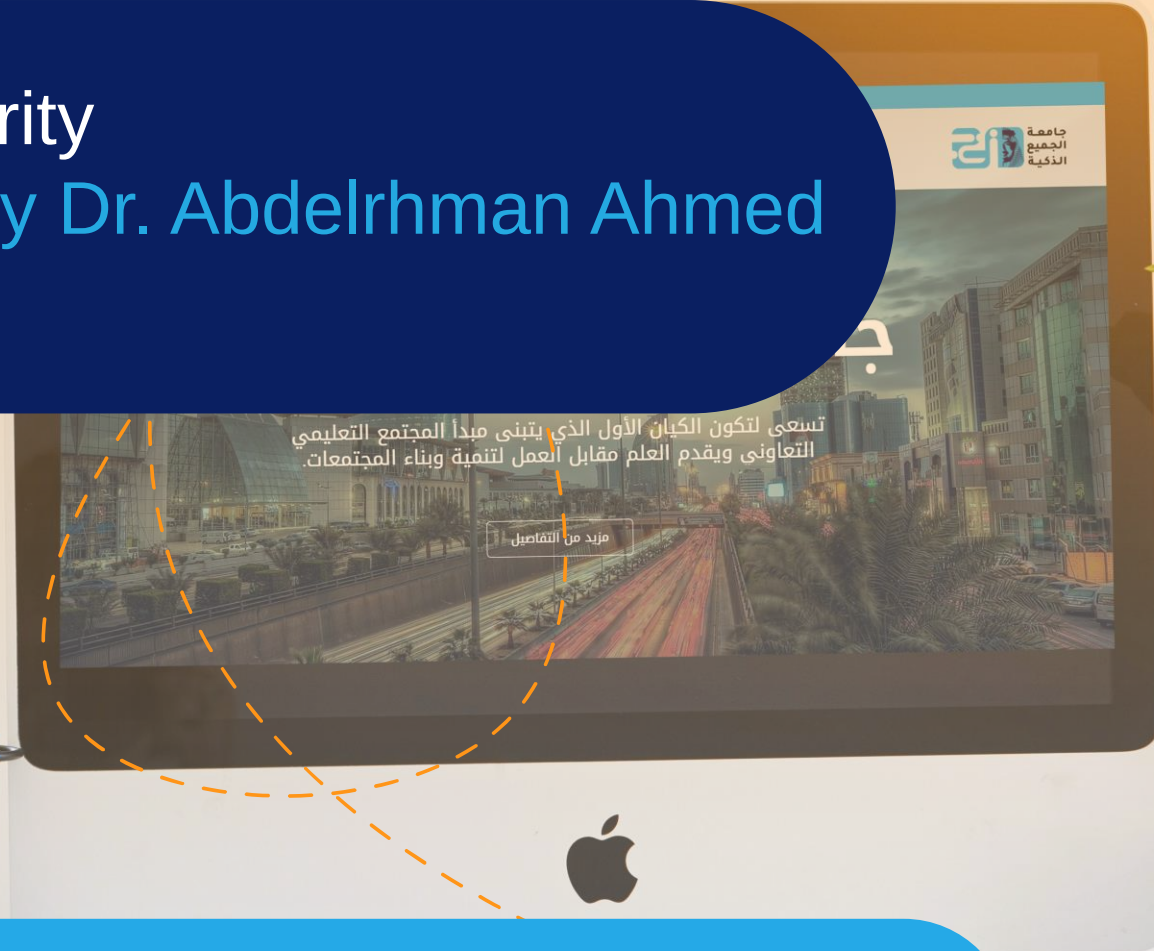


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 3

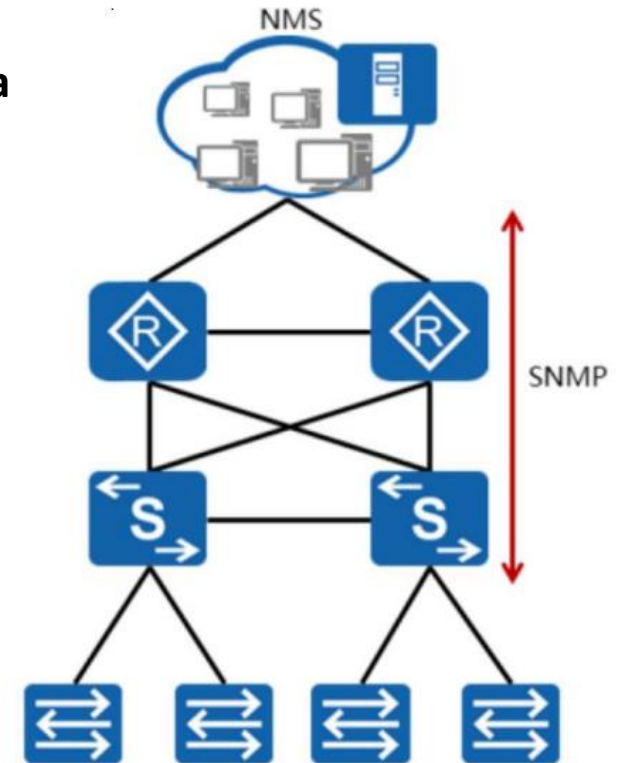


جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Common Network Protocols

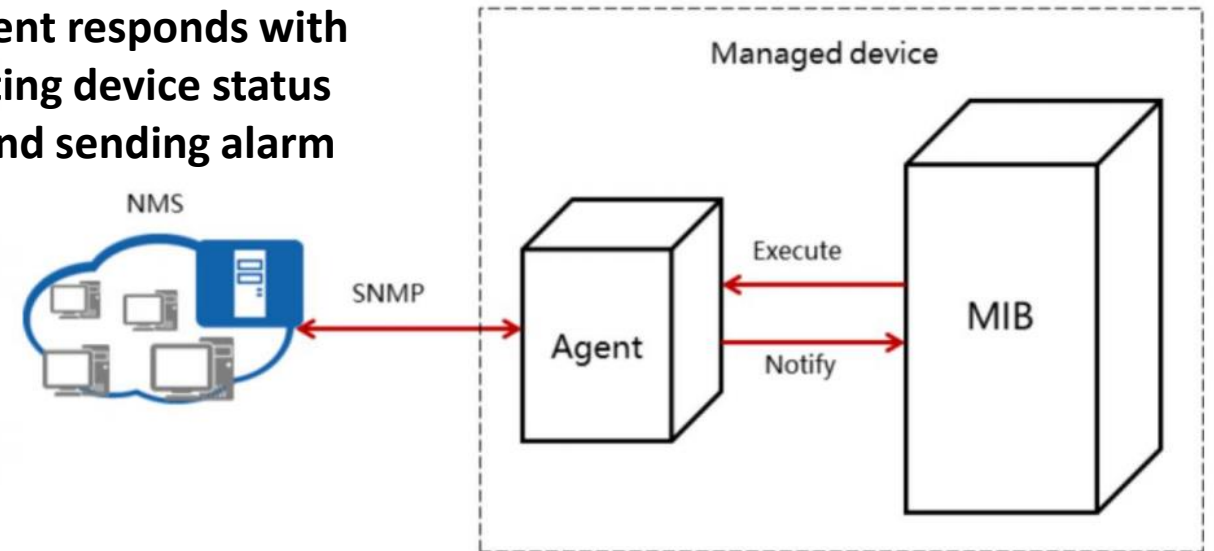
Introduction to SNMP

- **SNMP** is used to transmit management information between the network management system (NMS) and managed devices.
- **SNMP** is a network management protocol widely used in TCP/IP networks. It enables a network management workstation that runs the NMS to manage network devices.
- **SNMP** supports the following operations:
 - ❑ The NMS sends configuration information to network devices through SNMP.
 - ❑ The NMS queries and obtains network resource information through SNMP.
 - ❑ Network devices proactively report alarm messages to the NMS so that network administrators can quickly respond to network issues

