
</tbody>
</table>

Security

z/OS V1R11 Communications Server includes enhancements to security in the following areas:

- "IPSec enhancements"
- "AT-TLS enhancements" on page 52

IPSec enhancements

The Internet Key Exchange (IKE) daemon’s retransmission scheme better conforms to RFC 2408. Rather than using fixed intervals for IKE message retransmission, the daemon uses a geometrically increasing retransmission interval. Some fine-grained attributes are reported in the ipsec command reports as well as in the Network Management Interface (NMI) and System Management Facility (SMF) records.

Restriction: The existing DataRetries, DataWait, KeyRetries, and KeyWait parameters in the IKED configuration file are no longer honored. Instead, the new IkeRetries and IkeInitWait parameters control message retransmission for all IKE messages.

Using the IPSec enhancements

No explicit tasks are required to use the z/OS V1R11 Communications Server IPSec enhancements. If you use the Configuration Assistant to generate the IKED configuration file, you need to obtain the V1R11 Configuration Assistant. The files generated with the V1R11 version of the tool use the new defaults. You can optionally change these settings in the Advanced IKE Daemon Settings dialog box under the IKE Daemon Settings tab under the IPSec perspective for the z/OS image.

If you manually edit your IKED configuration file, the new IkeRetries and IkeInitWait parameters both have default values, and because of the nature of the geometrically increasing intervals, the same default value should be sufficient for all IKE partners. However, if you have a specific need to control the initial retransmission interval or number of retries, code the corresponding IkeInitWait and IkeRetries parameters in the IKED configuration file and then apply the new configuration by issuing a MODIFY IKED,REFRESH command.
Optionally, you can also remove any DataRetries, DataWait, KeyRetries, and KeyWait parameters from the IKED configuration file because they are no longer honored.

AT-TLS enhancements

In z/OS V1R11 Communications Server, AT-TLS supports the System SSL functions that have been added since z/OS V1R7. This includes support for the following:

- The TLSv1.1 protocol
- RFC 3280 for certificate validation
- FIPS 140-2
- PKCS #11 Token names for Keyring
- Negotiation and use of a truncated Hash Message Authentication Code (HMAC)
- Negotiation and use of a maximum SSL fragment size
- Negotiation and use of handshake server name indication
- Setting the CRL LDAP server access security level

IBM Configuration Assistant for z/OS is enhanced to define use of these new AT-TLS functions.

Restrictions:

- Applications using the Pascal application programming interface are not supported by AT-TLS. The new functions are not supported for Pascal applications.
- To enable FIPS 140-2 support, Security Level 3 FMID (JCPT3B1) must be installed.

Using the AT-TLS enhancements

If you want to use this function, perform the task in Table 26.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Define the new AT-TLS statements in the Policy Agent configuration files. | Specify the new AT-TLS statements in the configuration files that are identified with the CommonTTLSConfig and TTLSSConfig statements by using one of the following methods:  
  - Use the z/OS Network Security Configuration Assistant.  
  - Code the required statements directly into an HFS file or MVS data set. | IBM Configuration Assistant for z/OS Communications Server online helps |

If FIPS 140-2 is enabled, configure System SSL for FIPS 140-2 support. | Complete the steps described in z/OS Cryptographic Services System SSL Programming to set up System SSL to run in FIPS-mode. | z/OS Cryptographic Services System SSL Programming |
Simplification and consumability

z/OS V1R11 Communications Server includes enhancements to simplification and consumability in the following areas:

- “Configuration Assistant enhancements”
- “syslogd enhancements”
- “syslogd browser and search facilities” on page 54
- “Policy infrastructure management enhancements” on page 55
- “MVS console support for select TCP/IP commands” on page 57
- “IBM Health Checker for z/OS DNS server check” on page 57

Configuration Assistant enhancements

The IBM Configuration Assistant for z/OS Communications Server V1R11 (Configuration Assistant) simplifies the installation and setup of policies. In addition to installing policy files, the Configuration Assistant guides the administrator through all of the tasks that are necessary to get the Communications Server function (such as IPSec) active and running on the z/OS system. These tasks include everything from setting up RACF security to starting Policy Agent and other daemons that might be used by the function.

The following list identifies the new Configuration Assistant functions:

- Configure the Policy Agent configuration file
- Configure the Defense Manager Daemon (DMD)
- Configure the base location
- Customize EBCDIC codepage support
- Set up Policy Agent tasks
- Install an all files option
- Notify the administrator when configuration data is changed

Using the Configuration Assistant enhancements

If you want to use the Configuration Assistant enhancements, perform the task in Table 27.

Table 27. Configuration Assistant enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the Configuration Assistant.</td>
<td>Install the IBM Configuration Assistant for z/OS V1R11 and refer to the help topics.</td>
<td>You can download the GUI from the z/OS Communications Server product support Web page. Invoke the Configuration Assistant Help System.</td>
</tr>
</tbody>
</table>

syslogd enhancements

In z/OS V1R11 Communications Server, the internal structure of syslog daemon (syslogd) provides more efficient processing of log messages. The syslogd job name matches the name of the cataloged procedure, and a set of operator commands starts, stops, and controls the daemon. The syslog daemon also performs automatic archival of z/OS UNIX files, based on configurable options.
Using the syslogd enhancements

If you want to use the syslogd enhancements, perform the tasks in Table 28.

Table 28. syslogd enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Use operator commands to control the syslog daemon. | Perform the following steps:  
1. Issue the STOP command to stop the syslog daemon. The effect is the same as sending a SIGTERM signal.  
2. Issue the MODIFY procname,RESTART command to restart the syslog daemon. The effect is the same as sending a SIGHUP signal. | STOP command and MODIFY command: Syslog Daemon in z/OS Communications Server: IP System Administrator's Commands |
| Configure the syslog daemon to perform automatic archival of eligible z/OS UNIX files at a specific local time of day or based on a file-system threshold. | Specify the following configuration statements or parameters in the syslogd configuration file:  
- ArchiveTimeOfDay statement to specify a specific local time of day for archiving  
- ArchiveThreshold and ArchiveCheckInterval statements to specify the threshold archiving for the z/OS UNIX file system  
- BeginArchiveParms statements to specify archive details for eligible z/OS UNIX files  
- -N or -X parameter on syslogd rules that have a z/OS UNIX file destination. The -N and -X parameters specify archive details for the file or that the file should be reinitialized. | Configuring the syslog daemon (syslogd) in z/OS Communications Server: IP Configuration Guide  
- Syslog daemon in z/OS Communications Server: IP Configuration Reference |
| Display z/OS UNIX file system usage data for configured syslogd z/OS UNIX files. | Issue the MODIFY procname,DISPLAY,ARCHIVE command. | MODIFY command: Syslog daemon in z/OS Communications Server: IP System Administrator's Commands |
| Perform an on-demand archive of all eligible syslogd z/OS UNIX files. | Issue the MODIFY procname,ARCHIVE command. | MODIFY command: Syslog daemon in z/OS Communications Server: IP System Administrator's Commands |

syslogd browser and search facilities

In z/OS V1R11 Communications Server, an ISPF-based syslog daemon browser application is available. The browser supports browsing and searching active syslogd files (the files to which syslogd currently writes) and syslogd archive data sets that were created using the new syslogd archival function.

Using the syslogd browser and search facilities

If you want to use the syslogd browser and search facilities, see Table 29 on page 55.
Policy infrastructure management enhancements

In z/OS V1R11 Communications Server, the Policy Agent provides monitoring and automatic start and restart for the following set of related applications:

- Defense manager daemon (DMD)
- Internet key exchange daemon (IKED)
- Network security services daemon (NSSD)
- syslog daemon (syslogd)
- Traffic regulation management daemon (TRMD)

This function is similar to the AUTOLOG function in the TCP/IP stack, but it does not require the application to maintain a listening socket. This function provides simpler management and operations for a set of applications that are associated with the policy infrastructure.

A variety of EBCDIC code pages are supported for the configuration files and policy definition files for the following applications:

- Policy Agent
- syslogd
- IKED
- NSSD
- DMD

You can specify as a start option the TCP/IP stack name that the TRMD uses. You can still use the resolver configuration file to specify the stack name.

Using the policy infrastructure management enhancements

If you want to use the policy infrastructure management enhancements, perform the tasks in Table 30.

Table 30. Policy infrastructure management enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine the set of applications to be monitored by the Policy Agent.</td>
<td>Examine your z/OS Communications Server environment to determine which of the following daemons are currently used and which daemons you want Policy Agent to monitor:</td>
<td>Configuring Policy Agent to automatically monitor applications in z/OS Communications Server: IP Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>• DMD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IKED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NSSD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• syslogd</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TRMD</td>
<td></td>
</tr>
</tbody>
</table>
Table 30. Policy infrastructure management enhancements (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Configure the Policy Agent to monitor the target set of applications. | Specify the following configuration statements in the Policy Agent main configuration file:  
- AutoMonitorApps statement to specify the applications to be monitored, as well as application-specific parameters  
- AutoMonitorParms statement to specify global monitoring parameters |  
- Configuring Policy Agent to automatically monitor applications in z/OS Communications Server: IP Configuration Guide  
- AutoMonitorApps statement and AutoMonitorParms statement in z/OS Communications Server: IP Configuration Reference  
- Configuring Policy Agent to automatically monitor applications in z/OS Communications Server: IP Configuration Guide  
- MODIFY command: Policy Agent in z/OS Communications Server: IP System Administrator's Commands |
| Optionally, manage the target set of applications using Policy Agent MODIFY commands. | Do one or more of the following:  
- Issue the MODIFY proclname,MON,START,application command to start a monitored application that failed to start automatically.  
- Issue the MODIFY proclname,MON,STOP,application command to stop a monitored application and to also stop monitoring the application.  
- Issue the MODIFY proclname,MON,RESTART,application command to stop and restart a monitored application.  
- Issue the MODIFY proclname,MON,DISPLAY command to display the status of monitored applications. |  
- Configuring Policy Agent to automatically monitor applications in z/OS Communications Server: IP Configuration Guide  
- MODIFY command: Policy Agent in z/OS Communications Server: IP System Administrator's Commands |
| Specify the EBCDIC code page to be used for reading the Policy Agent configuration files and policy definition files. | Configure the CODEPAGE configuration statement in the main Policy Agent configuration file. | CODEPAGE statement in z/OS Communications Server: IP Configuration Reference |
| Specify the EBCDIC code page to be used for reading the configuration files for policy-related applications. | Specify the appropriate code page environment variable for the following applications:  
- syslogd: SYSLOGD_CODEPAGE  
- IKED: IKED_CODEPAGE  
- NSSD: NSSD_CODEPAGE  
- DMD: DMD_CODEPAGE | See the following topics in z/OS Communications Server: IP Configuration Reference  
- Syslog daemon  
- IKE Daemon  
- Network security services server  
- Defense Manager daemon |
| Specify the TCP/IP stack name to be used with TRMD. | Use the -p start option in your TRMD cataloged procedure, or on the z/OS UNIX shell command, when starting TRMD. The -p start option overrides the resolver configuration file. |  
- TRMD in z/OS Communications Server: IP Configuration Guide  
- Starting the traffic regulation manager daemon (TRMD) from the z/OS shell in z/OS Communications Server: IP Configuration Reference |
MVS console support for select TCP/IP commands

z/OS V1R11 Communications Server adds support for using selected z/OS UNIX shell commands from the MVS console, the TSO environment, and from IBM Tivoli® NetView for z/OS. The z/OS UNIX shell commands are supported by a new EZACMD command. The following z/OS UNIX shell commands are supported from the MVS console, TSO, and NetView: `trmdstat`, `ipsec`, `nssctl`, and `pasearch`. In addition, the z/OS UNIX `ping` command is supported from the MVS console and NetView.

**Restriction:** Only the following z/OS UNIX shell commands are supported by the EZACMD command: `trmdstat`, `ipsec`, `nssctl`, `pasearch`, and `ping`.

**Dependency:** Use of the EZACMD command from the MVS console depends on the System REXX component being configured and enabled.

**Using the MVS console support for select TCP/IP commands**

If you want to use the MVS console support for select TCP/IP commands, perform the tasks in Table 31.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Enable the use of EZACMD from the MVS console. | Configure and enable the System REXX component on z/OS. | - System REXX in [z/OS MVS Programming: Authorized Assembler Services Guide](https://www.ibm.com)  
- AXR00 (default System REXX data set concatenation) in [z/OS MVS Initialization and Tuning Reference](https://www.ibm.com) |
| Invoke select z/OS Communications Server UNIX commands from the MVS console, TSO, or NetView environments. | Use the new EZACMD command, specifying the z/OS UNIX command as input. | [EZACMD command in z/OS Communications Server: IP System Administrator’s Commands](https://www.ibm.com) |

IBM Health Checker for z/OS DNS server check

z/OS V1R11 Communications Server provides a new z/OS Health Checker for z/OS migration health check to help determine if you are using the BIND9 DNS server on your system. IBM has previously indicated in statements of direction that support of DNS server functions on z/OS will be removed in a future z/OS release.

**Dependency:** You must start the IBM Health Checker for z/OS before you can use the IBM Health Checker for z/OS enhancements.

**Using the IBM Health Checker for z/OS DNS server check**

If you want to use this function, perform the task in Table 32 on page 58.
Table 32. IBM Health Checker for z/OS DNS server check

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Use the IBM Health Checker for z/OS migration check support. | Perform the following steps:  
1. Configure and start the IBM Health Checker for z/OS.  
2. Review check output for potential migration actions. | See the following topics in IBM Health Checker for z/OS: User's Guide:  
- Setting up IBM Health Checker for z/OS  
- Working with check output  
- Managing checks |

SNA and Enterprise Extender

z/OS V1R11 Communications Server includes enhancements to SNA and Enterprise Extender (EE) in the following areas:

- Display potential model application name
- Include data space VIT with INOP dump
- HPR performance enhancements on page 59
- APPN topology database update enhancements on page 62
- Provide ACF/TAP as part of z/OS Communications Server on page 63

Display potential model application name

In z/OS V1R11 Communications Server, the DISPLAY MODELS command can identify which application model definition will be used to build a dynamic application definition. You can use the DISPLAY MODELS command to prevent dynamic application definitions from being built incorrectly.

Displaying the potential model application name

If you want to use this function, perform the task in Table 33.

Table 33. Display potential model application name

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Discover the model application definition that will be used for building the dynamic definition for an application (APPL1). | Perform the following steps:  
1. Issue the DISPLAY NET,MODELS,APPL=APPL1 command.  
2. Examine the output (message IST2302I is included if a model was found and message IST2303I is included if no model was found).  
3. If IST2304I is also displayed, determine if the existence of another resource using the same name will present a problem. | DISPLAY MODELS in z/OS Communications Server: SNA Operation  
- Shadow resources in z/OS Communications Server: SNA Network Implementation Guide |

Include data space VIT with INOP dump

In z/OS V1R11 Communications Server, the VTAM INOP dump processing automatically captures the VTAM internal trace (VIT) data space (ISTITDS1) in the dump when the VIT data space is in use.

VTAM INOP dump processing automatically specifies the inclusion of the data space VIT (ISTITDS1) in all INOP dumps. To make the inclusion of the data space...
effective in all cases, you might need to increase the size of your system dump data sets to accommodate the possible increase in size of INOP dumps. To use the function, you must use the additional information included in a complete INOP dump. These tasks are described in Table 34.

Table 34. Include data space VIT with INOP dump

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Ensure that your system dump data sets are large enough to accommodate the potential increase of 10 to 50 megabytes in the size of INOP dumps. | Perform the following steps:  
1. Examine your system dump data set allocation procedure.  
2. Increase the size of the data sets by up to 50 megabytes as needed to relieve constraint. | [A - allocate new data set in z/OS ISPF User’s Guide Vol IV] |
| Ensure that the data space VIT is active on the system so that additional VIT data will be captured by an INOP dump. | Do one of the following:  
• Activate the data space VIT when VTAM starts by coding the DSPSIZE operand with a value of 1 through 5 (5 is suggested) on any TRACE,TYPE=VTAM,MODE=INT start option that is included in the VTAM start list or on the VTAM START command.  
• Activate the VIT data space after VTAM starts by issuing the MODIFY vtamproc,TRACE,TYPE=VTAM command. | [TRACE for MODULE, STATE (with OPTION), or VTAM internal trace in z/OS Communications Server: SNA Resource Definition Reference] [MODIFY TRACE command in z/OS Communications Server: SNA Operation] |
| Set up VTAM to take an INOP dump when a link inoperative situation occurs. | Do one of the following:  
• Activate INOPDUMP when VTAM starts by coding INOPDUMP=ON in the VTAM start list or on the VTAM START command.  
• Activate INOPDUMP after VTAM starts by issuing the MODIFY vtamproc,INOPDUMP=ON command. Optionally, specify a TRLE name. | [INOPDUMP start option in z/OS Communications Server: SNA Resource Definition Reference] [MODIFY INOPDUMP command in z/OS Communications Server: SNA Operation] |
| Diagnose problems using the VIT data in the INOP dump. | Use the VIT entries in ISTITDS1 that provide a longer history of traced events than the VIT in ECSA. | [z/OS Communications Server: SNA Diagnosis Vol 1. Techniques and Procedures] [z/OS Communications Server: SNA Diagnosis Vol 2. FFST Dumps and the VIT] |

HPR performance enhancements

z/OS V1R11 Communications Server improves high performance routing (HPR) performance in the following ways:
• A new progressive-mode adaptive rate-based (ARB) flow control algorithm increases performance in virtualized or CPU-constrained environments.
• Unproductive path switches are reduced or eliminated when an HPR endpoint is unresponsive.
• ECSA and CSM storage utilization of HPR control blocks is reduced.
• Storage and CPU usage are reduced when packet loss occurs.
**Restriction:** Progressive-mode ARB applies only to one-hop HPR pipes that traverse Enterprise Extender (EE) connections (which includes a single physical hop across a two-hop EE virtual routing node [VRN]).

**Coexistence considerations for HPR performance enhancements**
If you are enabling the new ARB level as the HPR flow control algorithm on z/OS V1R11 Communications Server, you must apply the PTFs for APAR OA26490 on prior releases of z/OS Communications Server. The PTFs for APAR OA26490 are required to prevent a prior release from regressing its HPR pipes to base-mode ARB.

Table 35 indicates the PTFs for APAR OA26490 that are required to make the supported releases compatible with V1R11.

<table>
<thead>
<tr>
<th>z/OS Communications Server version</th>
<th>PTF for APAR OA26490</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1R8</td>
<td>UA44024</td>
</tr>
<tr>
<td>V1R9</td>
<td>UA44025</td>
</tr>
<tr>
<td>V1R10</td>
<td>UA44023</td>
</tr>
</tbody>
</table>

For VTAM to successfully negotiate the use of progressive-mode ARB to distributed Communications Servers or to other HPR products, those products must implement the logic needed to support progressive-mode ARB. If the destination HPR platform does not support progressive-mode ARB, the ARB mode is negotiated to either base-mode ARB or responsive-mode ARB.

The progressive-mode ARB enhancement is in the Version 6.4 release of the following products:
- Communications Server for Windows®
- Communications Server for AIX®
- Communications Server for Linux for System z (s390x)
- Communications Server for Linux (i686, x84_64, ppc64)

**Using the HPR performance enhancements**
If you want to use this function, perform the tasks in Table 36.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay the start of HPR path switching logic for 5 seconds for all HPR connections.</td>
<td>Specify HPRPSDLY=5 in the appropriate ATCSTRxx VTAM start list or on the VTAM START command. Optionnally, when VTAM is active, issue the MODIFY procname,VTAMOPTS, HPRPSDLY=5 command.</td>
<td>• HPRPSDLY start option in z/OS Communications Server: SNA Resource Definition Reference • START command and MODIFY VTAMOPTS command in z/OS Communications Server: SNA Operation</td>
</tr>
<tr>
<td>Task</td>
<td>Procedure</td>
<td>Reference</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| Delay the start of HPR path switching logic for 15 seconds for some Enterprise Extender connections. | Specify HPRPSDLY=15 on the following definition statements:  
- For Enterprise Extender connection networks, define this parameter on the connection network GROUP definition statements in the EE XCA major node.  
- For dial-in Enterprise Extender connections that have associated PUs that are dynamically created, define this parameter on the model major node (DYNTYPE=EE) PU definition statement.  
- For predefined Enterprise Extender connections, define this parameter on the PU definition statement in the switched major node. | See the following topics in z/OS Communications Server: SNA Resource Definition Reference:  
- HPRPSDLY XCA major node  
- HPRPSDLY model major node  
- HPRPSDLY switched major node |
| Delay the start of HPR path switching logic long enough to allow the Enterprise Extender Keep-Alive mechanism to make the EE connection inoperable if connectivity to the partner is lost. | Specify HPRPSDLY=EEDELAY on the following definition statements:  
- For Enterprise Extender connection networks, define this parameter on the connection network GROUP definition statements in the EE XCA major node.  
- For dial-in Enterprise Extender connections that have their associated PUs dynamically created, define this parameter on the model major node (DYNTYPE=EE) PU definition statement.  
- For predefined Enterprise Extender connections, define this parameter on the PU definition statement in the switched major node. | See the following topics in z/OS Communications Server: SNA Resource Definition Reference:  
- HPRPSDLY XCA major node  
- HPRPSDLY model major node  
- HPRPSDLY switched major node |
| Display the HPR path switch delay value associated with a specific HPR pipe. | Perform the following steps:  
1. Issue the DISPLAY ID=rtp_pu,HPRDIA=YES command.  
2. Locate the path switch information in the HPRDIAG output. The value is displayed in message IST2271L. | DISPLAY ID command in z/OS Communications Server: SNA Operation |
Table 36. HPR performance enhancements (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Designate that progressive-mode ARB is to be used for an EE connection. | Specify the new HPREEARB keyword on the following definition statements:  
- For Enterprise Extender connection networks, define this parameter on the connection network GROUP definition statements in the EE XCA major node.  
- For dial-in Enterprise Extender connections that have their associated PUs dynamically created, define this parameter on the model major node (DYNTYPE=EE) PU definition statement.  
- For predefined Enterprise Extender connections, define this parameter on the PU definition statement in the switched major node. | See the following topics in z/OS Communications Server: SNA Resource Definition Reference:  
- HPREEARB XCA major node  
- HPREEARB model major node  
- HPREEARB switched major node |
| Determine which ARB mode is being used for a specific HPR pipe. | Perform the following steps:  
1. Issue the DISPLAY ID=rtp_pu,HPRDIAG=YES command.  
2. Locate the ARB information in the HPRDIAG output.  
   - If message IST1697I is present, then the responsive-mode ARB algorithm is being used.  
   - If message IST2267I is present, then progressive-mode ARB algorithm is being used.  
   - If neither message IST1697I nor IST2267I is present, then the base-mode ARB algorithm is being used. | DISPLAY ID command in z/OS Communications Server: SNA Operation |

APPN topology database update enhancements

z/OS V1R11 Communications Server enhances APPN topology database update (TDU) processing in the following ways:

- Topology updates sent to partner network nodes in TDUs will now include unknown topology control vectors based on each partner node’s ability to receive them. Any topology control vectors added since the original APPN architecture are considered to be unknown vectors. Unknown topology vectors are not sent to a partner network node that does not have this support. Previously, unknown topology control vectors were not included in TDUs sent to any partner network node if at least one partner network node did not support the receipt of unknown vectors.
- Serviceability enhancements aid in the identification of the network nodes involved in a TDU war, which is the endless exchange of TDUs in contention over the same topology resource that results in continuous performance degradation of the APPN network.

Using APPN topology database update enhancements

If you want to use this function, perform the task in Table 37 on page 63.
### Provide ACF/TAP as part of z/OS Communications Server

z/OS V1R11 Communications Server includes Advanced Communications Function/Trace Analysis Program (ACF/TAP). ACF/TAP was previously included only as part of the Advanced Communications Function/System Support Program (ACF/SSP) product. ACF/TAP provides a full set of functions to format trace information, including VTAM buffer traces, VTAM internal traces, and NCP traces.

#### Using ACF/TAP as part of z/OS Communications Server

If you want to use this function, perform the task in Table 38.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format VTAM internal traces.</td>
<td>Specify the ACF/TAP INPUT=VIT control parameter.</td>
<td>ACF/TAP parameters in z/OS Communications Server: ACF/TAP Trace Analysis Handbook</td>
</tr>
<tr>
<td>Format VTAM buffer traces.</td>
<td>Specify the ACF/TAP INPUT=BUFFER control parameter.</td>
<td>ACF/TAP parameters in z/OS Communications Server: ACF/TAP Trace Analysis Handbook</td>
</tr>
<tr>
<td>Format line traces.</td>
<td>Specify the ACF/TAP INPUT=LINE control parameter.</td>
<td>ACF/TAP parameters in z/OS Communications Server: ACF/TAP Trace Analysis Handbook</td>
</tr>
<tr>
<td>Format generalized path information unit (PIU) traces.</td>
<td>Specify ACF/TAP INPUT=GPT control parameter.</td>
<td>ACF/TAP parameters in z/OS Communications Server: ACF/TAP Trace Analysis Handbook</td>
</tr>
<tr>
<td>Format scanner interface traces.</td>
<td>Specify the ACF/TAP INPUT=LINE control parameter.</td>
<td>ACF/TAP parameters in z/OS Communications Server: ACF/TAP Trace Analysis Handbook</td>
</tr>
</tbody>
</table>
Table 38. Provide ACF/TAP as part of z/OS Communications Server (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format network control program (NCP) transmission group traces.</td>
<td>Specify the ACF/TAP INPUT=LINE control parameter.</td>
<td>ACF/TAP parameters in z/OS Communications Server, ACF/TAP Trace Analysis Handbook</td>
</tr>
</tbody>
</table>

System management and monitoring

z/OS V1R11 Communications Server includes enhancements to system management and monitoring in the following areas:

- “IBM Health Checker for z/OS RFC 4301 compliance”
- “Network management enhancements”
- “Verbose Ping” on page 68

IBM Health Checker for z/OS RFC 4301 compliance

z/OS V1R11 Communications Server includes a new z/OS Health Checker for z/OS migration health check. This migration health check helps you determine whether IPSec filter rules that are not in compliance with RFC 4301 are active on your current systems. The check also provides guidance on the migration procedures and options available to migrate such IPSec filter rules to become compliant with RFC 4301.

Dependency: IBM Health Checker for z/OS must be active for you to use this function.

Using the IBM Health Checker for z/OS RFC 4301 compliance

If you want to use this function, perform the task in Table 39.

Table 39. IBM Health Checker for z/OS RFC 4301 compliance

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Use the migration health check. | Perform the following steps:  
1. Configure and start the IBM Health Checker for z/OS.  
2. Review the check output for potential migration actions. | See the following topics in IBM Health Checker for z/OS User’s Guide:  
- Setting up IBM Health Checker for z/OS  
- Working with check output  
- Managing checks |

Network management enhancements

z/OS V1R11 Communications Server enhances its network management functions to provide the following information:

- “Stack configuration data”
- “Detailed CSM usage” on page 65
- “OSA network traffic analyzer data” on page 66
- “Sysplex networking data” on page 67

Stack configuration data

z/OS V1R11 Communications Server provides TCP/IP stack profile information in a new SMF 119 event record. The same information is also provided in response to a new GetProfile request for the TCP/IP Callable NMI.
The new SMF 119 event record is subtype 4 and is written to the MVS SMF data sets. The new SMF 119 record can also be obtained from the real-time TCP/IP network monitoring NMI (SYSTCPSM). The new SMF record provides the initial profile information, as well as information about changes to the profile caused by VARY TCPIP,OBEYFILE processing.

The new GetProfile request for the TCP/IP Callable NMI, EZBNMIFR, provides complete profile information. Network management applications can use a combination of the GetProfile request and the new SMF 119 event records that are created during VARY TCPIP,OBEYFILE command processing to monitor changes to the TCP/IP profile settings.

**Obtaining stack configuration data:** If you want to obtain TCP/IP stack configuration data, perform the appropriate tasks in Table 40.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the creation of the SMF 119 subtype 4 event records that provide TCP/IP profile information.</td>
<td>Specify SMFCONFIG TYPE119 PROFILE in the PROFILE.TCPIP configuration file.</td>
<td>SMFCONFIG statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Optionally, configure the real-time TCP/IP network monitoring NMI (SYSTCPSM) to support the SMF 119 subtype 4 event records.</td>
<td>Specify NETMONITOR SMFSERVICE PROFILE in the PROFILE.TCPIP configuration file.</td>
<td>NETMONITOR statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Enable applications to obtain the SMF 119 subtype 4 event records from the real-time TCP/IP network monitoring NMI (SYSTCPSM).</td>
<td>Configure the user IDs that are associated with the applications to access the SYSTCPSM NMI interface.</td>
<td>Real-time TCP/IP network monitoring NMI Configuration and enablement in z/OS Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
<tr>
<td>Obtain TCP/IP stack profile information from the TCP/IP Callable NMI.</td>
<td>Develop or enhance an application to use the new TCP/IP Callable NMI request, GetProfile.</td>
<td>TCP/IP callable NMI (EZBNMIFR) in z/OS Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
</tbody>
</table>

**Detailed CSM usage**

The SNA network management interface (NMI) in z/OS V1R11 Communications Server provides additional storage ownership statistics in response to the Communication Storage Manager (CSM) statistics request. You can request all ownership statistics or a subset of statistics that is based on ASID values.

**Restriction:** The monitor application must explicitly request the additional storage ownership statistics on the CSM statistics request.

**Obtaining detailed CSM usage:** If you want to obtain detailed CSM usage data, perform the appropriate tasks in Table 41 on page 66.
Table 41. Network management interface enhancements - detailed CSM usage

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Update your SNA network monitoring NMI to collect all CSM storage ownership statistics. | Perform the following steps:  
1. Examine the initialization record returned by the VTAM server to verify that VTAM supports the inclusion of request filters on the CSM statistics request.  
2. Build a CSM statistics request. Include a request filter record that specifies a 0 as the ASID value.  
3. Send a CSM statistics request to the VTAM server.  
4. Read the CSM statistics response and parse the new CSM storage owner output section record to obtain the new storage ownership statistics. | SNA network monitoring NMI in z/OS Communications Server: IP Programmer’s Guide and Reference |
| Update your SNA network monitoring NMI to collect CSM storage ownership statistics for a specific ASID. | Perform the following steps:  
1. Examine the initialization record returned by the VTAM server to verify that VTAM supports the inclusion of request filters on the CSM statistics request.  
2. Build a CSM statistics request. Include up to four request filter records, where each individual record specifies a single ASID value for which storage ownership statistics are requested.  
3. Send a CSM statistics request to the VTAM server.  
4. Read the CSM statistics response and parse the new CSM storage owner output section record to obtain the new storage ownership statistics. | SNA network monitoring NMI in z/OS Communications Server: IP Programmer’s Guide and Reference |

OSA network traffic analyzer data

In z/OS V1R11 Communications Server, the OSA-Express network traffic analyzer trace facility provides real time trace collection similar to the SYSTCPIP packet trace collection.

Dependencies:
- To enable the OSA-Express network traffic analyzer, you must be running at least an IBM System z9 EC or z9 BC and OSA-Express2 feature in QDIO mode (CHPID type ONS). See the 2094DEVICE Preventive Service Planning (PSP) and the 2096DEVICE Preventive Service Planning (PSP) buckets for more information.
- To use this function, you must configure an AF_UNIX NETWORK statement in the BPXPRMxx parmlib member.

