Introduction to Mainframe (z/OS) Network Management

Share Session 16314

Junie Sanders – jrsandler@cisco.com
Kevin Manweiler - kmanweil@cisco.com

Insert Custom Session QR if Desired.

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence**.

Agenda

Introduction

Why Monitor IP in the Mainframe?

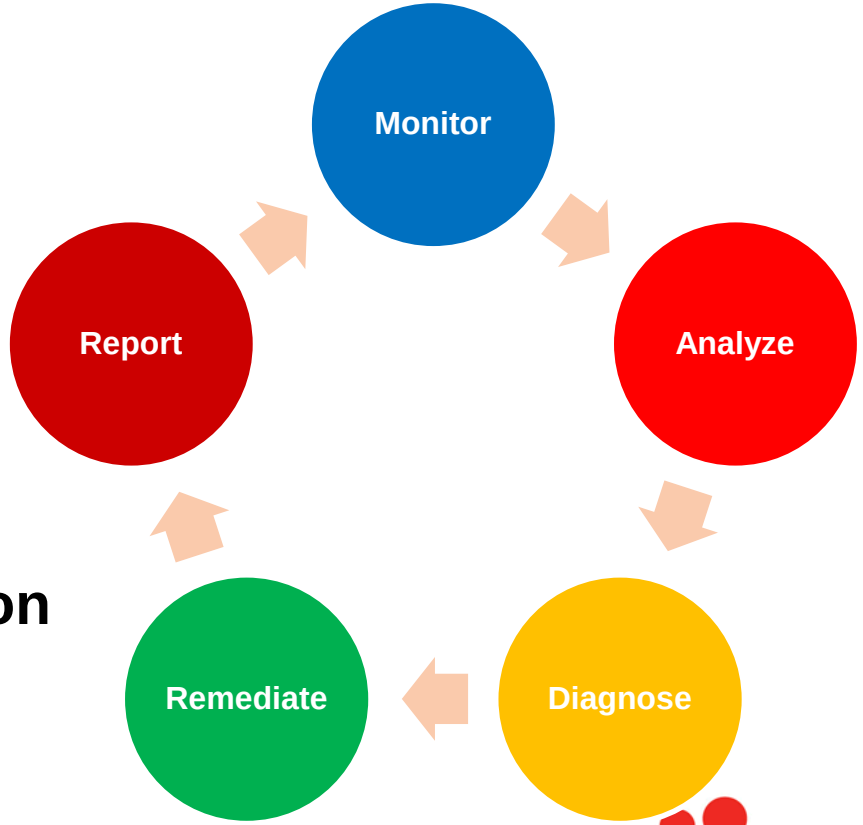
IP Monitoring Tools and Technologi

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

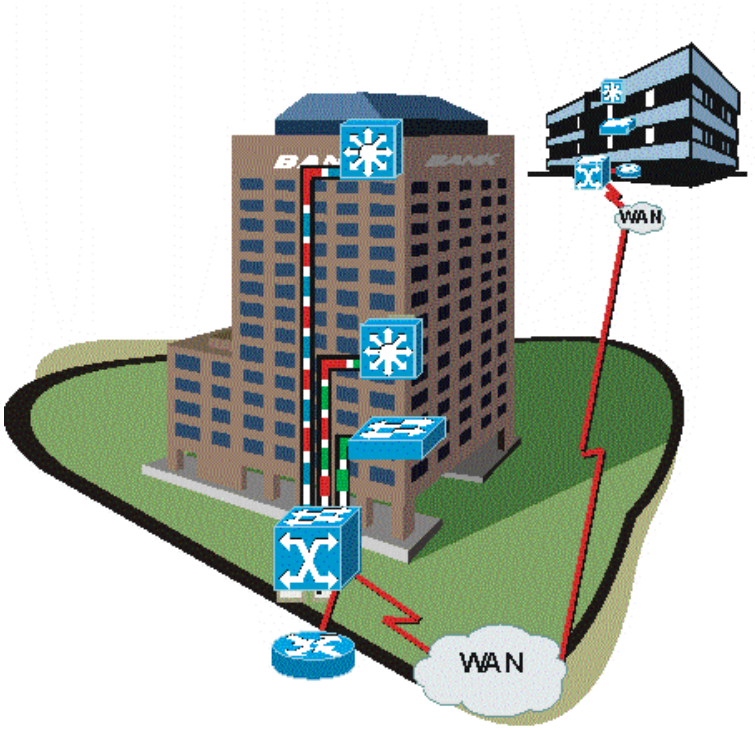
Fault Management
- What is the Status?

Configuration Management
- What is the configuration?

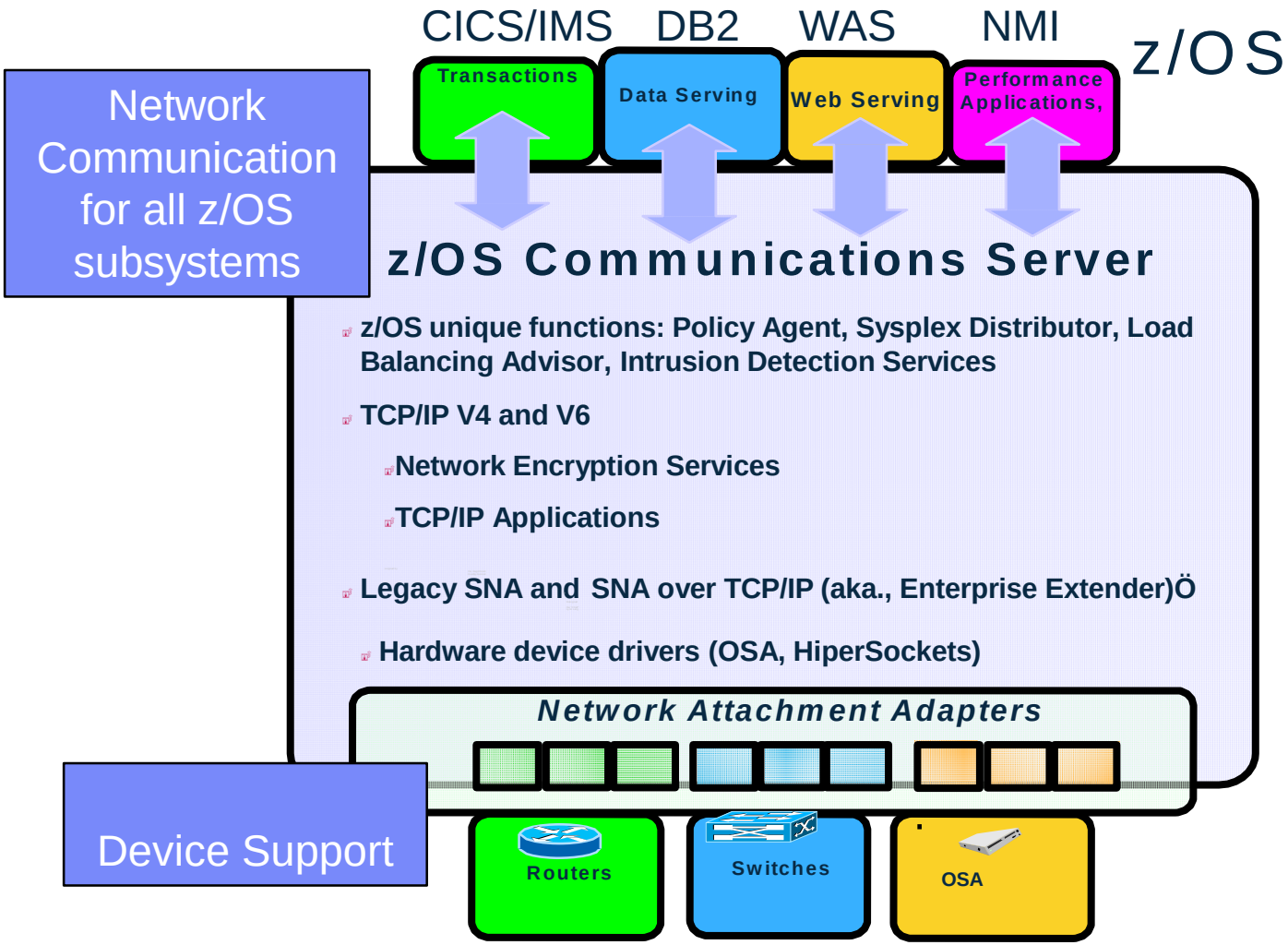
Availability Management
- What's down? What's available? What's up?

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



Agenda

Introduction

Why Monitor IP in the Mainframe?

