

CYB 310 Module Two Lab Worksheet

Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

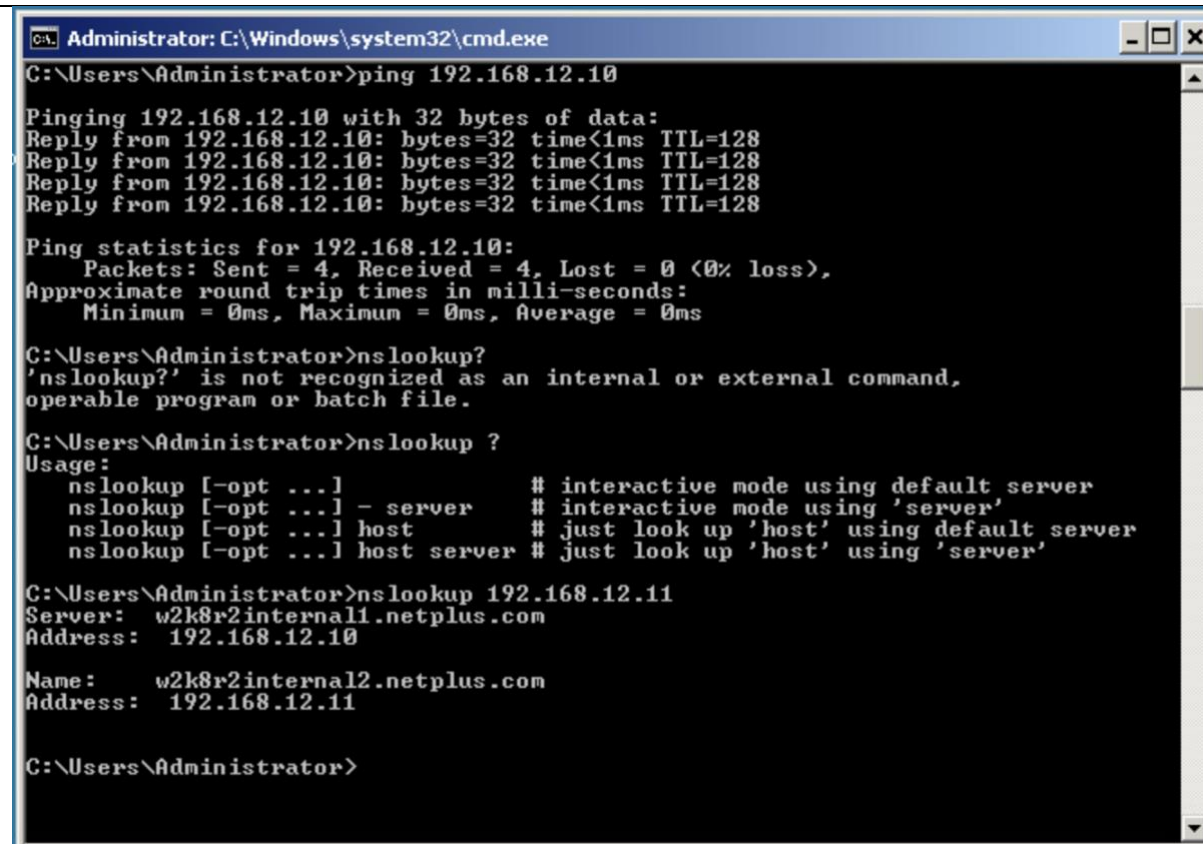
The OSI Model	
Prompt	Response
What HTTP message type is used to request data?	The HTTP message type used to request data is GET.
Identify which flags are set in each of the three segments of the three-way handshake.	SYN: The first segment, used to initiate a connection, sets the SYN flag. SYN-ACK: The second segment in response sets both SYN and ACK flags. ACK: The third segment confirms the connection by setting the ACK flag.
What command can be used on a Windows machine to view the MAC address?	The command ipconfig /all can be used on a Windows machine to view the MAC address.

Network Troubleshooting

Prompt

In the lab, “Troubleshooting a Suspected DNS issue Using CLI Utilities,” **Step 11**, type your name after the command prompt and take a screenshot of the output after running the nslookup command.

Response



```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 192.168.12.10

Pinging 192.168.12.10 with 32 bytes of data:
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>nslookup?
'nslookup?' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>nslookup ?
Usage:
    nslookup [-opt ...]           # interactive mode using default server
    nslookup [-opt ...] - server  # interactive mode using 'server'
    nslookup [-opt ...] host      # just look up 'host' using default server
    nslookup [-opt ...] host server # just look up 'host' using 'server'

C:\Users\Administrator>nslookup 192.168.12.11
Server:  w2k8r2internal1.netplus.com
Address: 192.168.12.10

Name:    w2k8r2internal2.netplus.com
Address: 192.168.12.11

C:\Users\Administrator>
  
```

In the lab, “Troubleshooting a Suspected DNS issue Using CLI Utilities,” **Step 14**, take a screenshot of the webpage after correcting the URL.



