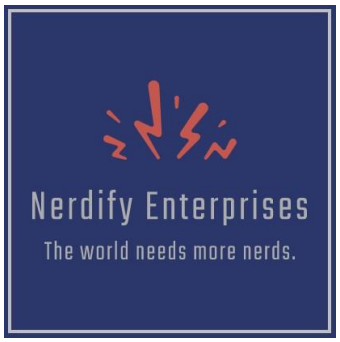
Using Wireshark to View IPv4 Header Information

Introduction

As a member of the IT team at Nerdify Enterprises, you notice an unusual amount of heavy traffic on the network. To make sure that all of the traffic is legitimate, you use a protocol analyzer named Wireshark to capture some random packets for further testing.



Objective

In this lab, the student will use Wireshark to view, examine, and document the fields in an IPv4 header.

Resources

- Computer with Internet connection
- Wireshark Protocol Analyzer application installed on the computer

ASSIGNMENT

Estimated Time for Completion: 30 minutes

1. **Open** the Wireshark Protocol Analyzer by clicking the icon on the computer desktop.

2. Click the **Capture** menu, then click **Interfaces**. You may also have your interface (network card) listed on the opening screen. If you do, then just click on the name of the Interface (NIC) card.

3. Open a command prompt window by clicking the **Start button**, type **cmd** in the Start menu search box, then Enter.

4. Ping the IPv4 address of Google's DNS servers by typing in **ping 8.8.8.8**.

5. Type **exit** and press **Enter** to close the command prompt window.

6. In Wireshark, click **Capture** on the menu bar and then click **Stop** (or you can click the **Stop** icon on the Toolbar).

7. Select a **TCP** or **UDP** packet in the packet list pane (the upper pane). *Hint: click on the Protocol field in the upper pane and the protocols will be listed in alphabetical order. Once they are listed in alphabetical order, just scroll down until you see the "T's" for the TCP packet or the "U's" for the UDP packet.*

8. In the packet details pane (the middle pane), click the + sign next to **Internet Protocol Version 4**.

9. What is the value listed for the **Version** field? Version 4

10. What is the value listed for the **Header Length** field? 20bytes

11. Click the + sign next to **Differentiated Services**.

12. What value is listed for the **Total Length** field? 40

13. What is the value listed for the **Identification** field? 0x33cb (13259)

14. Click the + sign next to **Flags**.

15. What value is listed for the **Time to Live** field? 44

16. What value is listed for the **Protocol** field? TCP (6)

17. What is the **Source IP Address** listed? (Answers will vary) 20.109.108.169

18. What is the **Destination IP Address** listed? (Answers will vary) 192.168.1.194

19. Click File, Save As, and save your Capture File as "IPv4 - *YourName*" and click Save. Include the packet capture with your assignment sheet. Which packet did you examine?

Reflection

1. What are the fields of an IPv4 packet? Version, header , total length , Identification, Flags , Time to live ,protocol , header check sum , Source and destination
2. What are the main functions of the fields in an IPv4 packet?

Version field sets the version of IP protocol.

Header tells us the size in bits

Total length is the total size of the packet.

Identification If the packet is broken down into segments the destination node uses the ID to put the packet together in the proper order

Flags are used to enable fragment.

Time to Live Used to discard the undeliverable packets.

Protocol determines the protocol that will receive the payload of the packet on the destination node.

Headercheck sum Provides a checksum on the header only the payload is not included in the checksum calculation.

Source Provides information on the sending device.

Destination Provides information on the destination device.

Rubric

Standards for This Competency	EXEMPLARY	ACCOMPLISHED	DEVELOPING	BEGINNING
Version field (format of the header) (10 points)	Correctly identified (10 pt)	Incorrect identification (0 pt)		

Header length field (# of bytes in header) (10 points)	Correctly identified (10 pt)	Incorrect identification (0 pt)
Total length field (# of bytes in packet) (10 points)	Correctly identified (10 pt)	Incorrect identification (0 pt)
Identification field (Value used to reassemble packets) (10 points)	Correctly identified (10 pt)	Incorrect identification (0 pt)
Listed Time to Live field (maximum hops before packet is discarded) (10 points)	Correctly identified (10 pt)	Incorrect identification (0 pt)
Listed protocol field (10 points)	Correctly identified (10 pt)	Incorrect identification (0 pt)
Source IP Address (IP of originating NIC)	Correctly identified (10 pt)	Incorrect identification (0 pt)

(10 points)		
Destination IP Address (IP of destination NIC) (10 points)	Correctly identified (10 pt)	Incorrect identification (0 pt)

Reflection Question #1	Answer is fully developed. (10 pt)	Answer is partially developed. (8 pt)	Answer lacks adequate support for chosen topology. (5 pt)	Answer shows lack of understanding of network topologies. (0 pt)
Reflection Question #2	Answer is fully developed. (10 pt)	Answer is partially developed. (8 pt)	Answer lacks adequate support for chosen topology. (5 pt)	Answer shows lack of understanding of network topologies. (0 pt)