Webinar on Network Monitoring and Management System

Date: 16-18 April 2021

Md. Mahedi Hasan

Network Engineer, University of Dhaka

cse.mahedi@gmail.com | www.Mahedi.me

/in/mahedicse/ | /mahedi.cse

Learning Objective

Day-1:

- Network Operation Center (NOC)
- Network Monitoring and Management System (NMS)
- Useful Tools are Using for NMS
- Agent based and Agent less tools
- SNMP, and its different version of SNMP
- Virtualization and Linux Basic
- Server Lab Setup with VirtualBox/VMware Workstation
- Virtual Server Installation and Networking (CentOS-8)

Network Operation Center (NOC)

Network Operation Center (NOC)

- A Network Operations Center, often called a NOC (pronounced "knock")
- Is typically a centralized location where the network operation staff provides 24x7x365 supervision, monitoring, and management of the network, servers, databases, firewalls, devices and related external services.
- This infrastructure environment may be located on-premises and/or with a cloud-based provider
- Network Operations refers to the activities performed by internal networking staff or third parties that companies and service providers rely on to monitor, manage, and respond to alerts on their network's availability and performance
- Staff that have primary responsibilities for network operations are often called Network Operations Executive (NOC Executive) or Network Operations Engineer (NOC Engineer)

Key Network Operation Activities Are:

- Network monitoring
- Incident response
- Communications management (Email, Voice and Text)
- Performance, quality, and optimization reporting
- Software/firmware installation, troubleshooting
- Patch management
- Backup management and Monitoring
- Firewall management and Monitoring

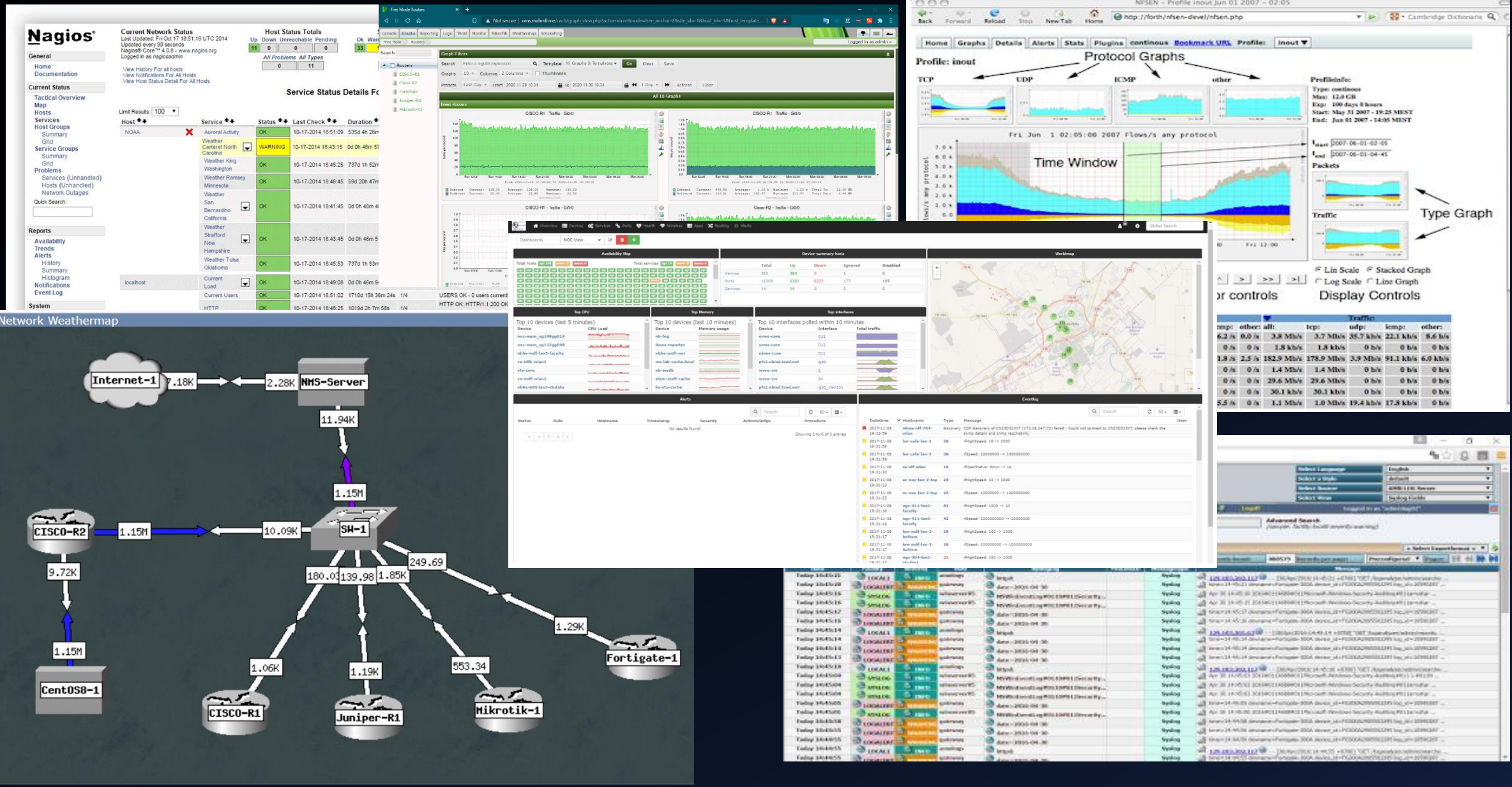
Key Network Operation Challenges:

- Lack of collaboration/coordination across teams
- Troubleshooting is time consuming because it often involves correlating data across multiple devices and tool sets and requires manual processes to arrive at sound diagnoses
- Many disparate tools from different vendors in use that may require staff work with different technologies, low-level utilities and Command Line Interfaces (CLI)
- Problems arise and then disappear by the time all information is collected that is necessary for troubleshooting
- Escalation to more senior staff is required frequently to assess root causes

Network Operations Best Practices

- Continuously monitoring a wide variety of information and network systems that include communications circuits, cloud resources, LAN/WAN systems, routers, switches, firewalls and applications.
- Providing timely response to all incidents, outages and performance issues.
- Categorizing issues for escalation to appropriate technical teams.
- Recognizing, identifying and prioritizing incidents in accordance with customer business requirements, organizational policies and operational impact.
- Collecting and reviewing performance reports for various systems, and reporting trends in performance to senior technical personnel to help them predict future issues or outages.
- Documenting all actions in accordance with standard company policies and procedures.
- Notifying customer and third-party service providers of issues, outages and remediation status.
- Working with internal and external technical and service teams to create and update knowledge base articles.
- Performing basic systems testing and operational tasks (installation of patches, network connectivity testing, script execution, etc.).
- Supporting multiple technical teams in 24x7 operational environments with high uptime requirements.

Network Monitoring and Management System (NMS)



Network Monitoring & Management

- Monitoring:
  - Check the status of a network
    - Systems/Devices
      - Routers
      - Switches
      - Servers
      - UPS etc.
    - Services/Applications
      - DNS
      - Web/HTTP
      - Mail/SMTP
      - Databases etc.
- Management:
  - Processes for successfully operating a network

Why do we Monitor?

- Are Systems and Services Reachable?
- Are they Available?
- What's their Utilisation?
- What's their Performance
  - Round-trip times, throughout
  - Faults and Outages
- Are they under Attack?

Why do we Monitor?

