

Module 10: Network Services

Instructor Materials

CyberOps Associate v1.0





Module 10: Network Services

CyberOps Associate v1.0

Module Objectives

Module Title: Network Services

Module Objective: Explain how network services enable network functionality.

Topic Title	Topic Objective
DHCP	Explain how DHCP services enable network functionality.
DNS	Explain how DNS services enable network functionality.
NAT	Explain how NAT services enable network functionality.
File Transfer and Sharing Services	Explain how file transfer services enable network functionality.
Email	Explain how email services enable network functionality.
НТТР	Explain how HTTP services enable network functionality.

10.1 DHCP

Network Services

CISCO

Dynamic Host Configuration Protocol

- Two types of addressing:
 - Dynamic Dynamic Host Configuration Protocol (DHCP) for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters.
 - **Static** The network administrator manually enters IP address information on hosts.
- When a host connects to the network, the DHCP server chooses an address from a configured range of addresses called a pool and assigns it to the host.
- DHCP can allocate IP addresses for a configurable period of time, called a lease period.



Medium-to-large networks – DHCP server is a local PC-based server Home network – DHCP server is on the local router connecting the home network to the ISP. © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 13

Network Services DHCP Operation

- DHCP operation includes: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, and DHCPNAK.
- When DHCP-configured device connects to the network, the client broadcasts a **DHCPDISCOVER** message to identify any available DHCP servers on the network.
- A DHCP server replies with a **DHCPOFFER** message, which offers a lease to the client.
- The client sends a **DHCPREQUEST** message that identifies the explicit server and lease offer that the client is accepting.





Network Services DHCP Message Format

- The DHCPv4 message format is used for all DHCPv4 transactions.
- The DHCPv4 messages are encapsulated within the UDP transport protocol.
- The below table lists the fields covered in the structure of the DHCPv4 message.

Fields in the structure of DHCPv4 Message			
Operation (OP) Code	Seconds	Gateway IP Address	
Hardware Type	Flags	Client Hardware Address .	
Hardware Address Length	Client IP Address	Server Name	
Hops	Your IP Address	Boot Filename	
Transaction Identifier	Server IP Address	DHCP Options	

10.2 DNS



DNS DNS Overview

- Domain Name System (DNS) provides domain names and their associated IP addresses.
- The DNS system consists of a global hierarchy of distributed servers that contain databases of name to IP address mappings.
- The client computer in the figure will send a request to the DNS server to get the IP address for <u>www.cisco.com</u> so that it can address packets to that server.
- Malicious DNS traffic can be detected through protocol analysis and the inspection of DNS monitoring information.



DNS Resolves Names to IP Addresses

The DNS Domain Hierarchy

- DNS consists of a hierarchy of generic top-level domains and numerous country-level domains.
- The second-level domains are represented by a domain name that is followed by a top-level domain.
- Subdomains are found at the next level of the DNS hierarchy and represent some division of the second-level domain.
- Fourth level domain can represent a host in a subdomain.
- Top-level domains represent either the type of organization or country of origin. Examples:
 (.org) a non-profit organization, (.au) Australia.



ىرايىرانى cısco

DNS The DNS Lookup Process

- To resolve a name to an IP address, the resolver, will first check its local DNS cache. If the mapping is not found, a query will be issued to the DNS server.
- If the mapping is not found there, the DNS server will query other higher-level DNS servers that are authoritative for the top-level domain in order to find the mapping. These are known as recursive queries.
- The caching DNS servers can resolve recursive queries without forwarding the queries to higher level servers.





DNS

The DNS Lookup Process(Contd.)

Steps involved in DNS resolution:

Step 1 - The user types an FQDN into a browser application Address field.



Step 2 - A DNS query is sent to the designated DNS server for the client computer.



DNS

The DNS Lookup Process(Contd.)

Steps involved in DNS resolution:

Step 3 - The DNS server matches the FQDN with its IP address.

Step 4 - The DNS query response is sent back to the client with the IP address for the FQDN.



DNS The DNS Lookup Process(Contd.)

Steps involved in DNS resolution:

Step 5 - The DNS server matches the FQDN with its IP address.



