Smart Network Management with CA NetMaster Network Management

Craig Guess
CA Technologies

March 4th, 2011
Session # 8245

Agenda

- Challenges
- Overview of NetMaster
- Usage Scenarios
- Questions

Mainframe Networking Challenges

Increasing complexity

Network Consolidation

Mainframe Skil Shortage

Managing Compliance

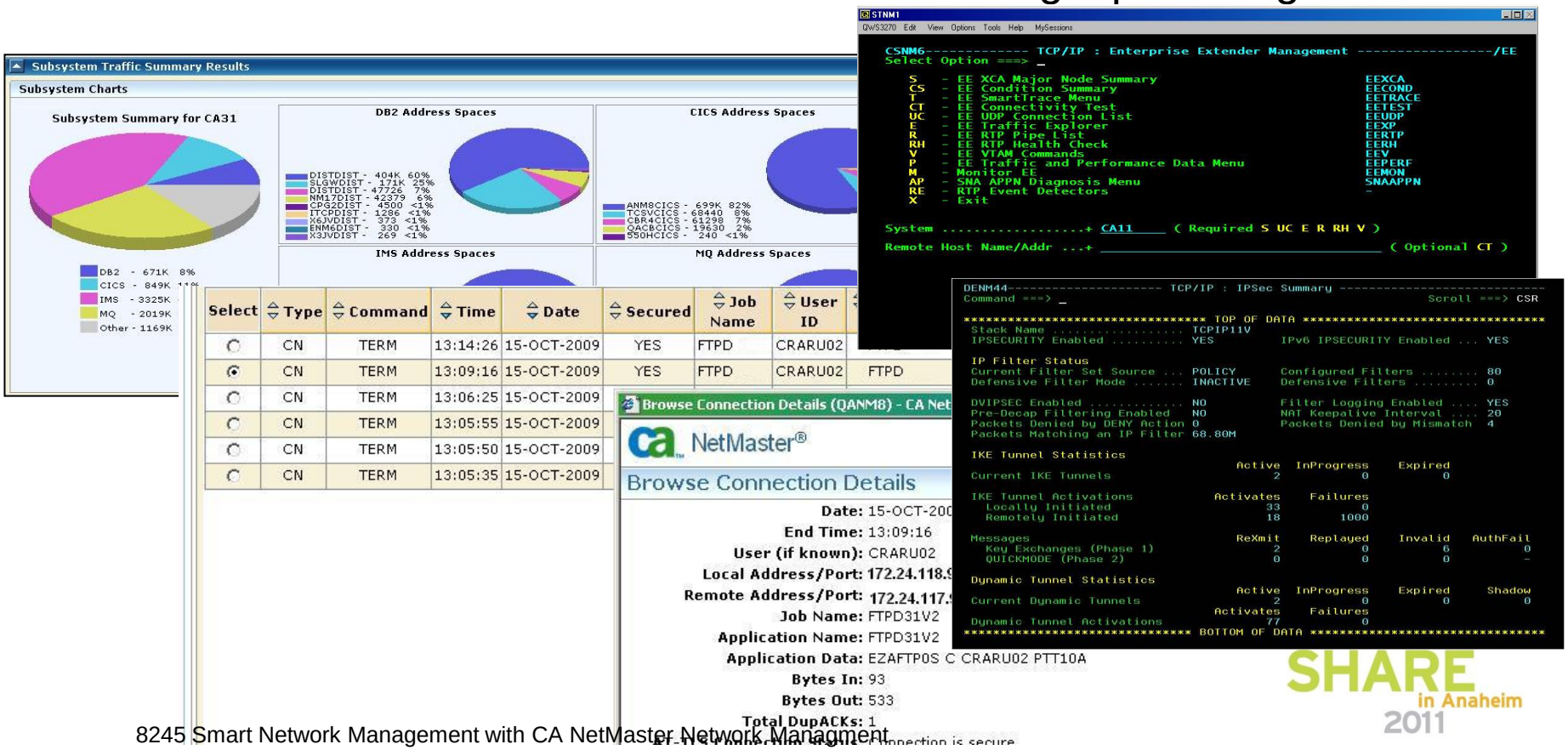
Cost Control

Security and Governance

SHARE
Technology • Connections • Results

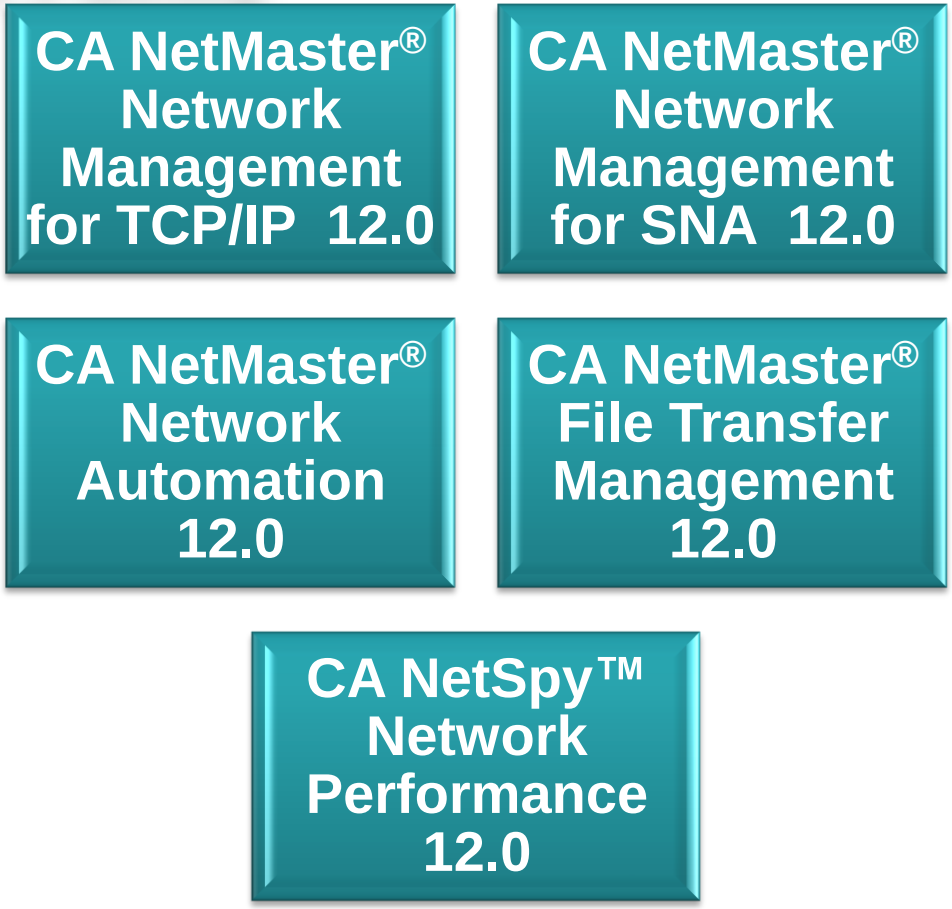
Product Description

- CA NetMaster Network Management empowers new and experienced network administrators to easily identify and resolve network issues before they impact the end user and plan for future demands with a choice of interfaces on a single pane of glass.



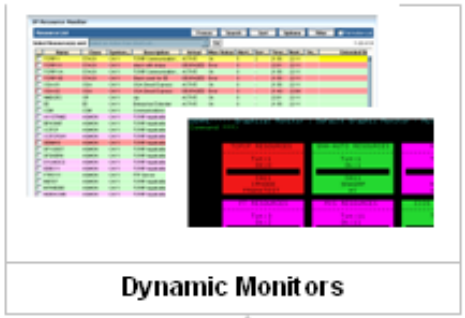
SHARE in Anaheim 2011

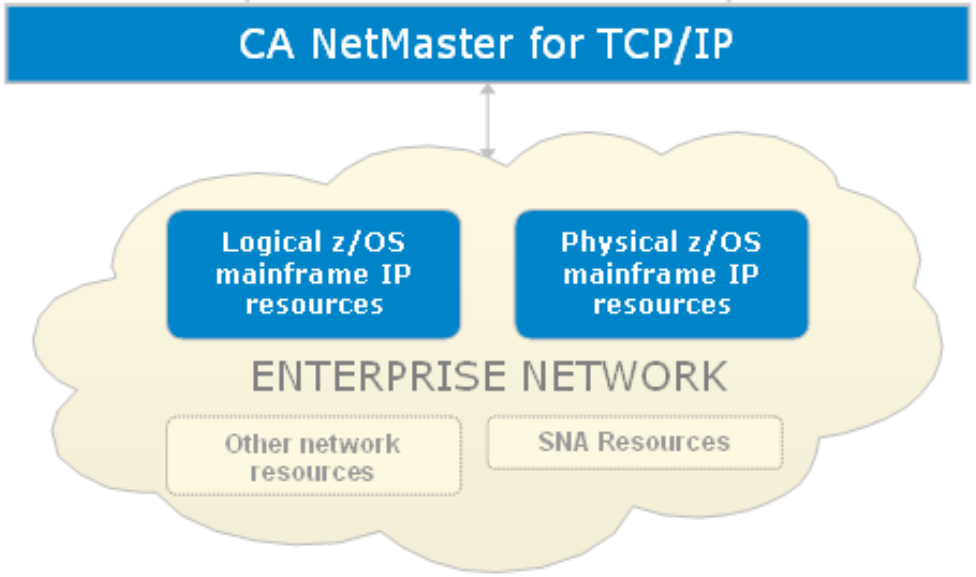
CA Mainframe Network Management Product Family



Comprehensive Toolset

- First delivered in 1982
- Founders - 4 IBM developers
- Veteran seasoned team
  - Several original dev.
  - Support
  - SWAT





NetMaster Strengths

Monitoring Functions	• SNA, TCP/IP, MVS, File Transfers, other
Historical Information	• Trends, Reporting, Diagnosis
Diagnostics	• Proactive, Intuitive, Flexible
Reporting	• Intuitive, Flexible

The zIIP capabilities

- zIIP utilization: a growing factor in assessing the true value of mainframe software purchases.
- CA NetMaster delivers the best zIIP exploitation capabilities:
  - Code specifically designed to execute on a zIIP
  - Measures its own zIIP eligible and actual zIIP CPU consumption

Usage Scenarios

1. What application traffic is being carried now on this stack interface?
2. How much IP Filtering is being done on this LPAR?
3. How many of our current Telnet sessions are secured?
4. How can I view our connection details in a spreadsheet?
5. I'm a z/OS DB2 DBA. What SQL payload is flowing over this DB2 connection to ABC?
6. I'm a z/OS Web developer.
   How can I see more of what my application is doing?
7. How DB2 TCP/IP connections are there a day? Is this growing?
8. Are we getting a lot of connection failures?

* Network Traffic Analysis

Scenario 1

What application traffic is being carried now on this stack interface?

- You have traffic figures for each stack interface – and for each appl.
  But are they correlated?
- For stack interface ABC, what applications are contributing to its current traffic?
- For application XYZ, what stack interfaces are its current traffic flowing over?