- Know when there are problems – before our customers!
- Track resource utilisation, and bill our customers
- To Deliver on Service Level Agreements (SLAs)
  - What does management expect?
  - What do customers expect?
  - What does the rest of the Internet expect?
- To prove what we're delivering
  - Have we achieved Five Nines? 99.999%
- To ensure we meet SLAs in the future

Uptime Expectations

- What does it take to deliver 99.9 % uptime?
  - 30.5 x 24 = 732 hours a month
  - (732 - (732 x .999)) x 60 = 43.92 minutes
  - only 45 minutes of downtime a month!
- Need to shut down one hour a week?
  - That's only 99.4% uptime ((732-4)/732 = .9945355...)
- Maintenance might be negotiated in SLAs
- What does it mean that the network is up?
  - Does it work at every location? Every host?
  - Should the network be reachable from the Internet?
- Site to calculate: https://uptime.is/

$$Availability\ \% = \frac{(Agreed\ service\ time - Downtime)}{Agreed\ service\ time}$$

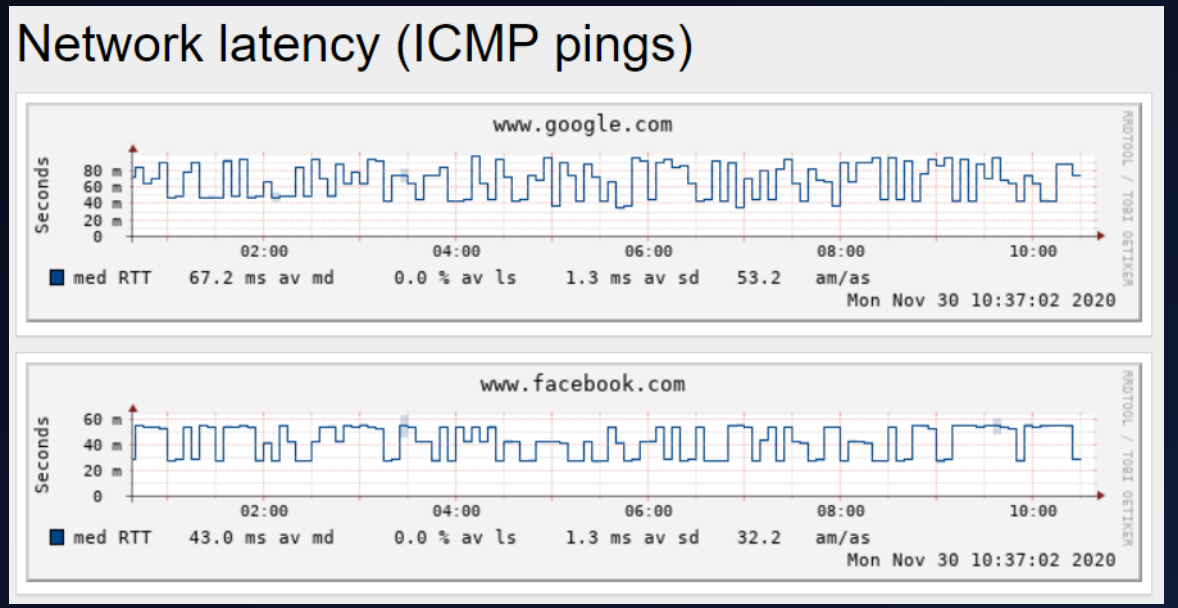
Availability percentages vs service downtime

Availability %	Downtime per year	Downtime per month	Downtime per week
90% (one nine)	36.5 days	72 hours	16.8 hours
99% (two nines)	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.9% (three nines)	8.76 hours	43.8 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% (four nines)	52.56 minutes	4.32 minutes	1.01 minutes
99.999% (five nines)	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% (six nines)	31.5 seconds	2.59 seconds	0.605 seconds
99.99999% (seven nines)	3.15 seconds	0.259 seconds	0.0605 seconds

Source:

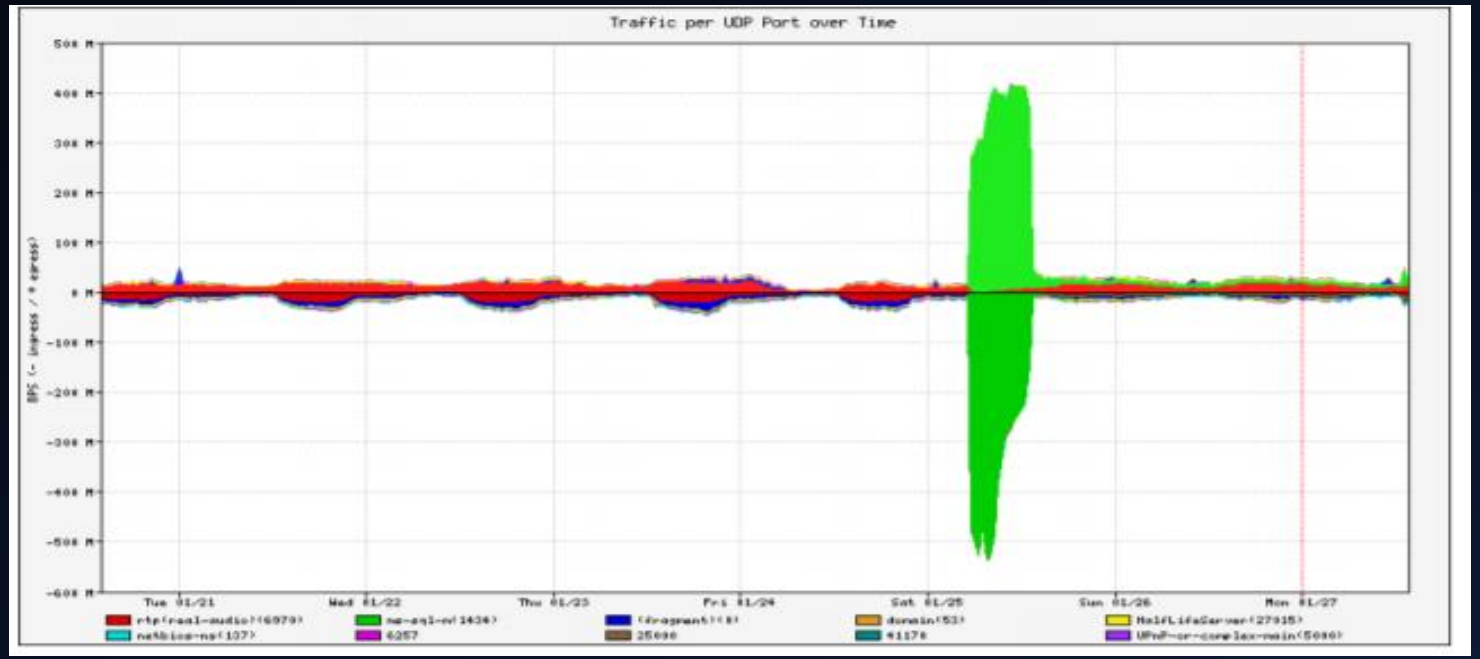
Establishing a Baseline

- Monitoring can be used to Establish a Baseline
- Baseline = What's normal for your network?
  - Typical latency across paths
  - Jitter across paths
  - Load on links
  - Percent Resource Utilisation
  - Typical amounts of noise
- Network scans & random attacks from the Internet
- Dropped packets
- Reported errors or failures



Detecting Attacks

- Deviation from baseline can mean an attack
- Are there more flows than usual?
- Is the load higher on some servers or services?
- Have there been multiple service failures?
- These things could mean an attack

