Fondamenti di Internet

Network Services and Applications

Prof. Gianluca Reali

Foreword

- The Internet has become an integral part of our lives, with a wide range of applications such as file transfer, email sending, online video, web browsing, and online gaming. Because of the layered network model, common users can use various services provided by the application layer, without knowing technical details such as communication technology implementations.
- In previous courses, we have learned technologies related to the data link layer, network layer, and transport layer. This chapter will describe common network services and applications such as FTP, DHCP, and HTTP.

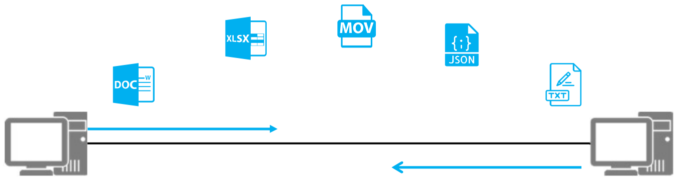
Objectives

- On completion of this course, you will be able to:
  - Understand FTP fundamentals.
  - Understand TFTP fundamentals.
  - Understand DHCP fundamentals.
  - Understand Telnet fundamentals.
  - Understand HTTP fundamentals.
  - Understand DNS fundamentals.
  - Understand NTP fundamentals.

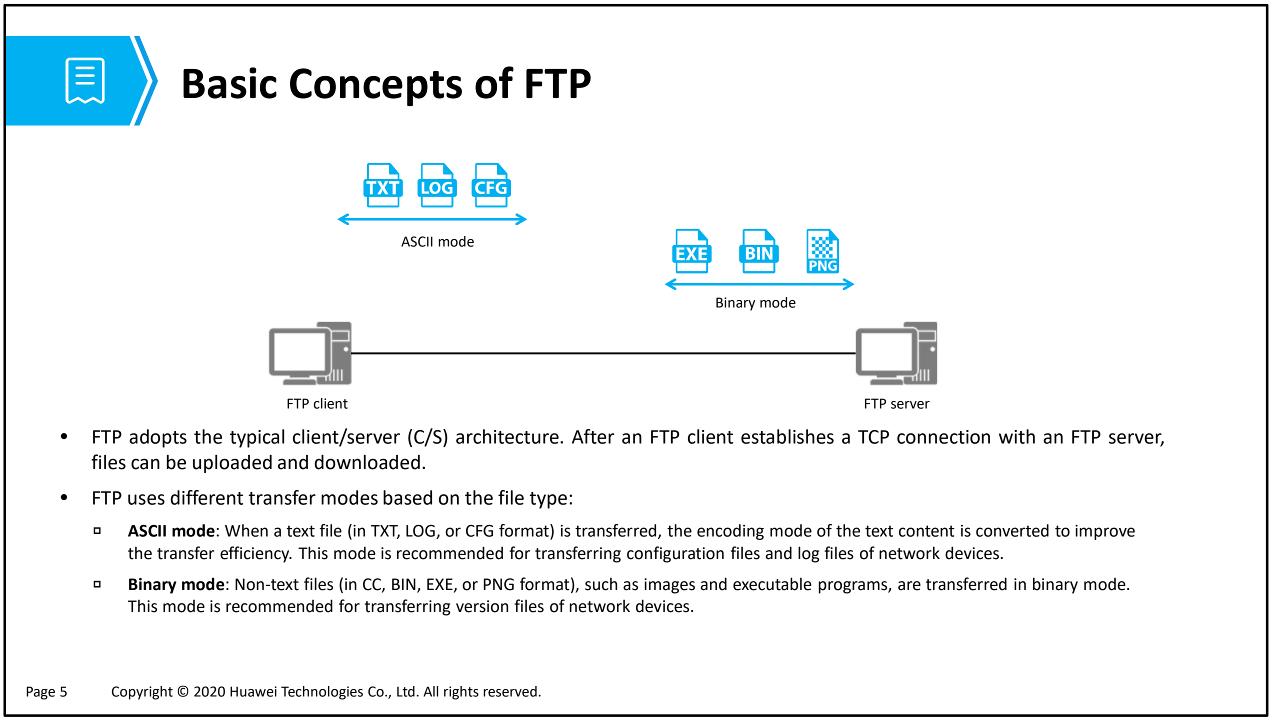
Contents

1. **File Transfer**
   - **FTP**
   - TFTP
2. Telnet
3. DHCP
4. HTTP
5. DNS
6. NTP

File Transfer Protocols



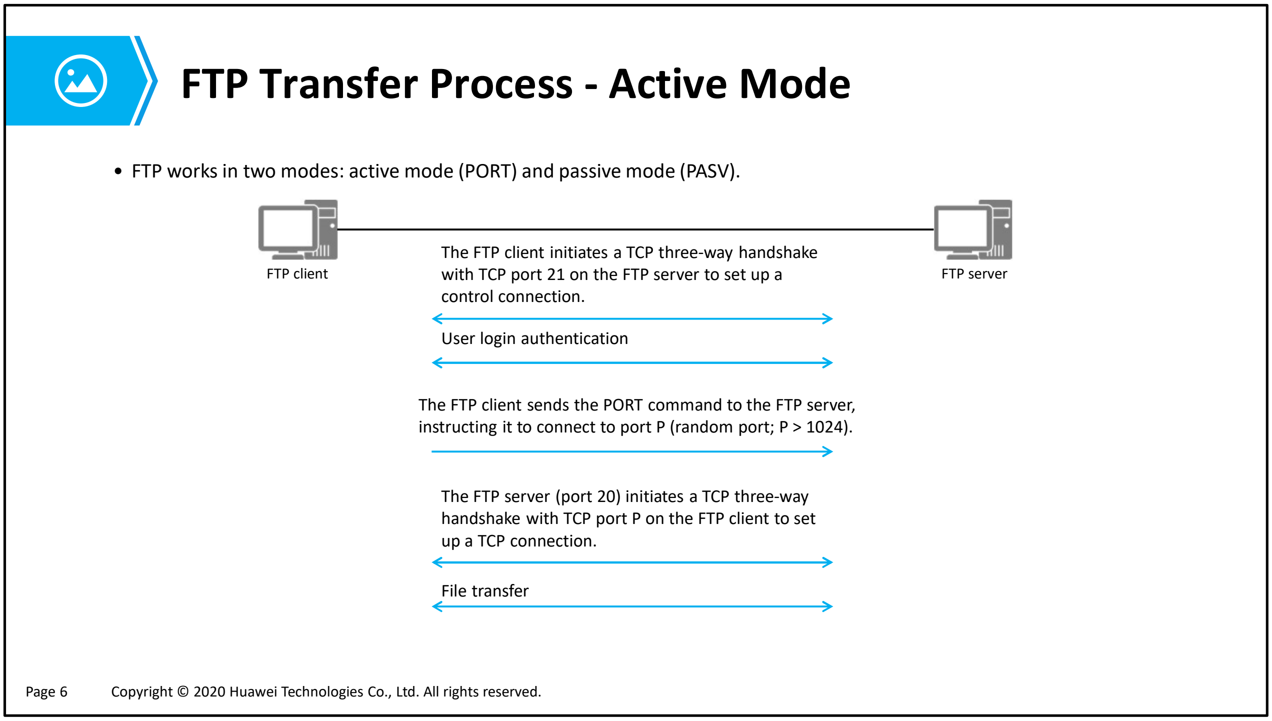
- File transfer between hosts is an important function of IP networks. Nowadays, people can conveniently transfer files using web pages and mailboxes.
- However, in the early Internet era when the World Wide Web (WWW) did not come into being and operating systems used command-line interfaces, people transferred files via command-line tools. The most commonly used protocols for transferring files at that time are File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP).



Basic Concepts of FTP

- FTP adopts the typical client/server (C/S) architecture. After an FTP client establishes a TCP connection with an FTP server, files can be uploaded and downloaded.
- FTP uses different transfer modes based on the file type:
  - **ASCII mode**: When a text file (in TXT, LOG, or CFG format) is transferred, the encoding mode of the text content is converted to improve the transfer efficiency. This mode is recommended for transferring configuration files and log files of network devices.
  - **Binary mode**: Non-text files (in CC, BIN, EXE, or PNG format), such as images and executable programs, are transferred in binary mode. This mode is recommended for transferring version files of network devices.

- FTP supports two transfer modes: ASCII and binary.
- The ASCII mode is used to transfer text files. In this mode, the sender converts characters into the ASCII code format before sending them. After receiving the converted data, the receiver converts it back into characters. The binary mode is usually used to send image files and program files. In this mode, the sender can transfer files without converting the file format.
- CC: VRP system file extension



FTP Transfer Process - Active Mode

- FTP works in two modes: active mode (PORT) and passive mode (PASV).

The FTP client initiates a TCP three-way handshake with TCP port 21 on the FTP server to set up a control connection.

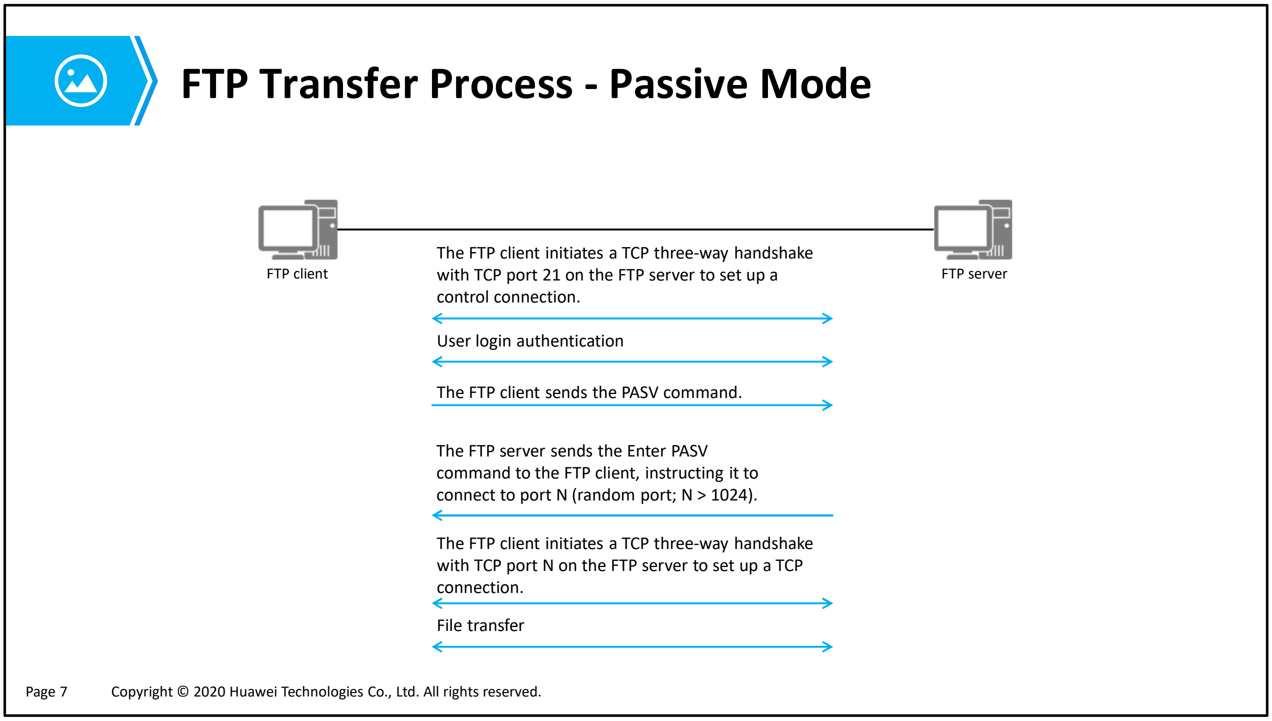
User login authentication

The FTP client sends the PORT command to the FTP server, instructing it to connect to port P (random port; P > 1024).

The FTP server (port 20) initiates a TCP three-way handshake with TCP port P on the FTP client to set up a TCP connection.

File transfer

- In active mode, the FTP client uses a random port (with the number greater than 1024) to send a connection request to port 21 of the FTP server. After receiving the request, the FTP server sets up a control connection with the FTP client to transmit control messages. In the meantime, the FTP client starts to listen on port P (another random port with the number greater than 1024) and uses the PORT command to notify the FTP server. When data needs to be transmitted, the FTP server sends a connection request from port 20 to port P of the FTP client to establish a TCP connection for data transmission.



