IBM TRAINING

E18

TCP/IP for VSE 1.5E Update

Don Stoever

IBM
SYSTEM z9 AND zSERIES EXPO
October 9 - 13, 2006

Orlando, FL

RETURN TO INDEX

TCP/IP 1.5E Enhancements to:

- Stack
- FTP
- Security
- SSL
- Message Logging
- Telnet
- Email
- BSD/C API
- Miscellaneous
- SeeVSE

Stack Enhancements

- TCP/IP Retransmission
  - Improved connection reliability
  - Flexibility for environments that mix local and Internet traffic…
  - DEFINE ROUTE command new parameters
  - MODIFY ROUTE command added
    - Parameters made available at the route level to permit customization down to the level of a single host…

Stack Enhancements

- ID=
  - For MODIFY, must specify an existing route
- AFTER=
  - For MODIFY, the specified existing route will be moved to a position following the indicated route name.
- MAXSegment=
  - Specifies the Maximum Segment Size (MSS)
    - Range: 576 – 65535
    - Default: SET MAXSEGMENT=

Stack Enhancements

- CRETran=
  - Time TCP/IP should wait before resending a unacknowledged connection (SYN) request
  - Value remains constant and is not dynamically adjusted…
    - Range: 10 – 1000
    - Default: SET RETRANSMIT=

Stack Enhancements

- DRETran=
  - Time TCP/IP should wait before resending an unacknowledged data packet
    - If Fixed Retransmit is enabled, the value is used for all transmissions
    - If Fixed Retransmit is disabled DRETRAN is used as a starting value only, and the actual time is adjusted according to the perceived delay on the connection
    - Range: 10 – 5000
    - Default: SET RETRANSMIT=

Stack Enhancements

- FIXRetran=
  - If YES, the DRETRAN time interval will always elapse before a retransmission occurs
  - If NO, the time interval will be adjusted to meet the current conditions of the network
    - Default: SET FIXED_RETRANSMIT=

Stack Enhancements

- MINRet=
  - Specifies a "floor" for the retransmission algorithm
  - Following the calculation of a new value for determining when to enter retransmission mode, it will be increased to the MINRET value.
  - Range: 10 – 1000
  - Default: 500

Stack Enhancements

- MAXRet=
  - Specifies a "ceiling" for the retransmission algorithm
  - Following the calculation of a new value for determining when to enter retransmission mode, it will be decreased to the MAXRET value
  - Range: 10 – 5000
  - Default: 2000

Stack Enhancements

- RETRY=
  - Once retransmission mode is entered, an unacknowledged transmission will be resent the specified number of times before the connection is flagged as "dead“
  - Range: 5 – 1000
  - Default: 50

Stack Enhancements

- RPAuse=
  - Time interval that will elapse between each retransmission and the subsequent retransmission.
  - Value is independent of that used during normal transmission
  - Range: 10 – 5000
  - Default: 500

Stack Enhancements

- WINdow=
  - Maximum size of the receive window
  - This is the maximum number of unacknowledged bytes that the stack is prepared to receive
  - Range: 1500 – 65535
  - Default: SET WINDOW=

Stack Enhancements

- PULse=
  - Time interval, in seconds, that a connection may be dormant before a probe is sent to test the connection
  - Range: 0 (no pulse) – 9999999
  - Default: SET PULSE_TIME=

Stack Enhancements

- QUERY ROUTES
  - ID: ALL Link ID: L3172E
  - IP Address: 0.0.0.0 Mask: 255.255.255.0
  - Net: -- Subnet: -- Host: --
  - Gateway IP Address: 68.77.189.194
  - MTU: 1500 Max Seg: 32684 Pulse: 60s
  - SYN Retran: 1000ms Data Retran: 1000ms
  - Fixed: NO
  - Retran Min: 500ms Max: 2000ms
  - Retry Delay: 500ms Retries 50

Stack Enhancements

- QUERY CONNECTIONS
  - New display format
  - Restrict display by IP address, port
  - Display option to display sequence numbers in decimal or hexadecimal
- DIAGNOSE PERFORM
  - Enahanced to help set values