IP Monitoring Tools and Technologies

Best Practices

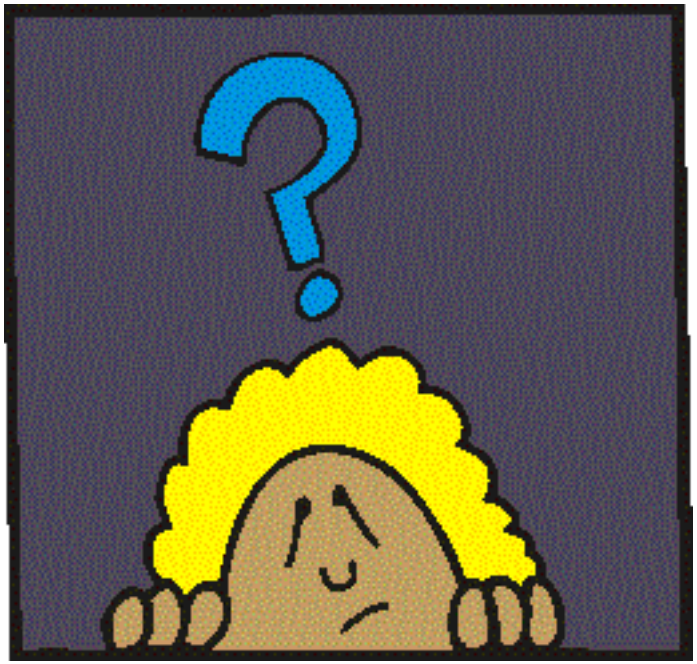
Murphy's Law

If anything can go wrong, it will

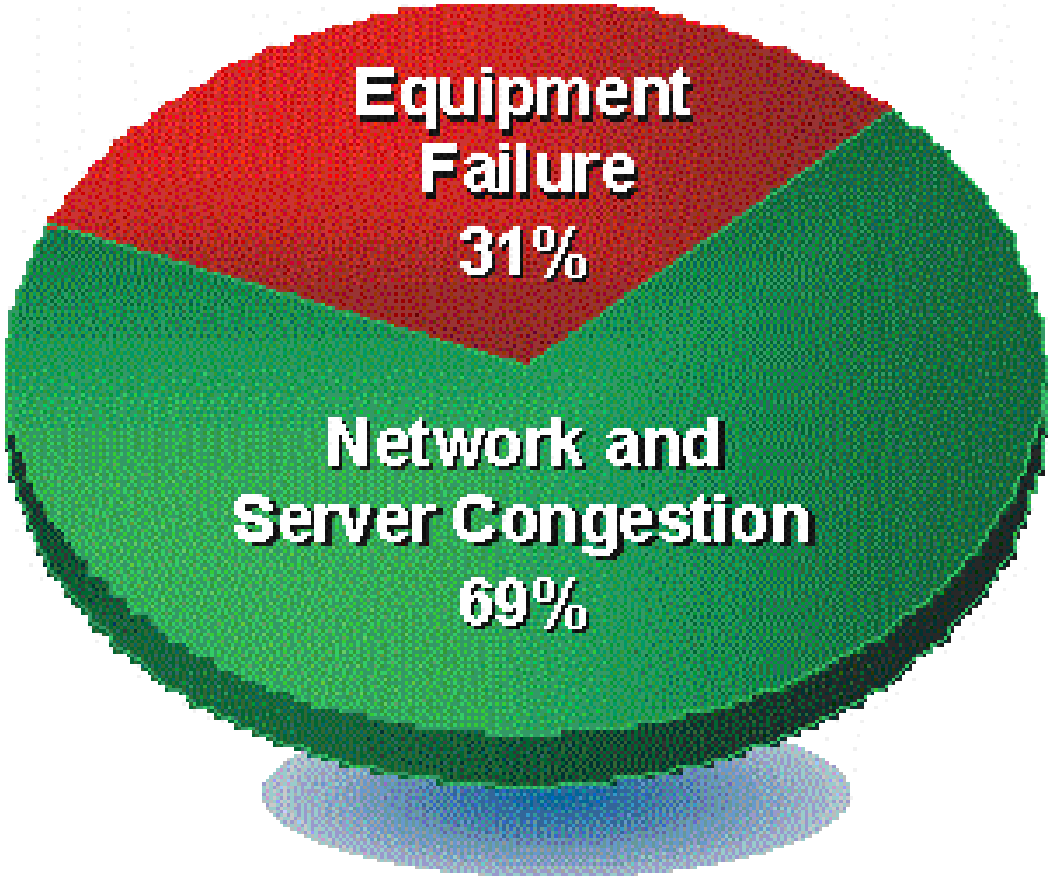
If anything just cannot go wrong it will

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



Common Problems

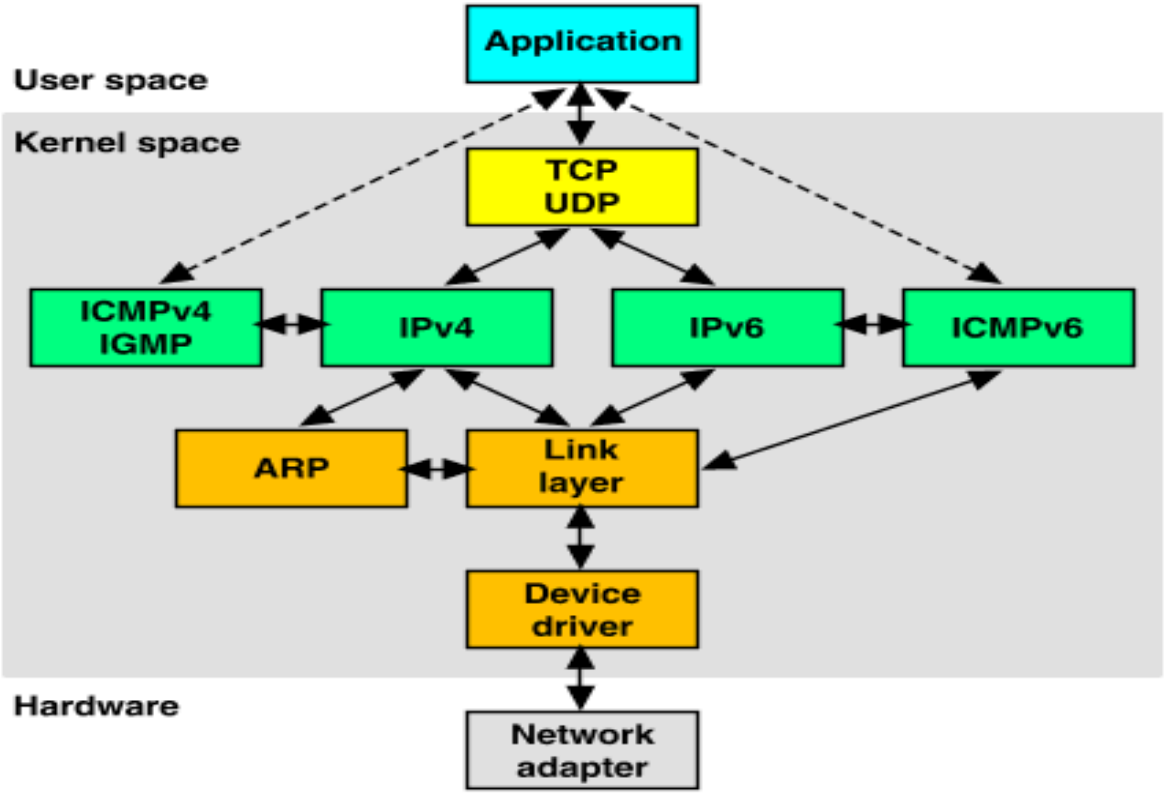
- Hardware failure
- Configuration change
- Firmware change
- Traffic rate change
- New application deployment
- Network failure
- Security attack
- Routing changes
- Buffer shortages
- Resource shortage
- Spanning Tree problems
- Illegal access to resources

Why Monitor IP?

Browser **Server**

Application TCP Transmission Control Protocol	WWW, mail, file transfer, remote access Application interfaces End-to-end delivery	Application TCP Transmission Control Protocol
IP Internet Protocol	Best effort delivery	IP Internet Protocol
Network Interface and hardware	Physical connection	Network Interface and hardware

A View of IP


Application
User space
Kernel space
TCP
UDP
ICMPv4
IGMP
IPv4
IPv6
ICMPv6
ARP
Link
layer
Device
driver
Hardware
Network
adapter

Agenda

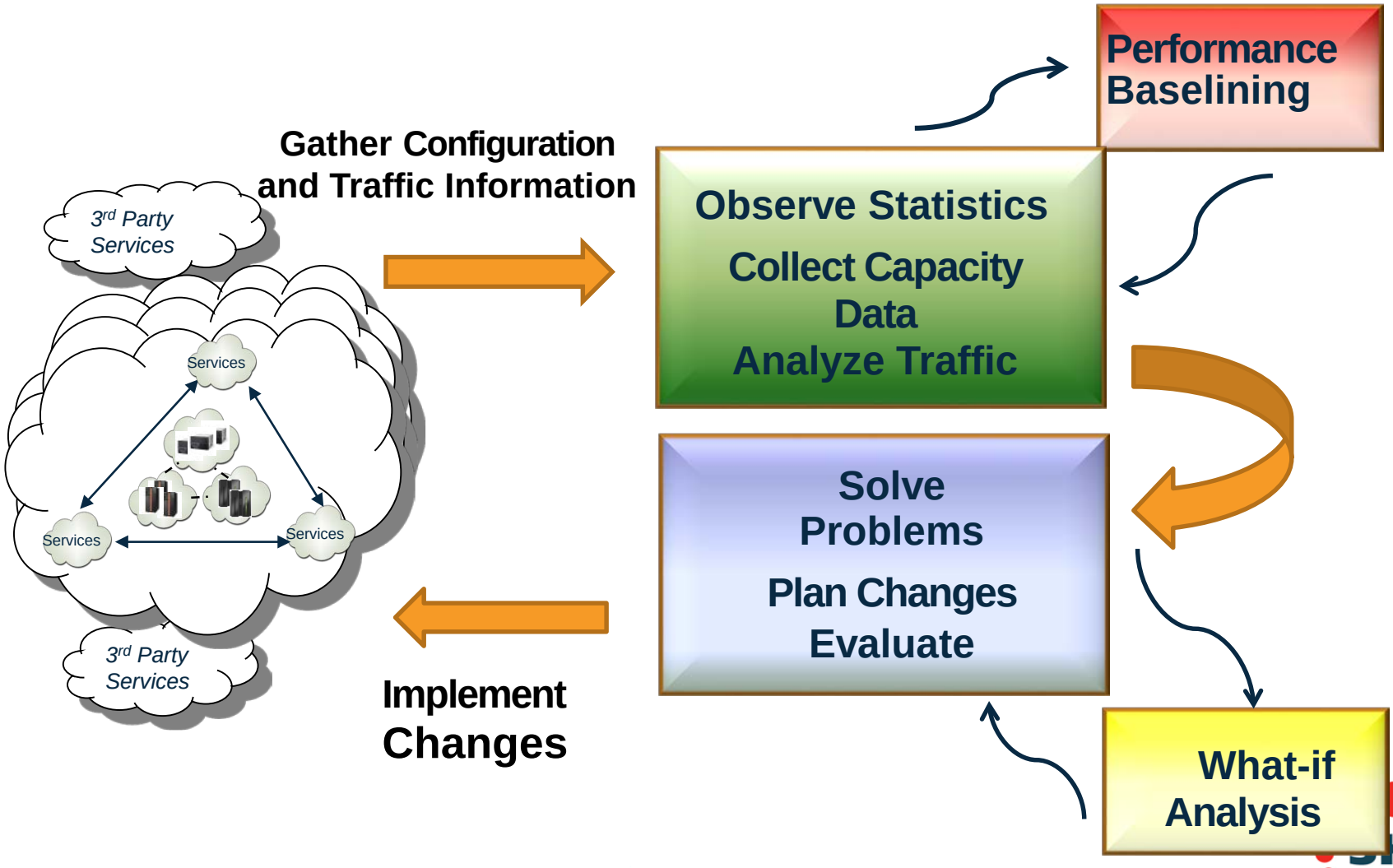
Introduction and goals

Why Monitor IP in the Mainframe?