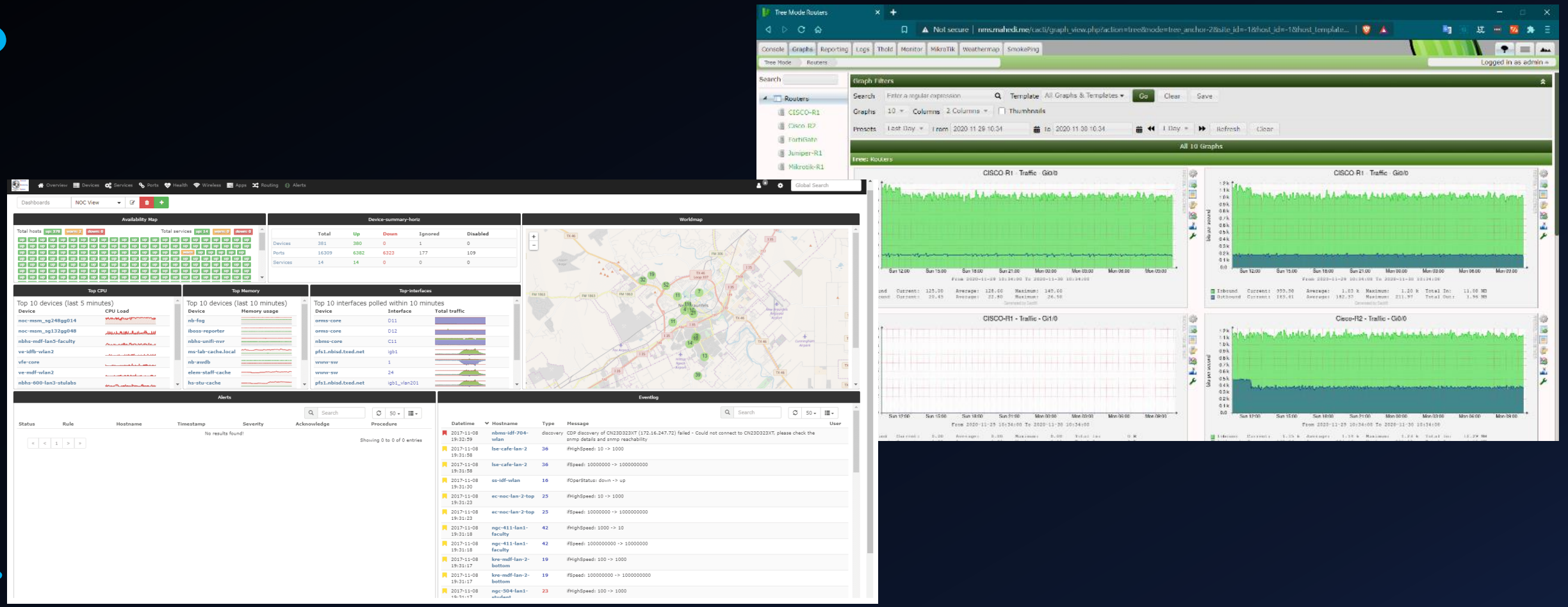


Why do we Manage?

- To ensure we meet business requirements for service level, incident response times etc
- To make efficient use of our resources (including staff)
- To learn from problems and make improvements to reduce future problems
- To plan for upgrades, and make purchasing decisions with sufficient lead time

