Networking

Networking Operations

3.1.1 Performance Metrics

What are some performance measures for networks?

Overview

Given a scenario, the student will use the appropriate statistics and sensors to ensure network availability.

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CYBER.ORG

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 3.1

- Given a scenario, use the appropriate statistics and sensors to ensure network availability.
    - Performance metrics/sensors
        - Device/chassis
            - Temperature
            - Central processing unit (CPU) usage
            - Memory
        - Network metrics
            - Bandwidth
            - Latency
            - Jitter
    - Baselines
    - NetFlow data
    - Uptime/downtime

Performance Metrics

Troubleshooting

When monitoring a network, the first thing we look at is if the network is available or not. Unfortunately, if the network is down, it may be down for a variety of reasons. Some issues may be because of the device itself while others may have to do with the network.

When considering issues caused by the device, three important items to consider are ***temperature***, ***CPU usage***, and ***memory***. If a device gets too hot (or is too cold but minimum temperatures are only a concern in Antarctica, outside), the device will either turn off entirely as a protective measure or may implement techniques such as thermal throttling. Thermal throttling automatically slows down the computer allowing it to cool down. By default, thermal throttling turns on when the CPU reaches a temperature of 90 degrees Celsius. The CPU could also be overwhelmed by too many processes and applications running. We notice this with older computers trying to run current software. Another issue with older hardware trying to run current software would be insufficient memory (RAM). Too important numbers to look at are the size of the RAM, e.g. 4GB, 8GB, 16GB, etc. and the frequency.

Teacher Notes:

Frequencies with DDR4 RAM modules can range from 800Hz to 4200Hz, but many motherboards have a maximum frequency they can handle by default. These components can typically be monitored via software and may include built in sensors to let us know if there are any issues.

With the network itself, three important measures are ***bandwidth***, ***latency***, and ***jitter***. Bandwidth is the maximum transfer throughput capacity of a network, being measured in bits, megabits, or gigabits per second. A common misconception is that bandwidth increases the speed of a network because we increase the amount of data that can be sent at once, not actually increase the speed the data is transmitted. However, if bandwidth is low, this will decrease the amount of data that can be sent at once, "slowing" down the network. Latency is an actual measure of speed, telling us the amount of time it takes for a packet to travel from its source to its destination. The biggest issue with latency is having too many users trying to access a network at once. IT administrators can monitor usage and determine which users are on the network with necessary work-related applications and which users are on the network with non-work-related applications. Finally, jitter is the difference in packet delay. The two main causes of jitter are network congestion and route changes. Most of the time, jitter and latency suffer at the same time because they are caused by the same issues. Correcting one may improve the other as well.

A ***baseline*** is the standard level of performance of a device or network. Baselines are what we expect "normal" to be within the device or network.

SNMP is a powerful tool for managing and troubleshooting a network, but it is also useful to be able to track TCP/IP flows within a network too. This TCP/IP network traffic that is collected is referred to as the NetFlow Data. This is the reason we collect ***NetFlow data*** with an application simply called NetFlow. The NetFlow data is then analyzed to create a picture of network traffic flow and volume.

Uptime/downtime refer to the amount of time a system is up and accessible to end users or down and inaccessible, respectively. When quantifying uptime, we refer to them with names such as four-nine or five-nine, meaning the network is up 99.99% or 99.999% of the time.