FTP Transfer Process - Passive Mode

The FTP client initiates a TCP three-way handshake with TCP port 21 on the FTP server to set up a control connection.

User login authentication

The FTP client sends the PASV command.

The FTP server sends the Enter PASV command to the FTP client, instructing it to connect to port N (random port; N > 1024).

The FTP client initiates a TCP three-way handshake with TCP port N on the FTP server to set up a TCP connection.

File transfer

- In passive mode, the FTP client uses a random port (with the number greater than 1024) to send a connection request to port 21 of the FTP server. After receiving the request, the FTP server sets up a control connection with the FTP client to transmit control messages. In the meantime, the FTP client starts to listen on port P (another random port with the number greater than 1024) and uses the PASV command to notify the FTP server. After receiving the PASV command, the FTP server enables port N (a random port with the number greater than 1024) and uses the Enter PASV command to notify the FTP client of the opened port number. When data needs to be transmitted, the FTP client sends a connection request from port P to port N on the FTP server to establish a transmission connection for data transmission.
- The active mode and passive mode differ in data connection methods and have their own advantages and disadvantages.
  - In active mode, if the FTP client is on a private network and a NAT device is deployed between the FTP client and the FTP server, the port number and IP address carried in the PORT packet received by the FTP server are not those of the FTP client converted using NAT. Therefore, the FTP server cannot initiate a TCP connection to the private IP address carried in the PORT packet. In this case, the private IP address of the FTP client is not accessible on the public network.
  - In passive mode, the FTP client initiates a connection to an open port on the FTP server. If the FTP server lives in the internal zone of a firewall and inter-zone communication between this internal zone and the zone where the FTP client resides is not allowed, the client-server connection cannot be set up. As a result, FTP transfer fails.

Configuration Commands (Device as FTP Server)

A user accesses a device through FTP.

1. Enable the FTP server function.

```
[Huawei]ftp [ ipv6 ] server enable
```

   By default, the FTP server function is disabled.

2. Configure a local FTP user.

```
[Huawei]aaa
[Huawei]local-user user-name password irreversible-cipher password
[Huawei]local-user user-name privilege level level
[Huawei]local-user user-name service-type ftp
[Huawei]local-user user-name ftp-directory directory
```

   The privilege level must be set to level 3 or higher. Otherwise, the FTP connection fails.

Configuration Commands (Device as FTP Client)

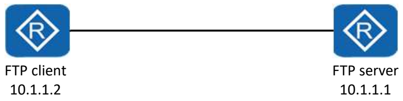
1. A VRP device that functions as an FTP client accesses an FTP server.

```
<FTP Client>ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):ftp
331 Password required for ftp.
Enter password:
230 User logged in.
```

2. Common commands used when the VRP device functions as an FTP client.

```
ascii     Set the file transfer type to ASCII, and it is the default type
binary    Set the file transfer type to support the binary image
ls        List the contents of the current or remote directory
passive   Set the toggle passive mode, the default is on
get       Download the remote file to the local host
put       Upload a local file to the remote host
```

Configuration Example



- One router functions as the FTP server, and the other as the FTP client.
- Enable the FTP service on the FTP server and create an FTP login account. Then, the FTP client logs in to the FTP server and runs the **get** command to download a file.

Configurations on the FTP server:

```
<Huawei> system-view
[Huawei] sysname FTP_Server
[FTP_Server] ftp server enable
[FTP_Server] aaa
[FTP_Server-aaa] local-user admin1234 password irreversible-cipher
Helloworld@6789
[FTP_Server-aaa] local-user admin1234 privilege level 15
[FTP_Server-aaa] local-user admin1234 service-type ftp
[FTP_Server-aaa] local-user admin1234 ftp-directory flash:
```

Operations on the FTP client:

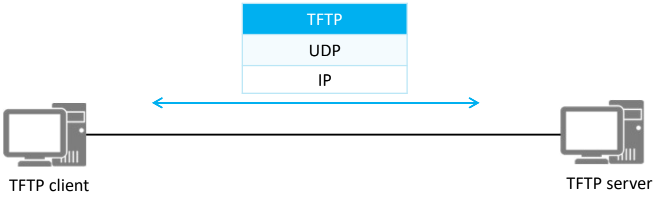
```
<FTP Client>ftp 10.1.1.1
[FTP Client-ftp]get sslvpn.zip
200 Port command okay.
FTP: 828482 byte(s) received in 2.990 second(s) 277.08Kbyte(s)/sec.
```

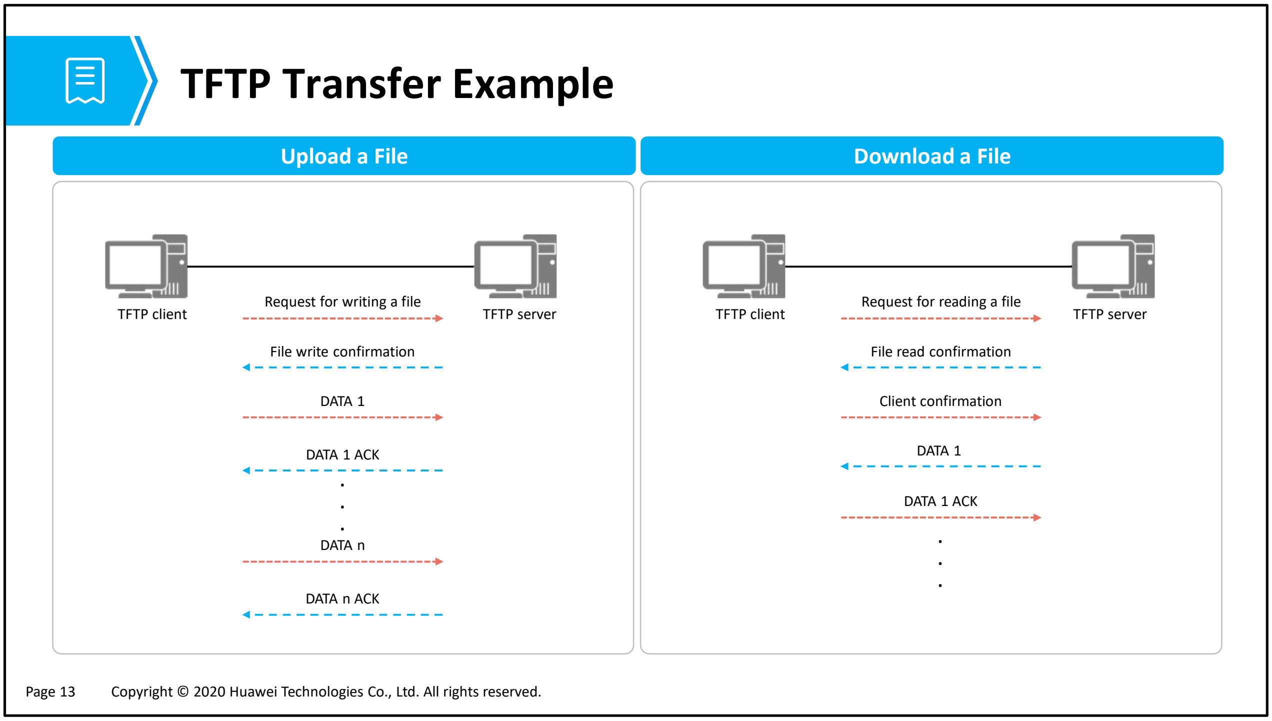
Contents

1. **File Transfer**
   - FTP
   - **TFTP**
2. Telnet
3. DHCP
4. HTTP
5. DNS
6. NTP

Basic Concepts of TFTP

- Compared with FTP, TFTP is designed to transfer small files and is easier to implement.
  - Using UDP (port 69) for transmission
  - Authentication not required
  - You can only request a file from or upload a file to the server, but cannot view the file directory on the server.





TFTP Transfer Example

Upload a File

TFTP client

TFTP server

Request for writing a file

File write confirmation

DATA 1

DATA 1 ACK

.
.
.

DATA n

DATA n ACK

Download a File

TFTP client

TFTP server

Request for reading a file

File read confirmation

Client confirmation

DATA 1

DATA 1 ACK

.
.
.

- TFTP supports five packet formats:
  - RRQ: read request packet
  - WRQ: write request packet
  - DATA: data transmission packet
  - ACK: acknowledgment packet, which is used to acknowledge the receipt of a packet from the peer end
  - ERROR: error control packet

Configuration Commands (Device as TFTP Client)

1. Download a file (VRP device functioning as a TFTP client).

   ```
   <HUAWEI> tftp tftp_server get filename
   ```

   You do not need to log in to the TFTP server, and only need to enter the IP address of the TFTP server and the corresponding command.

2. Upload a file (VRP device functioning as a TFTP client).

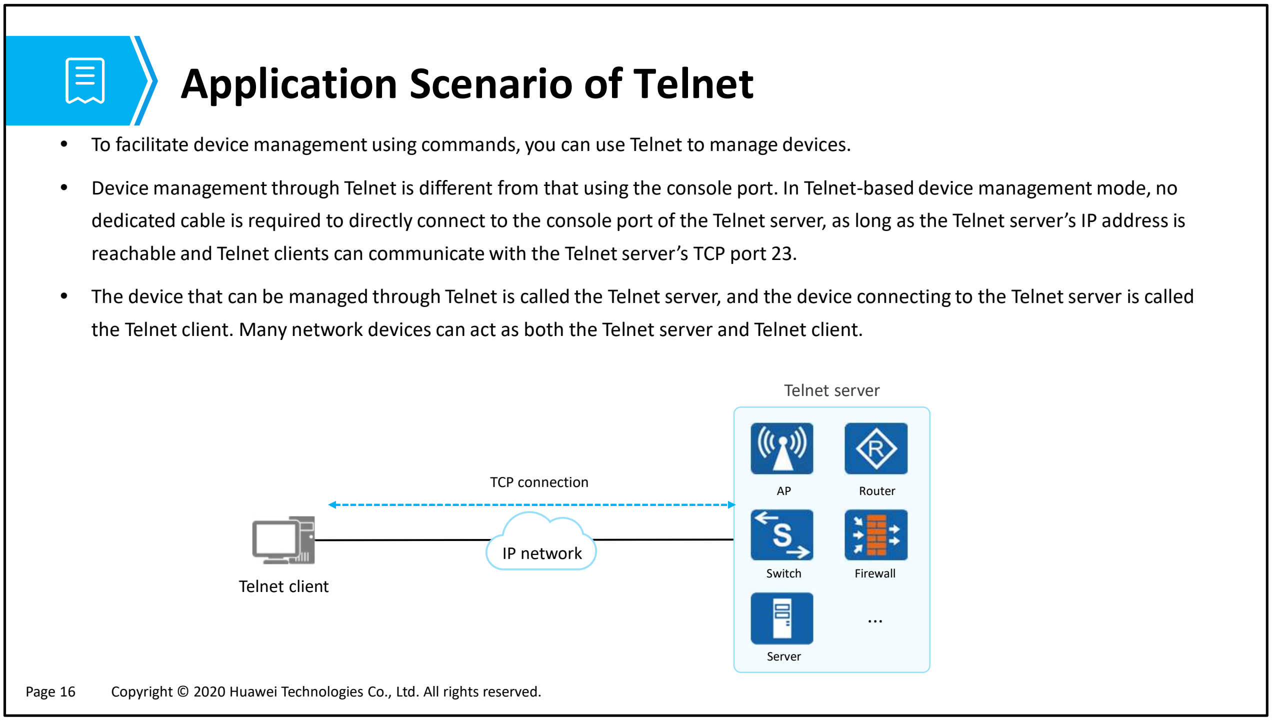
   ```
   <HUAWEI> tftp tftp_server put filename
   ```

   You do not need to log in to the TFTP server, and only need to enter the IP address of the TFTP server and the corresponding command.

   Currently, VRP devices can function only as TFTP clients.