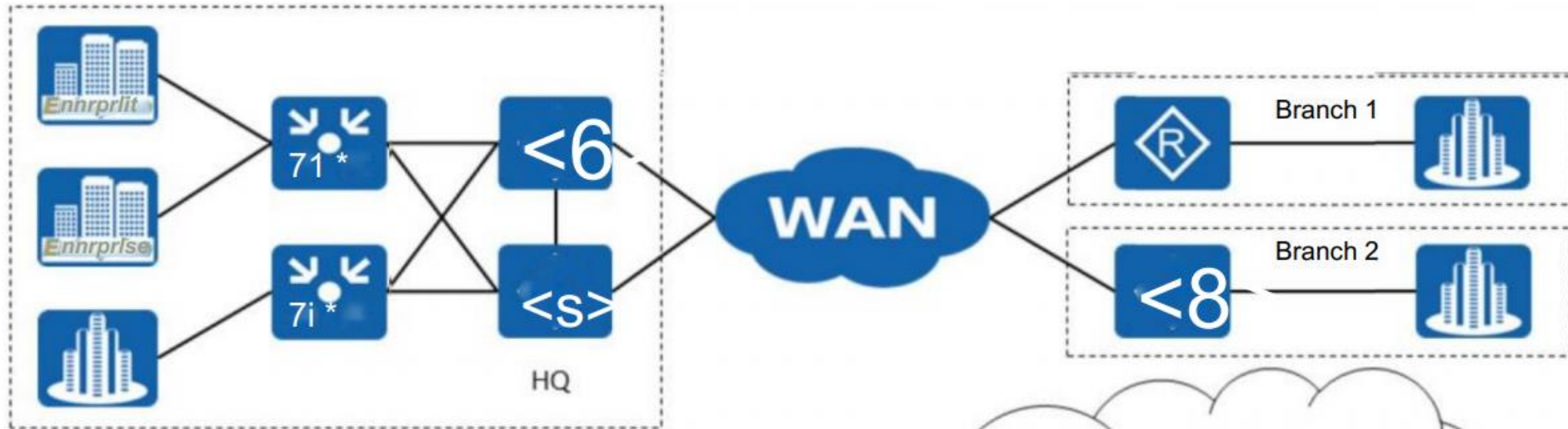


SNMP Architecture

- SNMP includes the NMS, agent, and MIB.
- An agent is a process performed on the managed devices.
- A MIB is a database that contains variables maintained by managed devices.
- The NMS is network management software running on a workstation. It enables network administrators to monitor and configure managed network devices.
- An agent is a network management process running on a managed device. After the managed device receives a request sent from the NMS, the agent responds with operations. The agent provides the following functions: collecting device status information, enabling the NMS to remotely operate devices, and sending alarm messages to the NMS.



- A MIB is a virtual database of device status information maintained on a managed device. An agent searches the MIB to collect device status information.
- Multiple versions of SNMP are available. Typically, these versions are as follows:
 - ❑ **SNMPv1:** Easy to implement but has poor security.
 - ❑ **SNMPv2c:** The security is low. It is not widely used.
 - ❑ **SNMPv3:** Defines a management framework to provide a secure access mechanism for users.
- **SNMPv1:** The NMS on the workstation and the Agent on the managed device exchange SNMPv1 packets to manage the managed devices.
- Compared with SNMPv1, SNMPv2c has greatly improved its performance, security, and confidentiality.
- **SNMPv3** has an enhanced security and management mechanism based on SNMPv2. The architecture used in SNMPv3 uses a modular design and enables administrators to flexibly add and modify functions. SNMPv3 is highly adaptable and applicable to multiple operating environments. It can not only manage simple networks and implement basic management functions, but also provide powerful network management functions to meet the management requirements of complex networks.



- Understand the traffic trend of all branches and identify the devices and branches that need expansion.
- Analyze the distribution of branch traffic identify the value points for capacity expansion.
- Rank changes in branch traffic and allocate existing network resources accordingly.

IT engineer: Branch 1 has exhausted its bandwidth on the XYZ port. We need to purchase a new device to expand the network capacity.
 Supervisor: Are you sure we need to expand the capacity? Is the network fully optimized or is the service application developing rapidly?
 IT engineer: I have detailed network application development reports for each branch



- **Basic concept**

- The eSight Network Traffic Analyzer (NTA) is a software-only solution. No hardware probe is required, and no additional investment is needed. The NetFlow, NetStream, and sFlow protocols are used to collect and analyze common IP packets, provide a customer analysis report, and monitor network-wide traffic in real time. This is a powerful tool for enterprise O&M management.

- **Functions**

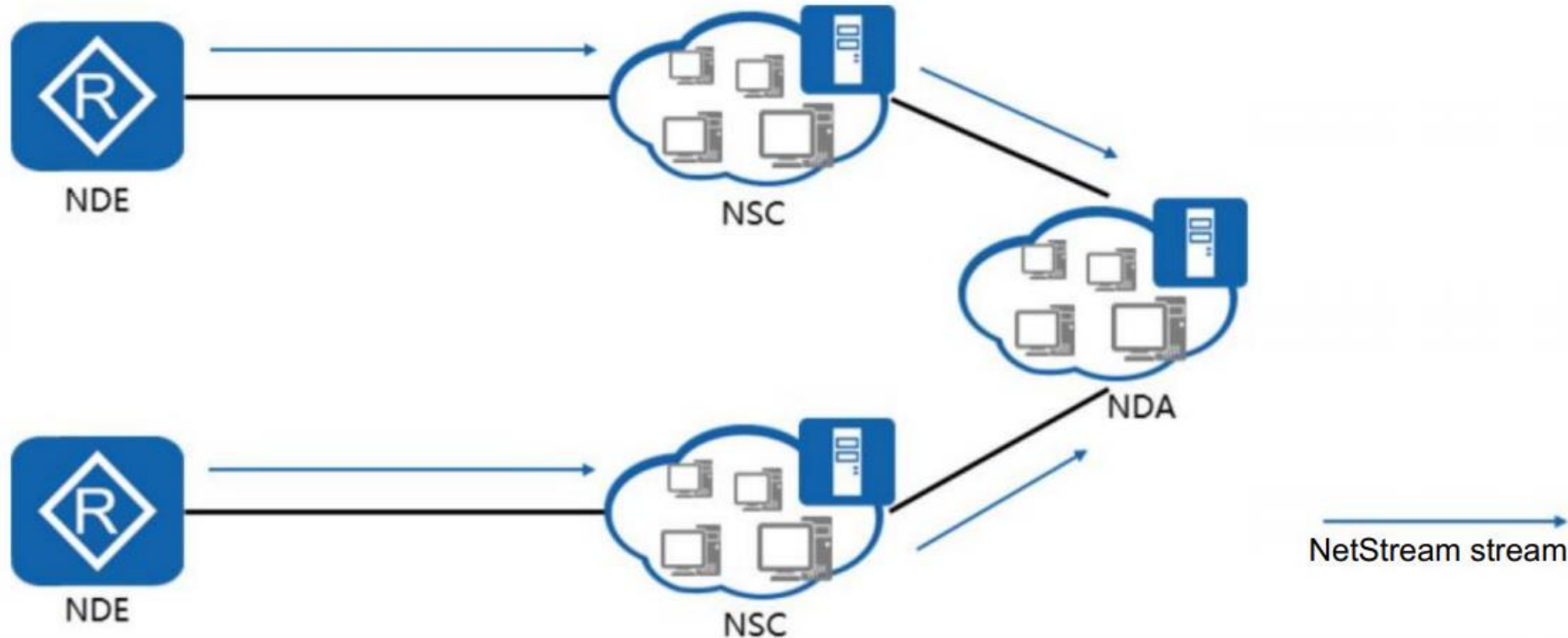
- The eSight NTA provides a convenient way to monitor and analyze networks. By using the IP network traffic information provided by network devices that support NetFlow, NetStream, and sFlow, the eSight NTA analyzes network-wide traffic, provides traffic analysis reports, and displays traffic analysis results in various charts. This helps users learn about network-wide traffic, including the traffic distribution, and detect abnormal network traffic.

