Hidden Gems in *CA NetMaster for TCP/IP*: Come Explore where You May Have Missed Them

Craig Guess
Rob Scalzo
CA Technologies

August 5th, 2014
Session 16080

#SHAREorg

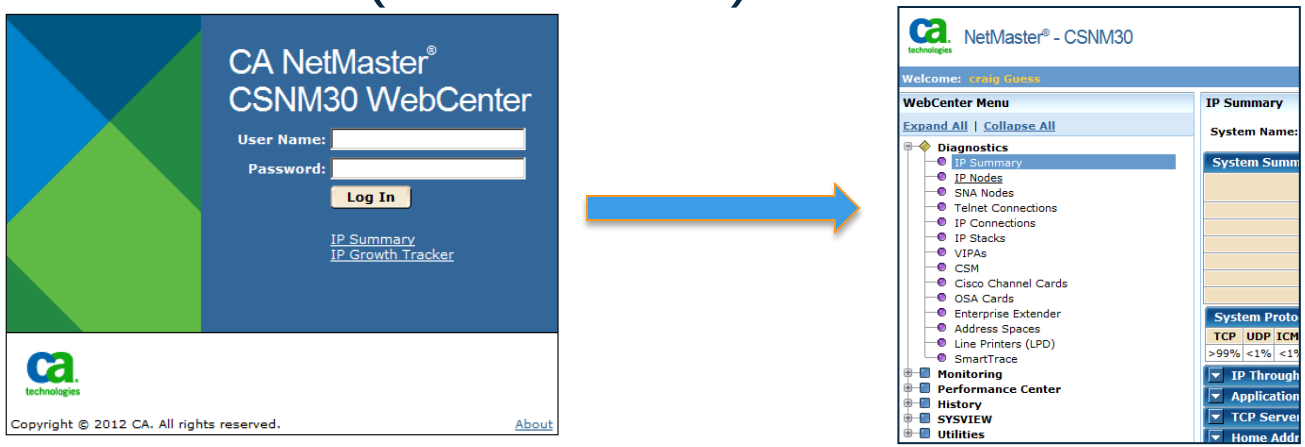
Agenda

- WebCenter
- Traffic Stats vs /Perf
- Event Detectors
- SmartTrace
- Growth Tracker
- Creating Emails
- Performance Charts and Graphs
- Integration to OPS/MVS, SYSVIEW

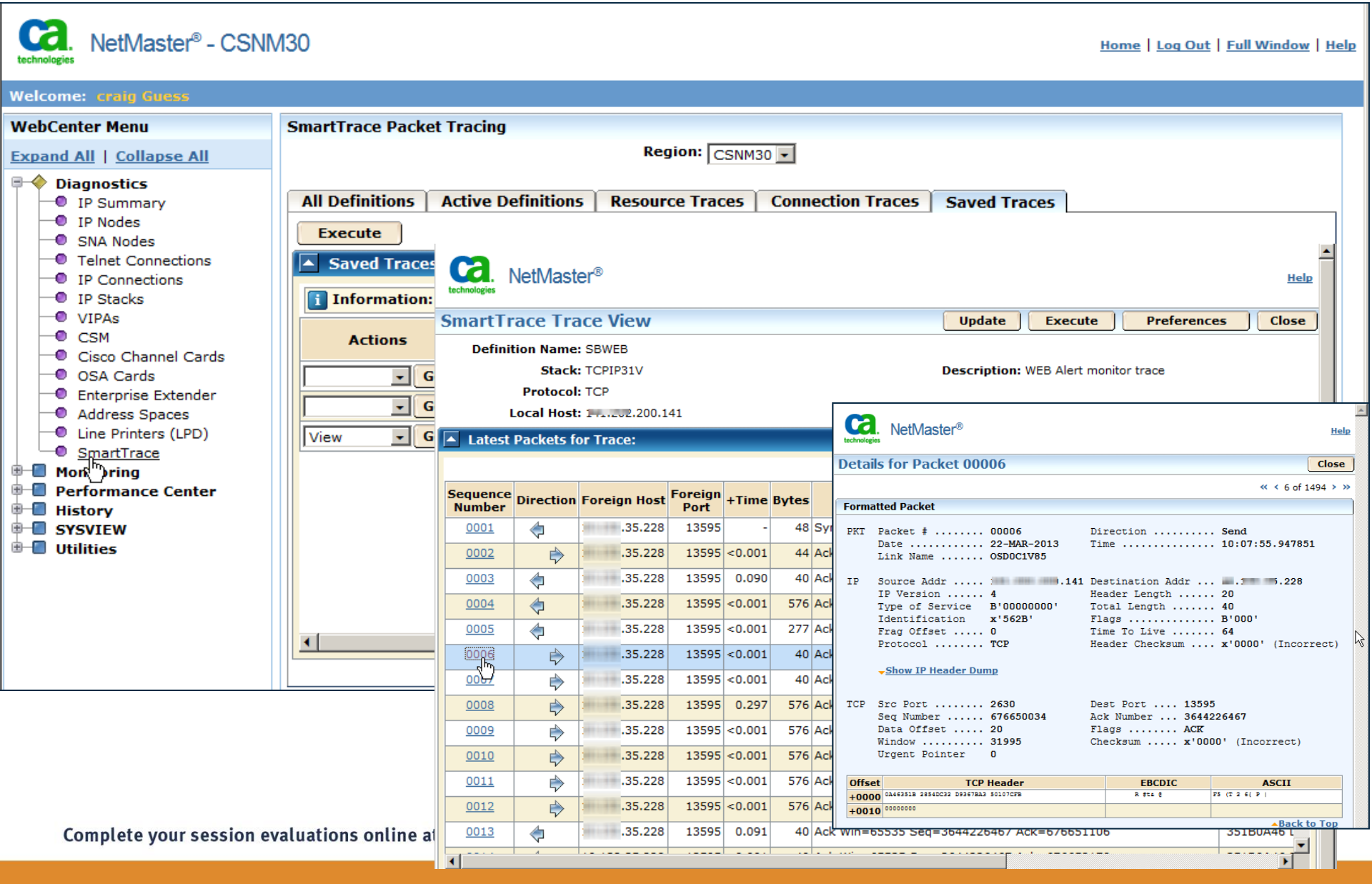
WebCenter

WebCenter

- No need for external web servers
- Easily configured and instantly available
- Can be secured with SSL if required
- Can control access to WebCenter menu options programmatically by using the variables in the CC2DEXEC($W3MH01X)



Flexibility

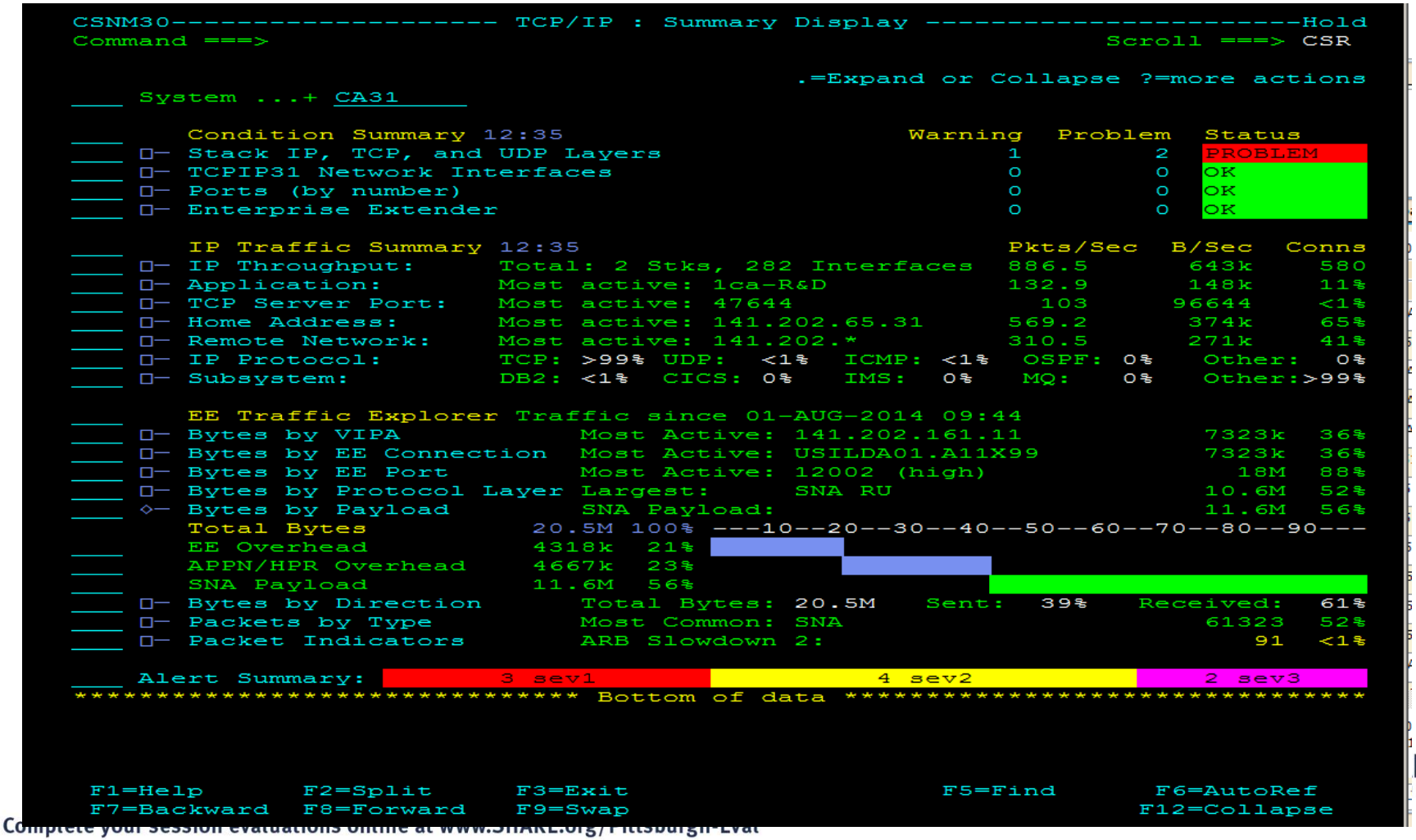


Complete your session evaluations online at

Traffic Stats vs /Perf

Traffic Summary - /IPSUM
Real-time information

- Real-time information on everything NetMaster is monitoring
  - Provides a way to view lots of data at a glance.