Obtaining OSA network traffic analyzer data: If you want to obtain OSA network traffic analyzer data, perform the appropriate tasks in Table 42 on page 67.
### Table 42. OSA network traffic analyzer data

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Define the AF_UNIX socket domain  (necessary only if AF_UNIX socket is not already defined). | Add the following to the BPXPRMxx parmlib member:  
FILESYSTYPE TYPE(UDS)  
ENTRYPOINT (BPXTUIN1)  
NETWORKDOMAINNAME(AF_UNIX)  
DOMAINNUMBER(1) MAXSOCKETS(nnn)  
TYPE(UDS)  
where nnn is the maximum number of AF_UNIX sockets. | z/OS UNIX System Services Planning |
| Enable the OSAENTA services on this TCPIP stack. | Specify the NTATRCSERVICE parameter on the NETMONITOR profile statement. | NETMONITOR in z/OS Communications Server: IP Configuration Reference |
| Optionally, limit access to these trace services to specific applications by using RACF (or an equivalent external security manager). | If you are using RACF, issue the following commands:  
SETROPTS CLASSACT(SERVAUTH)  
RDEFINE SERVAUTH EZIP.ETMGT.sysname.tcpiprcname.* UACC(NONE)  
PERMIT EZIP.ETMGT.sysname.tcpiprcname.* USERID(userid)  
SETROPTS RACLIST(REFRESH)  
where userid is the client’s user ID that is permitted.  
This generic profile covers all the TCP/IP Network Management interfaces. Create individual profiles to attain granularity. | z/OS Communications Server: IP Configuration Guide |
| Update or create an application that uses the real-time asynchronous data collection and formatting interfaces. | Review the instructions in z/OS Communications Server: IP Programmer’s Guide and Reference | Real-time TCP/IP network monitoring NMI in z/OS Communications Server: IP Programmer’s Guide and Reference |

### Sysplex networking data

In z/OS V1R11 Communications Server, the TCP/IP Callable NMI, EZBNMIFR provides sysplex networking data. The new request types are as follows:

- GetSysplexXCF - Obtains information about dynamic XCF addresses for all TCP/IP stacks in the sysplex
- GetDVIPAList - Obtains information about dynamic virtual IP addresses (DVIPAs)
- GetDVIPAPortDist - Obtains information about DVIPA port distribution
- GetDVIPARoute - Obtains information about DVIPA routes
- GetDVIPACConnRTab - Obtains information about DVIPA connections

The DVIPA information provided by EZBNMIFR is similar to information that can be obtained from the IBM TCP/IP MVS Enterprise-specific MIB using SNMP.

**Obtaining sysplex networking data:** If you want to obtain sysplex networking data, perform the task in Table 43 on page 68.
Table 43. NMI sysplex networking data

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Update your NMI application that uses the EZBNMIFR interface to collect the sysplex networking data. | Specify one of the new request types when invoking the EZBNMIFR interface:  
  - Use request type NWMSYXCFCTYPE to obtain information about dynamic XCF addresses for all TCP/IP stacks in the sysplex.  
  - Use request type NWMDVLISTTYPE to obtain information about DVIPAs.  
  - Use request type NWMDVPORTDISTTYPE to obtain information about DVIPA port distribution.  
  - Use request type NWMDVROUETYPE to obtain information about DVIPA routes.  
  - Use request type NWMDVCNNRTABTYPE to obtain information about DVIPA connections. | TCP/IP callable NMI (EZBNMIFR) in z/OS Communications Server: IP Programmer’s Guide and Reference |

Verbose Ping

In z/OS V1R11 Communications Server, the Verbose/–v parameter causes the Ping command to display details of the echo reply packets that have been received, and summary statistics regarding the echo packets (number of requests sent, number of replies received, and number of packets lost), and the round-trip times (minimum, maximum, average, and standard deviation) based on the response times from the echo replies that were received.

Using the Verbose Ping command

If you want to use this function, perform the task in Table 44.

Table 44. Verbose Ping

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the Ping command to display details for the echo reply packets that were received and to display summary statistics.</td>
<td>Invoke the TSO PING command with the Verbose parameter, or the z/OS UNIX ping or oping command with the -v parameter, and vary the size of the outbound echo request packet.</td>
<td>Ping in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
</tbody>
</table>

Virtualization

z/OS V1R11 Communications Server includes enhancements to virtualization in the following areas:

- “QDIO enhancements for Workload Manager IO priority”
- “QDIO support for OSA interface isolation” on page 69

QDIO enhancements for Workload Manager IO priority

z/OS V1R11 Communications Server introduces a new WLMPRIORITYQ parameter on the GLOBALCONFIG profile statement. You can use this parameter to establish a mapping of Workload Manager (WLM) service classes to outbound Queued Direct I/O (QDIO) priorities. This mapping is used to determine the...
QDIO write priority for outbound packets. This function automatically extends the preferential treatment of the most important workloads for a business through the QDIO device driver all the way to the LAN.

You can also use the WLMPRIORITYQ parameter to apply the outbound priority to forwarded packets.

**Restrictions:**
- Prioritization using the WLM service class is effective only when enabled and when the ToS or Traffic Class value is 0.
- Prioritization using the WLM service class is ineffective for interfaces other than OSA-Express features in QDIO mode.
- Prioritization of forwarded packets is ineffective unless DATAGRAMFWD is specified on the IPCONFIG statement, the IPCONFIG6 statement, or both statements.
- The WLMPRIORITYQ setting for forwarded packets has no effect on accelerated packets.

**Using the QDIO enhancements for WLM IO priority**

If you want to use this function, perform the tasks in Table 45.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the WLMPRIORITYQ parameter using the default mapping.</td>
<td>Perform the following steps:</td>
<td><strong>GLOBALCONFIG in z/OS Communications Server: IP Configuration Reference</strong></td>
</tr>
<tr>
<td></td>
<td>1. Specify the WLMPRIORITYQ parameter on the GLOBALCONFIG statement in the TCP/IP profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Start TCP/IP or issue the VARY OBEYFILE command.</td>
<td></td>
</tr>
<tr>
<td>Enable the WLMPRIORITYQ parameter using a mapping other than the default.</td>
<td>Perform the following steps:</td>
<td><strong>GLOBALCONFIG in z/OS Communications Server: IP Configuration Reference</strong></td>
</tr>
<tr>
<td></td>
<td>1. Specify the WLMPRIORITYQ IOPRIn control_values parameter on the GLOBALCONFIG statement in the TCP/IP profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Start TCP/IP or issue the VARY OBEYFILE command.</td>
<td></td>
</tr>
<tr>
<td>Display the current WLMPRIORITYQ mapping.</td>
<td>Issue the Netstat CONFIG/-f command.</td>
<td><strong>Netstat CONFIG/-f report in z/OS Communications Server: IP</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>System Administrator's Commands</strong></td>
</tr>
</tbody>
</table>

**QDIO support for OSA interface isolation**

z/OS V1R11 Communications Server enables a stack that is using an OSA-Express feature to prevent packets from flowing directly between two stacks that are sharing the OSA device. This is called connection isolation and when it is in effect, the OSA-Express feature discards packets whose next-hop address was registered by a sharing stack. The OSA-Express feature requires that both stacks that share the port be non-isolated for direct routing to occur.

**Restrictions:**
- OSA-Express connection isolation is supported only for OSA-Express features in QDIO mode.
• OSA-Express connection isolation is not supported when the OSA-Express feature is defined using a DEVICE and LINK statement.

Dependency: This function is limited to OSA-Express2 or OSA-Express3 Ethernet features in QDIO mode (CHPID type OSD) and running at least an IBM System z9 Enterprise Class (EC) or z9 Business Class (BC). See the 2094DEVICE, 2096DEVICE, 2097DEVICE, or 2098DEVICE Preventive Service Planning (PSP) bucket for more information.

Using the QDIO support for OSA interface isolation
If you want to use this function, perform the appropriate tasks in Table 46.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine the Licensed Internal Code level of the OSA-Express feature.</td>
<td>Use the VTAM DISPLAY TRL command to determine the OSA-Express Licensed Internal Code level that is currently installed. See the DISPLAY TRL command for more information.</td>
<td>DISPLAY TRL command in z/OS Communications Server: SNA Operation</td>
</tr>
<tr>
<td>Enable OSA-Express connection isolation.</td>
<td>Perform the following steps: 1. Specify the ISOLATE parameter on the INTERFACE statements in the TCP/IP profile. 2. Start TCP/IP.</td>
<td>INTERFACE — IPAQENET OSA-Express QDIO interfaces and INTERFACE — IPAQENET6 OSA-Express QDIO interfaces in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Display information about the OSA-Express connection isolation.</td>
<td>Issue the Netstat DEvlinks/-d command.</td>
<td>Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
</tbody>
</table>
Chapter 4. V1R10 new function summary

This information contains topics about every function or enhancement introduced in z/OS V1R10 Communications Server. Each function is described and the following information is presented if applicable:

- Restrictions, dependencies, and coexistence considerations of the function
- A task table that identifies the actions necessary to use the function
- References to the documents that contain more detailed information

See Table 8 on page 21 for a complete list of the IP functional enhancements of the current and recent releases.

See z/OS Migration for information about how to migrate and maintain the functional behavior of previous releases.

See z/OS Summary of Message and Interface Changes for information about new and changed messages and interfaces.

Support considerations in V1R10

z/OS V1R10 Communications Server removes support for the traffic regulation (TR) policy as part of the Quality of Service (QoS) policy type. The TR policy function is still available, but only as part of the Intrusion Detection Services (IDS) policy type. See “Remove support of traffic regulation policy in Policy Agent” on page 87 for details.

In a future release of z/OS, support for the following is planned to be discontinued:

- Network Database (NDB) function
- Dynamic Host Configuration Protocol (DHCP) server
- Boot Information Negotiation Layer (BINL) function
- Berkeley Internet Name Domain 4.9.3 (BIND 4.9.3) DNS server, including the Connection Optimization (DNS/WLM) function

z/OS V1R10 Communications Server provides four new IBM Health Checker for z/OS checks to help you determine whether these four functions are active on your current systems. See “IBM Health Checker for z/OS enhancements” on page 109 for more information about the new checks.

See z/OS Migration for detailed information about all the z/OS V1R10 Communications Server support considerations, including the steps you should take to migrate.

Performance improvements for IP in V1R10

z/OS V1R10 Communications Server improves performance in the following areas:

- “TCP/IP performance improvements” on page 72
- “IPSec cryptography performance improvements” on page 72
- “TN3270E Telnet server ECSA reduction” on page 72
TCP/IP performance improvements

In z/OS V1R10 Communications Server, TCP/IP performance is improved in the following ways:

- The TCP/IP data path has improved pathlength and scalability, and it provides virtual storage constraint relief. Specifically, z/OS V1R10 Communications Server does the following:
  - Reduces extended common storage area (ECSA) consumption for TCP/IP workloads. Earlier releases of z/OS Communications Server housed portions of inbound datagrams in ECSA, and in certain circumstances, system outages caused by ECSA usage spikes could occur. z/OS V1R10 Communications Server does not use ECSA to hold inbound IP traffic.
  - Reduces system pathlength for the TCP/IP data path. This results in more efficient TCP/IP communications (potentially lower utilization of the LPAR), and can lead to improved network response time if the z/OS image is currently MIPs-constrained.
  - Improves scalability. On System z LPAR images with a large number of CPs, this performance improvement reduces contention in the machine's internal memory hierarchy. This can result in improved scalability on large multiprocessors.

See “TCP/IP performance improvements for SNA” on page 135 for details about how TCP/IP performance is improved for SNA.

- The UDP layer is enhanced to enable more efficient processing of incoming datagrams when an application has multiple threads concurrently reading datagrams from the same datagram socket. With this enhancement, the UDP layer now wakes up only a single thread to process an incoming datagram, which reduces overhead by avoiding the unnecessary resumption and suspension of multiple threads for every incoming datagram.

This function is automatically enabled.

IPSec cryptography performance improvements

In z/OS V1R10 Communications Server, IPSec processing provides reduced CPU use and latency. This function is automatically enabled.

TN3270E Telnet server ECSA reduction

z/OS V1R10 Communications Server reduces the ECSA storage requirements for TN3270E Telnet Server receive processing. This function is also available for SNA; see “TN3270E Telnet server ECSA reduction” on page 129.

This function is automatically enabled.

Security

z/OS V1R10 Communications Server improves security in the following areas:

- “DataPower integration with NSS SAF access service” on page 73
- “Defensive filtering” on page 74
- “Allow routed traffic in default filter policy” on page 75
- “IPSec RFC currency” on page 75
- “Enhanced port access control” on page 77
- “Enhanced rpcbind application registration control” on page 77
- “FTP security enhancements” on page 81
DataPower integration with NSS SAF access service

IBM DataPower Service Oriented Architecture (SOA) appliances are network devices that simplify, help to secure, and accelerate your XML and Web services deployments while extending your SOA infrastructure. XML appliances also secure and accelerate the parsing and transformation of many message formats, including XML-based messages.

In z/OS V1R10 Communications Server, z/OS network security services (NSS) adds a new XMLAppliance discipline that provides the basic infrastructure for XML appliance security. This discipline provides the XML appliance acting in the role of NSS client with the ability to act as a logical extension of z/OS security.

The new discipline adds the XMLAppliance SAF access service to the NSS server, which provides NSS with the capability to invoke a selected set of SAF functions on behalf of its clients. This allows NSS to become the conduit for making remote SAF calls.

By connecting as an NSS client, IBM DataPower SOA appliances can access these SAF functions as part of their security offerings.

A network administrator can monitor the different types of NSS clients and the associated client connections using the new nssctl command. Each type of NSS client appears in the client listing, with pertinent information such as their NSS discipline, the services they are accessing, name, connection state, connection time, the time of the last message received, and the services they have selected and enabled.

Dependencies for DataPower integration with NSS SAF access service

NSS XMLAppliance clients must secure communications to the NSS server using Transport Layer Security (TLS).

Using DataPower integration with NSS SAF access service

If you want to use this function, perform the appropriate tasks in Table 47.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the NSS server to enable only the security disciplines that will be used.</td>
<td>Add the Discipline parameter on the NssConfig statement in the NSS configuration file to specify which disciplines to enable.</td>
<td>Network security services in z/OS Communications Server: IP Configuration Guide</td>
</tr>
<tr>
<td>Define required SERVAUTH profiles on the NSS server to enable network security services for XML appliances.</td>
<td>Add corresponding SERVAUTH definitions to SAF-compliant security product profiles.</td>
<td>Network security services in z/OS Communications Server: IP Configuration Guide</td>
</tr>
<tr>
<td>Permit users to use the nssctl command.</td>
<td>Add the SERVAUTH definition EZB.NETMGM.T.sysname.sysname.NSS.DISPLAY to SAF-compliant security product profiles.</td>
<td>Network security services in z/OS Communications Server: IP Configuration Guide</td>
</tr>
</tbody>
</table>
Table 47. DataPower integration with NSS SAF access service (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor different types of NSS clients that are currently connected to the NSS server.</td>
<td>Use the <code>nsscti -d</code> command</td>
<td>z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
</tbody>
</table>

**Defensive filtering**

Defensive filtering provides a mechanism for an external security information and event manager to install defensive filters in a TCP/IP stack to block detected attacks. An external security information and event manager analyzes and correlates information that it receives from systems throughout the network. If an attack is detected, the external manager can install one or more defensive filters that can discard packets associated with the attack.

z/OS V1R10 Communications Server provides an enhanced z/OS UNIX `ipsec` command to add and manage defensive filters on a local system. The command can be issued autonomically by an external security information and event manager or manually by an authorized user.

A Defense Manager daemon (DMD) provides persistence for the defensive filters. If a TCP/IP stack is restarted, the DMD will reinstall the applicable defensive filters.

**Restrictions for defensive filtering**

IP security must be enabled for a TCP/IP stack before defensive filters can be installed in the stack.

**Dependencies for defensive filtering**

The DMD depends on the following:

- z/OS UNIX System Services for its runtime environment
- RACF (or an equivalent external security manager) to manage resource profiles

**Using defensive filtering**

If you want to use this function, perform the appropriate tasks in Table 48.

Table 48. Defensive filtering

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Configure the TCP/IP profile for IP security, if not already configured. | Perform the following steps to create a minimal IP security policy:
1. Specify the IPSECURITY parameter on the `IPCONFI` statement in the TCPIP profile.
2. Optionally, specify the IPSECURITY parameter on the `IPCONFI6` statement in the TCPIP profile.
3. Define a default filter rule to permit all traffic using the `IPSEC` statement in the TCPIP profile. | z/OS Communications Server: IP Configuration Reference |
| Provide event logging for defensive filters by ensuring that TRMD automatically starts with the stack. | Modify the AUTOLOG section of the TCPIP profile. | z/OS Communications Server: IP Configuration Guide |
Table 48. Defensive filtering (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the Defense Manager daemon.</td>
<td>Create the configuration file manually using a text editor.</td>
<td>- Defensive filtering in z/OS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communications Server: IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- DMConfig and DmStackConfig</td>
</tr>
<tr>
<td></td>
<td></td>
<td>statements in z/OS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communications Server: IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration Reference</td>
</tr>
<tr>
<td>Authorize resources for the</td>
<td>Use a SAF-compliant security product to create the profiles.</td>
<td>- Defensive filtering in z/OS</td>
</tr>
<tr>
<td>Defense Manager daemon.</td>
<td></td>
<td>Communications Server: IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System Administrator’s Commands</td>
</tr>
<tr>
<td>Define the required SERVAUTH profiles for</td>
<td>Use a SAF-compliant security product to create the profiles.</td>
<td>- Managing network security in</td>
</tr>
<tr>
<td>the  ipsec command.</td>
<td></td>
<td>z/OS Communications Server: IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration Reference</td>
</tr>
<tr>
<td>Start the Defense Manager daemon.</td>
<td>Use one of the methods described in &quot;Controlling the Defense Manager daemon&quot;</td>
<td>- Defensive filtering in z/OS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communications Server: IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration Guide</td>
</tr>
<tr>
<td>Manage defensive filter information</td>
<td>Issue the ipsec -F command to add, update, delete, and display defensive</td>
<td>- Managing network security in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>filters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>z/OS Communications Server: IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System Administrator’s Commands</td>
</tr>
</tbody>
</table>

Allow routed traffic in default filter policy

Prior to z/OS V1R10 Communications Server, only local traffic could be permitted with the default policy filter rules specified in the TCP/IP profile. In z/OS V1R10 Communications Server, you can permit local and routed traffic with the default filter policy.

If you want to use this function, perform the task in Table 49.

Table 49. Allow routed traffic in default filter policy

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit routed traffic in the default filter policy.</td>
<td>Specify the value ROUTED or EITHER for the ROUTING parameter on the IPSECRULE and IPSEC6RULE statement in the TCP/IP Profile.</td>
<td>- See the IPSECRULE and IPSEC6RULE parameters on the IPSEC statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
</tbody>
</table>

IPSec RFC currency

In z/OS V1R10 Communications Server, IPSec RFC currency implements the mandatory support that is required by RFCs 4301, 4302, 4303, 4304, 4305, 4308, and 4835, with the exception of the requirements that depend on Internet Key Exchange version 2 (IKEv2).

Enhancements to virtual private network (VPN) support for mobile users allow identification by Internet Key Exchange (IKE) identity rather than IP address. IP filtering controls and handling of packets in VPN tunnels are improved in accordance with the new standards. You can restrict VPN tunnel negotiation parameters to limit the data addresses that an IKE peer can protect.
**Using IPSec RFC currency**

If you want to use this function, perform the appropriate tasks in Table 50.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable support for additional packet filtering parameters.</td>
<td>Specify a range of ICMP types and codes, a range of ICMPv6 types and codes, or a range of mobile IPv6 header (MIPv6) message types on the IpService statement in the Policy Agent IPSec configuration file.</td>
<td>IpService statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Enable support for filtering OPAQUE selector values (such as for the IPv6 protocol values for fragmented packets when the protocol is not known) and for filtering fragmented packets.</td>
<td>Specify the OPAQUE selector or the FragmentsOnly parameter on the IpService statement in the Policy Agent IPSec configuration file.</td>
<td>IpService statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Use the reserved SPI range for manual tunnels to prevent conflict with dynamic tunnels.</td>
<td>Specify inbound SPI values in the range 256 - 4096.</td>
<td>IpManVpnAction statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Enable support for IPv4 multicast SAs.</td>
<td>Configure two IpFilterRule statements and an appropriate IpManVpnAction statement to protect multicast traffic.</td>
<td>Multicast traffic in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Control passthrough of Don't-Fragment (DF) bit and Differentiated Services Code Point (DSCP) QoS field from inner to outer IP header in tunnel mode.</td>
<td>Configure the PassthroughDSCP and PassthroughDF parameters on the IpDynVpnAction and IpManVpnAction statements.</td>
<td>IpDynVpnAction and IpManVpnAction statements in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Enable support for sending ICMP or ICMPv6 errors for packets discarded by IPSec.</td>
<td>Specify the ICMP value for the DiscardAction parameter on the IpGenericFilterAction statement in the Policy Agent IPSec configuration file.</td>
<td>IpGenericFilterAction statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Use the industry standard VPN-A suite in IPSec configuration.</td>
<td>Specify the VPN-A security level in the z/OS Communications Server Configuration Assistant.</td>
<td>none</td>
</tr>
<tr>
<td>Restrict the range of data endpoint IP addresses for which an IKE peer can negotiate IPSec protection.</td>
<td>Specify the ConstrainSource and ConstrainDest parameters on the KeyExchangeAction statement.</td>
<td>KeyExchangeAction statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Display new IP filter options using the ipsec command.</td>
<td>Issue the ipsec -f command to view the new option settings on the IpFilterRule statement.</td>
<td>IP filter (-f) primary option in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Display new dynamic tunnel options using the ipsec command.</td>
<td>Issue the ipsec -y command to view the new option settings on the IpDynVpnAction statement.</td>
<td>Dynamic tunnel (-y) primary option in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
</tbody>
</table>
Table 50. IPSec RFC currency (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display new manual tunnel options using the <code>ipsec</code> command.</td>
<td>Issue the <code>ipsec -m</code> command to view the new option settings on the IpManVpnAction statement.</td>
<td>Manual tunnel (-m) primary option in Z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
<tr>
<td>Retrieve new IP filtering and IP tunnel options using the IPSec network management interface (NMI).</td>
<td>Issue the following NMI requests:</td>
<td>Network management interfaces (NMIs) in Z/OS Communications Server: IP Programmer's Guide and Reference</td>
</tr>
<tr>
<td></td>
<td>• NMsec_GET_IPFLTCURR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NMsec_GET_IPFLTDEFAULT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NMsec_GET_IPFLTPOLICY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NMsec_GET_IPTUNDYNSTACK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NMsec_GET_IPTUNMANUAL</td>
<td></td>
</tr>
</tbody>
</table>

Enhanced port access control

In z/OS V1R10 Communications Server, you can use the PORT profile statement to control application access to port numbers that are not reserved by a PORT or PORTRANGE statement.

Using enhanced port access control

If you want to use this function, perform the appropriate tasks in Table 51.

Table 51. Enhanced port access control

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine the access to unreserved ports that you want to control.</td>
<td>Review the implications of controlling explicit bind access or TCP listen access.</td>
<td>Port access control in Z/OS Communications Server: IP Configuration Guide</td>
</tr>
<tr>
<td>Establish access control for unreserved ports.</td>
<td>Configure one or more PORT UNRSV statements in your TCP/IP profile.</td>
<td>PORT statement in Z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Display the jobs that can access an unreserved port.</td>
<td>Issue the Netstat PORTList/-o command to view entries that have the port number value UNRSV. If there are no such entries for a protocol, all jobs using that protocol are permitted to access an unreserved port.</td>
<td>Netstat PORTList/-o report in Z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
</tbody>
</table>

Enhanced rpcbind application registration control

z/OS V1R10 Communications Server enhances rpcbind in the following areas:

-Rpcbind supports an additional level of security when registering or unregistering applications. You can now define a SERVAUTH resource profile that controls which applications or users can register and unregister with rpcbind.

- Rpcbind is supported in a multilevel secure (MLS) environment. When a target assistance procedure is running in a multilevel security environment, rpcbind switches to the security label of the requester. This ensures that the correct port-of-entry information is presented to the target server.
Restrictions for enhanced rpcbind application registration control

Although rpcbind is now a trusted application in a multilevel secure environment, not all applications that use rpcbind are trusted in a multilevel secure environment. For example, NDB can use rpcbind in place of portmapper, but NDB is not a trusted application.

Dependencies for enhanced rpcbind application registration control

The following dependencies apply for the rpcbind registry enhancement:

- In a multilevel secure environment, applications are not able to register or unregister with rpcbind unless the profile EZB.RPCBINDsystemname.rpcbindname.REGISTRY in the SERVAUTH class is defined. When the profile is defined, only applications invoked by user IDs that have READ access can register and unregister with the rpcbind server.

In environments that are not multilevel secure, defining the RACF profile is optional. If you do define the SERVAUTH profile, all RPC applications that register or unregister with rpcbind must be invoked by user IDs that have READ access to the profile.

The rpcinfo utility unregisters applications with rpcbind and portmapper when the utility is invoked with the -d option. When rpcbind is in use and the SERVAUTH profile is defined, you can enable users to unregister applications with rpcinfo by granting their user IDs READ access to the SAF profile.

See the first task in Table 52 on page 79 to help identify whether your applications register or unregister with rpcbind. When rpcbind is in use and the SERVAUTH profile is defined, these applications must be invoked by user IDs that have READ access to the profile.

The following dependencies apply for the rpcbind Target Assistance enhancement when the rpcbind server is running in a multilevel secure environment:

- When the SAF profile BPX.POE is defined in the SERVAUTH class, the rpcbind user ID must have READ access to the profile to enable the rpcbind server to invoke target assistance requests.
  - If the profile BPX.POE is not defined in the SERVAUTH class, the rpcbind user ID must be assigned UID(0) to enable the rpcbind server to invoke target assistance requests.
  - The RPC library functions, pmap_rmtcall() and clnt_broadcast(), send a target assistance procedure RPC on behalf of the caller to rpcbind or portmapper, whichever is running on the target host. If your installation supports applications that issue these library calls, you must permit the rpcbind user ID to the SAF profile, or assign UID(0) to the rpcbind user ID.
  - The rpcinfo utility issues a target assistance request when the utility is invoked with the -b option. If you want to enable users to query the rpcbind server on your host with the rpcinfo -b option, you must permit the rpcbind user ID to the SAF profile, or assign UID(0) to the rpcbind user ID.

Coexistence requirements for enhanced rpcbind application registration control

You must use rpcbind rather than portmapper to use this function. Portmapper is not trusted in the MLS environment.

Using the enhanced rpcbind application registration control

If you want to use this function, perform the appropriate tasks in Table 52 on page 79 and Table 53 on page 80.
<table>
<thead>
<tr>
<th>Task (for registry updates)</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Determine whether your application registers or unregisters with portmapper or rpcbind. | Analyze your application to determine whether it does one of the following:  
- Issues the following RPC library calls:  
  - `registerrpc()`  
  - `svc_register()`  
  - `pmap_set()`  
  - `pmap_unset()`  
- Sends the following RPCs to the rpcbind server:  
  - `PMAPPROC_SET`, `PMAPPROC_UNSET`, `RPCBPROC_SET`, `RPCBPROC_UNSET`  
Rules:  
- Server applications that require portmapper or rpcbind to be started probably register and unregister with portmapper or rpcbind.  
- Network data base (NDB) and NFS are server applications that register and unregister with portmapper or rpcbind. | • Registering with rpcbind and Remote procedure calls in the z/OS Communications Server environment in z/OS Communications Server: IP Programmer’s Guide and Reference  
• RFC 1833: Binding Protocols for ONC RPC Version 2 |
| Control which applications can register or unregister with the rpcbind server. | Perform the following steps:  
1. Define this SERVAUTH class resource profile to your security product:  
   `EZB.RPCBIND.systemname.rpcbindname.REGISTRY`.  
2. Enable applications to register and unregister with rpcbind by granting the user IDs that they run under at least READ access to the resource profile.  
Result: When the environment is not multilevel secure and you do not define a profile in the SERVAUTH class, all applications on the rpcbind server host can register and unregister with the rpcbind server. | • Configuring Security Server (RACF or equivalent) items in z/OS Communications Server: IP Configuration Guide  
• z/OS Communications Server: IP Programmer’s Guide and Reference  
• z/OS Security Server RACF Command Language Reference |
| Control which users can use rpcinfo to delete application registrations. | Perform the following steps:  
1. Define this SERVAUTH class resource profile to your security product:  
   `EZB.RPCBIND.systemname.rpcbindname.REGISTRY`.  
2. Grant the user IDs that you want to enable to delete application registrations at least READ access to the resource profile.  
Result: When the environment is not multilevel secure and you do not define a profile in the SERVAUTH class, only UID(0) users can delete registrations using rpcinfo. | • Configuring Security Server (RACF or equivalent) items in z/OS Communications Server: IP Configuration Guide  
• `rpcinfo` in z/OS Communications Server: IP System Administrator’s Commands and The z/OS UNIX System Services `rpcinfo`/`rpcinfo` command: Display server information in z/OS Communications Server: IP System Administrator’s Commands  
• z/OS Security Server RACF Command Language Reference |
Table 52. Enhanced rpcbind application registration control - Registry updates (continued)

<table>
<thead>
<tr>
<th>Task (for registry updates)</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable applications to register or unregister with the rpcbind server in a multilevel secure environment.</td>
<td>Perform the following steps:&lt;br&gt;1. Define this SERVAUTH class resource profile to your security product: EZB.RPCBIND.&lt;br&gt;systemname.&lt;br&gt;daemonname.&lt;br&gt;REGISTRY.&lt;br&gt;2. Enable applications to register and unregister with rpcbind by granting the user IDs that they run under at least READ access to the resource profile.</td>
<td>• Rccinfo in z/OS Communications Server: IP System Administrator’s Commands&lt;br&gt;• z/OS Security Server RACF Command Language Reference&lt;br&gt;• z/OS UNIX rpcbind server in z/OS Communications Server: IP Configuration Guide&lt;br&gt;<strong>Result:</strong> If you do not define a profile, applications in a multilevel secure environment cannot register or unregister with the rpcbind server.</td>
</tr>
</tbody>
</table>

Control which users can use rpcinfo to delete application registrations in a multilevel secure environment.

Perform the following steps:<br>1. Define this SERVAUTH class resource profile to your security product: EZB.RPCBIND.<br>systemname.<br>daemonname.<br>REGISTRY.<br>2. Grant the user IDs you want to enable to delete rpcbind registrations with rpcinfo READ access or greater to the resource profile.<br><br>**Result:** When you do not define a profile, users cannot use rpcinfo to delete application registrations.

Table 53. Enhanced rpcbind application registration control - Target assistance requests

<table>
<thead>
<tr>
<th>Task (for target assistance requests)</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine whether your application issues target assistance requests.</td>
<td>Analyze your application to determine whether it does one of the following:&lt;br&gt;• Issues these RPC library calls:&lt;br&gt;  pmap_rmtcall()&lt;br&gt;  chnt_broadcast&lt;br&gt;• Sends these RPCs to the rpcbind server:&lt;br&gt;  PMAPPROC_CALLIT, RPCBPROC_CALLIT,&lt;br&gt;  RPCBPROC INDIRECT, RPCBPROC_BCAST</td>
<td>• Portmapper and rpcbind target assistance in z/OS Communications Server: IP Programmer’s Guide and Reference&lt;br&gt;• Configuring Security Server (RACF or equivalent) items in z/OS Communications Server: IP Configuration Guide&lt;br&gt;• RFC 1833: Binding Protocols for ONC RPC Version 2</td>
</tr>
</tbody>
</table>

Enable the rpcbind server to support target assistance requests when profile BPX.POE is defined in the FACILITY class.

Grant the rpcbind user ID at least READ access to the profile BPX.POE in class FACILITY.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant the rpcbind user ID at least READ access to the profile BPX.POE in class FACILITY.</td>
<td>• Configuring Security Server (RACF or equivalent) items in z/OS Communications Server: IP Configuration Guide&lt;br&gt;• z/OS Security Server RACF Command Language Reference</td>
</tr>
</tbody>
</table>
Table 53. Enhanced rpcbind application registration control - Target assistance requests (continued)

<table>
<thead>
<tr>
<th>Task (for target assistance requests)</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the rpcbind server to respond to rpcinfo -b requests when profile BPX.POE is defined in the FACILITY class on the rpcbind host.</td>
<td>Grant the rpcbind user ID at least READ access to the profile BPX.POE.</td>
<td>• Configuring Security Server (RACF or equivalent) items in z/OS Communications Server: IP Configuration Guide • z/OS Security Server RACF Command Language Reference</td>
</tr>
</tbody>
</table>

FTP security enhancements

This topic provides information for the FTP security enhancements. See "FTP enhancements" on page 120 for the other (non-security related) FTP items.

z/OS V1R10 Communications Server enhances FTP server logins in the following ways:

• You can configure the FTP server to restrict the users that can log in to the FTP server to only those users who are granted READ access to a resource profile in the SERVAUTH class.