- The eSight NTA provides users with reliable and convenient traffic analysis solutions, monitors network-wide traffic in real time, and provides multi-dimensional traffic analysis reports. This solution helps users detect abnormal traffic in a timely manner and learn about both network bandwidth usage and traffic distribution. In addition, it helps enterprises implement traffic visualization, fault query, and planning.

- **Features:**

- ☐ **Traffic visualization:** Monitors IP traffic in real time, displays the network traffic trend, and helps administrators detect and handle exceptions in a timely manner.
- ☐ **Exception detectability:** Through the NTA, users can analyze and audit the original IP traffic to identify the root cause of abnormal traffic.
- ☐ **Proper planning:** The traffic trend and customized reports provided by the NTA provide reference for administrators to plan network capacity.

NetStream is a Huawei-patented technology used to collect and distribute statistics about network traffic. The NDE sends the obtained statistics to the NSC for further processing and sends the statistics to the NDA for analysis. The results of the analysis provide a basis for network accounting and planning.



- **NetStream provides data that is useful for many purposes, including:**

- ❑ Network management and planning
- ❑ Enterprise accounting and departmental charging
- ❑ ISP billing report
- ❑ Data storage
- ❑ Data mining for marketing purposes

- **NetStream is implemented using the following devices:**

- ❑ **NetStream Data Exporter (NDE):** Samples the traffic and exports the traffic statistics.
- ❑ **NetStream Collector (NSC):** Parses packets from the NDE and sends statistics to the database for the NDA to parse.
- ❑ **NetStream Data Analyzer (NDA):** Analyzes and processes the statistics, generates reports, and provides a foundation for various services, such as traffic charging, network planning, and monitoring.

- **The NetStream system works as follows:**

- ❑ **NDE** configured with the NetStream function periodically sends the collected traffic statistics to the NSC.
- ❑ **NSC** processes the traffic statistics and sends them to the NDA.
- ❑ **NDA** analyzes the data for applications such as charging and network planning.



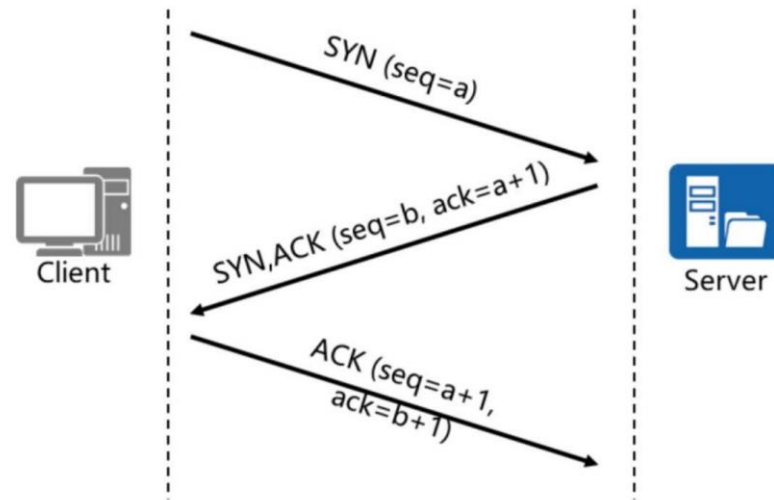
- To establish a connection, TCP uses a three-way handshake process. This process is used to confirm the start sequence number of the communications parties so that subsequent communications can be performed in an orderly manner. The process is as follows:

n When the connection starts, the client sends a SYN to the server. The client sets the SYN's sequence number to a random value a .

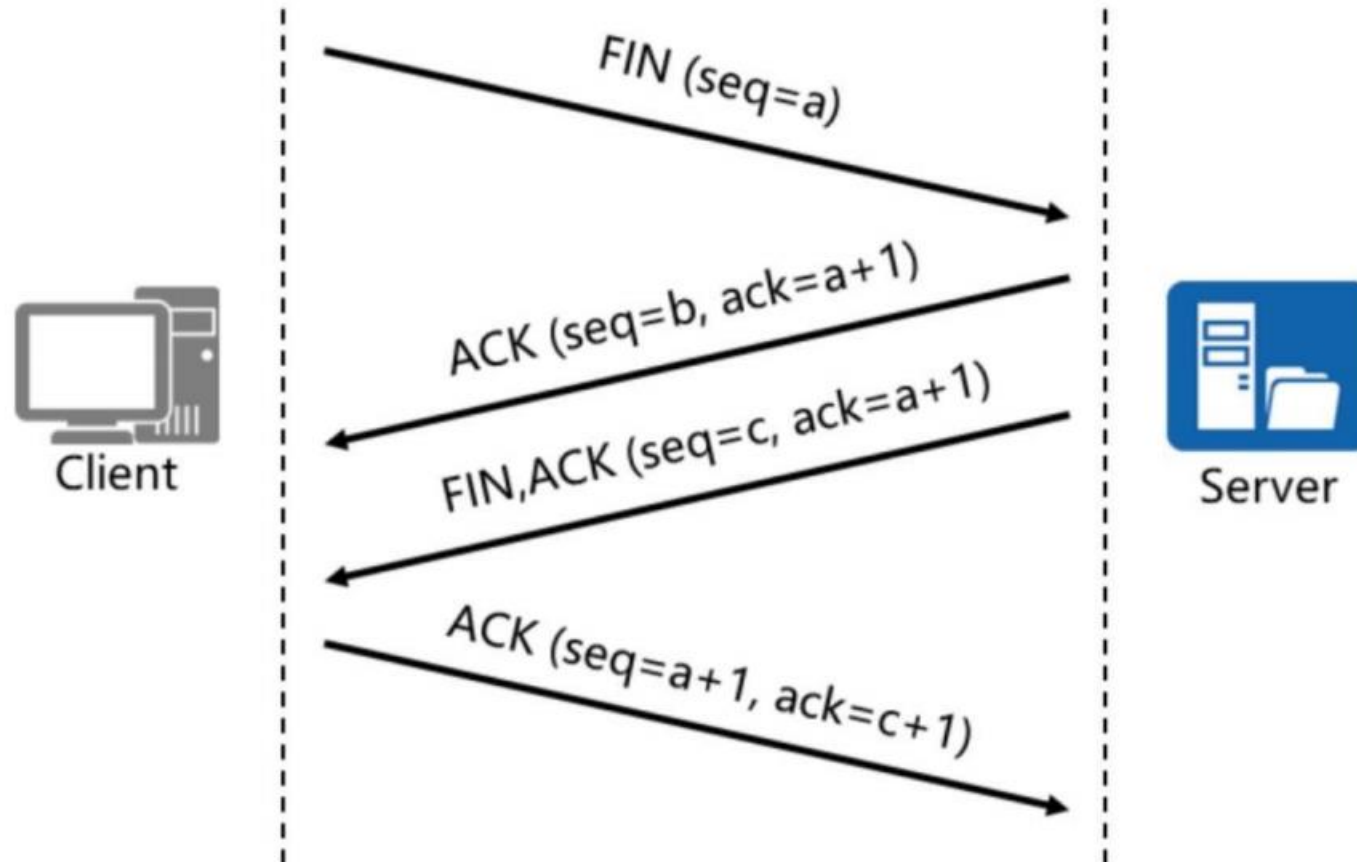
- After receiving the SYN, the server replies with a SYN+ACK. The server sets the ACK's acknowledgment number as the received sequence number plus one (that is, $a + 1$), and the SYN's sequence number as a random value b .