A: Use the new Interface-Application traffic figures

- A TCP connection can send packets over more than one interface!
- The NetMaster Packet Analyzer correlates traffic for stack network interfaces with NetMaster's own 'business applications' – and vice versa
- Available from IP Summary

Interface-Application Traffic, by Interface

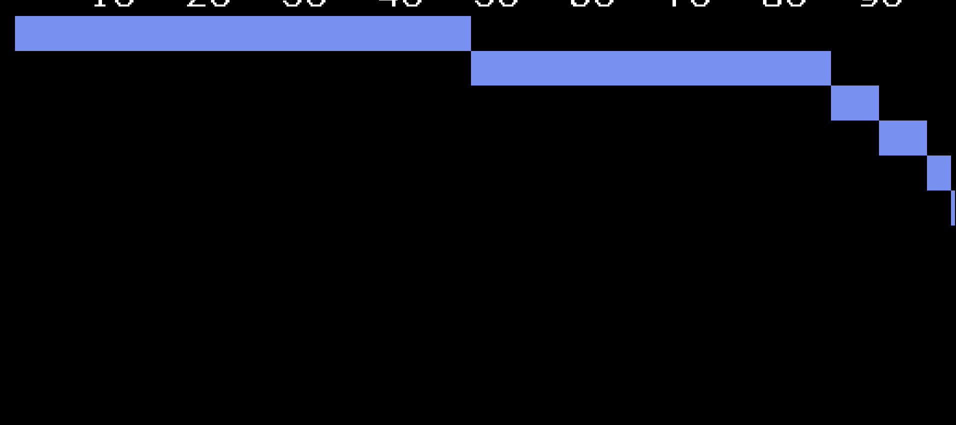
```
DENM17------------------ TCP/IP : IP Throughput Summary --------------------------
Command ===>                                                        Scroll ===> CSR

                                              .=Expand or Collapse ?=more actions
____ IP Throughput:      Total: 4 Stks, 277 Interfaces  122.4      46211     103
     |      Stack/                Connections ---Packets/Second----  ----Bytes/Seco
     |         Interface Name     Active          In         Out          In        O
____ |-- CA31:                      103        59.1       63.33       18707      275
____ |  |-- TCPIP31                 102 >99%  51.54  87% 55.46  88%  17604  94% 259
____ |  |  |- LOOPBACK               -        24.62  48% 24.62  44%  12754  72% 127
S___ |  |  |- OSA1                   -        26.91  52% 17.99  32%   4850  28%  70
____ |  |  |- OSA2                   -        0.003  <1%  12.7  23%    0.2  <1%  61
____ |  |  |- HIPERLFF               -            0   0%  0.14  <1%      0   0%  24
____ |  |  |- LOOPBACK6              -            0   0%     0   0%      0   0%
____ |  |  └ LNKVIPA                 -            0   0%     0   0%      0   0%
```

```
DENM17-------------- TCP/IP : Interface Traffic Statistics ----------------------
Command ===>                                                        Scroll ===> CSR

     Stack Name .......... TCPIP31
     Interface Name ..... OSA1

____ Applications     Bytes    74.3M 100% ---10--20--30--40--50--60--70--80--90---
     FTP                         36M  48%
     OTHER                     27.1M  37%
     Unassigned                4645k   6%
     CCITCPGW                  3463k   5%
     Hermes-31                 2327k   3%
     TELNET                     244k  <1%
     MVSNFSC                    232k  <1%
     STNM2                      191k  <1%
     DENM17                    51466  <1%
     CCITCP                    22776  <1%
     VANQAV62                   9358  <1%
     SMTPMAIL                   1674  <1%
```



Interface-Application Traffic, by Application

SHARE
Technology • Connections • Results

```
DENM17--------------- TCP/IP : Application Usage Summary ---------------------
Command ===>                                                 Scroll ===> CSR

                                                .=Expand or Collapse ?=more actions
___ Applications:       Most active: OTHER                29.05      17010     74%
      System/       Connections  ---Packets/Second----  ----Bytes/Second-----
        Appl.       Active              In        Out          In          Out
____  - CA31              96        24.25      28.25        7484        16756
____    - OTHER           71   74%  12.22   50% 16.83   60%  4657   62% 12353   74%
____    - Hermes-31        6    6%   1.86    8% 1.307    5% 391.6    5%  1714   10%
S___    - DB2              3    3%  1.347    6% 1.237    4%  1287   17% 348.8    2%
____    - QAM1R4           1    1%  1.077    4% 1.167    4% 320.7    4%  1258    8%
____    - CCITCPGW         1    1%   0.77    3%  0.74    3% 432.3    6% 462.8    3%
____    - QAM1             1    1%   1.76    7%  1.32    5% 110.9    1% 348.8    2%
____    - STNM2            2    2%    0.3    1%   0.4    1%  21.6   <1%  26.8   <1%
____    - MVSNFSC          3    3%  0.067   <1% 0.087   <1%  20.8   <1% 11.89   <1%
____    - DENM17           1    1%   0.18   <1% 0.253   <1% 14.03   <1% 18.54   <1%
____    - FTP              0    0%   0.16   <1% 0.167   <1%  8.12   <1% 13.44   <1%
```

```
DENM17------------ TCP/IP : Application Traffic Statistics --------------------
Command ===>                                                 Scroll ===> CSR

     Application Name ... DB2

___  Stack Interface  Bytes   9453k 100%  ---10--20--30--40--50--60--70--80--90---
     TCPIP31-LOOPBACK          9442k >99%
     Indeterminate             11424  <1%

___  Application Traffic Statistics through stack: TCPIP31
          Packets In          Packets Out          Bytes In           Bytes Out
     Time  Stk%   Amount      Stk%   Amount      Stk%   Amount      Stk%   Amount
___  23.02   3%     37         2%     32         19% 37999          1%   9478
___  23.01  14%   1100 ■■■■■   14%   1092 ■■■■■   53% 1545k ■■■■■   12%   393k ■■■■■
___  23.00   6%     67         4%     61         27% 64356          2% 17333
___  22.59   6%     83         5%     76         26% 81777          3% 21882
___  22.58   6%     93         4%     85         25% 82191          2% 23271
```

* Security Awareness

Scenario 2

How much IP Filtering is being done on this LPAR?