Performance Overview - /Perf
Longer periods of time

```
CSNM9-------------------- Performance Overviews Menu ------------------------CA11
Command ===>                                                  Scroll ===> CSR

                                                S=Show Performance Overview from CA11
____  Business Views              Business Applications
____  Applications                Telnet Applications
____                              Address Spaces
____                              CSM
____  Sessions and Connections    Stack IP Connections
____                              Home Addresses
____                              Network IP Connections
____                              Stack Telnet Connections
____                              Network Telnet Connections
____                              Stack FTP Connections
____                              FTP Users
____                              Network FTP Connections
____  Protocols and Ports         Stack IP, TCP, and UDP
____                              Ports
____  IP Networking               Stack IP, TCP, and UDP
____                              IP Nodes
____  Logical Devices             Enterprise Extender
____                              Enterprise Extender Connections
____                              APPN/HPR
____                              VIPA
____  Devices and Links           Stack Network Interfaces
____                              OSA Cards
____                              Cisco Channel Cards            (not monitored)
____                              NCPs
```

Performance Overview
Review up to 10 weeks of data

- Allows one to review Hourly, Daily and Weekly information
  - Weekly Interval List, can drill down to see Days and hourly

```
CSNM9---------------- TCP/IP Performance : Baseline List --------------------CA11
Command ===>                                                  Scroll ===> CSR

     Performance Data .... Connection Workload, by Application
     Resource ............ Business Application $Bank-FX

                                        S=Samples H=Hours D=Days W=Weeks B=BLvalues
                                  Last Start   HourOfDay HourOfDay   DayOfWeek
      Attribute    Stack       Summary  Hour    Baseline     % Diff    Baseline
____  ConActive    TCPIP11        18.2  12:00        10.8       +68%        12.2
____  ConBytes     TCPIP11       17.9M  12:00         8.1M      +120%       367.4M
_w_   ConConnects  TCPIP11       737.0  12:00         1.0K       -28%         2.4K
    **END**
```

```
CSNM9------------------- TCP/IP : Weekly Interval List -------------------------
Command ===>                                                  Scroll ===> CSR

     Performance Data .... Connection Workload, by Application
     Resource ID ......... Business Application $Bank-FX, Stack TCPIP11
     Attribute ID (Type)   ConConnects (counter)
     Description ......... Connections for application
     Period .............. Last 10 weeks

                                        D=Show days of this week  H=Show hours
     Week          Date and Time        Hourly Total Daily Total
____ This week     Fri 01-Aug-2014 13:00         5.2K        25.5K
____ 1 week ago    Fri 25-Jul-2014 13:00         4.5K        48.6K
____ 2 weeks ago   Fri 18-Jul-2014 13:00         4.5K        19.2K
____ 3 weeks ago   Fri 11-Jul-2014 13:00         80.0        57.0K
____ 4 weeks ago   Fri 04-Jul-2014 13:00         80.0        14.2K
____ 5 weeks ago   Fri 27-Jun-2014 13:00         4.7K        33.3K
____ 6 weeks ago   Fri 20-Jun-2014 13:00          3.0        36.8K
____ 7 weeks ago   Fri 13-Jun-2014 13:00        208.0        35.8K
____ 8 weeks ago   Fri 06-Jun-2014 13:00         4.5K        42.4K
____ 9 weeks ago   Fri 30-May-2014 13:00         4.5K        27.3K
   **END**
```

Event Detectors

Event Detectors – proactive management

- CONNSTAT – Monitors number of connections with a client.
  - Insure minimum number of connections present, i.e., EE requirements.
- SVRRESET – Monitors TCP connections that are reset by server.
  - Alerts if client trying to connect but can't, helps insure PCI compliancy.
- SSLHFAIL – Monitors Secure Sockets Layer(SSL) handshake failures
  - Many levels of SSL Handshake errors possible, helps eliminate wasted time in determining cause of failure.
- TCPSTART – Monitors client/server connections.
  - Restrict the detection to specified client-server connections

Event Detector
TCP Connection Status – (CONNSTAT)

- Detects when a server has 0 connections
  - When you have mission-critical connections to a z/OS IP application that must remain up 24 x 7.
  - You must maintain a certain number of connections to a z/OS IP application to provide the necessary health indication, traffic throughput, or volume.

```
------------------------ TCP/IP : TCP Connection Status ----------------------------
Command ===>                                                  Function=Browse

Short Description ..... SAMPLE: Server has 0 connections        Status INACTIVE

Monitor TCP Connection Status for:
Stack Name ............ TCPIP99
Server Host ........... 123.123.123.123
Server Ports .......... 12345
Client Host ........... 234.234.234.234
Connections Active .... 1
Auto Alert Clear? ..... NO


Create Alert:
Description  &$IPSTDDESC
Severity ... 4

Initiate Actions:
**NONE**
```

Event Detector
TCP Server Reset – (SVRRESET)

- Detects when an established connection is reset
  - All server reset connection failures involving a specific application.
  - Any server reset connection failures and who they are most often happening to.

```
CSNM9------------------ TCP/IP : TCP Server Reset Detector ----------------------
Command ===>                                                 Function=Browse

Short Description ..... SAMPLE: RST sent by server 12345       Status INACTIVE

Monitor TCP Server Resets for:
Server Host ............ 123.123.123.123
Server Port ............ 12345
Active Alert Limit .... 5




Create Alert:
Description   &$IPSTDDESC
Severity ... 4

Initiate Actions:
**NONE**
```

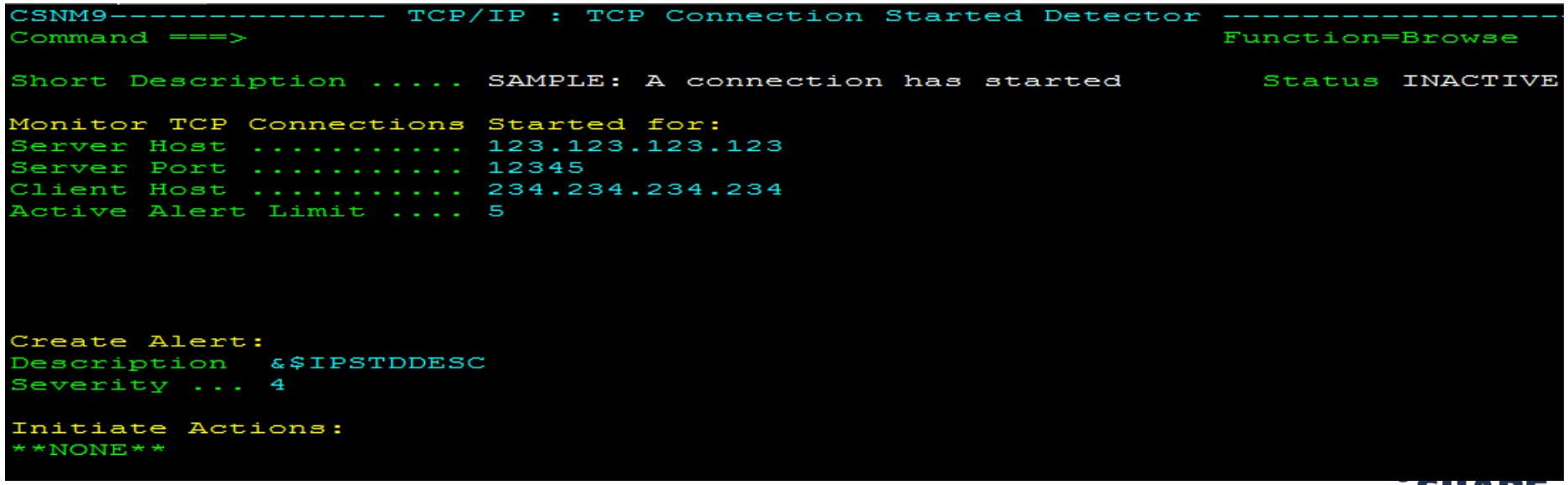
Event Detector
SSL Handshake failure – (SSLHFAIL)

- Detects when SSL security negotiation fails
  - You need to be notified of all connection failures of a specific critical secure connection.
  - You need to be notified of all connection failures to a secure application.
  - You want to know of any SSL handshake problems and where they are occurring most often.

```
CSNM9--------------- TCP/IP : SSL Handshake Failure Detector --------------------
Command ===>                                                 Function=Update

Short Description ..... SAMPLE: SSL failure for a server       Status INACTIVE

Monitor SSL Handshake Failures for:                            (F4 to set)
Server Host ........... 123.123.123.123
Server Port ........... 12345
Active Alert Limit .... 5




Create Alert:                                                  (F5 to set)
Description   &$IPSTDDESC
Severity ... 4

Initiate Actions:                                              (F6 to set)
**NONE**
```

Event Detector
Connection started – (TCPSTART)

- Detects when a connection has started for local/remote host or port
  - You need to be notified of all connections from a specific remote host, such as an external gateway.
  - You want to know of all connections to a restricted application and where they come from.
  - You want to know all connections between specific remote host and application.



SmartTrace

SmartTrace Gems

Both Simple and advanced options use the same set of tools and interface for viewing the trace – no additional learning curve.

