Introduction

5.0.1

Why should I take this module?

Welcome to ACLs for IPv4 Configuration!

In the gated community where your grandparents live, there are rules for who can enter and leave the premises. The guard will not raise the gate to let you in to the community until someone confirms that you are on an approved visitor list. 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. How do you configure these ACLs? How do you modify them if they are not working correctly or if they require other changes? How do ACLs provide secure remote administrative access? Get started with this module to learn more!

5.0.2

What will I learn to do in this module?

Module Title: ACLs for IPv4 Configuration

Module Objective: Implement IPv4 ACLs to filter traffic and secure administrative access.

Topic Title	Topic Objective
Configure Standard IPv4 ACLs	Configure standard IPv4 ACLs to filter traffic to meet networking requirements.
Modify IPv4 ACLs	Use sequence numbers to edit existing standard IPv4 ACLs.
Secure VTY Ports with a Standard IPv4 ACL	Configure a standard ACL to secure VTY access.
Configure Extended IPv4 ACLs	Configure extended IPv4 ACLs to filter traffic according to networking requirements.

4.5
Module Practice and Quiz

5.1
Configure Standard IPv4 ACLs