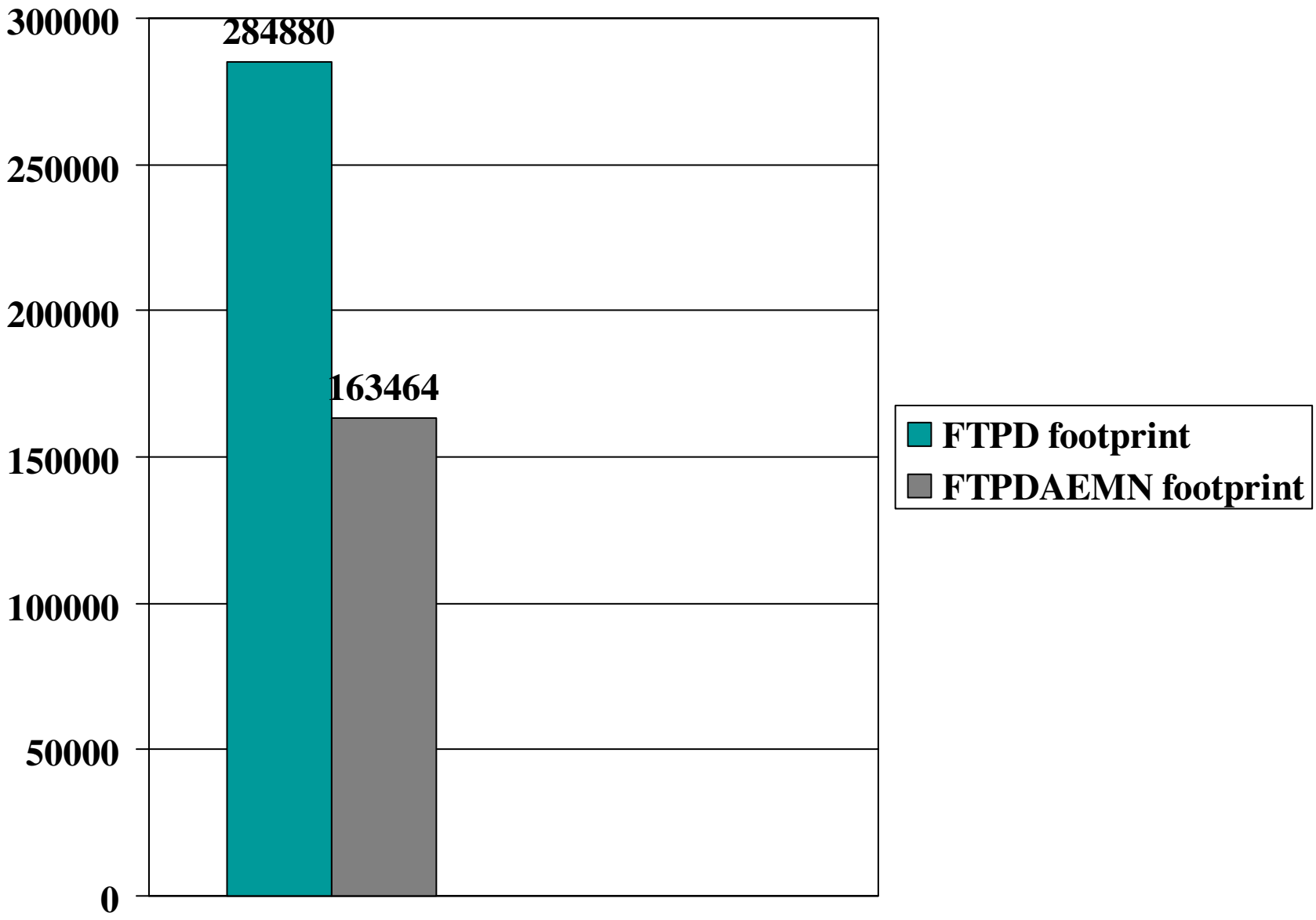
FTP Enhancements

- New FTPDAEMN.phase
  - Define FTPD…DRIVER=FTPDAEMN is default
  - Functionally same as FTPD.phase
- Old FTPD.phase
  - Define FTPD…DRIVER=FTPD to use it
  - No changes other than corrective service
  - FTPD is not reentrant
  - Each FTP session required about 280K of 24-bit storage…

FTP Enhancements

- New FTPDAEMN is reentrant
  - 1 copy for all ftp sessions
- Performance improved
  - 10-20% faster
  - Uses less cpu and storage to do the same amount of work…

FTPD vs. FTPDAEMN



FTP Enhancements

- FTPD
  - Multiple tasks started at the same time with listens on the same port
- FTPDAEMN
  - Single task started in a listen state
  - New tasks dynamically attached for each new session…
  - Pseudo tasks used for internal daemons
  - Real VSE tasks used for external ftpbatch daemon

FTP Enhancements

- New FTPDAEMN
  - BUFSIZE=65536 BUFFCNT=2
    - 2-31-bit transfer buffers allocated on 1st RETR or STOR..
    - Released at end of session
  - Set Transfer_buffers setting is ignored…

FTP Enhancements

- New FTPDAEMN
  - COUNT=nnn
    - Treated as synonym of MAXACTIVE
  - MAXACTIVE=3
  - Whichever is larger used to set maximum number of concurrent sessions
  - No need for multiple DEFINE FTPD commands

FTP Enhancements

- New FTPDAEMN
  - Welcome=
    - Read once at startup uses new LIBR interface
  - Hesitate=NO/YES/nnn
    - Yes or Non-zero causes wait for ack on each buffer sent during retrieve
  - IDLETIME=0
    - Use 36000 to terminate idle sessions