- IP Filters are usually used with IPSec, but can be used alone
- IPSec capabilities are provided by IBM Communications Server. IPSec management involves monitoring IP Filters, IKE tunnels, Dynamic tunnels and Manual tunnels
- *IPSec configuration and management on z/OS is not for the faint-hearted….*

A: Use the new IPSec Summary and other NetMaster IPSec functions

- NetMaster provides many management & productivity enhancement tools for z/OS IPSec
- Management of filters and tunnels
- IPSec performance monitoring – special IPSec related attributes
- IPSec Packet Trace header decoding (*not* decryption)

* Security Awareness

Scenario 3

How many of our current Telnet sessions are secured?

- A z/OS IP host can have any combination of unsecured Telnet connections, Telnet connections to a specific Telnet/SSL port, and Telnet connections automatically secured by AT-TLS
- Right now, what is your exact combination of secure and unsecure Telnet connections?

A: Use the new IP Security Telnet Summary

- NetMaster provides 4 different Secured Connection Summary lists: for all SSL/TLS, for AT-TLS only, for FTP, and for Telnet
- Secure FTP and Telnet lists can optionally include un-secured connections, so these can be compared

Secured Connection Summary Lists


```
---- IP Security Menu - Help ------------------Page 1 of 2


S    - SSL/TLS Summary
Select this option to display counts of active
connections using SSL or TLS, summarized by task name.
This information is provided by the Packet Analyzer,
based on examination of packets flowing on the
connections.

A    - AT-TLS Summary
Select this option to display counts of active
connections using AT-TLS, summarized by task name, and
showing the policy states and security levels.

F    - FTP Summary
Select this option to display counts of active FTP
connections, summarized by user ID, and showing the
security mechanisms and levels in use.

T    - Telnet Summary
Select this option to display counts of active Telnet
connections, summarized by VTAM application, and showing
the security mechanisms and levels in use.
```

Secured Telnet and Secured FTP Summary Lists

SHARE
Technology · Connections · Results

```
DENM44-------------------- TCP/IP : Telnet Summary ---------------------TCPIP31
Command ===>                                                Scroll ===> CSR

     Active Secured Telnet Connections ... 2
                                                        S=Display Connections
                        Active    --AT-TLS Secured--  -----Security Method-----
     Appl      Stack     Conns      No     Yes  Inpro   Basic  AT-TLS SecurePort
     A31IT081  TCPIP31        1       0       1      0       0       1          0
     TPX31     TCPIP31       14      13       1      0      13       1          0

Page 2...
                        Active    --AT-TLS Secured--  ------Security Level--------
      Appl      Stack     Conns      No     Yes  Inpro  SSLv2  SSLv3  TLSv1  TLSv1.1
      A31IT081  TCPIP31        1       1       1      0      0      1      0        0
      TPX31     TCPIP31       14      13       1      0      0      1      0        0
```

```
DENM44---------------------- TCP/IP : FTP Summary ----------------------TCPIP31
 Command ===>                                                Scroll ===> CSR

      Active Secured FTP Connections ... 4
                                                        S=Display Connections
                        ---Conns---  --Security Status--  ---Security Method---
      UserId    Stack     Cntl  Data  Clear Private  Safe  AT-TLS GSSAPI TLS-FTP
      ADUPR01   TCPIP31       2     0      0       0     2       2      0       0
      GAODI01   TCPIP31       2     0      0       0     2       2      0       0

Page 2...
                        ---Conns---  ---------Security Level---------
      UserId    Stack     Cntl  Data    SSLv2   SSLv3   TLSv1  TLSv1.1
      ADUPR01   TCPIP31       2     0       0       2       0        0
      GAODI01   TCPIP31       2     0       0       2       0        0
```

* History and Auditing

Scenario 4

How can I view our connection details in a spreadsheet?

- Offline z/OS IP connection details are useful for audit and reporting purposes
- Usually, this info needs to be manually moved from z/OS files