• When logging into the FTP server using the protected port (the port defined by the TLSPORT configuration statement), the FTP server and client initiate a TLS handshake without using the AUTH command. In previous releases, the FTP server had interoperability issues with non-z/OS FTP clients that connect to the protected port. With this enhancement, you can configure the FTP server to support non-z/OS FTP clients that connect to the protected port.

Using FTP security enhancements

If you want to use the FTP security enhancements, use the following tables and perform the appropriate tasks.

• **Table 54 on page 82** use this table to restrict the users that can log in to the FTP server to only those users who are granted read access to a resource profile in the SERVAUTH class.

• **Table 55 on page 82** use this table to configure the FTP server to support non-z/OS FTP clients that connect to the protected port.
Table 54. FTP enhancements: Restrict users that can log in to the FTP server

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict certain users from logging in to the FTP server when sessions are secured with TLS.</td>
<td>Do one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Code and install an FTCHKPWD exit routine that screens the user IDs that are allowed to log in to FTP.</td>
<td>Configuring the optional FTP user exits and Steps for customizing the FTP server for TLS in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td></td>
<td>• Set up the FTP server for TLS level 3 authentication.</td>
<td>The FTCHKPWD user exit in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td></td>
<td>• Code VERIFYUSER TRUE in the server’s FTP.DATA. If you choose this method, you must do the following:</td>
<td>z/OS Security Server RACF Command Language Reference</td>
</tr>
<tr>
<td></td>
<td>– Configure RACF with a profile for the FTP server port.</td>
<td>z/OS Security Server RACF Security Administrator’s Guide</td>
</tr>
<tr>
<td></td>
<td>– Grant users that you want to allow to log in to FTP at least READ access to the profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Activate and RACLIST the SERVAUTH class.</td>
<td></td>
</tr>
<tr>
<td>Restrict certain users from logging in to the FTP server when sessions are not secured with TLS.</td>
<td>Do one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Code and install an FTCHKPWD exit routine that screens the user IDs that are allowed to log in to FTP.</td>
<td>Configuring the optional FTP user exits in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td></td>
<td>• Code VERIFYUSER TRUE in the server’s FTP.DATA. If you choose this method, you must do the following:</td>
<td>The FTCHKPWD user exit and the VERIFYUSER (FTP server) statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td></td>
<td>– Configure RACF with a profile for the FTP server port.</td>
<td>z/OS Security Server RACF Command Language Reference</td>
</tr>
<tr>
<td></td>
<td>– Grant users you want to allow to log into FTP at least READ access to the profile.</td>
<td>z/OS Security Server RACF Security Administrator’s Guide</td>
</tr>
<tr>
<td></td>
<td>– Activate and RACLIST the SERVAUTH class.</td>
<td></td>
</tr>
</tbody>
</table>

Table 55. FTP enhancements: Configure the FTP server to support non-z/OS FTP clients that connect to the protected port

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>For implicitly secured TLS logins, configure the FTP server to support most OEM clients that connect to the server’s protected port.</td>
<td>Configure the FTP server to send reply 220 (the “good morning” reply) after the TLS handshake by coding these statements in FTP.DATA:</td>
<td>TLS client and server and the SECUREIMPLICITZOS (FTP client and server) statements in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td></td>
<td>TLSPORT SECUREIMPLICITZOS FALSE</td>
<td></td>
</tr>
<tr>
<td>For implicitly secured TLS logins, configure the FTP server to support z/OS FTP clients that connect to the server’s protected port.</td>
<td>Code these statements in the server’s FTP.DATA, specifying the same values that are configured or defaulted for the z/OS FTP client:</td>
<td>TLS client and server and the SECUREIMPLICITZOS (FTP client and server) statements in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td></td>
<td>TLSPORT SECUREIMPLICITZOS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tip: The z/OS FTP client and server use the same default values for TLSPORT and SECUREIMPLICITZOS.</td>
<td></td>
</tr>
</tbody>
</table>
Table 55. FTP enhancements: Configure the FTP server to support non-z/OS FTP clients that connect to the protected port (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| For implicitly secured TLS logins, configure the FTP server to send reply 220 immediately after accepting the connection and before the TLS handshake. | Code the following FTP.DATA statements: <br> TLSPORT <br> SECUREIMPLICITZOS TRUE | **TLS/SSL enablement for Load Balancing Advisor**<br><br>The z/OS Load Balancing Advisor collects load balancing data from Load Balancing Agents and sends recommendations to external load balancers. The ability to establish connections between the Advisor, Agents, and external load balancers should be restricted to authorized parties.  

In z/OS V1R10 Communications Server, you can secure and control access to all communications with the Load Balancing Advisor using TLS/SSL technologies. You can authenticate external load balancers, z/OS Load Balancing Agents, and ADNR clients that are connecting to the Load Balancing Advisor using client certificates, and you can perform access control checks using SAF-compliant security product profiles. You can use the AT-TLS feature of the Communications Server to obtain the TLS/SSL support for the Load Balancing Advisor, Agents, and the ADNR function.  

**Restrictions for TLS/SSL enablement for Load Balancing Advisor**<br>To use AT-TLS with client authentication, access control, and encryption, both ends of the connections must support TLS/SSL. Specifically, the following restrictions apply: |
The Advisor must be V1R10 or later for client authentication.

The Agent can be V1R7 or later (AT-TLS was added in V1R7), but the host_connection statement in the Agent configuration file is optional only in V1R10 or later.

ADNR can be V1R8 or later (ADNR was introduced in V1R8), but the host_connection_addr parameter in the ADNR configuration file is optional only in V1R10 and later.

**Dependencies for TLS/SSL enablement for Load Balancing Advisor**
To use AT-TLS for a connection between the Advisor and an external load balancer, this function requires an external load balancer that supports TLS/SSL.

**Tip:** Even if the external load balancer does not support or is not configured for TLS/SSL, the connections between the Advisor and Agents or ADNR can still use AT-TLS.

**Prerequisites for TLS/SSL enablement for Load Balancing Advisor**
Before you begin using this new function, perform the following steps if you have not already done so:

1. Enable Application Transparent Transport Layer Security (AT-TLS). For more information, see the following:
   - Application Transparent Transport Layer Security data protection in [z/OS Communications Server: IP Configuration Guide](#)
   - TCPCONFIG in [z/OS Communications Server: IP Configuration Reference](#)

2. Set authorization for the `pasearch` command. For more information, see Steps for configuring the Policy Agent in [z/OS Communications Server: IP Configuration Guide](#).

3. Enable AT-TLS configuration for Policy Agent. For more information, see the following topics in [z/OS Communications Server: IP Configuration Guide](#):
   - Policy-based networking
   - Application Transparent Transport Layer Security data protection

**Using the TLS/SSL enablement for Load Balancing Advisor**
If you want to use this function, perform the appropriate tasks in Table 56 on page 85.
### Table 56. TLS/SSL enablement for Load Balancing Advisor

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Depending on your network design, determine whether AT-TLS will be  | Determine which Agents and ADNR applications (if used) will have their connections secured with TLS/SSL using AT-TLS instead of using configuration statements for validation, and determine which load balancers will use TLS/SSL.   | See the following topics in Z/OS Communications Server: IP Configuration Guide:  
  - Application Transparent Transport Layer Security data protection  
  - Steps for configuring the z/OS Load Balancing Advisor  
  - Enabling TLS/SSL for z/OS Load Balancing Advisor (optional)  
  - Step 1: Decide which sysplex resources should be managed by ADNR |
| to secure some or all of the connections to the Load Balancing       |                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                      |
| Advisors.                                                            |                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                      |
| If you want to control access by using SAF, define the necessary    | Issue security product commands to establish authorization for user IDs. You can configure the Advisor’s clients (Agents, ADNR, and external load balancers) to present security credentials, including a user ID. If the security credentials are configured, you must set up the security manager on the Advisor system to accept the credentials. The format of the SERVAUTH profile is: EZB.LBA.LBACCESS.sysname.tcpsysplexgroupname EZB.LBA.AGENTACCESS.sysname.tcpsysplexgroupname If the Advisor can run on more than one system name, you must set up all the system names. | Steps for configuring the z/OS Load Balancing Advisor and Enabling TLS/SSL for z/OS Load Balancing Advisor (optional) in Z/OS Communications Server: IP Configuration Guide  
  - z/OS Security Server RACF Command Language Reference |
| SERVAUTH profiles and permit authorized users to these profiles.     |                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                      |
| Define AT-TLS policies in Policy Agent configuration files.         | Specify the AT-TLS policies for the Advisor, Agents, and ADNR in the configuration files that are identified with the CommonTTLSConfig and TTLSConfig statements.                                               | Application Transparent Transport Layer Security data protection, Steps for configuring the z/OS Load Balancing Advisor, and Enabling TLS/SSL for z/OS Load Balancing Advisor (optional) in Z/OS Communications Server: IP Configuration Guide  
  - AT-TLS policy statements in Z/OS Communications Server: IP Configuration Reference  
  - IBM Configuration Assistant for z/OS Communications Server online helps |
**Task** | **Procedure** | **Reference**
--- | --- | ---
Create z/OS server (Advisor) and z/OS client (Agent, ADNR) key rings and necessary certificate authority certificates. | Create server and client key rings. The server key ring must contain a server certificate and any certificates that are used to sign it. The server needs access to the private keys of the server certificate. The client key ring needs the root certificate that is used to sign the server certificates. **Requirement:** The user ID used for the certificates must be the user ID that is permitted to the LBACCESS or AGENTACCESS SERVAUTH profiles. | • For a TLS/SSL primer and some step-by-step examples, see [TLS/SSL security in z/OS Communications Server: IP Configuration Guide](https://www.ibm.com/support/knowledgecenter/SSEPGG_11.2.0/com.ibm.zos.r12.doc/tlsslsecurity.pdf).  
• For more information on managing key rings and certificates with RACF and the RACDCERT command, see [z/OS Security Server RACF Security Administrator’s Guide](https://www.ibm.com/support/knowledgecenter/S5A923_11.2.0/com.ibm.zos.ea5.r12.rrdoc/racg.htm).  
• For detailed information on managing key rings and certificates with gskkyman, see [z/OS Cryptographic Services System SSL Programming](https://www.ibm.com/support/knowledgecenter/S5API2_11.2.0/com.ibm.zos.ea5.r12.rrdoc/gskkyman.htm). |
Configure the external load balancer for TLS/SSL. | Create certificates for the external load balancer. **Requirement:** The user ID used for the certificates must be the user ID that is permitted to the LBACCESS SERVAUTH profile. | See the documentation for the external load balancer. |
Ensure that the Advisor will start if you are using Policy Agent. | Start the Policy Agent before starting the Load Balancing Advisor. | [Steps for configuring the Policy Agent in z/OS Communications Server: IP Configuration Guide](https://www.ibm.com/support/knowledgecenter/S5A923_11.2.0/com.ibm.zos.ea5.r12.rrdoc/pagent.htm) |
Optionally, display policy-based networking information. | Use the `pasearch` command to query the Advisor, Agent, and ADNR policy information from the Policy Agent. | [Displaying policy-based networking information in z/OS Communications Server: IP System Administrator’s Commands](https://www.ibm.com/support/knowledgecenter/S5A923_11.2.0/com.ibm.zos.ea5.r12.rrdoc/pasearch.htm) |
Optionally, display z/OS Load Balancing Advisor, Agent, and ADNR AT-TLS policies. | Use the `netstat` command to display the Advisor, Agent, and ADNR AT-TLS policies. | [Netstat AT-TLS/-x report in z/OS Communications Server: IP System Administrator’s Commands](https://www.ibm.com/support/knowledgecenter/S5A923_11.2.0/com.ibm.zos.ea5.r12.rrdoc/netstat.htm) |
Optionally, if AT-TLS is being used to perform client authentication and to access control checks for all connections to the Load Balancing Advisor, remove the keywords specifying load balancer and Agent IP addresses and ports in the Advisor, Agent, and ADNR configuration files. | Edit the Advisor, Agent, and ADNR configuration files by removing the following statements or parameters (they are optional if TLS/SSL is used for all connections to the Advisor).  
• Advisor configuration file statements  
  – agent_id_list  
  – lb_id_list  
• Agent configuration file statement  
  – host_connection  
• ADNR configuration file parameter on the `gwm_id` statement  
• Automated domain name registration in z/OS Communications Server: IP Configuration Guide](https://www.ibm.com/support/knowledgecenter/S5A923_11.2.0/com.ibm.zos.ea5.r12.rrdoc/endomreg.htm)
Remove support of traffic regulation policy in Policy Agent

z/OS V1R10 Communications Server does not support the traffic regulation (TR) policy as part of the Quality of Service (QoS) policy type. The TR policy function is still available, but only as part of the Intrusion Detection Services (IDS) policy type.

To adjust for the removal of support of traffic regulation policy in Policy Agent, perform the appropriate tasks in Table 57.

In conjunction with Table 57, use the conversion tables as you migrate from QoS TR policies to IDS TR policies. The tables are defined in the IP Services: Migrate from QoS TR policy to IDS TR policy topic of z/OS Migration.

### Table 57. Remove support of traffic regulation policy in Policy Agent

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Convert QoS policies that specify the PolicyScope TR parameter on the PolicyAction statement to IDS policies. | You must convert any PolicyRule statements that reference PolicyAction statements that specify PolicyScope TR to the IDSRule statement with the ConditionType TR parameter. You must also convert the PolicyAction statements to the IDSAction statements with the ActionType TR parameter. You must configure the new IDS policies in an existing or new IDS configuration file. You must configure the new IDS policies in an existing or new IDS configuration file. | • Policy-based networking and Intrusion Detection Services in z/OS Communications Server: IP Configuration Guide
• IP Services: Migrate from QoS TR policy to IDS TR policy in z/OS Migration |
| Configure IDS configuration files. | If you were not using IDS policies prior to the conversion, specify the IDSConfig statement to point to the new image-specific IDS configuration file. Optionally, configure the IDS policies in both common and image-specific configuration files, and also specify the CommonIDSConfig statement. | • Policy-based networking and Intrusion Detection Services in z/OS Communications Server: IP Configuration Guide
• Policy Agent and policy applications in z/OS Communications Server: IP Configuration Reference |
| Refresh the policies. | Refresh the policies by issuing the MODIFY procname,UPDATE command, waiting for the refresh interval to expire, or restarting the Policy Agent. If you are using UNIX files and you previously started the Policy Agent using the -i startup option, then no action is necessary; the new policies are refreshed when the configuration files are saved. | See z/OS Communications Server: IP Configuration Guide for details on refreshing policies. |

Security options for centralized policy server connections

z/OS V1R10 Communications Server enhances the Policy Agent to allow connections between the policy client and policy server to be established without using SSL or AT-TLS. If your installation does not require a secure connection between the policy client and policy server, you can omit the SSL configuration on the policy client, and you do not have to define AT-TLS policies on the policy server for these connections. The policy server still authenticates the policy clients using the user ID and credentials (password or PassTicket) supplied by the policy...
clients. This function allows for authentication only; if SSL or AT-TLS are not used to protect the connection, any sensitive policy information flows in the clear.

**Using the security options for centralized policy server connections**

If you want to use this function, perform the appropriate tasks in Table 58.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate whether you need secure connections</td>
<td>Determine whether your network environment is such that sensitive policy</td>
<td>Security in z/OS Communications Server: IP Configuration Guide</td>
</tr>
<tr>
<td>between policy clients and the policy server.</td>
<td>information needs to be encrypted and sent over secure connections, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>whether authentication using user ID and credentials is sufficient.</td>
<td></td>
</tr>
<tr>
<td>Configure the appropriate level of security.</td>
<td>Do the following:</td>
<td>• Application Transparent Transport Layer Security data protection and</td>
</tr>
<tr>
<td></td>
<td>• On the policy clients, configure the SSL parameters (if needed) on the</td>
<td>Steps for configuring the Policy Agent in z/OS Communications Server: IP</td>
</tr>
<tr>
<td></td>
<td>ServerConnection statement in the main Policy Agent configuration file, or</td>
<td>Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>omit them if secure connections are not needed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On the policy server, configure AT-TLS policies to protect connections</td>
<td>• ServerConnection and Application Transparent Transport Layer Security</td>
</tr>
<tr>
<td></td>
<td>from policy clients, or omit them if secure connections are not needed.</td>
<td>(AT-TLS) policy statements in z/OS Communications Server: IP Reference</td>
</tr>
<tr>
<td></td>
<td>You might have to perform other configuration steps, or you might be</td>
<td></td>
</tr>
<tr>
<td></td>
<td>able to omit steps, depending on whether you are configuring policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clients and servers for the first time or modifying an existing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configuration. See the topics in the Reference column to help determine</td>
<td></td>
</tr>
<tr>
<td></td>
<td>what you need to do.</td>
<td></td>
</tr>
</tbody>
</table>

**Autolog support for AT-TLS dependent applications**

z/OS Communications Server provides the following enhancements to autolog:

- Autolog supports delaying the automatic start of certain procedures that depend on AT-TLS services. In the AUTOLOG profile, you can specify which procedures delay starting until after AT-TLS services are available. This is similar to the existing capability of delaying procedures until dynamic VIPA processing has completed.

  With this support, you can delay the start of a procedure until after AT-TLS services are available, or until dynamic VIPA processing has completed, or both.

- TCP/IP issues a new message, EZZ4250I, when TCP/IP has completed initialization for AT-TLS. You can use this message to trigger automation processes that start applications that rely on TTLS services being active.

**Using the autolog support for AT-TLS dependent applications**

If you want to use this function, perform the appropriate tasks in Table 59 on page 89.
**Table 59. Autolog support for AT-TLS dependent applications**

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay automatically starting a procedure until AT-TLS services are available.</td>
<td>Specify the DELAYSTART parameter with the TTLS subparameter in the AUTOLOG entry for the procedure in the TCPIP profile.</td>
<td>AUTOLOG statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Delay automatically starting a procedure until dynamic VIPA configuration processing has completed.</td>
<td>Specify the DELAYSTART parameter with the DVIPA subparameter in the AUTOLOG entry for the procedure in the TCPIP profile or specify DELAYSTART with no subparameters.</td>
<td>AUTOLOG statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Delay automatically starting a procedure until both AT-TLS services are available and dynamic VIPA configuration processing has completed.</td>
<td>Specify the DELAYSTART parameter with the TTLS and DVIPA subparameters in the AUTOLOG entry for the procedure in the TCPIP profile.</td>
<td>AUTOLOG statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Determine which procedures (automatically started by the Autolog function) that will not be started until one or more services or resources are available.</td>
<td>Invoke the Netstat CONFIG/-f report and view the Autolog information that displays DELAYSTART with its active subparameters for each AUTOLOG entry.</td>
<td>Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
</tbody>
</table>

---

**Business resiliency**

z/OS V1R10 Communications Server improves business resiliency in the following ways:

- “TN3270E Telnet server LU name coordination in a sysplex”
- “Subplex support for Load Balancing Advisor” on page 92

**TN3270E Telnet server LU name coordination in a sysplex**

In z/OS V1R10 Communications Server, the TN3270E Telnet server provides shared LU name management among a group of servers that are running on the same system or in the same Telnet subplex in a sysplex. Before this enhancement, LU names had to be manually partitioned among the TN3270E Telnet servers to prevent the same LU name from being concurrently assigned to clients connected to different servers. With this enhancement, one TN3270E Telnet server in the group acts as an LU name server and allocates shared LU names to other TN3270E Telnet servers in the group. Load balancing across multiple TN3270E Telnet servers that have consistent configurations is possible. The automated takeover and recovery provides improved LU name server availability.

Telnet LU name management can benefit your installation if the following statements are true:

- If you currently run multiple Telnet servers and manually partition LU names between them
- If you want to load balance a Telnet port over several Telnet servers.

**Restrictions for the TN3270E Telnet server LU name coordination in a sysplex**

Shared LU name management services are available only to TN3270E Telnet servers that are running on a single system or in the same Telnet subplex in a sysplex that become members of the Telnet XCF group. You can partition groups of
Telnet servers into separate Telnet subplexes. All of the Telnet servers in a Telnet XCF group must run on VTAMs that are in the same network and must have IP connectivity to each other.

**Dependencies for the TN3270E Telnet server LU name coordination in a sysplex**

Shared LU name management requires XCF local services to create a Telnet XCF group on a single system or in a sysplex.

**Using the TN3270E Telnet server LU name coordination in a sysplex**

If you want to use this function, perform the appropriate tasks in Table 60.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Plan your Telnet subplexing. | Perform the following steps:  
1. If you currently use VTAM or TCP/IP subplexing, consider using the same boundaries for Telnet subplexing as the ones used by VTAM or the TCP/IP subplex.  
2. If you plan to load balance several Telnet ports that each use independent LU name ranges that do not overlap, consider using a Telnet subplex that puts the different name ranges into different Telnet subplexes. | [Shared LU name groups for Telnet servers in z/OS Communications Server: IP Configuration Guide](https://www.ibm.com) |

| Configure an IP address or static VIPA address on the stacks on which a Telnet server with LUNS PRIMARY or LUNS BACKUP will run. If the primary LUNS and backup LUNS use different stacks, VIPARANGE can be used. | Define a primary and backup Telnet LU name server (LUNS) for each Telnet subplex by performing the following steps:  
1. Configure a static VIPA or VIPARANGE address on the stacks on which a Telnet server with LUNS PRIMARY or LUNS BACKUP will run.  
2. Choose a port for the LUNS.  
3. Create two new Telnet configuration files that contain a TELNETGLOBALS block. One file should have an XCFGROUP block with a LUNS PRIMARY statement and the other file should have a LUNS BACKUP statement.  
4. Start the two XCF LUNS Telnet servers. | [Virtual IP Addressing and Customizing the TN3270E Telnet server configuration data sets in z/OS Communications Server: IP Configuration Guide](https://www.ibm.com) |

| Manage LU names that are shared among different Telnet ports on separate Telnet servers. | Perform the following steps:  
1. Add an XCFGROUP statement to the TELNETGLOBALS block in the profile of each Telnet server.  
2. Change existing LUGROUP, PRTGROUP, DEFAULTLUS and DEFAULTPRT blocks to SLUGROUP, SPRTGROUP, SDEFAULTLUS and SDEFAULTPRT blocks to define the shared LU group objects in the profile of each Telnet server. | [Associated printer function in z/OS Communications Server: IP Configuration Guide](https://www.ibm.com) |
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| **Load balance a Telnet port over several Telnet servers.** | Perform the following steps:  
1. Choose a distributed DVIPA address for the Telnet port.  
2. Add an XCFGROUP statement to the TELNETGLOBALS block in a central profile to be shared by the load balanced Telnet servers.  
3. Use SLUGROUP, SPRTGROUP, SDEFAULTLUS and SDEFAULTPRT blocks to define the shared LU group objects in the shared profile.  
4. Configure the DVIPA on the systems on which the Telnet servers will run.  
5. Define Timed Affinity for connections that are distributed to the Telnet ports.  
6. Include the shared definitions in the profile of each participating Telnet server.  
7. Start the XCF Telnet servers. | [Virtual IP Addressing and Customizing the TN3270E Telnet server configuration data sets in z/OS Communications Server: IP Configuration Guide](#) |
| **Display the status of all members of a Telnet XCF group.** | Issue the following command:  
DISPLAY TCP/IP,tnproc,XCF,GROUP  
where *tnproc* is the job name of any Telnet server in the group. | • [Telnet diagnostic tools in z/OS Communications Server: IP Configuration Guide](#)  
• [Operator commands and system administration and DISPLAY TCP/IP,tnproc,XCF<,GROUP> command in z/OS Communications Server: IP System Administrator's Commands](#) |
| **Display information about shared LU name objects in a Telnet XCF group.** | Issue the following command:  
DISPLAY TCP/IP,tnproc,LUNS,OBJECT  
where *tnproc* is the job name of the active Telnet LUNS in the group. | [DISPLAY command: TN3270E Telnet server address space in z/OS Communications Server: IP System Administrator's Commands](#) |
| **Manually direct a standby LUNS to takeover the LU name management function for a Telnet XCF group.** | Issue the following command:  
VARY TCPIP,tnproc,LUNS,START  
where *tnproc* is the job name of the standby Telnet LUNS that you want to take over the group. | • [Managing Telnet in z/OS Communications Server: IP Configuration Guide](#)  
• VARY TCPIP,tnproc,LUNS in z/OS Communications Server: IP System Administrator's Commands](#) |
| **Manually quiesce a standby LUNS to prevent it from being used during a recovery procedure.** | Issue the following command:  
VARY TCPIP,tnproc,LUNS,QUIESCE  
where *tnproc* is the job name of the standby Telnet LUNS that you want to quiesce. | • [Managing Telnet in z/OS Communications Server: IP Configuration Guide](#)  
• VARY TCPIP,tnproc,LUNS in z/OS Communications Server: IP System Administrator's Commands](#) |
Table 60. TN3270E Telnet server LU name coordination in a sysplex (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually resume a quiesced LUNS.</td>
<td>Issue the following command: VARY TCPIP,tnproc,LUNS,RESUME, where tnproc is the job name of the standby Telnet LUNS that you want to resume.</td>
<td>- Managing Telnet in z/OS Communications Server: IP Configuration Guide. VARY TCPIP,tnproc,LUNS in z/OS Communications Server: IP System Administrators Commands.</td>
</tr>
</tbody>
</table>

Subplex support for Load Balancing Advisor

z/OS V1R10 Communications Server enhances the Load Balancing Advisor and Load Balancing Agent function so they can participate in a sysplex subplexing environment. A sysplex subplexing environment is one in which the sysplex is divided into groups (of VTAM instances and TCP/IP stacks) for which communication through dynamic XCF, SameHost, and HiperSockets is allowed between members of a group, but is prevented between members in different groups. You can configure Load Balancing Advisors and Agents for each subplex group in the sysplex.

Using the subplex support for Load Balancing Advisor

If you want to use this function, perform the appropriate tasks in Table 61.

Table 61. Subplex support for Load Balancing Advisor

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan which subplexes you need in your system, and identify the subplexes that require load balancing support through the Load Balancing Advisor and Agents.</td>
<td>Determine which applications in the sysplex require load balancing, and determine the subplexes on which they will reside.</td>
<td>Sysplex subplexing and Steps for configuring the z/OS Load Balancing Advisor with subplexing in z/OS Communications Server: IP Configuration Guide.</td>
</tr>
</tbody>
</table>
| Optionally, configure automatic restart for the Advisor and the Agent. | Configure the Automatic Restart Manager (ARM) or other automation software to restart each Advisor on any z/OS system in the sysplex that supports the subplex that was configured for that Advisor, and to restart the Agent on the same z/OS system on which it was previously running. | - z/OS MVS Setting Up a Sysplex
  - Steps for configuring the z/OS Load Balancing Advisor with subplexing in z/OS Communications Server: IP Configuration Guide. |
| Optionally, configure automatic restart for ADNR. | Configure the Automatic Restart Manager (ARM) or other automation software to restart each ADNR on any z/OS system in the sysplex that supports the subplex with which the ADNR will be associated. Configure the arm_element_suffix statement in each ADNR configuration file so that ADNR registers a unique element name. | - z/OS MVS Setting Up a Sysplex
  - Steps for using the ADNR application in a sysplex subplexing environment in z/OS Communications Server: IP Configuration Guide.
  - Starting the automated domain name registration application (ADNR) in z/OS Communications Server: IP Configuration Reference. |
### Table 61. Subplex support for Load Balancing Advisor (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Configure one Advisor per subplex.                                  | Specify the subplex that the Advisor will be associated with by specifying the sysplex_group_name statement in the configuration file of the Advisor. | • Steps for configuring the z/OS Load Balancing Advisor with subplexing in z/OS Communications Server: IP Configuration Guide  
• Advisor configuration file in z/OS Communications Server: IP Configuration Reference |
| For each z/OS system in the sysplex, configure one Agent per subplex in that z/OS system. | Configure the subplex that the Agent will be associated with by specifying the sysplex_group_name statement in the configuration file of the Agent. | • Steps for configuring the z/OS Load Balancing Advisor with subplexing in z/OS Communications Server: IP Configuration Guide  
• Agent configuration file statements in z/OS Communications Server: IP Configuration Reference |
| Configure the external load balancers.                             | When you are configuring the external load balancers, ensure that all the target applications that are being load balanced for a subplex reside in the same subplex. | Specific load balancer product documentation |
| For each z/OS system, start one Agent for each subplex that will be involved in workload balancing. | Issue the Start command for the Agent procedure. Once the Agent starts, it tries repeatedly to connect to the Advisor for that subplex until the connection is successful (or the agent is stopped). | Starting the z/OS Load Balancing Agent in z/OS Communications Server: IP Configuration Reference |
| Start an Advisor for each subplex in the sysplex that will be involved in workload balancing. | For each subplex, issue the Start command for the Advisor procedure. When the Advisor starts, it listens for a load balancer. If the load balancer is configured correctly, the load balancer connects to the Advisor to get load balancing data from the Advisor. The Advisor also listens and accepts connections from the Agents that support its subplex. | Starting the z/OS Load Balancing Advisor in z/OS Communications Server: IP Configuration Reference |
| Start ADNR instances as appropriate.                                | When DNS is using ADNR for resource registration, ensure that an instance of ADNR is started in each subplex where DNS resources that are registered with ADNR exist. Use a configuration file that specifies the IP address of the LB Advisor for that subplex. | • Steps for using the ADNR application in a sysplex subplexing environment in z/OS Communications Server: IP Configuration Guide  
• Starting the automated domain name registration application (ADNR) in z/OS Communications Server: IP Configuration Reference |
| Start the Load Balancer if it is not already started.              | Ensure there is an external Load Balancer with connectivity to each subplex in the sysplex that has a Load Balancing Advisor that is running. | Specific load balancer product documentation |
Hardware-related enhancements

z/OS V1R10 Communications Server introduces hardware-related enhancements in the following areas:

- "INTERFACE statement support for QDIO"
- "Multiple VLAN support" on page 95
- "HiperSockets multiple write facility" on page 96
- "OSA-Express3 multi-port support for IP" on page 98

INTERFACE statement support for QDIO

In z/OS V1R10 Communications Server, you can use the INTERFACE statement in the TCP/IP profile to configure IPv4 definitions for OSA-Express QDIO rather than using DEVICE/LINK/HOME. This improves stack configuration for IPAQENET interfaces.

Restrictions for INTERFACE statement support for QDIO

This function is limited to OSA-Express Ethernet features in QDIO mode.

Using INTERFACE statement support for QDIO

If you want to use this function, perform the appropriate tasks in Table 62.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Convert IPv4 QDIO definitions to use the INTERFACE statement. | Perform the following steps:  
1. Replace DEVICE and LINK statements for IPAQENET with the new IPv4 INTERFACE statement for IPAQENET.  
2. Remove the HOME entry and any BSDROUTINGPARMS entry for the interface.  
3. If you are currently configuring any static routes over the interface using the GATEWAY statement, convert the GATEWAY statement to a BEGINROUTES block.  
4. If you currently have an IPAQENET6 definition for the same OSA, ensure that the corresponding TRLE definition has enough DATAPATH devices such that one is available for the IPv4 interface and one is available for the IPv6 interface.  
5. If you currently have an IPAQENET6 definition for the same OSA and you currently configure the same virtual MAC address (VMAC) on both the IPAQENET LINK statement and IPAQENET6 INTERFACE statement, change one of the VMACs so that these are unique or change to request OSA-generated VMACs. | • INTERFACE — IPAQENET6 OSA-Express QDIO interfaces and BEGINROUTES statement in z/OS Communications Server: IP Configuration Reference  
• TRLE in z/OS Communications Server: SNA Resource Definition Reference |
| Start or stop an IPv4 QDIO interface that was defined with the INTERFACE statement | Use the interface_name value as the name on the START or STOP statement or on the VARY TCPIP,START or VARY TCPIP,STOP command. | VARY TCPIP,START or VARY TCPIP,STOP in z/OS Communications Server: IP System Administrator’s Commands |
Table 62. INTERFACE statement support for QDIO (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control the OSA ARP processing for VIPAs to limit the processing to VIPAs that are in the same subnet as the OSA.</td>
<td>Specify a subnet mask on the IPADDR parameter on the IPAQENET INTERFACE statement.</td>
<td>INTERFACE — IPAQENET6 OSA-Express QDIO interfaces and BEGINROUTES statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Display information about IPv4 interfaces that are defined with the INTERFACE statement.</td>
<td>Issue the Netstat DEvlens/-d command.</td>
<td>Netstat DEvlens/-d report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Display IPv4 home addresses and determine whether each address is associated with a LINK definition or an INTERFACE definition.</td>
<td>Issue the Netstat HOme/-h command.</td>
<td>Netstat HOme/-h report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Retrieve SNMP MIB object information for IPv4 interfaces that are defined with the INTERFACE statement.</td>
<td>Use the ibmTcpipMvsIfTable interface table (which contains all interfaces) rather than the ibmTcpipMvsLinkTable interface table (which contains only interfaces defined with the LINK statement).</td>
<td>TCP/IP subagent in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
</tbody>
</table>

Multiple VLAN support

With z/OS V1R10 Communications Server, you can configure multiple VLANs from the same TCP/IP stack for a single OSA-Express feature.