- SAVE – stored all traces in one repository (no additional dataset required).
- PRINT – a choice of printers or external data sets/HFS or even email.
- EXPORT – to 3rd party formats CTRACE (IBM only) and libpcap (distributed platform), collect the packets in SmartTrace and use your favourite packet viewer.

SmartTrace
Utilities

- Easy to use interface and utilities for managing traces
  - SAVE, EXPORT, PRINT

```
CSNM9---------------------- TCP/IP : Packet Tracing Menu ----------------------/SMART
Select Option ===>

   A    - Add SmartTrace Definition                                  TRADD
   L    - List All SmartTraces                                       TRALL
   LA   - List Active and Ended SmartTraces                          TRACES
   LS   - List All Saved SmartTraces                                 TRSAV
   EE   - EE SmartTrace Menu                                         EETRACE
   IM   - Import libpcap Trace File                                  LIBPCAP
   CT   - Packet Tracing using Component Trace (CTRACE)              CTRACE
   X    - Exit


Link Name .....+ CSNM9_______   (
```

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

                                                            S/V=View P=Print
   Definition DBTEST2
   Stack .... TCPIP11                    Description  FTP causing lunchtime c
   Local Host *                       <--> Foreign Host 138.42.36.40
   Protocol   TCP

        Local Host      LPort Dir Port   +Time Bytes  Summary Information
___ 00001 141.202.66.11   21    <-  1169       -    48  Syn     Win=65535 Seq=3
___ 00002 141.202.66.11   21     -> 1169  <0.001    44  Ack Syn Win=32768 Seq=1
___ 00003 141.202.66.11   21    <-  1169   0.059    40  Ack     Win=65535 Seq=3
___ 00004 141.202.66.11   21     -> 1169   0.063   106  Rsp: 220-FTPD111 IBM FT
___ 00005 141.202.66.11   21    <-  1169   0.239    40  Ack     Win=65469 Seq=3
___ 00006 141.202.66.11   21     -> 1169  <0.001   100  Rsp: 220 Connection wil
___ 00007 141.202.66.11   21    <-  1169   0.059    54  Req: user CAMTHA4
___ 00008 141.202.66.11   21     -> 1169   0.001    67  Rsp: 331 Send password
___ 00009 141.202.66.11   21    <-  1169   0.059    55  Req: PASS Saddam90
___ 00010 141.202.66.11   21     -> 1169   0.222    40  Ack Psh Win=32753 Seq=1
___ 00011 141.202.66.11   21     -> 1169   4.296   101  Rsp: 230 CAMTHA4 is log
___ 00012 141.202.66.11   21    <-  1169   0.059    48  Req: TYPE A
 F1=Help      F2=Split     F3=Exit                F5=Find
 F7=Backward  F8=Forward   F9=Swap     F10=Left    F11=Right
```

Exporting Traces and Reports

```
CSNM2---------------------------------- SmartTrace : Export Packet Trace ----------------------------------
Command ===>                                                                          Function=Export

 Trace Details ------------------------------------------------------------------------------------------
 Definition Name ..... TEST1023 - 1023test
 Stack ............... TCPIP11
 Description ......... CSNM2 packet trace to 1023
 Saved ............... 02-MAY-2012 at 18:39 by BEEST03
 Number of Packets ... 28
 -------------------------------------------------------------------------------------------------------

 Export Details -----------------------------------------------------------------------------------------
 Dataset or HFS File:

      ____________________________________________________
      ____________________________________________________
      ____________________________________________________

 Adjust Time By ......          (+/-hh:mm, mm must be 00 or 30)
 Output Format ....... LIBPCAP (LIBPCAP or CTRACE)
 -------------------------------------------------------------------------------------------------------
```

Export Trace

```
CSNM9---------------------- SmartTrace : Trace Reports ----------------------------
Command ===>                                                  Scroll ===> CSR

                                        S/V=View P=Print SAV=Save ?=More Actions

        IPCS Reports
____  □— UDP Sessions Report (70)
____  ◇— Flag Report
____  ◇— Interface Report
____  ◇— IP Address Report
____  ◇— UDP Port Report
s___  ◇— Protocol Summary Report
____  ◇— Session Summary Report
********************************** Bot
```

GR - listing Report - viewing

```
CSNM9------------- SmartTrace : IPCS Protocol Summary Report --------------------
Command ===>                                                  Scroll ===> CSR

Protocol Report

  Total     Input          Data   Output          Data       First yyyy/mm/dd hh.mm.ss
    250       175         24422       75          8891           1 2013/01/31 16:34:10
    250       175         24422       75          8891   Total

     1 Protocol(s) found

Protocol Summary Report
                    Input                          Output                        Total
Protocol   Packets          Bytes   Packets          Bytes   Packets          Bytes
Tcp              0              0         0              0         0              0
Udp            175          24422        75           8891       250          33313
Icmp             0              0         0              0         0              0
SNA              0              0         0              0         0              0
Other            0              0         0              0         0              0

Data Byte Totals
  Ip header:                5000
  Protocol Header:          2000
  Data :                   33313
  Total:                   40313