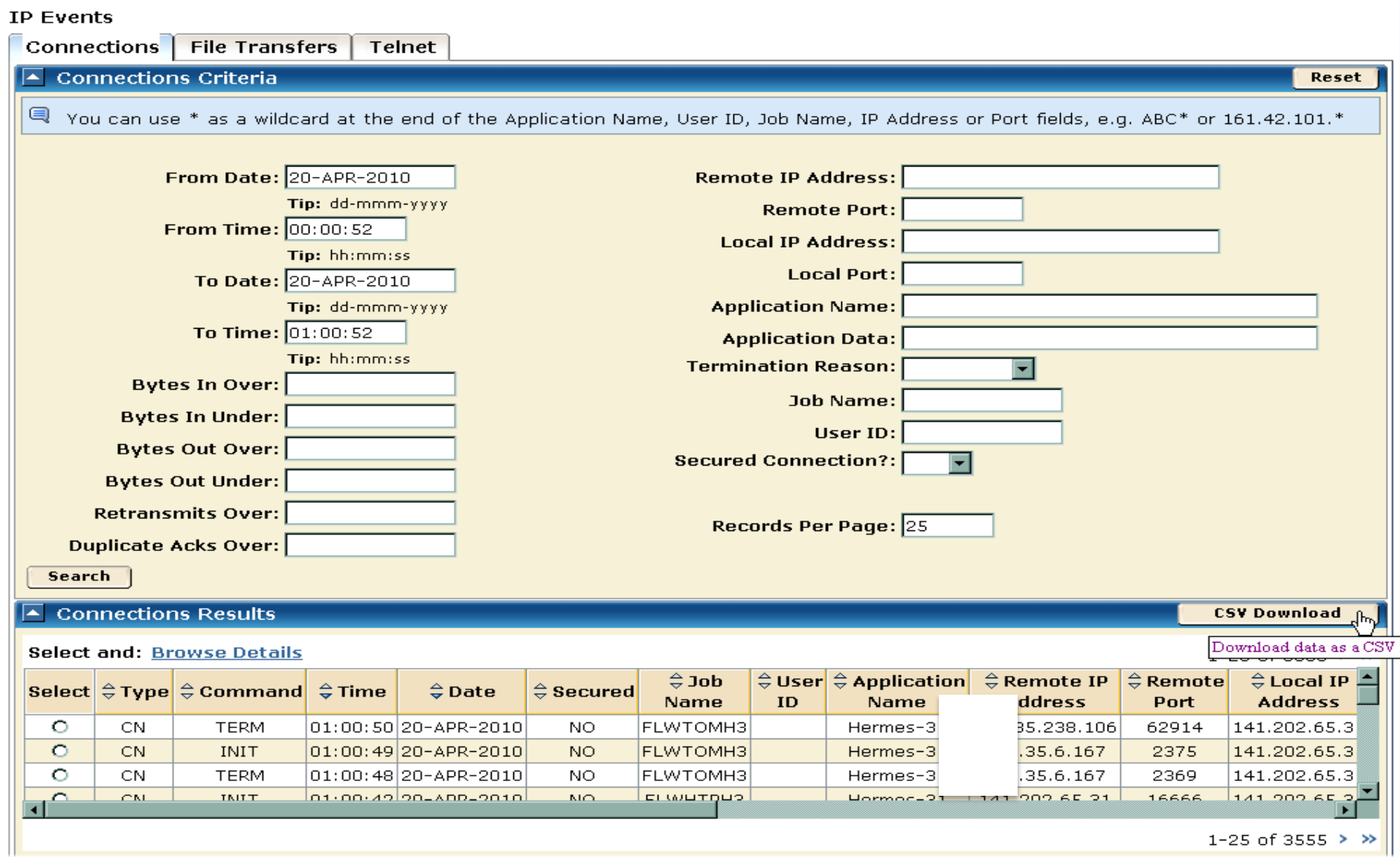
A: Use the new Web IP Event History

- Displays the same data as the 3270 option (enhanced with secured events lists)

```
DENM17------------------- TCP/IP : Browse Events
Command ===>

    Description
___ List All Connection Events
___ List All FTP Events
___ List All Telnet Events
___ List Failed File Transfers
___ List Secured Connection Events
___ List Secured FTP Events
___ List Secured Telnet Events
___ Perform Custom Search
___ Search Connection Events
___ Search FTP Events
___ Search Telnet Events
    **END**
```

WebCenter IP Event History



* DB2 Analysis

Scenario 5

I'm a z/OS DB2 DBA.
What SQL payload is flowing over this DB2 connection to ABC?

- The Subsystem Traffic Explorer identifies the busiest DB2 SSIDs
- Connection Lists show individual connections to z/OS DB2
- An individual connection looks busy / wrong / interesting / dangerous ....

  What is it doing? And you need to find out in a hurry...

A: Use the new SmartTrace DRDA decoding

- NetMaster SmartTrace Packet Tracing will - of course - show the packet flow and content of DB2 connections.
- So you trace it. But what are you looking at?
- You are looking at DRDA. **DRDA** is the protocol used for IP communications by DB2. DRDA consists of many DDM commands – some of these contain SQL, some don't

SmartTrace DB2 Trace: without Decoding


```
Definition D81ADIST5141
Stack .... T                          Description  e     `  NSM DB2 JCBC ac
Local Host 1  .202.65.31          <--> Foreign Host 1  .42.241.84
Local Port 5 41                        Foreign Port 4   4
Protocol   TCP

      ---Packet Data In Hex (16 Bytes)--- -----EBCDIC----- -----ASCII------
     Initial packets for connection:
00001 13781415 35ADEA88 00000000 7002FAF0|      h        0| x  5       p
00002 14151378 BE97B9BC 35ADEA89 60128000|    p     i-     |   x    5   `
00003 13781415 35ADEA89 BE97B9BD 5010FAF0|      i p  &  0  | x  5       P
00004 13781415 35ADEA89 BE97B9BD 5018FAF0|      i p  &  0  | x  5       P
00005 14151378 BE97B9BD 35ADEB47 50187F42|    p      & "   |   x    5  GP  B
00006 13781415 35ADEB47 BE97BA28 5018FA85|       p   &  e  | x  5  G   (P
00007 14151378 BE97BA28 35ADEC49 50187EFE|    p      & =   |   x   (5  IP ~
00008 13781415 35ADEC49 BE97BADD 5018F9D0|       p   & 9}  | x  5  I    P
00009 14151378 BE97BADD 35ADEE19 50187E30|    p      & =   |   x    5   P ~0
00010 13781415 35ADEE19 BE97BC7D 5018F830|       p '& 8    | x  5       }P  0
00011 14151378 BE97BC7D 35ADEFFF 50187E1A|    p '    & =   |   x   }5   P ~
00012 13781415 35ADEFFF BE97BE58 5018F655|       p   & 6   | x  5       XP  U
00013 14151378 BE97BE58 35ADF207 50187DF8|    p    2 & '8   |   x   X5   P }
00014 13781415 35ADF207 BE97C033 5018FAF0|     2   p{ &  0  | x  5       3P
00015 14151378 BE97C033 35ADF39A 50187E6D|    p{   3 & =_  |   x   35   P ~m
00016 13781415 35ADF39A BE97C233 5018F8F0|     3   pB & 80  | x  5       3P
00017 14151378 BE97C233 35ADF561 50187E39|    pB   5/& =   |   x   35  aP ~9
00018 13781415 35ADF561 BE97C40E 5018F715|     5/  pD & 7   | x  5  a    P
00019 14151378 BE97C40E 35ADF570 50187FF1|    pD   5 & "1   |   x    5  pP
00020 13781415 35ADF570 BE97C449 5018F6DA|     5   pD & 6   | x  5  p    IP
     Traced packets:
00021 14151378 BE97C449 35ADF721 50187E4F|    pD   7 & =|  |   x   I5  !P ~O
00022 13781415 35ADF721 BE97C6A2 5018FAF0|     7   pFs&  0  | x  5  !    P
00023 14151378 BE97C6A2 35ADF730 50187FF1|    pFs  7 & "1   |   x    5  0P
00024 13781415 35ADF730 BE97C6DD 5010FAB5|     7   pF &     | x  5  0    P
00025 13781415 35ADFCDC BE97C6DD 5018FAB5|         pF &     | x  5       P
```