What utility can be used to find out the IP address, subnet mask, and default gateway configured on a computer?

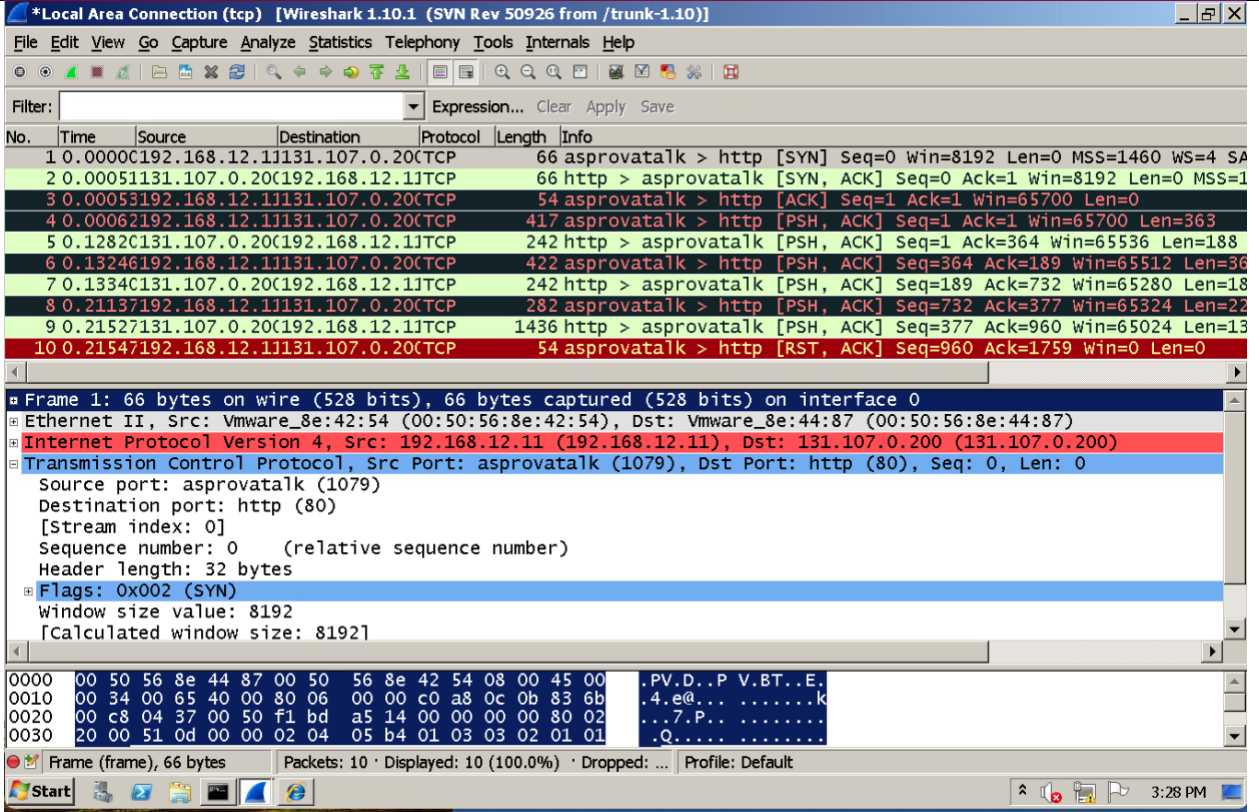
The utility **ipconfig /all** can be used to find out detailed information including the IP address, subnet mask, and default gateway configured on a computer.

What is the function of the ipconfig/release and the ipconfig/renew commands?