Restrictions for multiple VLAN support

The stack supports a maximum of eight VLANs for each OSA for each IP version (IPv4 and IPv6).

An OSA-Express2 on a IBM System z9 Enterprise Class (EC) or z9 Business Class (BC) is limited to supporting 15 concurrently active DATAPATH devices per TRLE. For other limits, see System z10, System z9 and zSeries OSA-Express Customer’s Guide and Reference.

Dependencies for multiple VLAN support

This function is limited to OSA-Express Ethernet features in QDIO mode (CHPID type OSD) that support the Layer 3 Virtual MAC address (VMAC) function. Therefore, you must be running at least an IBM System z9 Enterprise Class (EC) or z9 Business Class (BC) and an OSA-Express or OSA-Express2. See the 2094DEVICE Preventive Service Planning (PSP) and the 2096DEVICE Preventive Service Planning (PSP) buckets for further information.

Using multiple VLAN support

If you want to use this function, perform the appropriate tasks in Table 63.

Table 63. Multiple VLAN support

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine the microcode level of the OSA-Express feature.</td>
<td>Issue the DISPLAY NET;TRL,TRLE= command. Ensure that the microcode level supports virtual MAC (VMAC).</td>
<td>DISPLAY TRL command in z/OS Communications Server: SNA Operation</td>
</tr>
</tbody>
</table>
### Table 63. Multiple VLAN support (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Configure multiple VLANs for an OSA-Express feature. | Perform the following steps:  
1. For IPv4, use the new IPv4 INTERFACE statement for IPAQENET. For IPv6 use the existing IPv6 INTERFACE statement for IPAQENET6. For each interface, specify the VLAN ID using the VLANID parameter. The VLAN IDs must be unique within an IP version.  
2. For each interface, configure (or request OSA to generate) a virtual MAC address using the VMAC parameter and specify (or default to) the ROUTEALL attribute. The VMAC macaddr value, if specified, must be unique.  
3. For each IPv4 interface for this OSA-Express feature, configure a unique subnet using the subnet mask specification on the IPADDR parameter. | INTERFACE — IPAQENET6  
OSA-Express QDIO interfaces in  
/z/OS Communications Server: IP  
Configuration Reference |
| Verify that the TRLE definition for the OSA-Express feature is sufficient for the number of VLANs that you want. | Ensure that the TRLE definition has enough DATAPATH devices such that one will be available for each IPv4 interface and for each IPv6 interface for this OSA-Express. | TRLE in  
z/OS Communications Server: SNA Resource Definition  
Reference |
| Display information about the interfaces for each VLAN for an OSA-Express feature. | Use the Netstat DEvlinks/-d command. | Netstat DEvlinks/-d report in  
z/OS Communications Server: IP  
System Administrator’s Commands |
| Limit a Netstat display to show information only about the interfaces associated with a specific OSA-Express feature. | Specify the OSA-Express port name on the INTFNAME/-K filter of the Netstat DEvlinks/-d or H0me/-h command. | DISPLAY TCPIP,NETSTAT in  
z/OS Communications Server: IP  
System Administrator’s Commands |

### HiperSockets multiple write facility

In z/OS V1R10 Communications Server, a HiperSockets interface can move multiple output data buffers in a single write operation. CPU usage might be reduced and there might be a performance improvement for large outbound messages typically generated by traditional streaming workloads such as file transfer, and interactive web-based services workloads such as Extensible Markup Language (XML) or SOAP.

You can also direct the HiperSockets multiple write support to an IBM System z10 Integrated Information Processor (zIIP). Using a zIIP can lower the computing cost incurred for large outbound messages transported over HiperSockets, while at the same time it can increase the processing capacity of your general purpose central processors (CPs).

### Restrictions for HiperSockets multiple write facility

- HiperSockets multiple write is used only for large outbound messages typically generated by traditional streaming workloads such as file transfer, and interactive web-based services workloads such as XML or SOAP.
The only HiperSockets multiple write traffic that is eligible for processing on an available zIIP is TCP protocol traffic that originates on the TCP/IP stack that is doing the multiple write.

**Incompatibilities for HiperSockets multiple write facility**
You cannot use HiperSockets multiple write if you are running a z/OS system as a guest in a z/VM® environment.

**Dependencies for HiperSockets multiple write facility**
To use the HiperSockets multiple write support, you must be running on an IBM System z10.

**Using HiperSockets multiple write facility**
If you want to use this function, perform the appropriate tasks in Table 64. If you have not configured zIIPs but you want to project eligible zIIP use for current HiperSockets multiple write workload, perform the tasks in Table 65 on page 98.

**Table 64. HiperSockets multiple write facility with zIIPs configured**

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable HiperSockets multiple write.</td>
<td>Add the IQDMULTIWRITE parameter to the GLOBALCONFIG statement.</td>
<td>GLOBALCONFIG in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Optionally, enable zIIP assist for HiperSockets multiple write.</td>
<td>Add the ZIIP IQDIOMULTIWRITE parameter to GLOBALCONFIG statement.</td>
<td>GLOBALCONFIG in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Determine whether HiperSockets multiple write is configured and whether zIIP assist for HiperSockets multiple write is configured.</td>
<td>Review the Netstat CONFIG/-f output.</td>
<td>Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Determine whether a HiperSockets interface is enabled for multiple write and whether zIIP assist for HiperSockets multiple write is enabled.</td>
<td>Review the Netstat DEvlkns/-d output for a HiperSockets interface.</td>
<td>Netstat DEvlkns/-d report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Determine whether HiperSockets multiple write is being used.</td>
<td>Initiate VTAM tuning statistics for the HiperSockets interface. Monitor the IST2242I message for nonzero values.</td>
<td>MODIFY TNSTAT command in z/OS Communications Server: SNA Operation</td>
</tr>
<tr>
<td>Retrieve the SNMP MIB object, ibmMvslIFlag, to determine whether an IPAQIDIO or IPAQIDIO6 interface is enabled for HiperSockets multiple write.</td>
<td>The procedure you use depends on the management application. For the snmp command, no additional action is required. For the NetView SNMP command, use the most current copy of the sample MIBDESC.DATA file in SEZAINST(MIBDESC). Other management applications might require different changes.</td>
<td>TCP/IP subagent in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
</tbody>
</table>
### Table 65. HiperSockets multiple write facility with zIIPs not configured

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gain a basic understanding of zIIP.</td>
<td>Read the referenced documents to learn about zIIP, including how to acquire, define, and activate it, and to learn how to measure its usage.</td>
<td>• Using z/Series Integrated Information Processor (zIIP) in z/OS MVS Planning: Workload Management&lt;br&gt;• Support of IBM System z9 Integrated Information Processors (zIIP) in z/OS RMF Report Analysis&lt;br&gt;• Record Type 30 (1E) – Common Address Space Work in z/OS MVS System Management Facilities (SMF)</td>
</tr>
<tr>
<td>Configure Communications Server to simulate HiperSockets multiple write on a zIIP.</td>
<td>Do the following:&lt;br&gt;• Add the IQDMULTIWRITE parameter to the GLOBALCONFIG statement.&lt;br&gt;• Add the ZIIP IQDIOMULTIWRITE parameter to the GLOBALCONFIG statement.</td>
<td>GLOBALCONFIG in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Enable the MVS PROJECTCPU function.</td>
<td>Specify PROJECTCPU=YES in the SYS1.PARMLIB member IEAOPTxx.</td>
<td>Statements/parameters for IEAOPTxx in z/OS MVS Initialization and Tuning Reference</td>
</tr>
<tr>
<td>Run your HiperSockets multiple write facility workload, then review accounting data for zIIP projection purposes.</td>
<td>Review RMF® or SMF reports for zIIP-eligible work that is run on CPs.</td>
<td>• z/OS RMF Report Analysis&lt;br&gt;• Record Type 30 (1E) – Common Address Space Work and Record Type 30 7x in z/OS MVS System Management Facilities (SMF)</td>
</tr>
</tbody>
</table>

### OSA-Express3 multi-port support for IP

z/OS V1R10 Communications Server introduces support for the OSA-Express3 features that are available with an IBM System z10 EC.

This support includes the following:

- Multiple port support per Channel path ID (CHPID); you can use all the QDIO ports available on an OSA-Express3 CHPID.
- Transparent error handling enhancements, which provide more direct and efficient I/O processing.

An OSA-Express3 is defined in TCP/IP as an OSA-Express device in QDIO mode, exactly as an OSA-Express or OSA-Express2 would be. For OSA-Express3 features that are configured in QDIO mode, see “OSA-Express3 multi-port support for SNA” on page 137 for details on TRLE definition changes.

#### Dependencies for OSA-Express3 multi-port support for IP

OSA-Express3 features are available only with an IBM System z10.

#### Using OSA-Express3 multi-port support

You do not have to perform any steps to use the transparent error handling enhancements on OSA-Express3 features. They are automatically enabled by z/OS Communications Server. If you want to use the multiple port support per CHPID, perform the appropriate tasks in Table 102 on page 137.
Consumability

z/OS Communications Server provides consumability support in the following areas:

- "Configuration Assistant: Import of policy configuration data"
- "Configuration Assistant: IP address groups" on page 100

Configuration Assistant: Import of policy configuration data

In z/OS V1R10 Communications Server, the Policy Agent provides configuration file import services for the IBM Configuration Assistant for z/OS Communications Server. The Configuration Assistant uses the Policy Agent to read and validate one or more configuration files. The Configuration Assistant imports the resulting policies into a new or existing configuration. You can use the imported policies in the Configuration Assistant and you can save the new configuration for the Policy Agent.

This function is supported for the following policy types:

- IP Security (IPSec)
- Application Transparent Transport Layer Security (AT-TLS)
- Intrusion Detection Services (IDS)
- Policy Based Routing (PBR)

Using the Configuration Assistant to import policy configuration data

If you want to use this function, perform the appropriate tasks in Table 66.

Table 66. Configuration Assistant: Import of policy configuration data

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the Policy Agent to perform configuration file import services.</td>
<td>Specify the ServicesConnection statement in the main Policy Agent configuration file.</td>
<td>• Policy-based networking in z/OS Communications Server: IP Configuration Guide</td>
</tr>
<tr>
<td>Enable AT-TLS for secure connections.</td>
<td>If you specify the Security Secure parameter on the ServicesConnection statement, enable AT-TLS processing for the TCP/IP stack by configuring the TTLS parameter on the TCPCONFIG statement in the TCP/IP profile. You specify the affected TCP/IP stack using the ImageName parameter on the ServicesConnection statement. The default is the resolver-supplied TCP/IP user ID or the TCP/IP job name, or INET if the Policy Agent is unable to determine the default TCP/IP stack name.</td>
<td>• Application Transparent Transport Layer Security data protection in z/OS Communications Server: IP Configuration Guide</td>
</tr>
<tr>
<td>Authorize the user IDs that the import requestors use to access the requested policy types.</td>
<td>Issue security product commands to permit the import requestor user IDs to the following SERVAUTH profile: EZB.PAGENT.sysname.image.ptype The image value is the import request name used by the import requestor. For local policies, this name is the TCP/IP stack name specified on the TcpImage statement.</td>
<td>• Policy-based networking in z/OS Communications Server: IP Configuration Guide</td>
</tr>
</tbody>
</table>

Chapter 4. V1R10 new function summary 99
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start the Policy Agent.</td>
<td>Start Policy Agent from a started procedure or from the UNIX shell.</td>
<td>• Starting and stopping the Policy Agent in z/OS Communications Server: IP Configuration Guide</td>
</tr>
<tr>
<td>Import policies into the IBM Configuration Assistant for z/OS</td>
<td>Perform the following steps:</td>
<td>• Policy Agent and policy applications in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Communications Server.</td>
<td>1. Install the V1R10 Configuration Assistant.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Right click on a node in the Navigation Tree and select Import Policy Data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Complete the information in the Import Policy Data panel and select Go.</td>
<td></td>
</tr>
<tr>
<td>Force Policy Agent to listen for services requestor connections.</td>
<td>Issue the MODIFY procname,SRVLSTN command in the following situations:</td>
<td>• ServicesConnection in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td></td>
<td>• If you specified a TCP/IP stack using the ImageName parameter on the ServicesConnection statement, but you did not specify a TcpImage statement for the same TCP/IP stack, and the TCP/IP stack was not active when Policy Agent was started, issue the MODIFY command when the stack becomes active to restart the listen for services requestor connections.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you retrieve AT-TLS policies from a policy server, but the policies cannot be retrieved immediately as a result of a network or policy server problem, issue the MODIFY command to reinstall the AT-TLS policy that was generated. This forces Policy Agent to listen for services requestor connections.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you specify Security Secure on the ServicesConnection statement, the generated AT-TLS policy is installed successfully, and the key ring contents are changed but the key ring name is unchanged, issue the MODIFY command. Policy Agent reinstalls the generated AT-TLS policy so that the updated key ring changes are used.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Assistant: IP address groups**

In z/OS V1R10 Communications Server, you can do the following tasks in regard to IP addressing:

- You can collect IP addresses, subnets, and IP address ranges into named address groups. Previously, you were required to define multiple connectivity rules to secure traffic between distinct endpoints using the same requirements map. You can now create a single connectivity rule to apply a requirements map to a group of endpoints to cover traffic between multiple addresses and ranges. This results in a simpler configuration.

This function is supported for the following policy types:
- IP Security (IPSec) - this support is new in z/OS V1R10 Communications Server
- Application Transparent Transport Layer Security (AT-TLS) - this support is new in z/OS V1R10 Communications Server
- Policy Based Routing (PBR) - this support was introduced in z/OS V1R9 Communications Server
- For IPSec, you can specify IP address groups, subnets, or ranges as security endpoints on IPSec key exchange policies.

**Incompatibilities for Configuration Assistant support for IP address groups**
This function is not available for remote policy clients that are at a lower release level than z/OS V1R10.

**Using the Configuration Assistant: IP address groups**
If you want to use this function, perform the appropriate tasks in Table 67.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Using the Configuration Assistant, add address groups to the IPSecurity or AT-TLS configuration. | Perform the following steps: 1. Install the V1R10 Configuration Assistant. 2. Select the IPSec or AT-TLS perspective. Select reusable objects of type address group. 3. Add new address groups and reference them in the connectivity rules. | Bring up the Configuration Assistant Help System. Use the Search facility to find help references to “Address Groups”.
|
| If you are not using the Configuration Assistant, use address groups for IPSec key exchange policies. | Specify the LocationGroupRef parameter on the LocalSecurityEndpoint or RemoteSecurityEndpoint statements. | LocalSecurityEndpoint and RemoteSecurityEndpoint statements in z/OS Communications Server: IP Configuration Reference
|
| If you are not using the Configuration Assistant, use local security endpoint address ranges for IPSec key exchange policies. | Specify the LocationSetRef parameter on the LocalSecurityEndpoint statement. | LocalSecurityEndpoint statement in z/OS Communications Server: IP Configuration Reference
|

**Middleware enablement**

z/OS Communications Server provides middleware enablement in the following areas:
- “Network management interface enhancements”
- “FRCA cache enhancements for WebSphere Application Server” on page 103
- “SNMP enhancements” on page 104
- “Socket API timeout support” on page 105
- “Optimize asynchronous socket receive use of 64-bit shared memory” on page 107

**Network management interface enhancements**
z/OS V1R10 Communications Server enhances the network management interface (NMI) in the following areas:
- “NMI: IP security enhancements” on page 102
- “NMI: Timestamps collection” on page 102
FTP application data is available to NMI application programs through the EZBNMIFR programming interface. See “FTP application data enhancements” on page 120 for more information.

NMI: IP security enhancements

z/OS V1R10 Communications Server provides new SMF119 records for IP security. These records are written to the traditional MVS SMF exit routines, and also to the NMI real-time SMF interface, SYSTCPSM. These new records provide information about the following types of events related to IP security:

- IKE tunnel activation, deactivation, expiration, and refresh
- IPSec dynamic tunnel activation, deactivation, and refresh
- TCP/IP stack addition and removal of IPSec dynamic tunnels
- TCP/IP stack activation and deactivation of IPSec manual tunnels

The existing SMF119 record subtype 8 (TCP/IP Stack Start/Stop) is enhanced to indicate whether IPSecurity is enabled. These enhancements, along with the IP security polling NMI, help you better manage IP security resources.

Using the NMI: IP security enhancements: If you want to use this function, perform the appropriate tasks in Table 68.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure IKE to write the new SMF records (subtypes 73 - 76) to the traditional MVS SMF exit interface.</td>
<td>Add the new SMF119 parameter to the IKE Daemon configuration file.</td>
<td>IKE Daemon in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Configure the TCP/IP stack to write the new IP security SMF records (subtypes 77 - 80) to the traditional MVS SMF exit interface.</td>
<td>Alter the SMFCONFIG and IPSECURITY PROFILE.TCPIP configuration statements.</td>
<td>TCP/IP profile (PROFILE.TCPIP) and configuration statements in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Cause IP security SMF events to be written to the real-time NMI for SMF recording (SYSTCPSM). Records are generated by the IKE daemon and the TCP/IP stack and are written to the NMI.</td>
<td>Configure the following statements in the PROFILE.TCPIP configuration statement: • NETMONITOR • SMFSERVICE • IPSECURITY</td>
<td>TCP/IP profile (PROFILE.TCPIP) and configuration statements in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Use new SMF records.</td>
<td>Develop or alter a C, C++, or Assembler application to gather and format SMF records using the data mappings provided.</td>
<td>• SMF type 119 records in z/OS Communications Server: IP Configuration Reference • Local IPSec NMI in z/OS Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
<tr>
<td>Display the IP security SMF parameters.</td>
<td>Issue the Netstat -f or NETSTAT CONFIG command.</td>
<td>Netstat in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
</tbody>
</table>

NMI: Timestamps collection

z/OS V1R10 Communications Server enhances the EZBNMIFR NMI so that it collects timestamps for messages that are in queues.

For TCP connections that have data on the receive queue, NMI collects timestamps of the date and time of the oldest message on the receive queue; for TCP
connections that have data on the send queue, NMI collects timestamps of the date and time of the oldest message on the send queue.

For UDP connections that have a socket with data on the receive queue, NMI collects timestamps of the date and time of the oldest message on the receive queue.

When an application is not functioning correctly, data can accumulate on the send or receive queues for its connections, which can adversely affect storage. This enhancement helps in diagnosing these problems.

**Using the NMI: Timestamps collection enhancement:** If you want to use this function, perform the appropriate tasks in Table 69.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieve timestamp information about data on the UDP receive queue and the TCP send and receive queues.</td>
<td>Issue one of the following NMI calls:</td>
<td>TCP/IP callable NMI</td>
</tr>
<tr>
<td></td>
<td>• GetUDPTable call for UDP sockets</td>
<td>[EZBNMIFR] Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
<tr>
<td></td>
<td>• GetConnectionDetail call for TCP connections</td>
<td></td>
</tr>
</tbody>
</table>

**FRCA cache enhancements for WebSphere Application Server**

In z/OS V1R10 Communications Server, the Fast Response Cache Accelerator (FRCA) function for high-speed web serving is enhanced to support a shared cache. This enhancement can improve performance for the WebSphere Application Server for z/OS, while limiting the amount of memory required to cache objects in TCP/IP. The FRCA function is extended so that Web traffic can be carried on an IPv6 network (FRCA in previous releases was limited to IPv4 traffic).

**Dependencies for the FRCA cache enhancements for WebSphere Application Server**

The FRCA function is transparently enabled by a signal from WebSphere for z/OS; TCP/IP configuration statements are not required to enable this support. See the WebSphere Application Server Information Center for information about configuring the FRCA support within WebSphere. A link to this Information Center is available at WebSphere Application Server Information Center.

**Using the FRCA cache enhancements for WebSphere Application Server**

If you want to use this function, perform the appropriate tasks in Table 70.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consider whether to control access to the FRCA function.</td>
<td>Read the referenced topic to determine whether you want to control the access to the function.</td>
<td>Considerations for Fast Response Cache Accelerator in z/OS Configuration Guide</td>
</tr>
<tr>
<td>View the WebSphere Application Server to determine the z/OS usage of the FRCA shared cache.</td>
<td>Invoke the Netstat CACHINFO/-C report option.</td>
<td>Netstat CACHINFO/-C report in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
</tbody>
</table>
SNMP enhancements

z/OS V1R0 provides the following enhancements to the Communications Server SNMP support:

- The SNMP support for IPv6 management data is upgraded from the IETF internet draft version of the MIB modules to the RFC version. In z/OS V1R5 and V1R6, SNMP support was added for version-neutral (IPv4 and IPv6) SNMP management data defined in IETF internet drafts. These internet drafts were shipped with Communications Server and installed in the /usr/lpp/tcpip/samples file system directory, with the following file names:
  - iaddrmib.mi2 INET-ADDRESS-MIB
  - ipfwdmib.mi2 IP-FORWARD-MIB
  - ipmib.mi2 IP-MIB
  - tcpmib.mi2 TCP-MIB
  - udpmib.mi2 UDP-MIB
These internet drafts are now RFCs, so the SNMP support is upgraded to the RFC version of the MIB modules. The internet draft versions of the MIB modules are not included with Communications Server anymore. The following list includes the supported RFCs:
  - RFC 4001 INET-ADDRESS-MIB
  - RFC 4292 IP-FORWARD-MIB
  - RFC 4293 IP-MIB
  - RFC 4022 TCP-MIB
  - RFC 4113 UDP-MIB
Of these MIB modules, only the RFC version of the IP-MIB defines changes to management data that was previously supported in the internet draft.

- Interface state change notification changes
  - New `ibmMvsTcpipIntfUp` and `ibmMvsTcpipIntfDown` notifications are now provided in the IBM MVS TCP/IP Enterprise-specific MIB to identify the name of the interface in the notification. Like the standard linkUp and linkDown notifications from the IF-MIB, these notifications indicate that the state of an interface is changing. These new notifications are sent in addition to the standard linkUp and linkDown notifications.
  - Support for linkUp and linkDown notifications for VIPA interfaces is removed.
  VIPA interfaces, both static and dynamic, do not change their operational state. If the interfaces are successfully defined, then they are always active. You cannot stop the interfaces by using the VARY TCPIP,STOP command, and a linkDown notification is not currently created when they are deleted. For these reasons, the support for linkUp and linkDown notifications is removed for VIPA interfaces.

- Agent z/OS UNIX connection changes
  - A new SNMP Agent parameter, `-C`, controls z/OS UNIX connections from an SNMP subagent to the Agent.
    For subagents that are not defined as z/OS UNIX superusers, this new parameter enables you to set the appropriate file access permission bits for the z/OS UNIX file used for subagent connections to the Agent.
  - A default z/OS UNIX file is created in the /var z/OS UNIX file system directory.
    Currently, the default file created by the SNMP Agent, to be used for subagent z/OS UNIX connections, is /tmp/dpi_socket. This can cause
problems if you periodically delete the files in the /tmp directory to ensure
that there is enough free space for the system. The more appropriate directory
for this type of file is the /var directory, so the Agent now creates file
/var/dpi_socket as the default file.

**Using the SNMP enhancements**

If you want to use this function, perform the appropriate tasks in Table 71.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Retrieve changed SNMP management data defined in IETF RFC MIB modules. | Perform the following steps:
  - Modify the network management applications that use the changed IP-MIB MIB objects so that the applications continue to access the same data.
  - If you have network management applications that are using shipped internet draft sample files for the MIB modules, replace the sample files with the RFC version of the MIB modules. | Copies of the IETF RFCs, are available at: http://www.rfc-editor.org/rfc.html |
| Use the new ibmMvsTcpipIntfUp and ibmMvsTcpipIntfDown notifications. | Update your network management application to recognize the new notifications. | See the definition of these notifications in the IBM MVS TCP/IP Enterprise-specific MIB module shipped as z/OS UNIX file /usr/lpp/tcpip/samples/mvstcpip.mi2. |
| Adjust to the removal of linkUp and linkDown notifications for VIPA interfaces. | Update your network management application if it contains VIPA-specific support for these notifications. For dynamic VIPA interfaces, change your network management application to use the proprietary dynamic VIPA notifications in the IBM MVS TCP/IP Enterprise-specific MIB module. | • See SNMP Enterprise-specific trap types in System Administrator's Commands for a description of the dynamic VIPA notifications
  • See the definition of the dynamic VIPA notifications in the IBM MVS TCP/IP Enterprise-specific MIB module shipped as z/OS UNIX file /usr/lpp/tcpip/samples/mvstcpip.mi2. |
| Control z/OS UNIX Agent connections for subagents that are not superusers. | Use the -C Agent parameter to set the file access permissions for the z/OS UNIX file. | OSNMPD parameters in z/OS Communications Server: IP Configuration Reference |
| Ensure that the default z/OS UNIX file for the Agent is created in the /var file system directory. | If you are permitting the Agent to create its z/OS UNIX connection file in the default /tmp directory, and you have copied the OSNMPD.DATA sample file to /etc/osnmpd.data, refresh it from the updated sample in /usr/lpp/tcpip/samples/osnmpd.data. The value for the dpiPathNameForUnixStream MIB object in this sample has been changed to /var/dpi_socket. | OSNMPD.DATA example in z/OS Communications Server: IP Configuration Reference |

**Socket API timeout support**

Applications can use two new socket API options to indicate the amount of time that receive-type and send-type socket API calls wait for their operations to complete. Applications can prevent indefinite blocking inside TCP/IP for these types of socket API calls. After these options are set on a specific socket, TCP/IP
monitors receive-type and send-type API calls on the socket and times out any requests that have exceeded this time interval without completing.

**Tip:** These new socket options apply to both synchronous and asynchronous receive- and send-type socket APIs.

Prior to z/OS V1R10 Communications Server, several mechanisms for implementing timeout of receive and send type of socket API calls were available and they continue to be supported with no impact to existing applications that use them.

**Restrictions for the socket API timeout support**
The new socket API options are not available for the TCP/IP C Socket application programming interface and the Pascal application programming interface.

**Using the socket API timeout support**
If you want to use this function, perform the appropriate tasks in Table 72.

**Table 72. Socket API timeout support**

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Enable a timeout on the receive- and the send-type socket API call. | Issue the setsockopt() call with a nonzero timeout value for the following socket options:  
- SO_RCVTIMEO  
- SO_SNDTIMEO | - getsockopt(), setsockopt() in z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference  
- getsockopt(), setsockopt() calls in z/OS Communications Server: IP CICS Sockets Guide  
- GETSOCKOPT and SETSOCKOPT in z/OS Communications Server: IP IMS Sockets Guide  
- getsockopt(), setsockopt() in z/OS XL C/C++ Run-Time Library Reference  
- getsockopt(), setsockopt(), and BPXYSOCK in z/OS UNIX System Services Programming: Assembler Callable Services Reference |
| Remove a previously set timeout value on the receive- and the send-type socket API call. | Issue the setsockopt() call with the timeout value 0 for the following socket options:  
- SO_RCVTIMEO  
- SO_SNDTIMEO | - getsockopt(), setsockopt() in z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference  
- getsockopt(), setsockopt() calls in z/OS Communications Server: IP CICS Sockets Guide  
- GETSOCKOPT and SETSOCKOPT in z/OS Communications Server: IP IMS Sockets Guide  
- getsockopt(), setsockopt() in z/OS XL C/C++ Run-Time Library Reference  
- getsockopt(), setsockopt(), and BPXYSOCK in z/OS UNIX System Services Programming: Assembler Callable Services Reference |
Optimize asynchronous socket receive use of 64-bit shared memory

In z/OS V1R10 Communications Server, applications using the optimized Asynchronous Socket I/O option of z/OS UNIX System Services (designated by the AioCommBuff bit in the AIOCB) can use 64-bit shared memory objects. Previously, use of the optimized receive processing designated by the AioCommBuff bit was restricted to 31-bit Common Storage Area (CSA) or Common Data Space storage.

With this enhancement, applications are no longer constrained by 31-bit addressability because they can use buffers residing in 64-bit shared memory objects on the BPX4AIO callable service for receive processing, but still retain the performance benefits that the AioCommBuff option provides. The application allocates a shared memory object and issues a new IOCTL SIOCSMOCTL that allows TCP/IP to establish access to the memory object or remove access to the memory object.

Restrictions when using the optimized asynchronous socket I/O option

Socket applications that use the SIOCSMOCTL IOCTL must be authorized (the socket applications must be running in supervisor state or in system key, or they must be APF authorized).

Using the optimized asynchronous socket I/O option

If you want to use this function, perform the task in Table 73.

Table 73. Optimize asynchronous socket receive use of 64-bit shared memory

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use buffers in shared memory objects for asynchronous socket I/O.</td>
<td>Change 64-bit applications to allocate socket I/O buffers in shared memory objects and to issue the SIOCSMOCTL IOCTL to establish and remove access from TCP/IP to those objects.</td>
<td>SIOCSMOCTL IOCTL in z/OS Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
</tbody>
</table>
RAS and customer satisfaction

z/OS V1R10 Communications Server provides reliability, availability, serviceability (RAS) and other customer enhancements in the following areas:

- “Path MTU discovery for Enterprise Extender for IP”
- “IBM Health Checker for z/OS enhancements” on page 109
- “Netstat enhancements” on page 110
- “OMPROUTE enhancements” on page 111
- “Diagnostic enhancements for TCP/IP host name configuration problems” on page 113
- “IPCS formatter enhancements” on page 113
- “Data trace enhancements” on page 114
- “Packet trace enhancements” on page 115
- “TCP/IP SMF record enhancements” on page 116
- “Allow DNS BIND 9 server to run with BPX.SUPERUSER authorization” on page 117
- “ASID reuse for TCP/IP, TN3270E, and resolver” on page 118
- “Resolver support for EDNS0” on page 120
- “FTP enhancements” on page 120

Path MTU discovery for Enterprise Extender for IP

In z/OS V1R10 Communications Server, path MTU discovery for Enterprise Extender (EE) enables VTAM to dynamically determine any MTU size changes that are associated with IPv4 and IPv6 EE connections in the IP network. VTAM can segment the HPR data to avoid IP packet fragmentation.

See “Path MTU discovery for Enterprise Extender for SNA” on page 128 for the SNA considerations for this function.

Dependencies for path MTU discovery for Enterprise Extender for IP

Path MTU discovery uses ICMP fragmentation-needed errors to detect the PMTU for a path. You must permit ICMP errors to flow at all hosts along the path of a connection. Path MTU discovery does not function if a firewall blocks ICMP errors.