******************************** Bottom of data ********************************
```

Growth Tracker

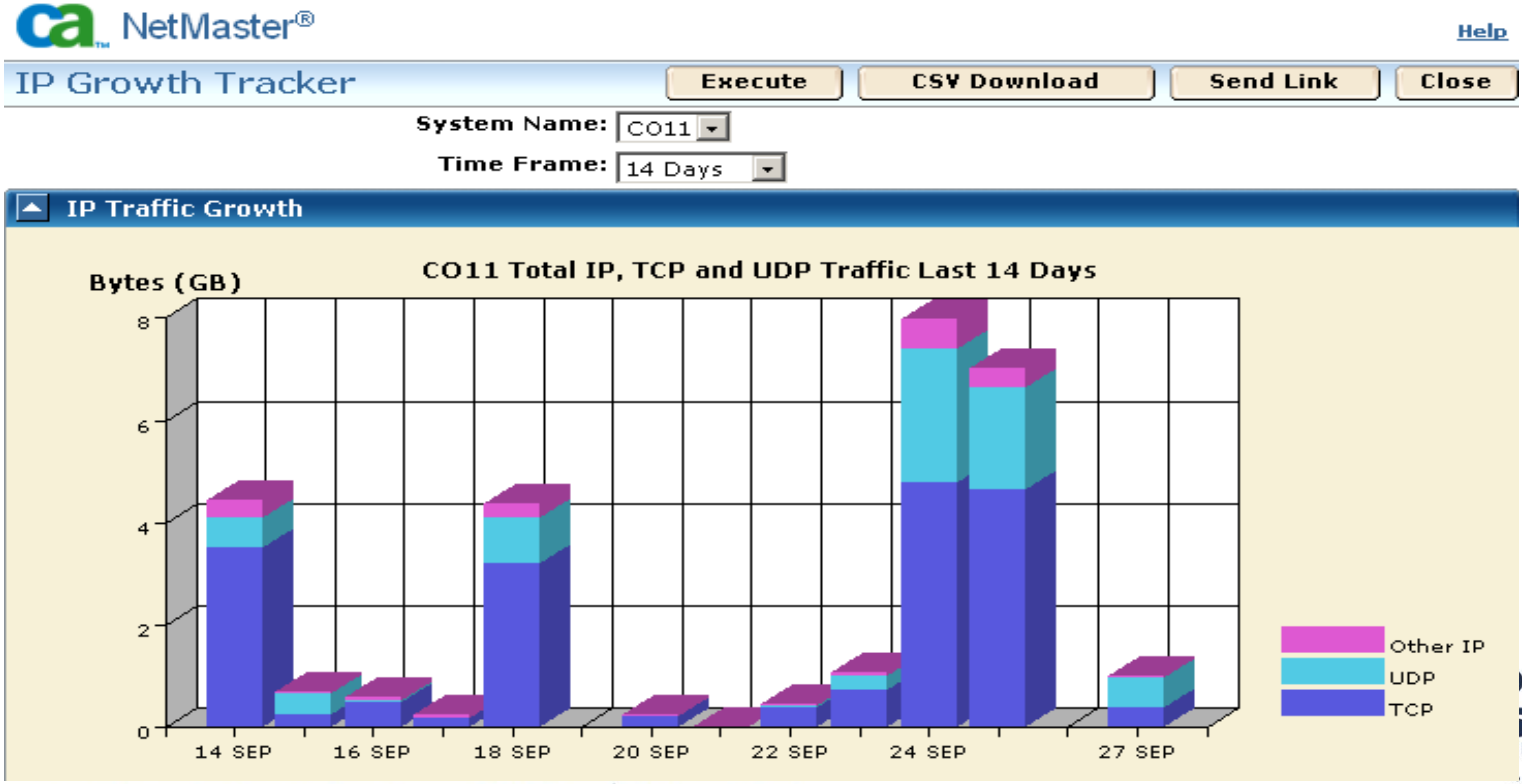
Growth Tracker

Out-of-the-box historical reporting on network activity

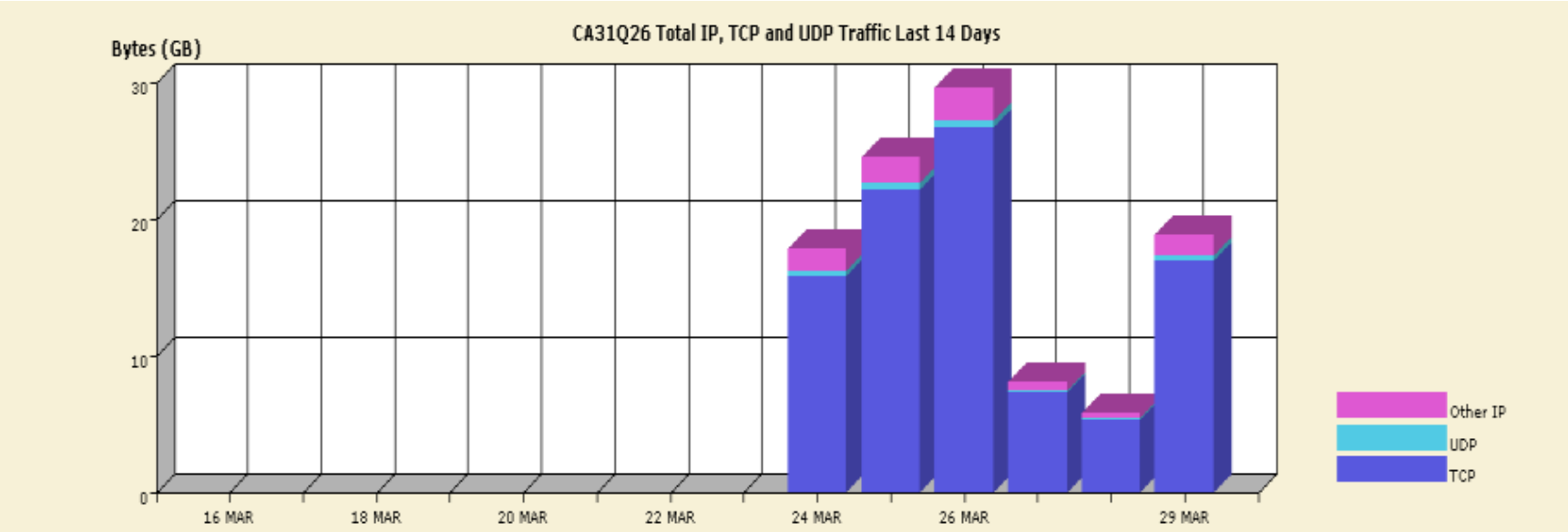
- IP Volumes, connections counts and connection durations are summed each day
  - Stored indefinitely
  - Multiple timeframes for reports supported
    - *14,30,60,90 day reports*
    - *6, 12 and ALL month reports*
- Provides meaningful insights into network activity
- Assists in network planning

Growth Tracker

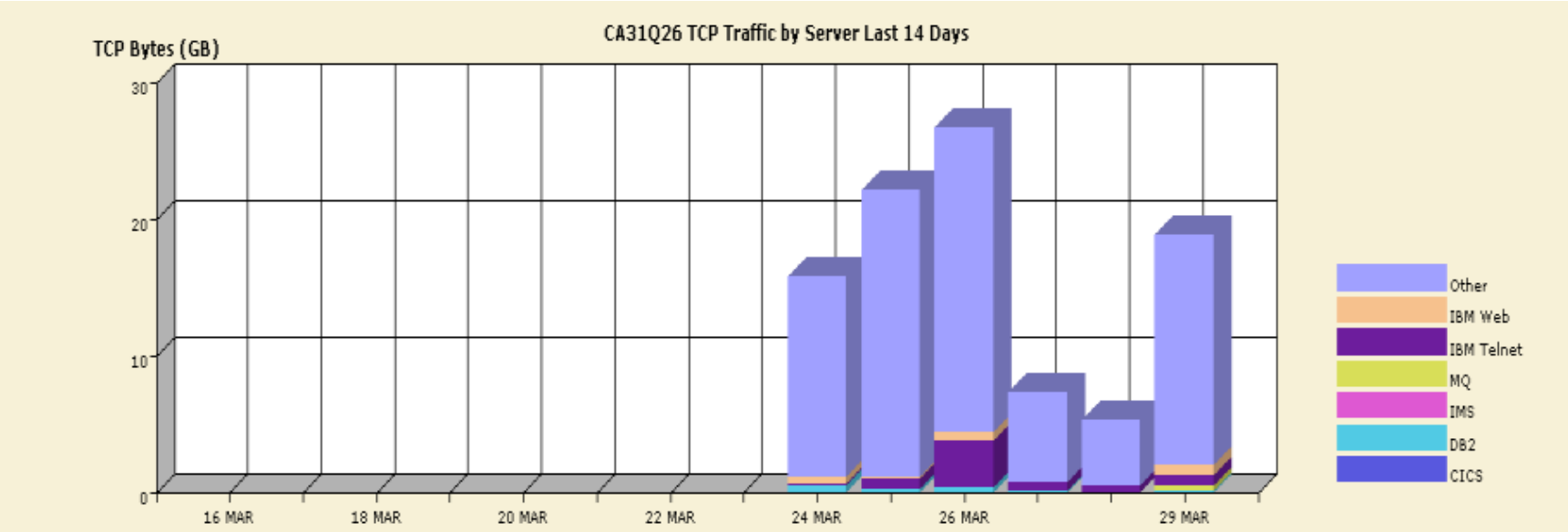
- Records growth in total mainframe IP usage over time.
  - IP Volumes, connections counts and connection durations are summed each day- stored indefinitely.



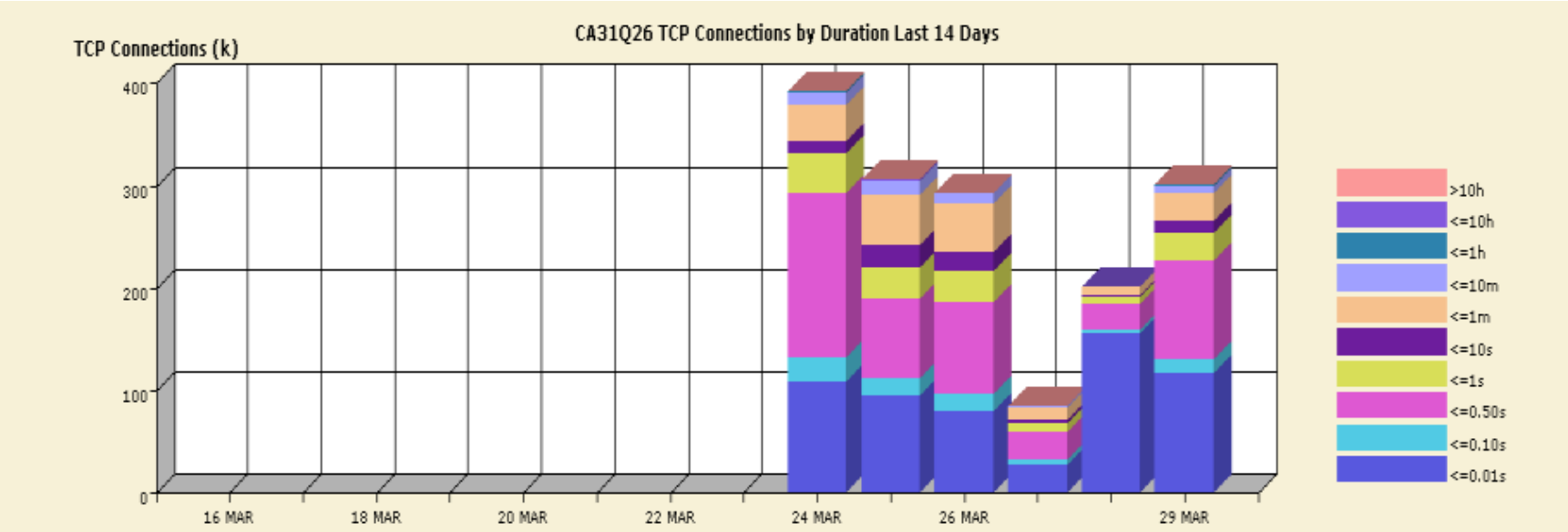
Total IP, TCP and UDP traffic



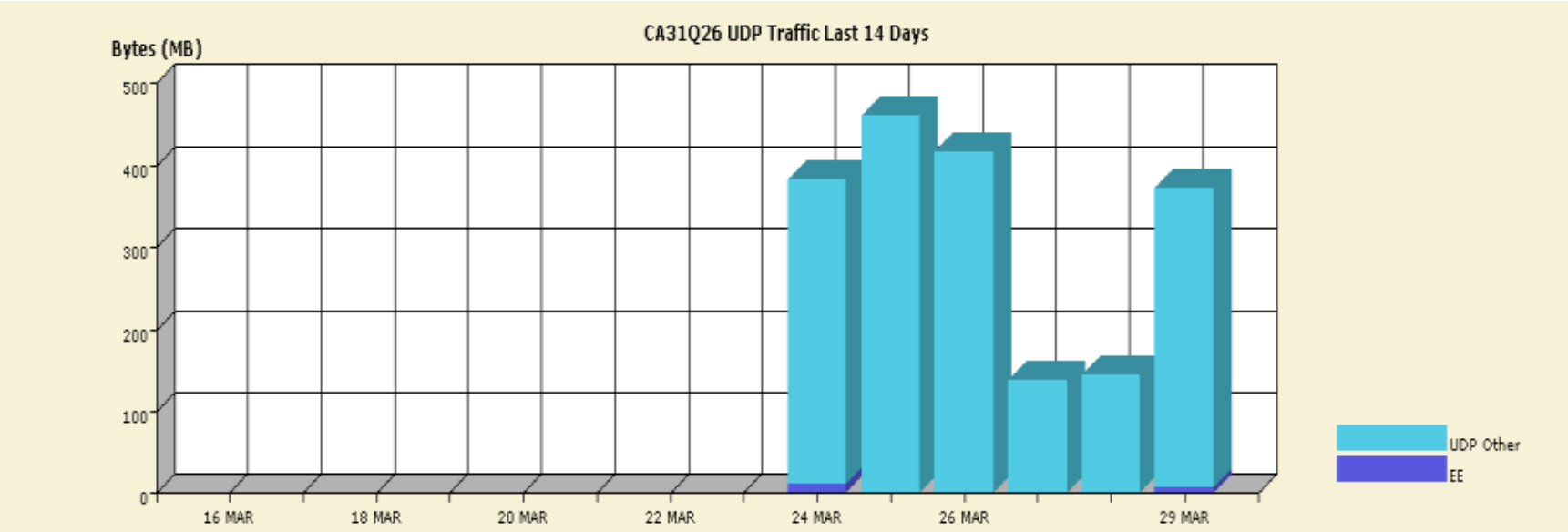
TCP traffic by server



TCP connections by duration



total UDP traffic



Predicting Growth

Problem quotes

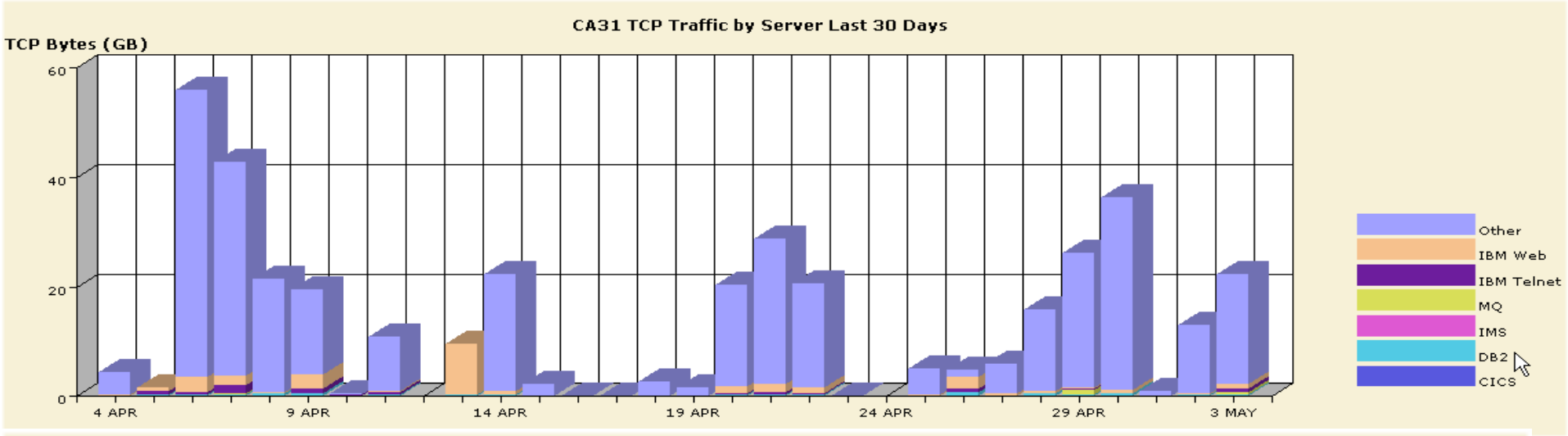
- *"Our SNA sessions to DB2 haven't changed much for years… but surely DB2 remote access is growing? If I can show that, I can get more resources for my DB2 group."*

- *"Maybe the growth is with users coming in with TCP/IP?"*

Use 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

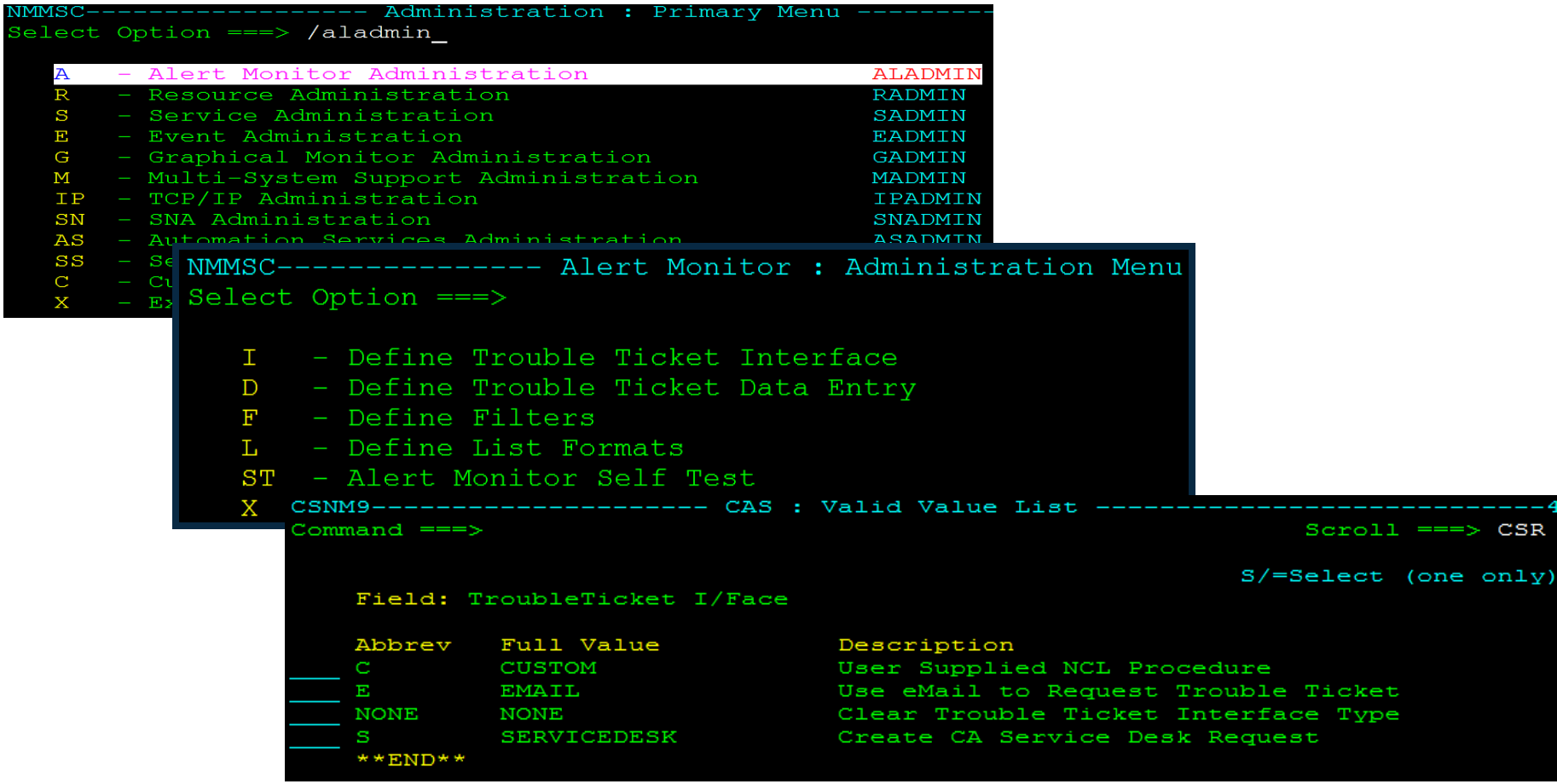
IP Growth Tracker, TCP Traffic Growth



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

Creating Emails

Where to find it



Alert Monitor
Email Interface set up