- After receiving the SYN+ACK, the client replies with an ACK. The client sets the ACK's acknowledgment number as the received sequence number plus one (that is, $b+1$).

- Three-way handshake



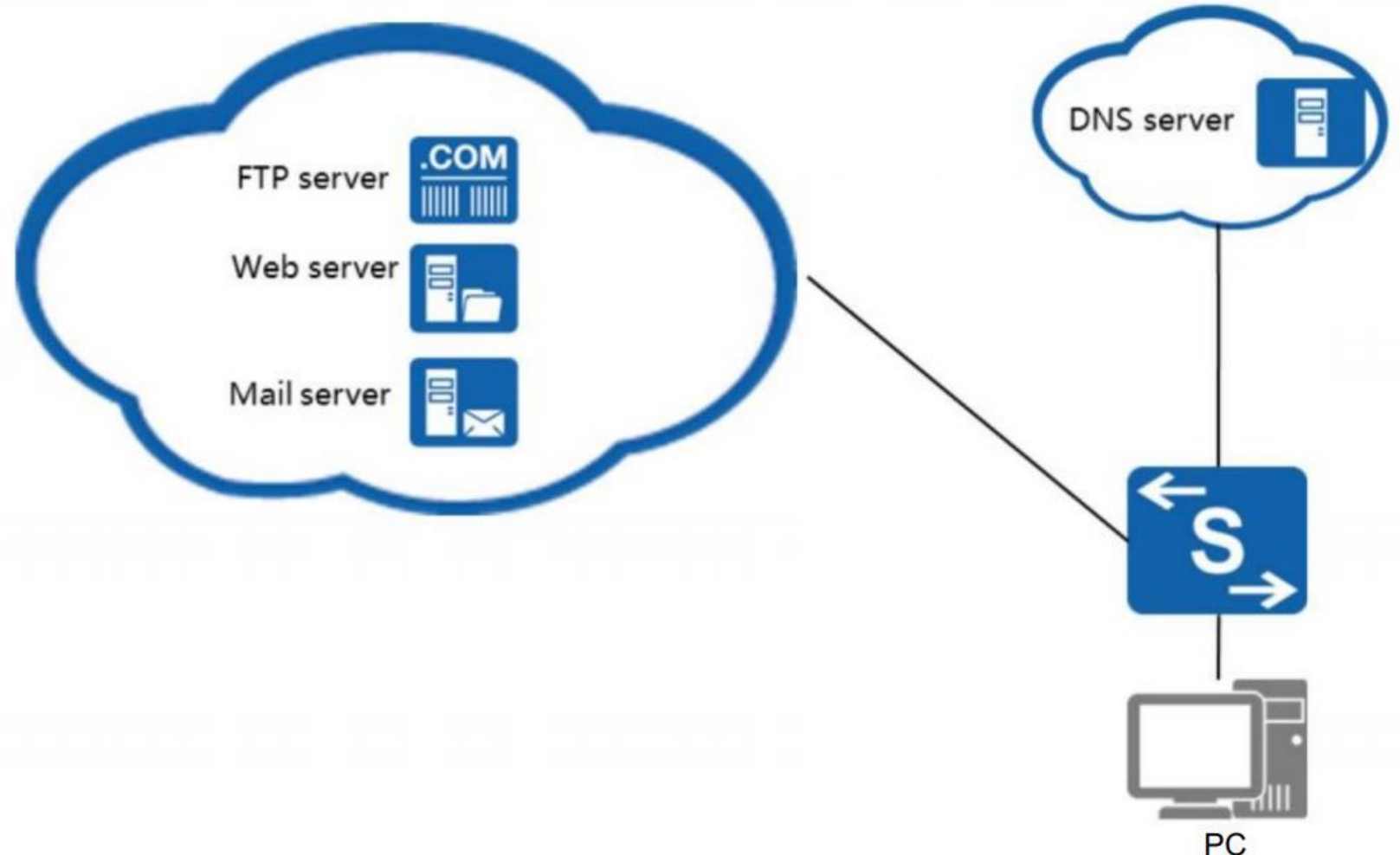
- 4-way handshake



- To terminate a connection, TCP uses a four-way handshake process. The process is as follows:

- ❑ The client sends a connection release packet (FIN = 1) to the server and stops sending data. The client sets the FIN's sequence number as a (seq=a) and enters the FIN-WAIT-1 state.
- ❑ After receiving the FIN, the server replies with an acknowledgement packet (ACK=1). The server sets the ACK's acknowledgement number as the received sequence number plus one (ack=a + 1), sets the sequence number as b, and enters the CLOSE-WAIT state.
- ❑ After receiving the ACK, the client enters the FIN-WAIT-2 state and waits for the server to send a FIN.
- ❑ After the server finishes sending any remaining data, it sends a connection release packet to the client: FIN = 1; ack=a + 1. Because the connection is in the half-closed state, the server may send more data. Assume that the sequence number is seq=c. The server then enters the LAST-ACK state and waits for acknowledgement from the client.
- ❑ After receiving the connection release packet from the server, the client replies with an acknowledgement packet (ACK=1). The client sets the acknowledgement number to ack=c+1 and sequence number to seq=a + 1. The client then enters the TIME-WAIT state.
- ❑ After receiving the ACK from the client, the server enters the CLOSED state immediately and ends the TCP connection.

