Security+ SY0-601

Module 7: Ports and Protocols.

aci LEARNING [HUBS]

Table of Contents.

1 General overview.

2 Resolution and directory services.

3 Network communication and management.

4 Email.

5 Voice and database.

6 Authentication Protocols.

aci LEARNING

Learning objectives.

Upon completion of this module, you should be able to:

- Identify email protocols along with any associated secure protocols.
- Identify voice and database protocols along with any associated secure protocols.
- Identify authentication protocols and any associated security they may have.
- Explain the purpose of cryptography and why different algorithms are used.

Learning objectives.

Upon completion of this module, you should be able to:

- Identify resolution and directory service protocols along with any associated secure protocols.
- Identify network communication and management protocols along with any associated secure protocols.

General Overview.

GENERAL OVERVIEW.

Key concepts.

In this section, we will cover the following key concepts:

- Ports.
- Protocols.
- Headers.

aci LEARNING

GENERAL OVERVIEW.

Port numbers.

A port number is a software-defined number assigned to a network protocol. There are 65,535 available port numbers which are grouped into sets of ports based on the port number.

Ports numbers are mostly standardized and recorded in the IANA port number registry.

As a security professional, you will study and work with port numbers in a variety of contexts, such as firewalls and ACLs, and settings for various protocols, such as which email ports to use.

CONTINUED ON NEXT SLIDE >

aci LEARNING

GENERAL OVERVIEW.

Port numbers.

Well-known ports range from 0 to 1023 and represent numbers that tend to be studied by technicians. These ports are controlled.

Registered ports range from 1024 to 49151 and are used mostly for software and protocols that are not so universal; however, many well-known protocols have port numbers in this range. These ports may be registered for use.

Dynamic/Private/Ephemeral ports range from 49152 to 65535 and are short-term and may be used for any purpose. These ports are not controlled.

GENERAL OVERVIEW.

Protocols.

A protocol is a set of rules for performing a certain set of tasks, such as communications, transmissions, and connectivity. Protocols can be shared from network to network, from machine to machine, to enable them to work together.

Ethernet is a protocol for transferring data on a local area network; it is at the second layer of the OSI model.

Internet Protocol is a set of rules for addressing and routing packets of data across a network so they arrive at the destination; it resides at the third layer of the OSI model.

GENERAL OVERVIEW.

Protocols.

User Datagram Protocol provides connection-less, non-guaranteed communication with no flow control or sequencing; it is useful when not all packets need to arrive at the destination and is used for audio, video, and gaming.

Transmission Control Protocol provides connection-oriented, guaranteed communication with flow control and sequencing; it is used when the entire file needs to arrive at the destination. Should a packet not arrive, the destination will ask for a retransmission of the packet.

GENERAL OVERVIEW.

Ethernet header.

Preamble – Ethernet frame starts with a 7-byte preamble, a pattern of alternative 0s and 1s, which indicates the starting of the frame and allows the sender and receiver to establish bit synchronization.

Start of frame delimiter (SFD) – Always set to 10101011. SFD indicates that upcoming bits are starting the frame, which is the destination address.

Destination address – Contains the MAC address of the machine for which data is destined.

Source address – Contains the MAC address of the source machine. As the source address is always an individual address (Unicast), the least significant bit of the first byte is always 0.

CONTINUED ON NEXT SLIDE >

GENERAL OVERVIEW.

Ethernet header.

Length – Indicates the length of the entire Ethernet frame. The length cannot be larger than 1500 because of some own limitations of Ethernet.

Data – Where actual data is inserted, also known as payload. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet.

Cyclic Redundancy Check (CRC) – Contains a 32-bit hash code of data, which is generated over the destination address, source address, length, and the data field.

Note: The size of the frame of Ethernet IEEE 802.3 varies from 64 bytes to 1518 bytes, including data length (46 to 1500 bytes). The maximum data length, 1500 bytes, is known as the Maximum Transmission Unit (MTU).

GENERAL OVERVIEW.

IP header (version 4).

Version – Indicates the format of the internet header.

Header length – Is the length of the internet header.

Service type – Indicates in the abstract the quality of service.

Total length – Length of the datagram, including header and data.

Identification – Value sent to aid in assembling fragments of a datagram.

Flag – A control flag indicating if the datagram is fragmented.

Fragmentation offset – Indicates where in the datagram this fragment belongs.

CONTINUED ON NEXT SLIDE >

ACI LEARNING

GENERAL OVERVIEW.

IPv4 header.

Time to Live – Time the datagram can remain in the internet system.

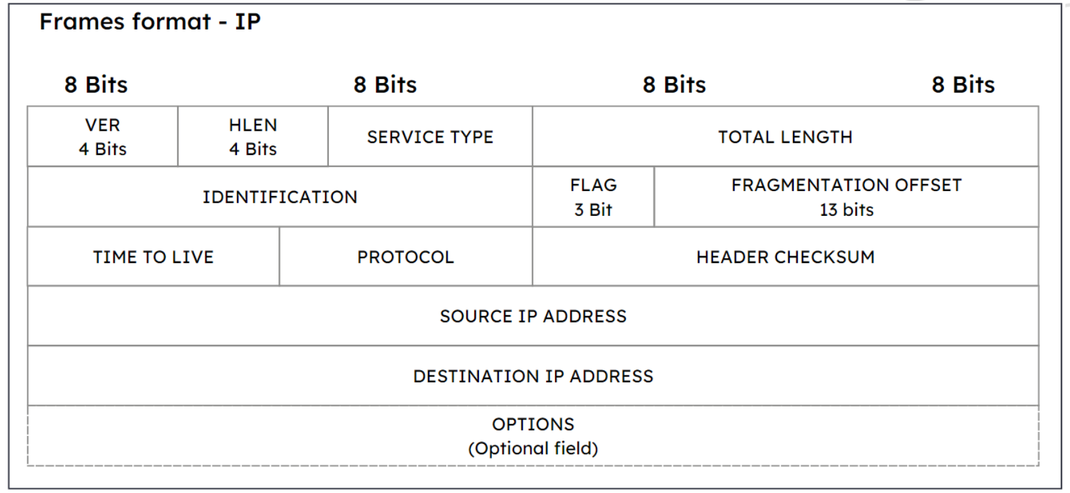
Protocol – Indicates next-level protocol used.