```
CSNM9--------------- Alert Monitor : Email A Trouble Ticket -Columns 00001 00072
Command ===>                                        Function=Update Scroll ===> CSR

Mail Address                    &$USRNAM
Host Name          (IBM)        USI1DAMD
SMTP Node Name     (IBM)        USILDAMD
SMTP Job Name      (IBM)        SMTP
SMTP DEST Id (TCPaccess)        _________
Exit Procedure Name             _________
Subject                         &$AMSDESC

                                  Enter Mail Text Below

****** ******************************** TOP OF DATA ********************************
000001 SERIALNM.................. &$AMSERIALNM
000002 DATE...................... &$AMDATE
000003 TIME...................... &$AMTIME
000004 DAY....................... &$AMDAY
000005 SYSTEMID.................. &$AMSYSTEMID
000006 SOURCE.................... &$AMSOURCE
000007 DESC...................... &$AMDESC
000008 APPLID.................... &$AMAPPLID
000009 CLASSID................... &$AMCLASSID
000010 RESCLASS.................. &$AMRESCLASS
000011 RESTYPE................... &$AMRESTYPE
****** ***************************** BOTTOM OF DATA ********************************

 F1=Help       F2=Split      F3=File       F4=Save       F5=Find       F6=Change
 F7=Backward   F8=Forward    F9=Swap      F10=Left      F11=Right     F12=Cancel
```

Alert Monitor
Total parameters available

- **Parameters**
  - $AMAPPLID Application that created the alert
  - $AMDESC Alert short description
  - $AMDATE Date when the alert was generated
  - $AMDAY Day of the week when the alert was generated
  - $AMGMTOFFST Local time difference from Greenwich Mean Time (UTC)
  - $AMLASTDATE Date when the alert last occurred
  - $AMLASTTIME Time when the alert last occurred
  - $AMOCCURRED Number of times the alert has occurred
  - $AMSERIALNM Software generated alert identifier
  - $AMSEVERITY Severity of the alert
  - $AMSYSTEMID System that created the alert
  - $AMTEXT* Alert text line * (1 through 5)
  - $AMTIME Time when the alert was generated
  - $AMUPDDATE Date when the alert was last updated
  - $AMUPDTIME Time when the alert was last updated
  - $AMRECM* Alert recommended action line * (1 through 20) when not retrieved from a CAS message
  - $AMCLASSID Class of the alert
  - $AMCLOSDATE Date when the alert was closed
  - $AMCLOSTIME Time when the alert was closed
  - $AMRESOURCE Resource name causing the alert
  - $AMRESID Resource name if a second one is needed
  - $AMRESCLASS The resource class
  - $AMRESTYPE The resource class type
  - $AMELAPTIME The amount of time (hh:mm) between when

Alert Monitor Email Interface
Sample NCL Procedure

