Here is a **comprehensive, professionally formatted breakdown** of the document titled **“204. Wireless Authentication Notes”**. It is written in a **structured bullet-point study note format**, suitable for **CompTIA A+ 1102 preparation**, and optimized for **clean pasting into Microsoft Word**. Numbered topics provide clarity, with no excessive spacing.

**CompTIA A+ 1102 – Wireless Authentication (Section 204) Professional Study Notes**

**Wireless authentication** is the process of verifying the **identity** of a **user** or **device** attempting to connect to a **wireless** **network**. It ensures that only **authorized users** gain **access** and helps **protect** network resources from unauthorized access or attacks.

**1. Overview of Authentication in Enterprise Networks**

An authenticator is a network device — typically a wireless access point, VPN gateway, or network switch — that serves as a middleman between a user (supplicant) and an authentication server during the login or network access process.

It does not perform authentication itself but rather:

* Collects credentials from the user/device
* Forwards them to an authentication server using a protocol like RADIUS or TACACS+
* Enforces the result (grant or deny access)
* Numerous authentication protocols are used in enterprise networks:  
  ▫ RADIUS  
  ▫ TACACS+  
  ▫ Diameter  
  ▫ LDAP  
  ▫ Kerberos  
  ▫ 802.1X  
  ▫ EAP (and its variants)

**2. RADIUS (Remote Authentication Dial-In User Service) – A network protocol used to authenticate users, authorize services, and account for service usage.**

* **Purpose**: Authenticates, authorizes, and accounts (AAA) for users accessing network services, including dial-up, VPN, and wireless.
* **Centralized administration**: Supports 802.1X and EAP-based authentication.
* **OSI Layer**: Application Layer (Layer 7).
* **Transport Protocol**: Uses **UDP**, making it **faster** but **less reliable** than TCP.

A computer screen with text and a diagram

AI-generated content may be incorrect.

**🔄 2. How It Works (Authentication Flow)**

Here’s a simplified version of the **802.1X authentication model**:

| **Component** | **Role** |
| --- | --- |
| **Supplicant** | The device/user trying to access the network |
| **Authenticator** | The network device (like an AP or switch) that receives the request |
| **Authentication Server** | The backend server (e.g., RADIUS or TACACS+) that checks credentials |

**Step-by-Step:**

1. User connects to a network (e.g., secure Wi-Fi)
2. **Authenticator** receives the login request
3. Authenticator **uses a protocol** (like RADIUS or TACACS+) to send the credentials to the authentication server
4. Server **verifies** credentials and responds with **Accept** or **Reject**
5. Authenticator device allows or blocks access accordingly

Radius and TACACS+ **protocols used by the authentication server** (which is often a dedicated system or service)

**3. TACACS+ (Terminal Access Controller Access Control System Plus) – A proprietary protocol developed by Cisco to provide separate authentication, authorization, and accounting services.**

* **Developer**: Cisco (proprietary protocol).
* **Functionality**: Separates **authentication**, **authorization**, and **accounting**.
* **Transport Protocol**: Uses **TCP**, offering **reliability** and **security**.
* **Advantage**: More **granular access control** than RADIUS.
* **Best Use**: Preferred when using **Cisco devices across the network**.
* Encrypts the **entire packet**, unlike RADIUS which only encrypts the password

| **Feature** | **RADIUS** | **TACACS+** |
| --- | --- | --- |
| Used For | Network access (Wi-Fi, VPN) | Device admin access (CLI/console) |
| Protocol | UDP | TCP |
| Encryption | Password only | Entire packet |
| Vendor Neutral | Yes | Cisco-proprietary |
| Authentication | Combined with authorization | Separated |

**4. Diameter – A peer-to-peer protocol most commonly used in 3g, IP multimedia systems, and LTE 4G cellular networks.**

* **Successor to RADIUS**: Designed for next-gen authentication.
* **Architecture**: Peer-to-peer, not client-server.
* **Use Cases**: Often used in **3G, LTE, and IP multimedia systems**.

**5. LDAP (Lightweight Directory Access Protocol) – A Database that centralizes client and object information on the network.**

* **Purpose**: Stores and manages information about network objects (users, groups, devices).
* **Structure**: Hierarchical, derived from **X.500 directory service**.
  + **Contains a hierarchical organization of users, groups, servers, and systems**.
* **Cross-platform**: Works across different operating systems.
* **Once the authenticator (like a Wi-Fi access point or network switch) receives the user’s credentials, it forwards them to the authentication server using a protocol like RADIUS or TACACS+. That server then queries a directory service — such as LDAP or Active Directory — to verify those credentials.**

**6. Active Directory & Kerberos**

**6.1 Active Directory (AD):** Is going to be used to organize and manage everything including your clients your servers, devices, and your users. Once the user logs into the Windows Domain they can access all the enterprise networks resources using those same credentials as long as they have been given access into those resources based on their role or their group membership.

