Filename: cisco-ccna200301-5-3-1-security_password_policy_components
ShowName: Cisco CCNA (200-301)
Topic: 5.0 Security Fundamentals
EpisodeName: Security Password Policies Components
Description: In this episode, Aubri and Ronnie review the basics of establishing a security password policy. The duo, show the basics of management including what to do when the password to a device is lost using password-recovery. They discuss complexity requirements and alternatives.

Security Password Policy Components

- 5.4 Describe security password policies elements
    - Management
        - How are passwords managed on Cisco Devices?
            - enable password
            - Username/password database
            - Line console password
            - line vty password
        - Locally stored on router in startup-config
        - Can use Remote Authentication
            - RADIUS/TACACS+
        -
          ```
          password-recovery 0x2142
          ```
    - Complexity
        - Passwords should not be easy
        - Should involve level of complexity
            - No names, dates, sequence of numbers
            - Should include alphabetic, numbers, special characters
            - Min of 8 characters
            - e.g. NOT: Password1. but P4t@2B9$7VJb%xYt
        -
          ```
          NYEDGE1#
          NYEDGE1#show passwords configuration
          NYEDGE1#configure terminal
          NYEDGE1(config)#security password min length 8
          NYEDGE1#show passwords configuration
          ```
    - Password Alternatives
        - multifactor authentication (2 of 3)
            - Something you know (PIN, Pattern or Password)
            - Something you have (e.g. Yubikey)
            - Something you are
                - biometrics (Fingerprint, FaceID, Iris ID)
        - certificates (digital)
            - `crypto key generate rsa`