FTP Enhancements

- FTPDAEMN
  - SSL=NO ,YES, YESCLAUTH
    - SSLKEY=lib.sublib.memname/SDFILES
    - SSLVERSION=0300/0301/SSLV3,TLSV1
    - SSLCIPHER=ALL/WEAK/STRONG
    - SSLDATACONN=Clear/Private
  - UNIX=Yes/No/Binary
    - Binary same as unix=yes, but binary=ascii is supressed

FTP Enhancements

- Query ACTIVE TYPE=FTP
  - ID: FTPD0021 Port: 21 Driver: FTPDAEMN
  - Buffers: 2 Buffer size: 131072 bytes
  - Xmit hesitation: 300, Idle timeout: 120 seconds
  - Maximum sessions: 3, Current: 1
  - Userid: DSTOEVER connected from 66.193.91.130,57870
  - Started at: 17:12:02 2005/05/19
  - Last Command: LIST
  - Last Command time: 17:12:12 2005/05/19
  - Last reply: 226 Closing data connection
  - Last reply time: 17:12:12 2005/05/19

FTP Enhancements

- New FTPDAEMN
  - A root directory can be defined for a user on the DEFINE USER command using the ROOT= option
  - This will restrict the user to that directory or lower
  - Setting a ROOT of / or \ will start the user in either UNIX or VSE mode

FTP Enhancements

- New FTPDAEMN
  - SITE RECORD_CONTINUE ON
  - will take ASCII or EBCDIC records longer than the LRECL and span them across several records. When the file is retrieved it will put the records back together
  - This functions the same as setting the file type as TEXTC in the EXTTYPES table, but will allow for record lengths other than 80

FTP Enhancements

- New FTPDAEMN
  - SITE LEADZERO on/off
  - Allows a 227 reply to a PASV command to have no leading zeros
    - CuteFTP thinks leading zeros mean octal numbers instead of decimal…
  - SITE WTO
    - can be issued anywhere, used to be only allowed when in Power directory
  - SITE EXTTYPES OFF (ON is the default).

FTP Enhancements

- New FTPDAEMN
  - SITE TERSE OFF/ON
    - ON causes single line 150 and 226 messages
  - FTP statistics collected at end of session
  - Added support for ABORT command
  - Added support for new HFS file system

FTP Enhancements

- FTPBATCH as external server can have up to 28 concurrent sessions with new FTPDAEMN
  - Uses real VSE subtasks
  - Eliminated file I/O subtask
  - Parm MAXACT=nnn
    - Controls number of concurrent sessions

FTP Enhancements

- New FTPBATCH set commands
  - SET CHAPCNT nnn
    - Balances VSE subtasks when in server mode
  - SET EXTTYPES YES/NO
    - Suppress usage of exttypes.L
  - SET IDLETIME 36000
    - Use to terminate idle sessions
    - 36000/300 = 120 seconds = 2 minutes
  - SET JOURNAL
    - Used by HFS

FTP Enhancements

- New FTPBATCH set commands
  - SET CONSOLE none/warn/info/diag
    - Controls which messages types are display on the VSE system console
  - MSGSUPP FTP900
    - Suppress a specific msg
  - SET STAMP RIGHT/LEFT/NONE
    - Controls placement of timestamp on syslst

Security Enhancements

- Control and monitoring of security functions consolidated in:
  - SECURITY
  - QUERY SECURITY
- UserIDs can now be restricted to specific uses:
  - FTP, WEB, Telnet, LPR, SMTP, POP3
  - For example, having a valid ID for TN3270 access does not permit FTP access

Security Enhancements

- SECURITY command global options:
  - ON/OFF
    - Controls global security processing
  - EXTERNAL=ON/OFF
    - Control security usage FTPBATCH, etc.
  - MODE=WARN/FAIL
    - Warn or Fail security violations
  - LOGGING=ALL/FAIL/NONE
    - Controls logging of security requests
  - LOCK
    - Locks all security settings to their current values

Security Enhancements

- VSE system on the Big Internet:
  - SECURITY ON
    - Userid's/passwords validated
  - SECRUITY EXTERNAL=ON
    - Ftpbatch security calls enforced
  - SECURITY AUTO=ON
    - Use new automatic security exit
  - SECURITY MODE=FAIL
    - First use WARN then fail…
  - SECURITY LOGGING=FAIL
    - ALL or NONE

Security Enhancements

- QUERY SECURITY Command
  - Security Processing: Disabled
  - TCP/IP TCP/IP Security Settings
  - ARP Checking: Disabled
  - IP Address Checking: Disabled
  - Auto Data: Undefined
  - Exit Data: Undefined
  - Automatic Security: Disabled
  - Security Exit: Undefined
  - External Security: Disabled
  - Security Mode: Fail Logging: Fail
- Summarizes all security information