The same SmartTrace DB2 Trace: with DRDA Decoding


```
Definition D81ADIST5141
Stack .... TCPIP21                          Description  example NSM DB2 JCBC ac
Local Host 1   .202.65.31            <-->  Foreign Host 1   .42.241.84
Local Port 5141                             Foreign Port 4   4
Protocol   TCP

      Dir  +Time Bytes  Summary Information
     Initial packets for connection:
00001 <-        -     48  Syn      Win=64240 RelSeq=0 MaxSeg=1460 Sack-P
00002  -> <0.001     44  Ack Syn  Win=32768 RelSeq=0 RelAck=1 MaxSeg=1452
00003 <-   0.014     40  Ack      Win=64240 RelSeq=1 RelAck=1
00004 <-  <0.001    230  DDM-Req: 1(EXCSAT) 2(ACCSEC)
00005  -> <0.001    147  DDM-Rsp: 1(EXCSATRD) 2(ACCSECRD)
00006 <-   0.014    298  SQL-Cmd: 2(CONNECT)
00007  ->  0.005    221  DDM-Rsp: 1(SECCHKRM) 2(ACCRDBRM)
00008 <-   0.016    504  SQL-Cmd: 1(PREPARE; SELECT (1-(cast(sum(BP_SYNC_REA
00009  ->  0.002    456  SQL-Rsp: 2(100(02000))
00010 <-   0.021    526  SQL-Cmd: 1(COMMIT) 2(PREPARE; SELECT (1-(cast(sum(B
00011  ->  0.001    515  SQL-Rsp: 3(100(02000))
00012 <-   0.014    560  SQL-Cmd: 1(COMMIT) 2(PREPARE; SELECT (CAST((DB2_TCB
00013  ->  0.002    515  SQL-Rsp: 3(100(02000))
00014 <-   0.015    443  SQL-Cmd: 1(COMMIT) 2(PREPARE; SELECT DEADLOCK...) 3
00015  -> <0.001    552  SQL-Rsp: 3(100(02000))
00016 <-   0.015    495  SQL-Cmd: 1(COMMIT) 2(PREPARE; SELECT (1-(CAST(EDM_M
00017  -> <0.001    515  SQL-Rsp: 3(100(02000))
00018 <-   0.014     55  SQL-Cmd: 1(COMMIT)
00019  -> <0.001     99  DDM-Rsp: End Unit of Work Condition (Sev=4)
00020 <-   0.015    473  SQL-Cmd: 1(PREPARE; SELECT DISTINCT...) 2(OPEN)
     Traced packets:
00021  ->  0.001    641  SQL-Rsp: 2(100(02000))
00022 <-   0.015     55  SQL-Cmd: 1(COMMIT)
00023  -> <0.001     99  DDM-Rsp: End Unit of Work Condition (Sev=4)
00024 <-   0.017   1492  Ack      Win=64181 RelSeq=3240 RelAck=3361
00025 <-  <0.001    867  Ack Psh  Win=64181 RelSeq=4692 RelAck=3361
```

* Web Analysis

Scenario 6

I'm a z/OS Web developer. How can I see more of what my application is doing?

- More and more Java, Web and SoA applications are being hosted on z/OS
- Many native z/OS and USS diagnostics are verbose and unfriendly to use, particularly for programmers use to other platforms
- Productivity-enhancing z/OS-hosted tools are essential during development

A: Use the new SmartTrace HTTP/SOAP decoding & Data Flow Report

- SmartTrace provides one-step access to IP packet tracing
- **HTTP decoding** is now automatic
- **SOAP decoding** for Web services
- The **TCP Data Flow Report** is a special representation of TCP packet exchanges to show only the data exchanges between TCP peer applications. This removes all other information that an application programmer would not be interested in seeing or knowing. Enhanced with Packet Reassembly