Using path MTU discovery for Enterprise Extender for IP

If you want to use this function, perform the appropriate tasks in Table 74 on page 109.
### Table 74. Path MTU discovery for Enterprise Extender for IP

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable path MTU discovery support for IPv4 EE connections.</strong></td>
<td>Specify the PATHMTUDISCOVERY keyword on the IPCONFIG profile statement for the EE-enabled TCP/IP stack.</td>
<td>• PATHMTUDISCOVERY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PMTUD start option in z/OS Communications Server: SNA Resource Definition Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• START command and MODIFY VTAMOPTS command in z/OS Communications Server: SNA Operation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| **Allow path MTU discovery support in the EE-enabled TCP/IP stack, but disable path MTU discovery support for both IPv4 and IPv6 EE connections.** | Do the following:  
• Specify the PATHMTUDISCOVERY keyword on the IPCONFIG profile statement for the EE-enabled TCP/IP stack.  
• Specify PMTUD=NO in the appropriate ATCSTRxx VTAM start list or on the VTAM START command. Optionally, when VTAM is active, issue the MODIFY procname,VTAMOPTS, PMTUD=NO command. | • PATHMTUDISCOVERY | NOPATHMTUDISCOVERY parameters in the IPCONFIG statement in z/OS Communications Server: IP Configuration Reference. |
| | | • PMTUD start option in z/OS Communications Server: SNA Resource Definition Reference. |
| | | • START command and MODIFY VTAMOPTS command in z/OS Communications Server: SNA Operation. |

---

**IBM Health Checker for z/OS enhancements**

IBM Health Checker for z/OS is a z/OS component that installations can use to gather information about their system environment and system parameters to help identify potential configuration problems before they impact availability or cause outages. Individual products, z/OS components, or Independent Software Vendor (ISV) software can provide checks that take advantage of the IBM Health Checker for z/OS framework.

In a future release of z/OS, support for several functions is planned to be discontinued. z/OS V1R10 Communications Server provides four new IBM Health Checker for z/OS checks to help you determine whether selected Communications Server functions are active on your current systems:

• Boot Information Negotiation Layer (BINL) server  
• Berkeley Internet Name Domain 4.9.3 (BIND 4.9.3) DNS server  
• Dynamic Host Configuration Protocol (DHCP) server  
• Network Database (NDB) server

If you are using these functions, you are encouraged to migrate by finding replacement or alternative processes.

See [z/OS Migration](z/OS Migration) for detailed information about these functions, including the steps you should take to migrate to using replacement functions.
In addition to the four migration checks, z/OS V1R10 Communications Server provides a new IBM Health Checker for z/OS check in a Common INET (CINET) environment. The new check determines whether the port range specified by the INADDRANYPORT and INADDRANYCOUNT parameters in the BPXPRMxx parmlib member are reserved for OMVS on the TCP/IP stack. You can reserve a port range on a TCP/IP stack using the PORTRANGE TCP/IP profile statement. Reserving a port range prevents the stack from allocating a port that can later be allocated by CINET.

**Dependencies for the IBM Health Checker for z/OS enhancements**

You must start the IBM Health Checker for z/OS before you can use the IBM Health Checker for z/OS enhancements.

### Using the IBM Health Checker for z/OS enhancements

If you want to use these enhancements, perform the appropriate tasks in Table 75.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Use the IBM Health Checker for z/OS migration check support. | Perform the following steps:  
1. Configure and start the IBM Health Checker for z/OS.  
2. Review check output for potential migration actions. | See the following topics in IBM Health Checker for z/OS: User's Guide:  
• Setting up IBM Health Checker for z/OS  
• Working with check output  
• Managing checks |

| Use the IBM Health Checker for z/OS recommendations to improve your system configuration. | Perform the following steps:  
1. Configure and start IBM Health Checker for z/OS.  
2. Review check output for potential configuration problems before they impact availability or cause outages.  
3. Consider modifications to your configuration based on the recommendations included in check output. | See the following topics in IBM Health Checker for z/OS: User's Guide:  
• Setting up IBM Health Checker for z/OS  
• Working with check output  
• Managing checks |

### Netstat enhancements

z/OS V1R10 Communications Server provides the following enhancements to the DISPLAY TCPIP,,NETSTAT command:

- **Support for the Netstat ALL/-A report option**
  
The report provided by the Netstat ALL/-A option is now available when using the DISPLAY TCPIP,,NETSTAT command, in addition to being available using the TSO or z/OS UNIX shell environment.

- **Introduction of a configurable value for the command's MAX parameter**
  
  A new parameter, MAXRECS, is available on the GLOBALCONFIG TCP/IP profile statement for configuring a default value for the DISPLAY TCPIP,,NETSTAT command's MAX parameter.

- **Report truncation when the maximum output is displayed**
  
The DISPLAY TCPIP,,NETSTAT command can display a maximum of 65 533 output lines. If more information needs to be displayed, the command stops and displays a final output line, indicating that the report was truncated.
Using the Netstat enhancements

If you want to use the Netstat enhancements, perform the appropriate tasks in Table 76.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the Netstat ALL/-A report output.</td>
<td>Invoke the DISPLAY TCPIP,,NETSTAT,ALL command.</td>
<td>DISPLAY TCPIP,,NETSTAT in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
<tr>
<td>Configure a default value for the MAX parameter on the DISPLAY TCPIP,,NETSTAT command.</td>
<td>Specify the MAXRECS parameter on the GLOBALCONFIG TCP/IP profile statement.</td>
<td>GLOBALCONFIG in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Update your automation programs to detect truncated output from the DISPLAY TCPIP,,NETSTAT.</td>
<td>Change the programs to check for the new output line, REPORT TRUNCATED DUE TO GREATER THAN 65533 LINES OF OUTPUT.</td>
<td>DISPLAY TCPIP,,NETSTAT in z/OS Communications Server: IP System Administrator’s Commands</td>
</tr>
</tbody>
</table>

OMPROUTE enhancements

z/OS V1R10 Communications Server enhances OMPROUTE in the following ways:

- INCLUDE statements are processed in the OMPROUTE configuration file. You can group OMPROUTE configuration statements that can be common to several OMPROUTE instances into a single file and include that file in the configuration for each of those instances. You do not need to repeat the configuration information in multiple places.

- OMPROUTE detects and avoids futile neighbor state loops with designated routers that are not responding based on interfaces used to reach those routers. This improves performance and availability for IPv4 and IPv6 OSPF environments that involve configurations of primary and backup parallel interfaces that are attached to the same LAN segment. OMPROUTE console commands are provided to enable you to manually control interface reaction to futile neighbor state loops.

  For information about futile neighbor state loops, see Preventing futile neighbor state loops during adjacency formation in z/OS Communications Server: IP Configuration Guide.

Restrictions for OMPROUTE enhancements

The following restrictions apply:

- The futile neighbor state loop detection is restricted to multi-access broadcast interfaces (for example, IPAQNET, IPAQNET6, IPAQTR, IPAQIDIO, IPAQIDIO6, and LCS for ethernet LANs).

- The interface activation and suspension procedure in OMPROUTE requires that the corresponding physical interface in the TCP/IP stack be active.

  Result: Because the procedure results in OSPF interface changes, OSPF routes are recalculated and the connections using these routes might be disrupted.

Using the OMPROUTE enhancements

If you want to use this function, perform the appropriate tasks in Table 77 on page 112.
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the support for the INCLUDE statements in the OMPROUTE configuration file.</td>
<td>Group related OMPROUTE configuration statements into separate files and use the INCLUDE statement to include the statements in your OMPROUTE configuration files.</td>
<td><em>Steps for configuring OMPROUTE in z/OS Communications Server: IP Configuration Guide</em>&lt;br&gt;<em>INCLUDE statement in z/OS Communications Server: IP Configuration Reference</em></td>
</tr>
<tr>
<td>Report and control futile neighbor state loops.</td>
<td>Specify the DR_Max_Adj_Attempt parameter on the OSPF or IPv6_OSPF statement in the OMPROUTE configuration file.</td>
<td><em>Preventing futile neighbor state loops during adjacency formation in z/OS Communications Server: IP Configuration Reference</em></td>
</tr>
<tr>
<td>Display the threshold value for the futile neighbor state loop.</td>
<td>Use one or both of the following commands:&lt;br&gt;• DISPLAY TCPIP,OMPROUTE,OSPF, LIST,ALL&lt;br&gt;• DISPLAY TCPIP,OMPROUTE,IPV6OSPF, ALL</td>
<td><em>DISPLAY TCPIP,OMPROUTE in z/OS Communications Server: IP System Administrator's Commands</em></td>
</tr>
<tr>
<td>Display the interface state to determine whether the interface is suspended after detection of a futile neighbor state loop and to identify the alternate redundant interface that will be used for an adjacency attempt with the same neighbor.</td>
<td>Issue one or both of the following commands:&lt;br&gt;• DISPLAY TCPIP,OMPROUTE,OSPF,INTERFACE&lt;br&gt;• DISPLAY TCPIP,OMPROUTE,IPV6OSPF,INTERFACE</td>
<td><em>DISPLAY TCPIP,OMPROUTE in z/OS Communications Server: IP System Administrator's Commands</em></td>
</tr>
<tr>
<td>Display the number of times that the maximum threshold of adjacency attempts for futile neighbor state loop detection has been reset for a neighbor over this interface.</td>
<td>Issue one or more of the following commands:&lt;br&gt;• DISPLAY TCPIP,OMPROUTE,OSPF,INTERFACE,NAME= if_name&lt;br&gt;• DISPLAY TCPIP,OMPROUTE,IPV6OSPF,INTERFACE, NAME= if_name&lt;br&gt;• DISPLAY TCPIP,OMPROUTE,IPV6OSPF,INTERFACE,ID= if-id</td>
<td><em>DISPLAY TCPIP,OMPROUTE in z/OS Communications Server: IP System Administrator's Commands</em></td>
</tr>
<tr>
<td>Modify the OSPF interface state from suspend to active to permit adjacency formation attempts with neighboring designated routers over this interface.</td>
<td>Issue one or more of the following commands:&lt;br&gt;• MODIFY OMPROUTE,OSPF,INTERFACE,NAME=if_name,ACTIVATE&lt;br&gt;• MODIFY OMPROUTE,IPV6OSPF,INTERFACE,NAME= if_name, ACTIVATE&lt;br&gt;• MODIFY OMPROUTE,IPV6OSPF,INTERFACE,ID= if-id, ACTIVATE</td>
<td><em>MODIFY command: OMPROUTE in z/OS Communications Server: IP System Administrator's Commands</em></td>
</tr>
</tbody>
</table>
Table 77. OMPROUTE enhancements (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Modify the OSPF interface state from active to suspend to force destroying adjacencies with neighboring designated routers over this interface and to permit adjacency formations over an alternate redundant interface when available. | Issue one or more of the following commands:  
  - MODIFY OMPROUTE,OSPF,INTERFACE,NAME=if_name,SUSPEND  
  - MODIFY OMPROUTE,IPV6OSPF,INTERFACE,NAME=if_name,SUSPEND  
  - MODIFY OMPROUTE,IPV6OSPF,INTERFACE,ID=if-id,SUSPEND | MODIFY command: OMPROUTE in z/OS Communications Server: IP System Administrator's Commands |

Diagnostic enhancements for TCP/IP host name configuration problems

z/OS V1R10 Communications Server introduces a new message, EZZ0162I, that is issued when TCP/IP is started. The message contains the host name of the associated stack. The host name is returned by the stack when it processes a gethostname API call.

Using the TCP/IP host name configuration diagnostic enhancement

If you want to use this function, perform the task in Table 78.

Table 78. Diagnostic enhancements for TCP/IP host name configuration problems

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check that EZZ0162I has the expected host name.</td>
<td>Check the TCP/IP job log or system log for this message.</td>
<td>z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)</td>
</tr>
</tbody>
</table>

IPCS formatter enhancements

z/OS V1R10 Communications Server introduces a serviceability enhancement to the TCP/IP dump formatter, TCPIPCS, so that you can format the following:

- The functions that recently accessed the Transmission Control Protocol control blocks (TCBs), Telnet Server Client Connection Block (CVBs), and Connection Routing Hash Table Entries (CRHTEs); these are also known as in-flight recorders
- TCP/IP storage headers for a storage element, including the storage key, subpool, module name, and timestamp
- Summaries of the amount of data queued for a connection
- A listing of outstanding events for TCP, UDP, and RAW connections
- A report of all inbound and outbound TCP and socket send and receive activity on a per session basis. You can use a new formatting option, SESSION, that interprets TCPMIN and PFSMIN trace entries and produces a report of inbound and outbound TCP traffic activity. The report that is produced using this option might be especially useful (as compared to packet trace) in IPSec environments because this formatting option has access to unencrypted TCP headers.

Restrictions for the IPCS formatter enhancements

The SESSION formatting option is applicable for TCP traffic only.
Dependencies for the IPCS formatter enhancements
Because the SESSION report operates on TCPMIN and PFSMIN CTRACE options, those two options must be enabled in CTRACE in order to produce a meaningful report.

Using the IPCS formatter enhancements
If you want to use this function, perform the tasks in Table 79.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format TCP/IP storage headers.</td>
<td>Issue the TCPIPCS STORAGE subcommand. This subcommand accepts the address of a storage element as input and formats the appropriate TCP/IP storage headers for that storage element.</td>
<td>TCPIPCS command in z/OS Communications Server: IP Diagnosis Guide</td>
</tr>
<tr>
<td>Format waiting events.</td>
<td>Issue a TCPIPCS TCB, UDP, or RAW subcommand with the DETAIL option to format the EVENT control blocks.</td>
<td>TCPIPCS command in z/OS Communications Server: IP Diagnosis Guide</td>
</tr>
<tr>
<td>Format the in-flight recorder information, when available, for the control blocks TCB, CVB, and CRHTE. The in-flight recorder reports recent functions that refer to these control blocks.</td>
<td>Use the TCPIPCS subcommands TCB, TELNET, or XCF with the DETAIL option to format the in-flight recorder information that is in the TCB, CVB, and CRHTE control blocks.</td>
<td>TCPIPCS command in z/OS Communications Server: IP Diagnosis Guide</td>
</tr>
<tr>
<td>List connection control blocks that have data queued to the SEND queue, the RECEIVE queue, or both.</td>
<td>Issue the DATAQ parameter on the TCPIPCS TCB, UDP, or RAW subcommand to format only connection control blocks that have data queued to the SEND queue, the RECEIVE queue, or both.</td>
<td>TCPIPCS command in z/OS Communications Server: IP Diagnosis Guide</td>
</tr>
<tr>
<td>Enable TCPMIN and PFSMIN CTRACE options (in preparation for generating a session report for all inbound and outbound TCP and socket send and receive activity).</td>
<td>Issue the TRACE CT command.</td>
<td>Specifying trace options after initialization in z/OS Communications Server: IP Diagnosis Guide</td>
</tr>
</tbody>
</table>

Data trace enhancements
z/OS V1R10 Communications Server enhances socket data tracing (DATTRACE) to allow filtering by port number. A new PORTNUM parameter is supported on the VARY TCPIP,DATTRACE command that you can use to trace only packets that have a source or destination port that matches a specific port number.

Previously, the data trace did not capture or display information about the protocol, domain, or driver type of the traffic. In z/OS V1R10 Communications Server, the data trace is enhanced to capture this data, and the IPCS CTRACE command is enhanced to format it.

Using the data trace enhancements
If you want to use this function, perform the appropriate tasks in Table 80 on page 115.
Table 80. Data trace enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable PORTNUM filtering.</td>
<td>Specify the PORTNUM parameter on the VARY TCP,DATTRACE command.</td>
<td>• VARY TCP, DATTRACE in <a href="#">z/OS Communications Server: IP System Administrator's Commands</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VARY TCPIP DATTRACE in <a href="#">z/OS Communications Server: Quick Reference</a></td>
</tr>
<tr>
<td>Display data trace PORTNUM settings.</td>
<td>Issue the Netstat CONFIG/-f command to display the socket data trace PORTNUM settings.</td>
<td>• Displaying data traces in <a href="#">z/OS Communications Server: IP Diagnosis Guide</a></td>
</tr>
<tr>
<td>Format driver, domain, and protocol information from a data trace.</td>
<td>Perform the following steps: 1. Issue the IPCS CTRACE command to format the data trace records. 2. Configure the EZBCAPI network management interface to format the data trace records.</td>
<td>• Format Component Trace Entries in <a href="#">z/OS MVS IPCS Commands</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Processing the CTE records for SYSTCPDA and Packet and data trace formatting NMI in <a href="#">z/OS Communications Server: IP Programmer's Guide and Reference</a></td>
</tr>
</tbody>
</table>

Packet trace enhancements

z/OS V1R10 Communications Server enhances packet tracing in the following ways:
- The packet trace function of the TCP/IP stack can record inbound packets that are discarded by the stack. You can filter packet trace collection and formatting by using discard reason codes. The TCP/IP intrusion detection services trace can also capture and format discarded packets, and can filter by discard reason code.
- You can format SNA packets received through any of the TCP/IP services traces. You can format any SNA traffic collected by the OSA-Express Network Traffic Analyzer, packet trace, data trace, or Intrusion Detection Services trace.

Restrictions for packet trace enhancements

SNA data tracing is limited to the following data:
- Enterprise Extender data
- Data to and from Communication Controller for Linux (CCL) on System z through an OSA-Express adapter configured in QDIO Layer 2 mode

Dependencies for packet trace enhancements

To collect CCL data, you must enable the OSA-Express Network Traffic Analyzer (OSAENTA). OSAENTA requires at least an IBM System z9 and OSA-Express2 in QDIO mode (CHPID type OSD). See the OSA-Express2 Preventive Service Planning (PSP) bucket for further information.

Using the packet trace enhancements

If you want to use this function, perform the appropriate tasks in [Table 81](#).

Table 81. Packet trace enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect all discarded packets.</td>
<td>Issue the VARY TCPIP,PKTTRACE,DISCARD=* command.</td>
<td>VARY TCPIP,PKTTRACE in <a href="#">z/OS Communications Server: IP System Administrator's Commands</a></td>
</tr>
</tbody>
</table>

Chapter 4. V1R10 new function summary 115
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect packets that have a specific discard reason code.</td>
<td>Issue the VARY TCPIP,PKTTRACE,DISCARD=\textit{discard_code} command where \textit{discard_code} is the code, such as 4138.</td>
<td>VARY TCPIP,PKTTRACE in z/OS Communications Server: IP System Administrator's Commands</td>
</tr>
</tbody>
</table>
| Collect all packets that were not discarded. | Issue one of the following commands:  
- VARY TCPIP,PKTTRACE,DISCARD=NONE  
- VARY TCPIP,PKTTRACE | VARY TCPIP,PKTTRACE in z/OS Communications Server: IP System Administrator's Commands |
| Collect all packets that have a nonzero discard reason code. | Issue the VARY TCPIP,PKTTRACE,DISCARD=ALL command. | VARY TCPIP,PKTTRACE in z/OS Communications Server: IP System Administrator's Commands |
| Format all packets that have a nonzero discard reason code. | Issue the CTRACE OPTIONS(( FLAG(DISCARD) )) command. | z/OS Communications Server: IP Diagnosis Guide |
| Format all packets that have a specific discard reason code. | Issue the CTRACE OPTIONS(( DISCARD(4138) )) command. | z/OS Communications Server: IP Diagnosis Guide |
| Format the statistical report showing the number of packets by discard reason code. | Issue the CTRACE OPTIONS(( STATISTICS(DETAIL) )) command. | z/OS Communications Server: IP Diagnosis Guide |
| Display the value of the packet trace DISCARD parameter under the Packet Trace Setting section. | Issue the Netstat DEvlinks/-d command. | Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands |
| Display the value of the packet trace DISCARD parameter under the Packet Trace Setting section. | Issue the TCPIPCS STATE subcommand. | z/OS Communications Server: IP Diagnosis Guide |
| Display the PKTTRACE commands active at the time of a dump. | Issue the TCPIPCS PROFILE subcommand. | z/OS Communications Server: IP Diagnosis Guide |
| Select discarded packets for formatting using the EZBCTAPI network management interface. | Update the EZBYPTO parameter list to include a list of discard codes. After formatting your records, your application might want to act on the dropped packets. EZBYDROP describes the discard reason codes in the packet trace header. | z/OS Communications Server: IP Programmer's Guide and Reference |
| Format SNA information from DATTRACE, OSAENTA, PKTTRACE, or IDS CTRACE traces. | Specify the new SNA filter values on the OPTIONS parameter of the IPCS CTRACE command. For example, if you are using the values 10003, 0003, and 1, then issue the following command: CTRACE COMP(SYSCTCPOT) FULL OPTIONS((ELEMENT(‘x’10003’ x’0003’ SUBAREA(1)))) | Formatting packet traces using IPCS in z/OS Communications Server: IP Diagnosis Guide |

**TCP/IP SMF record enhancements**

z/OS V1R10 Communications Server provides new storage statistics for the following management interfaces, which improves monitoring and tuning of TCPIP storage usage:
- SMF 119 TCP/IP Stack Start and Stop Record
- SMF 119 TCP/IP Statistics Record
- NMI TCP/IP callable interface, EZBNMIFR, GetStorageStatistics Request
Using the TCP/IP SMF record enhancements

If you want to use the TCP/IP SMF record enhancements, perform the appropriate tasks in Table 82.

Table 82. TCP/IP SMF record enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use SMF to obtain information</td>
<td>Use the new SMF fields in the TCP/IP start and stop records and the TCP/IP statistics records to obtain information about ECSA and private storage usage. Update formatting routines to obtain additional information.</td>
<td>TCP/IP stack start/stop record and SMF record layout for TCPIPSTATISTICS in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Use NMI to obtain information</td>
<td>Update the NMI application that invokes the GetStorageStatistics function of the TCP/IP callable NMI (EZBNMIFR) to use the new ECSA and private storage usage fields NWMStgECSAFree and NWMStgPrivateFree mapped in the NWMStgStatEntry structure.</td>
<td>TCP/IP NMI request and response data structures in z/OS Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
</tbody>
</table>

Allow DNS BIND 9 server to run with BPX.SUPERUSER authorization

z/OS V1R10 Communications Server permits the DNS BIND 9 name server application to be started with a nonzero UID if the user ID associated with the BIND 9 name server is permitted access to the BPX.SUPERUSER class profile. UID(0) resources are better utilized in your installation.

Using the allow DNS BIND 9 server to run with BPX.SUPERUSER authorization function

If you want to use this function, perform the appropriate tasks in Table 83.

Table 83. Allow DNS BIND 9 server to run with BPX.SUPERUSER authorization function

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>If not already in place, define and activate the BPX.SUPERUSER resource in the FACILITY class.</td>
<td>Use a security product, such as RACF. For example, issue the following RACF commands: RDEFINE FACILITY BPX.SUPERUSER UACC(NONE) SETROPTS CLASSACT(FACILITY) SETROPTS RACLST(FACILITY) REFRESH</td>
<td>Steps for setting up BPX.SUPERUSER in z/OS UNIX System Services Planning</td>
</tr>
</tbody>
</table>
### Table 83. Allow DNS BIND 9 server to run with BPX.SUPERUSER authorization function (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Change the user ID associated with the BIND 9 name server from UID(0) to a unique nonzero UID. | Use a security product, such as RACF. For example, perform the following steps:  
  1. Issue the following RACF command:  
     ALTUSER userid OMVS(NUUID)  
  2. Do one of the following:  
     • Issue the following command to make RACF assign the UID automatically:  
       ALTUSER userid OMVS(AUTOUID)  
     • Issue the following RACF command to assign a specific nonzero UID, such as x:  
       ALTUSER userid OMVS(UID(x))  
  3. Issue the following RACF command:  
     PERMIT BPX.SUPERUSER CLASS(FACILITY) ID(userid)  
     ACCESS(READ)  
     SETROPTS RACLIST(FACILITY) REFRESH  
  4. Optionally, if the name server runs as swappable, issue the following RACF commands to define the BPX.STOR.SWAP FACILITY class profile to RACF with no universal access, if not already defined:  
     RDEFINE FACILITY BPX.STOR.SWAP  
     UACC(NONE)  
     PERMIT BPX.STOR.SWAP CLASS(FACILITY) ID(userid)  
     ACCESS(READ)  
     SETROPTS RACLIST(FACILITY) REFRESH  
  5. Determine whether values in the new BPXPRMxx member for the user ID associated with the BIND 9 name server are compatible with existing name server options. If the values are not compatible, adjust the settings of the following BIND 9 options:  
     • The coresize option can be used to lower the MAXCORESIZE value in the BPXPRMxx member.  
     • The files option uses a default value that is either the same as the value of the MAXFILEPROC option in the BXPPxx member or 2048, whichever is smaller.  
     The safest approach is to explicitly code the coresize and files configuration options in the DNS BIND 9 configuration file, removing any dependency on the settings in the underlying BPXPRMxx member. | • Steps for changing a superuser from UID(0) to a unique nonzero UID in z/OS UNIX System Services Planning  
• Step 10. Specify whether the name server is to run swappable or nonswappable in z/OS Communications Server: IP Configuration Guide  
• "options" section of BIND 9-based domain name system (DNS) in z/OS Communications Server: IP Configuration Reference |

---

### ASID reuse for TCP/IP, TN3270E, and resolver

z/OS V1R10 Communications Server provides support for the address space identifiers (ASIDs) reuse function for the TCP/IP, resolver, and TN3270E Telnet server (Telnet) address spaces. Because the TCP/IP, resolver, and Telnet address
spaces provide services that are entered using PC calls that must be accessible to other address spaces, the ASIDs associated with these programs are typically not reusable when the address space is stopped. If these address spaces are stopped many times, all available ASIDs might be exhausted, which prevents a new address space from being created on the system.

To help alleviate this potential problem, you can start the TCP/IP and Telnet address spaces as reusable ASIDs by specifying REUSASID=YES on the START command.

When the resolver is started as a result of the BPXPRMxx statement RESOLVER_PROC, it specifies REUSASID=YES. If the resolver is stopped and restarted, you can specify REUSASID=YES on the start command.

**Restrictions for ASID reuse for TCP/IP, TN3270E, and resolver**
The VMCF and TNF subsystems use nonreusable ASIDs; therefore, they cannot be defined to start as reusable ASIDs. Any products that use these services cannot use the reuse ASID function. This includes the following Communications Server applications, interfaces, and commands:
- SNMP Query Engine application
- Pascal Socket Interface
- SMTP and LPD servers
- TSO TELNET, HOMETEST, TESTSITE, RSH, REXEC, and LPR commands

Do not specify REUSASID=YES when you are starting other Communication Server address spaces. The ASIDs associated with these Communication Server address spaces are already reusable. Unnecessary use of REUSASID=YES can reduce the number of ASIDs that are available for ordinary address space requests.

**Dependencies for ASID reuse for TCP/IP, TN3270E, and resolver**
FFST APAR PK64094 must be applied before enabling this function.

**Using ASID reuse for TCP/IP, TN3270E, and resolver**
If you want to use this function, perform the appropriate tasks in Table 84.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the reuse ASID function on the z/OS system.</td>
<td>Specify REUSASID=YES in the DIAGxx parmlib member.</td>
<td>• Statements/parameters for DIAGxx in z/OS MVS Initialization and Tuning Reference&lt;br&gt;• Reusing ASIDs in z/OS MVS Programming: Extended Addressability Guide</td>
</tr>
<tr>
<td>Start TCP/IP as a reusable ASID.</td>
<td>Issue START tcpip_proc,REUSASID=YES, where tcpip_proc is the name of the TCP/IP procedure.</td>
<td>Starting a System Task from a Console in z/OS MVS System Commands</td>
</tr>
<tr>
<td>Start Telnet as a reusable ASID.</td>
<td>Issue START tnproc,REUSASID=YES, where tnproc is the name of the Telnet procedure.</td>
<td>Starting a System Task from a Console in z/OS MVS System Commands</td>
</tr>
<tr>
<td>Start the resolver if it is stopped and you want to restart it as a reusable ASID.</td>
<td>Issue START procname, REUSASID=YES, where procname is the name of the resolver procedure.</td>
<td>Starting a System Task from a Console in z/OS MVS System Commands</td>
</tr>
</tbody>
</table>
Resolver support for EDNS0

*z/OS Communications Server* provides support for extension mechanisms for DNS (EDNS0) standards. In *z/OS V1R10 Communications Server*, the *z/OS resolver* accepts DNS response messages in UDP packets that are up to 3072 bytes in length, compared to the previous maximum of 512 bytes. This support improves performance by avoiding the use of more costly TCP protocols to obtain large response records from a name server.

Dependencies for the resolver support for EDNS0

The following dependencies apply:

- The DNS name server must also support EDNS0 protocols in order to use UDP packets larger than 512 bytes.
- Firewalls that exist between the DNS name server and the *z/OS resolver* must be configured to accept DNS messages sent as UDP packets of greater than 512 bytes in order to use EDNS0 protocols.

Using the resolver support for EDNS0

You do not have to perform any steps to enable the resolver support for EDNS0; it is automatically enabled by *z/OS Communications Server*. The task in Table 85 is optional.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optionally, force the <em>z/OS resolver</em> to relearn name server EDNS0 capabilities (for example, after upgrading the name server to support the function).</td>
<td>Issue the MODIFY RESOLVER,REFRESH command of the resolver address space.</td>
<td>MODIFY command -- Resolver address space in <em>z/OS Communications Server: IP System Administrator’s Commands</em></td>
</tr>
</tbody>
</table>

Table 85. Resolver support for EDNS0

FTP enhancements

*z/OS V1R10 Communications Server* provides several FTP enhancements. See “FTP security enhancements” on page 81 for the FTP enhancements that are related to security. The other FTP enhancements are in the following areas:

- “FTP application data enhancements” on page 121
- “FTP client API for Java” on page 122
- “FTP JES enhancements” on page 122
- “FTP batch pipe subsystem enhancements” on page 123
- “FTP and MVS data set contention enhancements” on page 124
- “FTP keepalive enhancements” on page 125

FTP application data enhancements

*z/OS V1R10 Communications Server* enhances FTP so that it can associate application data with its sockets using the SIOCSAPPLDATA ioctl() call. With this enhancement, as with all SIOCSAPPLDATA data, the following statements are true:

- You can display the application data with the Netstat command.
- The application data is included in SMF Type 119 TCP Connection Termination records.
- The application data is available to NMI application programs through the EZBNMIFR programming interface.
Using the FTP application data enhancements: If you want to use this function, perform the appropriate tasks in Table 86.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Display and interpret application data associated with FTP sockets | Perform the following steps:  
  - Use the Netstat command to see available associated application data on ALL/-A report.  
  - Specify the Netstat command APPLDATA modifier to optionally see associated application data on ALLConn/-a or CONn/-c reports.  
  - Specify the Netstat command APPLD/-G filter ALL/-A, ALLConn/-a or CONn/-c reports to filter results. | • See the following topics in z/OS Communications Server: IP System Administrator’s Commands  
  - DISPLAY TCPIP,NETSTAT  
  - The z/OS UNIX netstat command syntax  
  • Application data in z/OS Communications Server: IP Configuration Reference  
  SMF type 119 records in z/OS Communications Server: IP Configuration Reference |
| Modify SMF record analysis programs to consider associated FTP application data. | Modify program to process self-defining section of SMF 119 TCP Connection Termination records. | See the GetTCPLListeners and GetConnectionDetail parameters in the EZBNMIFR — TCP/IP network management request topic in z/OS Communications Server: IP Programmer’s Guide and Reference |
| Modify TCP/IP Network Management Interface (NMI) applications to consider associated FTP application data. | Perform the following steps:  
  - Modify program to recognize presence of application data in TCP Listener Entry and TCP Connection Entry records.  
  - Modify program to filter results returned based on a supplied application data filter mask. | See the GetTCPLListeners and GetConnectionDetail parameters in the EZBNMIFR — TCP/IP network management request topic in z/OS Communications Server: IP Programmer’s Guide and Reference |

FTP client API for Java

z/OS V1R10 Communications Server introduces a new Java™ interface that you can use to invoke the FTP client programmatically. This API support extends the existing FTP client API to support the Java programming language and includes a sample Java program.

The Java interface is well-defined and is fully described in FTP Client Application Programming Interface (API) in z/OS Communications Server: IP Programmer’s Guide and Reference. Additional information about FTP is included in the following documents:

- z/OS Communications Server: IP Programmer’s Guide and Reference
- z/OS Communications Server: IP Configuration Guide
- z/OS Communications Server: IP User’s Guide and Commands

Restrictions for FTP client API for Java: The Java FTP Client API requires Java 5 or later.