IP Monitoring Tools and Technologies

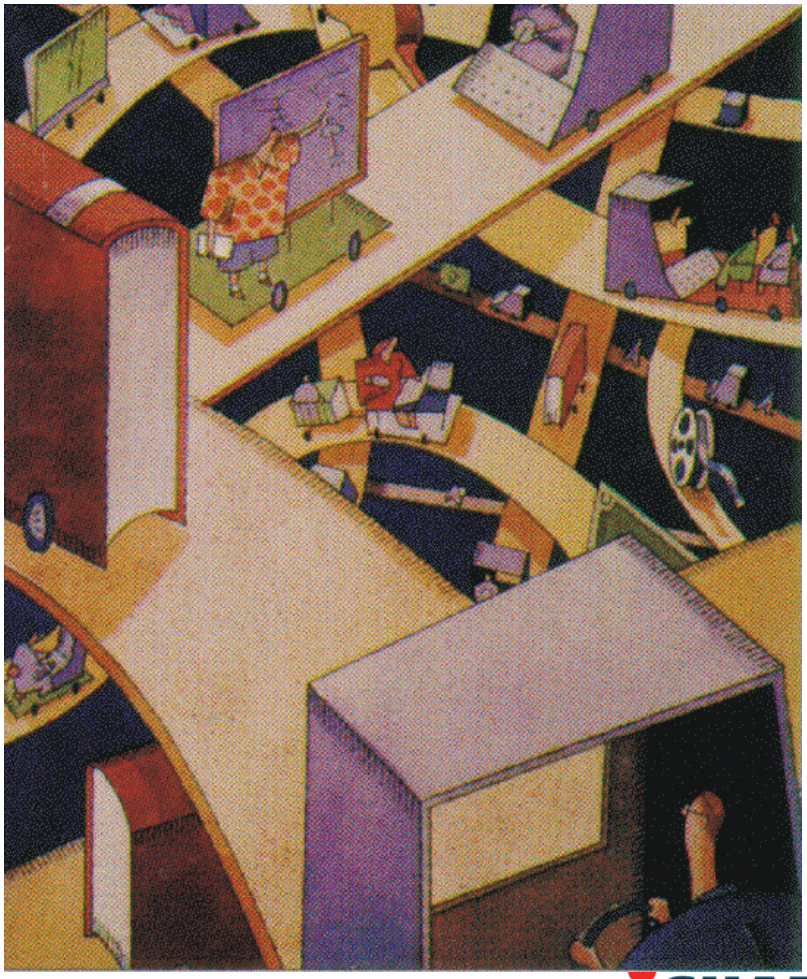
Best Practices

Effective Management



IP Resource Bottlenecks

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

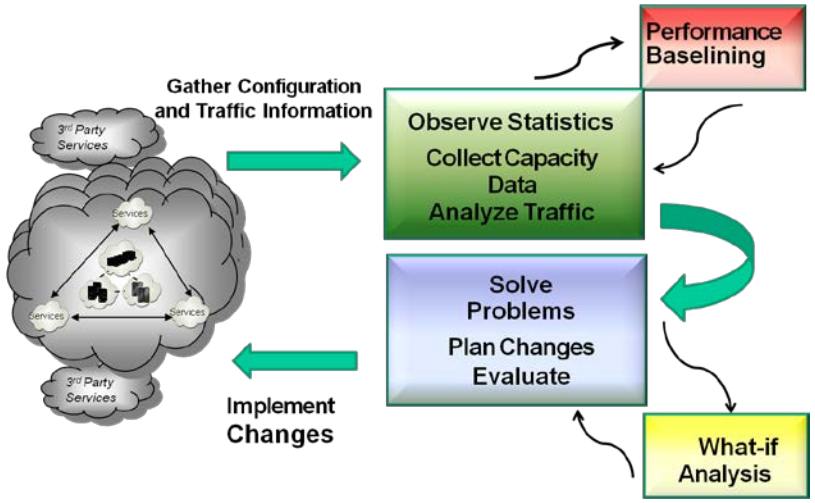


Results in:

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

Agenda

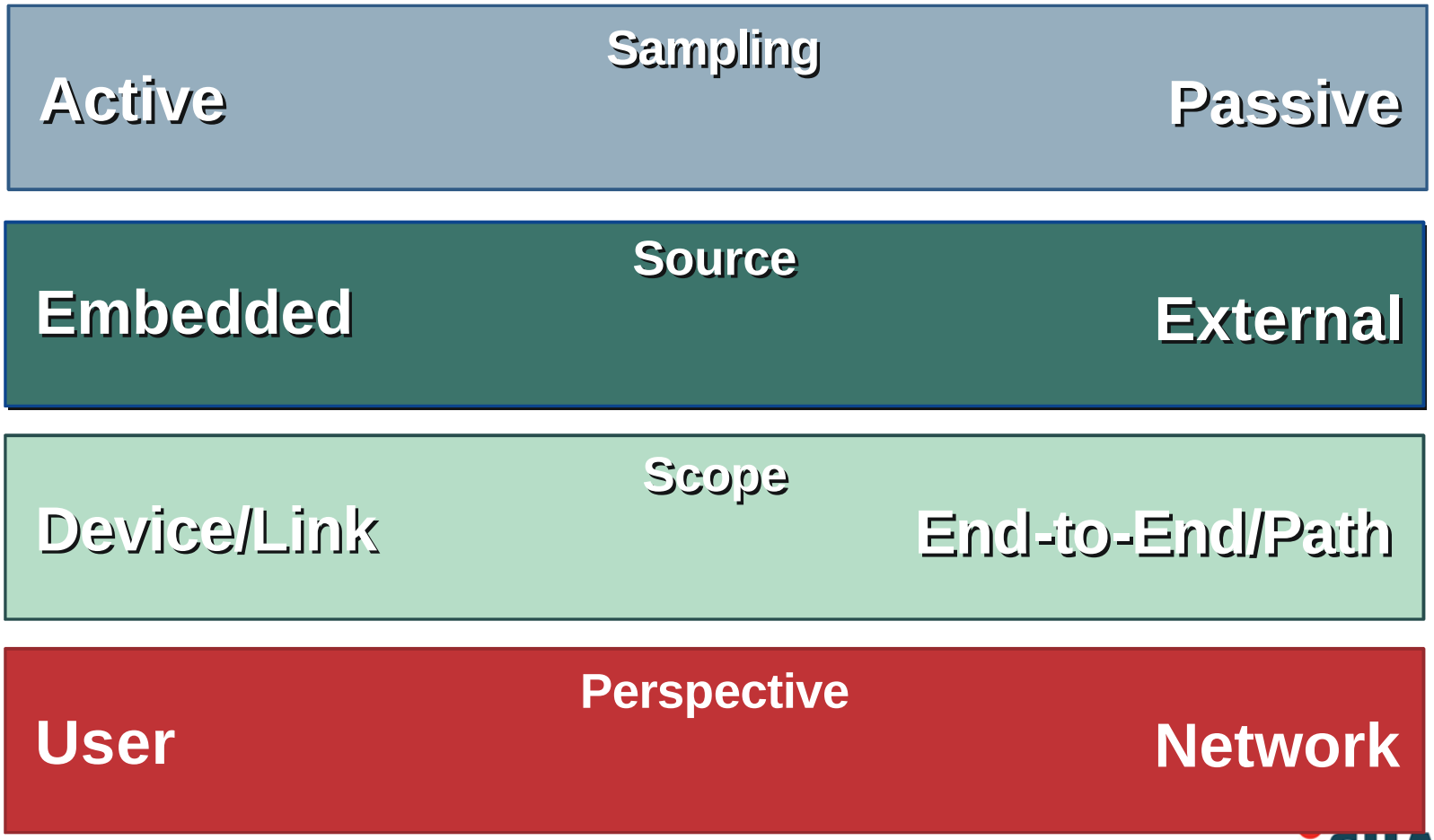
Introduction and goals

Why Monitor IP in the Mainframe?

IP Monitoring Tools and Technologies

Best Practices

Performance Management Practices



Core Mainframe IP Tools

TRACEROUTE

PING

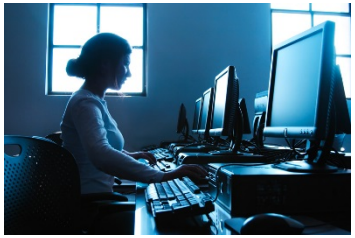
NETSTAT

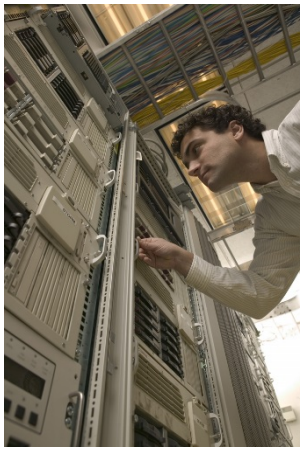
SNMP

NMAPI

Operating system or device specific
SMF for z/OS

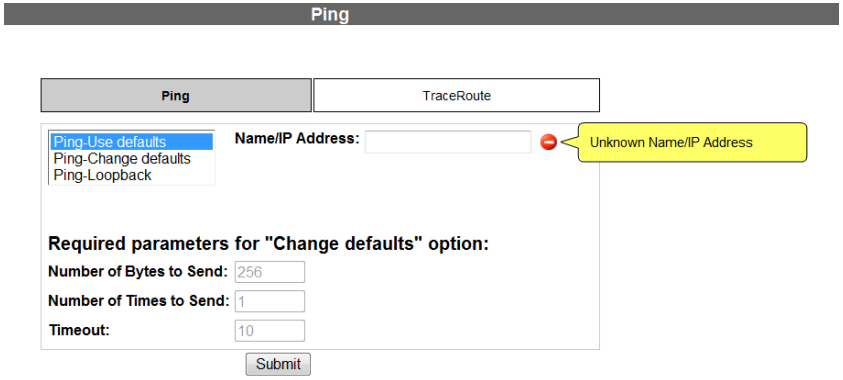
Basic Tools : PING



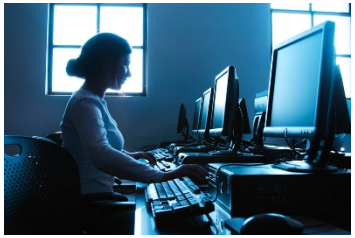


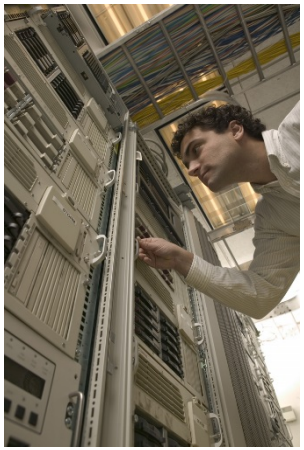
Tests connectivity to an IP device

Sends an ICMP frame to the destination



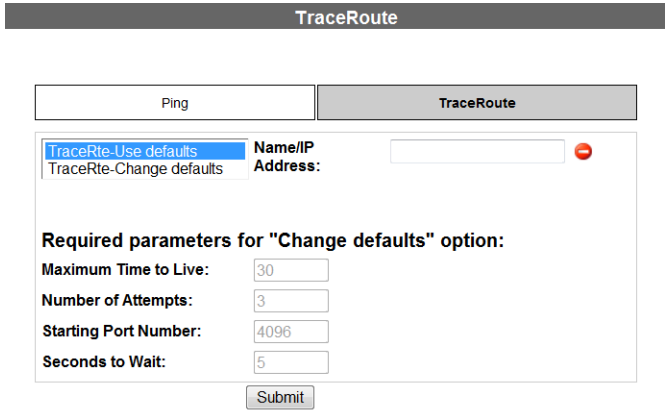
Basic Tools: Traceroute





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

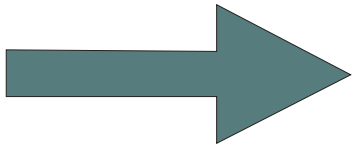
What is SNMP?

