Authentication Protocol

(communication protocol /cryptographic protocol)

-An **authentication protocol** is a type of computer communications protocol or cryptographic protocol.
-These protocols are specifically designed for transfer of authentication data between two entities.

Types -

- Authentication protocols developed for Point-to-point protocol(PPP).
  - PAP- Password Authentication protocol.
  - CHAP - Challenge-handshake authentication protocol.
  - EAP - Extensible authentication protocol.

- AAA architecture protocols (Authentication, Authorization, Accounting)
  - Complex protocols used in larger networks for verifying the user (Authentication)
  - Controlling access to server data (Authorization)
  - Monitoring network resources and information needed for billing of services (Accounting).

Network authentication protocol-

- LDAP -
  Lightweight Directory Access Protocol.
  IT is a Lightweight client-server protocol for accessing directory services.
  LDAP runs over TCP/IP or other connection oriented transfer services.
  LDAP is a software protocol for enabling organizations,individuals,and other resources such as files devices in a network, whether on the public Internet or on a corporate internet.
  There are three common ways to authenticate
    - Anonymous (anyone can bind like our public phone book example)
    - Simple(Its send in plain text Id & Password ,It's not secured)
    - SASL(Simple Authentication and Security Layer) Kerberos protocols used in SASL.

- Kerberos -
  Kerberos is a network authentication protocol.
  It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

- Oauth -
  OAuth2 is an authorization not an authentication framework that enables applications to obtain limited access to user accounts on HTTP services, such as Facebook,GitHub & DigitalOcean.
  User----> Application---->API(Facebook)
  When we authenticate any site behalf of a user then we use OAuth protocol.
  Ex-User---->PhotoApp(need access token from GDrive)
  --->GoogleDrive.(photo printing business)

- SAML -
  Security Assertion Markup Language(SAML) is an XML-based, open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.(Access to cloud applications)
  identity provider provides directory of user and authentication mechanism.
  User-->IdentityProvider--(SAMLToken)-->service Provider
  Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. It is often accomplished by using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers.
  SAML SSO works by transferring the user's identity from one place (the identity provider) to another (the service provider). This is done through an exchange of digitally signed XML documents.

- RADIUS -(AAA)
  Commonly used by ISP.
  Remote Authentication Dial-In User Service (RADIUS) is a full AAA protocol.
  Remote Authentication Dial-In User Service(RADIUS) is a networking protocol that provides centralized authentication,authorization and accounting(AAA) management for users who connect and use a network service.
  It uses NAS and UDP protocol for transport.

//Differences between Network Authentication Protocols

	LDAP	**Kerberos**	**OAuth**	**SAML SSO**	**RADIUS**
Long form	directory access protocol	-	Latest 2.0	Security Assertion Markup Language Single Sign-On	Remote Authentication Dial-In user Service
Authentication	YES	YES	-	YES	YES
Authorization	YES	-	YES	YES	YES
Accounting	-	-	-	-	YES
Advantages	1.LDAP Is an Open Standard Protocol. 2.LDAP Is Lightweight 3.LDAP Is Secure 4.It allows use of multiple independent directories. 5.It runs over TCP/IP and SSL directly. 6.	1.It is supported by various operating systems. 2.Tickets in Kerberos have a limited period. Also if the ticket gets stolen, it is hard to reuse the ticket because of strong authentication needs. (Kerberos uses the concept of a ticket as a token that proves the identity of a user) 3.Passwords are never sent over the network unencrypted. 4.In Kerberos, secret keys are shared which are	1.OAuth 2.0 is a very flexible protocol that relies on SSL (Secure Sockets Layer that ensures data between the web server and browsers remain private) to save user access tokens. 2.OAuth 2.0 relies on SSL which is used to ensure cryptography industry protocols and are being used to keep the data safe. 3.It allows limited access to the user's data and allows accessing	1.Simplifies password management 2.Time-Saving - the most obvious is the time saved not having to frequently login to multiple applications. 3.Reduces Password Loss - It also reduces the chance of losing a password, so the IT help desk spends less time trying to recover lost passwords 4.Easy Access of Applications - Logins are easier to remember and more convenient. Users can effortlessly	1.Avoids the pain of password management. 2.Central point for user and system authentication. 3.RADIUS allows for unique credentials for each user, which lessens the threat of hackers infiltrating a network (e.g. WiFi) since there is no unified password shared among a number of people. 4.reat tool for larger networks managed by multiple IT admins.

		more efficient than sharing public keys.	when authorization tokens expire. 4.It has the ability to share data for users without having to release personal information. 5.It is easier to implement and provides stronger authenticatio n.	sweep through applications without spending time with required logins.	
Disadvantages	1.It requires directory servers to be LDAP compliant for service to be deployed.	1.t is vulnerable to weak or repeated passwords. 2.It only provides authenticatio n for services and clients.	1.SSL takes time to run basic HTTP, so this will make the response time considerably slow 2.The lack of encryption makes the security risk fairly high. 3.In case an SSL / TLS connection is not implemented an MITM Attack may occur	1.If a hacker breaches your identity provider user account, all your linked systems could be open to attack. 2.When SSO is down, access to all connected sites is stopped 3.SSO using social networking services can create conflict.	1.Maintenance can be difficult and time-consumin g for on-prem hardware. 2.Vast array of configuration options. 3.Some options can be costly and require long-term commitments, while others are free, and some require extensive time and effort to implement
Features	1.OAuth 2.0 is a simple protocol that allows access	client/server applications by using	limited access to user accounts	1.SAML deals with XML as the data	RADIUS *can* store user identities for

	to resources of the user without sharing passwords. 2.It provides user agent flows for running clients applications using a scripting language, such as JavaScript. Typically, a browser is a user agent. 3.It accesses the data using tokens instead of using their credentials and stores data in an online file system of the user such as Google Docs or Dropbox account.	secret-key cryptography.	on an HTTP service	construct or token format. 2.Scope within an enterprise or enterprise to partner or enterprise to cloud scenarios.	authentication.
Applications	OpenVPN, Jenkins, Kubernetes, Docker, and many others.	Many UNIX-like operating systems, including FreeBSD, Apple's Mac OS X, Red Hat Enterprise Linux 4, Sun's Solaris, IBM's AIX, HP's OpenVMS, and others,	Facebook, GitHub, and DigitalOcean.	Salesforce, Gmail, Box and Expensify	Commonly used by ISP.