Security Enhancements

- Flow of a security request:
  - Application (eg, FTP) creates an SXBLOK
  - UserID/password (if present) is checked against DEFINE USER information
  - If specified Automatic processing is performed
  - If specified User Exit processing is performed
  - User exit may consider the result of the preceeding steps, or may override it…

Security Enhancements

- User security exit
- SECURITY command options:
  - PHASE=
    - Name of the user security exit phase
  - XDATA= 40-bytes user exit
  - ASMDATE=Assembly date
  - ASMTIME=Assembly time
  - VERSION=Version LEVEL=Modification level
  - EXIT=ON/OFF
    - Controls activation of User Security Exit

Security Enhancements

- User-provided Security Exit may send messages to the security logger
- Security requests passed to the user exit will now contain the type of usage requested
  - For example, FTP or LPR.
- 1.5D security exits see the same data as before, modifications need be made ONLY if use of new features is desired.

Security Enhancements

- SECURITY AUTO=ON
  - Automatic security means no need to assemble and linkedit custom code…
  - Can be used to replace current user exit…
  - ASECURITY ICMP=YES/NO
    - Controls pinging VSE!
  - ASECURITY FTPD=YES/NO
    - Controls establishing new FTP sessions with VSE
  - ASECURITY IPAV=YES/NO
    - Controls incoming IP datagrams

Security Enhancements

- SECURITY AUTO=ON
  - Create a FTP user with Read Only access to VSE/Power LST queue class=F
    - DEFINE USER,ID=CSIVSEDR,
    - DATA=YYNNNNNNYNNNNNYYYNNNNNNNNYNNY
    - ROOT='/POWER/LST/F',FTP=YES
  - DATA=YNNNYNNNY…
    - corresonds to resource number
  - See SXTYPE of SXBLOK…
    - SXTYPASS EQU 1 - Password Check
    - SXTYREAD EQU 2 - Read Check
    - SXTYWRIT EQU 3 - Write Check
    - SXTYCMD EQU 9 - SITE Command check

Securirty Enhancements

- SXTYUPDT EQU 4 - Update Check
- SXTYSTRT EQU 5 - Startup Security
- SXTYSHUT EQU 6 - Shutdown Security
- SXTYHARD EQU 7 - Hardware Address Verify
- SXTYIP EQU 8 - IP Address Verify
- SXTYCMD EQU 9 - SITE Command check
- SXTYDEL EQU 10 - Delete check
- SXTYREN EQU 11 - Rename check
- SXTYCRT EQU 12 - Create check
- SXTYEXEC EQU 13 - EXEC command check
- SXTYAPPE EQU 14 - APPEND check
- SXTYOPDI EQU 15 - OPDIR check

Security Enhamcements

- SXTYRDD EQU 16 - RDDIR check
- SXTYCWD EQU 17 - CWD Check
- SXTYSHEL EQU 18 - SHELL Check
- SXTYICMP EQU 19 - ICMP check
- SXTYLOGI EQU 20 - Daemon LOGIN request
- SXTYRPC EQU 21 - RPC Request
- SXTYWEBL EQU 22 - Web Logon Screen Request
- SXTYSCAN EQU 23 - HTTPD SCANBLOCK request
- SXTYMKD EQU 24 - Make directory
- SXTYRMD EQU 25 - Remove directory
- SXTYCWDL EQU 26 - Last CWD
- SXTYFCMD EQU 29 - FTPD command

