# AAA Analysis Worksheet

## Instructions

Complete all sections of this worksheet thoughtfully and thoroughly. Use your own words and provide specific examples where appropriate. Each response should demonstrate your understanding of the key concepts from the assigned reading. Citations should be completing in APA format.

### Section 1: Chapter Summaries (30 points)

#### 1.1 Assigning Administrative Roles (Chapter 5) Summary

**Instructions:** Summarize Chapter 5 in your own words. Your summary should cover the main themes, key concepts, and important points discussed in the chapter. Do not copy directly from the text.

**Response:** Chapter 5 covers topics pertaining to:

* privilege levels, i.e. the (0 – 15 levels) which can be switched between using various methods such as creating users or entering the Privileged EXEC mode via the ‘enable’ command.

Additionally, Chapter 5 covers:

* different ‘views’ which can be set up or already exist such as the Root View, CLI View and Superview, the last two can be created via configurations to be accessible with a great deal of customization, especially using role-based privileges.

#### 1.2 Device Monitoring and Management (Chapter 6) Summary

**Instructions:** Summarize Chapter 6 in your own words. Your summary should cover the main themes, key concepts, and important points discussed in the chapter. Do not copy directly from the text.

**Response:** Chapter 6 covers:

* securing boot files using the secure boot image command
* transferring files between computers & networking devices using SCP
* automatically locking down a router using the auto secure command which sets ‘sane’ defaults for your device to help improve the security outlook
* enabling authentication on routing protocols like OSPF
* bringing up topics like In-Band and Out-of-Band management which is a concept describing having internal access only for management or an entirely different infrastructure stack to manage a network avoiding specific complications
* syslog and the different alert levels like Emergency and Informational
* NTP or Network Time Protocol which is how devices determine how to set their clock and the breakdown of Stratums 0 – 16 with a lot of devices getting their time from other devices originating from an authoritative source like a GPS or atomic clock, the chapter also covers how to enable authentication on this protocol to avoid attacks.
* SNMP configuration, including different protocols and standards which slowly increase the usefulness and security of, with SNMPv3 being the latest and best option available. SNMP allows for remote monitoring of network infrastructure, so you can determine if hardware needs to be replaced or if network problems / an attack is occurring by performance metrics

#### 1.3 Authentication, Authorization, and Accounting (Chapter 7) Summary

**Instructions:** Summarize Chapter 7 in your own words. Your summary should cover the main themes, key concepts, and important points discussed in the chapter. Do not copy directly from the text.

**Response:** Chapter 7 covers:

* AAA, or Authentication, Authorization, Accounting which is a framework that can be used to ensure good security practices across and organization.
  + Authentication = who you are
  + Authorization = what can you do
  + Accounting = what have you done
* AAA servers in this chapter refer to TACACS or RADIUS servers which are authoritative sources of truth in an organization, providing the ability to ensure AAA across a large organization.
* Chapter 7 covers how to configure each of these AAA protocols on a cisco device
* Chapter 7 also covers the Cisco ISE which is Cisco’s offering of a AAA server

### Section 2: Learning Reflection (10 points)

#### 2.1 Key Learning

**Instructions:** Discuss something significant you learned from reading Chapters 5, 6, and 7. This could be a concept that was new to you, something that changed your perspective, or information that connected to your personal or professional experience. Provide a thoughtful analysis.

**Response:** I’d say the concept that was newest to me in this chapter was from the authentication on protocols like OSPF and NTP, it’s interesting to learn more about this. It’s quite funny that during this week in another class I’m taking SEC 450 we’re covering why not having OSPF properly authenticated is a bad thing, as we’ve directly attacked the protocol by poisoning OSPF creating routes that are more attractive than other’s allowing us to steal information from unsuspecting users by listening in on conversations we’re not supposed to.

### Section 3: AAA in Practice (30 points)

#### 3.1 Applying Authentication, Authorization, and Accounting

*Instructions:* Select THREE (3) different ways that AAA can be applied in a network environment (for example: multi-factor authentication, role-based access control, centralized logging/accounting). For each one, provide a detailed explanation of how it works and why it is important for maintaining secure and accountable access to systems and data.

**#1:** Centralized logging and accounting through protocols like RADIUS or TACACS+, setting up services like these in an organization allows for a large amount of activity in said organization to be logged and accounted for, providing insight to everyone’s specific activities in an org and the ability to detect malicious activity from insider threats or external threats.

**#2:** Role based access control, this is a methodology of using least privilege throughout an organization, especially when it comes to the abilities that certain accounts have when operating, i.e. being able to configure routers, access network mapped drives, etc. With the overall idea being that if an account were to be compromised that damage could be mitigated since they were not given access to all functions of a network within an organization.

**#3:** Multi-factor authentication, this is where you have people authenticate with a secondary option, either it be a passkey, geolocation or 2FA, it requires that they have multiple means of authentication, ensuring that whoever is attempting to login is genuinely them and not someone impersonating them. It’s even used here at Bellevue College!

### Section 5: Critical Thinking (30 points)

#### 5.1 Real-World Application

*Instructions:* Choose one of the AAA methods you discussed above and research a real-world example where failure to use it properly led to problems (such as a breach or misuse of access). Briefly describe the incident and analyze how AAA practices influenced the outcome.

**Response:** An example of a failure to implement AAA methods as described from these chapters would be the May 2021 Colonial Pipeline ransomware attack, which was a cyberattack against the Colonial Pipeline in Houston Texas which carried gasoline and jet fuel throughout the Southeastern United States. The primary means of attack was through a VPN service which did not use MFA but instead just password credentials which were leaked through another unrelated attack. Because of the lack of configuration regarding AAA policies attackers were able to just login to the remote network and gain full control of the pipeline’s infrastructure, shutting down operations and causing a local emergency in the southeastern United States where gas shortages were common in the following months until the damage could be reversed.

**References**