An Architecture for Monitoring of Financial Institutions in Real Time

Angus Telfer - angus.telfer@inetco.com

inetc

Who’s INETCO ...

in business over 20 years

inetc

produce transaction communications and monitoring products for banks and retail

customers in over 40 countries

inetc

some customers are very ...

BIG

some customers are very ...

SMALL

inetc

These customers have a problem ...

They don’t know the state of their transaction network !!!

transaction messages get lost in other data flow

data flow does not provide a true indication of transaction QoS

network layer failures do not show up at application monitoring points

What they currently do???

wait for customers to call

create scripts for analyzing logs and data scope traces after the event

custom engineer a solution
using HP OpenView, etc.

outsource the network so there's someone to blame

simply pass it off as part of the "overhead of doing business"

Why no standard solution ???

Technically, it’s difficult ...

getting the data in the first place

filtering out the relevant parts

supporting “high fan-in” to event processors

decoding all the relevant parts
in the correct context

correlating events into the correct meta-events (transactions, ...)

analysis (rates, concurrency, volume, errors, classifications, ...)

organizing results for different uses

outputting in different formats

ensuring security

ensuring privacy

ensuring data is not modified

There’s also conceptual issues ...

often seen as a transaction application add-on

often seen as customer specific
(i.e. an expensive contract job)

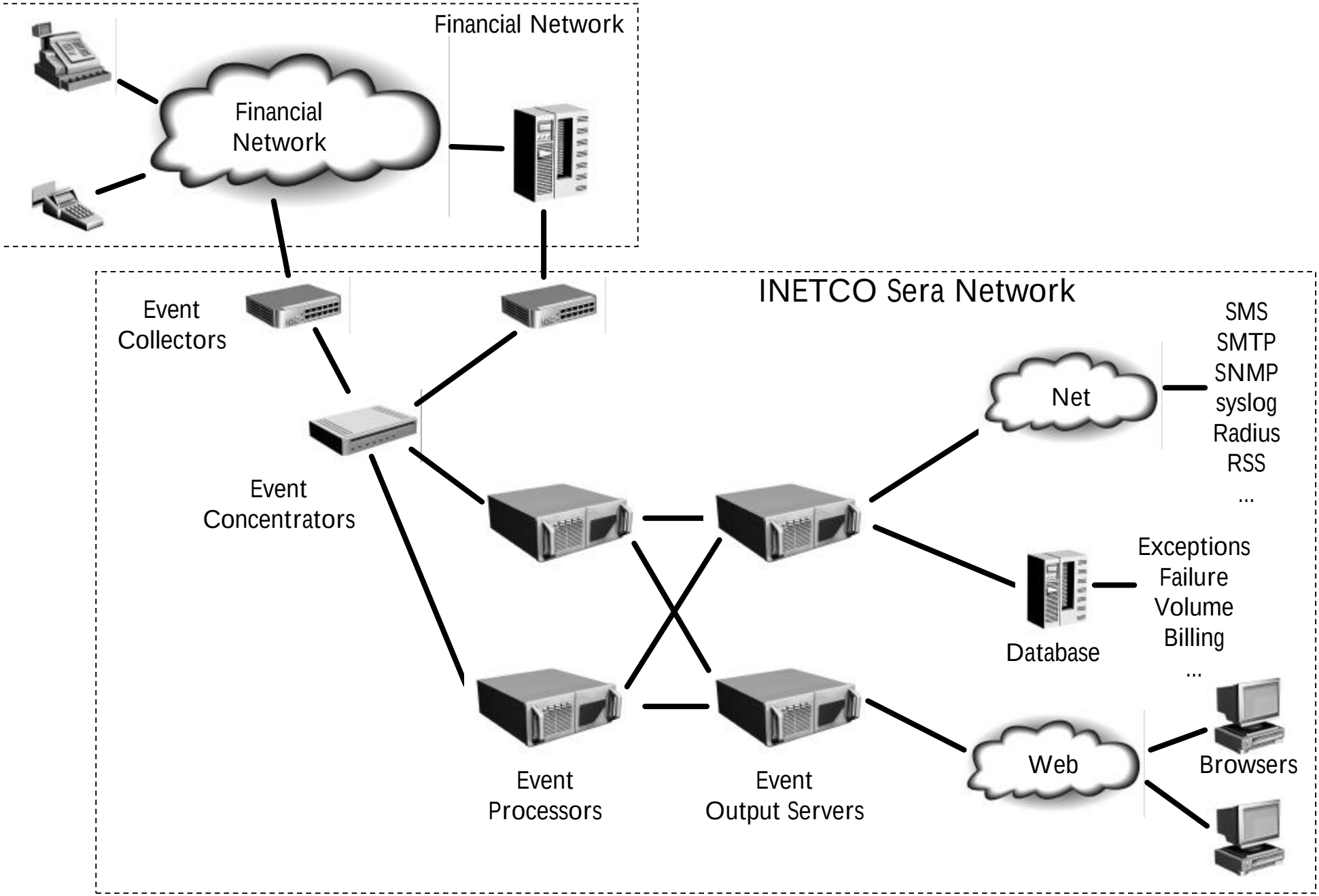
viewed as a server application,
not a network application