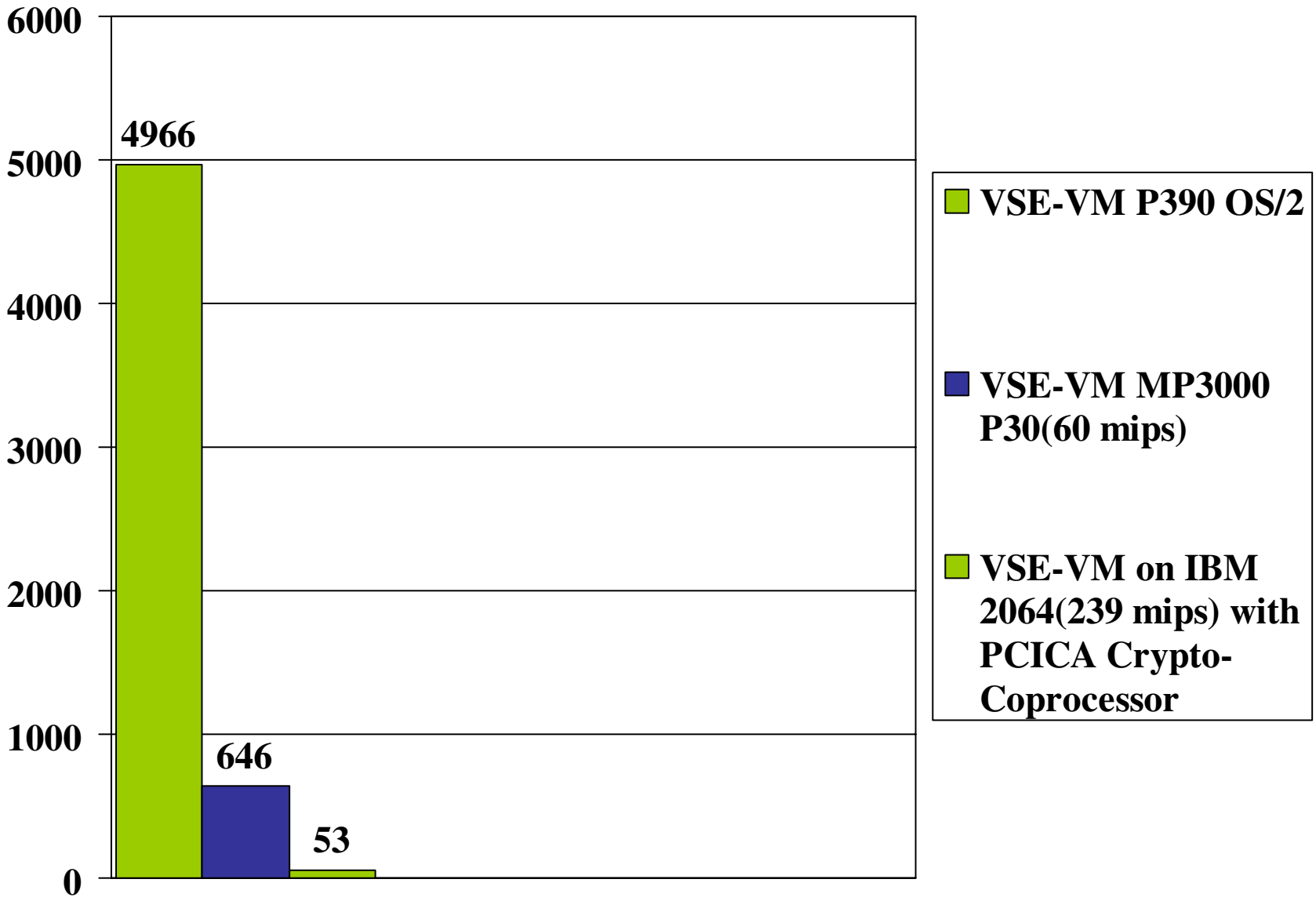
Security Enhancements

- New default userids
  - Event processing uses $EVENT/$EVENT
    - Override with DEFINE EVENT userid=,password=
  - LPR processing default $LPR/$LPR
    - Override with SET USER= command
  - HTTPD default $WEB/$WEB
    - Override with DEFINE HTTPD, userid=,password=
  - Should Add DEFINE USER,
    - ID=$WEB,PASSWORD=$WEB,WEB=YES
    - ID=$LPR,PASSWORD=$LPR,LPR=YES
    - ID=$EVENT,PASSWORD=$EVENT,LPR=YES

