6.12.2 Network Authentication Facts

Authentication is the process of validating user credentials that prove user identity. Authentication is typically the first step in connecting to a network. Following successful authentication, access controls can be implemented to allow or deny access to network resources.

A simple form of authentication sends a user name and password to an authentication server. If the password is sent in clear text, the authentication credentials can be intercepted and used to impersonate an authorized user. One method of protecting logon credentials is by using a challenge/response mechanism (also called a three-way handshake). Using this process:

1. Both the authentication server and the authenticator are configured with a common shared secret. This shared secret is usually a password associated with a user account.
2. The authentication server sends a challenge string to the authenticator.
3. The authenticator uses the shared secret to hash the challenge string and returns the user account name and the hashed value to the authentication server.
4. The authentication server uses its shared secret value to also hash the challenge string. If the two hashed values match, the authentication server assumes that the authenticator also knows the shared secret.

With the challenge/response method, the password is never sent through the network; only the hashed challenge string is exchanged. Be aware that the hashed challenge string is not an encrypted form of the password.

The following table describes various authentication methods used for network authentication, many of which use some form of challenge/response mechanism.

Protocol	Description
LAN Manager (LANMAN or LM)	LAN Manager was the original authentication mechanism for Windows computers. - LANMAN is the only authentication method supported by Windows 9x and pre-NT systems. - LANMAN is still used by some protocols and applications. - Passwords are protected using a hashing method called LANMAN Hash that uses DES and a proprietary algorithm. - LANMAN passwords are limited to a total of 14 characters. - LANMAN divides passwords longer than seven characters into two separate hashes (characters 1 - 7 are a single hash, and characters 8 - 14 are a separate hash). - LANMAN Hash is very weak and can be easily broken.
NT LAN Manager (NTLM)	NT LAN Manager is the replacement for LAN Manager on Microsoft networks. - NTLM was introduced with Windows NT and is supported by all current Windows operating systems. Windows 9x clients can be upgraded to support NTLM by installing the Active Directory client. - NTLM uses the SMB (Server Message Block) protocol - NTLM uses a challenge/response method identical to that used by MS-CHAP. - NTLM uses a stronger hashing method than LM. - NTLM Version 2 includes additional security enhancements and a stronger hashing method.
Kerberos	Kerberos is used for both authentication and authorization to services and is the default authentication method used by computers that are a part of an Active Directory domain. Kerberos grants *tickets* (also called a secure *token*) to authenticated users and to authorized resources. The process of using tickets to validate permissions is called *delegated authentication*. Kerberos uses the following components: - An authentication server (AS) accepts and processes authentication requests. - A service server (SS) is a server that provides or holds network resources. - A ticket granting server (TGS) grants tickets that are valid for specific resources on specific servers. - The authentication server and ticket granting server are often combined into a single entity known as the Key Distribution Center (KDC). Kerberos works uses the following process: 1. The client sends an authentication request to the authentication server. 2. The authentication server validates the user identity and grants a ticket granting ticket (TGT). The TGT validates the user identity and is good for a specific ticket granting server. 3. When the client needs to access a resource, it submits its TGT to the TGS. The TGS validates that the user is allowed access and issues a client-to-server ticket. 4. The client connects to the service server and submits the client-to-server ticket as proof of access. 5. The SS accepts the ticket and allows access. Be aware of the following: - Kerberos uses symmetric key cryptography. - Tickets are valid during the entire session and do not need to be re-requested, thereby providing single sign-on. - Kerberos requires that all servers within the process have synchronized clocks to validate tickets. - Kerberos shares a different secret key with every entity on the network. Knowledge of that secret key equals proof of identity (this system is called the *realm*).

	▪ Kerberos uses TCP port 88. ▪ The KDC is a single point of failure. ▪ Tickets are temporarily stored on the user's workstation and could be compromised. ▪ Initial authentication is vulnerable to password guessing. The KDC cannot know if an attack is in progress. ▪ Network traffic is not protected by Kerberos. ▪ When a user changes a password, it changes the secret key. Thus, the KDC database needs to be updated.
OAuth	*Open Authorization* (OAuth) is an open standard for token-based authentication and authorization on the internet. It allows access tokens to be issued to third-party clients by an authorization server with the approval of the resource owner. The third party then uses the access token to access the protected resources hosted by the resource server. This mechanism is used by companies like Google, Facebook, Microsoft and Twitter to permit the users to share information about their accounts with third-party applications or websites. OAuth specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. It is designed to work with Hypertext Transfer Protocol (HTTP). OAuth is a service that is complementary to and distinct from OpenID.
OpenID	*OpenID* is an open standard and decentralized authentication protocol. It allows users to be authenticated by co-operating sites using a third-party service and allowing users to log in to multiple unrelated websites without having to have a separate identity and password for each. Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign on to any website that accepts OpenID authentication. The OpenID protocol does not rely on a central authority to authenticate a user's identity. Because neither services nor the OpenID standard mandates how to authenticate users, authentication methods range from passwords to smart cards and biometrics. *OpenID Connect* (OIDC) is a simple identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of an end user based on the authentication performed by an authorization server. OpenID Connect allows a range of clients, including web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users. The specification suite is extensible, supporting optional features such as encryption of identity data, discovery of OpenID providers, and session management.
Shibboleth	Shibboleth is an open-source, single sign-on authentication protocol that is used for both network authentication and internet authentication. Shibboleth is a web-based protocol, and it uses the federated access control model. This lets clients use the same identification data to obtain access to every network in the group. Authentication messages are sent using the security assertion markup language (SAML), which allows a client to log on once for affiliated but separate websites or network resources. *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.

The Lightweight Directory Access Protocol (LDAP) is a lightweight protocol that allows users and applications to read from and write to an LDAP-compliant directory service, such as Active Directory, eDirectory, and OpenLDAP. The LDAP client must *bind* (authenticate) to the directory service before reading/writing to the database. The LDAP server can also authenticate to the client. This is known as mutual authentication.

LDAP supports the following authentication modes when binding to a directory service:

Mode	Characteristics
Anonymous	▪ Only a user name (no password) is required to authenticate.
Simple	▪ A username and password are required. ▪ Normally, the username and password are passed in cleartext. ▪ LDAP uses ports 389 and 636 by default. ▪ For unsecured sessions, LDAP uses port 389. ▪ To protect simple authentication, port 636 is used for LDAP over SSL.
Simple Authentication and Security Layer (SASL)	▪ SASL is an extensible mechanism for protecting authentication. ▪ Using SASL, you can use Kerberos, MD5, S/Key, IPSec, TLS, or many other mechanisms for authentication.