Header checksum – For integrity purposes.

Source IP address – Source address.

Destination IP address – Destination address.

Options – May or may not appear.

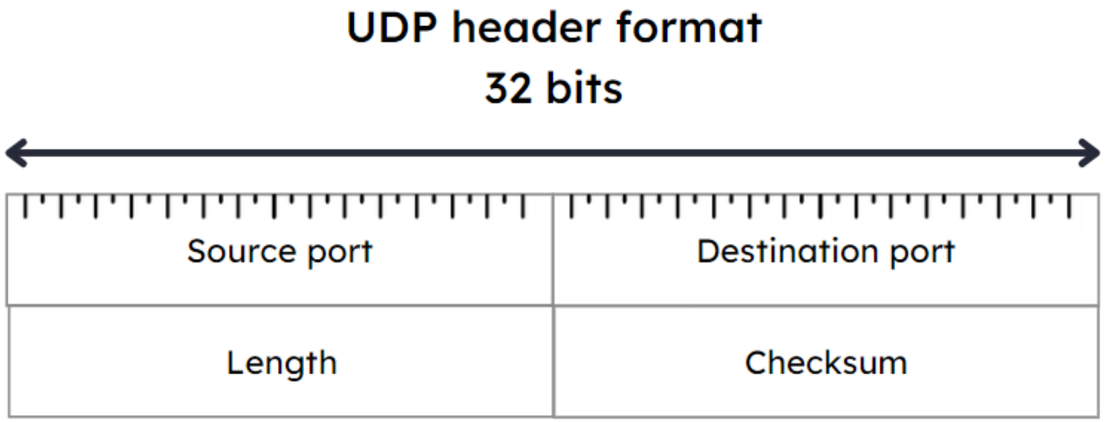


GENERAL OVERVIEW.

UDP header.

Source port – Port of the sending process.
Destination port – Port of the receiving process.
Length – Length of datagram including header and data.
Checksum – For integrity.

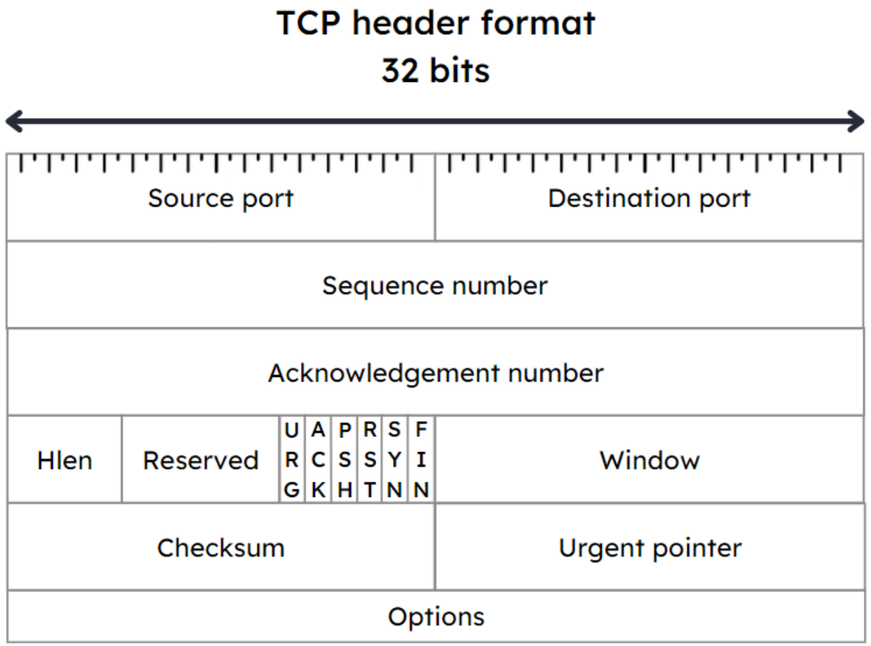
More information can be found at RFC 768: User Datagram Protocol (rfc-editor.org).



GENERAL OVERVIEW.

TCP header.

Source port – Source port number.
Destination port – Destination port number.
Sequence number – Sequence number of first data.
Acknowledgment number – Next sequence number the sender is expecting.
Header length – Number of 32-bit words in the TCP header. Indicates where the data begins.
Reserved – For future use.



GENERAL OVERVIEW.

TCP header.

FLAGS:

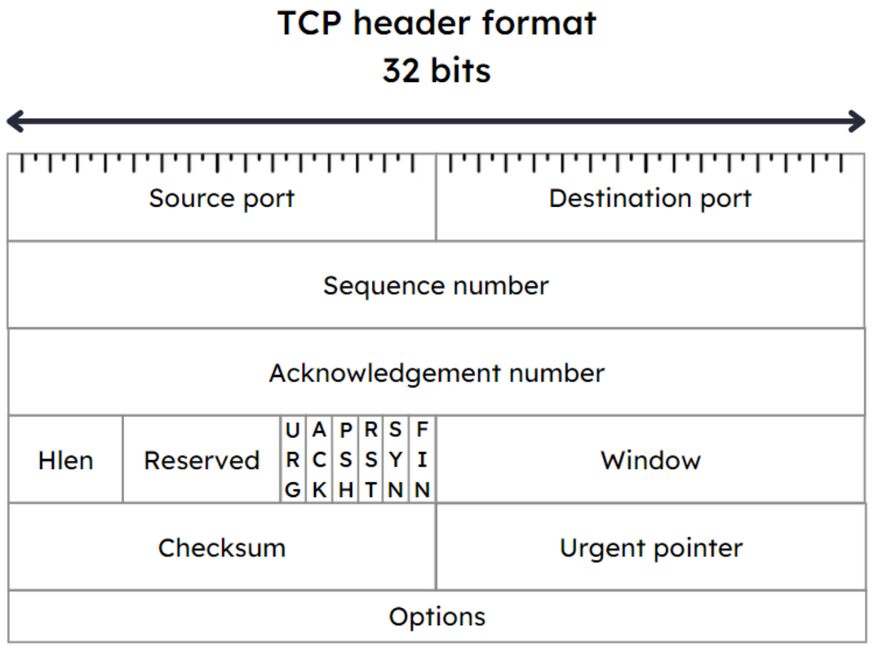
- URG – Urgent.
- ACK – Acknowledgement.
- PSH – Push function.
- RST – Reset the connection.
- SYN – Synchronize sequence numbers.
- FIN – No more data from the sender.

