13.5.5 Authentication Protocol Facts

An authentication protocol identifies how credentials are submitted, protected during transmission, and validated. Instead of a simple username and password, some authentication protocols require certificates and digital signatures for proof of identity.

- A *certificate* is a digital document that identifies a user or a computer. The certificate includes a subject name, which is the name of a user or a computer.
- Certificates are obtained from a *public key infrastructure* (PKI). A PKI is a collection of hardware, software, policies, and organizations that create, issue, and manage digital certificates.
- A PKI is made up of *certificate authorities* (CAs), also called certification authorities. A CA:
  - Accepts certificate requests.
  - Verifies the information provided by the requester.
  - Creates and issues the certificate to the requester.
  - Revokes certificates, which invalidates them.
  - Publishes a list of revoked certificates known as the *certificate revocation list* (CRL).
- You can obtain certificates from a public CA such as DigiCert or install your own PKI and CAs to issue certificates to users and computers in your organization.
- Computers accept any certificate issued by a trusted CA as valid. By default, most computers trust well-known public CAs. If you configure your own PKI, you need to configure each computer in your organization to trust your own CAs.

  In order for a certificate to be trusted by users outside of your organization, you must obtain a certificate from a third-party CA.

- A *digital signature* is a digital document that is altered in such a way that it could only have come from the subject identified in the certificate. A certificate obtained from a PKI is signed by the CA that issued the certificate (the digital signature of the issuing CA is included in the certificate).
- A computer that receives a certificate verifies the issuing CA's signature. If the CA is trusted, the computer will accept the user or computer's identity.

Protocol Descriptions

The following table describes several common authentication protocols. Each authentication protocol has a different authentication method as well as a specific use.

Protocol	Description
Challenge Handshake Authentication Protocol (CHAP)	CHAP is a three-way handshake (challenge/response) authentication protocol used for remote access connections. Both devices are configured with a password called a *shared secret*. For unique user authentication, this value is associated with a user account. The challenge/response authentication mechanism occurs in three steps: 1. The server generates a challenge message and sends it to the client. 2. The client responds with the username and a value created using a one-way hash function on the challenge message. 3. The server checks the response against its own value created using the same hash. If the values match, the client is authenticated. With CHAP, plaintext versions of the password are never sent; only the hashed challenge message is sent between devices.
Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)	MS-CHAP is Microsoft's proprietary challenge-response authentication method used for remote access connections. MS-CHAP: ▪ Encrypts the shared secret on each system so it is not saved in plaintext. ▪ Provides a mechanism for changing the password over the remote connection. ▪ Allows for mutual authentication, where the server authenticates to the client, if you use v2. Be aware that MS-CHAP and MS-CHAP v2 both have known security vulnerabilities and should be avoided if possible.
Extensible Authentication Protocol (EAP)	EAP allows the client and server to negotiate the characteristics of authentication. ▪ An EAP authentication scheme is called an EAP *type*. Both the client and authenticator have to support the same EAP type for authentication to function. ▪ When a connection is established, the client and server negotiate the authentication type that will be used based on the allowed or required authentication types configured on each device. ▪ The submission of authentication credentials occurs based on the rules defined by the authentication type. ▪ EAP is used to allow authentication with smart cards, biometrics, and certificate-based authentication.

	Other versions of EAP include: ▪ *PEAP*, also known as *protected extensible authentication protocol*. It is a more secure version of EAP. It provides authentication to a WLAN that supports 801.1X. PEAP uses a public key over TLS. ▪ *EAP-FAST*, also known as *flexible authentication via secure tunneling*. This version performs session authentication in wireless networks and point-to-point connections. ▪ *EAP-TLS* uses TLS protocol and is used mostly by wireless vendors. It is one of the most secure EAP standards.
Kerberos	Kerberos is used for both authentication and authorization to services. Kerberos grants *tickets* (also called security *tokens*) to authenticated users and 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) provides or holds network resources. ▪ A ticket granting server (TGS) grants tickets that are valid for specific resources on specific servers. Kerberos works as follows: 1. The client sends an authentication request to the AS. 2. The AS validates the user identity and grants a ticket granting ticket (TGT), which validates the user identity and is good for a specific TGS. 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 SS and submits the client-to-server ticket as proof of access. 5. The SS accepts the ticket and allows access. Tickets are valid during the entire session and do not need to be re-requested. Windows Active Directory uses Kerberos for user authentication and for controlling resource access. Kerberos requires that all servers within the process have synchronized clocks to validate tickets.
802.1x	802.1x is an authentication method used on a LAN to allow or deny access based on a port or connection to the network. ▪ 802.1x is used for port authentication on switches and authentication to wireless access points. ▪ 802.1x requires an authentication server for validating user credentials. This server is typically a RADIUS server. ▪ Authentication credentials are passed from the client, through the access point device, and on to the authentication server. ▪ The access point enables or disables traffic on the port based on the authentication status of the user. ▪ Authenticated users are allowed full access to the network; unauthenticated users only have access to the RADIUS server. ▪ 802.1x is based on EAP and can use a variety of methods for authentication (for example, usernames and passwords, certificates, or smart cards).