* **Developer**: Microsoft.
* **SSO System**: Provides **Single Sign-On (SSO)** – authenticate once, access multiple services.
* **Functions**:  
  ▫ Centralized control over users, groups, devices.  
  ▫ Group Policy enables security enforcement.
* **Active directory can be used as part of our enterprise security policies as well, and it allows us to perform access control through its group policy functions**.
* **Authentication and authorization are then going to be performed through the Kerberos system**.

**6.2 Kerberos – Uses symmetric encryption and the Key Distribution Center to conduct authentication and authorization functions.**

**A screen shot of a computer

AI-generated content may be incorrect.**

When the user logs onto the domain, they're going to get a ticket granting ticket or TGT from this key distribution center. This ticket granting ticket is then going to be provided to the domain controller anytime the user wants to access a resource, and then the domain controller is going to provide the user with a service ticket or a session key to use as appropriate for the function they're trying to do. These tickets are going to be presented to the resources, and access will be granted because the resource always trusts the domain controllers provided tickets that were given out to these users.

* **Authentication Protocol**: Used within Active Directory.
* **Mechanism**: Uses **symmetric encryption** and a **Key Distribution Center (KDC)**.
* **Ticketing System**:  
  ▫ User receives a **Ticket Granting Ticket (TGT)** upon login.  
  ▫ TGT used to request **Service Tickets** for network resources.  
  ▫ Resources trust the **domain controller** that issued the tickets.

**7. 802.1X Framework – A standardized framework that is used for port-based authentication on both wired and wireless networks.**

* **Purpose**: Provides **port-based authentication** on **wired and wireless networks**.
* **Components** (same as RADIUS):  
  ▫ **Supplicant** – User/device requesting access.  
  ▫ **Authenticator** – Network device (e.g., switch, AP).  
  ▫ **Authentication Server** – Validates credentials (e.g., RADIUS/TACACS+ server).
* **Integration**:  
  ▫ Works with RADIUS or TACACS+ to authenticate users.  
  ▫ Common in enterprise-grade network security.
* **Security Value**:  
  ▫ Prevents **rogue devices** from accessing the network.  
  ▫ Enforces authentication **before access is granted**.
* **Recommendation**:  
  ▫ Use **RADIUS** for general implementations.  
  ▫ Use **TACACS+** for **Cisco-heavy environments**.

**1. Core Requirement of 802.1X**

* 802.1X requires **three distinct roles** to function correctly.
* These roles are similar to those used in **RADIUS authentication environments**.

**2. Role 1: Supplicant**

* The **supplicant** is the **device or user** requesting access to the network.
* It initiates the authentication process.
* Examples: laptops, desktops, smartphones, printers, or IoT devices.

**3. Role 2: Authenticator**

* The **authenticator** is the **network device** through which the supplicant attempts access.
* It acts as a **gatekeeper**, passing authentication requests to the authentication server.
* Examples: switches, wireless access points (WAPs), or VPN concentrators.

**4. Role 3: Authentication Server**

* The **authentication server** is the **centralized system** that performs actual authentication.
* It verifies the credentials sent by the supplicant via the authenticator.
* Typically runs **RADIUS** or **TACACS+** protocols to validate access.

**5. Role Confusion Clarification**

* Although **RADIUS and TACACS+** perform **authentication protocol functions**,  
  they are **not authenticators** (they run on the authentication server).
* The **authenticator role is filled by network hardware** (e.g., switches or WAPs), not these protocols.

**6. TACACS+ Protocol Overview**

* **TACACS+ (Terminal Access Controller Access-Control System Plus)** is a **Cisco proprietary protocol**.
* Separates **Authentication**, **Authorization**, and **Accounting (AAA)** into **independent processes**.
* Uses **TCP**, which is **more secure** and **reliable**, but slightly **slower** than UDP.

**7. TACACS+ Capabilities and Suitability**

* **Supports all network protocols**, including legacy protocols like:  
  ▫ Remote Access Protocol  
  ▫ NetBIOS Frame Protocol  
  ▫ X.25 PAD connections
* Ideal for organizations using **Cisco infrastructure throughout the network**.