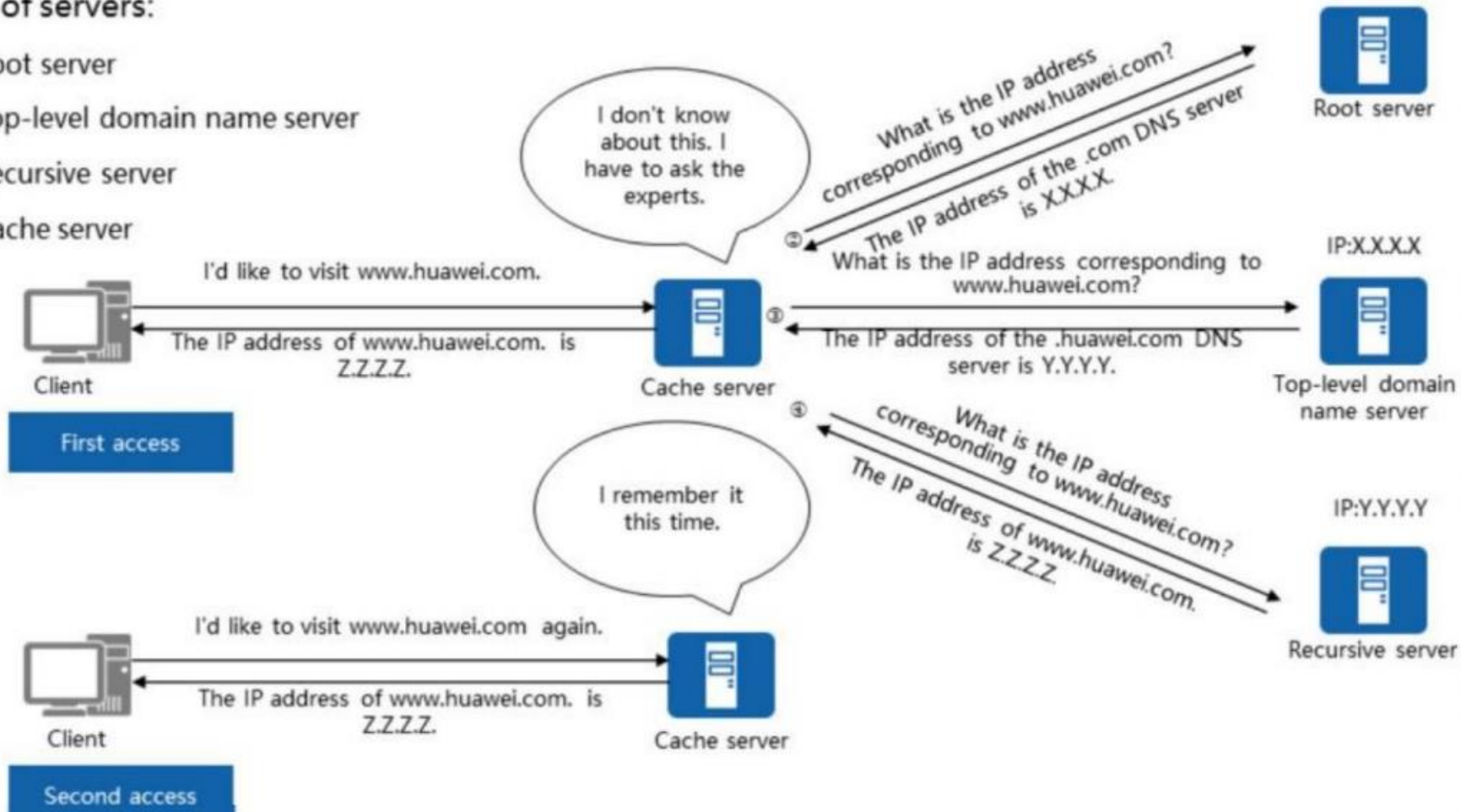
- **HTTP/HTTPS:** refers to Hypertext Transfer Protocol, which is a protocol used to browse web pages.
- **FTP protocol:** refers to File Transfer Protocol, which is used to upload and download file resources.
- **DNS protocol:** refers to Domain Name Resolution Protocol, which is used to resolve domain names to IP addresses.



- Domain name resolution is performed by a dedicated domain name system (DNS). The DNS involves the following:

types of servers:

- Root server
- Top-level domain name server
- Recursive server
- Cache server

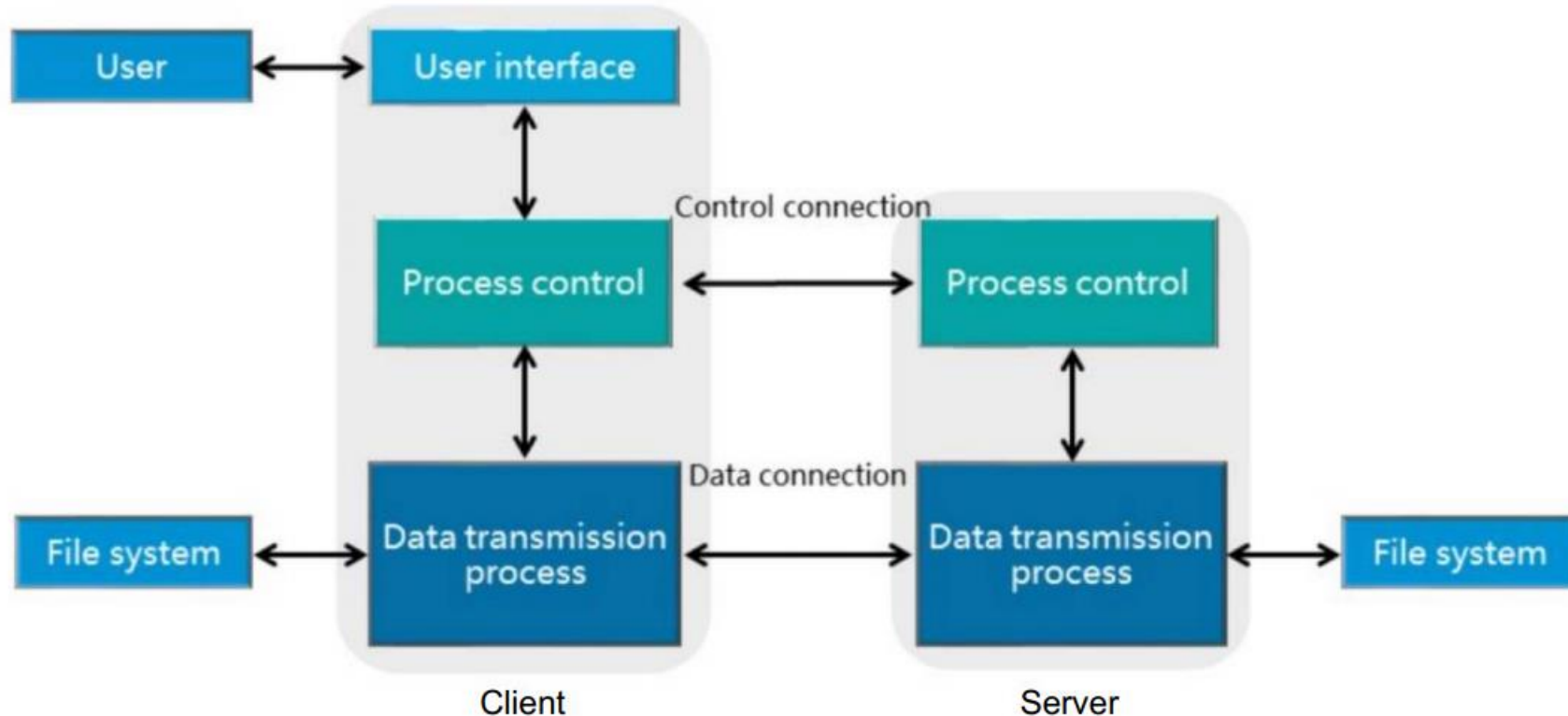


- A root server is primarily used to manage the main directory of the Internet. The number of root servers are limited to 13 server addresses in the world. Among the 13 nodes, 10 are set in the United States, and the other three are in the UK, Sweden and Japan. Although the network has no borders, servers still have national boundaries. All root servers are managed by the Internet domain name and number allocation agency ICANN, which is authorized by the US government.
- A top-level domain name server is used to store top-level domain names such as .com, .edu, and .cn.
- A recursive server is an authoritative server. It stores definitive domain name records (the resolution relationship between a domain name and an IP address) for the zone in which it servers. If every person accessing the Internet were to send requests to an authoritative server, the server would be overloaded. Therefore, a cache server is necessary.
- A cache server is equivalent to a proxy of the authoritative server and reduces the pressure of the authoritative server. Each time a user accesses the Internet, a request for domain name resolution is sent to the cache server. Upon receiving this request for the first time, the cache server requests the domain name and IP address resolution table from an authoritative server, and then stores the table locally. Subsequently, if a user requests the same domain name, the cache server directly replies to the user. The IP address of a website does not often change. However, entries in the resolution table are valid only for a certain period. When the validity period expires, the entry is automatically aged. The system queries the authoritative server again if a user request is sent. This aging mechanism ensures that the domain name resolution on the cache server is updated periodically.