Contents

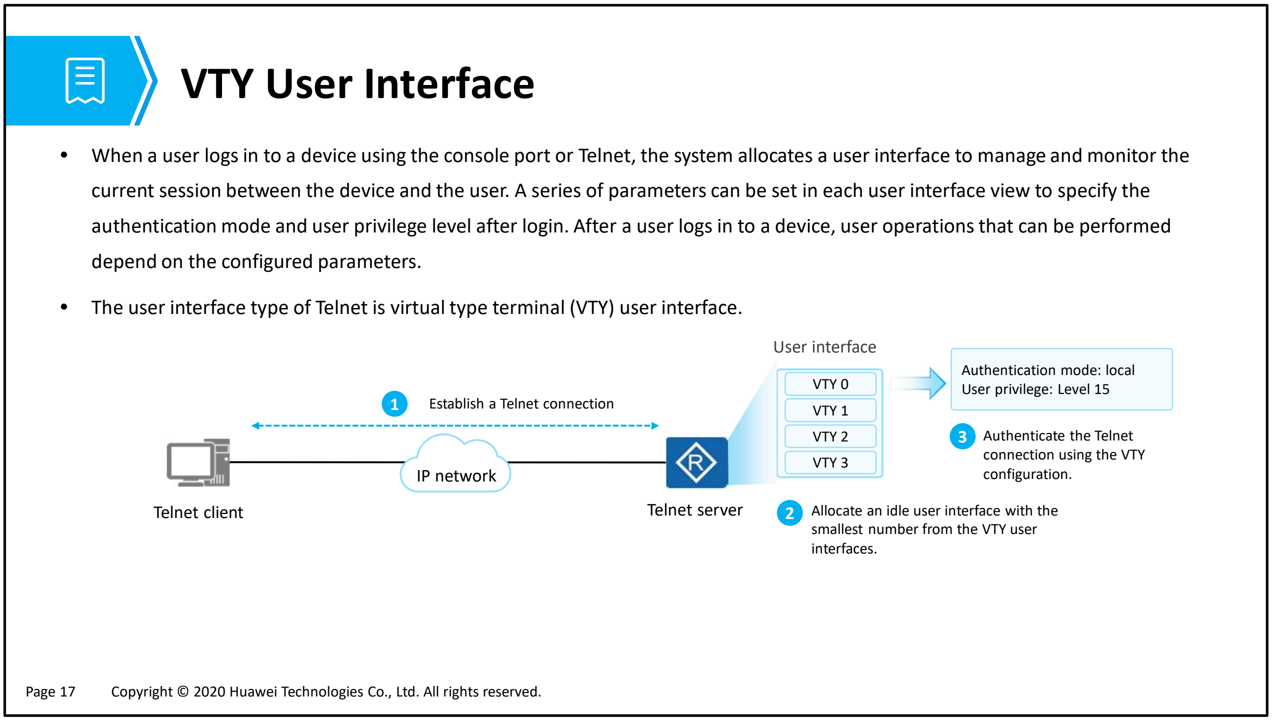
1. File Transfer
2. **Telnet**
3. DHCP
4. HTTP
5. DNS
6. NTP



Application Scenario of Telnet

- To facilitate device management using commands, you can use Telnet to manage devices.
- Device management through Telnet is different from that using the console port. In Telnet-based device management mode, no dedicated cable is required to directly connect to the console port of the Telnet server, as long as the Telnet server's IP address is reachable and Telnet clients can communicate with the Telnet server's TCP port 23.
- The device that can be managed through Telnet is called the Telnet server, and the device connecting to the Telnet server is called the Telnet client. Many network devices can act as both the Telnet server and Telnet client.

- Currently, mainstream network devices, such as access controllers (ACs), access points (APs), firewalls, routers, switches, and servers, can function as both the Telnet server and Telnet client.



VTY User Interface

- When a user logs in to a device using the console port or Telnet, the system allocates a user interface to manage and monitor the current session between the device and the user. A series of parameters can be set in each user interface view to specify the authentication mode and user privilege level after login. After a user logs in to a device, user operations that can be performed depend on the configured parameters.
- The user interface type of Telnet is virtual type terminal (VTY) user interface.

User interface
VTY 0
VTY 1
VTY 2
VTY 3
Authentication mode: local
User privilege: Level 15
1 Establish a Telnet connection
IP network
Telnet client
Telnet server
3 Authenticate the Telnet connection using the VTY configuration.
2 Allocate an idle user interface with the smallest number from the VTY user interfaces.

- Equipment generally supports up to 15 users simultaneously access through VTY

Configuration Commands (1)

1. Enable the Telnet server function.

```
[Huawei] telnet server enable
```

The Telnet server function is enabled on the device (disabled by default). To disable this function, run the **undo telnet server enable** command.

2. Enter the user view.

```
[Huawei] user-interface vty first-ui-number [ last-ui-number ]
```

The VTY user interface view is displayed. VTY user interfaces may vary according to device models.

3. Configure protocols supported by the VTY user interface.

```
[Huawei-ui-vty0-4]] protocol inbound { all | telnet | ssh}
```

By default, the VTY user interface supports Secure Shell (SSH) and Telnet.

Configuration Commands (2)

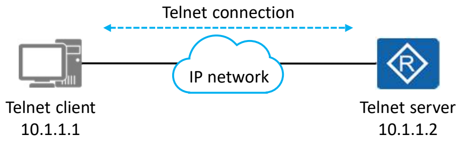
4. Configure the authentication mode and the authentication password in password authentication mode.

```
[Huawei-ui-vty0-4] authentication-mode {aaa | none | password}
[Huawei-ui-vty0-4] set authentication password cipher
```

By default, no default authentication mode is available. You need to manually configure an authentication mode.

The **set authentication password cipher** command implementation varies according to VRP versions. In some versions, you need to press **Enter** and then enter the password. In other versions, you can directly enter the password after the command.

Configuration Example (1)

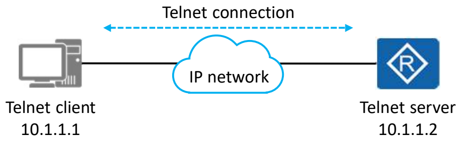


- Configure the router at 10.1.1.2 as the Telnet server and set the authentication mode to AAA local authentication. Create an account named **huawei**, set the password to **Huawei@123**, and set the privilege level to 15.
- Log in to and manage the Telnet server through the Telnet client.

Configurations on the Telnet server:

```
<Huawei> system-view
[Huawei] telnet server enable
[Huawei] aaa
[Huawei-aaa] local-user huawei password irreversible-cipher Huawei@123
[Huawei-aaa] local-user huawei privilege level 15
[Huawei-aaa] local-user huawei service-type telnet
[Huawei-aaa] quit
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode aaa
```

Configuration Example (2)



- Configure the router at 10.1.1.2 as the Telnet server and set the authentication mode to AAA local authentication. Create an account named **huawei**, set the password to **Huawei@123**, and set the privilege level to 15.
- Log in to and manage the Telnet server through the Telnet client.

Operations on the Telnet client:

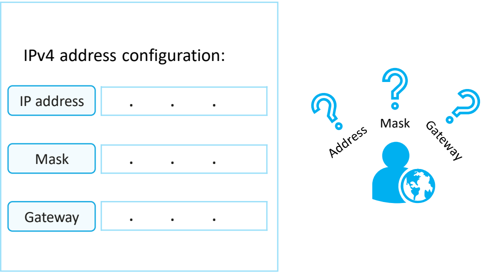
```
<Host>telnet 10.1.1.2
Login authentication

Username:huawei
Password:
Info: The max number of VTY users is 5, and the number
    of current VTY users on line is 1.
    The current login time is 2020-01-08 15:37:25.
<Huawei>
```

Contents

1. File Transfer
2. Telnet
3. **DHCP**
4. HTTP
5. DNS
6. NTP

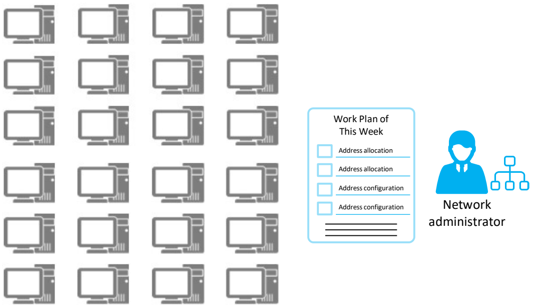
Issues Faced by Manual Network Parameter Configuration (1)

Too Many Hard-to-Understand Parameters



- Common users are not familiar with network parameters and misconfiguration often occurs, resulting in network access failure. Random IP address configuration may cause IP address conflicts.

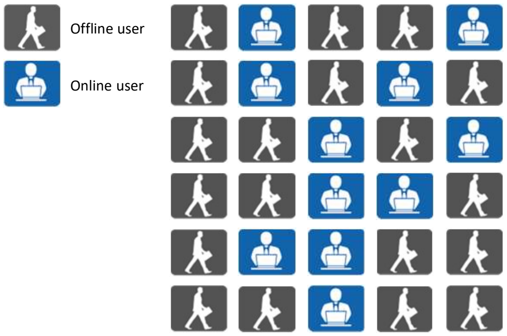
Huge Workload



- Network administrators centrally configure network parameters, with heavy workloads and repetitive tasks.
- Network administrators need to plan and allocate IP addresses to users in advance.

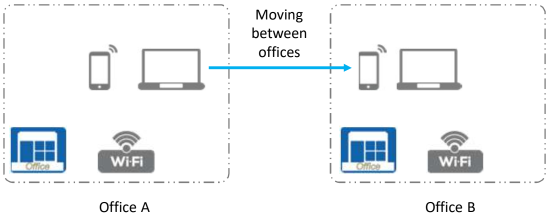
Issues Faced by Manual Network Parameter Configuration (2)

Low Utilization



- On an enterprise network, each user uses a fixed IP address. As a result, the IP address utilization is low, and some IP addresses may remain unused for a long time.

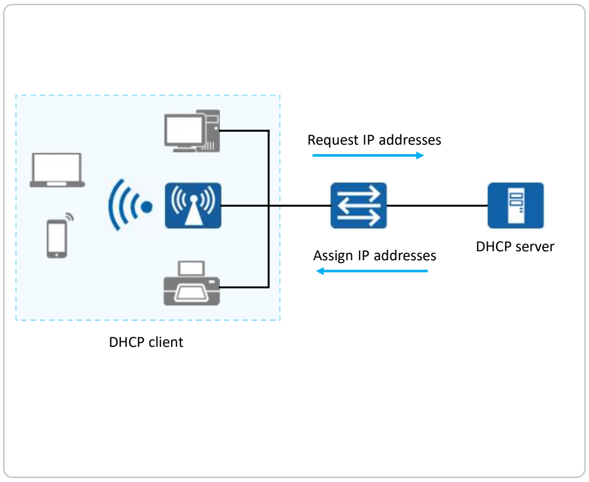
Poor Flexibility



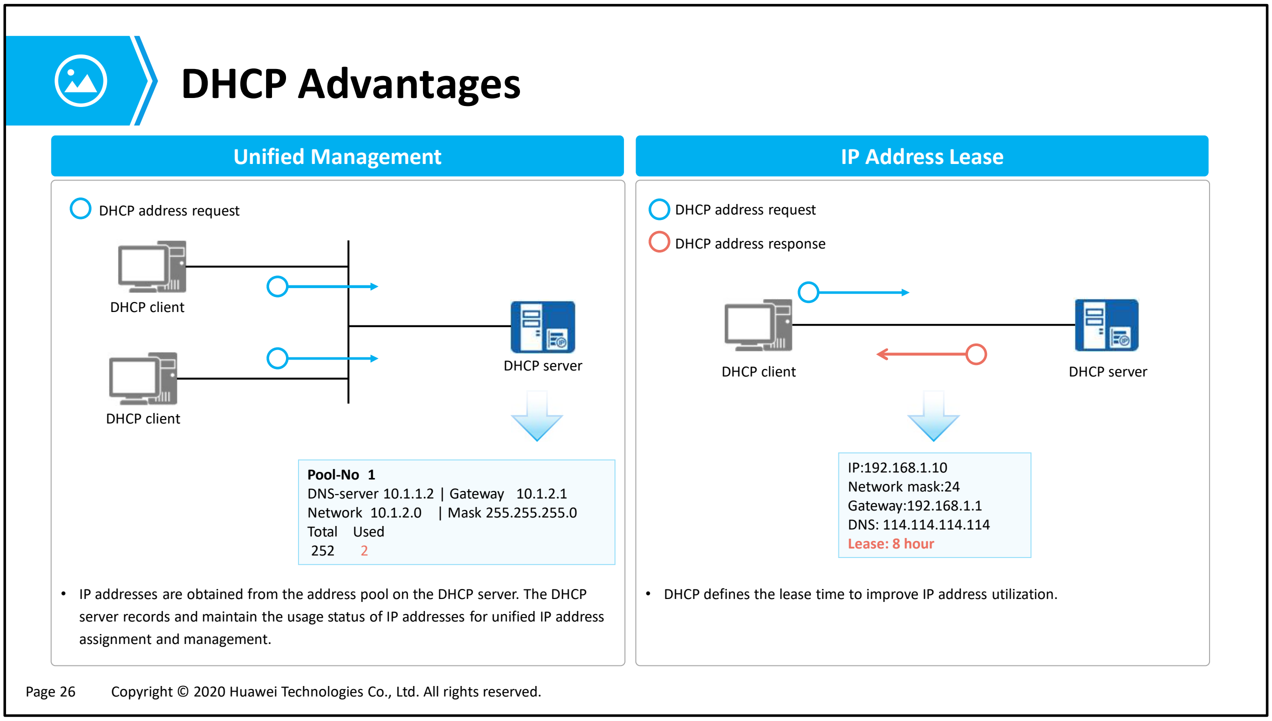
- Wireless local area networks (WLANs) allow for flexible station (STA) access locations. When a STA moves from one wireless coverage area to another, the IP address of the STA may need to be reconfigured.