Using the FTP client API for Java: If you want to use this function, perform the appropriate tasks in Table 87.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
Table 87. FTP client API for Java (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make EZAFTPKI accessible to the application.</td>
<td>Ensure that the interface module EZAFTPKI is accessible to the application in the linklist or in a STEPLIB or JOBLIB DD statement.</td>
<td>FTP Client Application Programming Interface (API) in z/OS Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
<tr>
<td>Modify the classpath so that the Java FTP Client API classes can be found.</td>
<td>Include EZAFTP.jar in your classpath.</td>
<td>FTP Client Application Programming Interface (API) in z/OS Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
<tr>
<td>Modify the $LIBPATH so that the JNI functions can be found.</td>
<td>Include the directory that contains libEZAFTP.so in $LIBPATH.</td>
<td>FTP Client Application Programming Interface (API) in z/OS Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
<tr>
<td>Control the z/OS FTP client using a Java program.</td>
<td>Invoke the Java FTP API to perform the desired actions.</td>
<td>FTP Client Application Programming Interface (API) in z/OS Communications Server: IP Programmer’s Guide and Reference</td>
</tr>
</tbody>
</table>

**FTP JES enhancements**

In z/OS V1R10 Communications Server, you can specify how the FTP server should use the foreign file name when retrieving a file that specifies FILEType=JES. The new server FTP.DATA statement JESGETBYDSN and new SITE subcommand options, JESGETBYDSN and NOJESGETBYDSN, provide this new function. With the previous method of file retrieval, you specified only the foreign file name as the number of a ddname.

**Dependencies for the FTP JES enhancements:** This function is available only when you specify JES as value for the FILETYPE command and when you code the JESINTERFACELEVEL 2 statement.

**Using the FTP JES enhancements:** If you want to use this function, perform the appropriate tasks in Table 88

Table 88. FTP JES enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the server has specified JESINTERFACELEVEL 2.</td>
<td>Do the following:</td>
<td>JESINTERFACELEVEL (FTP server) statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td></td>
<td>• Display the JESINTERFACELEVEL value by issuing the z/OS FTP server STAT command.</td>
<td>Site subcommand—Send site-specific information to a host and STATus subcommand—Retrieve status information from a remote host in z/OS Communications Server: IP User’s Guide and Commands</td>
</tr>
<tr>
<td></td>
<td>• If necessary, code the JESINTERFACELEVEL 2 statement in the FTP.DATA file of the FTP server.</td>
<td></td>
</tr>
</tbody>
</table>
Table 88. FTP JES enhancements (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Specify that you want to retrieve a JES spool file by JES data set name. | Perform the following steps:  
1. Verify that the server has specified JESINTERFACELEVEL 2.  
2. Do one of the following:  
   - Code the following statements in the FTPDATA file of the server:  
     JESGETBYDSN TRUE  
     FILETYPE=JES  
   - After logging in to FTP, use the z/OS FTP client SITE subcommand to set JESGETBYDSN and FILETYPE=JES. | • Site subcommand—Send site-specific information to a host and in z/OS Communications Server: IP User’s Guide and Commands  
• JESGETBYDSN (FTP server) and FILETYPE (FTP client and server) statements in z/OS Communications Server: IP Configuration Reference |

FTP batch pipe subsystem enhancements

z/OS V1R10 Communications Server enhances FTP to support writing to a batch pipe subsystem. You can use the new option SUBSYS on the SITE command to configure the FTP server to write data to a batch pipe subsystem as a destination.

Restrictions for FTP batch pipe subsystem enhancements: The following restrictions apply when the SUBSYS value is specified on the SITE command:

- The APPE and REST commands are not supported.
- Only binary (Type I) file transfer is supported.
- Only FILETYPE SEQ is supported.
- Checkpointing and restart of file transfer is not supported. See Restarting a failed data transfer in z/OS Communications Server: IP User’s Guide and Commands for a description of checkpointing.
- You cannot specify the SUBSYS value while SMF managed data sets are being transferred (data sets with an assigned storage class).
- Only the following RECFM values are supported: F, FB, V, and VB.

Dependencies for the FTP batch pipe subsystem enhancements: If you want to use the FTP server support for the batch pipe subsystem, you must have the IBM BatchPipes® subsystem installed.

Using the FTP batch pipe subsystem enhancements: If you want to use this function, perform the appropriate tasks in Table 89.

Table 89. FTP enhancements: Configure the FTP server to support writing to a batch pipe subsystem

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Configure the FTP server for file transfer to a batch pipe. | Perform the following steps:  
1. Issue the SITE command to do the following:  
   • Set the file type to SEQ (this is the default).  
   • Set the SUBSYS value.  
2. Set the file transfer type to binary (Image). | See the restrictions in the following topic: Site subcommand—Send site-specific information to a host in z/OS Communications Server: IP User’s Guide and Commands |
Table 89. FTP enhancements: Configure the FTP server to support writing to a batch pipe subsystem (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Transfer a file to a batch pipe. | Perform the following steps:  
1. Start the BatchPipes subsystem.  
2. Start the batch pipe reader job.  
3. Configure FTP server for batch pipe transfer.  
4. Issue the PUT subcommand, specifying the batch pipe as the target file. | • GA22-7459-00 IBM BatchPipes OS/390® V2R1 Introduction  
• SA22-7456-01 IBM BatchPipes OS/390 V2R1 BatchPipeWorks Reference  
• SUBSYS: Writing to BatchPipes and PUT subcommand—Copy data sets to the remote host in z/OS Communications Server: IP User’s Guide and Commands |

**FTP and MVS data set contention enhancements**

*z/OS V1R10* Communications Server enhances FTP so that it can wait for an MVS data set when the data set is held by one or more jobs. The configuration option DSWAITTIME controls how long FTP should wait for the data set contention to be resolved. Enabling this function reduces the number of failed batch jobs when FTP is invoked from a batch job that has time to wait for contention to be resolved. The enhanced contention messages and replies identify the holder of a data set so you can act quickly to resolve contention.

**Restrictions for the FTP and MVS data set contention enhancements:** The following restrictions apply:

- The DSWAITTIME configuration option is supported for MVS data sets only; z/OS UNIX file system data sets are not supported.
- The FTP server ignores the DSWAITTIME configuration option for the APPEND (APPE), RENAME FROM (RNFR), RENAME TO (RNTO), and DELETE (DELE) commands.

**Using the FTP and MVS data set contention enhancements:** If you want to use this function, perform the appropriate tasks in Table 90.

Table 90. FTP and MVS data set contention enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure FTP to wait for an MVS data set that is held by one or more jobs.</td>
<td>Code the DSWAITTIME configuration statement in the FTPDATA file for a customized default period of time.</td>
<td>• DSWAITTIME (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference</td>
</tr>
</tbody>
</table>
| Determine whether the FTP server will wait for an MVS data set that is in use. | Issue the STAT subcommand with the DSWAITTIME parameter from the z/OS FTP client.  
**Tip:** If your client is not the z/OS FTP client, you can issue the QUOTE subcommand with the parameters XSTA (DSWAITTIME). | • STATus subcommand—Retrieve status information from a remote host in z/OS Communications Server: IP User’s Guide and Commands |
| Determine whether the z/OS FTP client will wait for an MVS data set that is in use. | Issue the LOCSTAT subcommand with the DSWAITTIME option from the z/OS FTP client. | • LOCStat subcommand—Display local status information in z/OS Communications Server: IP User’s Guide and Commands |
| Modify the length of time that the z/OS FTP server will wait for an MVS data set that is currently in use. | Issue the SITE subcommand with the DSWAITTIME option. | • Site subcommand—Send site-specific information to a host in z/OS Communications Server: IP User’s Guide and Commands |
### FTP and MVS Data Set Contention Enhancements (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the time the z/OS FTP client will wait for an MVS data set that is currently in use.</td>
<td>Issue the LOCSITE subcommand with the DSWAITTIME option</td>
<td>LOCSite subcommand—Specify site information to the local host in z/OS Communications Server: IP User's Guide and Commands</td>
</tr>
<tr>
<td>Determine the remote job on the FTP server host that is holding an MVS data set.</td>
<td>Inspect the 125- reply to obtain information about the job or jobs that are holding the data set. (When the z/OS FTP server determines that a data set is held by one or more jobs, it sends a reply 125- to the client identifying the job name of the jobs that are holding the MVS data set.)</td>
<td>z/OS Communications Server: IP and SNA Codes</td>
</tr>
<tr>
<td>Determine the local job on the FTP client host that is holding an MVS data set.</td>
<td>Inspect message EZZA9819I, which is issued by the client, for information about the job or jobs that are holding the data set.</td>
<td>z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)</td>
</tr>
</tbody>
</table>

### FTP Keepalive Enhancements

z/OS V1R10 Communications Server introduces a new option, DATAKEEPALIVE, to configure the interval for keepalive packets on the data connection. You can use keepalive packets to keep the data connection open while FTP waits for another job to release an MVS data set, or while FTP waits for a submitted JES job to complete processing. Previously, the only method available to configure keepalive packets on the data connection was to use the TCPIP.PROFILE file, which affects all connections.

**Using the FTP keepalive enhancements:** If you want to use this function, perform the appropriate tasks in Table 91.

### Table 91. FTP Keepalive Enhancements

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override TCP/IP's configured interval for sending keepalive packets.</td>
<td>Code the DATAKEEPALIVE configuration statement in the FTP.DATA file</td>
<td>• DATAKEEPALIVE (FTP client and server) in z/OS Communications Server: IP Configuration Reference</td>
</tr>
<tr>
<td>Determine whether the FTP server has overridden TCP/IP's configured interval for keepalive packets.</td>
<td>Issue the STAT subcommand with the DATAKEEPALIVE parameter from the z/OS FTP client.</td>
<td>STATus subcommand—Retrieve status information from a remote host in z/OS Communications Server: IP User’s Guide and Commands</td>
</tr>
<tr>
<td>Tip: If your client is not the z/OS FTP client, you can issue the QUOTE subcommand with the XSTA (DATAKEEPALIVE) parameters.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determine whether the FTP client has overridden TCP/IP's configured interval for keepalive packets.</td>
<td>Issue the LOCSTAT subcommand with the DATAKEEPALIVE option from the z/OS FTP client.</td>
<td>LOCStat subcommand—Display local status information in z/OS Communications Server: IP User’s Guide and Commands</td>
</tr>
<tr>
<td>Modify the keepalive interval to be used by the z/OS FTP server for the data connection.</td>
<td>Issue the SITE subcommand with the DATAKEEPALIVE parameter and value from the z/OS FTP client.</td>
<td>SITE subcommand—Send site-specific information to a host in z/OS Communications Server: IP User’s Guide and Commands</td>
</tr>
<tr>
<td>Tip: If your client is not the z/OS FTP client, you can issue the QUOTE subcommand with the SITE DATAKEEPALIVE parameter and time interval.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 91. FTP keepalive enhancements (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the keepalive interval to be used by the z/OS FTP client for the data connection.</td>
<td>Issue the LOCSITE subcommand with the DATAKEEPALIVE parameter and time interval.</td>
<td>LOCSite subcommand—Specify site information to the local host in z/OS Communications Server: IP User’s Guide and Commands</td>
</tr>
</tbody>
</table>
| When you are logged in to a z/OS FTP server, prevent session termination caused by long periods of inactivity. | Do one of the following to prevent the data connection from timing out:  
  - Code the DATAKEEPALIVE configuration statement in the FTPDATA file of the FTP server.  
  - Issue the SITE subcommand to set the DATAKEEPALIVE value for the data connection | FTP configuration statements in FTPDATA in z/OS Communications Server: IP Configuration Reference  
  Site subcommand—Send site-specific information to a host in z/OS Communications Server: IP User’s Guide and Commands  
  Configuring PROFILE.TCPIP for FTP in z/OS Communications Server: IP Configuration Guide  
  TCPCONFIG in z/OS Communications Server: IP Configuration Reference |

Tip: Long periods of inactivity can occur when FTP is waiting for a data set held by one or more jobs, or during FILETYPE=JES transfers when waiting on job completion from the FTP server.

Prevent the control connection from timing out by configuring TCP/IP to send keepalive packets. Code the TCPCONFIG statement with the INTERVAL parameter in your TCPIP.PROFILE file.

Tips:
- If your client is not the z/OS FTP client, you can issue the QUOTE subcommand with the SITE DATAKEEPALIVE parameter and time interval.
- If your client is the z/OS FTP client, you can do one of the following:
  - Code FTPKEEPALIVE in the client’s FTPDATA file
  - Configure TCP/IP on the FTP server to send keepalive packets by coding the TCPCONFIG statement with the INTERVAL parameter in your TCPIP.PROFILE.
  - Issue the SITE command with the DATAKEEPALIVE parameter and time interval.
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
<th>Reference</th>
</tr>
</thead>
</table>
| When you are using the z/OS FTP client, prevent session termination   | Do one of the following to prevent the data connection from timing out:  
- Code the DATAKEEPALIVE configuration statement in the FTP client’s FTP.DATA file.  
- Issue the LOCATE subcommand to set the DATAKEEPALIVE time interval for the data connection.  
- Configure TCP/IP to send keepalive packets by coding the TCPCONFIG statement with the INTERVAL parameter in your TCPIP.PROFILE file. | **FTP configuration statements in FTP.DATA in** z/OS Communications Server: IP Configuration Reference | **FTP configuration statements in FTP.DATA in** z/OS Communications Server: IP Configuration Reference |
| caused by long periods of inactivity.                                 | Do one of the following to prevent the control connection from timing out:  
- Code the FTPKEEPALIVE configuration statement in the FTP client’s FTP.DATA file.  
- Issue the LOCATE subcommand to set the FTPKEEPALIVE time interval for the data connection.  
- Configure TCP/IP to send keepalive packets by coding the TCPCONFIG statement with the INTERVAL parameter in your TCPIP.PROFILE file. | **LOCATE subcommand—Specify site information to the local host in** z/OS Communications Server: IP User’s Guide and Commands | **LOCATE subcommand—Specify site information to the local host in** z/OS Communications Server: IP User’s Guide and Commands |
| **Tip:** Long periods of inactivity can occur when FTP is waiting for  | Do one of the following:  
- Code the DATAKEEPALIVE configuration statement in the FTP client’s FTP.DATA with a time interval of 0.  
- Issue the LOCATE subcommand to set the DATAKEEPALIVE value for the data connection of 0. | **Configuring PROFILE TCPIP for FTP in** z/OS Communications Server: IP Configuration Guide | **Configuring PROFILE TCPIP for FTP in** z/OS Communications Server: IP Configuration Guide |
| a data set held by one or more jobs, or during FILETYPE=JES transfers | **Requirement:** The FTP server must not be configured to send keepalive packets on data connection.                                       | **TCPCONFIG in** z/OS Communications Server: IP Configuration Reference   | **TCPCONFIG in** z/OS Communications Server: IP Configuration Reference   |
| when waiting for job completion from the FTP server.                 |                                                                                                                                           |                                                                          |                                                                          |
Table 91. FTP keepalive enhancements (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Allow the data connection for the z/OS FTP server to time out when no activity occurs on the data connection. | Do one of the following:  
- Code the DATAKEEPA=0 in the FTP server’s FTPDATA file (this is also the default).  
- Issue the SITE subcommand to set the DATAKEEPA value for the data connection equal to 0 if using the z/OS FTP client. | FTP configuration statements in FTPDATA in z/OS Communications Server: IP Configuration Reference  
Site subcommand—Send site-specific information to a host in z/OS Communications Server: IP User’s Guide and Commands  
Configuring PROFILE TCPIP for FTP in z/OS Communications Server: IP Configuration Guide  
TCPCONFIG in z/OS Communications Server: IP Configuration Reference |

Tip: If your client is not the z/OS FTP client, you can issue the QUOTE subcommand with the SITE DATAKEEPA parameter and time interval.

Requirement: The FTP client must not be configured to send keepalive packets on the data connection.

Path MTU discovery for Enterprise Extender for SNA

In z/OS V1R10 Communications Server, path MTU discovery for Enterprise Extender (EE) enables VTAM to dynamically learn any MTU size changes that are associated with IPv4 and IPv6 EE connections in the IP network. VTAM can segment the HPR data to avoid IP packet fragmentation. By default, path MTU discovery for EE is controlled by the TCP/IP stack that is enabled for EE. If you specify PATHMTUDISCOVERY on the IPCONFIG profile statement, then path MTU discovery is also enabled for IPv4 EE connections. For IPv6, path MTU discovery is always enabled in the TCP/IP stack; by default, path MTU discovery is also enabled for IPv6 EE connections.

See “Path MTU discovery for Enterprise Extender for IP” on page 108 for the IP considerations for this function.

Restrictions for path MTU discovery for Enterprise Extender

Both Enterprise Extender (EE) and RTP pipes must have endpoints on the same node for this function to work.

Dependencies for path MTU discovery for Enterprise Extender

Path MTU discovery uses ICMP fragmentation-needed errors to detect the PMTU for a path. You must permit ICMP errors to flow at all hosts along the path of a connection. Path MTU discovery does not function if a firewall blocks ICMP errors.

Using path MTU discovery for Enterprise Extender

If you want to use this function, perform the appropriate tasks in Table 92 on page 129.
Table 92. Path MTU discovery for Enterprise Extender

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable path MTU discovery support for IPv4 EE connections.</td>
<td>Specify the PATHMTUDISCOVERY keyword on the IPCONFIG profile statement for the EE-enabled TCP/IP stack.</td>
<td>• TCP/IP profile (PROFILE.TCPIP) and configuration statements in z/OS Communications Server: IP Configuration Reference. • PMTUD start option in z/OS Communications Server: SNA Resource Definition Reference. • START command and MODIFY VTAMOPTS command in z/OS Communications Server: SNA Operation.</td>
</tr>
<tr>
<td>Allow path MTU discovery support in the EE-enabled TCP/IP stack, but disable path MTU discovery support for both IPv4 and IPv6 EE connections.</td>
<td>Do the following: • Specify the PATHMTUDISCOVERY keyword on the IPCONFIG profile statement for the EE-enabled TCP/IP stack. • Specify PMTUD=NO in the appropriate ATCSTRxx VTAM start list or on the VTAM START command. Optionally, when VTAM is active, issue the MODIFY procname,VTAMOPTS, PMTUD=NO command.</td>
<td>• TCP/IP profile (PROFILE.TCPIP) and configuration statements in z/OS Communications Server: IP Configuration Reference. • PMTUD start option in z/OS Communications Server: SNA Resource Definition Reference. • START command and MODIFY VTAMOPTS command in z/OS Communications Server: SNA Operation.</td>
</tr>
<tr>
<td>Control the maximum transmission unit (MTU) size that VTAM will transmit over an Enterprise Extender connection.</td>
<td>Specify the new MTU keyword on the following definition statements: • For EE connection networks, define this parameter on the connection network GROUP definition statements in the EE XCA major major node. • For dial-in Enterprise Extender connections that have their associated PUs dynamically created, define this parameter on the model major node (DYNTYPE=EE) PU definition statement. • For predefined Enterprise Extender connections, define this parameter on the PU definition statement in the switched major node.</td>
<td>See the following topics in z/OS Communications Server: SNA Resource Definition Reference: • XCA Major Node / MTU • Model Major Node / MTU • Switched Major Node / MTU</td>
</tr>
</tbody>
</table>

TN3270E Telnet server ECSA reduction

z/OS V1R10 Communications Server reduces the ECSA storage requirements for TN3270E Telnet Server receive processing. This function is also available for IP; see “TN3270E Telnet server ECSA reduction” on page 72.

This function is automatically enabled.

Extended border node searching enhancement

In z/OS V1R10 Communications Server, APPN extended border node (EBN) support is enhanced so that you can restrict the searching capability of adjacent non-native nodes without coding a directory services management exit. The AUTHNETS value on the ADJCP statement specifies the list of authorized network
IDs for the adjacent control point. Searches received from that control point are rejected if the network ID of the destination LU is not in the authorized network ID list.

Using the extended border node searching enhancement

If you want to use this function, perform the appropriate tasks in Table 93.

Table 93. Extended border node searching enhancement

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify a network ID, or list of network IDs, that can be a destination search target for searches received by this extended border node from the adjacent non-native node defined by the ADJCP entry.</td>
<td>Specify the AUTHNETS=(netidxx,...) operand on the ADJCP minor nodes that correspond to the adjacent non-native nodes through which searches are to be controlled. AUTHNETS is the list of authorized DLU resource network IDs that the node is allowed to search for through this EBN.</td>
<td>Adjacent control point major node in z/OS Communications Server: SNA Resource Definition Reference</td>
</tr>
<tr>
<td>Display a list of network IDs that can be a destination search target for searches received by this extended border node from an adjacent non-native node.</td>
<td>Issue the DISPLAY ADJCP,ID=adj_netid.adj_non-native_CP_name command.</td>
<td>DISPLAY ADJCP command in z/OS Communications Server: SNA Operation</td>
</tr>
<tr>
<td>Change a network ID, or list of network IDs, that can be a destination search target for searches received by this extended border node from the adjacent non-native node, which is defined by the ADJCP entry.</td>
<td>Perform the following steps: 1. Inactivate the ADJCP major node. 2. Modify the AUTHNETS=(netidxx,...) operand on the ADJCP minor nodes that correspond to the adjacent non-native nodes through which searches are to be changed. 3. Active the ADJCP major node.</td>
<td>Adjacent control point major node in z/OS Communications Server: SNA Resource Definition Reference</td>
</tr>
</tbody>
</table>

TGN parameter for EE model PUs

z/OS V1R10 Communications Server adds a transmission group number parameter (the TGN parameter) to the DYNTYPE=EE PU definition statement in the model major node. You can specify up to four predefined transmission group numbers (TGNs) for the EE connections between EE nodes, which increases the predictability of the TG numbers used by EE connections. This function helps manage the EE network and helps diagnose EE connectivity issues.

Using the TGN parameter for EE model PUs

If you want to use this function, perform the appropriate tasks in Table 94.

Table 94. TGN parameter for EE model PUs

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a preferred TG number for dynamic EE PUs to use and prohibit another TG number from being used.</td>
<td>Perform the following steps: 1. Code TGN=x on a DYNTYPE=EE PU definition statement in a model major node. 2. Activate the model major node.</td>
<td>Model major node / TGN in z/OS Communications Server: SNA Resource Definition Reference • VARY ACT in z/OS Communications Server: SNA Operation</td>
</tr>
</tbody>
</table>
Table 94. TGN parameter for EE model PUs (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish up to four preferred TG numbers for use by dynamic EE PUs</td>
<td>Perform the following steps:</td>
<td>Model major node / TGN in z/OS Communications Server: SNA Resource Definition Reference</td>
</tr>
<tr>
<td>and do not allow another TG number to be used for these PUs.</td>
<td>1. Code TGN=(w,x,y,z) on a DYNTYPE=EE PU definition statement in a Model</td>
<td>VARY ACT in z/OS Communications Server: SNA Operation</td>
</tr>
<tr>
<td></td>
<td>Major Node, where w,x,y,z are the values in the order in which you</td>
<td></td>
</tr>
<tr>
<td></td>
<td>want them to be used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Activate the model major node.</td>
<td></td>
</tr>
<tr>
<td>Establish up to three preferred TG numbers for dynamic EE PUs to</td>
<td>Perform the following steps:</td>
<td>Model major node / TGN in z/OS Communications Server: SNA Resource Definition Reference</td>
</tr>
<tr>
<td>use and allow another TG number to be used for these PUs (if the</td>
<td>1. Code TGN=(w,x,y,ANY) on a DYNTYPE=EE PU definition statement in a</td>
<td>VARY ACT in z/OS Communications Server: SNA Operation</td>
</tr>
<tr>
<td>predefined TG numbers are not available).</td>
<td>model major node. w,x, and y are the preferred values in the order</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in which you want them to be used, and ANY indicates if w,x, and y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>are not available, the transmission group number will be</td>
<td></td>
</tr>
<tr>
<td></td>
<td>negotiated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Activate the model major node.</td>
<td></td>
</tr>
</tbody>
</table>

High Performance Routing enhancements

In z/OS V1R10 Communications Server, High Performance Routing (HPR) is enhanced in the following areas:

- “Stalled HPR pipe termination”
- “RTP pipe session limit control” on page 132
- “Display RTP enhancements” on page 133

Stalled HPR pipe termination

An HPR Rapid Transport Protocol (RTP) pipe stalls when the partner RTP requests retransmission of at least one network layer packet (NLP) but the request cannot be honored or the partner RTP repeatedly requests transmission of the same NLP. Prior to z/OS V1R10 Communications Server, there was no provision for stalled RTP pipes to stop automatically. You had to issue a VARY INACT command for the RTP PU to recycle it and terminate the stalled sessions.

z/OS V1R10 Communications Server introduces a new modifiable VTAM start option (HPRSTALL) that you can use to limit the length of time that an RTP pipe can remain continuously stalled. If that limit is exceeded, VTAM automatically stops the RTP pipe and issues a new unsolicited VTAM message (IST2253I) that indicates a timeout occurred.

Using the stalled HPR pipe termination function

If you want to use this function, perform the appropriate tasks in Table 95 on page 132.
### RTP pipe session limit control

*z/OS V1R10* Communications Server introduces a new High Performance Routing start option (HPRSESLM) that limits the number of sessions that are placed on each Rapid Transport Protocol (RTP) pipe. When an RTP pipe reaches the specified session limit, new sessions are not associated with that RTP pipe until the number of sessions on that RTP pipe drops below the specified session limit; instead, another RTP pipe is chosen or created for new sessions. Limiting the number of sessions on a single RTP pipe can result in significant performance improvement by allowing concurrent traffic on multiple RTP pipes.

#### Restrictions for RTP pipe session limit control

The value that you specify for HPRSESLM does not represent an absolute session limit. For information about why the actual number of sessions on an RTP pipe might exceed the specified session limit during normal operations, see [HPRSESLM start option in *z/OS Communications Server: SNA Resource Definition Reference*](#) for more details.
Coexistence for RTP pipe session limit control
This function requires all native and non-native HPR-capable VTAM APPN nodes to be running z/OS Communications Server V1R8 or later (or V1R7 with compatibility APAR/PTF OA22854/UA38026 applied) before you can start any VTAM interchange nodes with z/OS V1R10 Communications Server. You must be using one of these versions of z/OS Communications Server, regardless of whether the new HPRSESLM function is used by these VTAMs.

Using RTP pipe session limit control
If you want to use this function, perform the appropriate tasks in Table 96.

Table 96. RTP pipe session limit control
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Set the limit for the number of sessions on a single RTP pipe when VTAM is started. | Select an appropriate HPR session limit in the range 1000-2147483647 (sess_lim). Specify HPRSESLM=sess_lim in the appropriate ATCSTRxx start list or on the START command. | • START command in z/OS Communications Server: SNA Operation  
• HPRSESLM start option in z/OS Communications Server: SNA Resource Definition Reference |
| Ensure that the number of sessions on a single RTP pipe is not limited when VTAM is started. | Use the default value NOLIMIT for the HPRSESLM start option. Alternatively, specify HPRSESLM=NOLIMIT in the appropriate ATCSTRxx start list or on the START command. | • START command in z/OS Communications Server: SNA Operation  
• HPRSESLM start option in z/OS Communications Server: SNA Resource Definition Reference |
| Change the limit for the number of sessions on a single RTP pipe while VTAM is running. | Select an appropriate HPR session limit in the range 1000-2147483647 (sess_lim) and issue the MODIFY VTAMOPTS,HPRSESLM=sess_lim command. | MODIFY VTAMOPTS command in z/OS Communications Server: SNA Operation |
| Remove the limit for the number of sessions on a single RTP pipe while VTAM is running. | Issue the MODIFY VTAMOPTS,HPRSESLM=NOLIMIT command. | MODIFY VTAMOPTS command in z/OS Communications Server: SNA Operation |
| Display the limit specified for the number of sessions on a single RTP pipe. | Use any of the following variations of the DISPLAY VTAMOPTS command:  
• DISPLAY VTAMOPTS  
• DISPLAY VTAMOPTS,OPT=HPRSESLM  
• DISPLAY VTAMOPTS,FUNCTION=APPNCHAR  
• DISPLAY VTAMOPTS,FUNCTION=PERFTUNE  
• DISPLAY VTAMOPTS,FUNCTION=SESSCONT | DISPLAY VTAMOPTS command in z/OS Communications Server: SNA Operation |

Display RTP enhancements
z/OS V1R10 Communications Server enhances the DISPLAY RTPS command by providing a new REXMIT operand to specify a retransmission rate percentage value. The DISPLAY RTPS,REXMIT command output displays all RTPs that meet or exceed the retransmission rate percentage value specified on the REXMIT operand. This information can help you identify the RTP pipes that have low performance.
You can use the CLEAR operand on the DISPLAY RTPS command to clear the
diagnostic counters for specified RTP PUs. A subsequent display of an RTP PU
provides the diagnostic information since the last time the diagnostic counters
were cleared.

You can also use the CLEAR operand on the DISPLAY ID command, specifying an
RTP PU with HPRDIAG=YES, to display the diagnostic information for that RTP
PU and then clear the diagnostic counters.

**Displaying RTP enhancements**
If you want to use this function, perform the appropriate tasks in [Table 97](#).

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find all RTP pipes whose retransmission rate meets or exceeds a certain percentage.</td>
<td>Issue the DISPLAY RTPS,REXMIT=x command.</td>
<td>DISPLAY RTPS command in <a href="#">z/OS Communications Server: SNA Operation</a></td>
</tr>
<tr>
<td>Find all RTP pipes whose retransmission rate meets or exceeds a certain percentage, and clear the diagnostic counters for all RTP pipes.</td>
<td>Issue the DISPLAY RTPS,REXMIT=x,CLEAR=ALL command.</td>
<td>DISPLAY RTPS command in <a href="#">z/OS Communications Server: SNA Operation</a></td>
</tr>
<tr>
<td>Find all RTP pipes whose retransmission rate meets or exceeds a certain percentage, and clear the diagnostic counters for all RTP pipes destined to the specified CPNAME.</td>
<td>Issue the DISPLAY RTPS,REXMIT=x,CLEAR=ALL, CPNAME=cpname command.</td>
<td>DISPLAY RTPS command in <a href="#">z/OS Communications Server: SNA Operation</a></td>
</tr>
<tr>
<td>Clear the diagnostic counters of all RTP pipes.</td>
<td>Issue the DISPLAY RTPS,CLEAR=ALL command.</td>
<td>DISPLAY RTPS command in <a href="#">z/OS Communications Server: SNA Operation</a></td>
</tr>
<tr>
<td>Clear the diagnostic counters of all RTP pipes destined to a specified CPNAME.</td>
<td>Issue the DISPLAY RTPS,CLEAR=ALL,CPNAME=cpname command.</td>
<td>DISPLAY RTPS command in <a href="#">z/OS Communications Server: SNA Operation</a></td>
</tr>
<tr>
<td>Clear the diagnostic counters for a specified RTP pipe.</td>
<td>Issue the DISPLAY RTPS,CLEAR=ALL,ID=rtp.pu command.</td>
<td>DISPLAY RTPS command in <a href="#">z/OS Communications Server: SNA Operation</a></td>
</tr>
<tr>
<td>Display diagnostic information and clear diagnostic counters for a specified RTP pipe.</td>
<td>Issue the DISPLAY ID=rtp.pu,HPRDIAG=YES,CLEAR=ALL command.</td>
<td>DISPLAY ID command in <a href="#">z/OS Communications Server: SNA Operation</a></td>
</tr>
</tbody>
</table>
| Collect and display diagnostic counter information for an RTP pipe over a period of time. | Perform the following steps:  
  1. Issue the DISPLAY RTPS,ID=rtp.pu,CLEAR=ALL command.  
  2. Wait the period of time.  
  3. Issue the DISPLAY ID=rtp.pu,HPRDIAG=YES command. | DISPLAY RTPS command and DISPLAY ID command in [z/OS Communications Server: SNA Operation](#) |

**MAXLOCAT enhancement**
In z/OS V1R10 Communications Server, the MAXLOCAT start option is enhanced
to prevent excessive storage growth when search replies are sent. Use the
MAXLOCAT start option to suspend sending APPN search requests to an adjacent
CP after a maximum locate congestion threshold value is reached. After the
congestion threshold value is reached, APPN architecture still requires that search
replies be queued for sending. VTAM ends the CP-CP session with an adjacent CP if the number of queued requests plus the number of queued replies to the adjacent CP reaches a congestion termination threshold that is based on the MAXLOCAT value and a minimum time interval that is based on IOPURGE is exceeded.