DNS **DNS Message Format**

- DNS uses UDP port 53 for DNS queries and responses.
- If a DNS response exceeds 512 bytes, Dynamic DNS (DDNS) is used.
- The DNS protocol communications use a single format called a **message**.
- DNS uses the same message format for all types of client queries and server responses, error messages, and transfer of resource record information.



DNS DNS Message Format (Contd.)

Sections of DNS message format :

DNS message section	Description
Question	The question for the server. It contains the domain name to be resolved, the class of domain, and the query type.
Answer	The DNS resource record, or RR, for the query including the resolved IP address depending on the RR type.
Authority	Contains the RRs for the domain authority.
Additional	Relevant to query responses only. Consists of RRs that hold additional information that will make query resolution more efficient

DNS Dynamic DNS

CISCO

- Dynamic DNS (DDNS) allows a user or organization to register an IP address with a domain name as in DNS.
- The subdomain is mapped to the IP address of the user's server, or home router connection to the internet.
- When a change is detected, the DDNS provider is immediately informed of the change and the mapping between the user's subdomain and the internet IP address is immediately updated.



 The DDNS provider service supplies that IP address to the resolver's second level DNS server. This DNS server, either at the organization or ISP, provides the DDNS IP address to the resolver.

DNS The WHOIS Protocol

- WHOIS is a TCP-based protocol that is used to identify the owners of internet domains through the DNS system.
- The WHOIS application uses a query, in the form of a FQDN.
- WHOIS is a starting point for identifying potentially dangerous internet locations that may have been reached through the network.
- ICANN Lookup, an internet-based WHOIS tool, is used to obtain the registration record a URL.

A	简体中文 English	Français	Русский Espaf	Portu العربية أoi	guese
ICANNILOOKUP	ABOUT WHOIS I	POLICIES	GET INVOLVED	WHOIS COMPLAINTS	KNOWLEDGE CENTER

Domain Name Registration Data Lookup

Enter a domain name	Frequently Asked Questions (FAQ)	
Enter a domain		Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN <u>Privacy Policy</u>, and agree to abide by the website <u>Terms of Service</u> and the <u>Domain Name Registration Data Lookup Terms of Use</u>.

About ICANN's Domain Name Registration Data Lookup

This tool gives you the ability to look up the registration data for domain names. More information about this tool and how it works can be found here: https://lookup.icann.org/faq.

DOMAIN NAME REGISTRATION DATA LOOKUP TERMS OF USE

The Domain Name Registration Data Lookup conducts Registration Data Access Protocol (RDAP) queries. RDAP enables users to access current registration data and was created as an eventual replacement for the WHOIS protocol. The results displayed come directly from registry operators and/or registrars in real-time. ICANN does not generate, collect, retain, or store any data associated with an RDAP compliant lookup. If the queried information is not available in RDAP, the query will be redirected to whols.lcann.org (WHOIS failover lookup). In cases of WHOIS failover lookups, ICANN may generate, collect, retain or store the domain name queried and the results for the transitory duration necessary to show results in response to real-time queries.

The Domain Name Registration Data lookup and WHOIS failover lookup results are shown to help users obtain information about domain name registration records, and for no other purpose. Livers agree to use this data only for lawful purposes in accordance with the ICANN Privacy Policy and the

DNS

Lab - Using Wireshark to Examine a UDP DNS Capture

- In this lab, you will complete the following objectives:
 - Communicate with a DNS server by sending a DNS query using the UDP transport protocol.
 - Use Wireshark to examine the DNS query and response exchanges with the same server.

10.3 NAT



NAT IPv4 Private Address Space

- To allow a device with a private IPv4 address to access devices and resources outside the local network, the private address must be translated to a public address.
- NAT provides the translation of private addresses to public addresses.
- A single, public IPv4 address can be shared by thousands of devices, each configured with a unique private IPv4 address.
- The solution to the exhaustion of IPv4 address space and the limitations of NAT is the eventual transition to IPv6.

ululu cisco



NAT What is NAT?

- NAT is used to conserve public IPv4 addresses.
- NAT-enabled routers can be configured with one or more valid public IPv4 addresses which are known as the NAT pool.
- A NAT router typically operates at the border of a stub network.
- When a device inside the stub network wants to communicate with a device outside its network, the packet is forwarded to the border router and the router performs the NAT process.