Window – Number of octets the sender is willing to accept.

Checksum – For integrity.

Urgent pointer – Only if the URG flag is set. Value of the urgent pointer as offset from the sequence number.

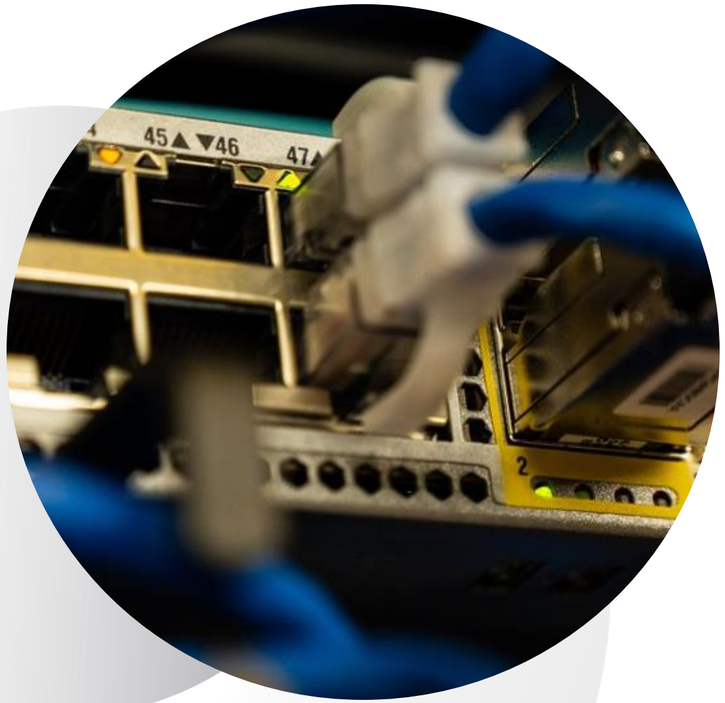
Options – May or may not be present.



More information can be found at RFC 793: Transmission Control Protocol (rfc-editor.org).

GENERAL OVERVIEW.

Secure vs. Insecure protocols.



- Many protocols have secure and unsecured versions. Secure versions encrypt transmissions, while unsecured ones do not.
- Unsecured protocols, like HTTP, might be used to send a transmission of data that is publicly available or for internal websites, whereas HTTPS might be used to securely access your bank's website.

aci LEARNING

GENERAL OVERVIEW.

Knowledge check.

Let's apply what we have covered:

- Which header has a field for TTL?
- Discuss the differences between UDP and TCP.

Resolution and Directory Services.

GENERAL OVERVIEW.

Key concepts.

In this section, we will cover the following key concepts:

- Address Resolution Protocol.
- Domain Name System.
- DNSSEC.
- LDAP.
- LDAPS.

aci LEARNING

Address Resolution Protocol (ARP).

Address Resolution Protocol (ARP) is a protocol that will resolve IP addresses to MAC addresses. A MAC address is a physical address permanently embedded in a device's NIC.

Understanding the function of ARP will allow an administrator to troubleshoot issues with data flow throughout the network or identify specific network attacks.

When isolating the function of each network device, routers contain Address Resolution Protocol (ARP) tables, and switches contain MAC tables. When data enters a network given a destination IP address, the network devices will use ARP to determine the correct physical address to send the data.

Domain Name System (DNS).

- A Domain Name System (DNS) is used to convert FQDNs (Fully-Qualified Domain Names) to IP addresses.
- Computers do not inherently understand domain names; rather, they request a DNS record to obtain the routable IP address that systems can use.
- DNS uses UDP port 53. DNS responses can’t exceed 512 Bytes which guarantees the response will not be fragmented.

RESOLUTION AND DIRECTORY SERVICES.

DNSSEC.

Domain Name System Secure (DNSSEC) uses digital signatures to add a layer of security to DNS. Delegation Signing (DS) data contains the digital signature.

Due to the increase in data due to DS, DNSSEC utilizes TCP port 53.

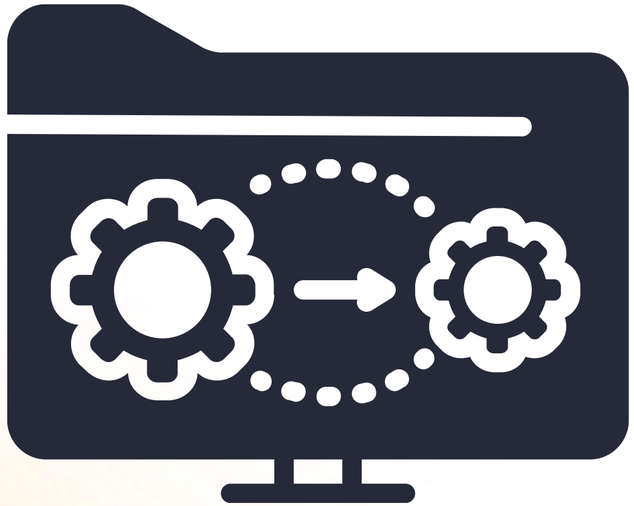
DNSSEC guarantees

- Authenticity
- Integrity
- The non-existence of a domain name

DNSSEC does not guarantee

- Confidentiality
- Protection against DoS

LDAP.



LDAP queries X.500 format directories using TCP/UDP port 389. The distinguished name (DN) identifies X.500 records. Each record has attributes. Typically, the CN is listed first. Some commonly used attributes in typical order include:

- CN – Common Name
- O – Organization
- OU – Organizational Unit
- C – Country
- ST – State
- L – Locality
- DC – Domain Component

RESOLUTION AND DIRECTORY SERVICES.

LDAPS.

Lightweight Directory Access Protocol Secure (LDAPS) is an encrypted implementation of LDAP over SSL/TLS over TCP port 636.

RESOLUTION AND DIRECTORY SERVICES.

Knowledge check.

Let's apply what we have covered:

- Describe the attributes used in LDAP.
- What does DNSSEC guarantee?

