Introduction to Mainframe (z/OS) Network Management
Share Session Boston 13402

Laura Knapp
WW Business Consultant
Laurak@aesclever.com

Agenda

Introduction

Why Monitor IP in the Mainframe?

IP Monitoring Tools and Technologies

Best Practices
Managing Fundamentals

- **FCAPS**
  - Fault
  - Configuration
  - Availability
  - Performance
  - Security

- **Leading to**
  - Service level achievement
  - Optimum resource utilization
  - Highly available systems
  - High performing systems
FCAPS

Fault Management
What is the Status?

Configuration Management
What is the configuration?

Availability Management
What’s down? What’s available? What’s up?

Performance Management
How consistent? How many? How much? How fast?

Security Management
Who can access? Identify yourself? Can everyone see it?
**z/OS Communication Server**

- **Network Communication for all z/OS subsystems**

- **z/OS unique functions**: Policy Agent, Sysplex Distributor, Load Balancing Advisor, Intrusion Detection Services
- **TCP/IP V4 and V6**
  - Network Encryption Services
  - TCP/IP Applications
- **Legacy SNA and SNA over TCP/IP (aka., Enterprise Extender) Ö**
- **Hardware device drivers (OSA, HiperSockets)**

**Network Attachment Adapters**

- Routers
- Switches
- OSA

Introduction

Why Monitor IP in the Mainframe?

IP Monitoring Tools and Technologies

Best Practices
Murphy’s Law

If anything can go wrong, it will

If anything just cannot go wrong it will

Left to themselves, things tend to go from bad to worse

If everything seems to be going well, you have obviously overlooked something
Congestion and Performance Degradation

- Equipment Failure: 31%
- Network and Server Congestion: 69%
Common Problems

Hardware failure
Configuration change
Firmware change
Traffic rate change
New application deployment
Network failure
Security attack
Routing changes
Buffer shortages
Resource shortage
Spanning Tree problems
Illegal access to resources
Why Monitor IP?

Browser

- Application
- TCP (Transmission Control Protocol)
- IP (Internet Protocol)
- Network Interface and hardware

Server

- Application
- TCP (Transmission Control Protocol)
- IP (Internet Protocol)
- Network Interface and hardware

WWW, mail, file transfer, remote access
Application interfaces
End-to-end delivery
Best effort delivery
Physical connection
A View of IP
Agenda

Introduction and goals

Why Monitor IP in the Mainframe?

IP Monitoring Tools and Technologies

Best Practices
Effective Management

Gather Configuration and Traffic Information

Observe Statistics
Collect Capacity Data
Analyze Traffic

Solve Problems
Plan Changes
Evaluate

What-if Analysis

Implement Changes

Performance Baselining

3rd Party Services
IP Resource Bottlenecks

CPU
Memory
Buffering, queuing, and latency
Interface and pipe sizes
Network capacity
Speed and Distance
Application Characteristics

Results in:

Network capacity problems
Utilization overload
Application slowdown or failure
Information to Collect and Resources to Monitor

Link/segment utilization
CPU Utilization
Memory utilization
Response Time
Round Trip Time
Queue/buffer drops
Broadcast volumes
Traffic shaping parameters
RMON statistics
Packet/frame drop/loss
Environment specific

TCP/IP stacks
Interfaces (OSA, Links, devices…)
Services (ports)
Gateways
Remote hosts
Unix System Services
zBX services
Management Plan Purpose

Develop information collection plan
  Define parameters to be monitored/measured and the thresholds
  Acquire proper authority to collect and monitor/measure
  Acquire proper authority to change thresholds
  Determine frequency of monitoring and reporting
  Define parameters that trigger alert mechanism

Define performance areas of interest

Report and interpret results

Determine tools for collecting information

Determine tools for analyzing information
Introduction and goals

Why Monitor IP in the Mainframe?

IP Monitoring Tools and Technologies

Best Practices
Performance Management Practices

- Active Sampling
- Passive Sampling

- Embedded Source
- External Source

- Device/Link Scope
- End-to-End/Path Scope

- User Perspective
- Network Perspective
Core Mainframe IP Tools

PING

TRACEROUTE

NETSTAT

SNMP

Operating system or device specific
SMF for z/OS

NMAPI
Basic Tools: PING

Tests connectivity to an IP device

Sends an ICMP frame to the destination
Basic Tools: Traceroute

Shows most likely path to an IP device and transmit times

Sends an ICMP frame to the destination
Netstat

Gathers information from buffers relating to the IP functions

Common functions
Network drivers
Interface cards
Router tables
Active server processes
Statistics by protocol

Vendors implement different functions
What is SNMP?