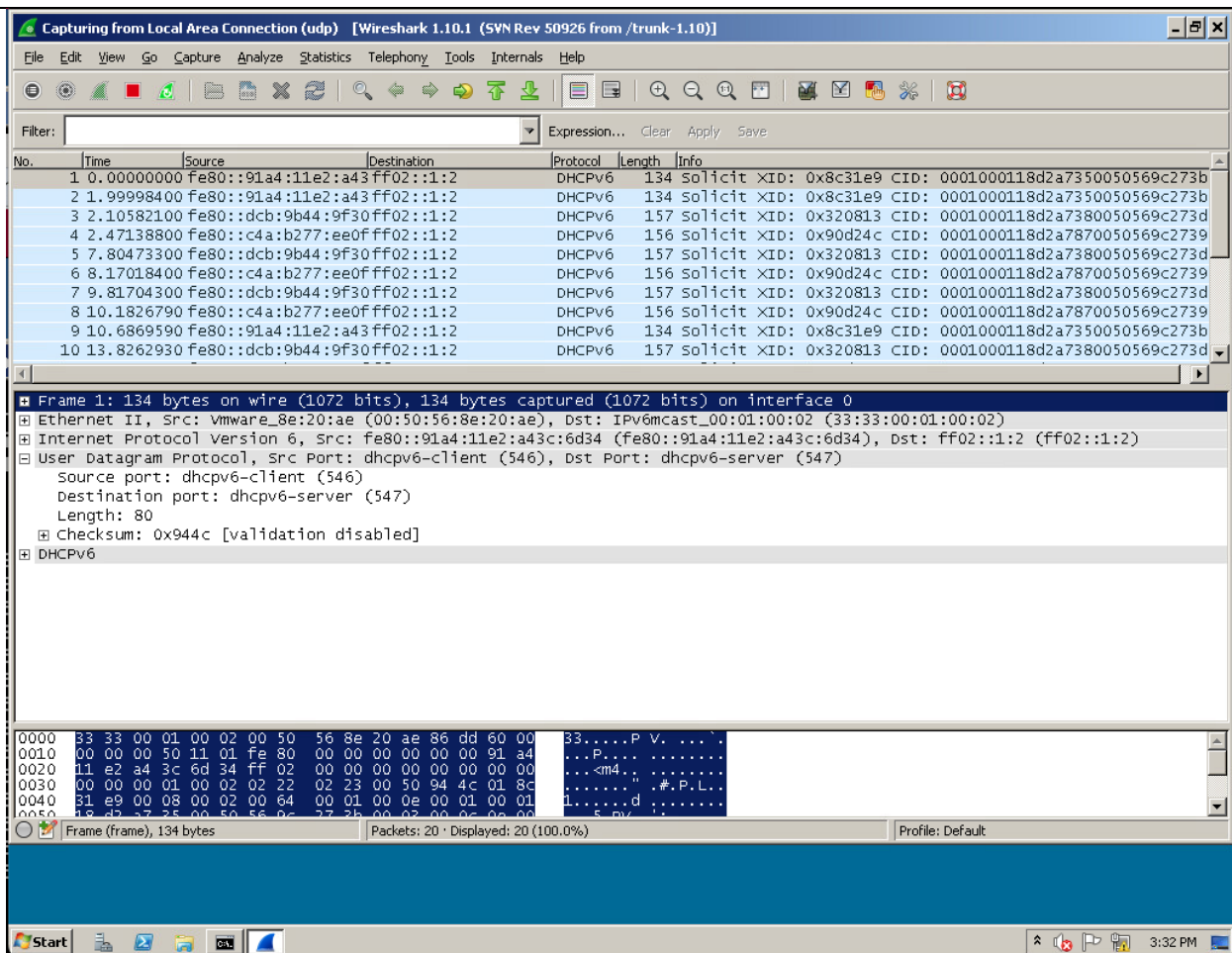
ipconfig/release: This command releases the IP address assigned to the computer.
ipconfig/renew: This command renews the IP address, allowing the computer to request a new IP address from the DHCP server.

<p>What type of devices would be better served to have static IP configuration?</p>	<p>Devices that require constant network availability and accessibility, such as servers, network printers, or other critical infrastructure components, would be better served to have static IP configuration.</p>
---	--

TCP/IP Protocols – The Core Protocols

Prompt	Response
<p>In the lab, “Capture and Analyze Transport Layer Protocol Packets,” Step 10, take a screenshot of the output of the field details of the TCP segment.</p>	 <p>The screenshot displays the Wireshark interface with a packet capture of an HTTP SYN request. The packet list shows 10 packets. Packet 1 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (SYN). The packet bytes pane shows the raw data in hexadecimal and ASCII.</p> <p>Packet 1 Details:</p> <ul style="list-style-type: none"> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 Ethernet II, Src: Vmware_8e:42:54 (00:50:56:8e:42:54), Dst: Vmware_8e:44:87 (00:50:56:8e:44:87) Internet Protocol Version 4, Src: 192.168.12.11 (192.168.12.11), Dst: 131.107.0.200 (131.107.0.200) Transmission Control Protocol, Src Port: asprovataik (1079), Dst Port: http (80), Seq: 0, Len: 0 <ul style="list-style-type: none"> Source port: asprovataik (1079) Destination port: http (80) [Stream index: 0] Sequence number: 0 (relative sequence number) Header length: 32 bytes Flags: 0x002 (SYN) Window size value: 8192 [Calculated window size: 8192] <p>Packet Bytes:</p> <pre> 0000 00 50 56 8e 44 87 00 50 56 8e 42 54 08 00 45 00 .PV.D..P.V.BT..E. 0010 00 34 00 65 40 00 80 06 00 00 c0 a8 0c 0b 83 6b .4.e@... ..k 0020 00 c8 04 37 00 50 f1 bd a5 14 00 00 00 00 80 02 ...7.P... .. 0030 20 00 51 0d 00 00 02 04 05 b4 01 03 03 02 01 01 .Q..... </pre>