Network communication and management.

Key concepts.

In this section, we will cover the following key concepts:

- ICMP.
- SNMP.
- DHCP.
- NTP.
- NetBIOS.
- Telnet.
- SSH.
- MSB.
- NFS.
- Syslog.
- RDP.
- Routing protocols.
- File transfer protocols.
- HTTP.
- HTTPS.

Internet Control Message Protocol (ICMP).

Internet Control Message Protocol (ICMP) is responsible for sending basic network messages, typically simplistic error messages. PING and TRACERT are based on the ICMP protocol.

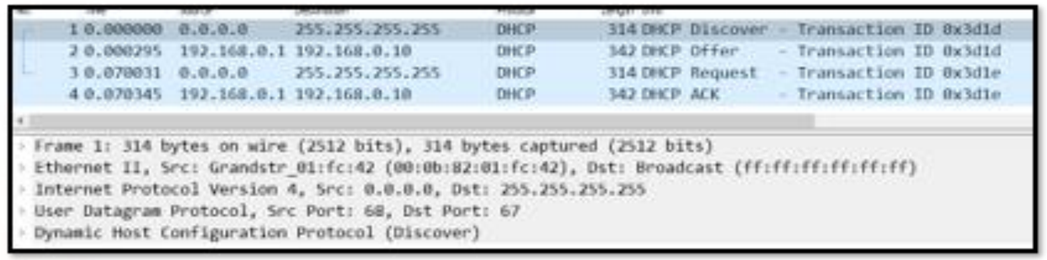
Simple Network Management Protocol (SNMP).

- Simple Network Management Protocol (SNMP), UDP ports 161/162, are used to manage networks; this protocol is specifically used when loading management or diagnostic software across a network.
- SNMP can collect data on specific network devices. When a specific type of network traffic needs to be assessed, administrators can use SNMP to send "SNMP get-requests," allowing requests for any data on specified traffic.

Dynamic Host Configuration Protocol (DHCP).

Dynamic Host Configuration Protocol (DHCP), UDP ports 67 and 68, are used to automatically or dynamically assign IP addresses and other configuration parameters within a network.

When a user connects to a network, DHCP issues an unused IP address from the scope and a pool of available IP addresses.



NTP.

Network Time Protocol (NTP) is used to synchronize the clocks of devices on a network. Synchronizing clocks ensures all logs are synchronized and any “jobs” dependent on time are running at the appropriate time.

NTP uses UDP port 123.

Stratum 1 servers obtain Coordinated Universal Time (UTC) and provide that information to Stratum 2 servers. This is considered an “authoritative time.”

Some publicly available time servers are:

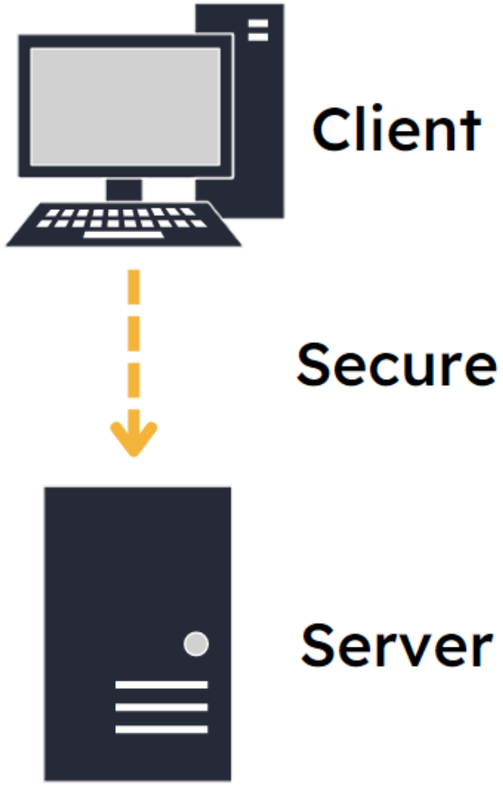
- time-a-g.nist.gov
- time.apple.com
- time.google.com

Telnet.

- Telnet is a TCP/IP protocol that enables command-line management of a remote system, functioning as a terminal emulator, using TCP port 23 by default.
- Telnet is not secure as all communications, including username and password, are sent in plain text.

Secure Shell (SSH).

Secure Shell (SSH), port 22, is a protocol that allows multiple computers to remotely connect to one another in a secure environment using a terminal emulator for remote system management; it encrypts all traffic between the admin computer and the remote machine.



NETWORK COMMUNICATION AND MANAGEMENT.

SMB.

Server Message Block (SMB) was created by IBM in 1982 to facilitate shared access to files and folders across a computer network.

Windows uses this as its main file and print-sharing service.

SMB uses TCP port 445.

For security reasons, it is best to disable SMB version 1.0 and use SMB encryption. Encryption is a standard feature of SMB version 3.0.

aci LEARNING

NETWORK COMMUNICATION AND MANAGEMENT.

NFS.

Network File System (NFS) was created by Sun Microsystems in 1984 to allow computers on a network to exchange files; it has been updated many times. NFS is an open IETF standard as defined in RFC 5661 (https://www.rfc-editor.org/rfc/rfc5661).

NFSv4 uses TCP port 2049 and is supported by both Unix and Windows computers.

aci LEARNING

Syslog.

Syslog is a protocol for logging and exchanging event messages on computers and network devices; it uses UDP port 514.

Rsyslog is an update of the original syslog specification; it uses the same file syntax but works over TCP and has a secure connection.

Syslog-ng is another update utilizing secure TCP communication but with an updated configuration file syntax.

NETWORK COMMUNICATION AND MANAGEMENT.

RDP.

Remote Desktop Protocol (RDP) is a graphical user interface for managing Windows-based computers; it provides an encrypted tunnel between the administrator's computer and the computer being administered.

RDP uses TCP port 3389.

For additional security, administrators should:

- Utilize RDP gateways.
- Enable Network Level Authentication (NLA).
- Enable Remote Credential Guard.