```
&DOWHILE .&ADDR&CNT NE .
   &WRITE LOG=YES COLOR=YELLOW DATA=&0 Mail sent to &ADDR&CNT
   -$AMEMAIL ACTION=SENDMAIL +
-*           ADDRESS=&ADDR&CNT +
             ADDRESS=guecr01@ca.com +
             SMTPJOB=SMTP +                    -* SMTP Jobname
-*           CLASS=X +                         -* output class
-*           SMTPNODE=USILCA31 +               -* SMTPNODE
-*           HOSTNAME=TCPIP31V.CA.COM  +       -* hostname
             SMTPNODE=USILCA11 +               -* SMTPNODE
             HOSTNAME=USILCA11.CAI.COM +       -* hostname
             FROM=testmail             +       -* FROM
             TYPE=IBM
   &CNT = &CNT + 1
&DOEND
&END
```

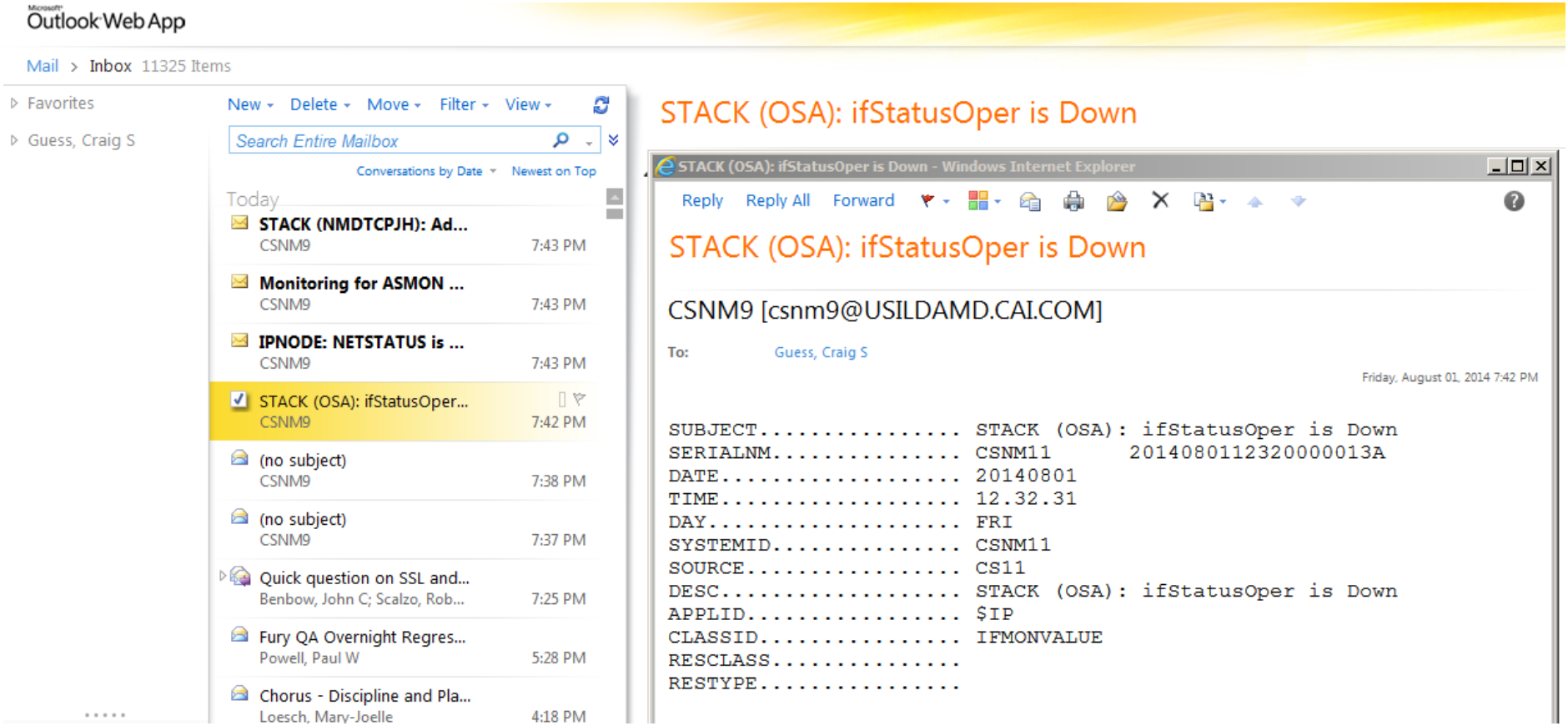
Via Process definition

```
CSNM9------------ Automation Services : Process Definition -----Function=Browse
Command ===>                                                  Scroll ===> CSR

 Process Definition
 System Name .+ $PROCESS   Version ...+ 0001
 Name ......... EMAIL
 Description .. Send Email message to a person or a pager

 Process Steps

                                                                    P=Parms
                      Condition
       StepName    Step/RC  Opr RC     Macro     Description
 ____  EMAIL                          STARTNCL START AN NCL PROCEDURE
      **END**
```

```
--------- Automation Services : STARTNCL Macro Parameter Definition ----------
Command ===>                                                  Function=UPDAT

  NCL Procedure Details

  NCL Name .... EMAIL

  Region .....+ BSYS        (AOMP, BLOG, BMON, BSYS, CNMP, LOGP or PPOP)

  Parameters .. GROUP=&GROUP SUBJECT="&SUBJECT"
                TEXT1="&TEXT1"
                TEXT2="&TEXT2"
                TEXT3="&TEXT3"