Simple Network Management Protocol

Internet standard

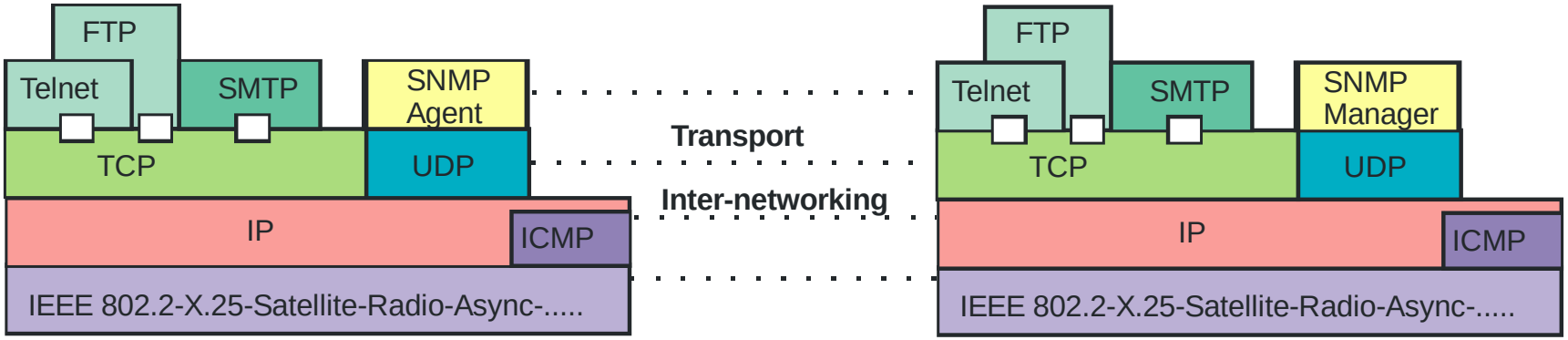
Initially tied to TCP/IP protocol

Set of functions
- monitor network elements
- control network elements



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

SNMP Layering



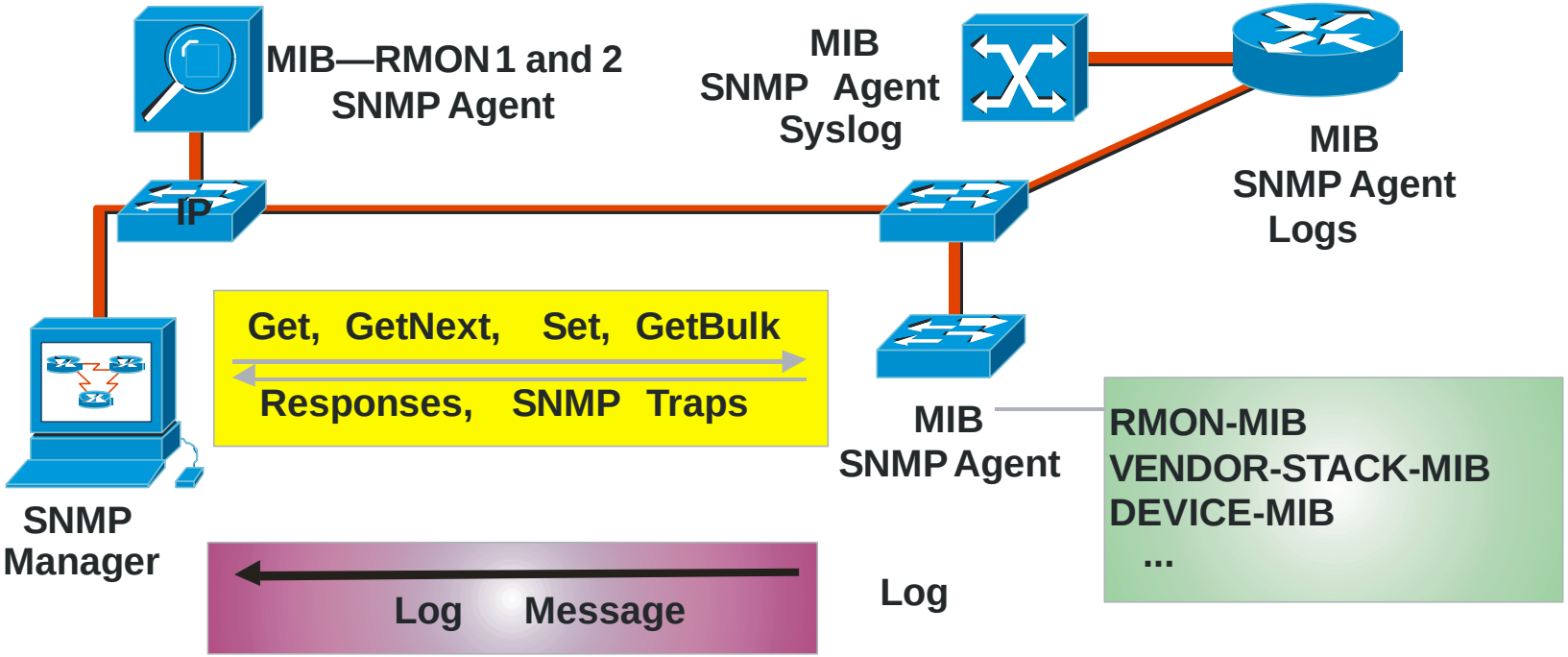
ICMP - Internet Control Message Protocol
UDP - User Datagram Protocol
Telnet Remote Access

- NFS Network File System
- RPC Remote Procedure Call
- SMTP Simple Mail Transfer Protocol

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

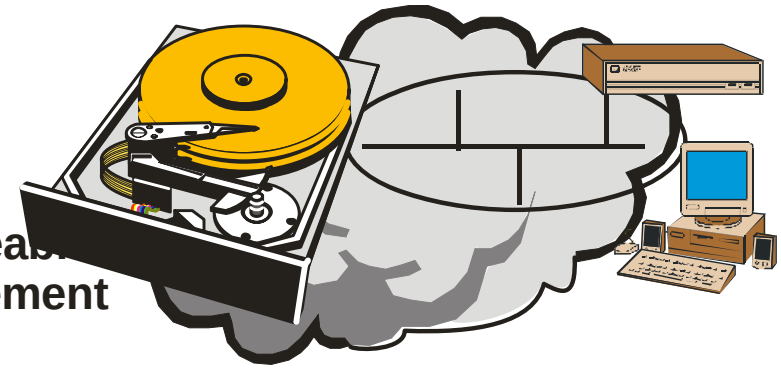
SNMP Flows



IP Connectivity	SNMP Traps/RMON	Log	Network Time Protocol	Vendor Specific

Management Information Base - MIB

How do the agents keep the information ?



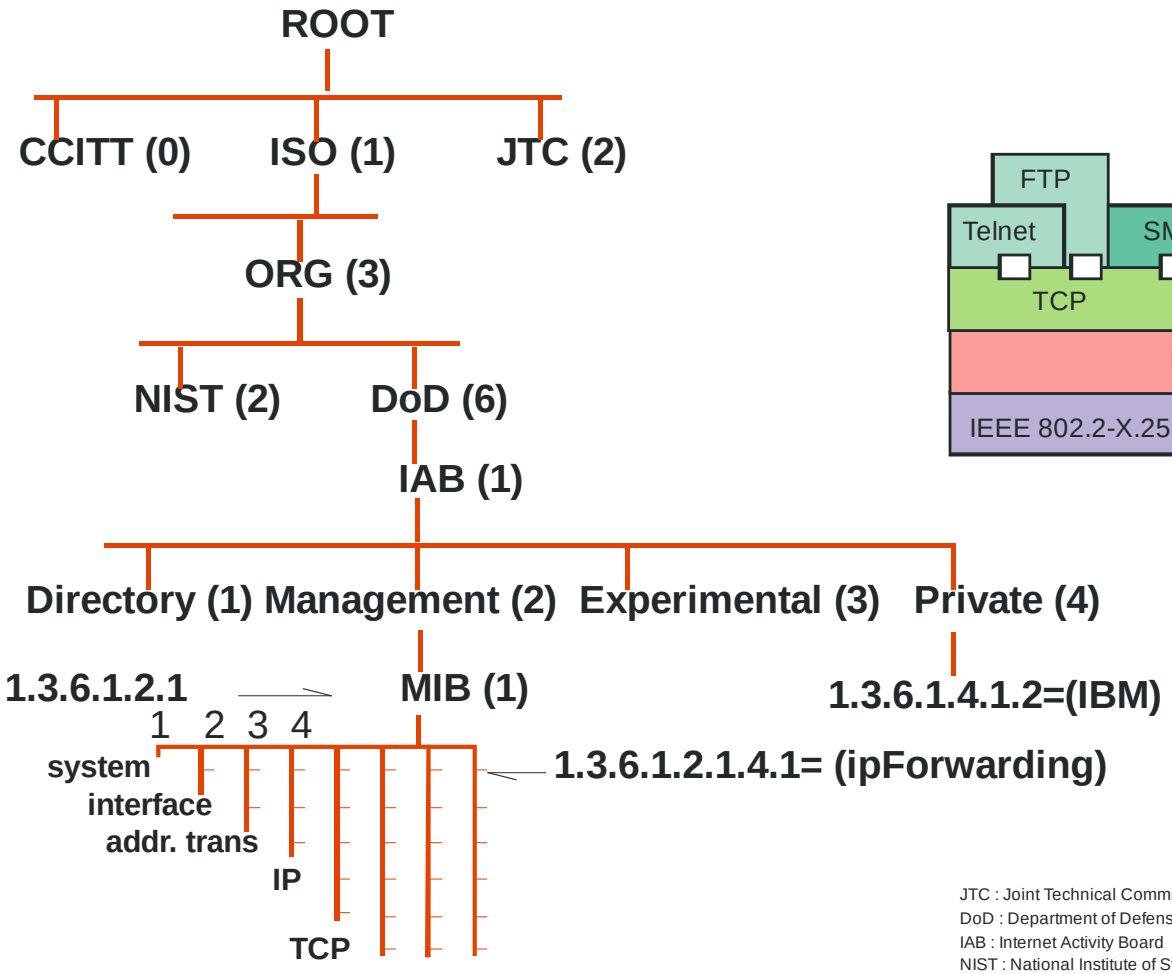
Universe of network manageable objects is called the Management Information Base (MIB).