**8. RADIUS Protocol Overview**

* **RADIUS (Remote Authentication Dial-In User Service)** is an **open standard**, **cross-platform protocol**.
* Combines **authentication and authorization** into a **single process**.
* Uses **UDP**, which is faster but less reliable than TCP.

**9. TACACS+ vs. RADIUS in 802.1X Environments**

| **Feature** | **TACACS+** | **RADIUS** |
| --- | --- | --- |
| Developed By | Cisco (Proprietary) | Open Standard |
| Transport Protocol | TCP (Reliable) | UDP (Faster) |
| AAA Structure | Separated (Auth, AuthZ, Acc) | Combined Authentication/AuthZ |
| Platform Compatibility | Cisco-only networks | Cross-platform |
| Legacy Protocol Support | Full | Limited (Excludes some protocols) |
| Preferred Use Case | Cisco-based networks | Mixed-platform environments |

**10. Security Architecture Design 802.1X**

* 802.1X should be considered a **critical security layer** in enterprise network design.
* It provides **port-based access control** to prevent unauthorized access.
* It prevents **rogue devices** from joining the internal network without authentication.

**11. How 802.1X Operates in Practice**

* Devices connecting to switches or wireless APs must **authenticate via 802.1X** before gaining access.
* It forces endpoints to present valid credentials **before full network connectivity is granted**.
* This control occurs **at the port level** (physical or virtual), securing both wired and wireless interfaces.

**8. EAP (Extensible Authentication Protocol)**

* **Definition**: A **framework**, not a single protocol.
* **Supports**: Multiple authentication mechanisms:  
  ▫ Passwords  
  ▫ Digital certificates  
  ▫ Public Key Infrastructure (PKI)

**8.1 EAP-MD5**

* **Type**: Uses passwords and CHAP-style challenges.
* 🔑 Uses simple password-based authentication
* ❌ Provides only one-way authentication (client to server)
* ❗ Vulnerable to password-based attacks if passwords are weak
* ✅ Use strong, complex passwords to reduce risk
* **Security**: One-way authentication; weak unless **long, complex passwords** are used.

**8.2 EAP-TLS**

* **Authentication**: Mutual authentication using **digital certificates** on both client and server.
* 🛡️ Uses digital certificates on both the client and the server
* 🔒 Provides mutual authentication
* 💡 Immune to password-based attacks (no passwords used)
* 🔐 Requires full PKI infrastructure (certificate deployment and management)
* ✅ Considered one of the most secure EAP types
* **Advantage**: Immune to password-based attacks.

**8.3 EAP-TTLS**

* **Server** uses a digital certificate; **client uses a password**.
* 🔐 Requires a digital certificate only on the server
* 🔑 The client can authenticate using password-based credentials
* ✅ More secure than EAP-MD5
* ❌ Less secure than full EAP-TLS (since only one side uses a certificate)
* **Security Level**: Stronger than EAP-MD5, weaker than EAP-TLS.

**8.4 EAP-FAST (Flexible Authentication via Secure Tunneling)**

* **Uses**: Protected Access Credentials (PACs) instead of certificates.
* 🔐 Uses a Protected Access Credential (PAC) instead of digital certificates
* ✅ Provides mutual authentication
* 📦 Developed by Cisco to simplify deployment without compromising too much security
* ⚙️ Easier to set up than certificate-based systems
* **Benefit**: Simplifies deployment while maintaining security.

**8.5 EAP-PEAP (Protected EAP)**

* **Authentication**: Server uses certificates; client uses Active Directory credentials.
* 🔐 Uses server-side digital certificates
* 🧾 Client credentials are typically validated against Active Directory or LDAP
* ✅ Provides mutual authentication
* 💡 Popular in Microsoft-based enterprise environments
* **Mutual authentication** supported.

**8.6 EAP-LEAP (Lightweight EAP)**

* **Developer**: Cisco (proprietary).
* 🔒 Cisco-proprietary protocol
* ❌ Known to be insecure (vulnerable to dictionary attacks)
* ⚠️ Only usable on Cisco networks
* 🔄 Being phased out in favor of more secure methods like EAP-FAST or EAP-TLS
* **Limitation**: Only usable with **Cisco-based networks**.

Here’s a **clear and comprehensive definition of EAP** along with its **7 major variants**, formatted professionally for **CompTIA A+ 1102 exam preparation** and ideal for pasting directly into Word.