  Segment Multi-word Parameter Variables ... NO      (YES or NO)
```

Alert Monitor Email Interface

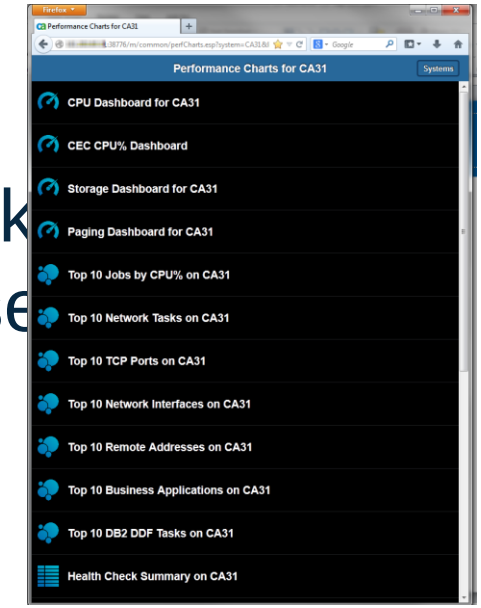
Receiving emails

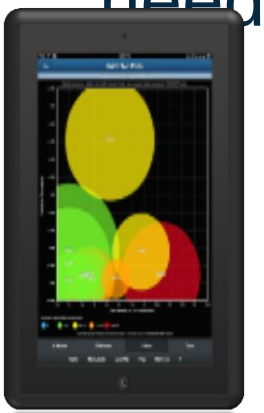


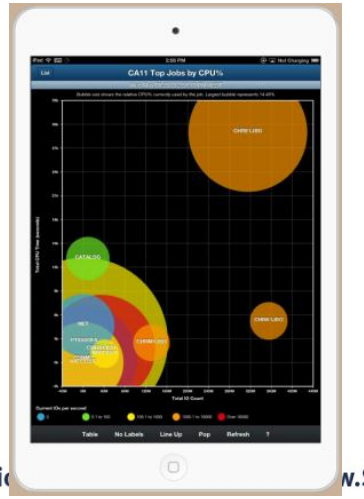
Charts and Graphs

Performance Charts/Alerts Mobility Post GA 12.1

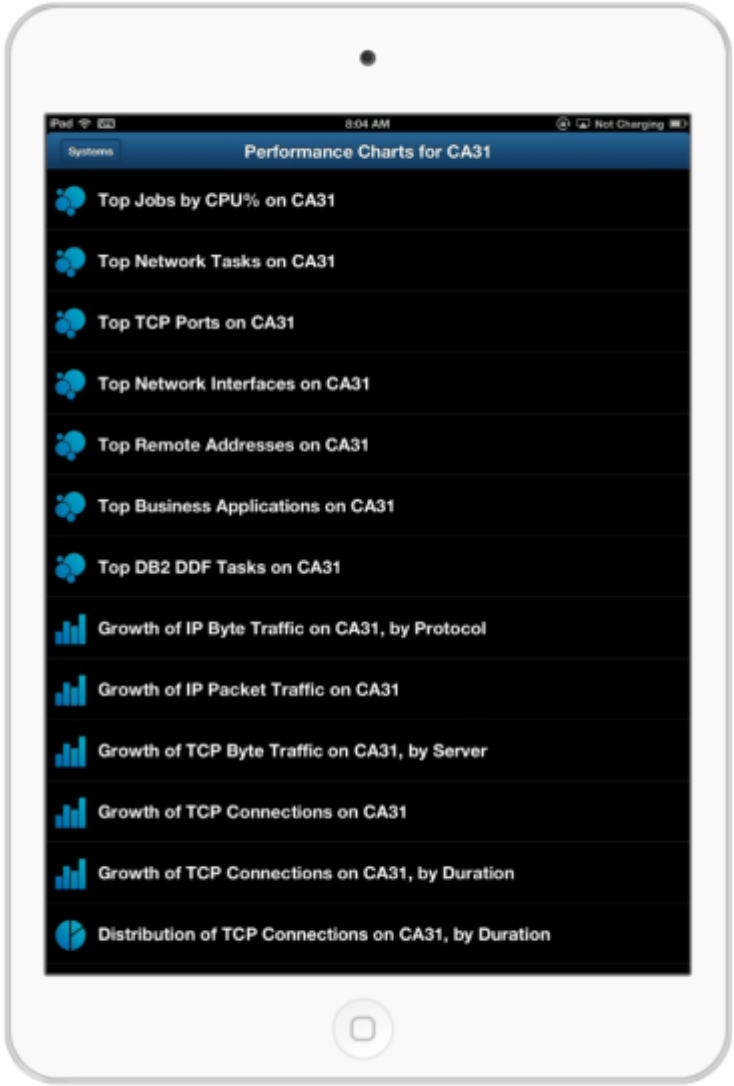
- Being truly mobile doesn't mean being tied to one device.
- Our solution work anywhere the use needs to be.







Mobility in the workplace



Performance Charts for Networks

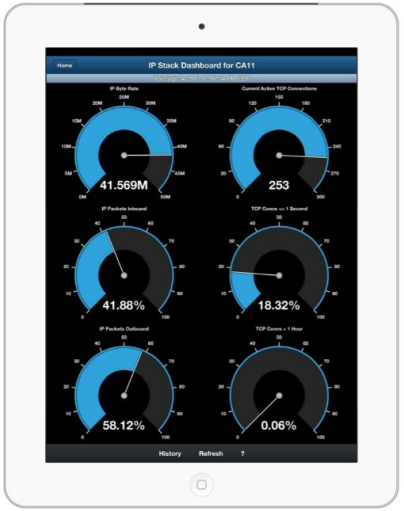
What it does

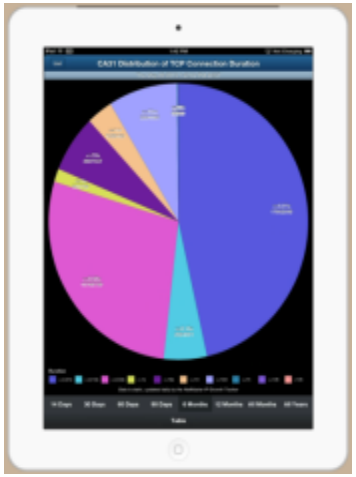
Mainframe server retrieves mainframe network performance data from NetMaster, then generates graphical mobile web pages to display it.

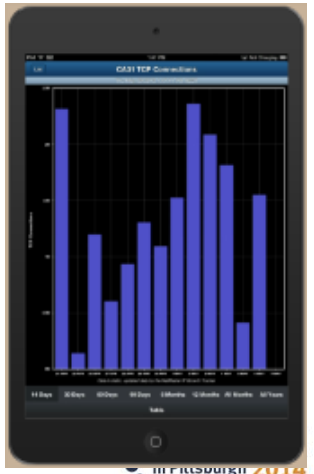
- Real-time IP network flow analysis data helps problem diagnosis, and shows network usage patterns of critical mainframe applications and servers.
- Historical high level TCP/IP network traffic growth data helps operational reviews and capacity planning.

What it looks like









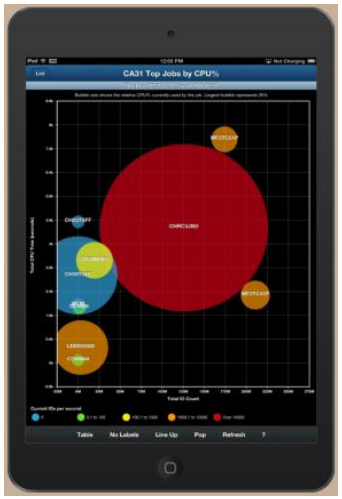
Performance Charts for Systems

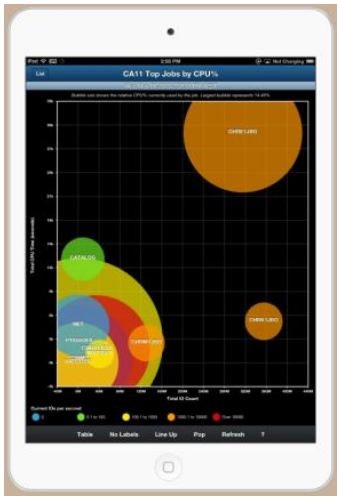
What it does