Basic Concepts of DHCP

DHCP Working Principle



- To overcome the disadvantages of the traditional static IP configuration mode, the Dynamic Host Configuration Protocol (DHCP) is developed to dynamically assign suitable IP addresses to hosts.
- DHCP adopts the client/server (C/S) architecture. Hosts do not need to be configured and can automatically obtain IP addresses from a DHCP server. DHCP enables host plug-and-play after they are connected to the network.



DHCP Advantages

Unified Management

Pool-No 1
DNS-server 10.1.1.2 | Gateway 10.1.2.1
Network 10.1.2.0 | Mask 255.255.255.0

Total	Used
252	2

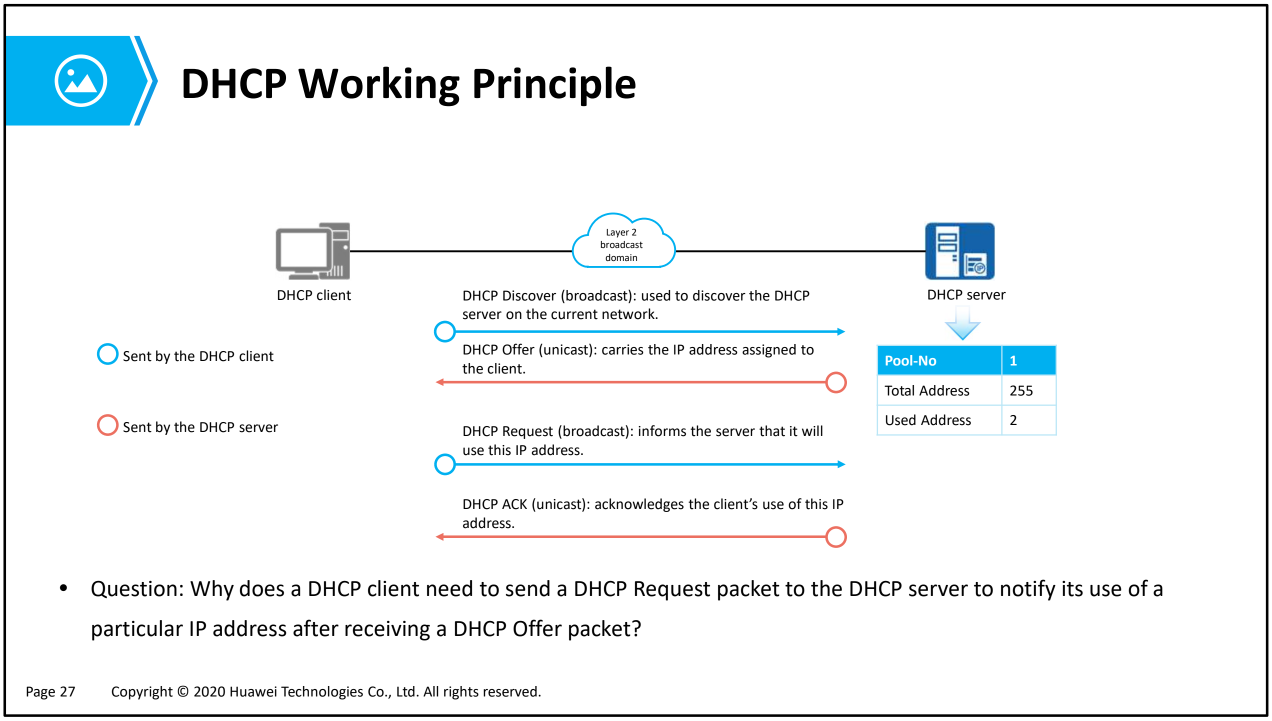
- IP addresses are obtained from the address pool on the DHCP server. The DHCP server records and maintain the usage status of IP addresses for unified IP address assignment and management.

IP Address Lease

IP:192.168.1.10
Network mask:24
Gateway:192.168.1.1
DNS: 114.114.114.114
Lease: 8 hour

- DHCP defines the lease time to improve IP address utilization.

- If a DHCP client does not renew the lease of an assigned IP address after the lease expires, the DHCP server determines that the DHCP client no longer needs to use this IP address, reclaims it, and may assign it to another client.



DHCP Working Principle

○ Sent by the DHCP client

○ Sent by the DHCP server

DHCP Discover (broadcast): used to discover the DHCP server on the current network.

DHCP Offer (unicast): carries the IP address assigned to the client.

DHCP Request (broadcast): informs the server that it will use this IP address.

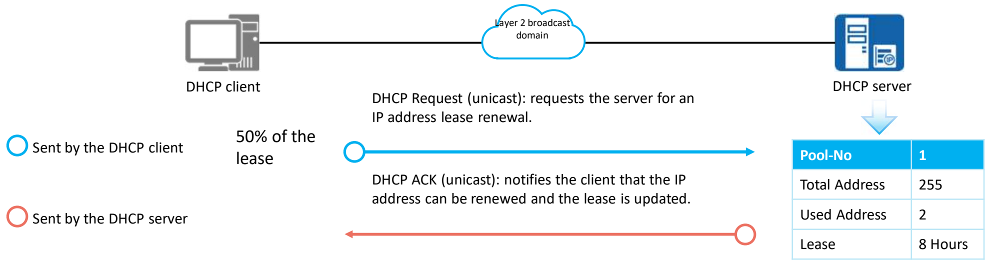
DHCP ACK (unicast): acknowledges the client’s use of this IP address.

Pool-No	1
Total Address	255
Used Address	2

- Question: Why does a DHCP client need to send a DHCP Request packet to the DHCP server to notify its use of a particular IP address after receiving a DHCP Offer packet?

- A client's DHCP Request packet is broadcast, so other DHCP servers on the network know that the client has selected a particular IP address assigned by the DHCP server. This ensures that other DHCP servers can release this IP address assigned to the client through the unicast DHCP Offer packet.
- If multiple DHCP servers reply with a DHCP Offer message to the client, the client accepts only the first DHCP Offer message it receives.

DHCP Lease Renewal



DHCP Request (unicast): requests the server for an IP address lease renewal.

DHCP ACK (unicast): notifies the client that the IP address can be renewed and the lease is updated.

Pool-No	1
Total Address	255
Used Address	2
Lease	8 Hours

- If the DHCP client fails to receive a response from the original DHCP server at 50% of the lease (known as T1), the DHCP client waits until 87.5% of the lease (known as T2) has passed. At T2, the client enters the rebinding state, and broadcasts a DHCP Request packet, to which any DHCP server can respond.

Configuration Commands (1)

1. Enable DHCP.

```
[Huawei] dhcp enable
```

2. Enable the interface to use the interface address pool to provide the DHCP server function.

```
[Huawei-Gigabitethernet0/0/0]dhcp select interface
```

3. Specify a DNS server IP address for the interface address pool.

```
[Huawei-Gigabitethernet0/0/0]dhcp server dns-list ip-address
```

4. Configure the range of IP addresses that cannot be automatically assigned to clients from the interface address pool.

```
[Huawei-Gigabitethernet0/0/0]dhcp server excluded-ip-address start-ip-address [ end-ip-address ]
```

5. Configure the lease of IP addresses in the interface address pool of the DHCP server.

```
[Huawei-Gigabitethernet0/0/0]dhcp server lease { day day [ hour hour [ minute minute ] ] | unlimited }
```

By default, the IP address lease is one day.

Configuration Commands (2)

6. Create a global address pool.

```
[Huawei]ip pool ip-pool-name
```

7. Specify the range of IP addresses that can be assigned dynamically in the global address pool.

```
[Huawei-ip-pool-2]network ip-address [ mask { mask | mask-length } ]
```

8. Configure the gateway address for DHCP clients.

```
[Huawei-ip-pool-2]gateway-list ip-address
```

9. Specify the DNS server IP address that the DHCP server delivers to DHCP clients.

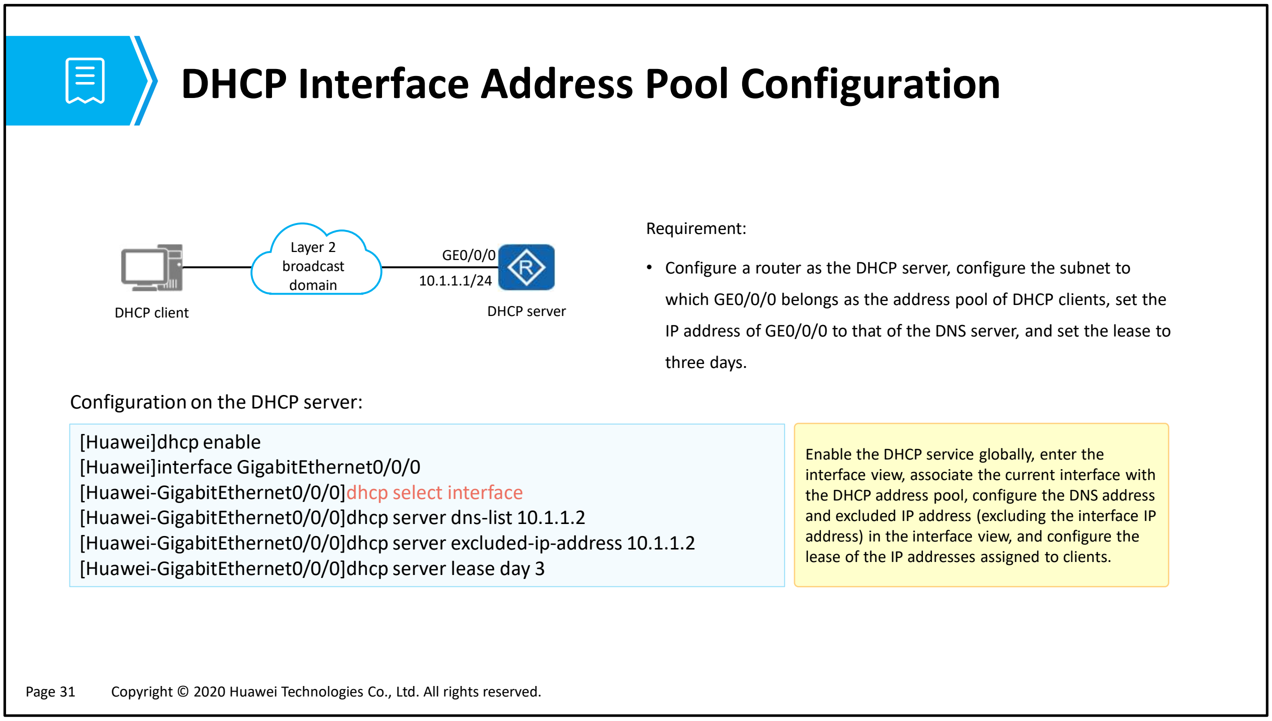
```
[Huawei-ip-pool-2]dns-list ip-address
```