**🔐 What is EAP (Extensible Authentication Protocol)?**

**EAP** is **not a single authentication protocol**, but a **framework** that supports multiple methods of authentication over wired and wireless networks. It is commonly used in **802.1X** environments and works in conjunction with protocols like **RADIUS** or **TACACS+** to verify the identity of users and devices.

**🧩 Core Purpose of EAP:**

* Used to provide **flexible, pluggable authentication mechanisms**
* Supports methods like **passwords, digital certificates, tokens, smart cards**, and **public key infrastructure (PKI)**
* Functions within the **authentication phase** of 802.1X deployments

**📚 The 7 Major EAP Variants**

**1. EAP-MD5 (Message Digest 5)**

* 🔑 Uses simple **password-based authentication**
* ❌ Provides **only one-way authentication** (client to server)
* ❗ Vulnerable to password-based attacks if passwords are weak
* ✅ Use **strong, complex passwords** to reduce risk

**2. EAP-TLS (Transport Layer Security)**

* 🛡️ Uses **digital certificates** on **both the client and the server**
* 🔒 Provides **mutual authentication**
* 💡 Immune to password-based attacks (no passwords used)
* 🔐 Requires full **PKI infrastructure** (certificate deployment and management)
* ✅ Considered **one of the most secure EAP types**

**3. EAP-TTLS (Tunneled Transport Layer Security)**

* 🔐 Requires a **digital certificate only on the server**
* 🔑 The client can authenticate using **password-based credentials**
* ✅ More secure than EAP-MD5
* ❌ Less secure than full EAP-TLS (since only one side uses a certificate)

**4. EAP-FAST (Flexible Authentication via Secure Tunneling)**

* 🔐 Uses a **Protected Access Credential (PAC)** instead of digital certificates
* ✅ Provides **mutual authentication**
* 📦 Developed by Cisco to simplify deployment without compromising too much security
* ⚙️ Easier to set up than certificate-based systems

**5. EAP-PEAP (Protected EAP)**

* 🔐 Uses **server-side digital certificates**
* 🧾 Client credentials are typically **validated against Active Directory or LDAP**
* ✅ Provides **mutual authentication**
* 💡 Popular in **Microsoft-based enterprise environments**

**6. EAP-LEAP (Lightweight EAP)**

* 🔒 Cisco-proprietary protocol
* ❌ Known to be insecure (vulnerable to dictionary attacks)
* ⚠️ Only usable on **Cisco networks**
* 🔄 Being phased out in favor of more secure methods like EAP-FAST or EAP-TLS

**7. EAP-SIM / EAP-AKA *(Bonus: Common in mobile environments)***

*(Not always tested on A+, but useful to know for broader understanding)*

* 📴 Used for authentication in **cellular/mobile networks**
* 🤳 Based on **SIM card credentials**
* 💡 Supports seamless mobile device integration into secure networks

**✅ Summary Table of EAP Variants**

| **Variant** | **Uses Certificates** | **Mutual Authentication** | **Secure?** | **Notes** |
| --- | --- | --- | --- | --- |
| EAP-MD5 | ❌ No | ❌ One-way only | 🚫 Weak | Password-based, outdated |
| EAP-TLS | ✅ Both sides | ✅ Yes | ✅ Very secure | Full certificate deployment needed |
| EAP-TTLS | ✅ Server only | ✅ Yes (partial) | ✅ Strong | Easier to deploy than EAP-TLS |
| EAP-FAST | ❌ No (uses PAC) | ✅ Yes | ✅ Secure | Cisco-developed alternative to TLS |
| EAP-PEAP | ✅ Server only | ✅ Yes | ✅ Secure | Works well with Active Directory |
| EAP-LEAP | ❌ No | ❌ Weak | 🚫 Insecure | Cisco-only, deprecated |

Let me know if you want a quiz on EAP variants, or a flashcard-style summary!

**9. Summary and Best Practices**

* **Authentication protocols in enterprise networks** include:  
  ▫ RADIUS  
  ▫ TACACS+  
  ▫ Diameter  
  ▫ LDAP  
  ▫ Kerberos  
  ▫ 802.1X  
  ▫ EAP (MD5, TLS, TTLS, FAST, PEAP, LEAP)
* **802.1X and EAP** provide essential frameworks for **securing wired and wireless access**.
* **EAP variants** allow flexibility in implementation depending on **security requirements** and **network design**.
* **TACACS+** offers better control in **Cisco environments**; **RADIUS** is preferred for **cross-platform compatibility**.
* **Kerberos** with **Active Directory** enables secure **SSO** in Windows domain environments.