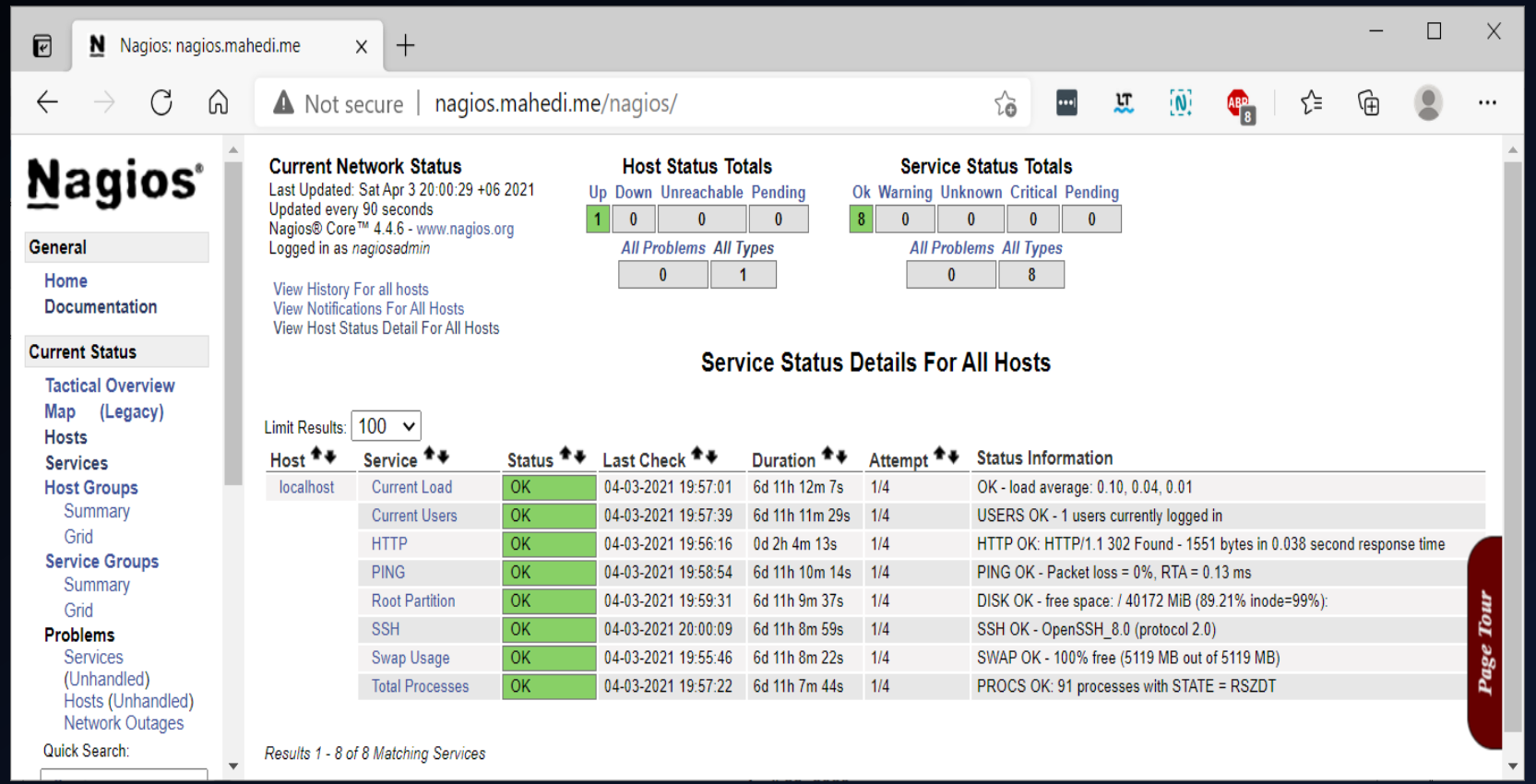
Useful Monitoring Tools

- Performance: Cacti, LibreNMS
  - Traffic, port utilisation, CPU, RAM, Disk, Processes