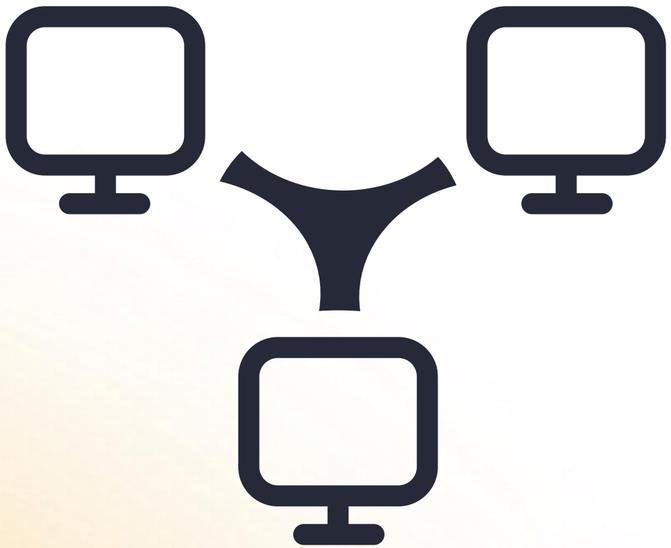
aci LEARNING

Routing protocols.

- Routing protocols are the methods and standards used by each router to determine the path that data will travel.
- Routing can be accomplished using static routing tables or by creating them dynamically.
- The two most common dynamic routing protocols are link-state and distance vector protocols. Distance vector protocols will use the hop count as the primary metric for determining a path, while link-state uses cost as a primary metric.

CONTINUED ON NEXT SLIDE >

Routing protocols.

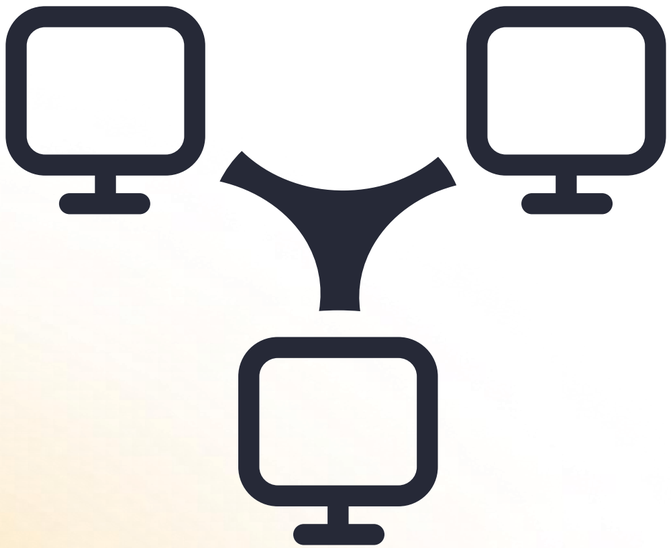


- Routing Information Protocol (RIP) is an older interior routing protocol that uses TCP port 520.
- RIPv2 provides for a level of authentication.
- Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco-developed interior routing protocol encapsulated directly into IP datagrams.

  It uses native IP port 88.

CONTINUED ON NEXT SLIDE >

Routing protocols.



- Open Shortest Path First (OSPF) is an interior routing protocol that links OSPF areas that uses OSPF's own datagram format.

  It uses native port 89.

- Border Gateway Protocol (BGP) is an exterior routing protocol linking autonomous systems (AS) on the internet.

  It uses TCP port 179.

FTP.

- File Transfer Protocol (FTP), one of the earliest protocols released as part of the TCP/IP protocol suite, enables uploading and downloading files between a local system and a remote server. TCP ports 20-21.
- Port 21 is used for the control connection, and port 20 carries the data connection, providing file transfer.

SFTP and SCP.

- Secure File Transfer Protocol (SFTP) runs over TCP port 22 and relies on SSH for encryption.
- A secure alternative to FTP, mainly used in Linux environments, Secure Copy Protocol (SCP), depends on SSH for encryption; therefore, it runs over TCP port 22, as does SSH.

FTPES and FTPS.

- Also known as Explicit TLS, FTPES establishes an unsecure connection to the server over TCP port 21, which is then upgraded to a secure connection to transfer user authentication using the AUTH TLS command.
- The control connection runs over TCP port 990, while the data transfer is over port 989.
- FTPES is preferred over FTPS due to deployment complexities when the firewall must be negotiated, as when the FTP server is accessed from a remote network.

CONTINUED ON NEXT SLIDE >

FTPES and FTPS.

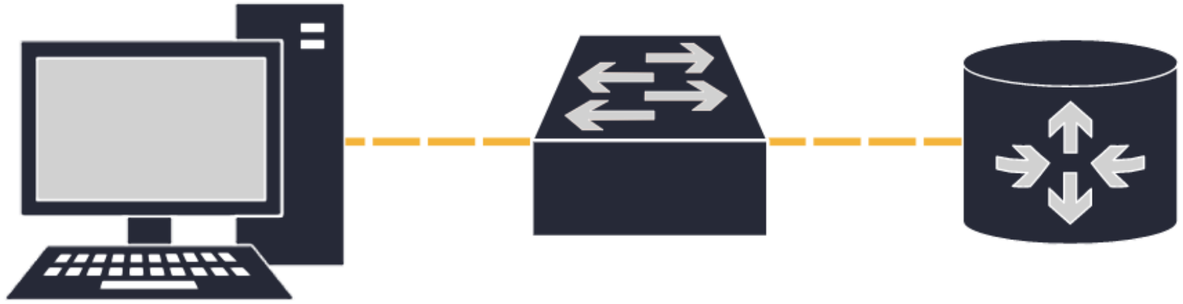
FTP over SSL/TLS relies on SSL/TLS for encryption. Also known as Implicit TLS, it negotiates an SSL/TLS tunnel before issuing any FTP commands.

TFTP.

Trivial File Transfer Program (TFTP) is an older method of transmitting small amounts of data. TFTP was used in conjunction with the BOOTP protocol to obtain an IP address and the network location of a boot image.

TFTP is not secure and should not be used anymore.