Note: The connection to the ISP may use a private address or a public address that is shared among customers. For the purposes of this module, a public address is shown.



NAT How NAT works?

- In this example, PC1 with private address 192.168.10.10 wants to communicate with an outside web server with public address 209.165.201.1.
- Click the Play button in the figure to view the animation.



NAT Port Address Translation

- Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.
- When a device initiates a TCP/IP session, it generates a TCP or UDP source port value, or a specially assigned query ID for ICMP, to uniquely identify the session.
- PAT ensures that devices use a different TCP port number for each session with a server on the internet.
- PAT adds unique source port numbers to the inside global address to distinguish between translations.

Click Play in the figure to view an animation of the PAT process.



10.4 File Transfer and Sharing Services



File Transfer and Sharing Services FTP and TFTP

- FTP allows data transfers between a client and a server.
- An FTP client runs on a computer and is used to push and pull data from an FTP server.
- FTP connections between the client and server:
 - **Control Connection**: The client opens the first connection to the server for control traffic.
 - Data Connection: The client opens the second connection to the server for data traffic.
 - Trivial File Transfer Protocol (TFTP) is a simplified file transfer protocol that uses wellknown UDP port number 69.



CISCO

File Transfer and Sharing Services SMB

- The Server Message Block (SMB) is a client/server file sharing protocol that describes the structure of shared network resources.
- SMB is a client/server, request-response protocol.
- Servers can make their own resources available to clients on the network.



File Transfer and Sharing Services SMB (Contd.)

- SMB messages can start, authenticate, and terminate sessions, control file and printer access, and allow an application to send or receive messages to or from another device.
- SMB file sharing and print services have become the mainstay of Microsoft networking.
- A file may be copied from PC to PC with Windows Explorer using the SMB protocol.



File Transfer and Sharing Services Lab - Using Wireshark to Examine TCP and UDP Captures

- In this lab, you will complete the following objectives:
 - Identify TCP Header Fields and Operation Using a Wireshark FTP Session Capture
 - Identify UDP Header Fields and Operation Using a Wireshark TFTP Session Capture

10.5 Email



Email

Email protocols

- Email is a store-and-forward method of sending, storing, and retrieving electronic messages across a network.
- Email clients communicate with mail servers to send and receive email.
- Email supports three separate protocols for operation: Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and IMAP.
- A client retrieves email using one of the two application layer protocols: POP or IMAP.



Email SMTP

- SMTP message formats require a message header and a message body.
- When a client sends an email, the client SMTP process connects with a server SMTP process on a well-known port 25.
- When the server receives the message, it either places the message in a local account, if the recipient is local, or forwards the message to another mail server for delivery.
- Periodically, the server checks the queue for messages and attempts to send them again. If the message is still not delivered after a predetermined expiration time, it is returned to the sender as undeliverable.



Email POP3

- POP3 is used by an application to retrieve a mail from a mail server.
- With POP3, email messages are downloaded to the client and removed from the server.
- The server starts the POP3 service by passively listening on TCP port 110 for client connection requests.
- The client sends a request to establish a TCP connection with the server.
- Once the connection is established, the POP3 server sends a greeting. The client and POP3 server then exchange commands and responses until the connection is closed or aborted.



Email

- IMAP is the protocol that describes a method to retrieve email messages.
- When the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted.
- Users view copies of the messages in their email client software.
- Users can create a file hierarchy on the server to organize and store mail.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



10.6 HTTP



HTTP

Hypertext Transfer Protocol and Hypertext Markup Language

- When a web address or Uniform Resource Locator (URL) is typed into a web browser, the web browser establishes a connection with the web service that is using the HTTP protocol.
- Lets take a look on how a web page is opened in a browser.
 Example: <u>http://www.cisco.com/index.html</u>

Step 1: The browser interprets the three parts of the URL:

- http (the protocol or scheme)
- <u>www.cisco.com</u> (the server name)
- index.html (the specific filename requested)



HTTP

Hypertext Transfer Protocol and Hypertext Markup Language (Contd.)

- Step 2: The client initiates an HTTP request to a server by sending a GET request to the server and asks for the index.html file.
- Step 3: In response to the request, the server sends the HTML code for this web page to the



• Step 4: The browser deciphers the HTML code and formats the page for the browser window.