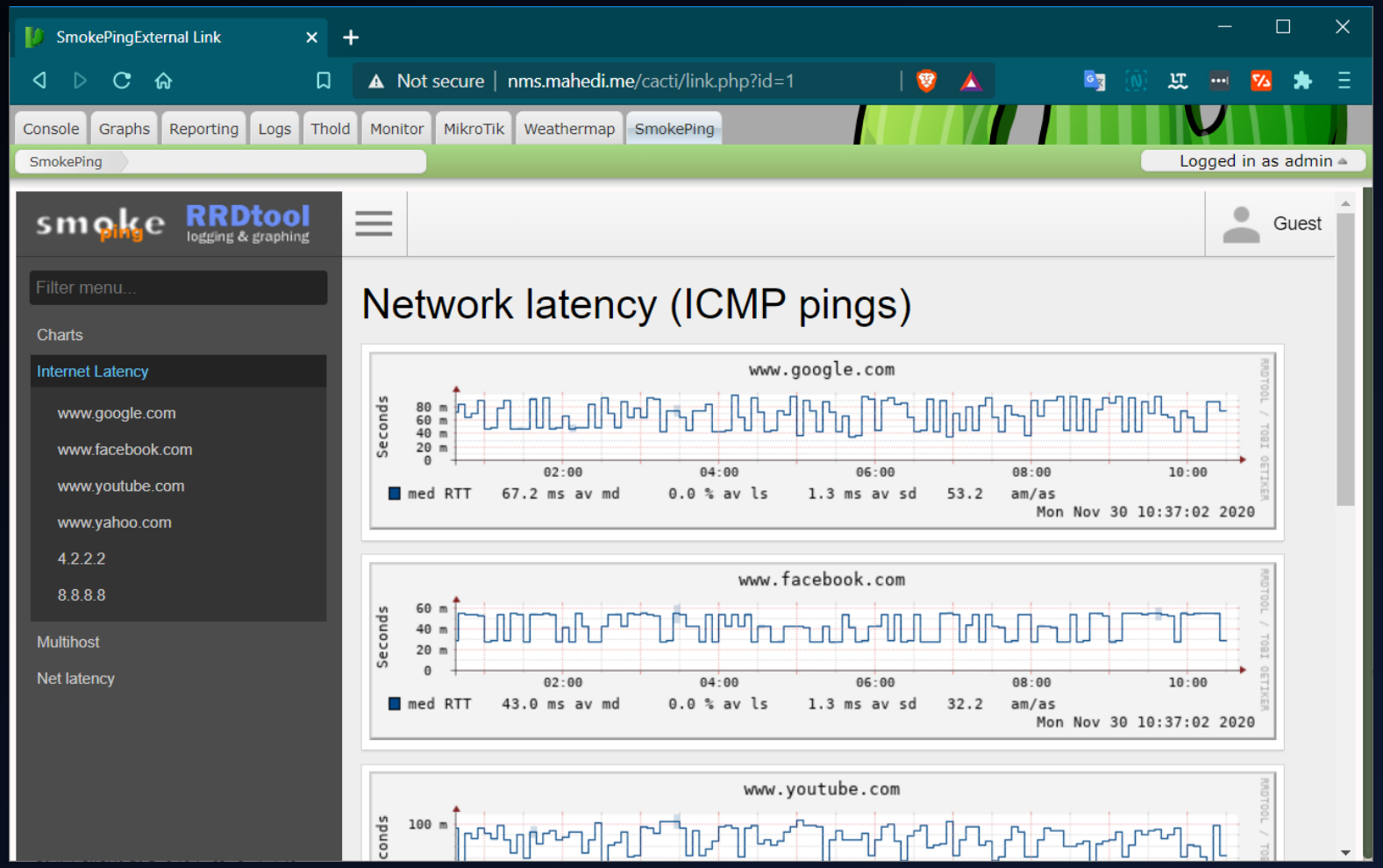
Useful Monitoring Tools

- Availability: Nagios
  - servers, services, routers, switches, environment



Useful Monitoring Tools

- Reliability: Smokeping
  - Connection health, rtt, service response time, jitter



Useful Monitoring Tools

- Traffic Analysis: Netflow, nfsen
  - Capture and analyse from gateway devices

Useful Monitoring Tools

- Ticket Systems: RT, OTRS, Trac
  - Manage provisioning & support
- Configuration Management: RANCID
  - Track router configurations
- Network Documentation:
  - Inventory, Location, Ownership of Network Assets

Agent-based Vs Agentless tools

Agent-Based	Agentless
1. Required to install Clients/Agent in every node to monitor	1. No Clients/Agent required to install in nodes
2. Many devices doesn't support to install Clients/Agent	2. Standard protocol use for all tools
3. Provide broader & deeper monitoring beyond what agentless can monitor e.g. richer info than SNMP, CIM, WMI etc. API.	3. Lower maintenance cost (no agent version update / upgrade etc.).
4. Network bandwidth efficiency - data is collected in local node & filter by agent before processed results are forwarded to centralized console	4. Suitable for large nodes deployment.
5. Better security - agent push data to central component instead of letting monitored node for direct remote collection.	5. Less resource usage e.g. CPU in the local node.