10. Set the IP address lease.

```
[Huawei-ip-pool-2] lease { day day [ hour hour [ minute minute ] ] | unlimited }
```

11. Enable the DHCP server function on the interface.

```
[Huawei-Gigabitthernet0/0/0]dhcp select global
```



DHCP Interface Address Pool Configuration

DHCP client

Layer 2 broadcast domain

GE0/0/0

10.1.1.1/24

DHCP server

Requirement:

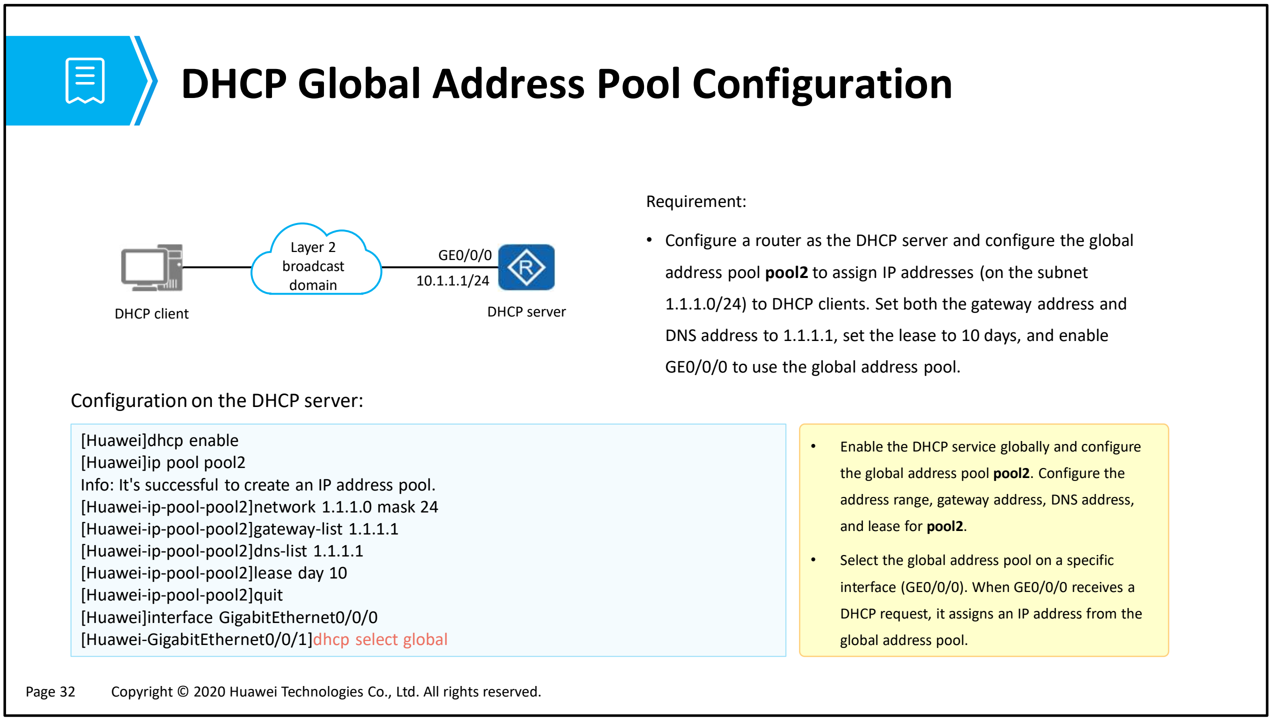
- Configure a router as the DHCP server, configure the subnet to which GE0/0/0 belongs as the address pool of DHCP clients, set the IP address of GE0/0/0 to that of the DNS server, and set the lease to three days.

Configuration on the DHCP server:

```
[Huawei]dhcp enable
[Huawei]interface GigabitEthernet0/0/0
[Huawei-GigabitEthernet0/0/0]dhcp select interface
[Huawei-GigabitEthernet0/0/0]dhcp server dns-list 10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server excluded-ip-address 10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server lease day 3
```

Enable the DHCP service globally, enter the interface view, associate the current interface with the DHCP address pool, configure the DNS address and excluded IP address (excluding the interface IP address) in the interface view, and configure the lease of the IP addresses assigned to clients.

- If a DHCP server based on a global address pool is configured, all online users of the server can obtain IP addresses from this address pool. The global address pool is used when the DHCP server and client are located on different network segments.
- If a DHCP server based on an interface address pool is configured, only users that go online from this interface can obtain IP addresses from this address pool. The interface address pool is used when the DHCP server and client are located on the same network segment.
- A switch the global address pool on the DHCP server. In this manner, DHCP clients on multiple network segments can share one DHCP server. This reduces costs and facilitates centralized managecan supports the DHCP relay. When this device functions as a DHCP relay agent, the client can communicate with a DHCP server on another network segment through the device, and obtain an IP address and other configuration parameters from ment.



DHCP Global Address Pool Configuration

Requirement:

- Configure a router as the DHCP server and configure the global address pool **pool2** to assign IP addresses (on the subnet 1.1.1.0/24) to DHCP clients. Set both the gateway address and DNS address to 1.1.1.1, set the lease to 10 days, and enable GE0/0/0 to use the global address pool.

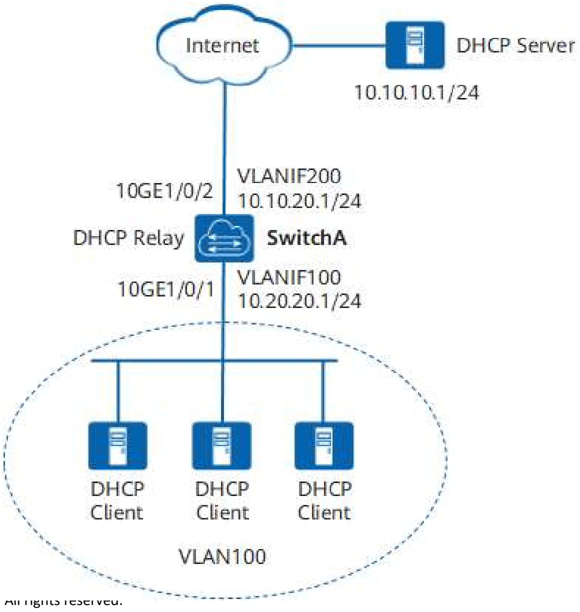
Configuration on the DHCP server:

```
[Huawei]dhcp enable
[Huawei]ip pool pool2
Info: It's successful to create an IP address pool.
[Huawei-ip-pool-pool2]network 1.1.1.0 mask 24
[Huawei-ip-pool-pool2]gateway-list 1.1.1.1
[Huawei-ip-pool-pool2]dns-list 1.1.1.1
[Huawei-ip-pool-pool2]lease day 10
[Huawei-ip-pool-pool2]quit
[Huawei]interface GigabitEthernet0/0/0
[Huawei-GigabitEthernet0/0/1]dhcp select global
```

- Enable the DHCP service globally and configure the global address pool **pool2**. Configure the address range, gateway address, DNS address, and lease for **pool2**.
- Select the global address pool on a specific interface (GE0/0/0). When GE0/0/0 receives a DHCP request, it assigns an IP address from the global address pool.

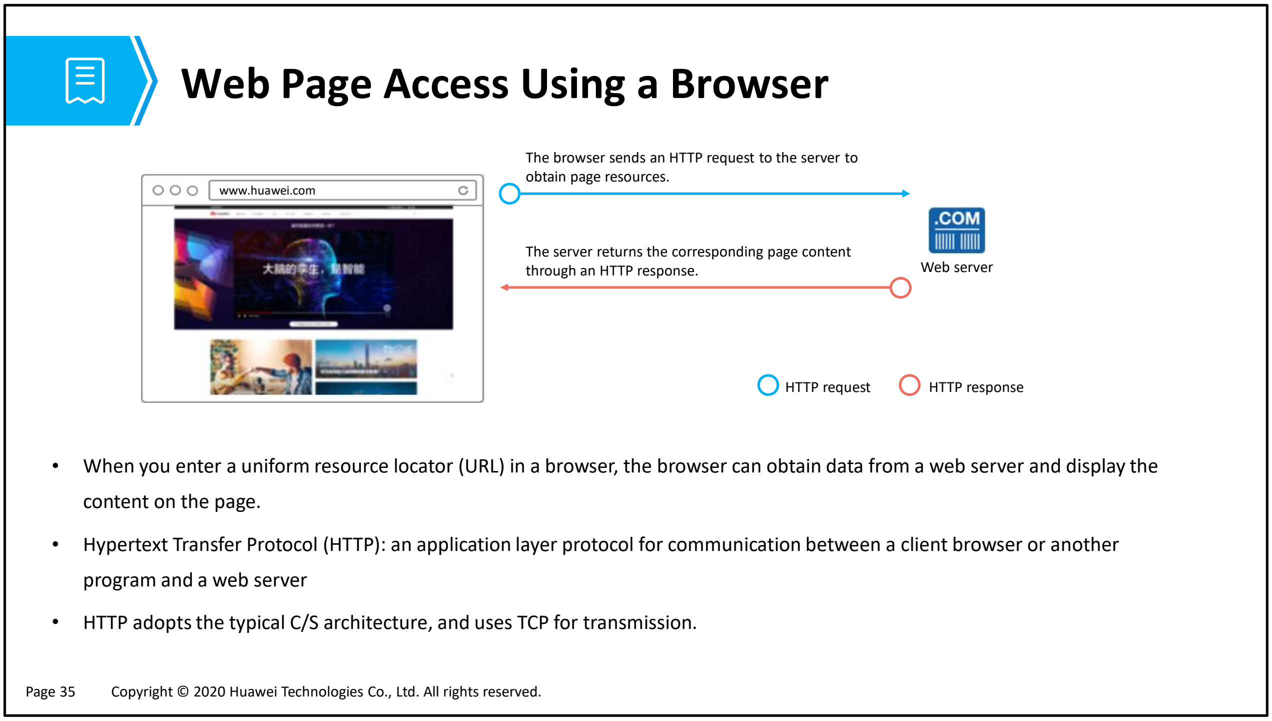
- The interface address pool takes precedence over the global address pool. If an address pool is configured on an interface, the clients connected to the interface obtain IP addresses from the interface address pool even if a global address pool is configured. On the S5700 switch, only logical VLANIF interfaces can be configured with interface address pools.

DHCP relay


Internet
DHCP Server
10.10.10.1/24
10GE1/0/2
VLANIF200
10.10.20.1/24
DHCP Relay
SwitchA
10GE1/0/1
VLANIF100
10.20.20.1/24
DHCP
Client
DHCP
Client
DHCP
Client
VLAN100

Contents

1. File Transfer
2. Telnet
3. DHCP
4. **HTTP**
5. DNS
6. NTP



Web Page Access Using a Browser

The browser sends an HTTP request to the server to obtain page resources.

The server returns the corresponding page content through an HTTP response.

.COM

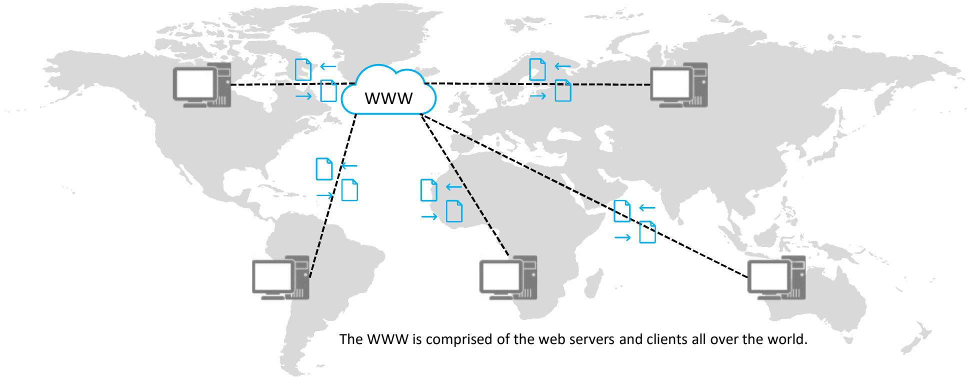
Web server

○ HTTP request ○ HTTP response

- When you enter a uniform resource locator (URL) in a browser, the browser can obtain data from a web server and display the content on the page.
- Hypertext Transfer Protocol (HTTP): an application layer protocol for communication between a client browser or another program and a web server
- HTTP adopts the typical C/S architecture, and uses TCP for transmission.

