13.6.3 Secure Protocol Facts

Many protocols were designed with little or no security controls. These protocols are considered unsecure because they do not provide authentication or they use clear text credentials, meaning authentication information is sent unencrypted. Security services (authentication and encryption) are often added to new or existing protocols using one of the following secure protocols:

- Secure sockets layer (SSL)
- Transport layer security (TLS)
- Secure shell (SSH)

Unsecure Protocols vs. Secure Protocols

The following table compares unsecure and secure protocols.

Unsecure Protocol	Secure Protocol	Description
Hypertext Transfer Protocol (HTTP)	HTTP over SSL (HTTPS)	HTTPS is a form of HTTP that uses SSL to encrypt data before it is transmitted.
Telnet Remote Shell (RSH)	Secure Shell (SSH)	SSH allows for secure interactive control of remote systems. SSH uses RSA public key cryptography for both connection and authentication. SSH is also a protocol that can be used to provide security services for other protocols. - Telnet should never be used. It uses clear text credentials for authentication and doesn't use any type of encryption. - Since public key algorithms tend to be slower and less safe than private keys, both SSH and TLS use a combination of the two for generating new keys.
File Transfer Protocol (FTP) Remote Copy Protocol (RCP) Trivial File Transfer Protocol (TFTP)	Secure FTP (SFTP) FTP over SSL (FTPS) Secure Copy Protocol (SCP)	Both SFTP and SCP are file copy protocols that use SSH for security. SSH provides authentication and encryption. FTPS uses SSL to encrypt data.
Simple Network Management Protocol (SNMPv1,SNMPv2)	SNMPv3	The original version of SNMP has several vulnerabilities, including: - No authentication of devices. Any device configured with the correct community name can send messages that will be received and processed. - Information sent in plain text. - The SNMP manager can send messages to a device, and the device will perform an action. SNMPv2 added some security features, but most security comes with SNMPv3. SNMPv3 adds the following: - Authentication for agents and managers. - Encryption of SNMP information. - Hashing is added to ensure data integrity so data is not altered in transit.
Serial Line Internet Protocol (SLIP)	Point-to-Point Protocol (PPP)	PPP is used to create a connection between two devices. It uses PAP or CHAP for authentication and can also provide encryption.