The resolution process of DNS is as follows:

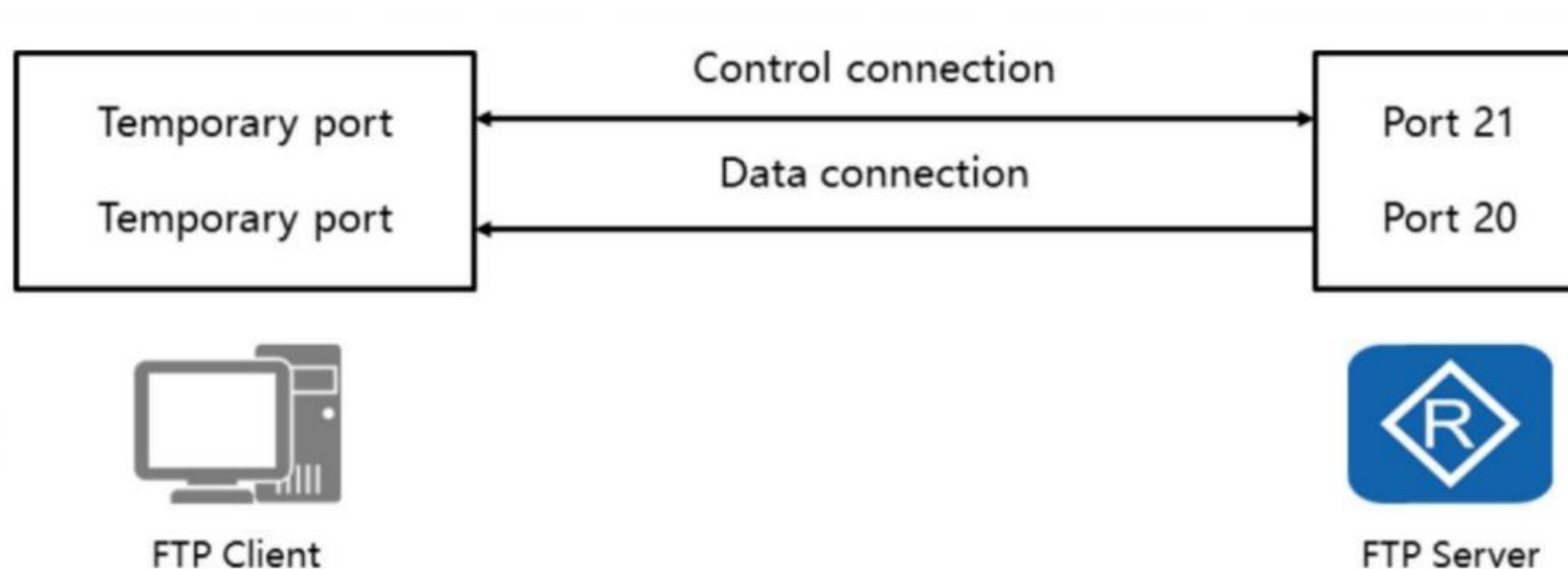
- ❑ The DNS client queries in recursive mode. The cache server first checks whether the local DNS server has the domain name resolution cache.
- ❑ If there is no local cache, the domain name is sent to the root server. After receiving the `www.vmall.com` request, the root server checks the authorization of the `.com` and returns the IP address of the top-level domain name server where the `.com` is located.
- ❑ The cache server continues to send a `www.vmall.com` resolution request to the top-level domain name server. After receiving the request, the top-level domain name server returns the recursive server IP address of the next-level `.vmall.com`.
- ❑ The cache server continues to send a `www.vmall.com` resolution request to the recursive server. After receiving the request, the recursive server returns a resolution address of `www.vmall.com`. If there are a large number of domain names, the recursive server also has multiple levels.
- ❑ After obtaining the IP address of `www.vmall.com`, the cache server sends the IP address to the client and caches the IP address locally.
- ❑ If a client requests the domain name resolution of `www.vmall.com` again, the cache server directly responds with the IP address.

- FTP provides an effective way to upload and download files between a server and a client.
- When used to transmit data, FTP establishes a control connection and a data connection between the server and the client..



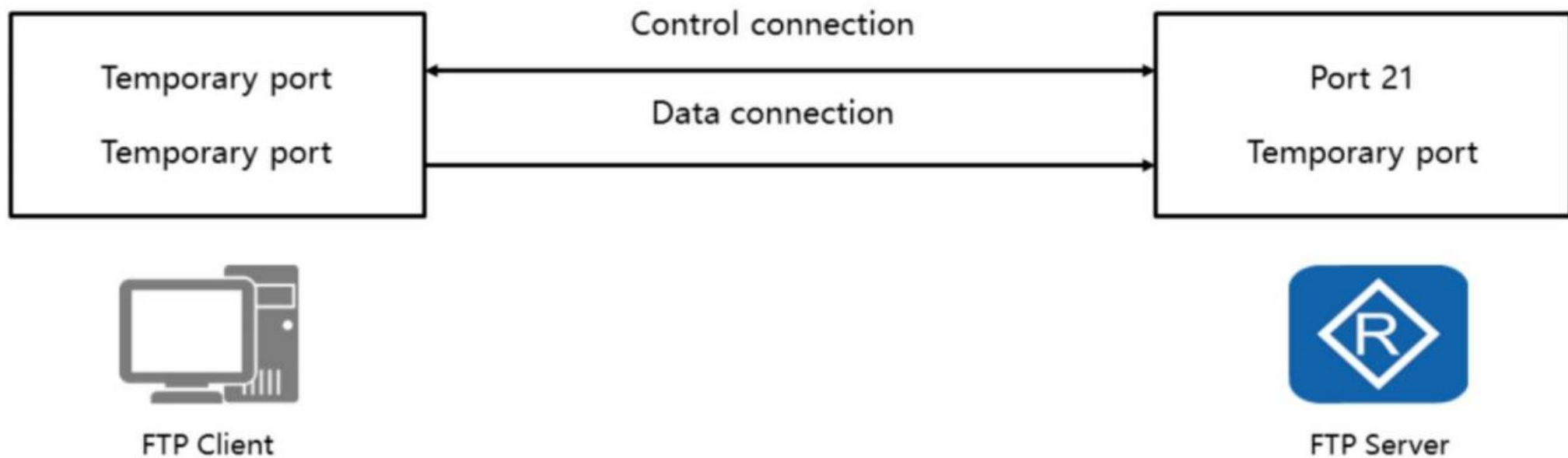
- When FTP is used to transfer files, two TCP connections are used. The first is the control connection between the FTP client and the FTP server. Enable port 21 on the FTP server and wait for the FTP client to send a connection request. The FTP client enables a random port and sends a connection setup request to the FTP server. The control connection is used to transfer control commands between the server and the client.
- The second is the data connection between the FTP client and the FTP server. The server uses TCP port 20 to establish a data connection with the client. Generally, the server actively establishes or interrupts data connections.
- Because the FTP is a multi-channel protocol, a random port is used to establish a data channel. If a firewall exists, the channel may fail to be set up. For details, see the following sections.