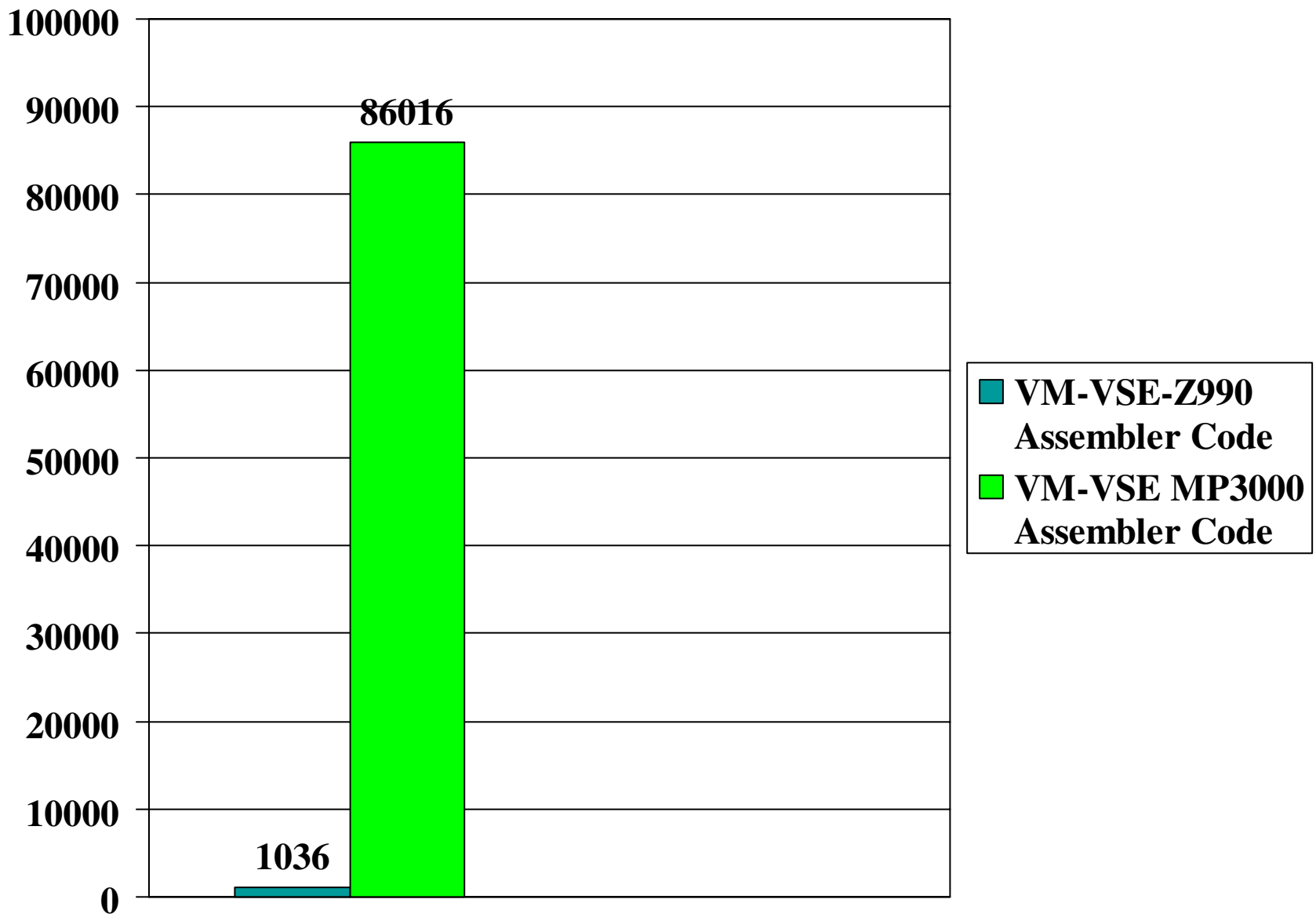
SSL Enhancements

- Changed SSL blocksize from 16k to 32k
- Added support for CryptoExpress2
- Added support for generalized time in a certificate
- Added support for Z architecture crypto instructions for SHA1, DES, Triple DES
  - Added support for AES-128 algorithm
- Added support for RSA-2048 bit with CEX2
- Enhanced SecureFTP to support implicit connection for port 990