SmartTrace Packet List including SOAP request


```
DENM44---------------------- SmartTrace : Packet List ---------------------------
Command ===>                                                  Scroll ===> CSR

                                                              S/V=View P=Print

     Definition WWSOAP
     Stack .... TCPIP11                          Description  SOAP request to USD and
     Local Host *                          <--> Foreign Host 141.202.194.125
     Protocol                                   Foreign Port 8080

          Lo      st       LPort Dir   +Time Bytes   Summary Information
____ 00006 14    65.11    6942   ->  <0.001   446   SOAP-Dat: <Body> <Login>
____ 00007 14    65.11    6942   <-   0.090   615   Rsp: HTTP/1.1 200 OK
____ 00008 14    65.11    6942   <-  <0.001    57   Ack Psh Win=64939 Seq=4658658
____ 00009 14    65.11    6942   ->  <0.001    52   Ack Psh Win=32200 Seq=1043352
____ 00010 14    65.11    6942   ->   0.045    52   Ack Psh Fin Win=32200 Seq=104
____ 00011 14    65.11    6942   <-  <0.001    52   Ack     Win=64939 Seq=4658658
____ 00012 14    65.11    6942   <-  <0.001    52   Ack Fin Win=64939 Seq=4658658
____ 00013 14    65.11    6942   ->  <0.001    52   Ack Psh Win=32200 Seq=1043352
____ 00014 14    65.11    6943   ->   0.040    60   Syn     Win=32768 Seq=1043420
____ 00015 14    65.11    6943   <-  <0.001    60   Ack Syn Win=65535 Seq=2007207
____ 00016 14    65.11    6943   ->  <0.001    52   Ack     Win=32768 Seq=1043420
____ 00017 14    65.11    6943   ->   0.008   263   Ack Psh Win=32768 Seq=1043420
____ 00018 14    65.11    6943   <-   0.141    52   Ack     Win=65324 Seq=2007207
s___ 00019 14    65.11    6943   ->  <0.001  1199   SOAP-Dat: <Body> <CreateReque
____ 00020 14    65.11    6943   <-   0.122   871   Rsp: HTTP/1.1 200 OK
____ 00021 14    65.11    6943   <-  <0.001    57   Ack Psh Win=64177 Seq=2007208
____ 00022 14    65.11    6943   ->  <0.001    52   Ack Psh Win=31944 Seq=1043422
____ 00023 14    65.11    6943   ->   0.016    52   Ack Psh Fin Win=31944 Seq=104
____ 00024 14    65.11    6943   <-   0.001    52   Ack     Win=64177 Seq=2007208
____ 00025 14    65.11    6943   <-  <0.001    52   Ack Fin Win=64177 Seq=2007208
____ 00026 14    65.11    6943   ->  <0.001    52   Ack Psh Win=31944 Seq=1043422
____ 00027 14    65.11    6944   ->   0.113    60   Syn     Win=32768 Seq=1043484
____ 00028 14    65.11    6944   <-  <0.001    60   Ack Syn Win=65535 Seq=3001297
____ 00029 14    65.11    6944   ->  <0.001    52   Ack     Win=32768 Seq=1043484
____ 00030 14    65.11    6944   ->   0.002   255   Ack Psh Win=32768 Seq=1043484
____ 00031 14    65.11    6944   <-   0.179    52   Ack     Win=65332 Seq=3001297
____ 00032 14    65.11    6944   ->  <0.001   403   SOAP-Dat: <Body> <Logout>
____ 00033 14    65.11    6944   <-   0.001   554   Rsp: HTTP/1.1 200 OK
____ 00034 14    65.11    6944   <-  <0.001    57   Ack Psh Win=64981 Seq=3001297
```

SmartTrace TCP Data Flow Report


```
DENM44--------------- SmartTrace : TCP Data Flow Report ----------------------
Command ===> _                                              Scroll ===> CSR

Local Host/Port:     <-----> Remote Host/Port:
141.202.65.11..8644          155.35.123.65..3176

Pkt#00013 Dir: IN  Date: 18-JUN-2007 Time: 01:37:05.173865
          (DataLen=394)
 <<
 << GET /common/main.esp HTTP/1.1
 << Accept: */*
 << Accept-Language: en-au
 << Accept-Encoding: gzip, deflate
 << User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; GIS IE 6.0
 <<             Build 20060616; .NET CLR 1.1.4322)
 << Host: us.[illegible]ca.com:8644
 << Connection: Keep-Alive
 << Cookie: WEBTRENDS_ID=155.35.123.65-1176695929.705262;
 <<         SOLVE8644=D0D34ACFC464E26AC0C1B1B3A0D1B431F0D3D4CCDF9DED4EBDEF9F9C8
 <<         C9F4ACF

Pkt#00014 Dir: OUT Date: 18-JUN-2007 Time: 01:37:05.176824 Elapsed: .002959
 F1=Help      F2=Split     F3=Exit      F4=Print     F5=Find      F6=Reassem
 F7=Backward  F8=Forward   F9=Swap                              F12=Session
```