need often overlooked totally(wasn’t needed when financial networks were single purpose)

There’s gotta be a better way …

There is ...

A general purpose, scalable, meta-event network architecture


Financial Network
Financial
Network
INETCO Sera Network
Event
Collectors
Event
Concentrators
Net
SMS
SMTP
SNMP
syslog
Radius
RSS
...
Database
Exceptions
Failure
Volume
Billing
...
Event
Processors
Event
Output Servers
Web
Browsers

Event Collectors …

- shared processor or data scope
- fast, low processor/memory footprint
- simple “match” filtering
- encrypted checksum and message number so
  - messages can’t be modified, deleted, or inserted
- efficient transfer of event data

Event Concentrators ...

- dedicated “black box”
- “module” based decode up to and including the session layer
- topic based filtering on messages
- no service specific knowledge

Event Processors ...

- dedicated server
- module based:
  - application layer decodes
  - correlation of messages into transactions
  - restricts use and dissemination of private data
  - basic statistical analysis (histograms, rates, ...)
  - dynamic routing between modules
  - real time, data based core

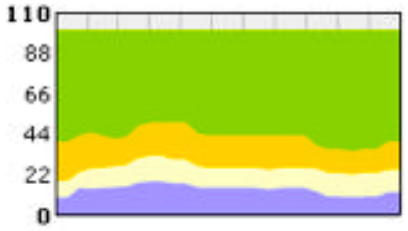
Event Output Servers...

- dedicated servers
- correlation into user specific meta events
  (alerts, performance measurements, ...)
- message formatting and output (WS
  Notification, SNMP, SMTP, SMS, RADIUS,
  syslog, SQL, ...)

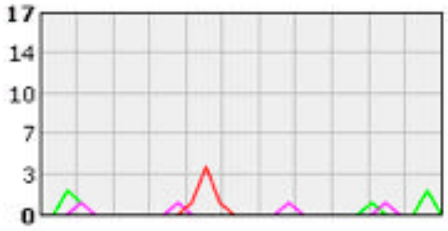
Sample output ...

Network

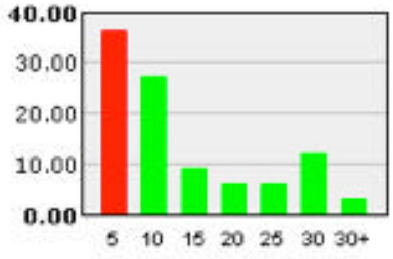
Transaction Ratio
% Datapac/Ip/Wireless/Other



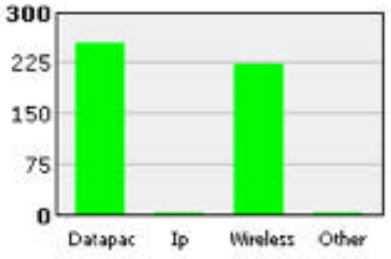
Transaction Rate
Appr/Decl/Fail/Unsup per Second



Transaction Duration
% Good/Bad by Duration



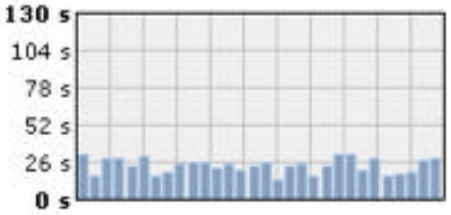
Concurrent Transactions
Transactions in Progress



