IBM eServer™

IBM

z/OS® V1R8 Communications Server Overview - Various TCP/IP Changes

@business on demand software

© 2007 IBM Corporation

Various TCP/IP changes

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

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

➢**Initial focus will be on the Communications Server health checker infrastructure and a few selected configuration options that are known to have caused problems in the past:**

  ► The default size of the TCP receive buffer size (the TCPMAXRCVBUFRSIZE option in the TCP/IP Profile)
  ► The default set of options for CTRACE
  ► Maximum amount of fixed CSM storage (the MAXFIX option in IVTPRMxx)
  ► Maximum amount of ECSA CSM storage (the MAXECSA option in IVTPRMxx)

z/OS V1R8 Communications Server Overview - Various TCP/IP Changes
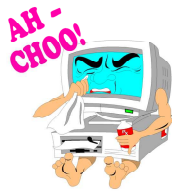
Various network management enhancements

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

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

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

Better tracking of DVIPA creation and deletion

➤ Netstat VDPT display enhancements for current number of active connections

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

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

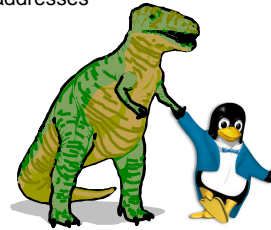➤ Include additional information regarding the creation of a DVIPA in the *netstat vipadyn* report:

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

Additional netstat command enhancements

➢ **Various Netstat enhancements**

- ► Enhanced ability to select only the listening socket of a server with many active connections - netstat all and netstat conn reports
  - – New modifier called SERVER

- ► Add information about autolog configuration to the existing netstat config report

  > • Autolog Configuration Information: Wait time 5
  > • Proc Name: xxxxxxxxx Job Name: yyyyyyyy
  > • Parmstring: zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
  > •   zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz

- ► Add new ipaddress+port selection filter to connection-oriented netstat reports
  - – IPPORT filter: ipaddress+port

- ► Add new modifier to the netstat slap report to select only active policies
  - – New modifier called ACTIVE

Retired TCP/IP Profile parameters

➢ **Support for the ASSORTEDPARMS and KEEPALIVEOPTIONS statements in the TCP/IP profile has been removed.**

➢ **These statements have been deprecated since z/OS V1R2 with warning messages issued.**

➢ **The parameters on these statements have equivalent parameters on the GLOBALCONFIG, IPCONFIG, IPCONFIG6, TCPCONFIG, and UDPCONFIG statements.**

Linux® message integration

- ➤ **Allow syslogd to receive syslog messages from zSeries® Linux systems over the UDP/IP network and write these messages to a new destination: /dev/operlog**

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

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

- ➤ **Support added for new destination: /dev/operlog**

8   z/OS V1R8 Communications Server Overview - Various TCP/IP Changes   © 2007 IBM Corporation

IPv6 support - extending integrated IP Security to IPv6 workloads

whatsnewVarious.ppt

Extending integrated IP Security functions to include IPv6 traffic

➤**z/OS V1R5 and V1R6 have both been IPv6 Ready Logo Phase-1 certified**

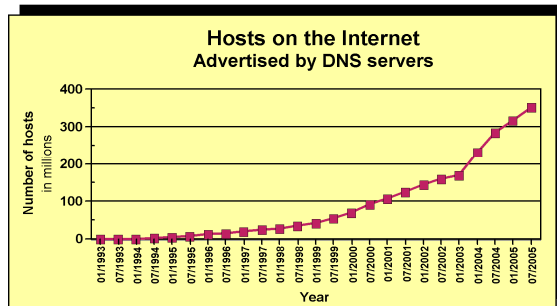➤**IPv6 Ready Logo Phase-2 has now been defined and the main addition is required support for IPv6 IP Security (IPSec)**
 - Standard requirement for all IPv6 platforms
 - Replace application-specific security, such as OSPFv3
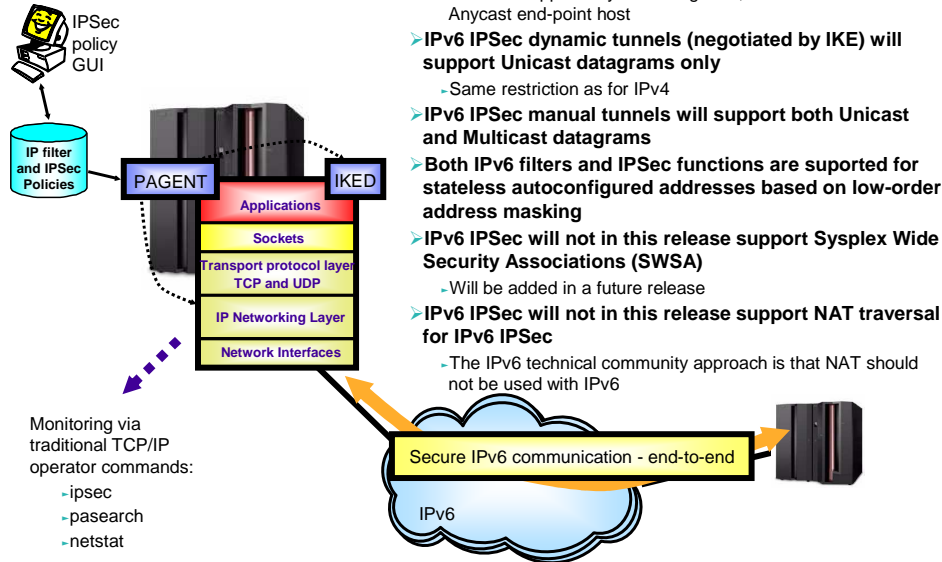 - Opportunity for end-to-end IPSec security between all IPv6 hosts

