1. **Device Access and Privilege Levels:**
   * Secure access using SSH for remote access.
   * User executive mode (level 1) and privileged executive mode (level 15).
   * Intermediate levels can be set, e.g., level 2 for specific commands.
2. **Role-Based CLI Access:**
   * Different views for different user roles.
   * Superviews combine multiple views.
   * Root view includes all system commands.
3. **Cisco IOS Resilient Configuration Feature:**
   * Allows faster recovery if flash memory is reformatted or startup configuration file is erased.
   * Secures both IOS in flash and configuration file in NVRAM.
   * The combination of secured IOS and configuration files is called a Primary Bootset.
4. **Using Hash Functions to Protect Transmitted Data:**
   * Protect routing protocol messages (e.g., OSPF) and timing synchronization messages (e.g., NTP) using hash functions.
   * Use keys and passwords for message authentication.
5. **Securing Dynamic Routing Protocols:**
   * Automatically learn about networks and select the best path.
   * Prevent routing protocol spoofing by using MD5 or SHA for message authentication.
6. **Fault Logging and Syslog:**
   * Cisco IOS uses Syslog for fault logging.
   * Severity levels range from 0 (emergency) to 7 (debug).
   * Log messages can be displayed on the console, monitor, buffered in RAM, or sent to a Syslog server.
7. **Time Stamping Alarms:**
   * Ensure timestamps are sent with alarms using service timestamps log datetime.
8. **Network Time Protocol (NTP):**
   * Synchronizes device clocks to ensure consistent timestamps.
   * Hierarchical structure with atomic clocks as Stratum 0.
9. **Securing NTP with a Hash Function:**
   * Use a hash function (e.g., MD5) to secure NTP information.
   * Configure keys and passwords for authentication.
10. **Cisco Discovery Protocol (CDP):**
    * Enables Cisco devices to communicate and learn details about neighbouring devices.
    * View neighbours using show cdp neighbours detail.
11. **Link Layer Discovery Protocol (LLDP):**
    * A standard protocol similar to CDP, used for non-Cisco devices.
    * Turn off CDP, LLDP, and routing protocols on links connected to the Internet.
12. **Simple Network Management Protocol (SNMP):**
    * Monitors and manages network devices using a standardized database of variables (MIB).
    * SNMPv3 provides message integrity, encryption, and access control.
13. **SNMPv3 Security Configuration Example:**
    * **Step 1: Configure an ACL.**

**ip access-list standard PERMIT-ADMIN**

**permit 192.168.1.0 0.0.0.255**

* + **Step 2: Define an SNMP view.**

**snmp-server view SNMP-RO iso included**

* + **Step 3: Configure an SNMP group.**

**snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN**

* + **Step 4: Configure an SNMP user.**

**snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128** **cisco54321**

1. **Storing IOS and Configurations on Servers:**
   * Store copies of IOS and configurations on a separate server using FTP or TFTP.
   * Use SCP or SFTP for secure transfers.
2. **Verifying IOS Code Integrity with MD5:**
   * Verify the integrity of the IOS file using the MD5 hash.
3. **Cisco Password Recovery:**
   * Use a password recovery procedure to access the router if you forget the password.
   * Change the Config Register and reload the router.

# Combined Packet Tracer Commands Example

1. **Enable AAA Globally and Configure Servers:**

**Router(config)#** **aaa new-model**

**Router(config)#** **tacacs-server host 192.168.1.101**

**Router(config)#** **tacacs-server key TACACS-Pa55w0rd**

**Router(config)#** **radius-server host 192.168.1.100**

**Router(config)#** **radius-server key RADIUS-Pa55w0rd**

1. **Configure Authentication:**

**Router(config)#** **aaa authentication login default group tacacs+ group radius local-case**

**Router(config)#** **aaa local authentication attempts max-fail 3**

1. **Add Usernames and Passwords:**

**Router(config)#** **username John password Sexton**

**Router(config)#** **username admin secret adminpass**

1. **Configure Console and VTY Lines:**

**Router(config)#** **line console 0**

**Router(config-line)#** **login authentication default**

**Router(config)#** **line vty 0 15**

**Router(config-line)#** **login authentication default**