Mainframe server retrieves performance data from SYSVIEW then generates graphical mobile web pages to display it.

- SYSVIEW reaches deep into the operating system to measure every aspect of system, user and resource activity.
- .

What it looks like

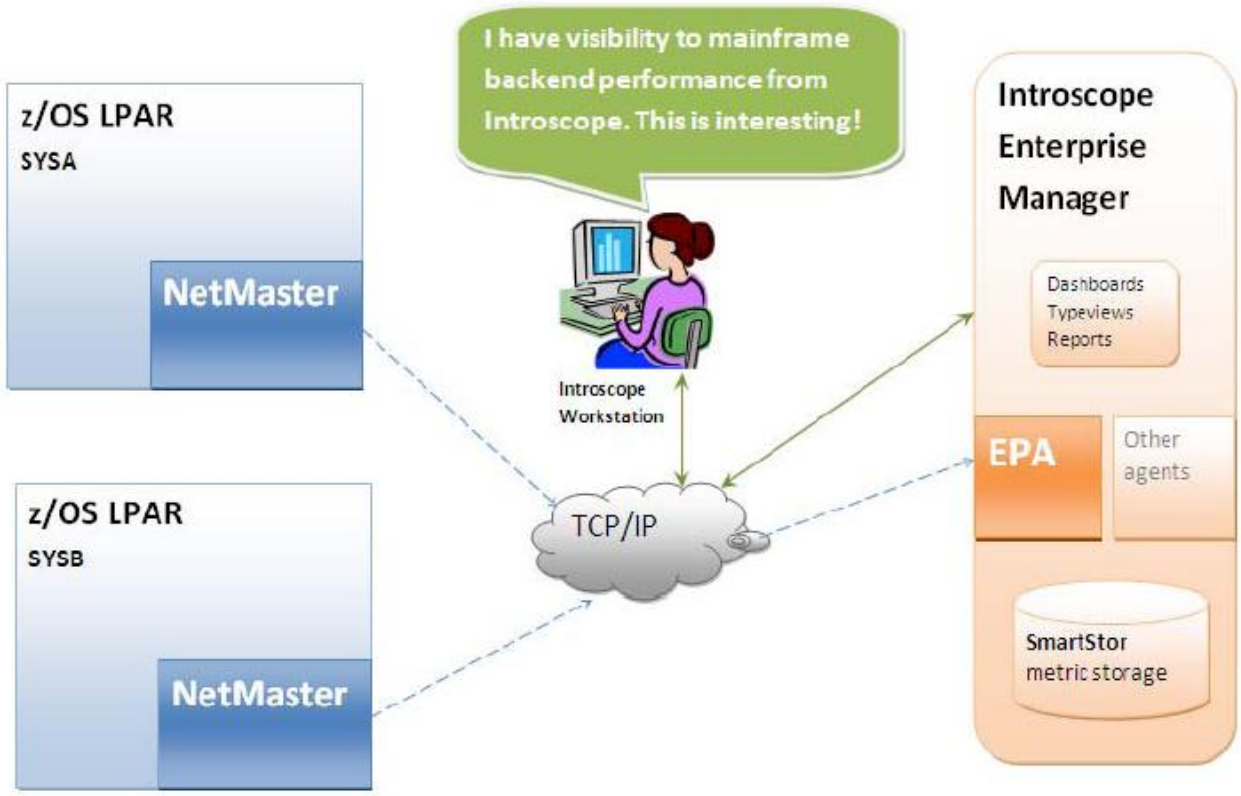




Integration to other CA Products

NetMaster – CA CE APM Integration

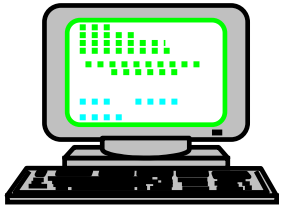
- Provides metric feeds from CA NetMaster®
- Viewed via Introscope Investigator
  - Introscope dashboards
  - Introscope reports



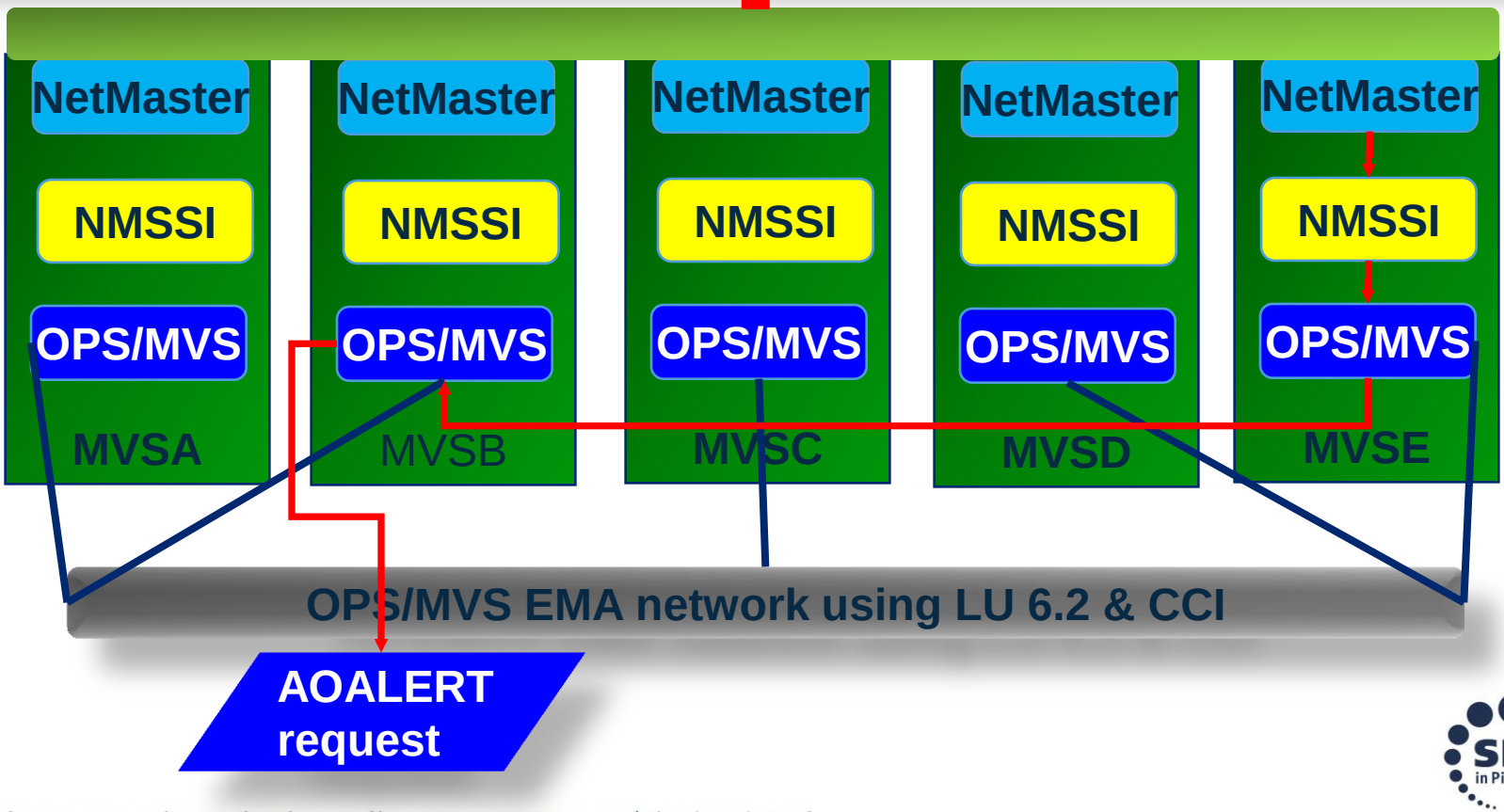
CA NetMaster® r12.1 and CA APM 9.x on Linux or Windows

NetMaster – OPS/MVS Integration

Alert forwarding from OPS/MVS EMA

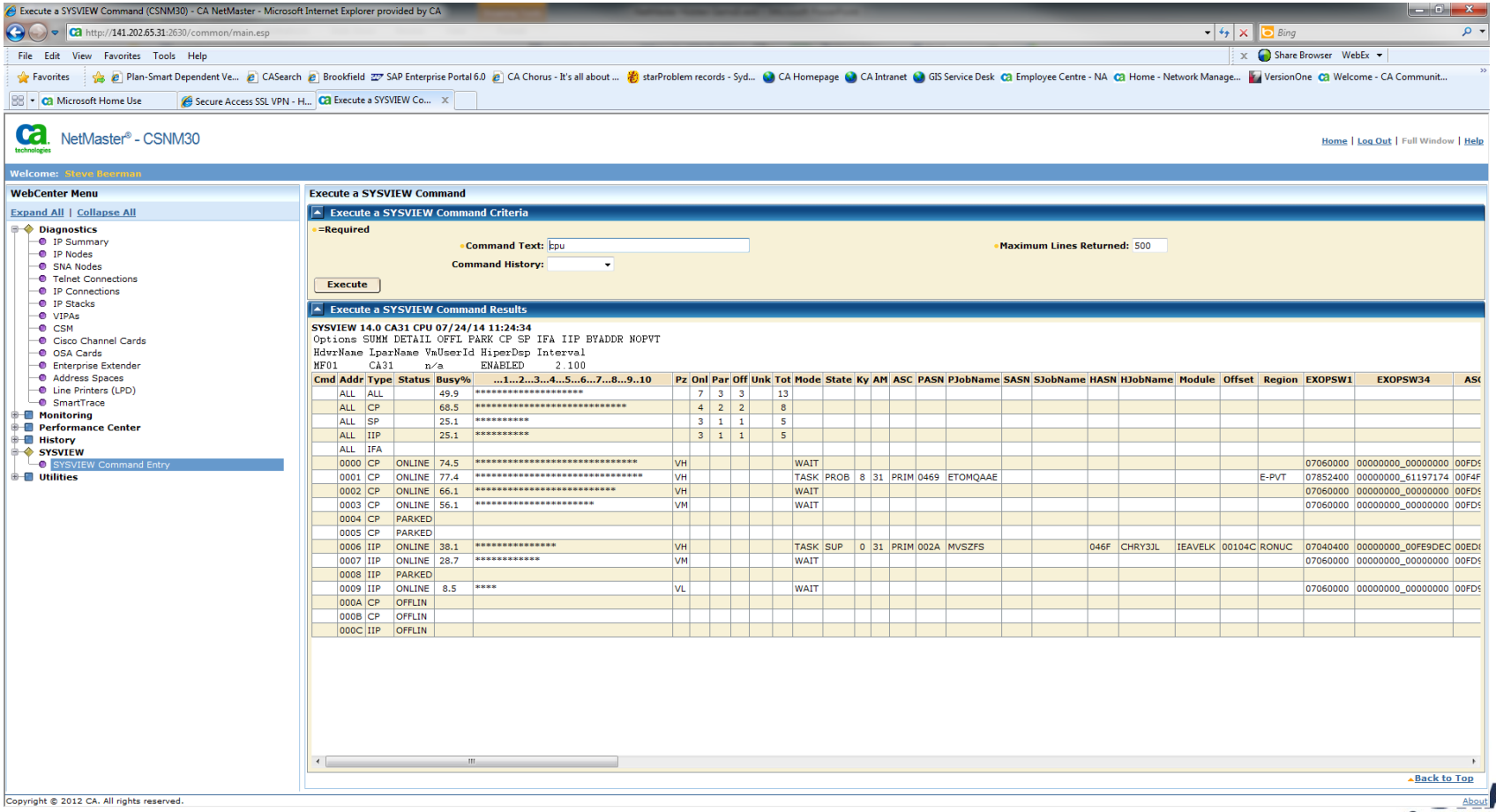


NetMaster Links enables all alerts to be seen and processed on every NetMaster

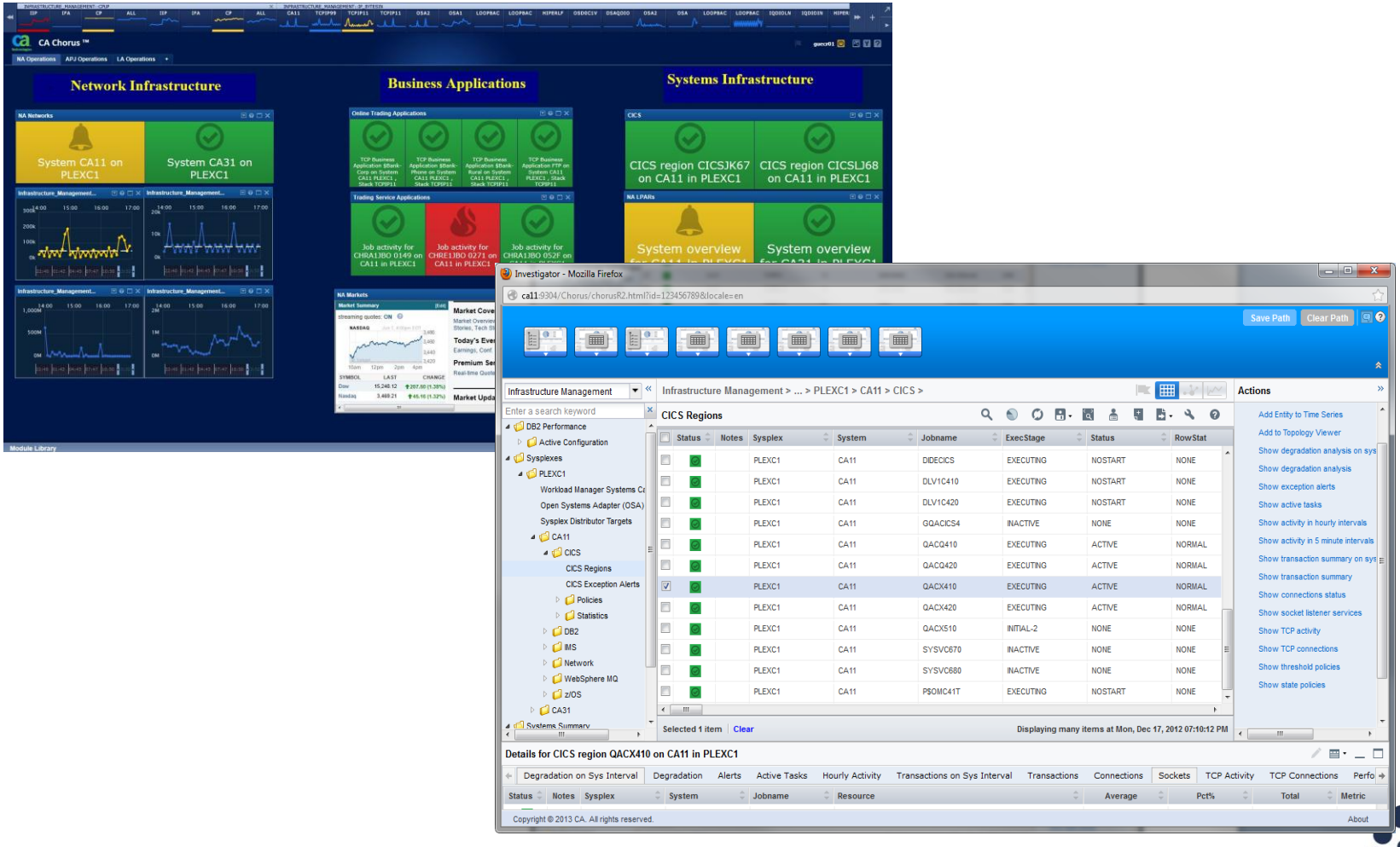


Integration with other products
SysView Command entry

- Issue Sysview commands from WebCenter



CA Chorus™ Infrastructure Management for Networks and Systems



Q&A

Hidden Gems in *CA NetMaster for TCP/IP*: Come Explore where You May Have Missed Them

Craig Guess
Rob Scalzo
CA Technologies

August 5th, 2014
Session 16080

#SHAREorg