Phase-1

Phase-2

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

➤**z/OS V1R8 extends IPSec support to IPv6**

Hosts on the Internet
Advertised by DNS servers

Number of hosts in millions

400
300
200
100
0

01/1993 07/1993 01/1994 07/1994 01/1995 07/1995 01/1996 07/1996 01/1997 07/1997 01/1998 07/1998 01/1999 07/1999 01/2000 07/2000 01/2001 07/2001 01/2002 07/2002 01/2003 07/2003 01/2004 07/2004 01/2005 07/2005

Year

IPv6 IPSec support details

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

IPSec policy GUI

IP filter and IPSec Policies

PAGENT   IKED

Applications

Sockets

Transport protocol layer TCP and UDP

IP Networking Layer

Network Interfaces

Monitoring via traditional TCP/IP operator commands:
- ipsec
- pasearch
- netstat

Secure IPv6 communication - end-to-end

IPv6

The Journey to IPv6 for z/OS Communications Server

> **The first phase (z/OS V1R4)**
>> ► Stack support for IPv6 base functions - (APIs, Protocol layers)
>> ► Resolver
>> ► High speed attach (OSA Express QDIO))
>> ► Service tools (Trace, Dump, etc.)
>> ► Configuration and netstat, ping, traceroute, SMF
>> ► Static Routing
>> ► FTP, otelnetd,unix rexec, unix rshd/rexecd

> **The second phase (z/OS V1R5)**
>> ► Network Management
>>> – Applications and DPI®
>>> – Version-neutral Tcp/Ip Standard MIBs
>>> – Additional SMF records
>> ► Applications/Clients/APIs
>>> – Tn3270 server,CICS sockets, sendmail,ntp,dcas, rxserve,rsh client
>> ► Enterprise Extender
>> ► Point to Point - type DLCS
>> ► Dynamic Routing Protocol w/ OMPROUTE (only RIPng)

> **The third phase (z/OS V1R6)**
>> ► Sysplex Exploitation (Dynamic VIPA, Sysplex Distributor functions)
>> ► Dynamic Routing Protocol w/ OMPROUTE (OSPFv3)
>> ► Additonal Network Management MIBs

> **The fourth phase (z/OS V1R7)**
>> ► SNMP UDP standard MIB (RFC2013) and IBM MVS TCP/IP Enterprise-specific MIB for UDP
>> ► Advanced Socket API support - RFC3542
>> ► IPv6 Two Default Routers - required for IPv6 compliance
>> ► Hipersockets

> **The fifth phase (z/OS V1R8)**
>> ► Integrated IPSec for IPv6

> **After z/OS V1R8**
>> ► Complete Advanced Socket APIs
>> ► Extended Stats MIB, OSPFv3 MIB
>> ► Intrusion Detection Services
>> ► IPv6 mobility support
>> ► FRCA support for IPv6

The Internet - a worldwide digital utility.

Objective is to have IPv6 production ready on the platform when you need it!
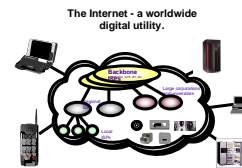
Connectivity for *anyone* from *anywhere* (car, home, office) to *anything*!

Trademarks, copyrights, and disclaimers

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

Current	DPI	IBM	MVS	z/OS	zSeries

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

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. 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 in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

© Copyright International Business Machines Corporation 2007. All rights reserved.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.

z/OS V1R8 Communications Server Overview - Various TCP/IP Changes

© 2007 IBM Corporation