Networking

Networking Operations

3.1.3 - Interface Stats and Alert

What are some interface stats that help ensure network availability?

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).

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 3.1

- Given a scenario, use the appropriate statistics and sensors to ensure network availability
    - Interface statistics/status
        - Link state (up/down)
        - Speed/Duplex
        - Send/receive traffic
        - Cyclic redundancy checks (CRCs)
        - Protocol packet and byte counts
    - Interface errors or alerts
        - CRC errors
        - Giants
        - Runts
        - Encapsulation errors

Interface Stats and Alerts

Interface Statistics/Status

We need to be able to analyze interface statistics to find any problems. There are some important factors to consider when doing so. Usually, the most important metric on an interface is its ***link state***. Simply put, is it up or down? The first thing we should check if our network management tools alert us of a link error is the link status.

We can determine the status on a router or switch with the command "show run." Typically, ***duplex*** and ***speed*** are set to auto and will be displayed when running that command. Most modern switched networks are full-duplex, meaning devices can send and receive communication at the same time. This doubles the throughput effectively doubling the speed of the network.

Occasionally, we will want to check how well traffic is flowing into and out of a device, regardless of type. "Show run" also displays this information. We could also use the command "sh int s0/0" to see the rate of input and output.

Teacher Notes:

The next factor, ***cyclic redundancy checks (CRCs)*** is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. When CRC errors occur, something has corrupted the received packet.

Finally, the "show run" command also displays the number of packets received from protocols and the number of bytes received.

Interface Errors or Alerts

As said above, CRC errors tell us packets have been damaged. This could be caused by a faulty port or bad ethernet cable, both relatively easy fixes. Other possibilities include a duplex mismatch, collisions, or a station transmitting bad data.

Giants are packets that are discarded because they exceed the maximum packet size allowed. Ethernet packets greater than 1518 bytes are considered giants. ***Runts***, as the name implies, are packets that are discarded because they do not meet the minimum packet size allowed. A malfunctioning NIC may places frames on a network that are too short or too long. If we use a cable that is too long, rather than getting giants or runts, we could get late collisions.

Finally, a failed ***encapsulation error*** message indicates that the router has a layer 3 packet it is trying to forward but is missing some element from the layer 2 header that is needed for forwarding the packet to the next hop. If we look at the router logs, this will be clearly displayed as "encapsulation failed."