Using the MAXLOCAT enhancement

If you want to use this function, perform the task in Table 98.

Table 98. MAXLOCAT enhancement

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Set the number of APPN searches that can be queued to an adjacent CP before it is considered congested. | Select an appropriate MAXLOCAT limit in the range 100 - 65535 (loc_lim). Specify MAXLOCAT=loc_lim in the appropriate ATCSTRxx start list, on the START command, or issue the MODIFY VTAMOPTS,MAXLOCAT=loc_lim command. | • MODIFY VTAMOPTS command in z/OS Communications Server: SNA Operation
• MAXLOCAT start option in z/OS Communications Server: SNA Resource Definition Reference
• Avoiding congestion in z/OS Communications Server: SNA Network Implementation Guide |

Start option for CSDUMP triggers

In z/OS V1R10 Communications Server, a new CSDUMP start option specifies a VTAM message or sense code that triggers a dump of the VTAM address space and current address space, the VTAM Internal Trace dataspace, and optionally a TCP/IP address space. This start option can improve serviceability by performing the same function as the existing MODIFY CSDUMP command, but the triggers are effective when VTAM is initialized; you do not have to manually issue a command.

Using the start option for CSDUMP triggers

If you want to use this function, perform the appropriate tasks in Table 99.

Table 99. Start option for CSDUMP triggers

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause VTAM to take a dump when a specific message is issued.</td>
<td>Specify the CSDUMP,MESSAGE=xxxxxxxx start option.</td>
<td>CSDUMP start option in z/OS Communications Server: SNA Resource Definition Reference</td>
</tr>
<tr>
<td>Cause VTAM to take a dump when a specific sense code is issued.</td>
<td>Specify the CSDUMP,SENSE=xxxxxxxx start option.</td>
<td>CSDUMP start option in z/OS Communications Server: SNA Resource Definition Reference</td>
</tr>
</tbody>
</table>

TCP/IP performance improvements for SNA

In z/OS V1R10 Communications Server, the SNA data link control support for the TCP/IP data path has improved pathlength and scalability. The PCID and SIGA VTAM Internal Trace (VIT) entries are changed from CIO option entries to CIA option entries. While you cannot prevent the internal tracing of CIO option entries, you can configure whether CIA option entries are traced internally; you can prevent the tracing of PCID and SIGA entries by turning the CIA VIT option off.
This change provides you with a means of reducing the pathlength of the OSA-Express QDIO or HiperSockets data path through VTAM.

**Using the TCP/IP performance improvements for SNA**

If you want to use this function, perform the appropriate tasks in Table 100.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Trace all OSA-Express QDIO or HiperSockets adapter data path activity. | Specify the CIA VIT option on the TRACE,TYPE=VTAM start option at VTAM start, or on a MODIFY TRACE command. | See the following topics in z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT:  
  - Using the VTAM internal trace (VIT)  
  - SIGA entry for Signal Adapter event  
  - PCIx entry for program-controlled or suspend interrupt |
| Do not trace OSA-Express QDIO or HiperSockets adapter data path activity. | Do not specify the CIA VIT option on the TRACE,TYPE=VTAM start option, or specify that option on a MODIFY NOTRACE command. | See the following topics in z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT:  
  - Using the VTAM internal trace (VIT)  
  - SIGA entry for Signal Adapter event  
  - PCIx entry for program-controlled or suspend interrupt |

**IPCS support of VTAM display commands**

VTAM provides DISPLAY commands that are useful for problem diagnosis. z/OS V1R10 Communications Server introduces a new TSO operator DNET command that you can use to issue the same commands against a dump and to examine the resulting output directly from the TSO session. This provides information about a dumped system during post-failure problem analysis.

**Restrictions of the IPCS support of VTAM display commands**

The following restrictions apply:

- The DNET command does not recognize the existence of coupling facility structures.
- The DNET command does not perform any action that tests, pings, or otherwise modifies a live VTAM resource.
- The DNET VTMSTOR command does not return accurate information if directed at certain major VTAM control block structures, such as the ATCVT.

**Dependencies of the IPCS support of VTAM display commands**

The following dependencies apply:

- IPCS must be running under ISPF, which must be running on a TSO user address space.
- The dump must contain both VTAM private and common memory areas.

**Using the IPCS support of VTAM display commands**

If you want to use this function, perform the appropriate tasks in Table 101 on page 137.
Table 101. IPCS support of VTAM display commands

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change an ISPF panel to invoke IPCS as a CLIST.</td>
<td>Edit the appropriate ISPF panel. Restart ISPF after returning to the TSO READY prompt.</td>
<td>Customizing ISPF interface in z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures</td>
</tr>
<tr>
<td>Issue VTAM display commands against a VTAM dump.</td>
<td>From an IPCS command line, issue the TSO DNET command, where command is the VTAM display command that you would issue from the console, using the TSO command version of the syntax rules.</td>
<td>Using DNET for IPCS dump analysis in z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures</td>
</tr>
</tbody>
</table>

**OSA-Express3 multi-port support for SNA**

z/OS V1R10 Communications Server introduces support for the OSA-Express3 features available with an IBM System z10 EC.

This support includes the following:

- Multiple port support per channel path ID (CHPID), which enables you to use all the QDIO ports that are available on an OSA-Express3 CHPID.
- Transparent error handling enhancements to provide more direct and efficient I/O processing.

**Dependencies for OSA-Express3 multi-port support for SNA**

OSA-Express3 features are available only with an IBM System z10.

**Using OSA-Express3 multi-port support for SNA**

Transparent error handling enhancements on OSA-Express3 features are automatically enabled by z/OS Communications Server; you do not have to perform explicit exploitation tasks. If you want to use the multi-port support per CHPID, or monitor the transparent error handling enhancement, perform the appropriate tasks in Table 102.

Table 102. OSA-Express3 multi-port support

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define an OSA-Express3 feature configured in QDIO mode to z/OS Communications Server. Code the definition to use the second physical port on OSA-Express3.</td>
<td>Specify PORTNUM=1 on the QDIO TRLE definition statement.</td>
<td>• Transport resource list major node in z/OS Communications Server: SNA Resource Definition Reference</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Defining an OSA-Express device to z/OS Communications Server using QDIO in z/OS Communications Server: SNA Network Implementation Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• System z10, System z9 and zSeries OSA-Express Customer’s Guide and Reference</td>
</tr>
<tr>
<td>Task</td>
<td>Procedure</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Display the OSA-Express3 physical port that a specific QDIO TRLE is   | Issue the DISPLAY TRL,TRLE=trlename command. In the command response,     | • DISPLAY TRL command in [z/OS Communications Server: SNA Operation]
| using.                                                              | locate the PORTNUM value displayed in message IST2263I.                    | • Message IST2263 in [z/OS Communications Server: SNA Messages] |
|                                                                    |                                                                            |                                                                            |
| Determine whether frame invalidation errors are being presented by   | Initiate VTAM tuning statistics for the OSA-Express. Monitor the IST2185I  | • MODIFY TNSTAT command in [z/OS Communications Server: SNA Operation]
| an OSA-Express3 adapter.                                              | message for nonzero values.                                                | • Message IST2185 in [z/OS Communications Server: SNA Messages] |
Appendix A. Related protocol specifications

This appendix lists the related protocol specifications (RFCs) for TCP/IP. The Internet Protocol suite is still evolving through requests for comments (RFC). New protocols are being designed and implemented by researchers and are brought to the attention of the Internet community in the form of RFCs. Some of these protocols are so useful that they become recommended protocols. That is, all future implementations for TCP/IP are recommended to implement these particular functions or protocols. These become the de facto standards, on which the TCP/IP protocol suite is built.

You can request RFCs through electronic mail, from the automated Network Information Center (NIC) mail server, by sending a message to service@nic.ddn.mil with a subject line of RFC nnnn for text versions or a subject line of RFC nnnn.PS for PostScript versions. To request a copy of the RFC index, send a message with a subject line of RFC INDEX.

For more information, contact nic@nic.ddn.mil or at:

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA  22021

Hard copies of all RFCs are available from the NIC, either individually or by subscription. Online copies are available at the following Web address:

http://www.rfc-editor.org/rfc.html

See "Internet drafts" on page 154 for draft RFCs implemented in this and previous Communications Server releases.

Many features of TCP/IP Services are based on the following RFCs:

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title and Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 652</td>
<td>Telnet output carriage-return disposition option D. Crocker</td>
</tr>
<tr>
<td>RFC 653</td>
<td>Telnet output horizontal tabstops option D. Crocker</td>
</tr>
<tr>
<td>RFC 654</td>
<td>Telnet output horizontal tab disposition option D. Crocker</td>
</tr>
<tr>
<td>RFC 655</td>
<td>Telnet output formfeed disposition option D. Crocker</td>
</tr>
<tr>
<td>RFC 657</td>
<td>Telnet output vertical tab disposition option D. Crocker</td>
</tr>
<tr>
<td>RFC 658</td>
<td>Telnet output linefeed disposition D. Crocker</td>
</tr>
<tr>
<td>RFC 698</td>
<td>Telnet extended ASCII option T. Mock</td>
</tr>
<tr>
<td>RFC 726</td>
<td>Remote Controlled Transmission and Echoing Telnet option J. Postel, D. Crocker</td>
</tr>
<tr>
<td>RFC 727</td>
<td>Telnet logout option M.R. Crispin</td>
</tr>
<tr>
<td>RFC 732</td>
<td>Telnet Data Entry Terminal option J.D. Day</td>
</tr>
<tr>
<td>RFC 733</td>
<td>Standard for the format of ARPA network text messages D. Crocker, J. Vittal, K.T. Pogran, D.A. Henderson</td>
</tr>
<tr>
<td>RFC</td>
<td>Title</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>903</td>
<td>Reverse Address Resolution Protocol</td>
</tr>
<tr>
<td>904</td>
<td>Exterior Gateway Protocol formal specification</td>
</tr>
<tr>
<td>919</td>
<td>Broadcasting Internet Datagrams</td>
</tr>
<tr>
<td>922</td>
<td>Broadcasting Internet datagrams in the presence of subnets</td>
</tr>
<tr>
<td>927</td>
<td>TACACS user identification Telnet option</td>
</tr>
<tr>
<td>933</td>
<td>Output marking Telnet option</td>
</tr>
<tr>
<td>946</td>
<td>Telnet terminal location number option</td>
</tr>
<tr>
<td>950</td>
<td>Internet Standard Subnetting Procedure</td>
</tr>
<tr>
<td>952</td>
<td>DoD Internet host table specification</td>
</tr>
<tr>
<td>959</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>961</td>
<td>Official ARPA-Internet protocols</td>
</tr>
<tr>
<td>974</td>
<td>Mail routing and the domain system</td>
</tr>
<tr>
<td>1006</td>
<td>ISO transport services on top of the TCP: Version 3</td>
</tr>
<tr>
<td>1009</td>
<td>Requirements for Internet gateways</td>
</tr>
<tr>
<td>1011</td>
<td>Official Internet protocols</td>
</tr>
<tr>
<td>1014</td>
<td>XDR: External Data Representation standard</td>
</tr>
<tr>
<td>1027</td>
<td>Using ARP to implement transparent subnet gateways</td>
</tr>
<tr>
<td>1032</td>
<td>Domain administrators guide</td>
</tr>
<tr>
<td>1033</td>
<td>Domain administrators operations guide</td>
</tr>
<tr>
<td>1034</td>
<td>Domain names—concepts and facilities</td>
</tr>
<tr>
<td>1035</td>
<td>Domain names—implementation and specification</td>
</tr>
<tr>
<td>1038</td>
<td>Draft revised IP security option</td>
</tr>
<tr>
<td>1041</td>
<td>Telnet 3270 regime option</td>
</tr>
<tr>
<td>1042</td>
<td>Standard for the transmission of IP datagrams over IEEE 802 networks</td>
</tr>
<tr>
<td>1043</td>
<td>Telnet Data Entry Terminal option: DODIIS implementation</td>
</tr>
</tbody>
</table>

Appendix A. Related protocol specifications 141
RFC 1044  Internet Protocol on Network System’s HYPERchannel: Protocol specification K. Hardwick, J. Lekashman
RFC 1053  Telnet X.3 PAD option S. Levy, T. Jacobson
RFC 1055  Nonstandard for transmission of IP datagrams over serial lines: SLIP J. Romkey
RFC 1058  Routing Information Protocol C. Hedrick
RFC 1060  Assigned numbers J. Reynolds, J. Postel
RFC 1071  Computing the Internet checksum R.T. Braden, D.A. Borman, C. Partridge
RFC 1072  TCP extensions for long-delay paths V. Jacobson, R.T. Braden
RFC 1073  Telnet window size option D. Waitzman
RFC 1079  Telnet terminal speed option C. Hedrick
RFC 1085  ISO presentation services on top of TCP/IP based internets M.T. Rose
RFC 1091  Telnet terminal-type option J. VanBokkelen
RFC 1094  NFS: Network File System Protocol specification Sun Microsystems
RFC 1096  Telnet X display location option G. Marcy
RFC 1101  DNS encoding of network names and other types P. Mockapetris
RFC 1112  Host extensions for IP multicasting S.E. Deering
RFC 1113  Privacy enhancement for Internet electronic mail: Part I — message encipherment and authentication procedures J. Linn
RFC 1118  Hitchhiker's Guide to the Internet E. Krol
RFC 1122  Requirements for Internet Hosts—Communication Layers R. Braden, Ed.
RFC 1123  Requirements for Internet Hosts—Application and Support R. Braden, Ed.
RFC 1146  TCP alternate checksum options J. Zweig, C. Partridge
RFC 1155  Structure and identification of management information for TCP/IP-based internets M. Rose, K. McCloghrie
RFC 1156  Management Information Base for network management of TCP/IP-based internets K. McCloghrie, M. Rose
RFC 1158  Management Information Base for network management of TCP/IP-based internets: MIB-II M. Rose
RFC 1166  Internet numbers S. Kirkpatrick, M.K. Stahl, M. Recker
RFC 1179  Line printer daemon protocol L. McLaughlin
RFC 1180  TCP/IP tutorial T. Socolofsky, C. Kale
RFC 1340  Assigned Numbers  J. Reynolds, J. Postel
RFC 1344  Implications of MIME for Internet Mail Gateways  N. Bornstein
RFC 1349  Type of Service in the Internet Protocol Suite  P. Almquist
RFC 1350  The TFTP Protocol (Revision 2)  K.R. Sollins
RFC 1351  SNMP Administrative Model  J. Davin, J. Galvin, K. McCloghrie
RFC 1352  SNMP Security Protocols  J. Galvin, K. McCloghrie, J. Davin
RFC 1353  Definitions of Managed Objects for Administration of SNMP Parties  K. McCloghrie, J. Davin, J. Galvin
RFC 1354  IP Forwarding Table MIB  F. Baker
RFC 1356  Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode  A. Malis, D. Robinson, R. Ullmann
RFC 1358  Charter of the Internet Architecture Board (IAB)  L. Chapin
RFC 1363  A Proposed Flow Specification  C. Partridge
RFC 1368  Definition of Managed Objects for IEEE 802.3 Repeater Devices  D. McMaster, K. McCloghrie
RFC 1372  Telnet Remote Flow Control Option  C. L. Hedrick, D. Borman
RFC 1374  IP and ARP on HIPPI  J. Renwick, A. Nicholson
RFC 1381  SNMP MIB Extension for X.25 LAPB  D. Throop, F. Baker
RFC 1382  SNMP MIB Extension for the X.25 Packet Layer  D. Throop
RFC 1387  RIP Version 2 Protocol Analysis  G. Malkin
RFC 1388  RIP Version 2 Carrying Additional Information  G. Malkin
RFC 1389  RIP Version 2 MIB Extensions  G. Malkin, F. Baker
RFC 1390  Transmission of IP and ARP over FDDI Networks  D. Katz
RFC 1393  Traceroute Using an IP Option  G. Malkin
RFC 1398  Definitions of Managed Objects for the Ethernet-Like Interface Types  F. Kastenholz
RFC 1408  Telnet Environment Option  D. Borman, Ed.
RFC 1413  Identification Protocol  M. St. Johns
RFC 1416  Telnet Authentication Option  D. Borman, ed.
RFC 1420  SNMP over IPX  S. Bostock
RFC 1428  Transition of Internet Mail from Just-Send-8 to 8bit-SMTP/MIME  G. Vaudreuil
RFC 1445  Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)  J. Galvin, K. McCloghrie
RFC 1447  Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)  K. McCloghrie, J. Galvin
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1464</td>
<td>Using the Domain Name System to Store Arbitrary String Attributes</td>
<td>R. Rosenbaum</td>
</tr>
<tr>
<td>RFC 1469</td>
<td>IP Multicast over Token-Ring Local Area Networks</td>
<td>T. Pusateri</td>
</tr>
<tr>
<td>RFC 1483</td>
<td>Multiprotocol Encapsulation over ATM Adaptation Layer 5</td>
<td>Juha Heinanen</td>
</tr>
<tr>
<td>RFC 1514</td>
<td>Host Resources MIB</td>
<td>P. Grillo, S. Waldbusser</td>
</tr>
<tr>
<td>RFC 1516</td>
<td>Definitions of Managed Objects for IEEE 802.3 Repeater Devices</td>
<td>D. McMaster, K. McCloghrie</td>
</tr>
<tr>
<td>RFC 1521</td>
<td>MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies</td>
<td>N. Borenstein, N. Freed</td>
</tr>
<tr>
<td>RFC 1535</td>
<td>A Security Problem and Proposed Correction With Widely Deployed DNS Software</td>
<td>E. Gavron</td>
</tr>
<tr>
<td>RFC 1536</td>
<td>Common DNS Implementation Errors and Suggested Fixes</td>
<td>A. Kumar, J. Postel, C. Neuman, P. Danzig, S. Miller</td>
</tr>
<tr>
<td>RFC 1537</td>
<td>Common DNS Data File Configuration Errors</td>
<td>P. Beertema</td>
</tr>
<tr>
<td>RFC 1540</td>
<td>Internet Official Protocol Standards</td>
<td>J. Postel</td>
</tr>
<tr>
<td>RFC 1571</td>
<td>Telnet Environment Option Interoperability Issues</td>
<td>D. Borman</td>
</tr>
<tr>
<td>RFC 1572</td>
<td>Telnet Environment Option</td>
<td>S. Alexander</td>
</tr>
<tr>
<td>RFC 1573</td>
<td>Evolution of the Interfaces Group of MIB-II</td>
<td>K. McCloghrie, F. Kastenholz</td>
</tr>
<tr>
<td>RFC 1577</td>
<td>Classical IP and ARP over ATM</td>
<td>M. Laubach</td>
</tr>
<tr>
<td>RFC 1583</td>
<td>OSPF Version 2</td>
<td>J. Moy</td>
</tr>
<tr>
<td>RFC 1591</td>
<td>Domain Name System Structure and Delegation</td>
<td>J. Postel</td>
</tr>
<tr>
<td>RFC 1594</td>
<td>FYI on Questions and Answers— Answers to Commonly Asked &quot;New Internet User&quot; Questions</td>
<td>A. Marine, J. Reynolds, G. Malkin</td>
</tr>
<tr>
<td>RFC 1644</td>
<td>T/TCP — TCP Extensions for Transactions Functional Specification</td>
<td>R. Braden</td>
</tr>
<tr>
<td>RFC 1646</td>
<td>TN3270 Extensions for LUname and Printer Selection</td>
<td>C. Graves, T. Butts, M. Angel</td>
</tr>
<tr>
<td>RFC 1647</td>
<td>TN3270 Enhancements</td>
<td>B. Kelly</td>
</tr>
<tr>
<td>RFC 1652</td>
<td>SMTP Service Extension for 8bit-MIMEtransport</td>
<td>J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker</td>
</tr>
<tr>
<td>RFC 1664</td>
<td>Using the Internet DNS to Distribute RFC1327 Mail Address Mapping Tables</td>
<td>C. Allochio, A. Bonito, B. Cole, S. Giordano, R. Hagens</td>
</tr>
<tr>
<td>RFC 1693</td>
<td>An Extension to TCP: Partial Order Service</td>
<td>T. Connolly, P. Amer, P. Conrad</td>
</tr>
<tr>
<td>RFC 1695</td>
<td>Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2</td>
<td>M. Ahmed, K. Tesink</td>
</tr>
<tr>
<td>RFC</td>
<td>Title</td>
<td>Authors</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>1701</td>
<td>Generic Routing Encapsulation (GRE)</td>
<td>S. Hanks, T. Li, D. Farinacci, P. Traina</td>
</tr>
<tr>
<td>1702</td>
<td>Generic Routing Encapsulation over IPv4 networks</td>
<td>S. Hanks, T. Li, D. Farinacci, P. Traina</td>
</tr>
<tr>
<td>1706</td>
<td>DNS NSAP Resource Records</td>
<td>B. Manning, R. Colella</td>
</tr>
<tr>
<td>1712</td>
<td>DNS Encoding of Geographical Location</td>
<td>C. Farrell, M. Schulze, S. Pleitner, D. Baldoni</td>
</tr>
<tr>
<td>1713</td>
<td>Tools for DNS debugging</td>
<td>A. Romao</td>
</tr>
<tr>
<td>1723</td>
<td>RIP Version 2—Carrying Additional Information</td>
<td>G. Malkin</td>
</tr>
<tr>
<td>1752</td>
<td>The Recommendation for the IP Next Generation Protocol</td>
<td>S. Bradner, A. Mankin</td>
</tr>
<tr>
<td>1766</td>
<td>Tags for the Identification of Languages</td>
<td>H. Alvestrand</td>
</tr>
<tr>
<td>1771</td>
<td>A Border Gateway Protocol 4 (BGP-4)</td>
<td>Y. Rekhter, T. Li</td>
</tr>
<tr>
<td>1794</td>
<td>DNS Support for Load Balancing</td>
<td>T. Brisco</td>
</tr>
<tr>
<td>1826</td>
<td>IP Authentication Header</td>
<td>R. Atkinson</td>
</tr>
<tr>
<td>1828</td>
<td>IP Authentication using Keyed MD5</td>
<td>P. Metzger, W. Simpson</td>
</tr>
<tr>
<td>1829</td>
<td>The ESP DES-CBC Transform</td>
<td>P. Karn, P. Metzger, W. Simpson</td>
</tr>
<tr>
<td>1830</td>
<td>SMTP Service Extensions for Transmission of Large and Binary MIME Messages</td>
<td>G. Vaudreuil</td>
</tr>
<tr>
<td>1832</td>
<td>XDR: External Data Representation Standard</td>
<td>R. Srinivasan</td>
</tr>
<tr>
<td>1833</td>
<td>Binding Protocols for ONC RPC Version 2</td>
<td>R. Srinivasan</td>
</tr>
<tr>
<td>1835</td>
<td>OSPF Version 2 Management Information Base</td>
<td>F. Baker, R. Coltun</td>
</tr>
<tr>
<td>1854</td>
<td>SMTP Service Extension for Command Pipelining</td>
<td>N. Freed</td>
</tr>
<tr>
<td>1869</td>
<td>SMTP Service Extensions</td>
<td>J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker</td>
</tr>
<tr>
<td>1870</td>
<td>SMTP Service Extension for Message Size Declaration</td>
<td>J. Klensin, N. Freed, K. Moore</td>
</tr>
<tr>
<td>1876</td>
<td>A Means for Expressing Location Information in the Domain Name System</td>
<td>C. Davis, P. Vixie, T. Goodwin, I. Dickinson</td>
</tr>
<tr>
<td>1883</td>
<td>Internet Protocol, Version 6 (IPv6) Specification</td>
<td>S. Deering, R. Hinden</td>
</tr>
<tr>
<td>1884</td>
<td>IP Version 6 Addressing Architecture</td>
<td>R. Hinden, S. Deering, Eds.</td>
</tr>
<tr>
<td>1886</td>
<td>DNS Extensions to support IP version</td>
<td>S. Thomson, C. Huitema</td>
</tr>
<tr>
<td>1888</td>
<td>OSI NSAPs and IPv6</td>
<td>J. Bound, B. Carpenter, D. Harrington, J. Houldsworth, A. Lloyd</td>
</tr>
<tr>
<td>1891</td>
<td>SMTP Service Extension for Delivery Status Notifications</td>
<td>K. Moore</td>
</tr>
<tr>
<td>1892</td>
<td>The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages</td>
<td>G. Vaudreuil</td>
</tr>
<tr>
<td>RFC</td>
<td>Title</td>
<td>Authors</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>1894</td>
<td>An Extensible Message Format for Delivery Status Notifications</td>
<td>K. Moore, G. Vaudreuil</td>
</tr>
<tr>
<td>1901</td>
<td>Introduction to Community-based SNMPv2</td>
<td>J. Case, K. McCloghrie, M. Rose, S. Waldbusser</td>
</tr>
<tr>
<td>1912</td>
<td>Common DNS Operational and Configuration Errors</td>
<td>D. Barr</td>
</tr>
<tr>
<td>1918</td>
<td>Address Allocation for Private Internets</td>
<td>Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear</td>
</tr>
<tr>
<td>1930</td>
<td>Guidelines for creation, selection, and registration of an Autonomous System (AS)</td>
<td>J. Hawkinson, T. Bates</td>
</tr>
<tr>
<td>1939</td>
<td>Post Office Protocol-Version 3</td>
<td>J. Myers, M. Rose</td>
</tr>
<tr>
<td>1981</td>
<td>Path MTU Discovery for IP version 6</td>
<td>J. McCann, S. Deering, J. Mogul</td>
</tr>
<tr>
<td>1982</td>
<td>Serial Number Arithmetic</td>
<td>R. Elz, R. Bush</td>
</tr>
<tr>
<td>1985</td>
<td>SMTP Service Extension for Remote Message Queue Starting</td>
<td>J. De Winter</td>
</tr>
<tr>
<td>1995</td>
<td>Incremental Zone Transfer in DNS</td>
<td>M. Ohta</td>
</tr>
<tr>
<td>1996</td>
<td>A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)</td>
<td>P. Vixie</td>
</tr>
<tr>
<td>2010</td>
<td>Operational Criteria for Root Name Servers</td>
<td>B. Manning, P. Vixie</td>
</tr>
<tr>
<td>2011</td>
<td>SNMPv2 Management Information Base for the Internet Protocol using SMIv2</td>
<td>K. McCloghrie, Ed.</td>
</tr>
<tr>
<td>2013</td>
<td>SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2</td>
<td>K. McCloghrie, Ed.</td>
</tr>
<tr>
<td>RFC 2018</td>
<td>TCP Selective Acknowledgement Options M. Mathis, J. Mahdavi, S. Floyd, A. Romanow</td>
<td></td>
</tr>
<tr>
<td>RFC 2026</td>
<td>The Internet Standards Process — Revision 3 S. Bradner</td>
<td></td>
</tr>
<tr>
<td>RFC 2033</td>
<td>Local Mail Transfer Protocol J. Myers</td>
<td></td>
</tr>
<tr>
<td>RFC 2034</td>
<td>SMTP Service Extension for Returning Enhanced Error Codes N. Freed</td>
<td></td>
</tr>
<tr>
<td>RFC 2045</td>
<td>Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies N. Freed, N. Borenstein</td>
<td></td>
</tr>
<tr>
<td>RFC 2052</td>
<td>A DNS RR for specifying the location of services (DNS SRV) A. Gulbrandsen, P. Vixie</td>
<td></td>
</tr>
<tr>
<td>RFC 2065</td>
<td>Domain Name System Security Extensions D. Eastlake 3rd, C. Kaufman</td>
<td></td>
</tr>
<tr>
<td>RFC 2066</td>
<td>TELNET CHARSET Option R. Gellens</td>
<td></td>
</tr>
<tr>
<td>RFC 2080</td>
<td>RIPng for IPv6 G. Malkin, R. Minnear</td>
<td></td>
</tr>
<tr>
<td>RFC 2096</td>
<td>IP Forwarding Table MIB F. Baker</td>
<td></td>
</tr>
<tr>
<td>RFC 2104</td>
<td>HMAC: Keyed-Hashing for Message Authentication H. Krawczyk, M. Bellare, R. Canetti</td>
<td></td>
</tr>
<tr>
<td>RFC 2119</td>
<td>Keywords for use in RFCs to Indicate Requirement Levels S. Bradner</td>
<td></td>
</tr>
<tr>
<td>RFC 2133</td>
<td>Basic Socket Interface Extensions for IPv6 R. Gilligan, S. Thomson, J. Bound, W. Stevens</td>
<td></td>
</tr>
<tr>
<td>RFC 2136</td>
<td>Dynamic Updates in the Domain Name System (DNS UPDATE) P. Vixie, Ed., S. Thomson, Y. Rekhter, J. Bound</td>
<td></td>
</tr>
<tr>
<td>RFC 2137</td>
<td>Secure Domain Name System Dynamic Update D. Eastlake 3rd</td>
<td></td>
</tr>
<tr>
<td>RFC 2163</td>
<td>Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM) C. Allocchio</td>
<td></td>
</tr>
<tr>
<td>RFC 2168</td>
<td>Resolution of Uniform Resource Identifiers using the Domain Name System R. Daniel, M. Mealling</td>
<td></td>
</tr>
<tr>
<td>RFC 2178</td>
<td>OSPF Version 2 J. Moy</td>
<td></td>
</tr>
<tr>
<td>RFC 2181</td>
<td>Clarifications to the DNS Specification R. Elz, R. Bush</td>
<td></td>
</tr>
<tr>
<td>RFC 2210</td>
<td>The Use of RSVP with IETF Integrated Services J. Wroclawski</td>
<td></td>
</tr>
<tr>
<td>RFC 2211</td>
<td>Specification of the Controlled-Load Network Element Service J. Wroclawski</td>
<td></td>
</tr>
<tr>
<td>RFC 2212</td>
<td>Specification of Guaranteed Quality of Service S. Shenker, C. Partridge, R. Guerin</td>
<td></td>
</tr>
<tr>
<td>RFC 2215</td>
<td>General Characterization Parameters for Integrated Service Network Elements S. Shenker, J. Wroclawski</td>
<td></td>
</tr>
<tr>
<td>RFC 2217</td>
<td>Telnet Com Port Control Option G. Clarke</td>
<td></td>
</tr>
</tbody>
</table>
RFC 2389  Feature negotiation mechanism for the File Transfer Protocol P. Hethmon, R. Elz
RFC 2401  Security Architecture for Internet Protocol S. Kent, R. Atkinson
RFC 2402  IP Authentication Header S. Kent, R. Atkinson
RFC 2403  The Use of HMAC-MD5–96 within ESP and AH C. Madson, R. Glenn
RFC 2404  The Use of HMAC-SHA–1–96 within ESP and AH C. Madson, R. Glenn
RFC 2405  The ESP DES-CBC Cipher Algorithm With Explicit IV C. Madson, N. Doraswamy
RFC 2406  IP Encapsulating Security Payload (ESP) S. Kent, R. Atkinson
RFC 2407  The Internet IP Security Domain of Interpretation for ISAKMPD. Piper
RFC 2409  The Internet Key Exchange (IKE) D. Harkins, D. Carrel
RFC 2410  The NULL Encryption Algorithm and Its Use With IPsec R. Glenn, S. Kent,
RFC 2428  FTP Extensions for IPv6 and NATs M. Allman, S. Ostermann, C. Metz
RFC 2445  Internet Calendaring and Scheduling Core Object Specification (iCalendar) F. Dawson, D. Stenerson
RFC 2459  Internet X.509 Public Key Infrastructure Certificate and CRL Profile R. Housley, W. Ford, W. Polk, D. Solo
RFC 2460  Internet Protocol, Version 6 (IPv6) Specification S. Deering, R. Hinden
RFC 2462  IPv6 Stateless Address Autoconfiguration S. Thomson, T. Narten
RFC 2463  Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification A. Conta, S. Deering
RFC 2464  Transmission of IPv6 Packets over Ethernet Networks M. Crawford
RFC 2476  Message Submission R. Gellens, J. Klensin
RFC 2487  SMTP Service Extension for Secure SMTP over TLS P. Hoffman
RFC 2505  Anti-Spam Recommendations for SMTP MTAs G. Lindberg
RFC 2523  Phat: Phat and Attributes P. Karn, W. Simpson
RFC 2535  Domain Name System Security Extensions D. Eastlake 3rd
RFC 2538  Storing Certificates in the Domain Name System (DNS) D. Eastlake 3rd, O. Gudmundsson
RFC 2539  Storage of Diffie-Hellman Keys in the Domain Name System (DNS) D. Eastlake 3rd
RFC 2540  Detached Domain Name System (DNS) Information D. Eastlake 3rd
RFC 2554  SMTP Service Extension for Authentication J. Myers
Appendix A. Related protocol specifications