**Simple Network Management Protocol**

- Internet standard
- Initially tied to TCP/IP protocol
- Set of functions
  - monitor network elements
  - control network elements

Routers, switches, Unix hosts, bridges, hubs, agents for many operating systems, etc
SNMP Layering

Manager/Agent Model

Agent acts as "server"
Manager acts as "client"
Manager polls agents for information
Agent keeps information and responds
Agent may proactively send information as traps
Opens UDP port 161, 162, 391, 1993
SNMP Flows

- MIB—RMON 1 and 2
- SNMP Agent

- Get, GetNext, Set, GetBulk
- Responses, SNMP Traps

- Log Message

- IP Connectivity
- SNMP Traps/RMON
- Log
- Network Time Protocol
- Vendor Specific
How do the agents keep the information?

Universe of network manageable objects is called the Management Information Base (MIB).

Items within the network elements which are manageable are called managed objects.

Objects within the MIB are organized into the following groups:

<table>
<thead>
<tr>
<th>MIB ....(114)</th>
<th>MIB-2 ....(171)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) System</td>
<td>1) System</td>
</tr>
<tr>
<td>2) Interface</td>
<td>2) Interface</td>
</tr>
<tr>
<td>3) Address Translation</td>
<td>3) Address Translation</td>
</tr>
<tr>
<td>4) IP</td>
<td>4) IP</td>
</tr>
<tr>
<td>5) ICMP</td>
<td>5) ICMP</td>
</tr>
<tr>
<td>6) TCP</td>
<td>6) TCP</td>
</tr>
<tr>
<td>7) UDP</td>
<td>7) UDP</td>
</tr>
<tr>
<td>8) EGP</td>
<td>8) EGP</td>
</tr>
<tr>
<td></td>
<td>9) CMOT</td>
</tr>
<tr>
<td></td>
<td>10) Transmission</td>
</tr>
<tr>
<td></td>
<td>11) SNMP I</td>
</tr>
</tbody>
</table>
Object Registration Hierarchy

ROOT

CCITT (0)       ISO (1)       JTC (2)

ORG (3)

NIST (2)       DoD (6)

IAB (1)

Directory (1) Management (2) Experimental (3) Private (4)

1.3.6.1.2.1

system
interface
addr. trans

1.3.6.1.4.1.2=(IBM)

1.3.6.1.4.1.41=(ipForwarding)

IEEE 802.2-X.25-Satellite-Radio-Async......

FTP
Telnet
SMTP
SNMP Manager
TCP
UDP
IP
ICMP

JTC : Joint Technical Committee
DoD : Department of Defense (U.S.)
IAB : Internet Activity Board
NIST : National Institute of Standards and Technology (U.S.)
SNMP: Review

Agents maintain management information in their MIB.

Management stations poll agents for MIB values.

Multiple polls required to determine data.

Agents may also send traps.

Community names used for authentication.

RMON allows distributed management functions.
Operating Specific Data Collection

Operating system data collection
- Log files
- Vendor specific storage

System Management Facility
- SMF on z/OS
- Standard way to collect z/OS system activity
- Network activity, I/O, software usage, ...
- Each SMF record has a numbered type ‘SMF 89’
- IBM uses SMF numbers 1-127
- Vendors specific SMF records begin at 128
- Data is stored in VSAM files
- TCP/IP statistics are captured in SMF 109, 118, 119
SMF Record Type Examples

• RMF records are in the range 70 through to 79. RMF's records are generally supplemented - for serious performance analysis - by Type 30 (subtypes 2 and 3) address space records.
• RACF type 80 records are written to record security issues, i.e. password violations, denied resource access attempts, etc. Other security systems such as ACF2 also use the type 80 and 81 SMF records.
• Products use SMF type 89 records indicate software product usage and are used to calculate reduced sub-capacity software pricing.
• DB2 writes type 100, 101 and 102 records, depending on specific DB2 subsystem options.
• CICS writes type 110 records, depending on specific CICS options.
• Websphere MQ writes type 115 and 116 records, depending on specific Websphere MQ subsystem options.
• WebSphere Application Server for z/OS writes type 120. Version 7 introduced a new subtype to overcome shortcomings in the earlier subtype records. The new Version 7 120 Subtype 9 record provide a unified request-based view with lower overhead
SMF 119 TCP/IP Statistics