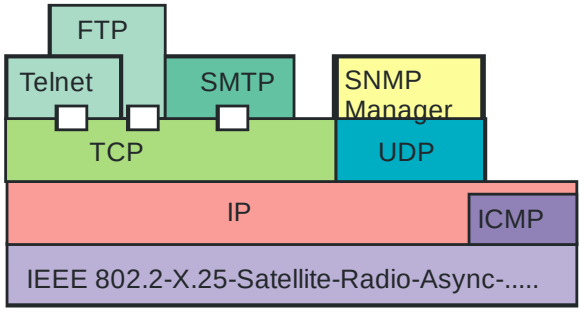
Items within the network elements which are manageable are called managed objects

Objects within the MIB are organized into the following groups:

MIB ....(114)	MIB-2 ....(171)
1) System	1) System
2) Interface	2) Interface
3) Address Translation	3) Address Translation
4) IP	4) IP
5) ICMP	5) ICMP
6) TCP	6) TCP
7) UDP	7) UDP
8) EGP	8) EGP
	9) CMOT
	10) Transmission
	11) SNMP I

Object Registration Hierarchy





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

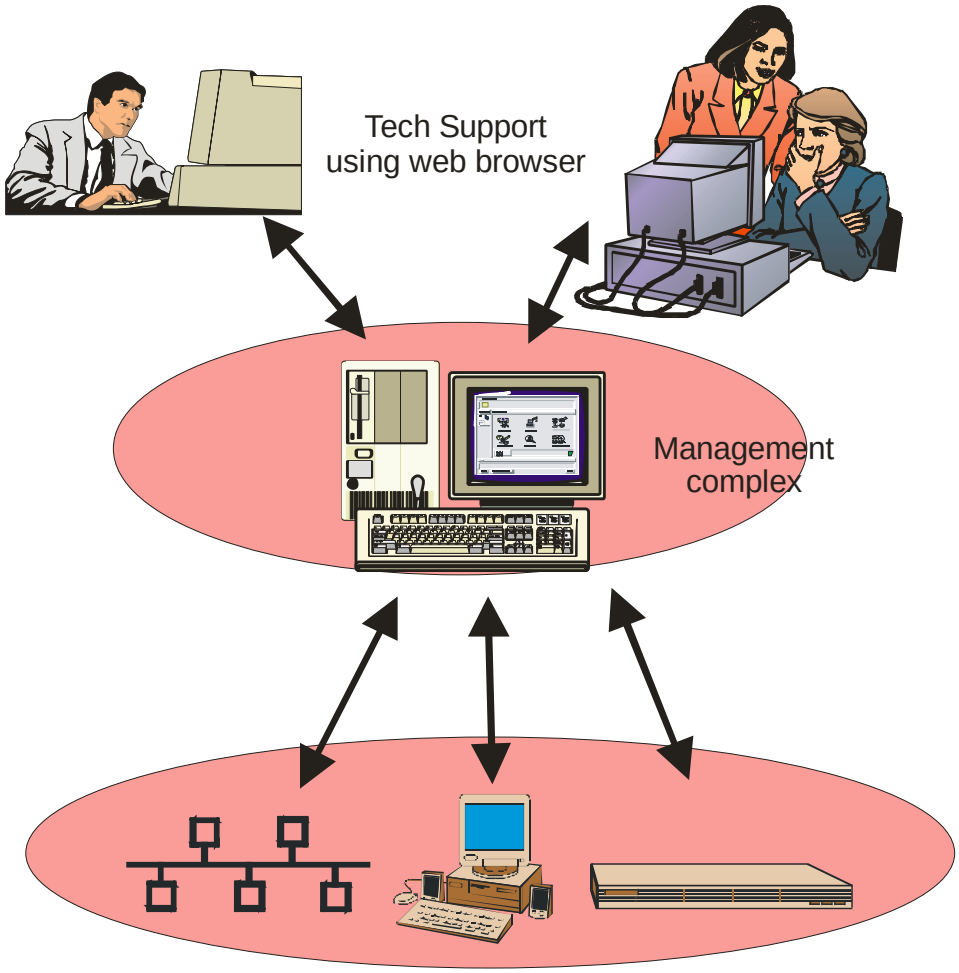
Management stations poll agents for MIB values

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

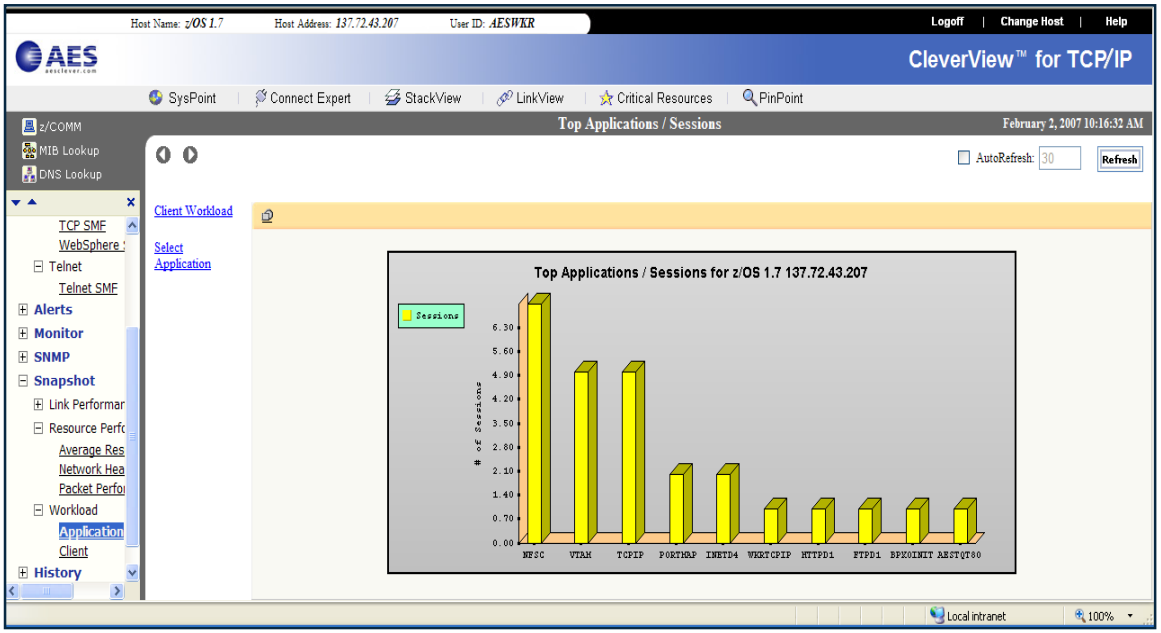
SMF Record Type Examples

- 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

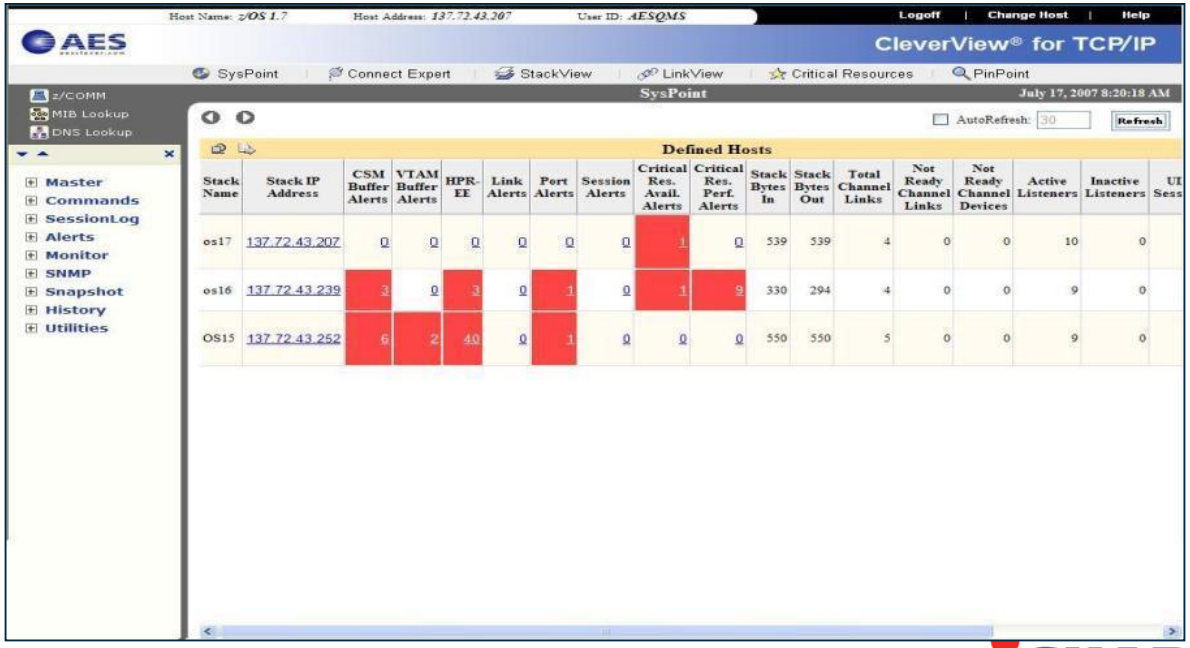
- Device and Link
- Interface
- VIPA
- Port details
- IKE
- IPSEC
- OMPROUTE
- SNALINK
- Buffer usage
- VTAM
- TN3270
- FTP
- Remote Print
- and more……