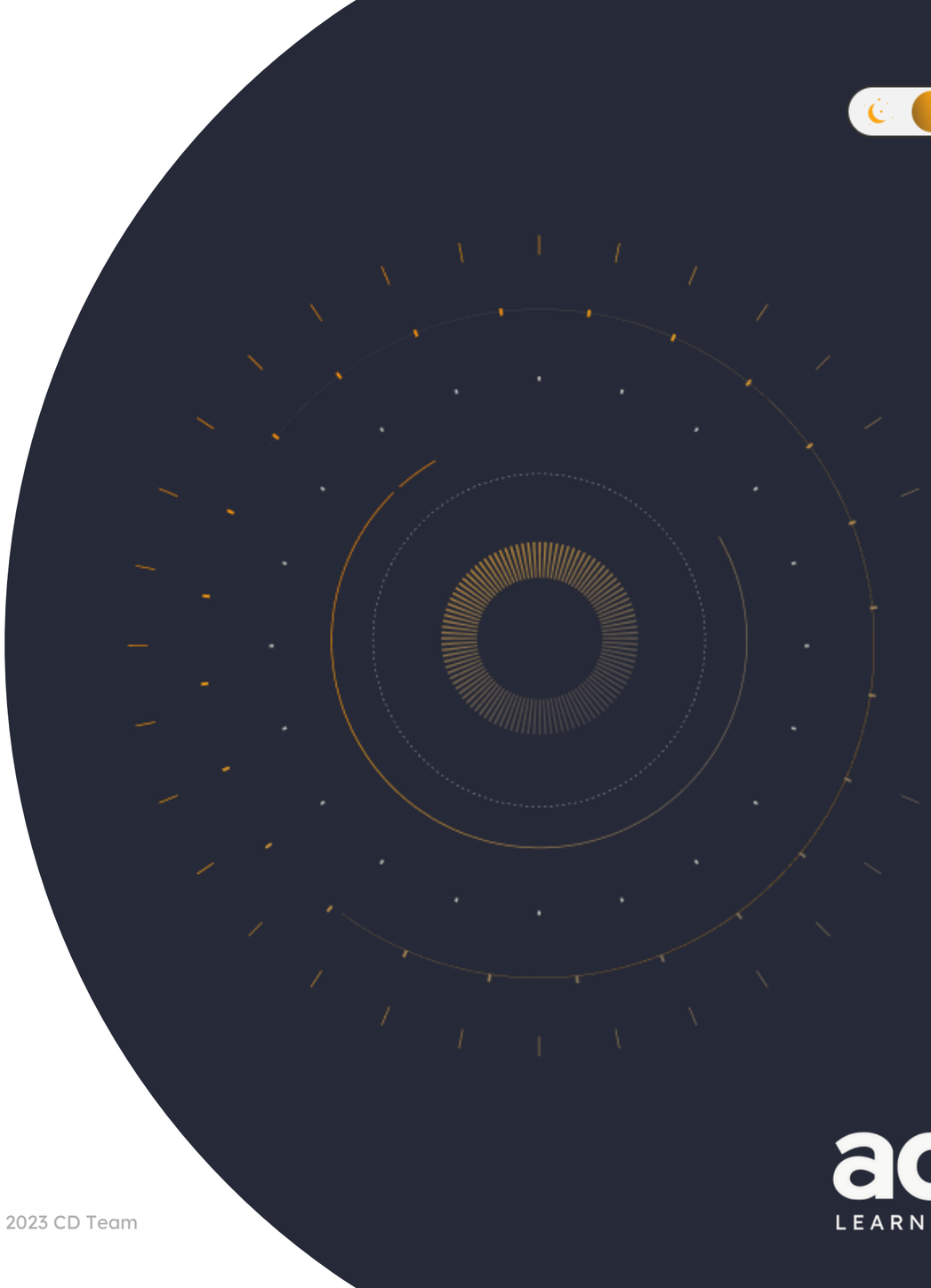
This protocol uses UDP port 69.



HTTPS.

- HTTP Secure (HTTPS) is used to provide secure communication between web browsers and web servers by encrypting the communication with SSL/TLS.
- Sites using this protocol can be identified by the lock icon, usually visible in the address bar. It uses TCP port 443 by default.

Knowledge check.



Let's apply what we have covered:

- Describe protocols used to securely remotely manage computers.
- Describe the difference between implicit and explicit when securing communications.

Email.

EMAIL.

Key concepts.

In this section, we will cover the following key concepts:

- SMTP.
- SMTPS.
- STARTTLS.
- S/MIME.
- POP3/POP3S.
- IMAP/IMAPS.

aci LEARNING

EMAIL.

SMTP.

Simple Mail Transfer Protocol (SMTP) transfers email from a local email program to the SMTP server.

SMTP is also used for message relays between SMTP servers or Message Transfer Agents (MTA). SMTP is unencrypted and runs over TCP port 25.

EMAIL.

SMTPS.

- Simple Mail Transfer Protocol over SSL/TLS (SMTPS), also referred to as Implicit TLS, uses SSL/TLS to encrypt email communications.
- SMTPS uses TCP port 465.
- This implementation is no longer recommended.

EMAIL.

STARTTLS.

- Secure implementation of SMTP, often referred to as Explicit TLS or opportunistic TLS, is used for mail delivery from an email client program to the email server. STARTTLS requires authentication before message submission.
- Email clients, also known as Mail Submission Agents (MSA), use TCP port 587 to submit messages to the SMTP server for transmission.

aci LEARNING

EMAIL.

S/MIME.

Secure/Multipurpose Internet Mail Extensions (S/MIMEs) are used for sending digitally signed and encrypted messages. S/MIME uses RSA for encryption. The digital signature verifies you as the legitimate sender (non-repudiation and integrity) and encrypts the message (confidentiality).

This is used specifically on the email client, not the email server; it allows each email to be encrypted from the moment it is sent from the email client.

EMAIL.

POP3 and POP3S.

- Post Office Protocol, currently in version 3, is an early protocol used to download emails from the email server to the local email program over TCP port 110.
- This is useful only if you have one device that will receive the emails.
- Communications are not encrypted, including the user's login credentials.

CONTINUED ON NEXT SLIDE >

aci LEARNING

EMAIL.

POP3 and POP3S.

Post Office Protocol over SSL/TLS (POP3S) provides encrypted email downloads from an email server to the local email client over TCP port 995.

This is useful only if you have one device that will receive the emails.

EMAIL.

IMAP and IMAPS.