- URL: uniquely identifies the location of a web page or other resources on the Internet. A URL can contain more detail, such as the name of a page of hypertext, usually identified by the file name extension .html or .htm.

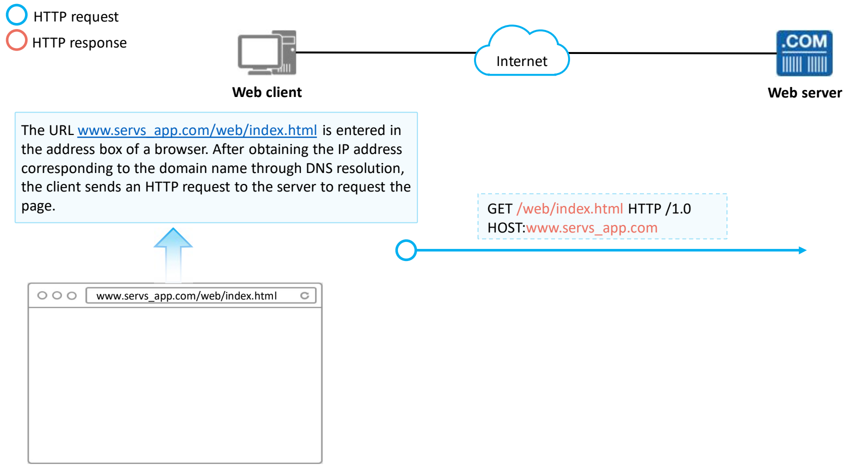
Background



The WWW is comprised of the web servers and clients all over the world.

- In the early days of the Internet, World Wide Web (WWW) was proposed to share documents.
- The WWW consists of three parts: Hypertext Markup Language (HTML) for displaying document content in a browser, HTTP for transmitting documents on the network, and URLs for specifying document locations on the network.
- WWW was actually the name of a client application for browsing HTML documents, and now represents a collection of technologies (HTML + HTTP + URL) and is commonly known as the Web.

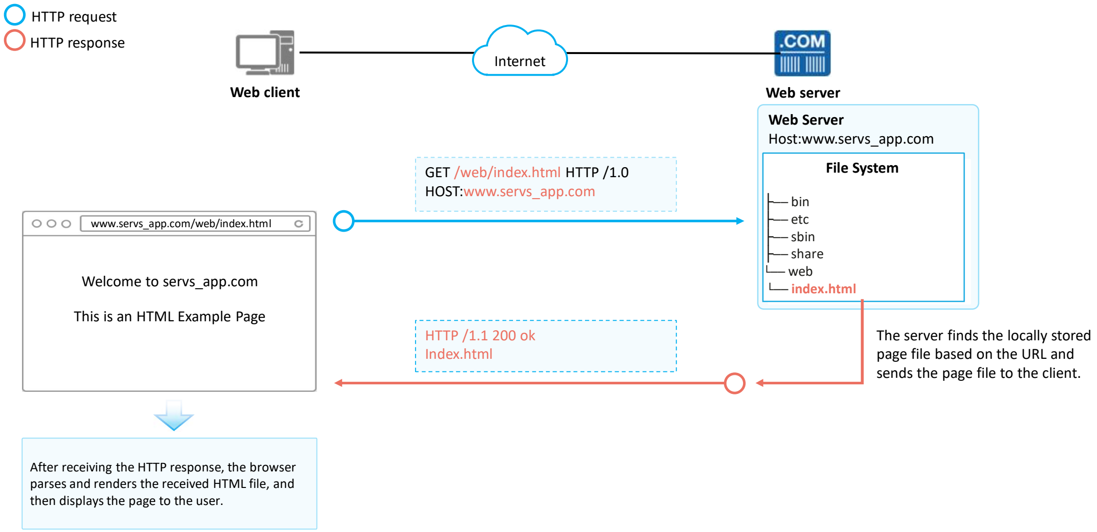
Transfer Example (1)



The URL www.servs_app.com/web/index.html is entered in the address box of a browser. After obtaining the IP address corresponding to the domain name through DNS resolution, the client sends an HTTP request to the server to request the page.

```
GET /web/index.html HTTP /1.0
HOST:www.servs_app.com
```

Transfer Example (2)



○ HTTP request

○ HTTP response

Web client

Internet

Web server

Web Server
Host:www.servs_app.com

File System

```
├── bin
├── etc
├── sbin
├── share
└── web
    └── index.html
```

GET /web/index.html HTTP /1.0
HOST:www.servs_app.com

www.servs_app.com/web/index.html

Welcome to servs_app.com

This is an HTML Example Page

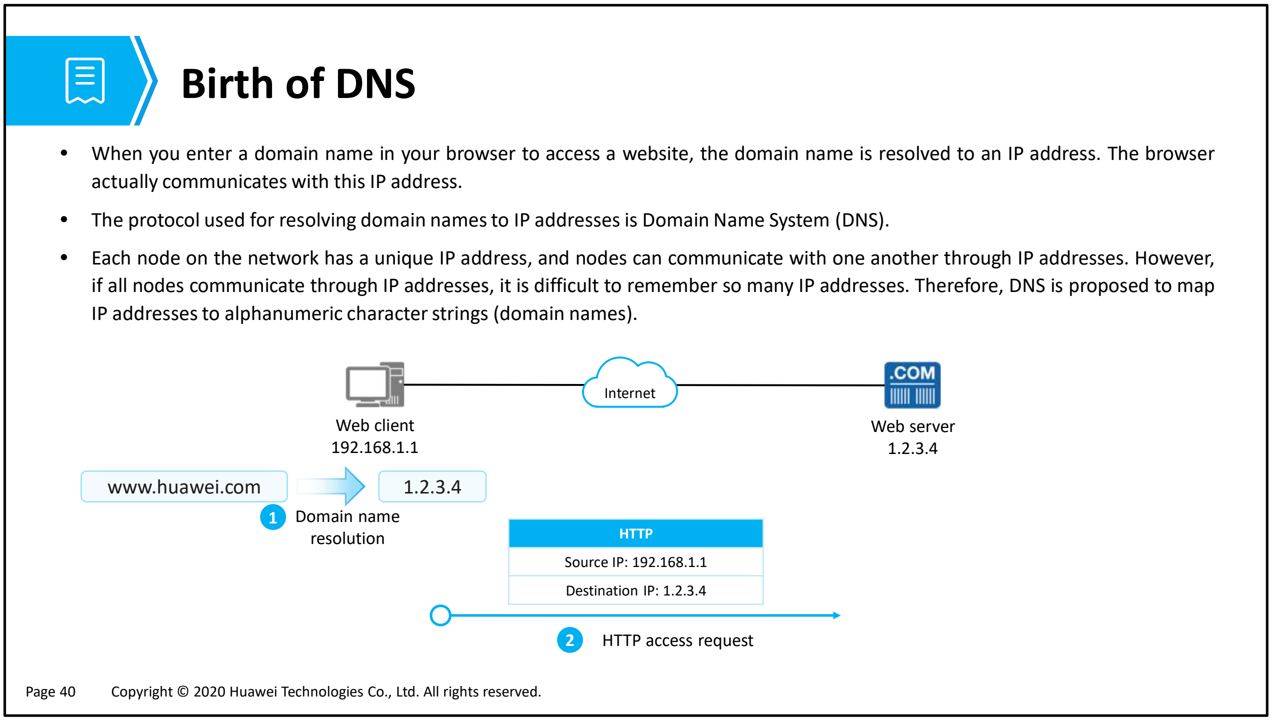
HTTP /1.1 200 ok
Index.html

The server finds the locally stored page file based on the URL and sends the page file to the client.

After receiving the HTTP response, the browser parses and renders the received HTML file, and then displays the page to the user.

Contents

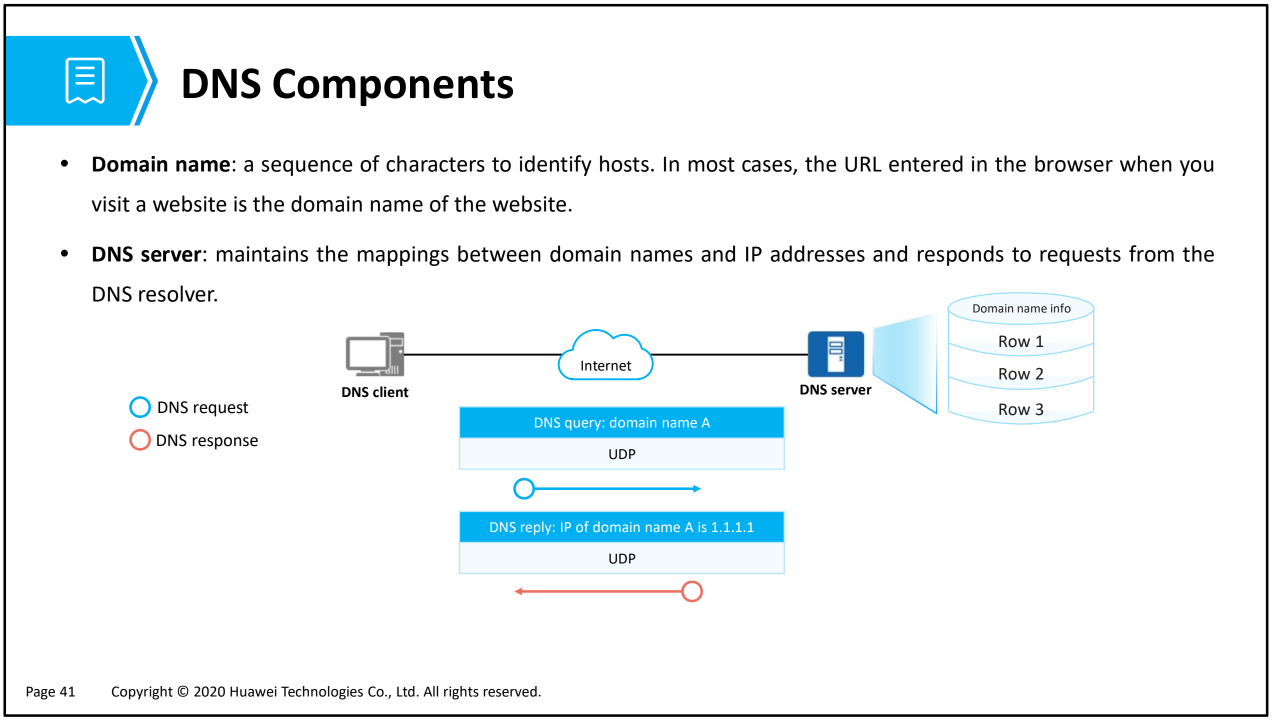
1. File Transfer
2. Telnet
3. DHCP
4. HTTP
5. **DNS**
6. NTP



Birth of DNS

- When you enter a domain name in your browser to access a website, the domain name is resolved to an IP address. The browser actually communicates with this IP address.
- The protocol used for resolving domain names to IP addresses is Domain Name System (DNS).
- Each node on the network has a unique IP address, and nodes can communicate with one another through IP addresses. However, if all nodes communicate through IP addresses, it is difficult to remember so many IP addresses. Therefore, DNS is proposed to map IP addresses to alphanumeric character strings (domain names).

- Advanced Research Projects Agency Network (ARPANET), the predecessor of the Internet, provides the mappings between host names and IP addresses. However, the number of hosts was small at that time. Only one file (HOSTS.txt) is required to maintain the name-to-address mapping. The HOSTS.txt file is maintained by the network information center (NIC). Users who change their host names send their changes to the NIC by email, and the NIC periodically updates the HOSTS.txt file.
- However, after ARPANET uses TCP/IP, the number of network users increases sharply, and it seems difficult to manually maintain the HOSTS.txt file. The following issues may occur:
  - **Name conflict**: Although the NIC can ensure the consistency of host names that it manages, it is difficult to ensure that the host names are not randomly changed to be the same as those being used by others.
  - **Consistency**: As the network scale expands, it is hard to keep the HOSTS.txt file consistent. The names of other hosts may have been changed several times before the HOSTS.txt file of the current host is updated.
- Therefore, DNS is introduced.