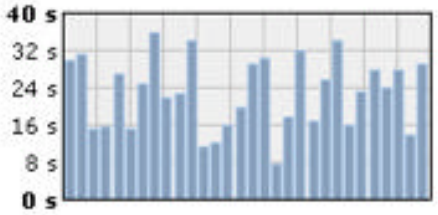
Network | Terminal Group

Ratio | Rate | Duration

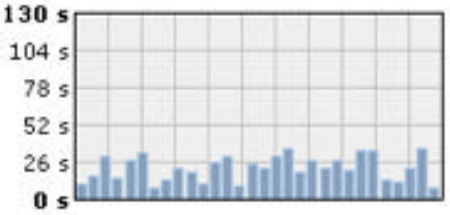
Datapac
Transaction History



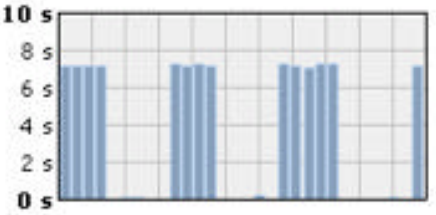
IP
Transaction History



Wireless
Transaction History



Other
Transaction History



Summary | Detail

Filter [ ] [ ] and [ ] [ ] Pause Log

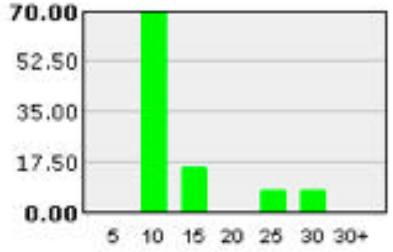
Time	Type	Status	Terminal ID	Terminal Group	Network	Duration
2006/08/03 11:09:17.89	Other	Unsupported		Other	Other	0.21 s
2006/08/03 11:09:17.91	Other	Unsupported		Other	Other	0.01 s
2006/08/03 11:09:22.91	Withdrawal	Declined	999999999999999	Burnaby	Other	7.24 s
2006/08/03 11:09:28.21	Withdrawal	Approved	jack00000000004	Vancouver	Wireless	11.236 s
2006/08/03 11:09:30.40	Withdrawal	Declined	999999999999999	Burnaby	Other	7.11 s
2006/08/03 11:09:31.22	Withdrawal	Approved	burnaby00000007	Coquitlam	IP	13.679 s
2006/08/03 11:09:37.51	Withdrawal	Approved	roger0000000002	Other	Wireless	20.819 s
2006/08/03 11:09:37.71	Withdrawal	Declined	999999999999999	Burnaby	Other	7.03 s
2006/08/03 11:09:44.37	Withdrawal	Approved	inetco000000005	Vancouver	Datapac	27.299 s
2006/08/03 11:09:44.43	Withdrawal	Approved	jeremy000000003	Vancouver	Datapac	27.619 s
2006/08/03 11:09:45.40	Withdrawal	Approved	999999999999999	Burnaby	IP	28.951 s
2006/08/03 11:09:45.44	Withdrawal	Declined	999999999999999	Burnaby	Other	7.24 s
2006/08/03 11:09:52.59	Withdrawal	Approved	stillcreek00006	Coquitlam	Wireless	35.35 s
2006/08/03 11:09:53.18	Withdrawal	Declined	999999999999999	Burnaby	Other	7.23 s