Simple Network Management Protocol (SNMP)

- The Simple Network Management Protocol (SNMP) is an Internet Standard protocol defined by the Internet Architecture Board in RFC1157.
- SNMP is used to exchange management information between network devices.
- It is one of the most common protocols used for network management.
- SNMP is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite as defined by the Internet Engineering Task Force
- SNMP generally uses User Datagram Protocol (UDP) port number 161/162.
- Organizations use SNMP to monitor and manage devices on a local area network (LAN) or wide area network (WAN).
- Most network devices in the market come bundled with SNMP agents
- Currently, there are three major versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3

Components of SNMP

- SNMP manager
  - The SNMP manager is the central system used to monitor the SNMP network. Also known as a network management station (NMS)
  - An SNMP manager is responsible for communicating with the SNMP-agent-implemented network devices.
  - It runs on a host on the network. The manager queries the agents, gets responses, sets variables in them, and acknowledges events from them.
- Managed devices
  - A managed device is an SNMP-enabled network entity that is managed by the SNMP manager. These are usually routers, switches, printers, or wireless devices.
- SNMP agent
  - An SNMP agent is a software process that responds to SNMP queries to provide status and statistics about a network node.
  - SNMP agents play the most important role in management.
  - They are locally located and associated with SNMP network devices from which they collect, store, and transmit monitoring data.
  - Data is transmitted to the designated SNMP manager when queried.

Components of SNMP

- SNMP MIB
  - A management information base (MIB) forms an integral part of network management models.
  - An SNMP MIB is a structure that defines the format of information exchange in an SNMP system. Every SNMP agent maintains an information database describing the parameters of the device it manages.
  - SNMP managers store collected data in a MIB as a commonly shared database between the agent and the manager.
  - MIBs are saved as a text file in a specific format that MIB editors, SNMP agent builders, network management tools, and network simulation tools can understand, facilitating network building, testing, deployment, and operations.
  - The managed objects in an MIB are called object identifiers (object IDs or OIDs).
- SNMP OID
  - Object Identifiers (OIDs) are identifiable by strings of numbers separated by dots. There are two types of managed objects:
  - Scalar: Objects defined by a single object instance (i.e. there can only be one result.)
  - Tabular: Objects defined by multiple related object instances that are grouped in MIB tables.

SNMP, and its different versions

- **SNMPv1:**
  - SNMPv1 is the first version of SNMP. It's easy to set up, as it only requires a plain text community.
  - Although it accomplished its goal of being an open, standard protocol, it was found to be lacking in key areas for certain managing applications.
  - For example, it only supports 32-bit counters and has poor security features - a community string is the only security method in the SNMPv1.

SNMP, and its different versions

- SNMPv2c:
  - Designed in 1993, SNMPv2c (where c stands for community) is a sub-version of SNMPv2.
  - SNMPv2c's key advantage over previous versions is the Inform command. Unlike Traps, which are simply received by a manager, Informs are positively acknowledged with a response message. If a manager does not reply to an Inform, the SNMP agent will resend the Inform.
    - Other advantages include:
    - Improved error handling
    - Improved SET commands
  - SNMPv2 security, just like for SNMPv1, comes into the form of community strings.
  - This is a password that your devices will need to able allowed to talk to each other and transfer information when SNMP requests occur

SNMP, and its different versions

- SNMPv3:
  - SNMPv3 is the newest version of SNMP. Its management framework features primarily involve enhanced security.
  - The SNMPv3 architecture introduces the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control.
  - SNMPv3 supports the SNMP "Engine ID" Identifier, which uniquely identifies each SNMP entity. Conflicts can occur if two entities have duplicate EngineID's.
  - The EngineID is used to generate the key for authenticated messages.
  - SNMP v3 security models come primarily in 2 forms: authentication and encrypting.
  - Authentication:
    - Authentication is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the EngineID of the entity. The key is shared with the intended recipient and used to receive the message.
  - Encrypting
    - Privacy encrypts the payload of the SNMP message to ensure that it cannot be read by unauthorized users. Any intercepted traps will be filled with garbled characters and will be unreadable. Privacy is especially useful in applications where SNMP messages must be routed over the Internet.
  - The SNMPv3 protocol also facilitates the remote configuration of the SNMP agents

References

- https://en.wikipedia.org/wiki/Network_monitoring
- https://www.thousandeyes.com/learning/techtorials/network-operations
- https://workshops.renu.ac.ug/2018/renu-bugema-cnmm/netmgmt/en/welcome-intro/network-management.pdf
- https://www.site24x7.com/network/what-is-snmp.html

Thank You

?