Introduction

4.0.1

Why should I take this module?

Welcome to ACL Concepts!

You have arrived at your grandparents' residence. It is a beautiful gated community with walking paths and gardens. For the residents safety, no one is permitted to get into the community without stopping at the gate and presenting the guard with identification. You provide your ID and the guard verifies that you are expected as a visitor. He documents your information and lifts the gate. Imagine if the guard had to do this for the many staff members that entered each day. They have simplified this process by assigning a badge for each employee to automatically raise the gate once the badge is scanned. You greet your grandparents who are anxiously awaiting you at the front desk. You all get back into the car to go down the street for dinner. As you exit the parking lot, you must again stop and show your identification so that the guard will lift the gate. Rules have been put in place for all incoming and outgoing traffic.

Much like the guard in the gated community, network traffic passing through an interface configured with an access control list (ACL) has permitted and denied traffic. The router compares the information within the packet against each ACE, in sequential order, to determine if the packet matches one of the ACEs. This process is called packet filtering. Let's learn more!

4.0.2

What will I learn to do in this module?

Module Title: ACL Concepts

Module Objective: Explain how ACLs are used as part of a network security policy.

Topic Title	Topic Objective
Purpose of ACLs	Explain how ACLs filter traffic.
Wildcard Masks in ACLs	Explain how ACLs use wildcard masks.
Guidelines for ACL Creation	Explain how to create ACLs.
Types of IPv4 ACLs	Compare standard and extended IPv4 ACLs.