Network Troubleshooting, Performance Tuning, and Management Fundamentals

Network Analysis and Performance Tuning

>> The purpose of network analysis:

1) Knowing the functioning of the network.

2) resolving network fault conditions and to improve overall network performance through performance tuning.

>> Knowing the network functions includes the following.

1) WAN link and LAN segment bandwidth utilization
2) WAN and LAN protocol usage
3) Average and peak utilization network response times
4) Network traffic flow patterns between segments, gateways, and servers
5) Network application services
6) Layer 2 and Layer 3 packet statistics

>> Doing the performance tuning without the actual knowledge of the trouble will make the problem worse.

Tools:

>> Commonly used tools to identify or resolve problems include packet analyzers or packet sniffers, time domain reflectors, bit error rate testers, and software tools like ping and traceroute.

Documentation:

>> Proper documentation about a network will help to visualize the role of each component in the network.

>> Proper network documentation is a set of documents that describes the following:

1) The topology of the network, each of its hardware components, and the protocols in use to transmit, transport, and manage data delivery.
2) The site's cabling infrastructure and labeling scheme, kind of cabling used (copper and fiber), types of connectors, patch panels, average cable length between the end-stations and the interconnect panel, and any certification documentation.
3) The servers on the network, their operating system, the function they perform, network address information, administrator information, and so on.
4) A management document that describes the general operational policies regarding the network.

>> Topology Maps: Full details about all the devices in the network, physical location, cabling, connectors. May have more than one map.

>> Device Information: Contains the following;

- Hostname/system name
- Installation location
- Network address(es) and supported protocols
- MAC address(es)
- Manufacture and model
- Vendor information and contact numbers
- Service contract number
- Local technical contact
- Data port assignments (what end-devices are connected to its ports)
- Software version
- Dependent or adjacent devices
- Description of primary function

>> Change Log: data about changes such as network patches, device moves, software and hardware upgrades, and device module additions and removals.

Protocol Analyzers:

>> Capture and display network protocol data.

>> Can perform real-time or offline analysis of some or all of the network segment traffic.

>> Collected traffic data can be saved and analyzed later.

>> Use filters and triggers.

>> Works in non-intrusive, promiscuous mode.

>> WAN analyzers come with passthrough interface cards that sit between the computing device (for example, a router) and the DSU/CSU.

>> Eg: Wireshark

Time Domain Reflectors (TDR):

>> Used for diagnosing cable failure and associated problems.

>> A typical TDR has two components: a TDR scope and a cable terminator. The scope is on one end and the terminator is connected to the other end of the segment.

>> Work by sending a test signal with a specific amplitude and rate into the cable segment and listening for an "echo" or reflection. if no echo is detected, the cable is free of errors.

>> If an echo is detected, the TDR scope can determine the type of problem based on the type of reflection (which is called Cable Signal Fault Signature (CSFS)).

>> It also tells at what distance the fault is detected.

Bit Error Rate Testers (BERT):

>> Used by Local Exchange Carriers to test telecom transmission circuits.

>> BERTs operate by sending different test patterns across the transmission circuit.

>> Test patterns can be fixed or pseudorandom (all consist of zeros and ones).

>> BERT testing can be intrusive or non-intrusive, depending on how the BERT is placed in the circuit path.

>> For non-intrusive testing, the BERT taps into the transmit and receive pairs and monitors the traffic stream.

>> With intrusive testing, one or two BERTs can be used to transmit and receive test patterns.

>> When two BERTs are used, they replace the DSU/CSU at the circuit's ends and exchange bit streams. When only one BERT is used, the remote DSU/CSU is placed in loopback mode and the BERT sends and receives the test pattern signals.

Packet Internet Groper (Ping)

>> IP-based tool for testing host reachability (began in UNIX).

>> Sends ICMP echo_request messages to the destination host which if in the network responds to the source host with ICMP echo_reply messages.

>> Generally displays the ICMP message size, its sequence number, its Time To Live (TTL) value, and its round-trip delivery time.

Traceroute:

>> To check the route to the destination host or to verify that all of the gateways in the transit path are up.

>> Uses ICMP echo-request messages to trace the gateway path one hop at a time.

>> This is accomplished by sending ICMP messages one by one with TTL starting from 1 and incrementing on each message, until a response from the destination is obtained.

Developing Troubleshooting Skills:

>> Problem resolution commonly takes place in either a proactive or reactive mode.

>> Proactive problem resolution identifies problems and resolve them before they impact service performance.

>> Reactive problem resolution (or fire-fighting mode) deals with problems as they arise.

>> Proactive monitoring is preferred for networks and reactive problem resolution comes in the identification and resolution of user problems.

>> Some guidelines to help when troubleshooting:

1) Know the real problem; whether the network is down, or only the performance has fallen, or losong the connection intermittently etc.
2) Ask the right questions to the user and listen to the answers.
3) Note/draw the details.
4) Define clear start and stop points.
5) Document everything on the process.
6) Look into every detail. Sometimes even a patch cord to a router can fail the entire network.

Network Management Functions:

- Physical infrastructure, interconnection cabling and patch panel design, installation and management, end-station patching and network hardware installation. Cable testing and length validation also fall into this category.
- Device configuration, bridge, router, switch, and repeater configuration. Backup, archiving, and documenting device configurations.
- Link and services monitoring, network performance baselining, and periodic performance revaluation. Proactive and reactive hardware, link and network service failure detection. Network security monitoring.

>> Small networks can be managed by a single administrator.

>> In large enterprises, a Network Management System (NMS) is generally required which is expensive and complicated. They require expensive hardware and software components and, trained staff to interpret the management data and do problem resolution.

NMS Architecture:

>> An NMS consists of

The network hardware components that need to be managed (router, end-device, etc)

A software or firmware-based management interface or agent (on the device itself).

A network management protocol (NMP).

A network management console (NMC).

>> The hardware components are classified into two categories: managed and unmanaged nodes.

>> Managed nodes have the ability to perform basic testing and diagnostics on themselves and report their operational status to a management entity.

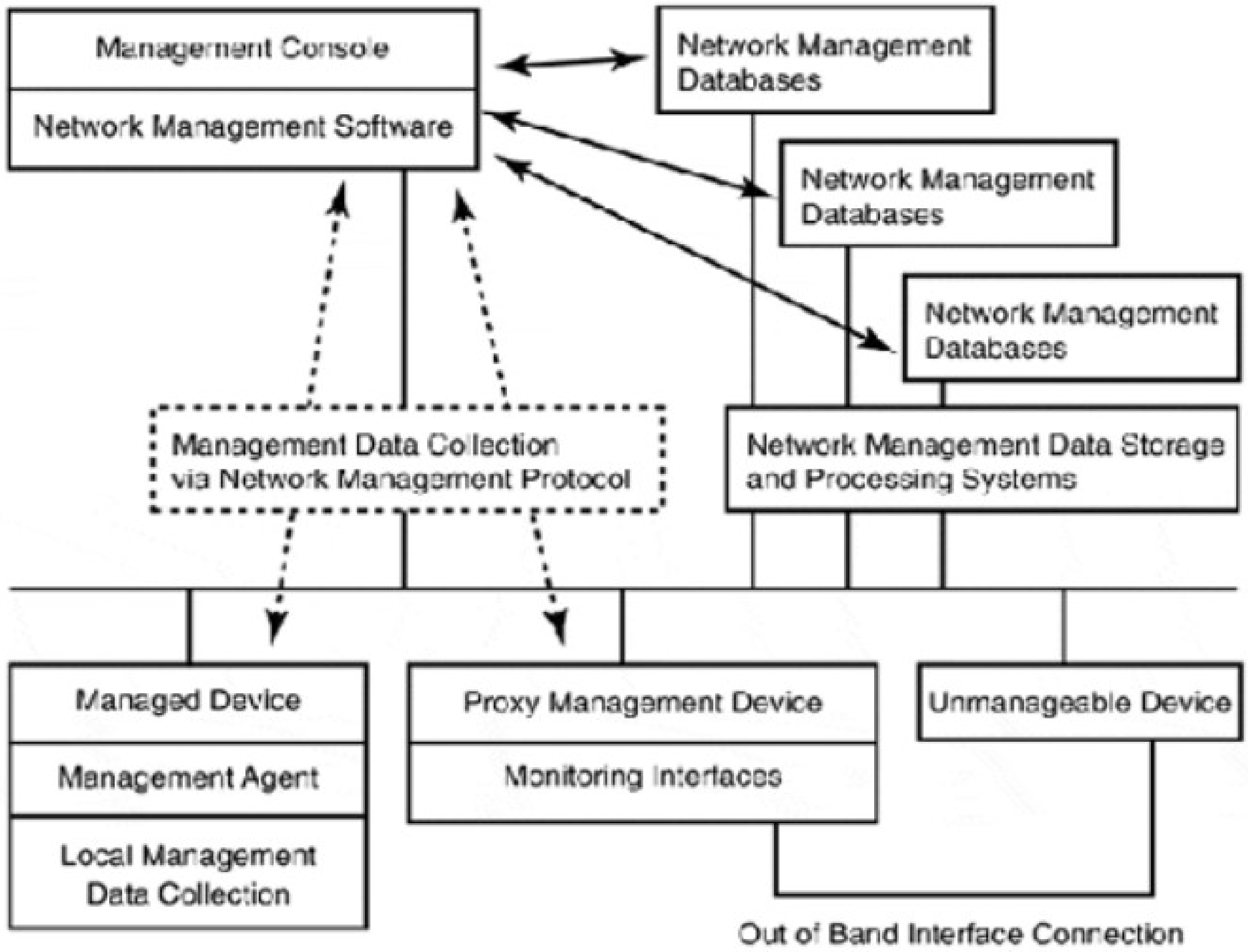
>> Unmanaged nodes are devices that cannot directly support a management agent. They are managed through end-devices/hardware-devices (called proxy) where an NMS is running.

>> NMP defines a format for exchanging management information (Eg: SNMP)

>> NMC is a computer that operates one or more management entities. There may several NMCs for large networks.

>> The management information are stored on network management databases ehich are constatntly updated and accessed by NMS.

NMS Architecture Diagram:


Management Console
Network Management Software
Network Management Databases
Network Management Databases
Network Management Databases
Management Data Collection via Network Management Protocol
Network Management Data Storage and Processing Systems
Managed Device
Management Agent
Local Management Data Collection
Proxy Management Device
Monitoring Interfaces
Unmanageable Device
Out of Band Interface Connection