- Internet Message Access Protocol (IMAP) is an email retrieval protocol that addresses some limitations of POP and provides mailbox management features such as creating folders.
- IMAP sends a copy of an email from the server to multiple devices, leaving the main message on the mail server; this is why you can view your email on many devices.
- IMAP (currently in version 4) uses TCP port 143.
- This version is not secure, as messages are not encrypted.

CONTINUED ON NEXT SLIDE >

aci LEARNING

EMAIL.

IMAP and IMAPS.

- Secure implementation of IMAP, IMAPS is an email retrieval protocol that uses TCP port 993. All communications are encrypted via an SSL/TLS tunnel.
- IMAPS is used to send copies of emails from the server to multiple devices.

EMAIL.

Knowledge check.

Let's apply what we have covered:

- How do POP and IMAP differ? How are they the same?
- What are MTA and MSA used for when describing the SMTP protocol?

Voice and Database.

VOICE AND DATABASE.

Key concepts.

In this section, we will cover the following key concepts:

- SIP/SIPS.
- RTP and RCTP.
- SRTP and RCTPS.
- MS SQL/Oracle.

VOICE AND DATABASE.

Session Initiation Protocol (SIP/SIPS).

When configuring Voice over IP (VoIP) and Video Telecommunication (VTC) solutions, use different protocols throughout the lifecycle of VoIP communications; these include:

- Session Control.
- Data Transport.
- Quality of Service.

Session Initiation Protocol (SIP) is a widely-used protocol that provides session management – creation and tear-down. It uses UDP port 5060.

CONTINUED ON NEXT SLIDE >

VOICE AND DATABASE.

Session Initiation Protocol (SIP/SIPS).

SIP addresses are used to identify specific endpoint addresses. Examples include:

- sip:jane.bloggs@212.123.456
- sip:support@telcoystem.xyz.com
- sip:22449832@telcosystem.xyz.com:6000

Secured SIP communications are established using SSL/TLS in SIPS using UDP port 5061.

VOICE AND DATABASE.

RTP/SRTP and RTCP/SRTCP.

Real-Time Transport Protocol (RTP) is a communications protocol utilizing UDP to transport audio, video, and media data minimizing packet loss and jitter.

Real-Time Transport Control Protocol (RTCP) monitors transmission statistics and controls data regarding the call to aid in transmission quality.

AES is used by both protocols for security (SRTP and SRTCP).

VOICE AND DATABASE.

Databases.

Microsoft SQL uses TCP port 1433 by default.

Oracle databases use TCP port 1521 by default.

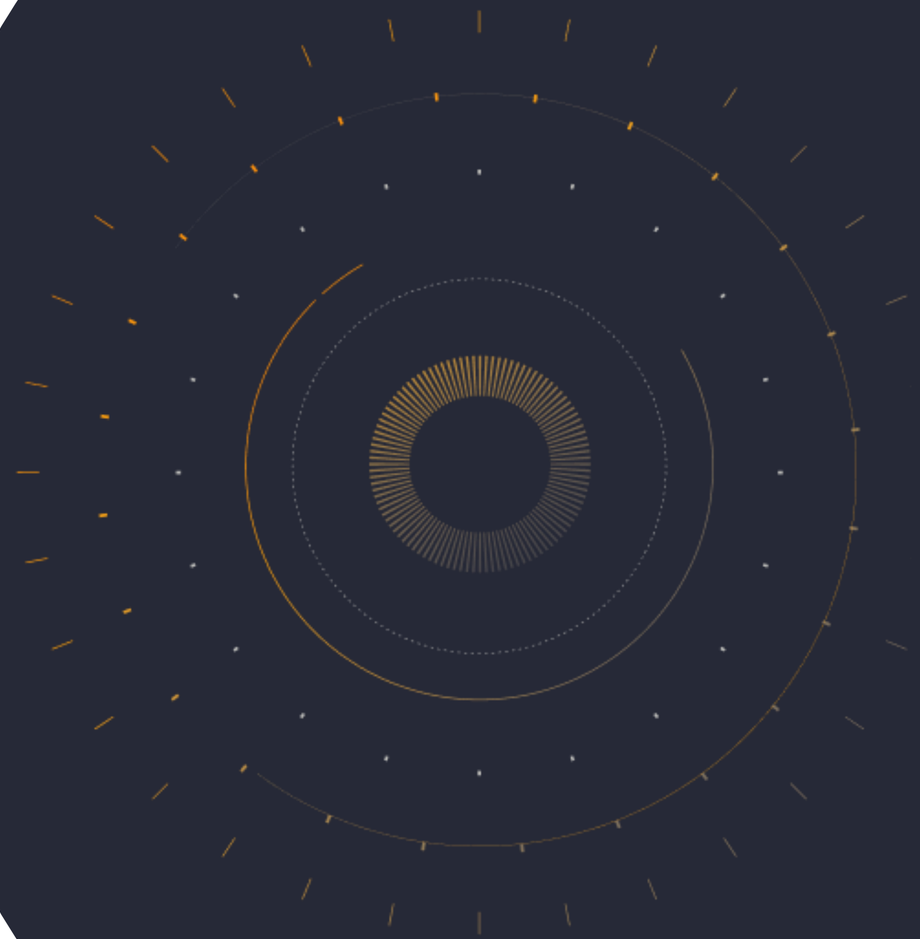
MySQL uses TCP port 3306 by default.

PostgreSQL uses TCP port 54323 by default.

Note: Database connections are not secure by default. Secure transmission of database connections needs to be set up using TLS. Self-signed digital certificates should not be used.

VOICE AND DATABASE.

Knowledge check.



Let's apply what we have covered:

- What protocol initiates VoIP communication?
- Describe how to secure database communications to a web server.

Authentication protocols.

AUTHENTICATION PROTOCOLS.

Key concepts.

In this section, we will cover the following key concepts:

- 802.1X.
- RADIUS.
- TACACS+.
- PAP.

aci LEARNING

AUTHENTICATION PROTOCOLS.

Key concepts.

In this section, we will also cover the following key concepts:

- CHAP.
- EAP.
- Kerberos.
- IPSec.

aci LEARNING

AUTHENTICATION PROTOCOLS.