Network - Burnaby Terminal Group

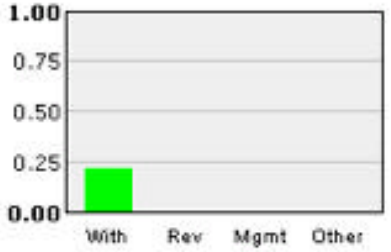
Transaction Volume
% Burnaby/Others

Transaction Rate
Appr/Decl/Fail/Unsup per Second

Transaction Duration
% Good/Bad by Duration

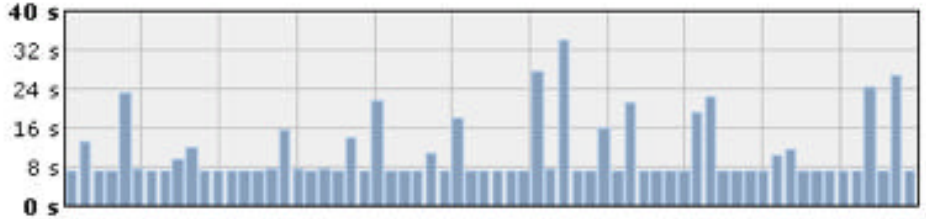


Transaction by Type
Good/Bad by Type

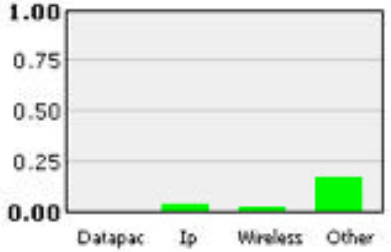


Transaction Rate
Transactions per Second

Transaction Duration
Transaction History

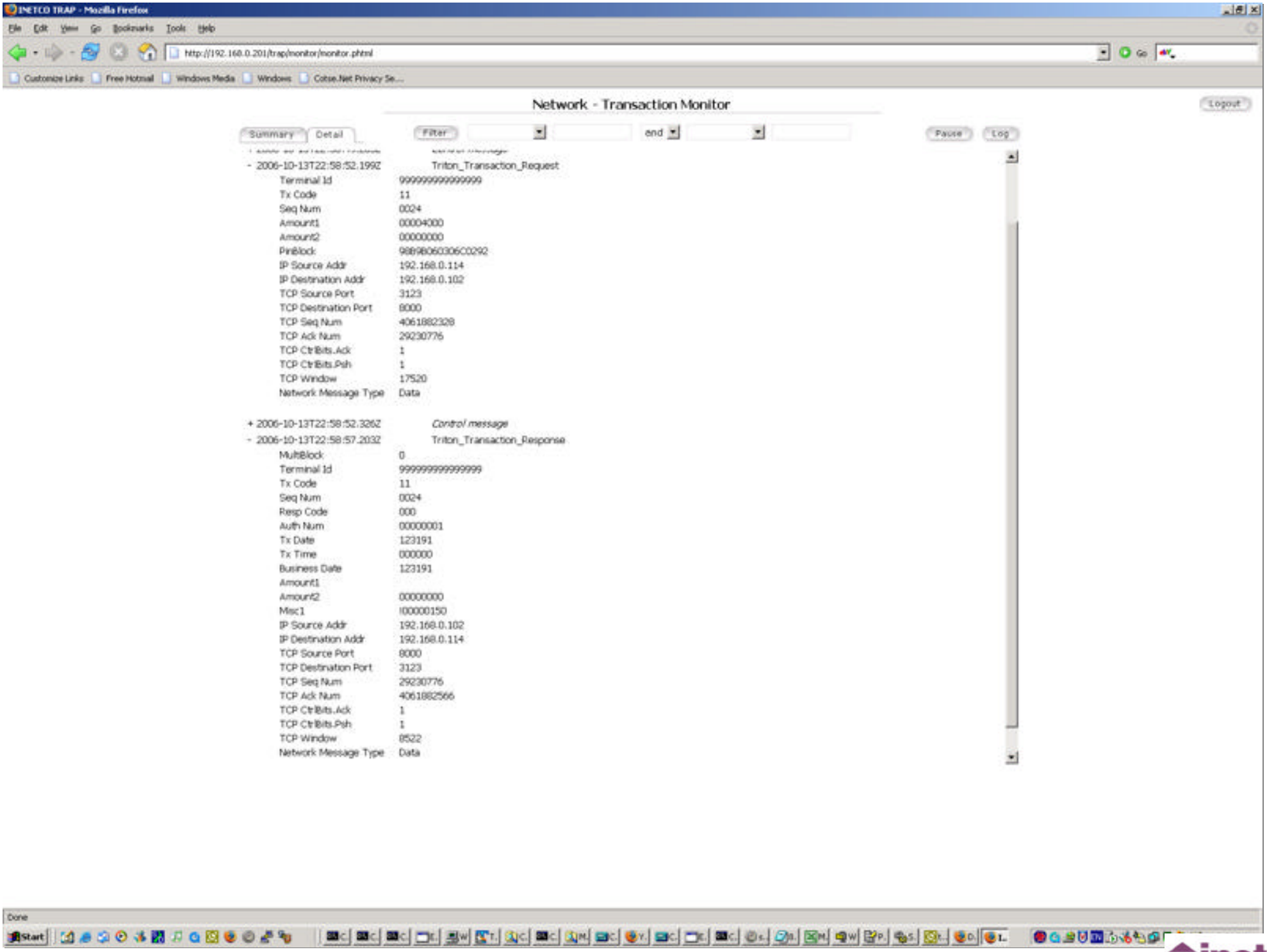


Transaction Rate
by Network



Summary | Detail | Filter | and | Pause | Log

Time	Type	Status	Terminal ID	Terminal Group	Network	Duration
2006/08/03 11:43:31.64	Withdrawal	Approved	999999999999999	Burnaby	Wireless	23.133 s
2006/08/03 11:43:38.16	Withdrawal	Declined	999999999999999	Burnaby	Other	7.34 s
2006/08/03 11:43:45.77	Withdrawal	Declined	999999999999999	Burnaby	Other	7.17 s
2006/08/03 11:43:53.43	Withdrawal	Declined	999999999999999	Burnaby	Other	7.01 s
2006/08/03 11:43:54.87	Withdrawal	Approved	999999999999999	Burnaby	Datapac	9.363 s
2006/08/03 11:43:58.37	Withdrawal	Approved	123450000000009	Burnaby	Other	11.816 s
2006/08/03 11:44:00.97	Withdrawal	Declined	999999999999999	Burnaby	Other	7.01 s
2006/08/03 11:44:08.64	Withdrawal	Declined	999999999999999	Burnaby	Other	6.869 s
2006/08/03 11:44:16.21	Withdrawal	Declined	999999999999999	Burnaby	Other	7.09 s
2006/08/03 11:44:23.87	Withdrawal	Declined	999999999999999	Burnaby	Other	7.24 s
2006/08/03 11:44:31.51	Withdrawal	Declined	999999999999999	Burnaby	Other	6.99 s
2006/08/03 11:44:32.04	Withdrawal	Approved	123450000000009	Burnaby	Datapac	7.53 s
2006/08/03 11:44:39.13	Withdrawal	Approved	999999999999999	Burnaby	Wireless	15.622 s
2006/08/03 11:44:39.32	Withdrawal	Declined	999999999999999	Burnaby	Other	7.3 s


INETCO TRAP - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.0.201/trap/monitor/monitor.phtml
Customize Links Free Hotmail Windows Media Windows Cotse.Net Privacy Se...
Network - Transaction Monitor
Logout
Summary Detail
Filter
end
Pause
Log
- 2006-10-13T22:58:52.199Z Triton_Transaction_Request
Terminal Id 99999999999999
Tx Code 11
Seq Num 0024
Amount1 00004000
Amount2 00000000
PinBlock 9898060306C0292
IP Source Addr 192.168.0.114
IP Destination Addr 192.168.0.102
TCP Source Port 3123
TCP Destination Port 8000