HTTP The HTTP URL

- HTTP URLs can specify the port on the server that should handle the HTTP methods.
- It can specify a query string and fragment.
- Query strings are preceded by a "?" character and typically consist of a series of name and value pairs.
- A fragment is preceded by a "#" character. It refers to a subordinate part of the resource that is requested in the URL.
- The parts of an HTTP URL are shown in the below figure:



HTTP Operation

- HTTP is a request/response protocol that uses TCP port 80.It is flexible but not a secure protocol.
- When a client sends a request to a web server, it will use one of the six methods specified by HTTP:
 - GET
 - POST
 - PUT

- DELETE
- OPTIONS
- CONNECT



HTTP HTTP Status Codes

- The HTTP Status codes are numeric, with the first number in the code indicating the type of message.
- The five status code groups are 1xx Informational, 2xx Success, 3xx Redirection,
 4xx Client Error and 5xx Server Error
- The below table explains some common status codes:

Code	Status	Meaning
1xx - Informational		
100	Continue	The client should continue with the request. The Server has verified that the request can be fulfilled.
2xx - Success		
200	OK	The request completed successfully.
202	Accepted	The request has been accepted for processing, but processing is not completed.

HTTP HTTP Status Codes (Contd.)

Code	Status	Meaning
4xx – Client Error		
403	Forbidden	The request is understood by the server, but the resource will not be fulfilled. This is possibly because the requester is not authorized to view the resource.
404	Not Found	The server could not find the requested resource. This can be caused by an out-of-date or incorrect URL.

HTTP HTTP/2

- The purpose of HTTP/2 is to improve HTTP performance by addressing latency issues that existed in the HTTP 1.1 version of the protocol.
- HTTP/2 uses the same header format as HTTP 1.1 and uses the same status codes.
- Few important features of HTTP/2 that a cybersecurity analyst must be aware of:
 - Multiplexing
 - Server PUSH
 - A binary protocol
 - Header compression

uluilu cisco



HTTP Securing HTTP – HTTPS

- For secure communication across the internet, the HTTP Secure (HTTPS) protocol is used.
- HTTPS uses authentication and encryption to secure data as it travels between the client and the server.
- HTTPS uses the same client request-server response process as HTTP, but the data stream is encrypted with Secure Socket Layer (SSL), or Transport Layer Security (TLS), before being transported across the network.
- HTTPS/2 is specified to use HTTPS over TLS with the Application-Layer Protocol Negotiation (ALPN) extension for TLS 1.2 or newer.
- Confidential information is transmitted over the Internet using HTTPS.

HTTP

Lab - Using Wireshark to Examine HTTP and HTTPS Traffic

- In this lab, you will complete the following objectives:
 - Capture and view HTTP traffic
 - Capture and view HTTPS traffic

10.7 Network Services Summary



Network Services Summary What Did I Learn in this Module?

- Dynamic Host Configuration Protocol (DHCP) for IPv4 automates the assignment of IPv4 addresses. This is referred to as dynamic addressing and is the alternative to static addressing.
- DHCP operation includes: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, and DHCPNAK.
- DNS resolves names to IP addresses. There are five steps involved in DNS resolution.
- NAT provides the translation of private addresses to public addresses. A NAT router typically operates at the border of a stub network.
- Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.
- FTP was developed to allow for file transfers between a client and a server. Trivial File Transfer Protocol (TFTP) is a simplified file transfer protocol that uses UDP port number 69.

Network Services Summary What Did I Learn in this Module? (Contd.)

- Email clients communicate with mail servers to send and receive email.
- Email supports three separate protocols for operation: SMTP, POP, and IMAP.
- Web browsers and web servers interact using the four steps.
- HTTP is a request/response protocol that uses TCP port 80.
- When a client sends a request to a web server, it will use one of six methods that are specified by the HTTP protocol: GET, POST, PUT, DELETE, OPTIONS, and CONNECT.
- HTTP status codes: 1xx, 2xx, 3xx, 4xx, and 5xx.
- For secure communication across the internet, HTTP Secure (HTTPS) is used.
- HTTPS uses authentication and encryption to secure data as it travels between the client and the server.

··II··II·· CISCO