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

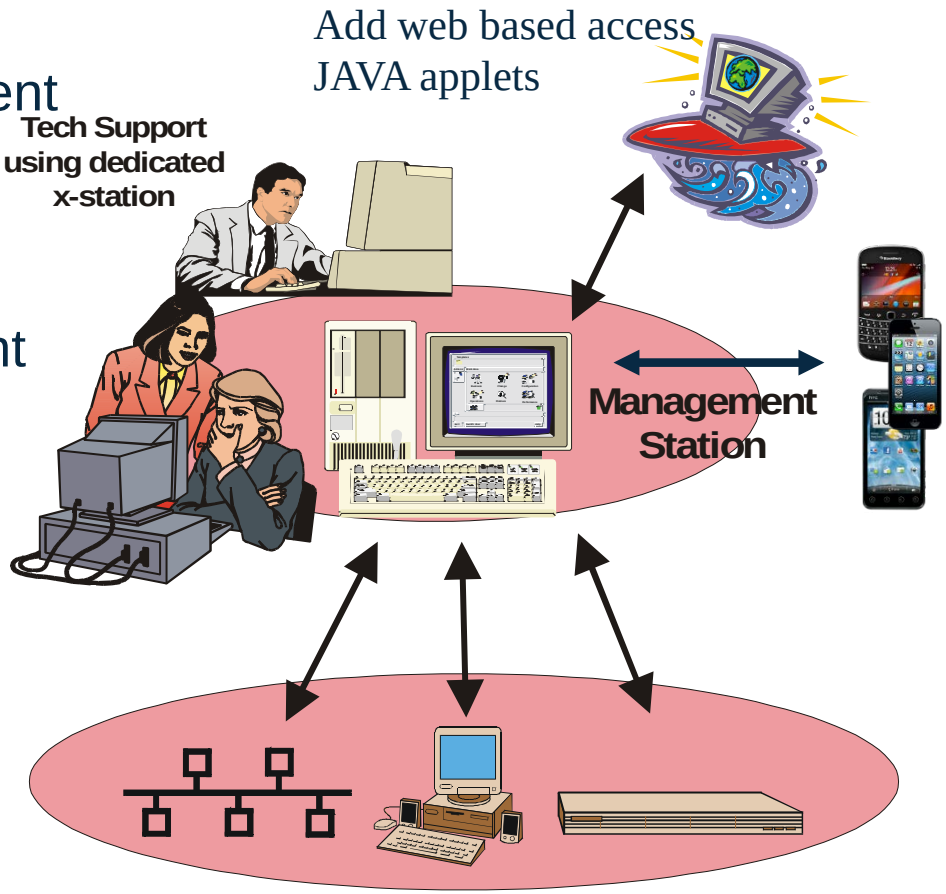
Real-time data

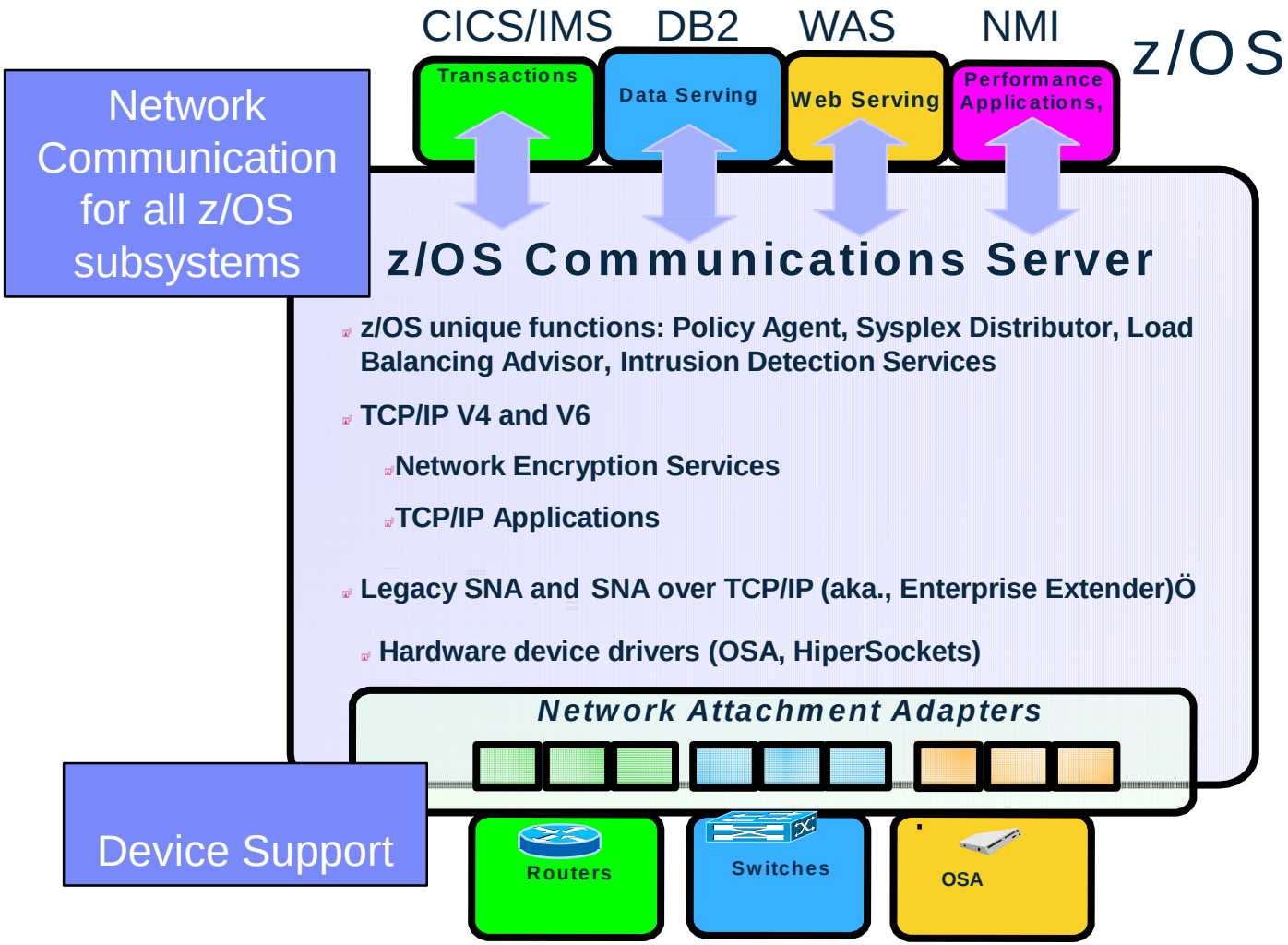
Pro-active Web and Mobile Based Management

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

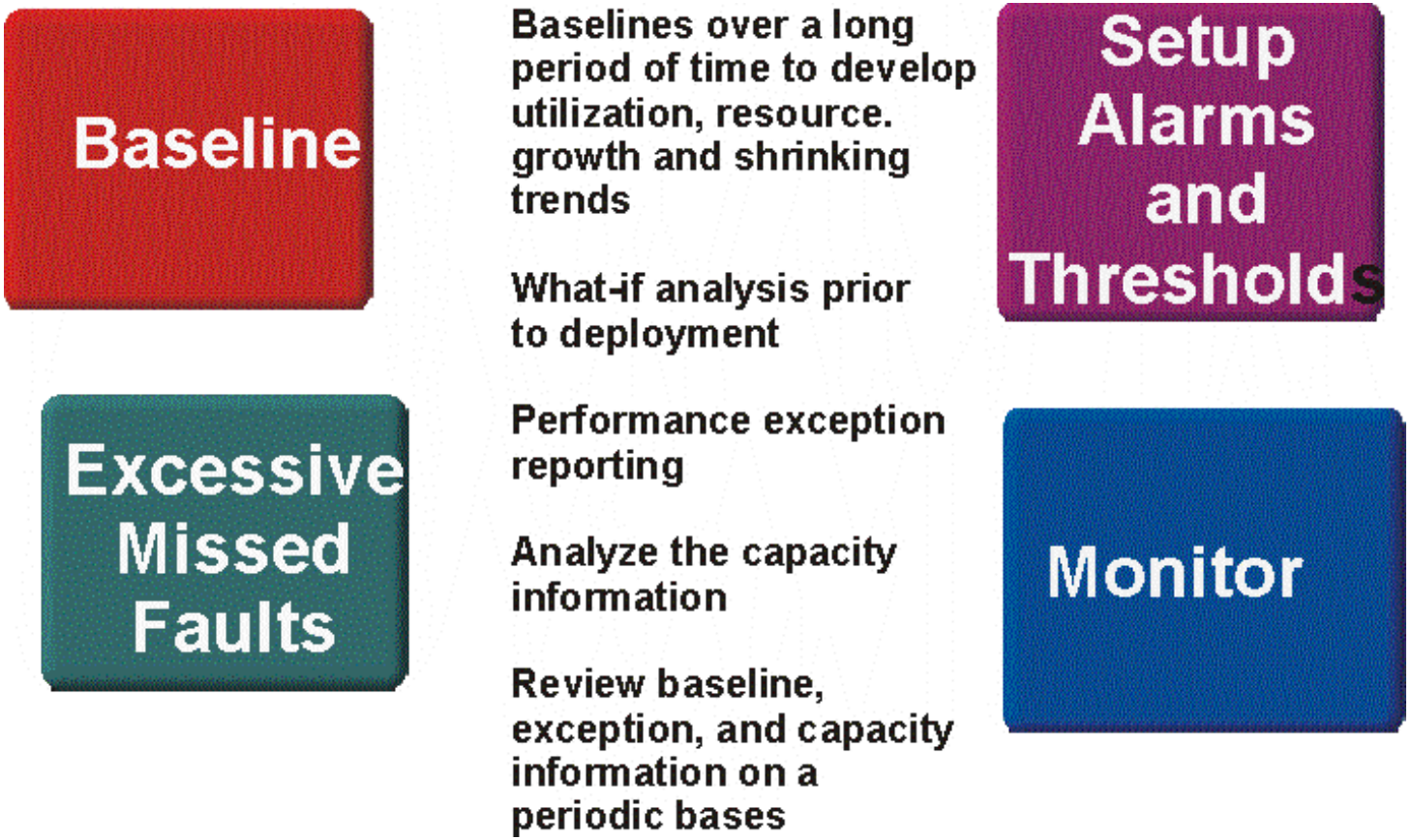
Reduces load on management stations processor