TCP Seq Num 4061882328
TCP Ack Num 29230776
TCP CtrlBits.Ack 1
TCP CtrlBits.Psh 1
TCP Window 17520
Network Message Type Data
+ 2006-10-13T22:58:52.326Z Control message
- 2006-10-13T22:58:57.203Z Triton_Transaction_Response
MultBlock 0
Terminal Id 99999999999999
Tx Code 11
Seq Num 0024
Resp Code 000
Auth Num 00000001
Tx Date 123191
Tx Time 000000
Business Date 123191
Amount1
Amount2 00000000
Misc1 I00000150
IP Source Addr 192.168.0.102
IP Destination Addr 192.168.0.114
TCP Source Port 8000
TCP Destination Port 3123
TCP Seq Num 29230776
TCP Ack Num 4061882566
TCP CtrlBits.Ack 1
TCP CtrlBits.Psh 1
TCP Window 8522
Network Message Type Data
Done
Start

Lessons learned ...

data volumes are bigger than what is first apparent

there’s much more data processing than is obvious

losing a single piece of data can be disastrous

large, unrestricted fan-in of events is an even bigger problem

complete definition of a meta-event is very difficult

event correlations involving timed events, overlapping meta-events, and incomplete descriptions of meta-events is tricky

a clear understanding of the business pain is a requirement before a solution can be crafted

you can’t just give the customer a toolbox any more than you can just give a potential home owner a hammer and saw

Issues outstanding ...

Large fan-in ...

- how to provide a general purpose scalable solution for large fan-in networks

Missing data ...

- how to determine what can be dropped
- how to keep missing data from distorting the entire picture
- how to “fill-in” gaps where necessary

Event correlation description ...

- how to define a meta-event and PROVE that the description is complete
- how to describe overlapping meta-events that can affect one another
- how to best incorporate timers into meta-event descriptions
- how to display a meta-event description so that it can be understood

Data from multiple processors ...

- how to allow views involving data from multiple processors without having a VERY thick client

Adhoc queries ...

how to allow adhoc queries while still being able to maintain a deterministic QoS

Privacy ...

- how to ensure privacy when users can create new relationships between the data

Performance...

- always an issue!!!