Type of information collected
- Device and Link
- Interface
- VIPA
- Port details
- IKE
- IPSEC
- OMPROUTE
- SNALINK
- Buffer usage
- VTAM
- TN3270
- FTP
- Remote Print
- and more……
Vendor Specific Tools

Vendors utilize these base functions to provide integrated usable tools:

- Single screen access to information gathered from multiple sources
- Correlation functions often provided
- Tabular and graphical displays
- Analysis
- Reporting
- Usable interfaces
- Alerting
- Historical data
- Real time data
- Exception reporting
- Baseline definition
Today’s Reactive Management

Dedicated level-1 personnel

24x7 coverage

Answer phone calls

Monitor an event control desk

Isolate problem

Log trouble tickets

Refers to level 2
Level 2 Reactive Challenges

Experienced personnel

Operates from personal desk or mobile

Little to no access to management station

Dispatched by level-1 with little information

Often wastes time traveling to remote site

No time for pro-active network analysis

Need

Historical data

Base lining

Threshold exceptions

Event notification

Smart agents

Real-time data
Pro-active Web and Mobile Based Management

Extends access to management station to all personal with Workstations and cell phones

Reduces load on management stations processor

Web and cell based performance tools allows greater visibility to level-2 and level 3 no matter where they are

Add web based access JAVA applets
Network Communication for all z/OS subsystems

z/OS Communications Server

- z/OS unique functions: Policy Agent, Sysplex Distributor, Load Balancing Advisor, Intrusion Detection Services
- TCP/IP V4 and V6
  - Network Encryption Services
  - TCP/IP Applications
- Legacy SNA and SNA over TCP/IP (aka., Enterprise Extender)
- Hardware device drivers (OSA, HiperSockets)

Network Attachment Adapters

Device Support

Routers

Switches

OSA
Steps to Effective Management

**Baseline**
- Baselines over a long period of time to develop utilization, resource growth and shrinking trends
- What-if analysis prior to deployment
- Performance exception reporting
- Analyze the capacity information
- Review baseline, exception, and capacity information on a periodic bases

**Setup Alarms and Thresholds**

**Excessive Missed Faults**

**Monitor**
Baseline Your Environment

Gather inventory information

Gather statistics at a given time(s)

Monitor statistics over time and study traffic flows

Have logical maps of network, server and application views

Know the protocols and traffic profiles

Document physical and logical network

Document detailed and measurable SLAs

Have a list of variable collected for your baseline

Be part of change control system
Agenda

Introduction and goals

Why Monitor IP in the Mainframe?

IP Monitoring Tools and Technologies

Best Practices
Performance Case Study

Catalog order processing system with TN3270E response time problems

User calls with problem

Help desk - where’s the problem?
Case Study Reaction

Problem diagnosis

Determine IP address of user
WINIPCFG
Netstat -r

Determine applications’ health
V Net LU=Catalog
Can help desk log on to application

What is network response time
Traceroute to determine path
Ping nodes in path to determine bottlenecks
Case Study – Bottleneck Diagnosis

SNA slowdown

Performance monitors
SMF records
VTAM commands

Network slowdown

Router diagnosis
CPU utilization
Memory utilization
Packet errors
Interface status
IP stack analysis
Case Study - Proactive Solution

Administrator alerted to the impending problem.....

TN3270 traffic monitored
Thresholds established for response times
Alert generated when threshold reached

Routers in the network monitored
Alerts generated for exceeded limits

Trend analysis information produces baseline
Review to determine need for more resources, network changes
Performance Interaction with Fault Management

Proactive fault management is the area that ties together fault, performance and change management into an ideal network management system.

Processing performance data may uncover network faults.

Excessive or repeated faults may lead to change of monitored resources.

Real-time notifications of performance related items.
Performance Interaction with Configuration Management

Analysis of performance data may lead to configuration changes.

Define and validate protocol usage by systems, servers, applications.

Ensure management protocols are appropriately defined.

Ensure correct interaction with management subsystems like DNS, NTP, etc.
Performance Interaction with Security Management

Read only access to devices

Use of SNMP views to restrict unauthorized use of SNMP information

Don’t make performance data collection a Denial of Service attack against the network or systems

Security logs may be used during performance analysis
Mainframe Management

Problems continue to evolve as business services evolve

Always new technologies to with which to contend (cloud, mobile, big data, IPv6….)

Emerging applications demand high performance

Problem determination data readily available … But the interpretation and action plans are lax

Performance data readily available …. But the interpretation and action plans are lax

Complexity increases with each new application, network device, or other change