- FTP supports two modes: active mode and passive mode. In active mode, which is used by default, the client sets up the control connection and the server sets up the data connection. In passive mode, the client sets up both connections. Users can switch the mode through commands.
- FTP connection setup in active mode:



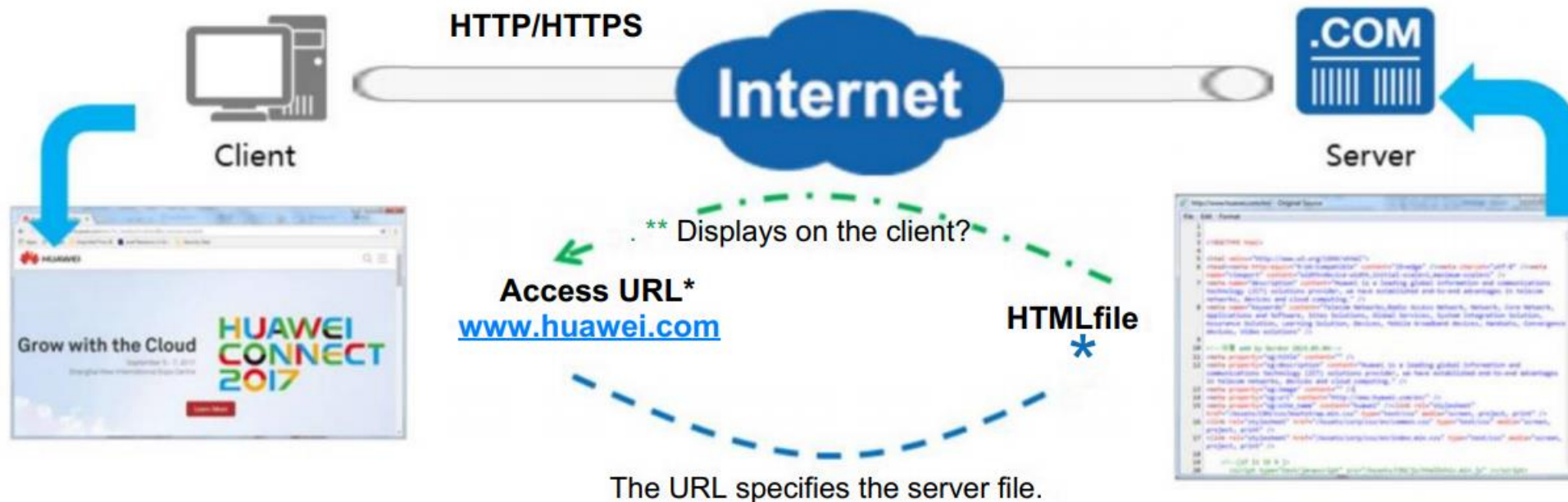
- In active mode, if a firewall is deployed, the data connection may fail to be established because it is initiated by the server. Passive mode solves this issue. The active mode facilitates the management of the FTP server but impairs the management of the client. The opposite is true in the passive mode.
- By default, port 21 of the server is used to transmit control commands, and port 20 is used to transmit data.
- The procedure for setting up an FTP connection in active mode is as follows:
 - n The server enables port 21 to listen for data and waits to set up a control connection with the client .
 - n The client initiates a control connection setup request, and the server responds,
 - n The client sends a PORT command through the control connection to notify the server of the temporary port number used for the client data connection.
 - n The server uses port 20 to establish a data connection with the client.

- FTP connection setup in passive mode:



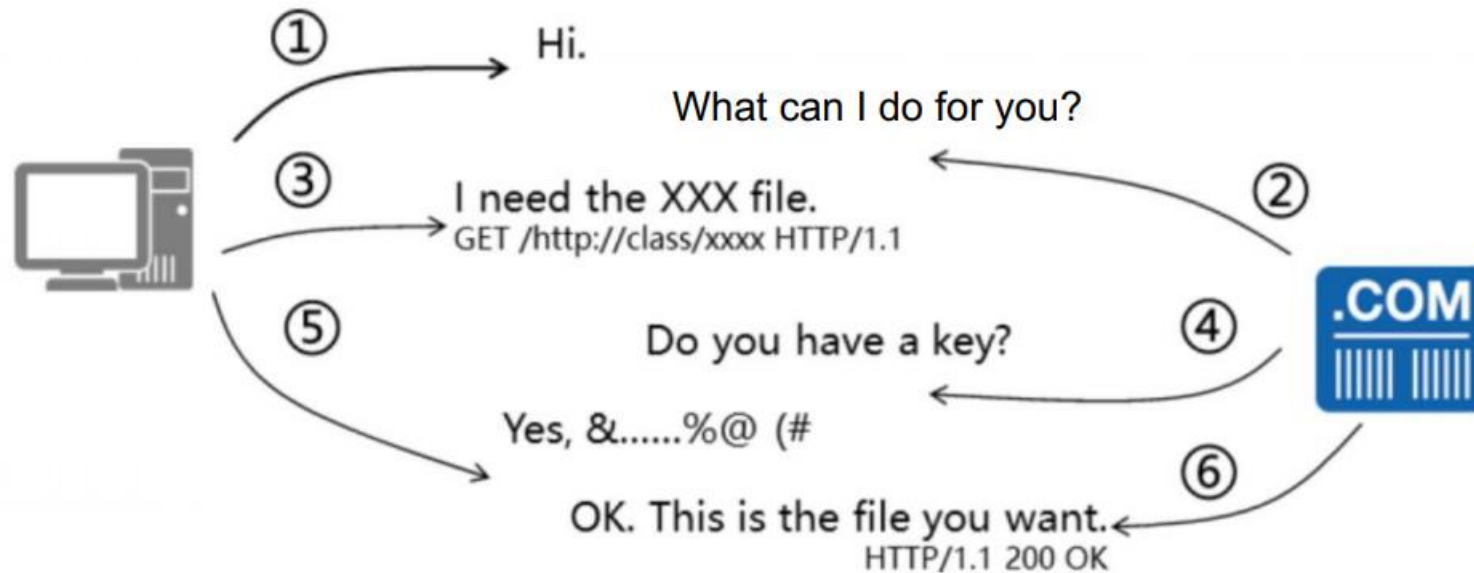
- The procedure for setting up an FTP connection in passive mode is as follows:
 - ❑ The server enables port 21 to listen for data and wait to set up a control connection with the client.
 - ❑ The client initiates a control connection setup request, and the server responds.
 - ❑ The client sends the PASV command through the control connection to notify the server that the client is in passive mode.
 - ❑ The server responds and informs the client of the temporary port number used for the data connection.
 - ❑ A data connection is set up between the client and the temporary port of the server.

- The web is built on a client-server architecture and relies on three essential technologies:
 - ❑ Using Hypertext Markup Language (HTML), used to describe a file
 - ❑ Using Uniform Resource Locator (URL), used to specify the file location
 - ❑ Using Hypertext Transfer Protocol (HTTP), used for client-server communication



- **WWW** is short for **World Wide Web**, also known as **3W** or **Web**. **Hypertext** is a holistic information architecture, which establishes links for the different parts of a document through keywords so that information can be searched interactively. **Hypermedia** is the integration of hypertext and multimedia.
- The Internet uses the combination of hypertext and hypermedia to extend the information link to the entire Internet. A web is a kind of hypertext information system. It enables the text to be switched from one position to another instead of being fixed at a certain position. The multi-link is a unique feature.
- HTTP relies on TCP to achieve connection-oriented state and does not have an encryption and verification mechanism. As a result, the security is insufficient. HTTPS is a secure version of HTTP and supports encryption. However, HTTPS can be used to hide malicious content that cannot be identified by security devices, which poses security risks on a network.