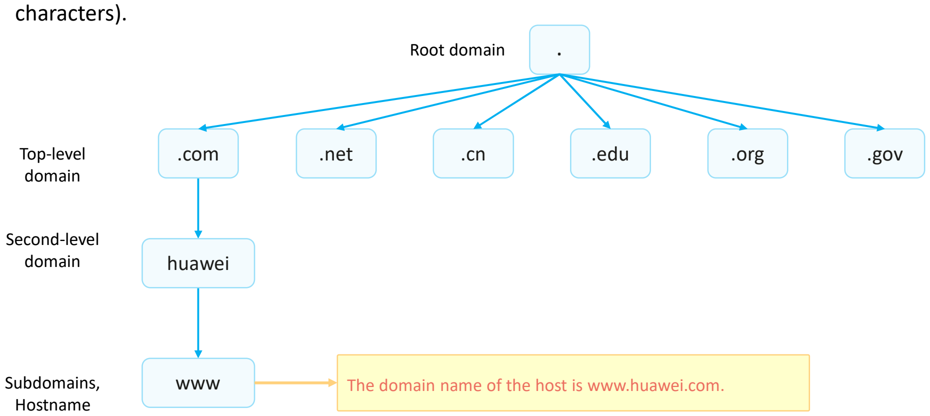
DNS Components

- **Domain name**: a sequence of characters to identify hosts. In most cases, the URL entered in the browser when you visit a website is the domain name of the website.
- **DNS server**: maintains the mappings between domain names and IP addresses and responds to requests from the DNS resolver.

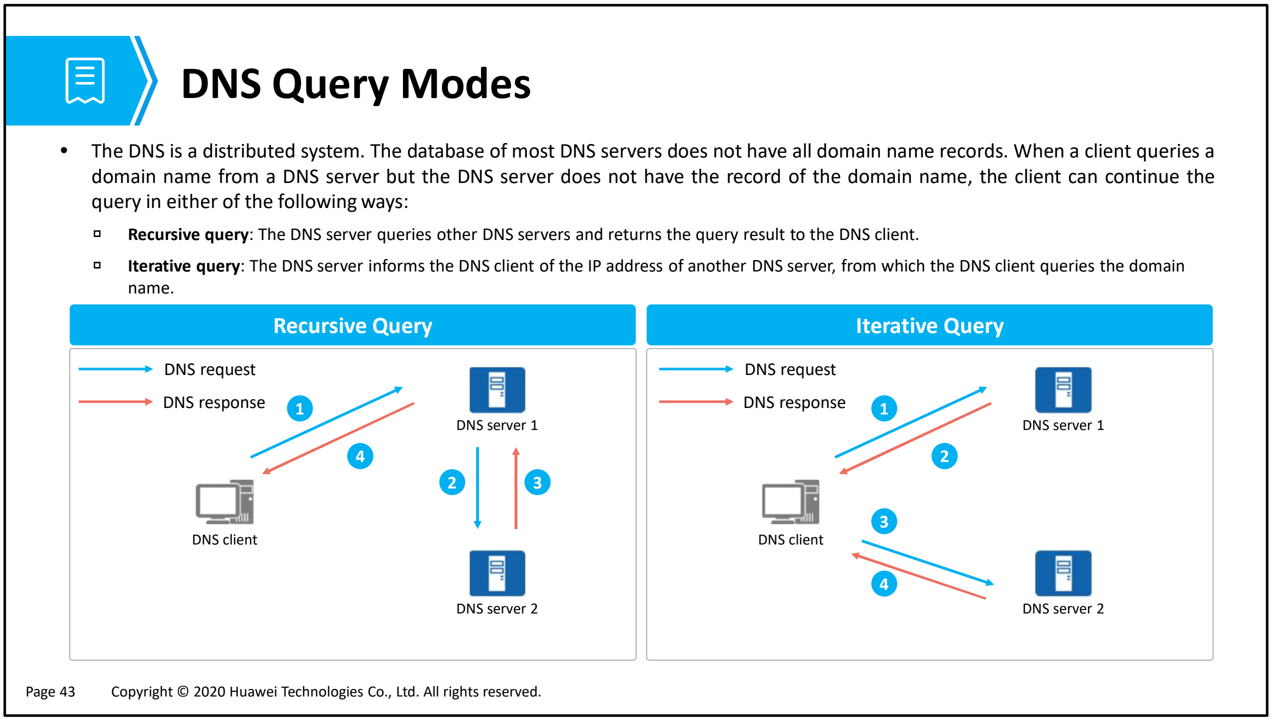
- The DNS adopts a distributed architecture. The database on each server stores only the mapping between some domain names and IP addresses.

Domain Name Format

- The domain name is in the format of *hostname.second-level domain.top-level domain.root domain*. The root domain is represented by a dot (.). Generally, the root domain is denoted by an empty name (that is, containing no characters).



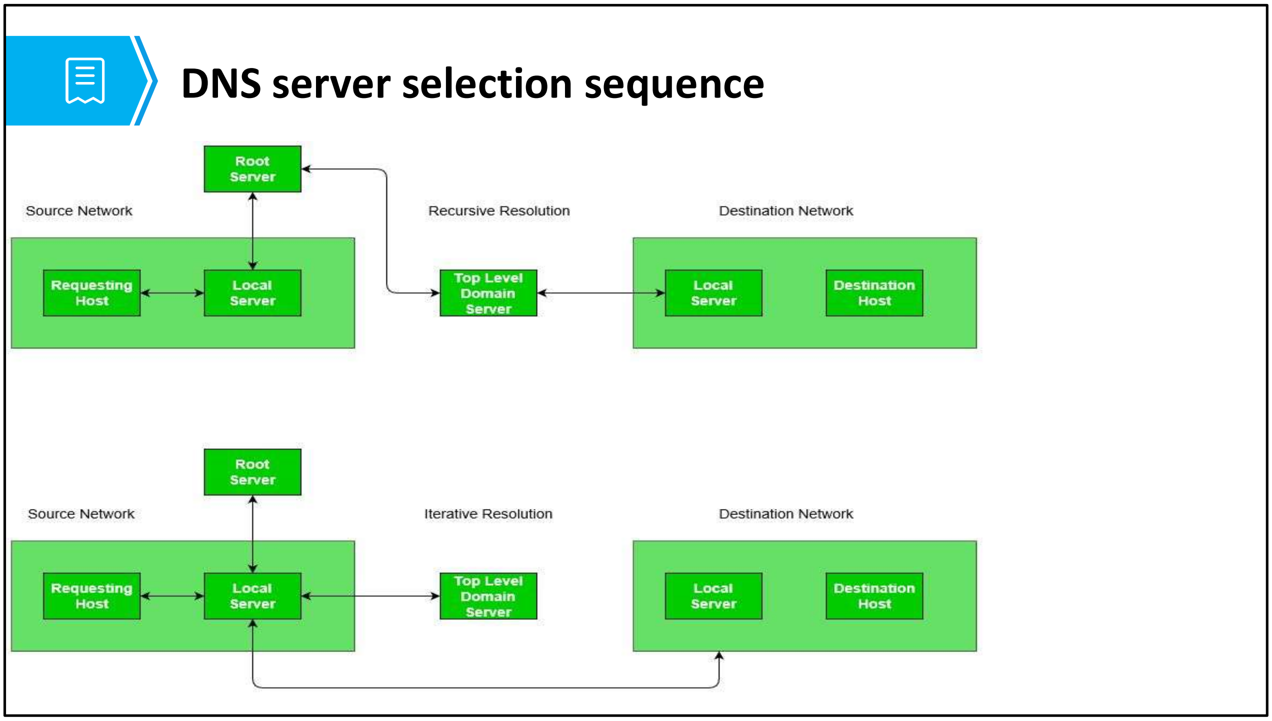
The domain name of the host is www.huawei.com.



DNS Query Modes

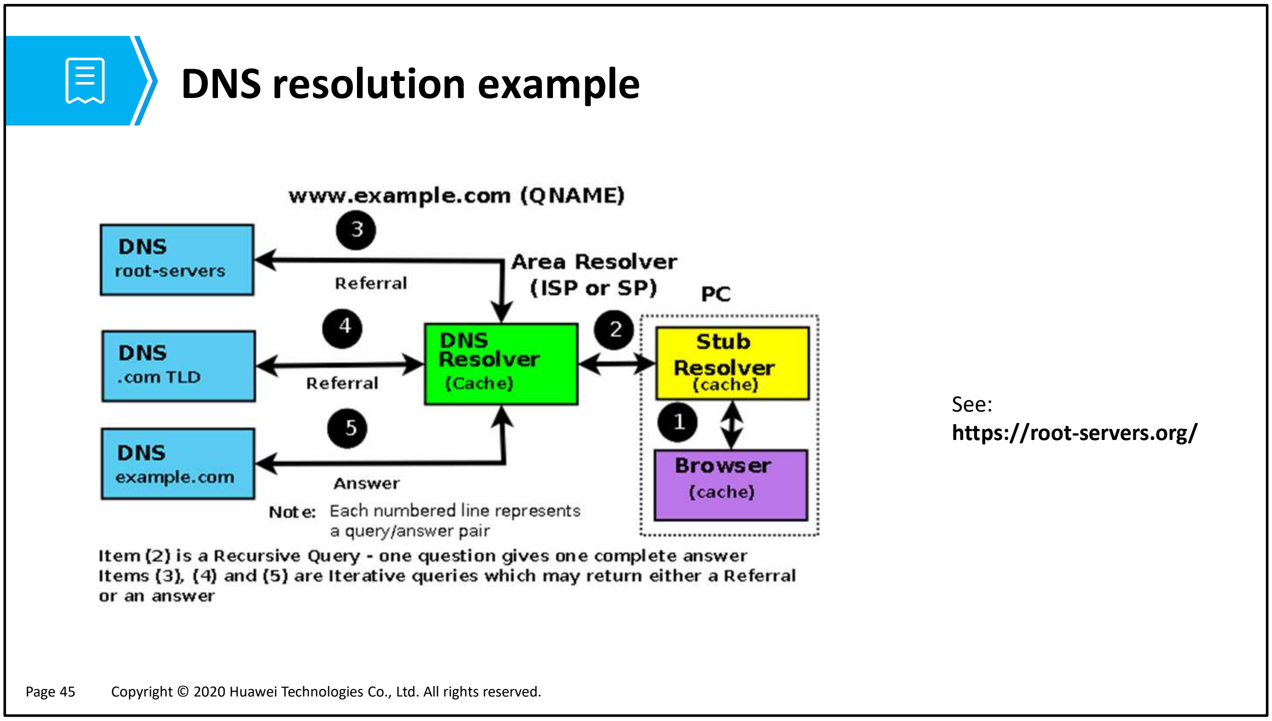
- The DNS is a distributed system. The database of most DNS servers does not have all domain name records. When a client queries a domain name from a DNS server but the DNS server does not have the record of the domain name, the client can continue the query in either of the following ways:
  - **Recursive query**: The DNS server queries other DNS servers and returns the query result to the DNS client.
  - **Iterative query**: The DNS server informs the DNS client of the IP address of another DNS server, from which the DNS client queries the domain name.

- The iterative query is different from the recursive query in that the DNS response returned by DNS server 1 contains the IP address of another DNS server (DNS server 2).



DNS server selection sequence

- The DNS protocol uses a common message format for all exchanges between client and server or between servers. The DNS messages are encapsulated over UDP or TCP using the "well-known port number" **53**. DNS uses UDP for message smaller than 512 bytes (common requests and responses). DNS uses TCP for bigger exchange (i.e. zone transfer).