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

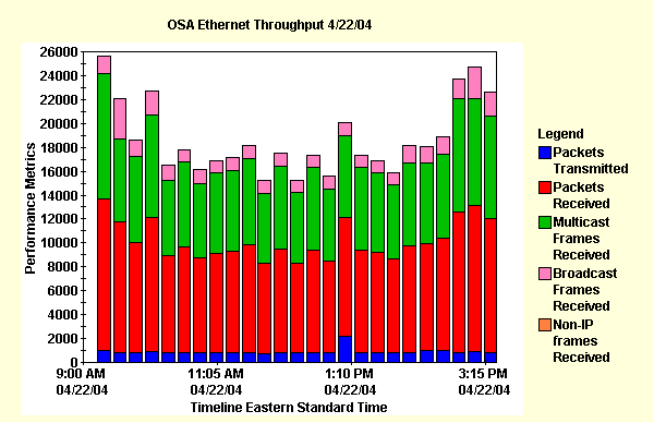



CICS/IMS
DB2
WAS
NMI
z/OS
Transactions
Data Serving
Web Serving
Performance Applications,
Network Communication for all z/OS subsystems
z/OS Communications Server
z/OS unique functions: Policy Agent, Sysplex Distributor, Load Balancing Advisor, Intrusion Detection Services
TCP/IP V4 and V6
Network Encryption Services
TCP/IP Applications
Legacy SNA and SNA over TCP/IP (aka., Enterprise Extender)Ö
Hardware device drivers (OSA, HiperSockets)
Network Attachment Adapters
Device Support
Routers
Switches
OSA

Steps to Effective Management



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

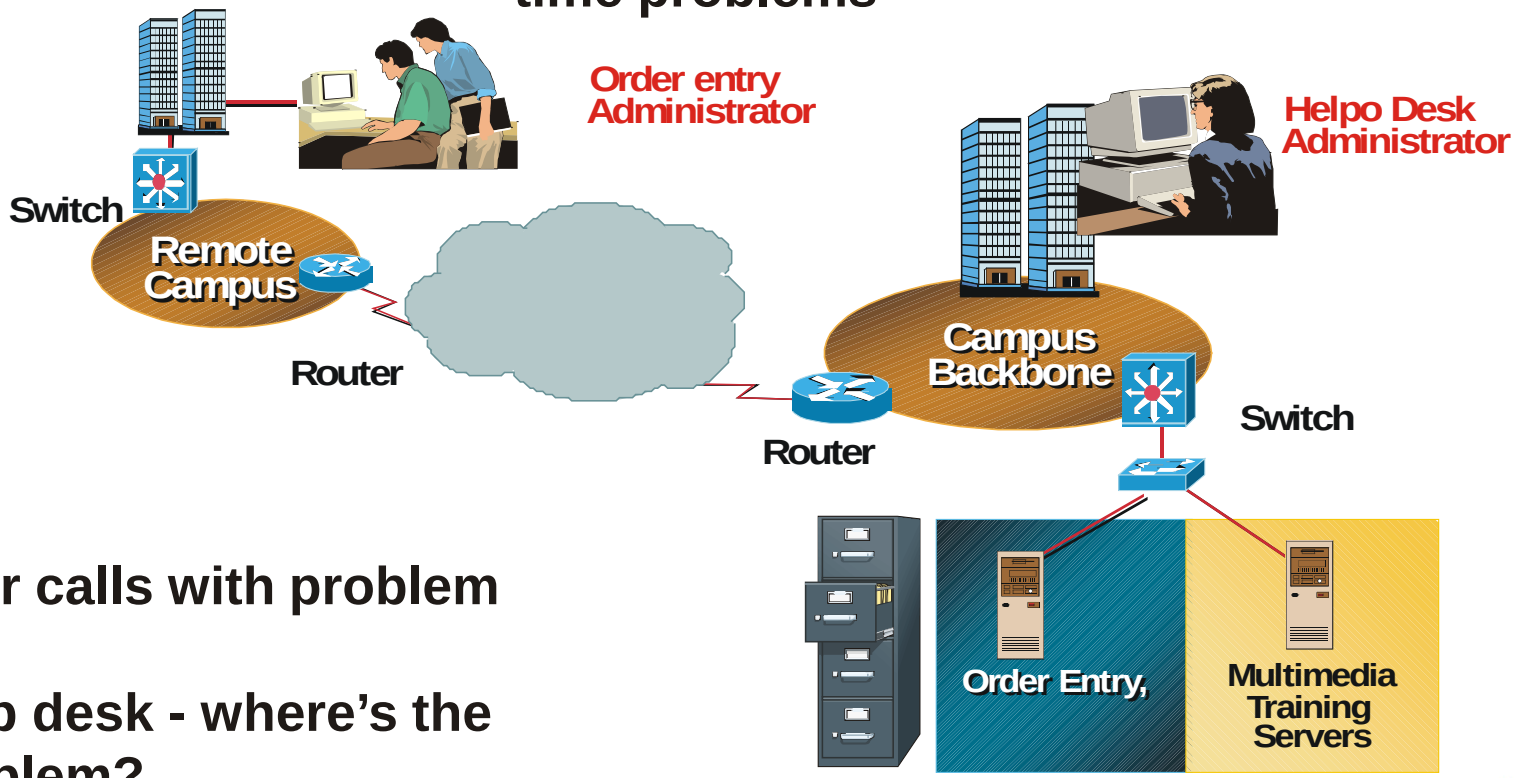
Why Monitor IP in the Mainframe?

IP Monitoring Tools and Technologies

Best Practices

Performance Case Study

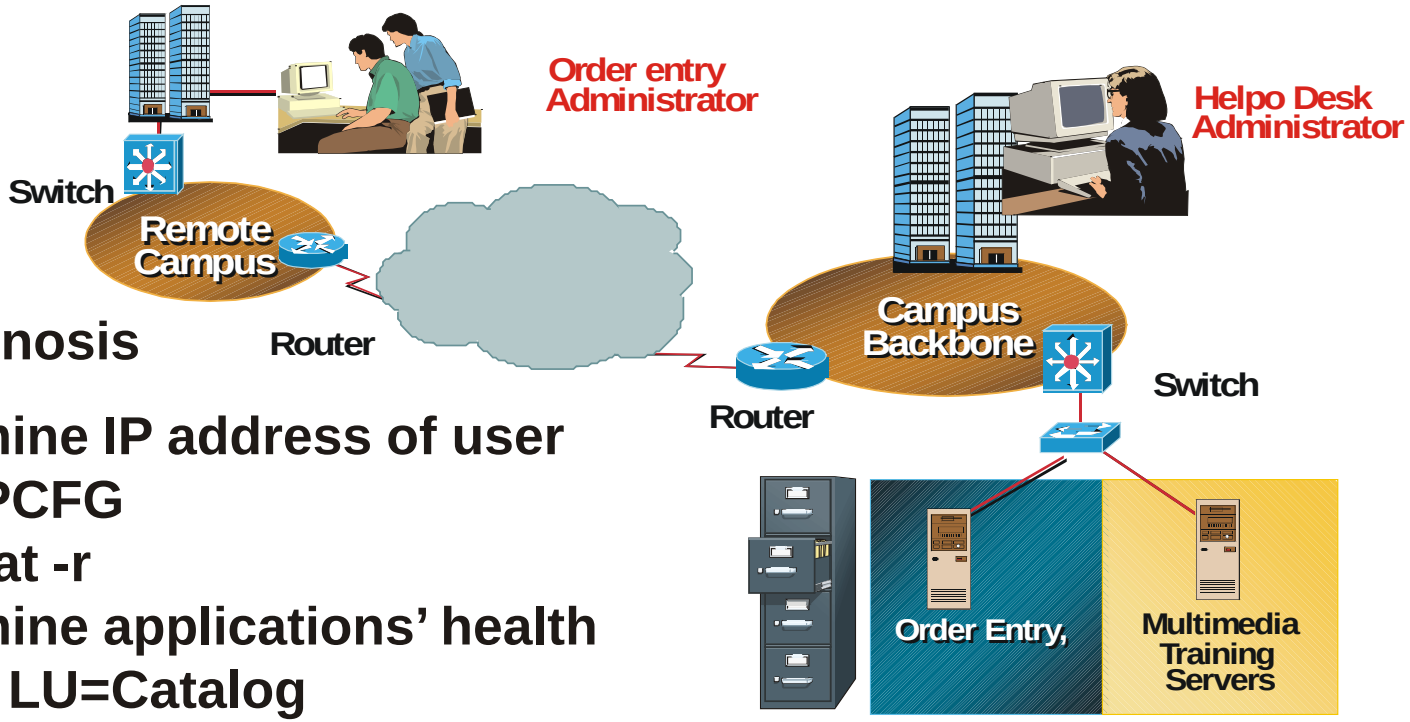
Catalog order processing system with TN3270E response time problems



User calls with problem

Help desk - where's the problem?