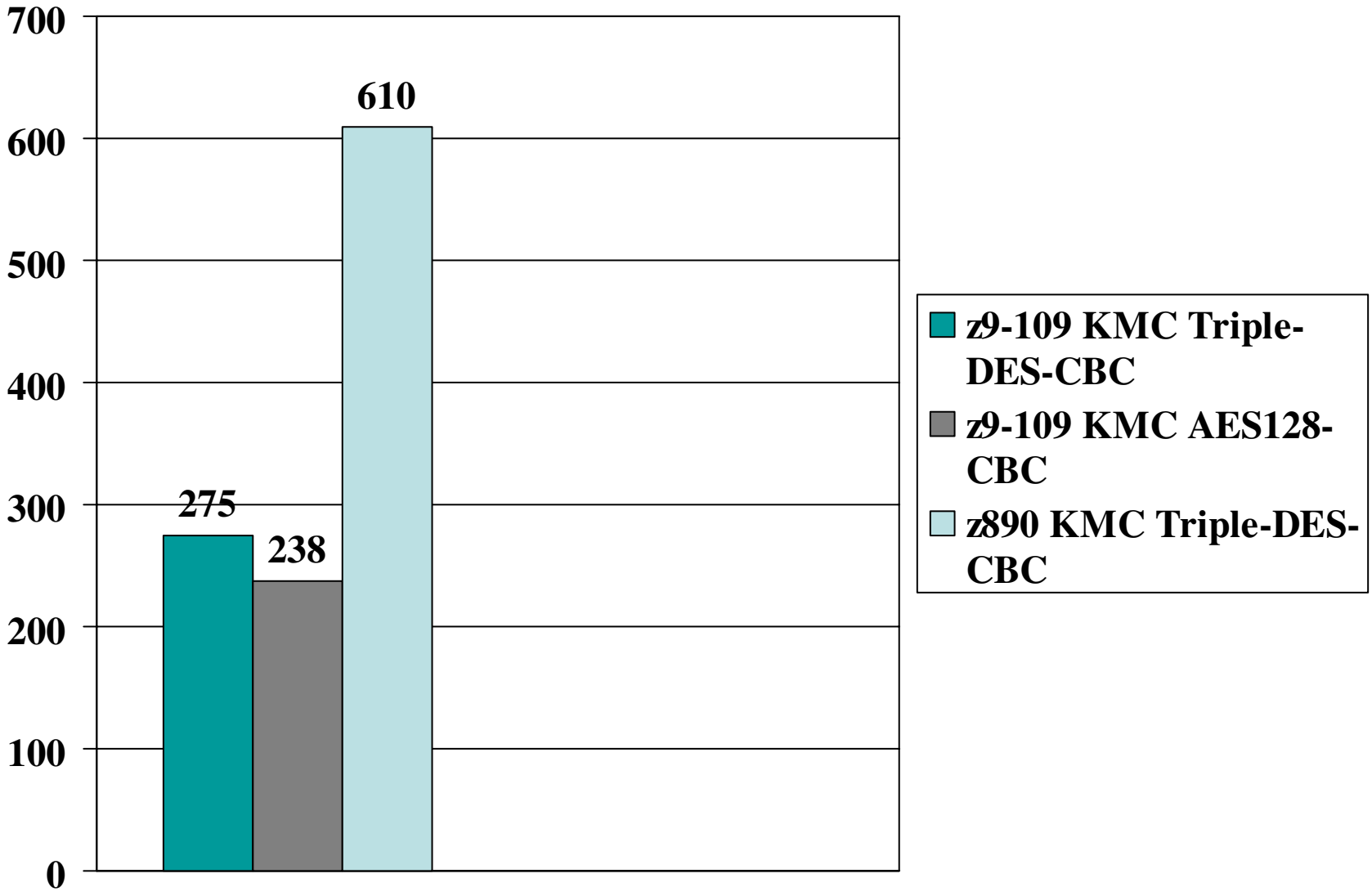
RSA 1024-bit Encrypt-Decrypt 1000 times



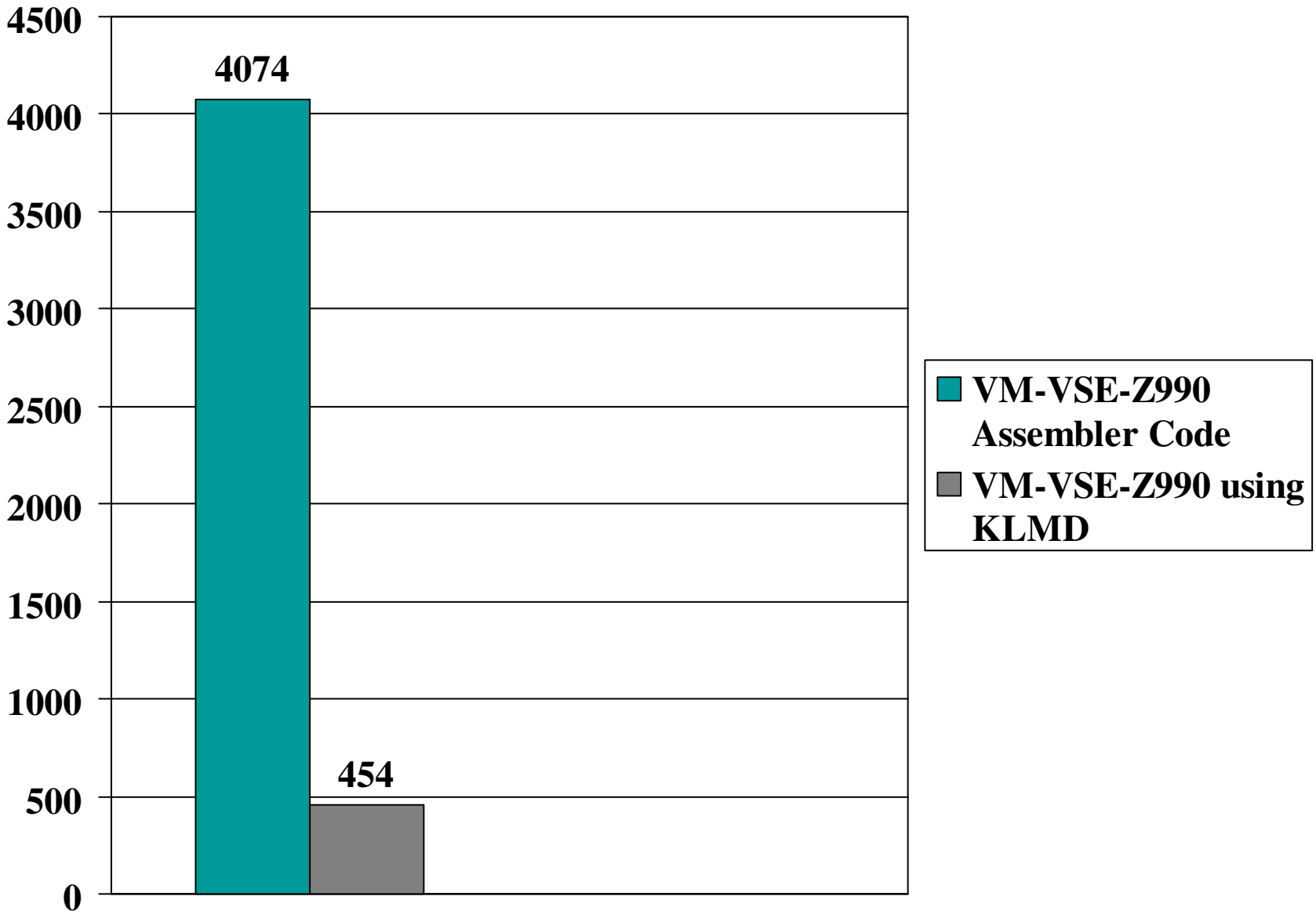
Triple-DES Encrypt of 16meg 2048 Times



Triple-DES vs. AES128 Encrypt/Decrypt of 16meg 1000 Times



SHA-1 Message Digest of 8k 100,000 times



Message Logging Enhancements

- New message writer in IPNET and batch utilities
- Messages classified into groups:
  - CRITICAL, IMPORTANT, WARN, INFO, SECURITY, RESPONSE, DIAGNOSE
- Groups controlled through LOG command
- Predefined CONSOLE and SYSLST logs
- Additional logs defined through DEFINE LOG command

Message Logging Enhancements

- Additional commands: QUERY LOG, MODIFY LOG and DELETE LOG
- Message documentation updated
  - Hyper-linked HTML
  - PDF
  - VSE Explain format to be loaded into the EXPLAIN file

Message Logging Enhancements

- CONSOLE_HOLD OFF
- MODIFY LOG,ID=SYSLST,TIMESTAMP=RIGHT
- MODIFY LOG,ID=CONSOLE,DIAG
- MESSAGE MSGID=IPC108,CONSOLE=NO
- MESSAGE MSGID=IPF100,CONSOLE=NO

Message Logging Enhancements

- No need to assgn syslst to disk
  - // JOB FTPBDIR
  - // ASSGN SYS007,30C
  - // DLBL MSGXLOG,'FTPBATCH.MSGXLOG',,SD
  - // EXTENT SYS007,DRSAAA,1,0,7860,30
  - // EXEC FTPBATCH,SIZE=FTPBATCH
  - ...
  - SET MSGXLOG ON
  - ...
  - DIR
  - ...

Telnet Enhancements

- LOCALECB ON/OFF command
  - Large system effect for Telnet
  - Default is OFF
  - ON will reduce CPU overhead

Email Enhancements

- SMTP Client
  - Sends email from VSE to any SMTP server…
- POP3 Client interface to POP3 servers
  - List the attributes of individual emails
  - Obtain a directory list of mail
  - Delete undesirable email
  - Download an email with attachments
- POP3 Repository
  - Store email on VSE

Email Enhancements

- POP3 Server
  - Delivers the email, provides information about it, and deletes it
  - All standard POP3 commands are supported.
  - Default port=110
- SMTP Server
