CN 201.3 - Computer Networks

Network Management

Madusanka Mithrananda

Lecturer

Department of Network and Security

What We Discuss

- Network Management
- Network Management Functional Areas
- Tools used in Network Management
- Network Mgt Protocols

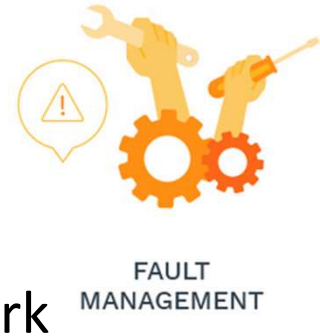
Network Management

- Network management refers to two related concepts. First is the process of configuring, monitoring, and managing the performance of a network. Second is the platform that IT and NetOps teams use to complete these ongoing tasks(Cisco,2024).
- Network management
  - ensure that enterprises run efficiently and effectively end to end.
  - is the process of controlling a complex data network to maximize its efficiency and productivity.
- The overall goal of network management is to help with the complexity of a data network and to ensure that data can go across it with maximum efficiency and transparency to the users.

Network Management

- The International Organization for Standardization (ISO) Network Management Forum divided network management into five functional areas:
  - Fault Management
  - Configuration Management
  - Security Management
  - Performance Management
  - Accounting Management

Fault Management



- The process of locating problems, or faults, on the data network
- Fault management applies a combination of technology and processes to detect, repair and document errors that could interfere with network operations.
- It involves the following steps:
  - Identification of the problem
  - Isolate the problem
  - Resolution
- This includes tools for monitoring network devices, identifying errors, and troubleshooting issues.

Configuration Management

- Adding, deleting, and modifying network device configurations.
- This ensures consistency and simplifies network management tasks.
- The configuration of certain network devices controls the behavior of the data network.

Configuration Management

- Configuration management improves network maintenance and helps keep track of connected devices, device configurations and device connections.
  - Reduce downtimes
- With configuration management, network teams can achieve three goals:
  - Maintain accurate configuration records
  - Enable efficient network scans
  - Enable network automation capabilities.

Performance Management

PERFORMANCE MANAGEMENT

- Aims to ensure acceptable service levels in the network to support optimal business operations
- Involves measuring the performance of the network hardware, software, and media
- A big component of performance management is collecting statistics on network service quality on an ongoing and consistent basis.
- Examples of measured activities are:
  - Overall throughput
  - Percentage utilization
  - Error rates
  - Response time

Security Management

- Implementing and maintaining network security measures to protect against unauthorized access, data breaches, and other threats.

Security Management

- Functions that fall under the security management umbrella include
  - Network authentication
  - Authorization
  - Auditing
- Most security management services incorporate foundational capabilities, such as network firewall configuration and management, vulnerability management, intrusion detection systems and unified threat management.
  - Organizations can use these to set and execute on policies.

Accounting Management

- Involves tracking individual's utilization and grouping of network resources to ensure that users have sufficient resources.
  - All businesses and government entities need to track utilization.
- Involves granting or removing permission for access to the network.
  - This information is essential for cost management.
  - It can also be important to recognize trends that indicate inefficiencies that might be caused by a configuration issue or some other error.
    - For larger enterprises, documenting which units and users are consuming bandwidth is crucial to justify the relevance of the network to business operations. IT is typically seen as a cost center, so this type of network management is vital, especially since IT is often under the aegis of the CFO.

Network Management Protocols

- A simple protocol defines common data formats and parameters and allows for easy retrieval of information
- A complex protocol adds some change capability and security
- An advanced protocol remotely executes network management tasks, is independent of the network protocol layer

Network Management Protocols

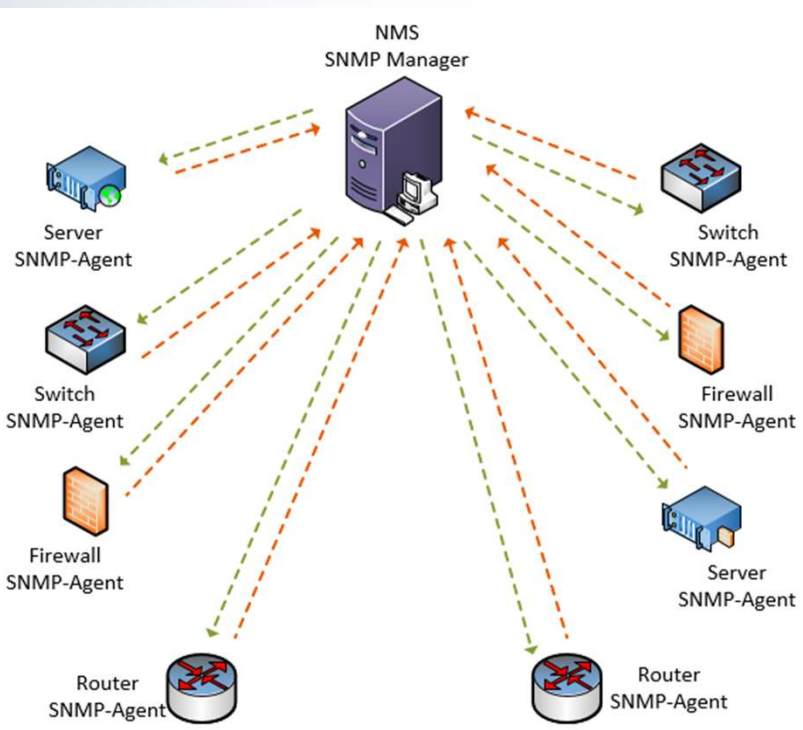
- **Simple Network Management Protocol (SNMP):** An open standard protocol that queries each network element and sends responses to the system for analysis.
- **Internet Control Message Protocol (ICMP):** A TCP/IP network layer that provides troubleshooting, control and error message services.
- **Streaming telemetry:** A protocol that transmits key performance indicators from network devices to the system in real-time.

Managed Devices

- A *managed device* is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information.
- Managed devices exchange node-specific information with the NMSs.
  - Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, cable modems, bridges, IP telephones, IP video cameras, computer hosts, and printers.

Agent and NMS

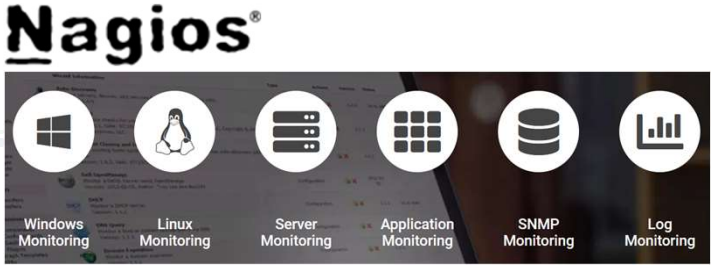
- An *agent* is a network-management software module that resides on a managed device.
  - An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.
- A *network management station* (NMS) executes applications that monitor and control managed devices.
  - NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.



Network Management Data Collection

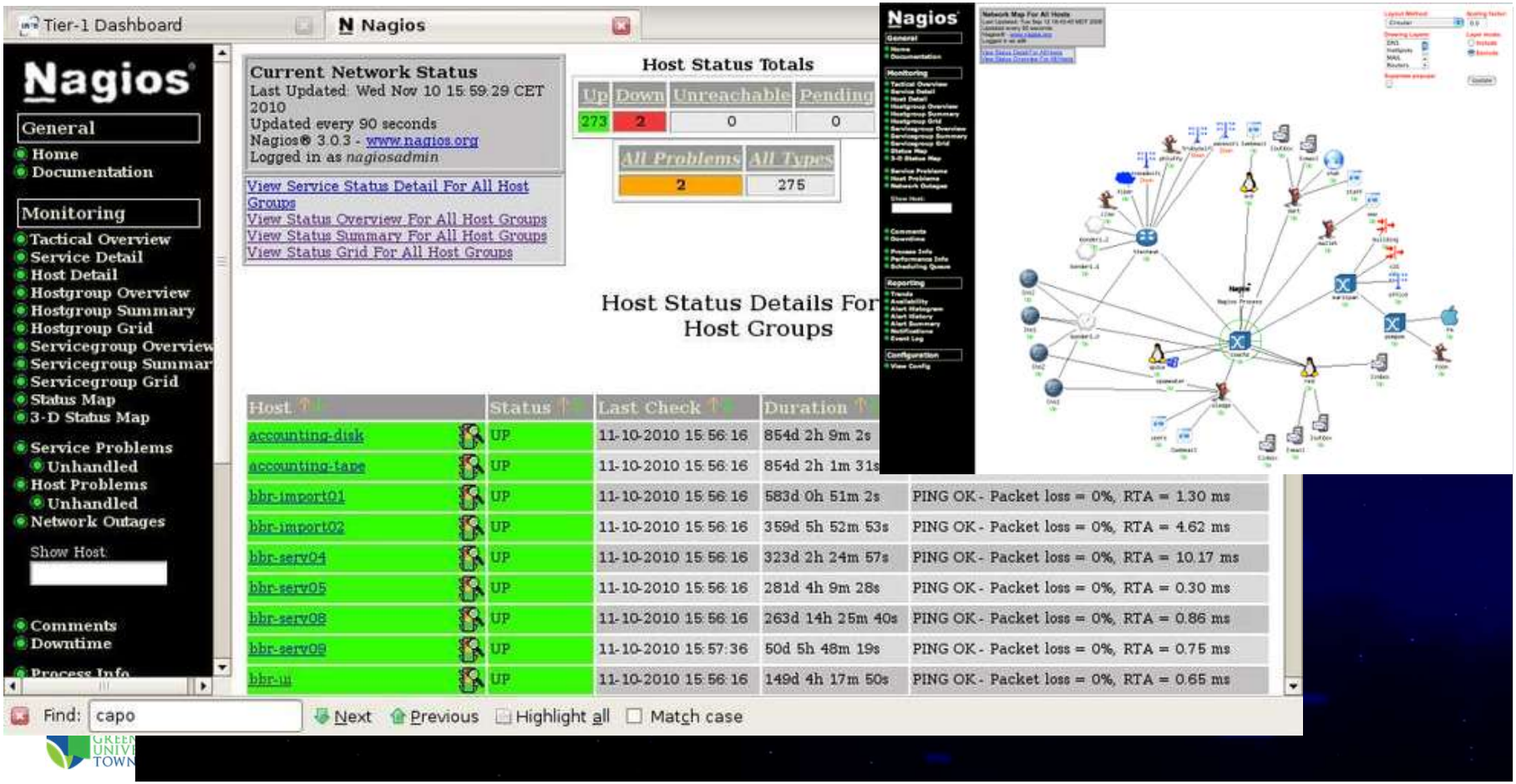
Data Category	Description	Examples	Data Source
Device and Configuration Data	Information about network devices and their configurations	- Inventory Data: Device type (router, switch, firewall), model, vendor, serial number, location - Configuration Data: Routing protocols, security settings (passwords, access control lists), VLAN configurations	- Network devices themselves (through SNMP or CLI)
Performance and Traffic Data	Data related to network traffic flow and performance	- Traffic Flow Data: Source and destination IP addresses, protocols used (TCP, UDP), port numbers, packet size - Performance Metrics: Bandwidth utilization, latency, packet loss, jitter	- Network monitoring tools, switches, routers (through SNMP or NetFlow)
Event and Log Data	Information about network events and device logs	- Syslog Messages: Errors, warnings, security breaches, device status changes - SNMP Traps: Real-time notifications for critical events - Application-Specific Logs: Information relevant to network performance or security from specific applications	- Network devices (Syslog messages, SNMP traps), applications themsevles
Additional Data Sources	Data collected by specialized tools for deeper network insights	- Network Monitoring Tools: Application performance metrics, user experience monitoring, network topology maps - Flow Analyzers: Traffic flow analysis to identify bandwidth hogs, potential security threats, and application usage patterns	- Network monitoring tools, flow analyzers (use data from network devices and traffic)

Some of the Tools used in the Industry



- Nagios
  - Currently the most widely implemented Open Source Network Management Solution Based on Linux
  - Provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure.
  - Hundreds of third-party addons provide for monitoring of virtually all in-house applications, services, and systems.
    - Pros: Free Open-Source Solution, very powerful agents
    - Cons: steep learning curve, devices and tests need to be managed via config files.

Nagios


Tier-1 Dashboard
Nagios
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summar
Servicegroup Grid
Status Map
3-D Status Map
Service Problems
Unhandled
Host Problems
Unhandled
Network Outages
Show Host
Comments
Downtime
Process Info
Current Network Status
Last Updated: Wed Nov 10 15:59:29 CET 2010
Updated every 90 seconds
Nagios® 3.0.3 - www.nagios.org
Logged in as nagiosadmin
View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups
Host Status Totals
Up
Down
Unreachable
Pending
273
2
0
0
All Problems
All Types
2
275
Host Status Details For
Host Groups
Host
Status
Last Check
Duration
accounting-disk UP 11-10-2010 15:56:16 854d 2h 9m 2s
accounting-tape UP 11-10-2010 15:56:16 854d 2h 1m 31s
bbr-import01 UP 11-10-2010 15:56:16 583d 0h 51m 2s PING OK - Packet loss = 0%, RTA = 1.30 ms
bbr-import02 UP 11-10-2010 15:56:16 359d 5h 52m 53s PING OK - Packet loss = 0%, RTA = 4.62 ms
bbr-serv04 UP 11-10-2010 15:56:16 323d 2h 24m 57s PING OK - Packet loss = 0%, RTA = 10.17 ms
bbr-serv05 UP 11-10-2010 15:56:16 281d 4h 9m 28s PING OK - Packet loss = 0%, RTA = 0.30 ms
bbr-serv08 UP 11-10-2010 15:56:16 263d 14h 25m 40s PING OK - Packet loss = 0%, RTA = 0.86 ms
bbr-serv09 UP 11-10-2010 15:57:36 50d 5h 48m 19s PING OK - Packet loss = 0%, RTA = 0.75 ms
bbr-ui UP 11-10-2010 15:56:16 149d 4h 17m 50s PING OK - Packet loss = 0%, RTA = 0.65 ms
Find: capo
Next
Previous
Highlight all
Match case

Cacti

- Cacti is an open-source, web-based network monitoring and graphing tool designed as a front-end application for the open-source, industry-standard data logging tool RRDtool.
- Cacti allows a user to poll services at predetermined intervals and graph the resulting data.

Developer(s): The Cacti Group, Inc

Initial release: September 23, 2001; 20 years ago

License: GNU General Public License

Stable release: 1.2.20 / 6 April 2022; 25 days ago

Programming language: PHP

Extra Reading

- https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-management.html
- https://www.ibm.com/topics/network-management