* Predicting Growth

Scenario 7

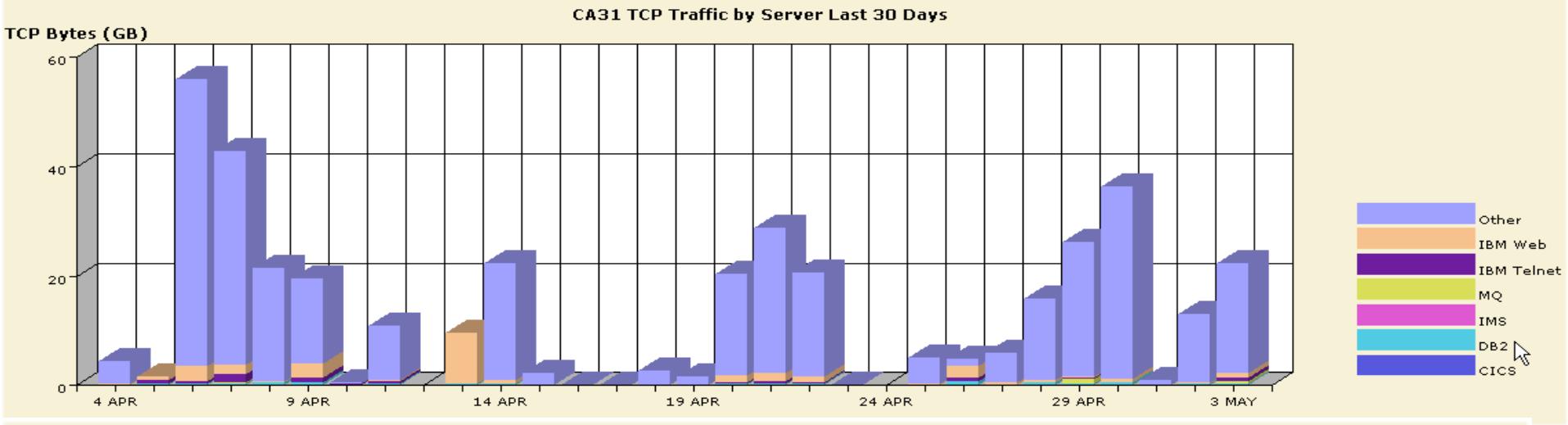
How DB2 TCP/IP connections are there a day? Is this growing?

- Our SNA sessions to DB2 haven't changed much for years… but surely DB2 remote access is growing?
- If I can show that, I can get more resources for my DB2 group. Maybe the growth is with users coming in with TCP/IP?
- Maybe I need to train more of my DB2 people in basic TCP/IP?

A: Use the NetMaster IP Growth Tracker

- Illustrate the increase over time in mainframe IP network activity
- Out-of-the-box tracking, no setup, no databases
- Connection and Traffic totals are kept indefinitely

IP Growth Tracker, TCP Traffic Growth



Date	TCP Bytes (Total)	CICS	DB2	IMS	MQ	IBM Telnet	IBM Web	TCP (Other)	TCP Connections
4 APR	4,390,539,717	0	119,860,682	0	0	725,826	135,771,444	4,134,181,765	245,126
5 APR	0	23,828	231,128,422	0	0	640,416,837	719,469,879	0	0
6 APR	56,014,335,211	167,864	275,604,934	0	148,229,496	362,247,365	2,722,615,492	52,505,470,060	394,942
7 APR	42,764,851,062	7,230	394,128,108	0	181,341,750	1,376,375,200	1,733,115,914	39,079,882,860	340,622
8 APR	21,442,093,761	546,862	459,633,662	0	33,099,406	94,920,342	93,672,059	20,760,221,430	284,298
9 APR	19,606,701,833	40,095,093	549,289,569	0	0	844,782,057	2,533,143,911	15,639,391,203	494,922
10 APR	534,175,687	0	197,727,488	0	0	41,769,322	1,558,254	293,120,623	124,117
11 APR	10,818,018,168	0	231,231,626	0	0	444,675,045	267,484,367	9,874,627,130	698,175
12 APR	0	0	0	0	0	0	0	0	0
13 APR	0	154,652	268,154,796	0	0	131,598,424	9,267,433,937	0	0
14 APR	22,238,183,725	13,191	255,481,129	0	0	74,130,762	636,777,449	21,271,781,194	353,671
15 APR	2,291,443,756	4,766	5,667,095	0	0	6,894,687	34,501,362	2,244,375,843	62,774
16 APR	989,183	2	2,446	0	0	2,976	14,893	968,865	27
17 APR	46,904,192	0	18,051,507	0	0	8,011	2,736,515	26,108,159	2,506

Code-free Automation

Scenario 8

Are we getting a lot of connection failures?

- Connection totals and active counts get lots of attention.
- What about connection failures?
- These can be close to invisible, but can indicate a wide variety of potential problems, such as:
- Security: is someone trying a random or brute force attack?
- Application performance: is an application unwell or unavailable?

A: Use the new Real-Time IP Event Detectors

- NetMaster Packet Analyzer detects packet-based events by watching real-time packet streams
- For ‘genuine’ connection failures caused by TCP Server RST, use the **SVRRESET** detector
- For connection attempt failures, use the **NOLISTEN** detector
- Normal NetMaster Alerts are raised

SVRRESET IP Event Detector Setup Criteria


```
DENM17------------------ TCP/IP : TCP Server Reset Criteria ---------------------
Command ===>

Short Description ..... WW Example 1                        Status ACTIVE

Server Host ........... ____________________________________ (Generic allowed)
Server Port ........... ____________________________________ (Range allowed)

Client Host ........... ____________________________________ (Generic allowed)
Client Port ........... ____________________________________ (Range allowed)

Active Alert Limit .... 5              (Maximum active alerts. Range 1 to 20)
```

A TCP Server Reset event detector watches the TCP connections and detects when an established connection is reset by the server end of the connection. If detected an alert is raised indicating the connection partners.

This is a real-time Packet Analyzer based event. Client-initiated resets are ignored. (Also ignored are resets sent by the stack, in response to connection attempts to non-existent port listeners.)

Note: This detector only applies to packets coming from or going to the z/OS system seen by the Packet Analyzer.

Use this type of event detector when you want to know of the following conditions:

- **All server reset connection failures involving a specific application**
- **Any server reset connection failures and who they are most often happening to**

Recap - Elements of success

NetMaster Strengths

Monitoring Functions	• SNA, TCP/IP, MVS, File Transfers, other
Historical Information	• Trends, Reporting, Diagnosis
Diagnostics	• Proactive, Intuitive, Flexible
Reporting	• Intuitive, Flexible

Questions?

Craig.guess@ca.com