DNS resolution example

Note: Each numbered line represents a query/answer pair

Item (2) is a Recursive Query - one question gives one complete answer
Items (3), (4) and (5) are Iterative queries which may return either a Referral or an answer

See:
https://root-servers.org/

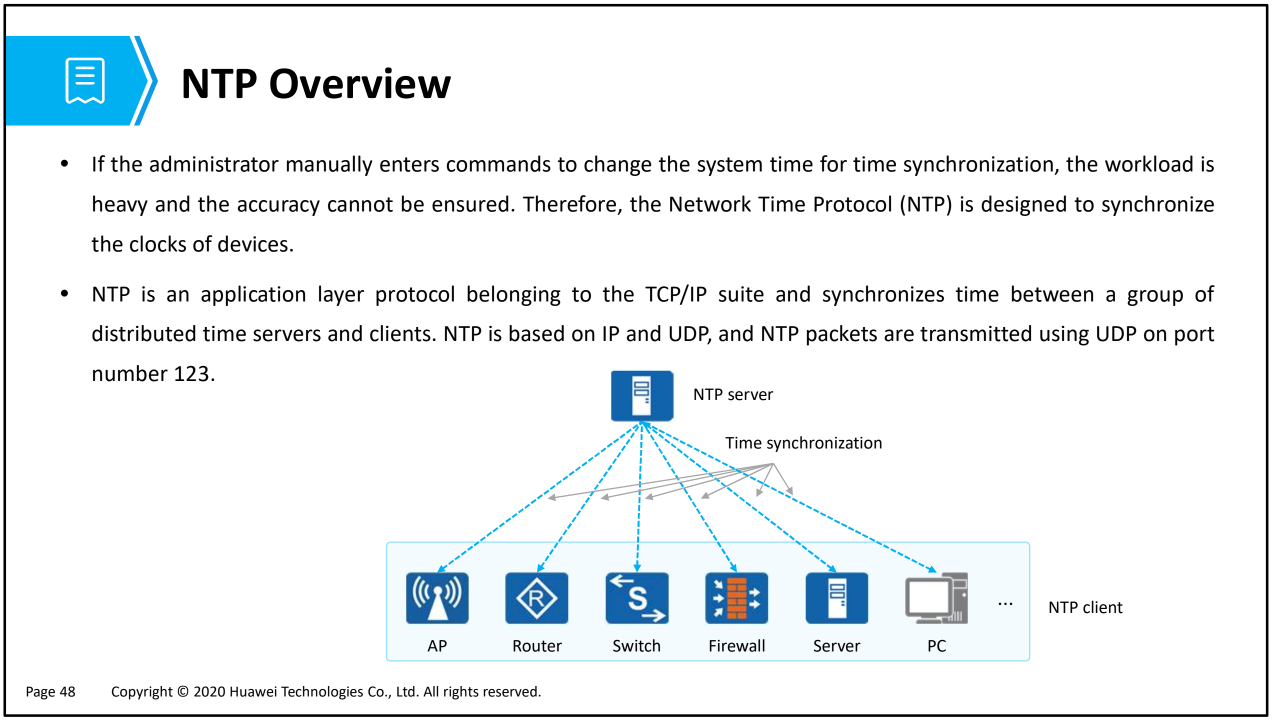
- The DNS protocol uses a common message format for all exchanges between client and server or between servers. The DNS messages are encapsulated over UDP or TCP using the "well-known port number" **53**. DNS uses UDP for message smaller than 512 bytes (common requests and responses). DNS uses TCP for bigger exchange (i.e. zone transfer).
- The RFC 3258 shows how anycast is used to provide authoritative DNS services. Also, the OpenDNS recursive DNS service uses anycast to distribute the load over its network.

Contents

1. File Transfer
2. Telnet
3. DHCP
4. HTTP
5. DNS
6. **NTP**

Time Synchronization Requirements

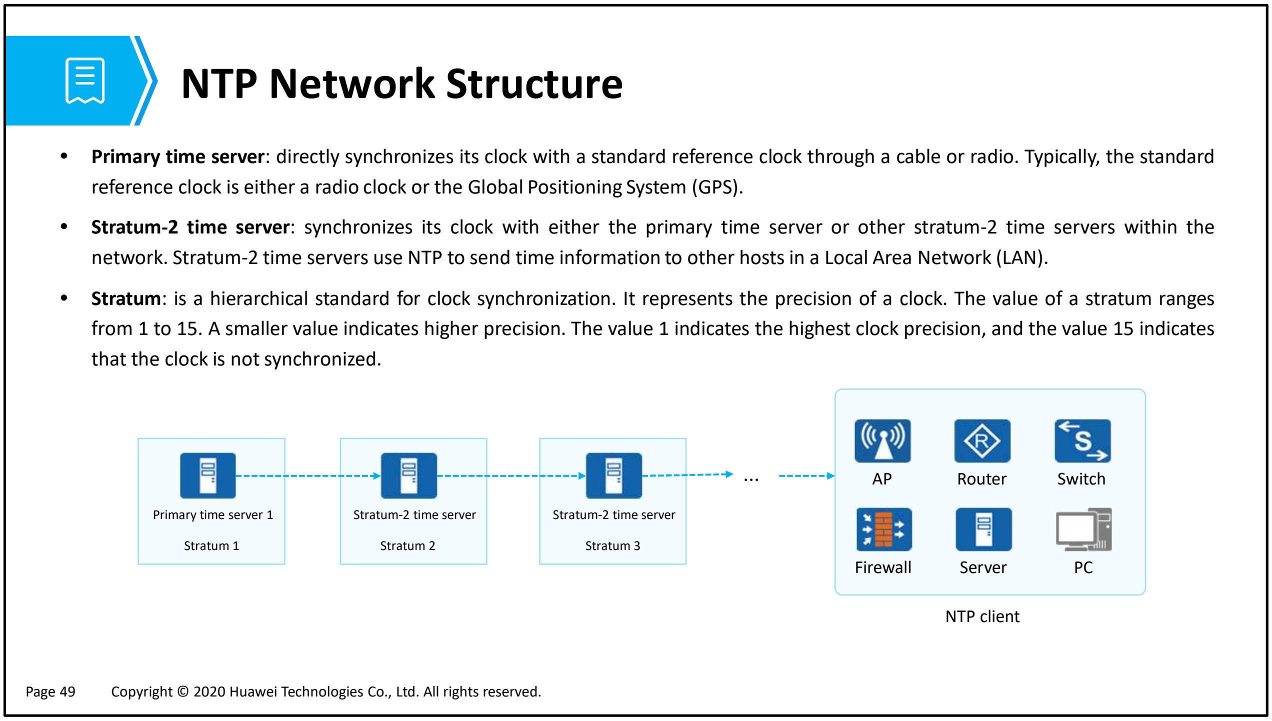
- Consistent clock of all devices is required in many scenarios on enterprise campus networks:
  - Network management: Analysis of logs or debugging messages collected from different routers needs time for reference.
  - Charging system: The clocks of all devices must be consistent.
  - Several systems working together on the same complicate event: Systems have to take the same clock for reference to ensure a proper sequence of implementation.
  - Incremental backup between a backup server and clients: Clocks on the backup server and clients should be synchronized.
  - System time: Some applications need to know the time when users log in to the system and the time when files are modified.



NTP Overview

- If the administrator manually enters commands to change the system time for time synchronization, the workload is heavy and the accuracy cannot be ensured. Therefore, the Network Time Protocol (NTP) is designed to synchronize the clocks of devices.
- NTP is an application layer protocol belonging to the TCP/IP suite and synchronizes time between a group of distributed time servers and clients. NTP is based on IP and UDP, and NTP packets are transmitted using UDP on port number 123.

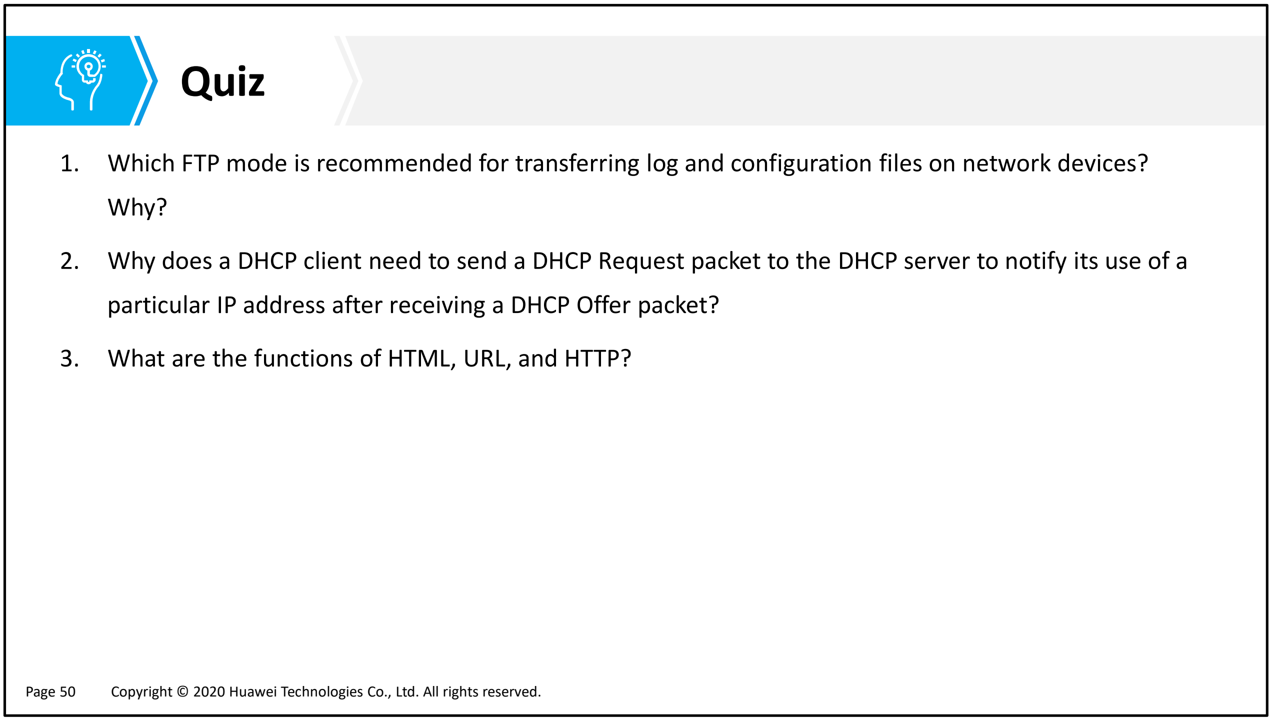
- Currently, mainstream network devices, such as access controllers (ACs), access points (APs), firewalls, routers, switches, and servers, basically serve as NTP clients, and some of the network devices can also serve as NTP servers.



NTP Network Structure

- **Primary time server**: directly synchronizes its clock with a standard reference clock through a cable or radio. Typically, the standard reference clock is either a radio clock or the Global Positioning System (GPS).
- **Stratum-2 time server**: synchronizes its clock with either the primary time server or other stratum-2 time servers within the network. Stratum-2 time servers use NTP to send time information to other hosts in a Local Area Network (LAN).
- **Stratum**: is a hierarchical standard for clock synchronization. It represents the precision of a clock. The value of a stratum ranges from 1 to 15. A smaller value indicates higher precision. The value 1 indicates the highest clock precision, and the value 15 indicates that the clock is not synchronized.

- See
- http://www.ntp.org/
- https://www.ntppool.org/it/use.html



Quiz

1. Which FTP mode is recommended for transferring log and configuration files on network devices? Why?
2. Why does a DHCP client need to send a DHCP Request packet to the DHCP server to notify its use of a particular IP address after receiving a DHCP Offer packet?
3. What are the functions of HTML, URL, and HTTP?

1. ASCII mode; The binary mode is more applicable to the transmission of non-text files that cannot be converted, such as EXE, BIN, and CC (VRP version file extension) files.
2. A client's DHCP Request packet is broadcast, so other DHCP servers on the network know that the client has selected a particular IP address assigned by the DHCP server. This ensures that other DHCP servers can release this IP address assigned to the client through the unicast DHCP Offer packet.
3. HTML is used to display page content, URL is used to locate the network location of a document or file, and HTTP is used for requesting and transferring files.

Summary

- FTP is used to transfer files. You are advised to use different transfer modes for different files. FTP is based on TCP and therefore can ensure the reliability and efficiency of file transfer.
- Dynamically assigning IP addresses through DHCP reduces the workload of the administrator and avoids IP address conflicts caused by manual configuration of network parameters.
- As the document transfer protocol of WWW, HTTP is widely used in today's network for encoding and transporting information between a client (such as a web browser) and a web server.

Thank You

www.huawei.com