RFC 2570  Introduction to Version 3 of the Internet-standard Network Management Framework J. Case, R. Mundy, D. Partain, B. Stewart
RFC 2573  SNMP Applications D. Levi, P. Meyer, B. Stewart
RFC 2575  View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) B. Wijnen, R. Presuhn, K. McCloghrie
RFC 2579  Textual Conventions for SMIv2 K. McCloghrie, D. Perkins, J. Schoenwaelder
RFC 2580  Conformance Statements for SMIv2 K. McCloghrie, D. Perkins, J. Schoenwaelder
RFC 2581  TCP Congestion Control M. Allman, V. Paxson, W. Stevens
RFC 2583  Guidelines for Next Hop Client (NHC) Developers R. Carlson, L. Winkler
RFC 2591  Definitions of Managed Objects for Scheduling Management Operations D. Levi, J. Schoenwaelder
RFC 2625  IP and ARP over Fibre Channel M. Rajagopalan, R. Bhagwat, W. Rickard
RFC 2635  Don’t SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*) S. Hambridge, A. Lunde
RFC 2640  Internationalization of the File Transfer Protocol B. Curtin
RFC 2665  Definitions of Managed Objects for the Ethernet-like Interface Types J. Flick, J. Johnson
RFC 2671  Extension Mechanisms for DNS (EDNS0) P. Vixie
RFC 2672  Non-Terminal DNS Name Redirection M. Crawford
RFC 2675  IPv6 Jumbograms D. Borman, S. Deering, R. Hinden
RFC 2710  Multicast Listener Discovery (MLD) for IPv6 S. Deering, W. Fenner, B. Haberman
RFC 2711  IPv6 Router Alert Option C. Partridge, A. Jackson
RFC 2740  OSPF for IPv6 R. Coltun, D. Ferguson, J. Moy
RFC 2753  A Framework for Policy-based Admission Control R. Yavatkar, D. Pendarakis, R. Guerin
RFC 2782  A DNS RR for specifying the location of services (DNS SRV) A.
        Gubrandsen, P. Vixix, L. Esibov
RFC 2821  Simple Mail Transfer Protocol J. Klensin, Ed.
RFC 2822  Internet Message Format P. Resnick, Ed.
RFC 2840  TELNET KERMIT OPTION J. Altman, F. da Cruz
RFC 2845  Secret Key Transaction Authentication for DNS (TSIG) P. Vixie, O.
        Gudmundsson, D. Eastlake 3rd, B. Wellington
RFC 2851  Textual Conventions for Internet Network Addresses M. Daniele, B.
        Haberman, S. Routhier, J. Schoenwaelder
RFC 2852  Deliver By SMTP Service Extension D. Newman
RFC 2874  DNS Extensions to Support IPv6 Address Aggregation and Renumbering
        M. Crawford, C. Huitema
RFC 2915  The Naming Authority Pointer (NAPTR) DNS Resource Record M.
        Mealling, R. Daniel
RFC 2920  SMTP Service Extension for Command Pipelining N. Freed
RFC 2930  Secret Key Establishment for DNS (TKEY RR) D. Eastlake, 3rd
RFC 2941  Telnet Authentication Option T. Ts’o, ed., J. Altman
RFC 2942  Telnet Authentication: Kerberos Version 5 T. Ts’o
RFC 2946  Telnet Data Encryption Option T. Ts’o
RFC 2952  Telnet Encryption: DES 64 bit Cipher Feedback T. Ts’o
RFC 2953  Telnet Encryption: DES 64 bit Output Feedback T. Ts’o
RFC 2992  Analysis of an Equal-Cost Multi-Path Algorithm C. Hopps
RFC 3019  IP Version 6 Management Information Base for The Multicast Listener
        Discovery Protocol B. Haberman, R. Worzella
RFC 3060  Policy Core Information Model—Version 1 Specification B. Moore, E.
        Ellesson, J. Strassner, A. Westerinen
RFC 3152  Delegation of IP6.ARPA R. Bush
RFC 3164  The BSD Syslog Protocol C. Lonvick
RFC 3207  SMTP Service Extension for Secure SMTP over Transport Layer Security
        P. Hoffman
RFC 3226  DNSSEC and IPv6 A6 aware server/resolver message size requirements
        O. Gudmundsson
RFC 3291  Textual Conventions for Internet Network Addresses M. Daniele, B.
        Haberman, S. Routhier, J. Schoenwaelder
RFC 3363  Representing Internet Protocol version 6 (IPv6) Addresses in the Domain
        Name System R. Bush, A. Durand, B. Fink, O. Gudmundsson, T.
        Hain
RFC 3376  Internet Group Management Protocol, Version 3 B. Cain, S. Deering, I.
        Kouvelas, B. Fenner, A. Thyagarajan
RFC 3390  Increasing TCP’s Initial Window M. Allman, S. Floyd, C. Partridge
RFC 3410  Introduction and Applicability Statements for Internet-Standard
        Management Framework J. Case, R. Mundy, D. Partain, B. Stewart
Appendix A. Related protocol specifications
Internet drafts

Internet drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Other groups may also distribute working documents as Internet drafts. You can see Internet drafts at [http://www.ietf.org/ID.html](http://www.ietf.org/ID.html)

Several areas of IPv6 implementation include elements of the following Internet drafts and are subject to change during the RFC review process.
Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification A. Conta, S. Deering
Appendix B. Architectural specifications

This appendix lists documents that provide architectural specifications for the SNA Protocol.

The APPN Implementers’ Workshop (AIW) architecture documentation includes the following architectural specifications for SNA APPN and HPR:

- APPN Architecture Reference (SG30-3422-04)
- APPN Branch Extender Architecture Reference Version 1.1
- APPN Dependent LU Requester Architecture Reference Version 1.5
- APPN Extended Border Node Architecture Reference Version 1.0
- APPN High Performance Routing Architecture Reference Version 4.0
- SNA Formats (GA27-3136-20)
- SNA Technical Overview (GC30-3073-04)

For more information, refer to the AIW documentation page at http://www.networking.ibm.com/app/aiwdoc.htm.

The following RFC also contains SNA architectural specifications:

- RFC 2353 APPN/HPR in IP Networks APPN Implementers’ Workshop Closed Pages Document

RFCs can be obtained from:

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

Many RFCs are available online. Hardcopies of all RFCs are available from the NIC, either individually or by subscription. Online copies are available using FTP from the NIC at [http://www.rfc-editor.org/rfc.html](http://www.rfc-editor.org/rfc.html).

Use FTP to download the files, using the following format:

RFC:RFC-INDEX.TXT
RFC:RFCnnnn.TXT
RFC:RFCnnnn.PS

where:

- *nnnn* is the RFC number.
- *TXT* is the text format.
- *PS* is the postscript format.

You can also request RFCs through electronic mail, from the automated NIC mail server, by sending a message to service@nic.ddn.mil with a subject line of RFC *nnnn* for text versions or a subject line of RFC *nnnn*.PS for PostScript® versions. To request a copy of the RFC index, send a message with a subject line of RFC INDEX.

For more information, contact nic@nic.ddn.mil.
Appendix C. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to z/OS TSO/E Primer, z/OS TSO/E User’s Guide, and z/OS ISPF User’s Guide Vol I for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer/Library Server versions of z/OS books in the Internet library at [www.ibm.com/systems/z/os/zos/bkserv/](http://www.ibm.com/systems/z/os/zos/bkserv/)
Notices

IBM may not offer all of the products, services, or features discussed in this document. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.
Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Site Counsel
IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, North Carolina 27709-2195
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application
programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

IBM is required to include the following statements in order to distribute portions of this document and the software described herein to which contributions have been made by The University of California. Portions herein © Copyright 1979, 1980, 1983, 1986, Regents of the University of California. Reproduced by permission. Portions herein were developed at the Electrical Engineering and Computer Sciences Department at the Berkeley campus of the University of California under the auspices of the Regents of the University of California.

Portions of this publication relating to RPC are Copyright © Sun Microsystems, Inc., 1988, 1989.

Some portions of this publication relating to X Window System** are Copyright © 1987, 1988 by Digital Equipment Corporation, Maynard, Massachusetts, and the Massachusetts Institute Of Technology, Cambridge, Massachusetts. All Rights Reserved.

Some portions of this publication relating to X Window System are Copyright © 1986, 1987, 1988 by Hewlett-Packard Corporation.

Permission to use, copy, modify, and distribute the M.I.T., Digital Equipment Corporation, and Hewlett-Packard Corporation portions of this software and its documentation for any purpose without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of M.I.T., Digital, and Hewlett-Packard not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T., Digital, and Hewlett-Packard make no representation about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.


Copyright © 1988, 1993 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this
   list of conditions and the following disclaimer in the documentation and/or
   other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must
   display the following acknowledgement:
   This product includes software developed by the University of
   California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be
   used to endorse or promote products derived from this software without
   specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software program contains code, and/or derivatives or modifications of code originating from the software program "Popper." Popper is Copyright ©1989-1991 The Regents of the University of California, All Rights Reserved. Popper was created by Austin Shelton, Information Systems and Technology, University of California, Berkeley.

Permission from the Regents of the University of California to use, copy, modify, and distribute the "Popper" software contained herein for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies. HOWEVER, ADDITIONAL PERMISSIONS MAY BE NECESSARY FROM OTHER PERSONS OR ENTITIES, TO USE DERIVATIVES OR MODIFICATIONS OF POPPER.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THE POPPER SOFTWARE, OR ITS DERIVATIVES OR MODIFICATIONS, AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE POPPER SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

Copyright © 1983 The Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright © 1991, 1993 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright © 1990 by the Massachusetts Institute of Technology

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore
if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original M.I.T. software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright © 1998 by the FundsXpress, INC. All rights reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of FundsXpress not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. FundsXpress makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.


Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be
given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include acknowledgement:
   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

This product includes cryptographic software written by Eric Young.


Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks of other companies:

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

PostScript is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

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

Other company, product, or service names may be trademarks or service marks of others.
Bibliography

This bibliography contains descriptions of the documents in the z/OS Communications Server library.

z/OS Communications Server documentation is available in the following forms:

- In softcopy on CD-ROM collections. See “Softcopy information” on page xiv.

z/OS Communications Server library updates


z/OS Communications Server information

z/OS Communications Server product information is grouped by task in the following tables.

### Planning

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS Communications Server: New Function Summary</td>
<td>GC31-8771</td>
<td>This document is intended to help you plan for new IP for SNA function, whether you are migrating from a previous version or installing z/OS for the first time. It summarizes what is new in the release and identifies the suggested and required modifications needed to use the enhanced functions.</td>
</tr>
<tr>
<td>z/OS Communications Server: IPv6 Network and Application Design Guide</td>
<td>SC31-8885</td>
<td>This document is a high-level introduction to IPv6. It describes concepts of z/OS Communications Server’s support of IPv6, coexistence with IPv4, and migration issues.</td>
</tr>
</tbody>
</table>

### Resource definition, configuration, and tuning

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS Communications Server: IP Configuration Guide</td>
<td>SC31-8775</td>
<td>This document describes the major concepts involved in understanding and configuring an IP network. Familiarity with the z/OS operating system, IP protocols, z/OS UNIX System Services, and IBM Time Sharing Option (TSO) is recommended. Use this document in conjunction with the z/OS Communications Server: IP Configuration Reference</td>
</tr>
</tbody>
</table>

© Copyright IBM Corp. 2004, 2009
<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
</table>
| z/OS Communications Server: IP Configuration Reference | SC31-8776  | This document presents information for people who want to administer and maintain IP. Use this document in conjunction with the [z/OS Communications Server: IP Configuration Guide](#). The information in this document includes:  
  - TCP/IP configuration data sets  
  - Configuration statements  
  - Translation tables  
  - SMF records  
  - Protocol number and port assignments |
| z/OS Communications Server: SNA Network Implementation Guide | SC31-8777  | This document presents the major concepts involved in implementing an SNA network. Use this document in conjunction with the [z/OS Communications Server: SNA Resource Definition Reference](#). |
| z/OS Communications Server: SNA Resource Definition Reference | SC31-8778  | This document describes each SNA definition statement, start option, and macroinstruction for user tables. It also describes NCP definition statements that affect SNA. Use this document in conjunction with the [z/OS Communications Server: SNA Network Implementation Guide](#). |
| z/OS Communications Server: SNA Resource Definition Samples | SC31-8836  | This document contains sample definitions to help you implement SNA functions in your networks, and includes sample major node definitions. |
| z/OS Communications Server: IP Network Print Facility | SC31-8833  | This document is for system programmers and network administrators who need to prepare their network to route SNA, JES2, or JES3 printer output to remote printers using TCP/IP Services. |

### Operation

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS Communications Server: IP User's Guide and Commands</td>
<td>SC31-8780</td>
<td>This document describes how to use TCP/IP applications. It contains requests that allow a user to log on to a remote host using Telnet, transfer data sets using FTP, send and receive electronic mail, print on remote printers, and authenticate network users.</td>
</tr>
<tr>
<td>z/OS Communications Server: IP System Administrator's Commands</td>
<td>SC31-8781</td>
<td>This document describes the functions and commands helpful in configuring or monitoring your system. It contains system administrator’s commands, such as TSO NETSTAT, PING, TRACERTE and their UNIX counterparts. It also includes TSO and MVS commands commonly used during the IP configuration process.</td>
</tr>
<tr>
<td>z/OS Communications Server: SNA Operation</td>
<td>SC31-8779</td>
<td>This document serves as a reference for programmers and operators requiring detailed information about specific operator commands.</td>
</tr>
<tr>
<td>z/OS Communications Server: Quick Reference</td>
<td>SX75-0124</td>
<td>This document contains essential information about SNA and IP commands.</td>
</tr>
</tbody>
</table>
## Customization

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS Communications Server:</td>
<td>SC31-6854</td>
<td>This document enables you to customize SNA, and includes the following:</td>
</tr>
<tr>
<td>SNA Customization</td>
<td></td>
<td>• Communication network management (CNM) routing table</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Logon-interpret routine requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Logon manager installation-wide exit routine for the CLU search exit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TSO/SNA installation-wide exit routines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SNA installation-wide exit routines</td>
</tr>
</tbody>
</table>

## Writing application programs

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS Communications Server:</td>
<td>SC31-8788</td>
<td>This document describes the syntax and semantics of program source code necessary to write your own application programming interface (API) into TCP/IP. You can use this interface as the communication base for writing your own client or server application. You can also use this document to adapt your existing applications to communicate with each other using sockets over TCP/IP.</td>
</tr>
<tr>
<td>IP Sockets Application Programming Interface Guide and Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z/OS Communications Server:</td>
<td>SC31-8807</td>
<td>This document is for programmers who want to set up, write application programs for, and diagnose problems with the socket interface for CICS using z/OS TCP/IP.</td>
</tr>
<tr>
<td>IP CICS Sockets Guide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z/OS Communications Server:</td>
<td>SC31-8830</td>
<td>This document is for programmers who want application programs that use the IMS TCP/IP application development services provided by IBM's TCP/IP Services.</td>
</tr>
<tr>
<td>IP IMS Sockets Guide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z/OS Communications Server:</td>
<td>SC31-8787</td>
<td>This document describes the syntax and semantics of a set of high-level application functions that you can use to program your own applications in a TCP/IP environment. These functions provide support for application facilities, such as user authentication, distributed databases, distributed processing, network management, and device sharing. Familiarity with the z/OS operating system, TCP/IP protocols, and IBM Time Sharing Option (TSO) is recommended.</td>
</tr>
<tr>
<td>IP Programmer’s Guide and Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z/OS Communications Server:</td>
<td>SC31-8829</td>
<td>This document describes how to use SNA macroinstructions to send data to and receive data from (1) a terminal in either the same or a different domain, or (2) another application program in either the same or a different domain.</td>
</tr>
<tr>
<td>SNA Programming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z/OS Communications Server:</td>
<td>SC31-8811</td>
<td>This document describes how to use the SNA LU 6.2 application programming interface for host application programs. This document applies to programs that use only LU 6.2 sessions or that use LU 6.2 sessions along with other session types. (Only LU 6.2 sessions are covered in this document.)</td>
</tr>
<tr>
<td>SNA Programmer’s LU 6.2 Guide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z/OS Communications Server:</td>
<td>SC31-8810</td>
<td>This document provides reference material for the SNA LU 6.2 programming interface for host application programs.</td>
</tr>
<tr>
<td>SNA Programmer’s LU 6.2 Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z/OS Communications Server:</td>
<td>SC31-8808</td>
<td>This document describes how applications use the communications storage manager.</td>
</tr>
<tr>
<td>CSM Guide</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### z/OS Communications Server: CMIP Services and Topology Agent Guide

**Description:** This document describes the Common Management Information Protocol (CMIP) programming interface for application programmers to use in coding CMIP application programs. The document provides guideline and reference information about CMIP services and the SNA topology agent.

### Diagnosis

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS Communications Server: IP Diagnosis Guide</td>
<td>GC31-8782</td>
<td>This document explains how to diagnose TCP/IP problems and how to determine whether a specific problem is in the TCP/IP product code. It explains how to gather information and describe problems to the IBM Software Support Center.</td>
</tr>
<tr>
<td>z/OS Communications Server: ACF/TAP Trace Analysis Handbook</td>
<td>GC23-8588</td>
<td>This document explains how to gather the trace data that is collected and stored in the host processor. It also explains how to use the Advanced Communications Function/Trace Analysis Program (ACF/TAP) service aid to produce reports for analyzing the trace data information.</td>
</tr>
<tr>
<td>z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures and SNA Diagnosis Vol 2, FFST Dumps and the VIT</td>
<td>GC31-6850, GC31-6851</td>
<td>These documents help you identify an SNA problem, classify it, and collect information about it before you call the IBM Support Center. The information collected includes traces, dumps, and other problem documentation.</td>
</tr>
<tr>
<td>z/OS Communications Server: SNA Data Areas Volume 1 and SNA Data Areas Volume 2</td>
<td>GC31-6852, GC31-6853</td>
<td>These documents describe SNA data areas and can be used to read an SNA dump. They are intended for IBM programming service representatives and customer personnel who are diagnosing problems with SNA.</td>
</tr>
</tbody>
</table>

### Messages and codes

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
</table>
| z/OS Communications Server: SNA Messages        | SC31-8790 | This document describes the ELM, IKT, IST, IUT, IVT, and USS messages. Other information in this document includes:
- Command and RU types in SNA messages
- Node and ID types in SNA messages
- Supplemental message-related information |
| z/OS Communications Server: IP Messages Volume 1 (EZA) | SC31-8783 | This volume contains TCP/IP messages beginning with EZA. |
| z/OS Communications Server: IP Messages Volume 2 (EZB, EZD) | SC31-8784 | This volume contains TCP/IP messages beginning with EZB or EZD. |
| z/OS Communications Server: IP Messages Volume 3 (EZY) | SC31-8785 | This volume contains TCP/IP messages beginning with EZY. |
| z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM) | SC31-8786 | This volume contains TCP/IP messages beginning with EZZ and SNM. |
| z/OS Communications Server: IP and SNA Codes     | SC31-8791 | This document describes codes and other information that appear in z/OS Communications Server messages. |
Index

Numerics
4301 compliance, IBM Health Checker for z/OS RFC 64
64-bit shared memory 107

A
accelerator, QDIO routing 46
accelerator, sysplex distributor connection routing 48
accept_and_recv socket API 41
access control, port 77
access service, NSS SAF 73
accessibility 159
ACF/SSP 63
ACF/TAP 63
adaptive rate-based (ARB) flow control algorithm, progressive-mode 59
address autoconfiguration, IPv6 stateless 36
Advanced Communications Function/Trace Analysis Program (ACF/TAP) 63
agent, VTAM topology 11
AioCommBuff bit 107
algorithm, progressive-mode adaptive rate-based (ARB) flow control 59
algorithms, WLM routing 40
analyzer data, OSA network traffic 66
APAR OA26490 60
API timeout support, socket 105
API to obtain IPv4 network interface MTU 38
API, accept_and_recv socket 41
appliances, IBM WebSphere DataPower 49
application definition, dynamic 58
applications, tier 1 and tier 2 48
APPN
default COS 11
default transmission groups 11
APPN topology database update (TDU) processing 62
archival of z/OS UNIX files 53
ASID reuse for TCP/IP, TN3270E, and resolver 118
Asynchronous Socket I/O option 107
AT-TLS 84
AT-TLS dependent applications, autolog support for 88
AT-TLS enhancements 52
attacks, defensive filtering 74
AUTHNETS 129
autoconfiguration, IPv6 stateless address 36
autolog support for AT-TLS dependent applications 88

B
balancing, workload 49
banner for otelnetd, pre-logon 35
batch pipe subsystem, FTP 123
BIND 4.9.3 DNS server support 25, 71
BIND 9 server, DNS 117
BIND9 DNS server 57
BINL support 25, 71
BPX.SUPERUSER authorization 117
browser and search facilities, syslogd 54
buffer size, deadlock caused by insufficient TCP receive 42
building dynamic application definition 58

C
cache enhancements for WebSphere Application Server, FRCA 103
cache, resolver DNS 45
Callable NMI, GetProfile request for the TCP/IP 64
certificate services for XML appliances 44
check, migration health 64
CICS sockets interface and listener 39
client for sending Internet mail, SMTP 26
code page, EBCDIC 55
commands, z/OS UNIX shell 57
Communications Server for z/OS, online information xvi
communications, TCP/IP 72
compliance, IBM Health Checker for z/OS RFC 4301 64
Configuration Assistant and IP address groups 100
Configuration Assistant and Policy Agent 99
Configuration Assistant enhancements 53
configuration data, stack 64
connection isolation 69
deadlock caused by insufficient TCP receive buffer size 42
defensive filtering 74
definition, dynamic application 58
delayed TCP acknowledgements, traffic stalls caused by Nagle algorithms 42
DELAYSTART parameter 88
deprecation of IPv6 type 0 route header 38
DHCP support 25, 71
disability 159
DISPLAY MODELS command 58
displaying FTP space statistics for volumes 33
DISTMETHOD SERVERWLM statement 40
distribution library data sets 4
DLC layer, forwarding at the 46
DNET command 136
DNS BIND 9 server 117
dns cache, resolver 45
dns server, BIND9 57
dns, online information xvii
domain name servers 25
DSWAITTIME 124
dump processing, VTAM INOP 58
dVIPA information provided by EZBNMIFR 67
dVIPAs in MOVING state 40
dynamic application definition 58

E
EBCDIC code page support 55
echo reply packets, displaying 68
ECSA consumption 72
ECSA reduction, TN3270E Telnet server 72, 129
ECSA storage constraint relief 43
ECSA storage relief 39
EDNS0, Resolver support for 120
EE model PUs, TGN parameter for 130
encryption features 2
Enterprise Extender 108, 128
Enterprise Extender IPSec performance improvements 44
event record, SMF 119 64
execution server, MVS remote 35
extended border node searching 129
EZACMD command 57
EZBNMIFR 102
EZBNMIFR and request types 67

F
files, archival of z/OS UNIX 53
filtering, defensive 74
firewall 33
flow control algorithm, progressive-mode adaptive rate-based (ARB) 59
formatting trace information 63
forwarding at the DLC layer 46
fragmentation, IP packet 108
FRCA cache enhancements for WebSphere Application Server 103
FTP access to UNIX named pipes 28
FTP application data 120
FTP batch pipe subsystem 123
FTP client API for Java 121
FTP JES 122
FTP keepalive 125
FTP passive mode 33
FTP reports 33
FTP security 81
FWFRIENDLY parameter 34

G
GetProfile request 64
GetProfile request for the TCP/IP Callable NMI 64
GLOBALCONFIG profile statement, WLMPRIORITYQ parameter 68

H
Health Checker for z/OS migration health check, z/OS 57
Health Checker for z/OS RFC 4301 compliance, IBM 64
health of a server application 46
HFS (hierarchical file system) parts for z/OS Communications Server 4
high performance routing (HPR) performance 59
HiperSockets and routing acceleration 46
HiperSockets multiple write facility 96
HiperSockets, storage conditions 39
host name configuration problems, TCP/IP 113
HPR 131, 132, 133
IBM Health Checker for z/OS 109
IBM Health Checker for z/OS RFC 4301 compliance 64
IBM Software Support Center, contacting xiii
IBM WebSphere DataPower appliances 49
IBMTGPS file (APPN) 11
IKE daemon's retransmission scheme 51
ILWEIGHTING parameter 40
inbound packets, forwarding 46
Information APARs xiv
INOP dump processing 58
interface isolation, QDIO support for OSA 69
INTERFACE statement support for QDIO 94
Internet Key Exchange version 2 (IKEv2) 75
Internet mail, SMTP client for sending 26
Internet, finding z/OS information online xvi
IP addressing 100
IP packet fragmentation 108
IP security 102
IPSec support of VTAM display commands 136
IPSec cryptography performance 72
IPSec enhancements 51
IPSec performance improvements, Enterprise Extender 44
IPSec RFC currency 75
IPv4 network interface MTU 38
IPv6 addresses, temporary 36
IPv6 stateless address autoconfiguration 36
IPv6 type 0 route header, RFC 5005 deprecation 38
IPv6, RTHDR option 38
isolation, QDIO support for OSA interface 69
ISPF-based syslog daemon browser application 54
Java, FTP client API for 121
JESGETDYDSN option 122
keepalive, FTP 125
keyboard 159

L
latency mode, OSA-Express3 optimized 50
license, patent, and copyright information 161
Load Balancing Advisor and Agent 92
Load Balancing Advisor, TLS/SSL enablement for 83
load modules 42
log messages, processing of 53
LOGONHERE parameter 36
LookAt xiv
LU name coordination in a sysplex, TN3270E Telnet server 89
mail, SMTP client for sending Internet 26
mainframe
  education xiv
managing security 74
mapping of Workload Manager (WLM) service classes to
outbound Queued Direct I/O (QDIO) priorities 68
MAXLOCAT start option 134
memory, 64-bit shared 107
message transfer agent (MTA), target 26
messages, processing of log 53
migration health check 64
migration health check, z/OS Health Checker for z/OS 57
MOVING DVIPAs 40
msg_waitall 42
MTA (target message transfer agent) 26
MTU size changes 108
MTU, API to obtain IPv4 network interface 38
multi-port support for SNA, OSA-Express3 137
multi-tier z/OS workloads, sysplex distributor
  optimization 48
multilevel secure (MLS) environment 77
multiple port support 98
multiple VLAN support 95
multiple write facility, HiperSockets 96
MVS console support 57
MVS data sets 4
MVS remote execution server 35
MVS, installing VTAM under 7

Nagle algorithms and delayed TCP acknowledgements 42
named pipes, FTP access to UNIX 28
NAT firewall 33
NDB support 25, 71
Netstat report 25
Netstat report of network interface MTU 38
network management interface and detailed CSM usage 65
network security services 73
network traffic analyzer data, OSA 66
NMI and IP security 102
NMI timestamps 102
NMI, GetProfile request for the TCP/IP Callable 64
NSS private key and certificate services for XML
  appliances 44
NSS SAF access service 73

O/S data sets used by VTAM 7
OA26490, APAR 60
OMPROUTE 25, 111
OMPROUTE processing 39
optimization for multi-tier z/OS workloads, sysplex
distributor 48
optimized latency mode, OSA-Express3 50
OPTLOCAL 48
OSA interface isolation 69
OSA network traffic analyzer data 66
OSA-Express feature and multiple VLAN support 95
OSA-Express in QDIO mode, storage conditions 39
OSA-Express QDIO and routing acceleration 46
OSA-Express3 feature 98
OSA-Express3 multi-port support for SNA 137
OSA-Express3 optimized latency mode 50
OSPF 25
otelnetd 35
ownership statistics, storage 65

packet flow between OSA devices 69
packet fragmentation, IP 108
packet tracing 115
packets, echo reply 68
packets, forwarding 46
PASSIVEIGNOREADDR configuration option 33
PASV reply 33
path MTU discovery 108, 128
path switches 59
pathlength, TCP/IP 42
performance, TCP/IP 72
Ping command, displaying echo details 68
pipes, FTP access to UNIX named 28
planning checklist 3
Policy Agent and Configuration Assistant 99
Policy Agent, monitoring applications 55
Policy Agent, security and connections 87
Policy Agent, traffic regulation policy in 87
policy filter rules 75
policy server connections 87
port access control 77
pre-logon banner for otelnetd 35
pre-requisite information xiv
priorities and mapping 68
processing of log messages and syslogd 53
processing, APPN topology database update (TDU) 62
PROCXCOST parameter 40
progressive-mode adaptive rate-based (ARB) flow control
  algorithm 59
PUs, TGN parameter for EE model 130

QDIO mode 98
QDIO mode, OSA-Express 39
QDIO routing accelerator 46
QDIO support for OSA interface isolation 69
QDIO INTERFACE statement support for 94
QDISK parameter 33
Queued Direct I/O (QDIO) priorities, mapping 68

read call() 42
real time trace collection 66
reconnect, TN3270 support of TSO logon 36
registration control 77
release considerations in V1R11 25
remote execution server, MVS 35
resolver DNS cache 45
resolver queries 25
Resolver support for EDNS0 120
REXMIT operand 133
RFC (request for comments) 139
  accessing online xvi
RFC 2408 51
RFC 4301 compliance, IBM Health Checker for z/OS 64
RFC 4941 36
RFC 5095 38

Index 177
V
Verbose Ping 68
virtual private network (VPN) 75
virtual storage constraint relief 43
VIT with INOP dump, data space 58
VLAN support 95
volumes, FTP reports 33
VTAM display commands 136
VTAM INOP dump processing 58
VTAM topology agent 11
VTAM topology agent, enabling 7
VTAM, online information xvi

W
WebSphere Application Server, FRCA cache enhancements for 103
window size, tuning 43
WLM routing algorithms 40
WLMPRIORITYQ parameter 68
workload balancing 49
Workload Manager (WLM) service classes to outbound Queue Direct I/O (QDIO) priorities 68
workload performance and OSA-Express3 optimized latency mode 50
workload, zIIP or zAAP targeted 40
workloads, sysplex distributor optimization for multi-tier z/OS 48

X
XML appliances 44
XMLAppliance 73

Z
z/OS Basic Skills information center xiv
z/OS Basic Skills Information Center xiv
z/OS Health Checker for z/OS migration health check 57
z/OS UNIX shell commands 57
z/OS V1R10 Communications Server release summary for IP 71
z/OS V1R11 Communications Server release summary 25
z/OS workloads, sysplex distributor optimization for multi-tier 48
z/OS, documentation library listing 171
zIIP or zAAP targeted workload 40
zIIP processor and HiperSockets 96
zSeries, definition of 1
zSystem, definition of 1
Communicating Your Comments to IBM

If you especially like or dislike anything about this document, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this document. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Please send your comments to us in either of the following ways:

• If you prefer to send comments by FAX, use this number: 1+919-254-1258
• If you prefer to send comments electronically, use this address:
  – comsvrcf@us.ibm.com
• If you prefer to send comments by post, use this address:
  International Business Machines Corporation
  Attn: z/OS Communications Server Information Development
  P.O. Box 12195, 3039 Cornwallis Road
  Department AKCA, Building 501
  Research Triangle Park, North Carolina 27709-2195

Make sure to include the following in your note:

• Title and publication number of this document
• Page number or topic to which your comment applies.