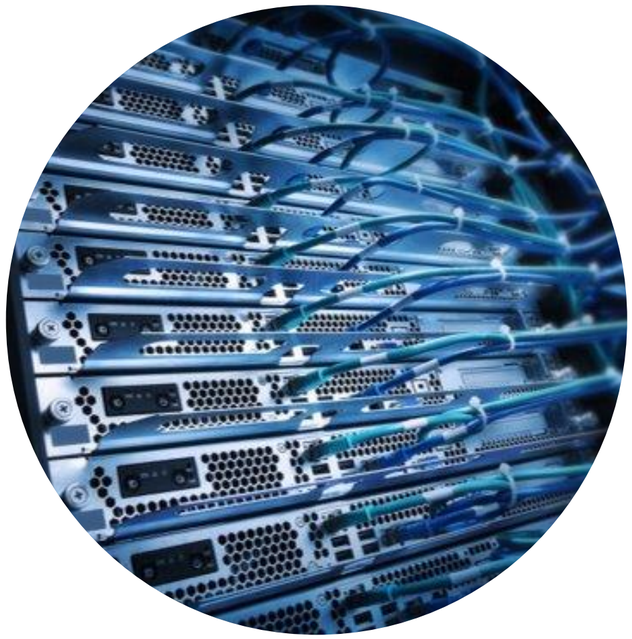
802.1X.

802.1x is an enterprise-level authentication standard that can use numerous authentication methods.

The components for 802.1X authentication include a supplicant, authenticator, and authenticating server.

AUTHENTICATION PROTOCOLS.

Remote Authentication Dial-In User Service (RADIUS).

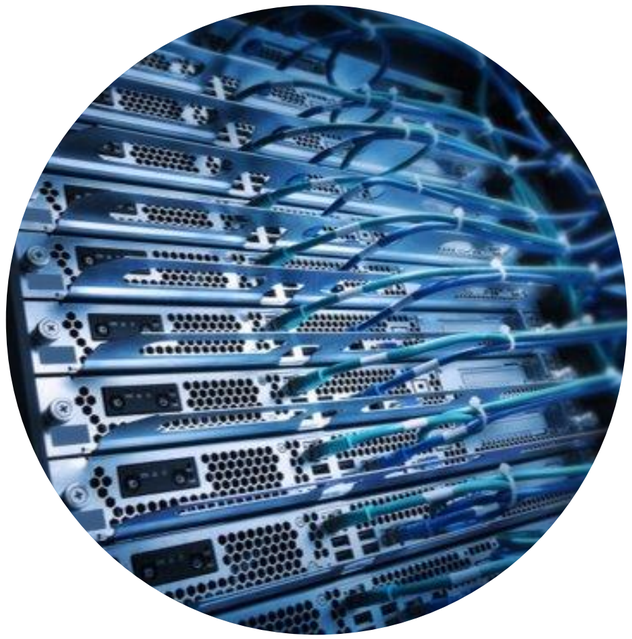


- Remote Authentication Dial-In User Service (RADIUS) is a protocol, but the term is typically used to describe a RADIUS server. RADIUS provides Authentication, Authorization, and Accounting (AAA) services.
- When a user attempts to log onto a network, the supplicant device will connect to an authenticator (VPN, WAP, etc.), which acts as an intermediary to authenticating server (RADIUS server).

CONTINUED ON NEXT SLIDE >

AUTHENTICATION PROTOCOLS.

Remote Authentication Dial-In User Service (RADIUS).



- The RADIUS server will respond by allowing or denying given the set of credentials.
- RADIUS uses UDP ports 1812 and 1813 and encrypts only the password.

AUTHENTICATION PROTOCOLS.

Terminal Access Controller Access-Control System (TACACS+).

TACACS+, or Terminal Access Controller Access-Control System, is the Cisco-developed alternative to the RADIUS authentication protocol. TACACS+ servers use TCP port 49 and act as the main authentication server for many Cisco devices and networks.

TACACS+ encrypts the username and password.

AUTHENTICATION PROTOCOLS.

PAP and CHAP.

Password Authentication Protocol (PAP): Sends a user's credentials in cleartext; it is not to be used for secure communications.

Challenge Handshake Authentication Protocol (CHAP): While still sending credentials using cleartext, this protocol adds shared secrets and hashing.

1. Server sends the client a challenge (key).
2. Client combines the key and its password. The result is hashed using MD5 and sent to the server.
3. Server compares hashes since it knows both the key and the client's password.

MS-CHAP: Microsoft's early implementation of CHAP used MD4 and encrypted all traffic from the client to the server.

MS-CHAPv2: Provides for mutual authentication and uses stronger keys.

AUTHENTICATION PROTOCOLS.

Extensible Authentication Protocol (EAP).

- Extensible Authentication Protocol (EAP) is an authentication framework for LANs. Many protocols and devices use EAP for authentication on a network.
- EAP has evolved into more specific versions, such as EAP-FAST, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-MSCHAPv2, etc.
- EAP allows for multiple login methods such as smartcards, certificates, and Kerberos; it is frequently used with RADIUS for RAS, wireless, and VPN solutions.

AUTHENTICATION PROTOCOLS.

Kerberos and IPSec.

Kerberos was developed by MIT. It is an open-source authentication protocol that provides time-sensitive authentication.

Kerberos is the default for Microsoft Active Directory.

CONTINUED ON NEXT SLIDE >

The components of Kerberos include:

- Authentication Server.
- Ticket-Granting Service.
- Network Service

The Authentication Server and the Ticket-Granting Service are often combined into a single Key Distribution Center (KDC).

Kerberos uses TCP port 88.

AUTHENTICATION PROTOCOLS.

Kerberos and IPSec.

Internet Security (IPSec) is a security protocol that encrypts IP traffic regardless of the application. In transport mode, only the payload is encrypted; in tunnel mode, the header and payload are encrypted.

Cryptography is accomplished using Authentication Header (AH), which authenticates the sender, or Encapsulating Security Payload (ESP), which encrypts the data.

IPSec uses UDP port 500.

AUTHENTICATION PROTOCOLS.

Knowledge check.

Let's apply what we have covered:

- Does RADIUS or TACACS+ encrypt only the password?
- Which IPSec communication mode encrypts the header and data?

End of Module.

For additional practice, please complete all associated self-study activities and labs.