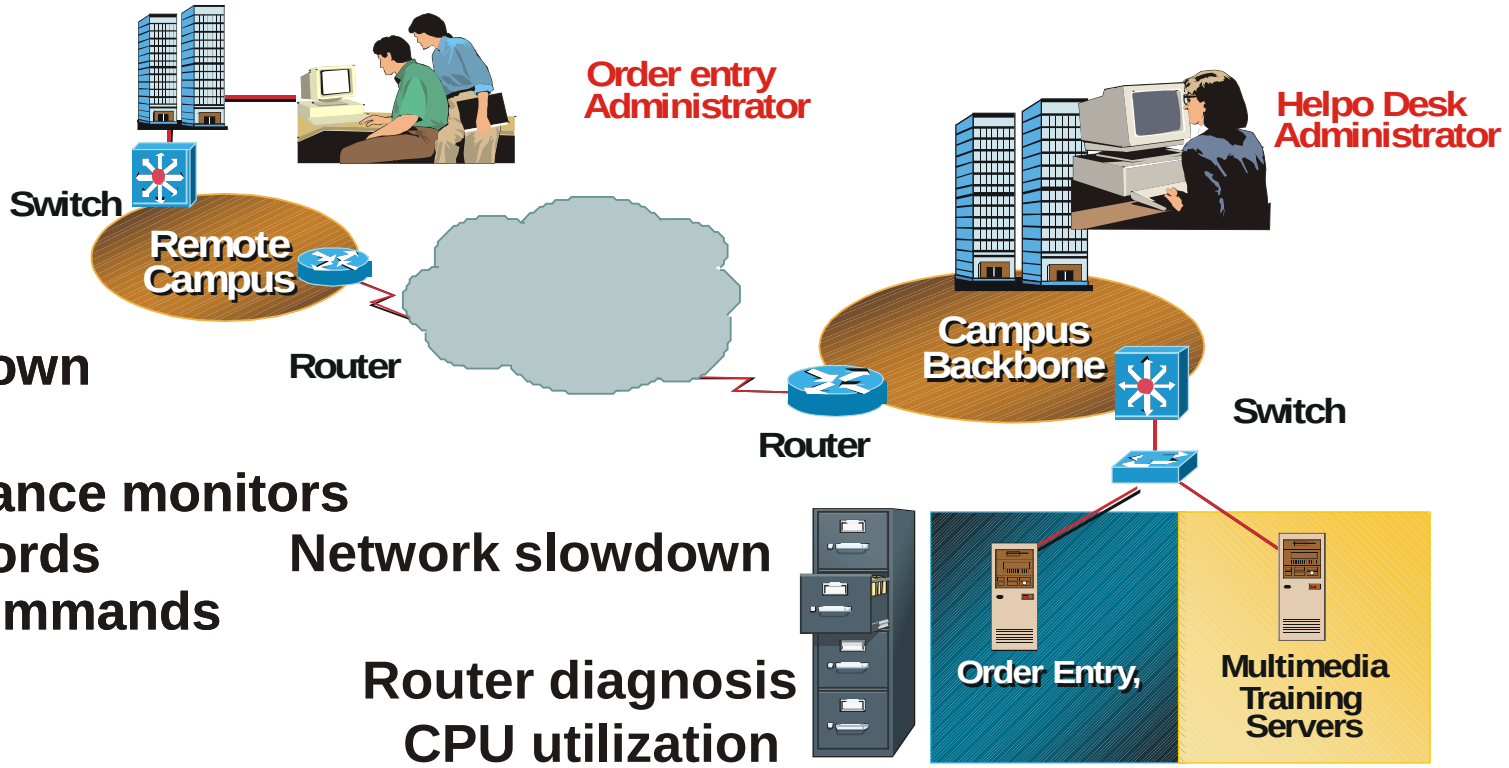
Case Study Reaction



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

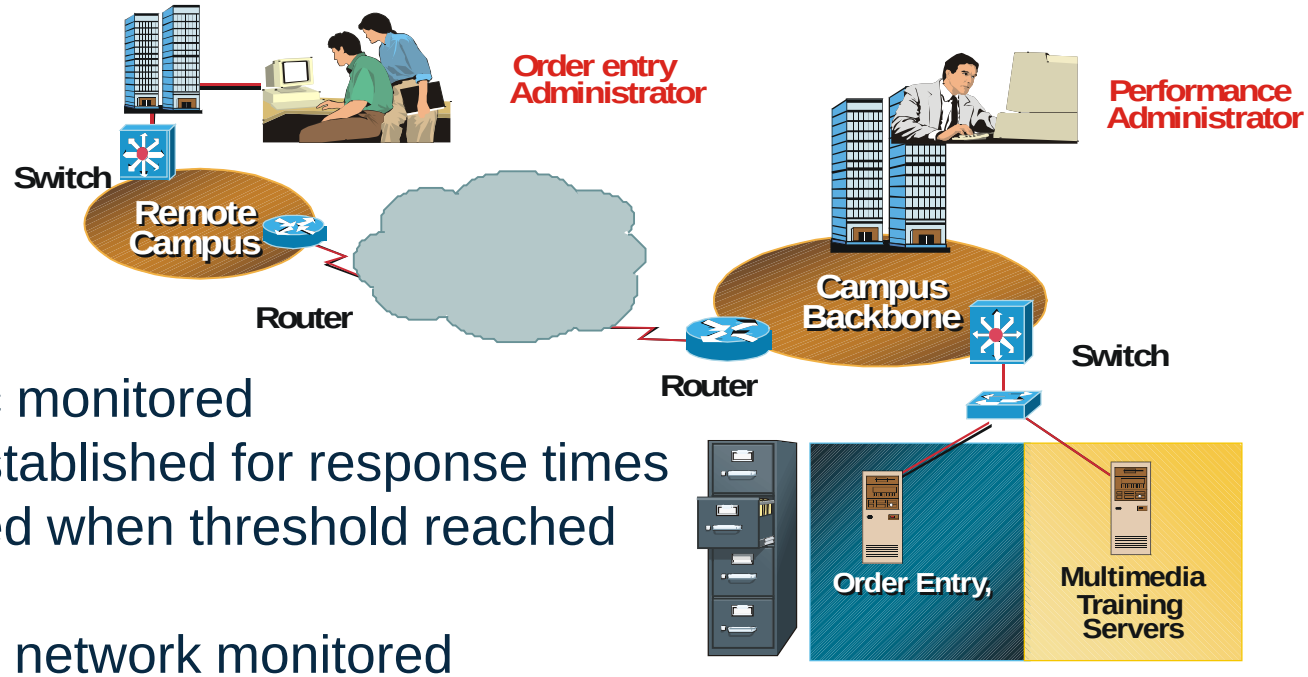
Network slowdown

Router diagnosis

- CPU utilization
- Memory utilization
- Packet errors
- Interface status
- IP stack analysis

Case Study - Proactive Solution

Administrator alerted to the impending problem.....

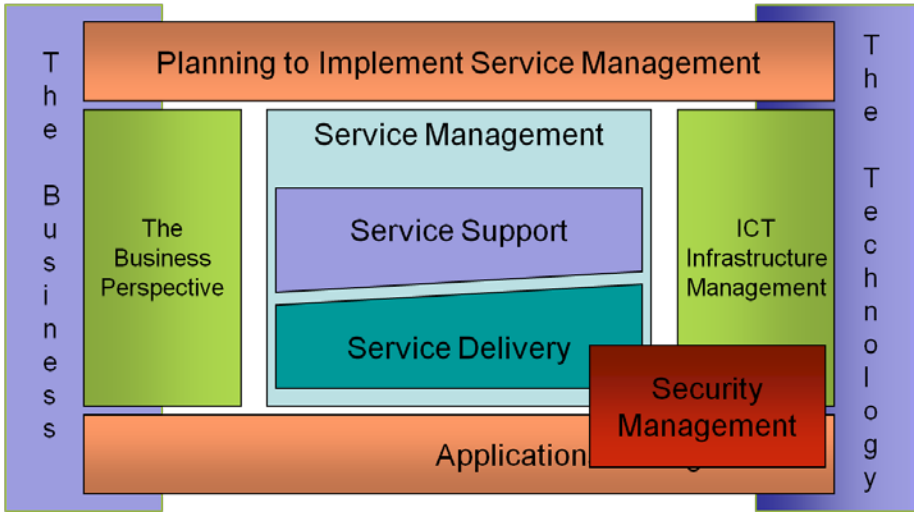


TN3270 traffic monitored
Thresholds established for response times
Alert generated when threshold reached

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



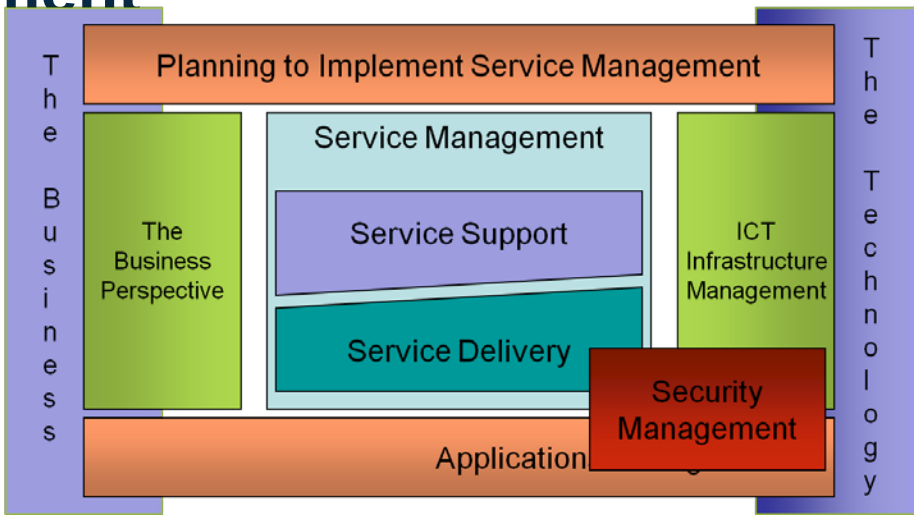
Proactive fault management is the area that ties together fault, performance and change management into an ideal network management system

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



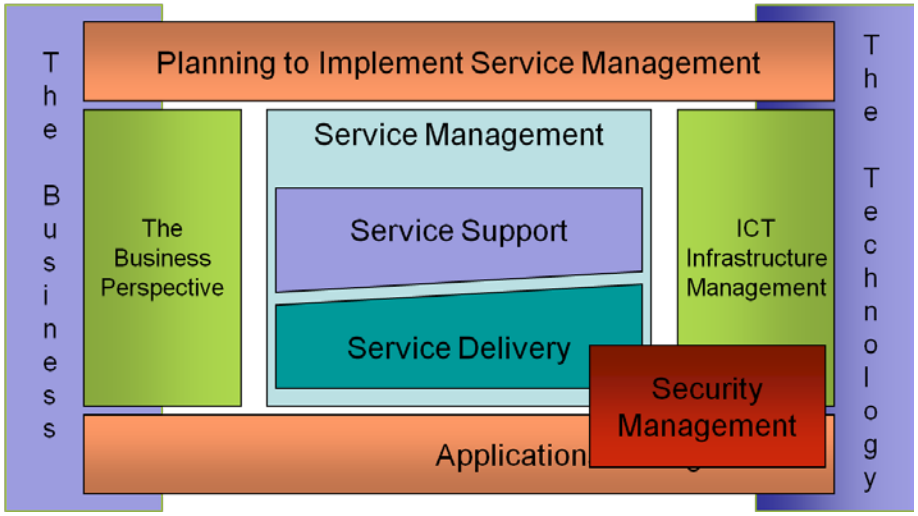
Analysis of performance data may lead to configuration changes

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

Questions?


Vielen
Dank


תודה


THANK YOU


Teşekkürler


Köszönettel


Obrigado!


Bedankt


Ευχαριστώ


ขอบคุณ


شكراً


Gracias


Merci


Díky


धन्यवाद


Hvala