In the lab, “Capture and Analyze a UDP Datagram,” **Step 8**, take a screenshot of the output of the User Datagram Protocol field details.



Capturing from Local Area Connection (udp) [Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	fe80::91a4:11e2:a43:ff02::1:2	ff02::1:2	DHCPv6	134	solicit XID: 0x8c31e9 CID: 0001000118d2a7350050569c273b
2	1.99998400	fe80::91a4:11e2:a43:ff02::1:2	ff02::1:2	DHCPv6	134	solicit XID: 0x8c31e9 CID: 0001000118d2a7350050569c273b
3	2.10582100	fe80::dcb:9b44:9f30:ff02::1:2	ff02::1:2	DHCPv6	157	solicit XID: 0x320813 CID: 0001000118d2a7380050569c273d
4	2.47138800	fe80::c4a:b277:ee0:ff02::1:2	ff02::1:2	DHCPv6	156	solicit XID: 0x90d24c CID: 0001000118d2a7870050569c2739
5	7.80473300	fe80::dcb:9b44:9f30:ff02::1:2	ff02::1:2	DHCPv6	157	solicit XID: 0x320813 CID: 0001000118d2a7380050569c273d
6	8.17018400	fe80::c4a:b277:ee0:ff02::1:2	ff02::1:2	DHCPv6	156	solicit XID: 0x90d24c CID: 0001000118d2a7870050569c2739
7	9.81704300	fe80::dcb:9b44:9f30:ff02::1:2	ff02::1:2	DHCPv6	157	solicit XID: 0x320813 CID: 0001000118d2a7380050569c273d
8	10.18267900	fe80::c4a:b277:ee0:ff02::1:2	ff02::1:2	DHCPv6	156	solicit XID: 0x90d24c CID: 0001000118d2a7870050569c2739
9	10.68695900	fe80::91a4:11e2:a43:ff02::1:2	ff02::1:2	DHCPv6	134	solicit XID: 0x8c31e9 CID: 0001000118d2a7350050569c273b
10	13.82629300	fe80::dcb:9b44:9f30:ff02::1:2	ff02::1:2	DHCPv6	157	solicit XID: 0x320813 CID: 0001000118d2a7380050569c273d

Frame 1: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0

- Ethernet II, Src: Vmware_8e:20:ae (00:50:56:8e:20:ae), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)
- Internet Protocol Version 6, Src: fe80::91a4:11e2:a43c:6d34 (fe80::91a4:11e2:a43c:6d34), Dst: ff02::1:2 (ff02::1:2)
- User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
 - Source port: dhcpv6-client (546)
 - Destination port: dhcpv6-server (547)
 - Length: 80
 - Checksum: 0x944c [validation disabled]
- DHCPv6

0000 33 33 00 01 00 02 00 50 56 8e 20 ae 86 dd 60 00 33P V. ...
 0010 00 00 00 50 11 01 fe 80 00 00 00 00 00 00 91 a4 ...P.....
 0020 11 e2 a4 3c 6d 34 ff 02 00 00 00 00 00 00 00 ...<m4.....
 0030 00 00 00 01 00 02 02 22 02 23 00 50 94 4c 01 8c#P.L..
 0040 31 e9 00 08 00 02 00 64 00 01 00 0e 00 01 00 1l.....d.....
 0050 18 47 37 25 00 50 56 0c 27 2b 00 02 00 0c 00 00 5.....

Frame (frame), 134 bytes Packets: 20 · Displayed: 20 (100.0%) Profile: Default

3:32 PM

What type of packet is an ARP request?

An ARP request is a broadcast packet used to request the MAC address of a host on the local network segment.

What type of packet is an ARP reply?	An ARP reply is a unicast packet sent in response to an ARP request, providing the requested MAC address.
--------------------------------------	---