  - Accepts requests from an email client.
  - Stores emails POP3 mailboxes
  - Default port=25

Email Enhancements

- **`EXEC EMAIL`** invokes the SMTP client
  - **`EMAIL.AUTOEXEC`** invoked at startup
- **`EXEC POPMAIL`** invokes POP3 client
  - **`POPMAIL.AUTOEXEC`** invoked at startup
- **`EXEC CLIENT`**
  - will still invoke the SMTP client, but it will warn you to migrate to **`EXEC EMAIL`**

BSD/C Socket Interface

- New programs
  - IPNRSTUB.OBJ included in application
  - IPNRBSDC loaded by the stack into 31-bit system GETVIS
- Fully compliant using command level functions for:
  - CICS/TS 1.1 and above
  - CICS/VSE 2.3 and above

BSD/C Socket Interface

- Improved performance 10-30%
- More debugging options
  - Standard SYSLST/Console options
  - CICS trace (CEDF & CEDX)
  - Restrict trace to specific calls
- See member SOCKDBG.A

Miscellaneous

- Product Authorization Codes
- Expiration message issued at start-up
- QUERY PRODKEYS[,ALL] command

Miscellaneous Enhancements

New DIAGNOSE Commands

- TCP
- UDP
- LINK (was CLAW)
- SMTP
- RETRANSMIT
- SECURITY
- ICMP

SeeVSE

- Distributed with TCP/IP 1.5E
- VSE Performance Monitoring
  - System CPU usage
  - Partition CPU and I/O
- TCP/IP Performance Monitoring
  - Overall IP activity
  - Connection blocks
  - FTP session statistics

SeeVSE

- Uses VSE Supervisor exits to count:
  - Start i/o (post-ssch)
  - I/O interrupts
  - Program checks
  - External interrupts
  - Phase loads (post-fetch)
  - SVC interrupts
- Provides system request/logging queue

SeeVSE

- Dynamically attaches a pseudo task in the TCP/IP partition
  - Uses access registers to copy TCP/IP connection control blocks to SeeVSE external partition
  - PC client polls VSE server for data
  - PC component stores VSE performance data in XML documents
  - PC charting used for graphical display and trend Analysis

Question’s ?

- *

RETURN TO INDEX