- HTTP is a stateless protocol that uses a request-response method for communication.
- HTTP has two types of packets:
 - Request packet: sent from the client to the server.
 - Response packet: returned from the server to the client.

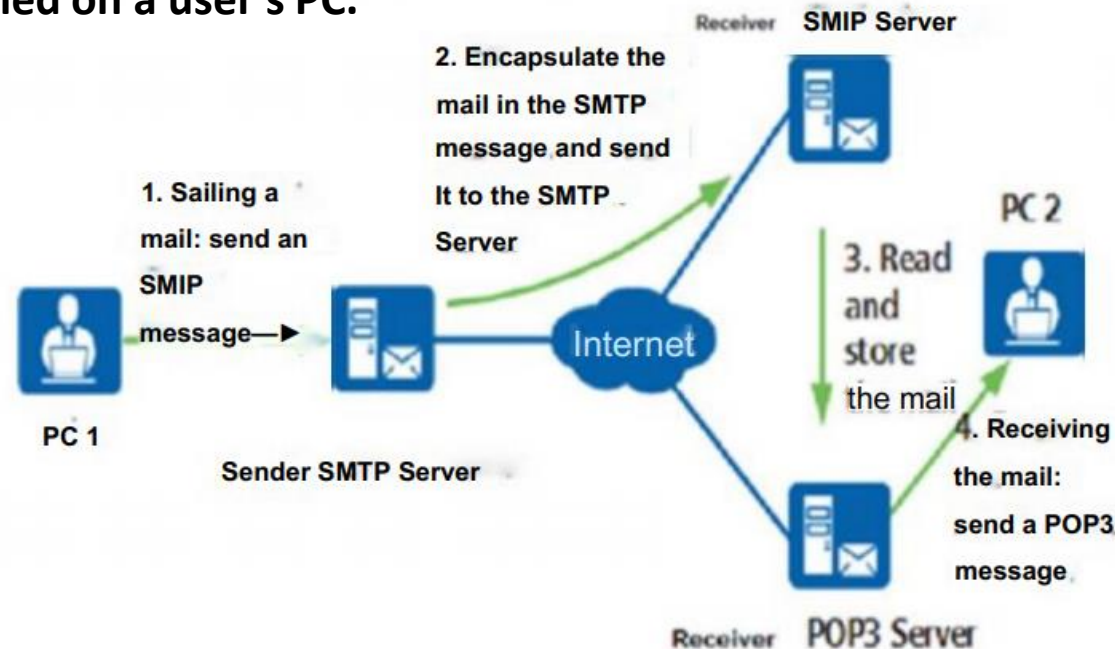


SMTP, POP3, IMAP: How Mail Is Sent and Received

- SMTP defines how PCs send mail to an SMTP server and how mail is transferred between SMTP servers.

Post Office Protocol 3 (POP3) and Internet Mail Access Protocol (IMAP) specify how PCs manage and download mail on the mail server through client software.

SMTP and POP3 (or IMAP) are deployed on the mail server by an administrator, and mail client software (such as Microsoft Outlook or Fox mail) is installed on a user's PC.



- **The mail sending process is as follows:**

1. The PC encapsulates the email content into an SMTP message and sends it to the sender's SMTP server.
2. The sender sends it to the recipient's SMTP server for storage.
3. After receiving the request from the user, the POP3 server obtains the email stored on the SMTP server.
4. The POP3 server encapsulates the email into a POP3 message and sends it to the PC.

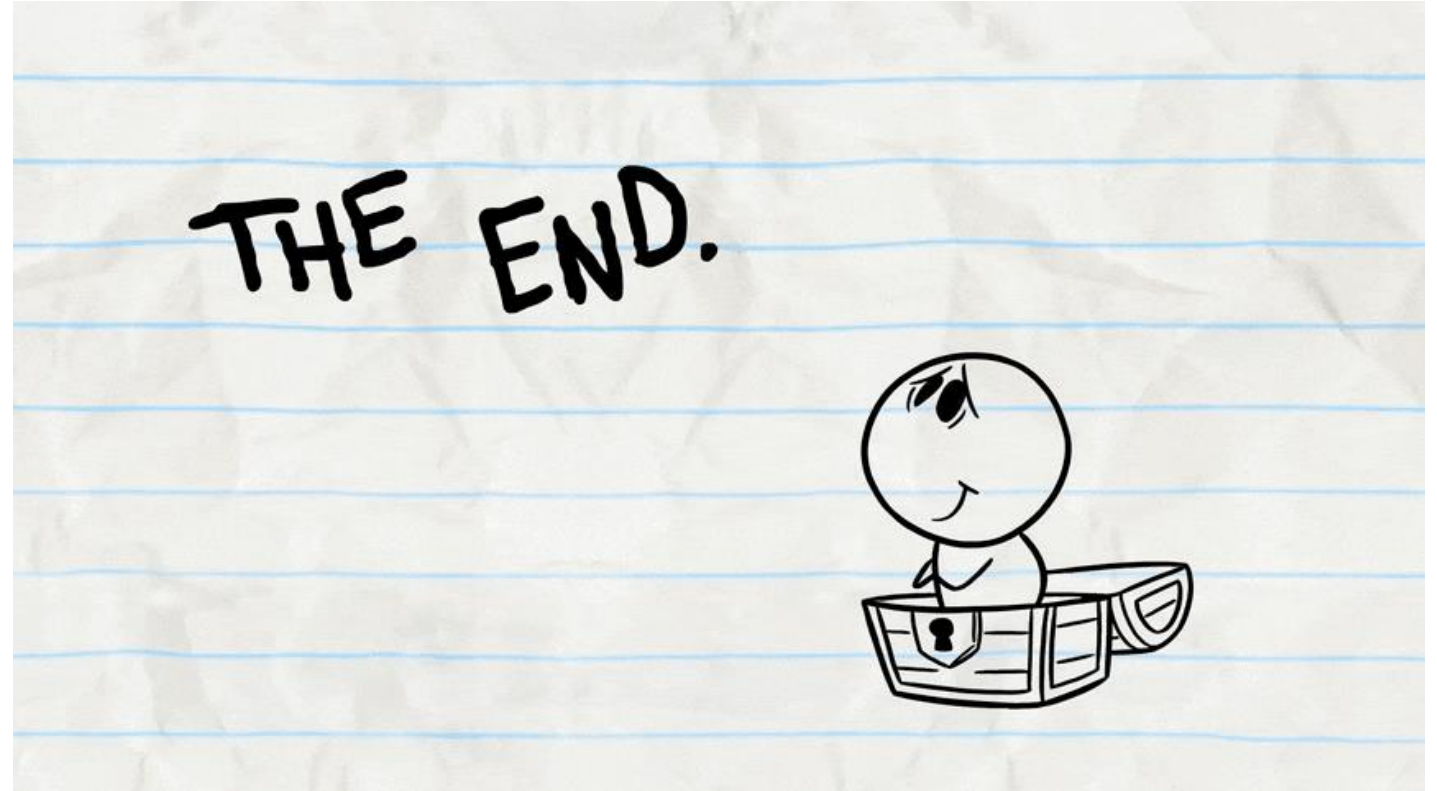
- SMTP Server, POP3 Server, and IMAP are management software that provides services for users and are deployed on hardware servers.

- The differences between IMAP and POP3 are as follows: When POP3 is used, after the client software downloads unread mails to the PC, the mail server deletes the mails. If IMAP is used, users can directly manage mails on the server without downloading all emails to the local PC.

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY