

Laboratorio 7

Jorge Parra Hidalgo

ITIT

13104

Trafico DNS

En las ventanas de información del PDU se presenta información sobre el tráfico que circula por los dispositivos de la red. En este caso, se detallan los procesos que tienen lugar en la capa 3 del modelo OSI, incluyendo las direcciones IP de origen y destino, los protocolos utilizados y los puertos. El tráfico que se muestra a continuación se ha generado entre una PC y un servidor utilizando DNS.

De ida:

The screenshot displays the 'PDU Information at Device: JorgeCoreULSA' window. It features three tabs: 'OSI Model' (selected), 'Inbound PDU Details', and 'Outbound PDU Details'. The 'OSI Model' tab shows a summary of the packet's path and details for each layer. The 'In Layers' column lists Layer 7 through Layer 1, with Layer 3 highlighted in yellow. The 'Out Layers' column lists Layer 7 through Layer 1, with Layer 3 highlighted in yellow. A large arrow points from the 'In Layers' column to the 'Out Layers' column, indicating the flow of the packet. Below the layers, a note states: '1. The device looks up the destination IP address in the routing table.'

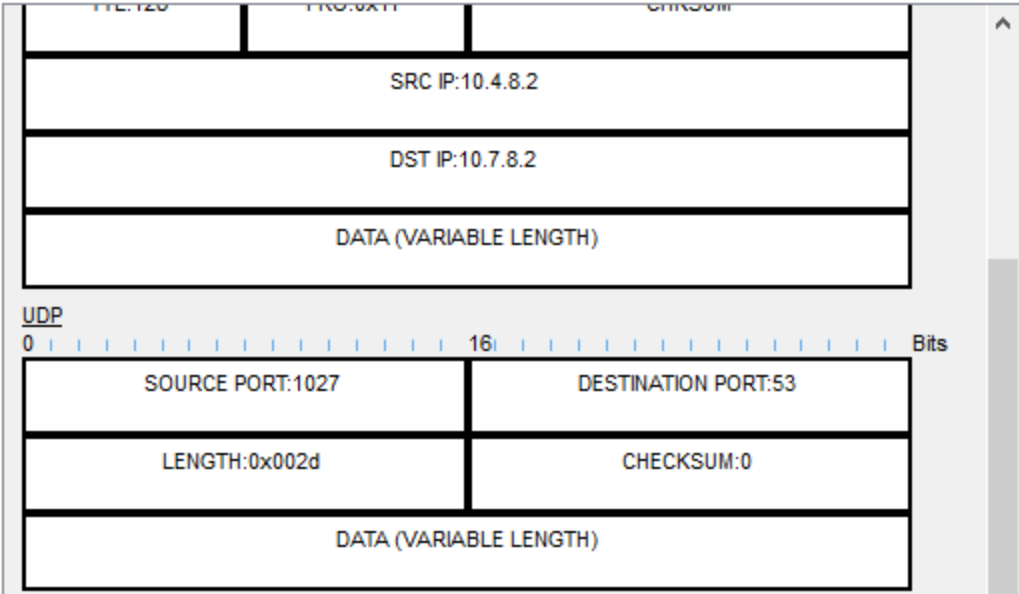
PDU Information at Device: JorgeCoreULSA	
At Device: JorgeCoreULSA Source: JorgeULSA10.4.8.2 Destination: 10.7.8.2	
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 10.4.8.2, Dest. IP: 10.7.8.2	Layer 3: IP Header Src. IP: 10.4.8.2, Dest. IP: 10.7.8.2
Layer 2: Ethernet II Header 0003.E43D.09C8 >> 0030.F2C4.2E01	Layer 2: Ethernet II Header 00E0.B057.8718 >> 000C.CFDA.5B01
Layer 1: Port GigabitEthernet1/0/1	Layer 1: Port(s): GigabitEthernet1/0/24

1. The device looks up the destination IP address in the routing table.

PDU Information at Device: JorgeCoreULSA

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats



De vuelta:

PDU Information at Device: Jorge Router DMZ

OSI Model Inbound PDU Details Outbound PDU Details

At Device: Jorge Router DMZ Source: JorgeULSA10.4.8.2 Destination: 10.7.8.2	
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 10.7.8.2, Dest. IP: 10.4.8.2	Layer 3: IP Header Src. IP: 10.7.8.2, Dest. IP: 10.4.8.2
Layer 2: Ethernet II Header 0001.636E.DD18 >> 00D0.FF23.6B01	Layer 2: Ethernet II Header 00D0.FF23.6B02 >> 0001.96B2.EB03
Layer 1: Port GigabitEthernet0/0	Layer 1: Port(s): GigabitEthernet0/1

1. The device looks up the destination IP address in the CEF table.

PDU Information at Device: Jorge Router DMZ

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

ID:0x0009		FLA GS:0	FRAG OFFSET:0x000
TTL:127	PRO:0x11	CHKSUM	
SRC IP:10.7.8.2			
DST IP:10.4.8.2			
DATA (VARIABLE LENGTH)			

UDP

SOURCE PORT:53		DESTINATION PORT:1027	
LENGTH:0x0050		CHECKSUM:0	
DATA (VARIABLE LENGTH)			

0 16 Bits

Trafico HTTP

Después de que se han transmitido todos los datos de la PC al servidor (y viceversa) a través de DNS, se activa el protocolo HTTP. En la capa 3 del modelo OSI, se observa que los switches en cada sección de la red buscan las IPs de destino en sus tablas de enrutamiento antes de proceder con el tráfico de datos. Además, en los detalles de Inbound se indica que se está utilizando el puerto 80 en lugar del puerto 53, que es el que corresponde al protocolo DNS.

De ida:

PDU Information at Device: JorgeCoreULSA



OSI Model Inbound PDU Details Outbound PDU Details

At Device: JorgeCoreULSA
Source: JorgeULSA10.4.8.2
Destination: HTTP CLIENT

In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 10.4.8.2, Dest. IP: 10.7.8.2
Layer 2: Ethernet II Header 0003.E43D.09C8 >> 0030.F2C4.2E01
Layer 1: Port GigabitEthernet1/0/1

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 10.4.8.2, Dest. IP: 10.7.8.2
Layer 2: Ethernet II Header 00E0.B057.8718 >> 000C.CFDA.5B01
Layer 1: Port(s): GigabitEthernet1/0/24

1. The device looks up the destination IP address in the routing table.

PDU Information at Device: JorgeCoreULSA



OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

ID:0x0011		FLA GS:0	FRAG OFFSET:0x000
TTL:128	PRO:0x06	CHKSUM	
SRC IP:10.4.8.2			
DST IP:10.7.8.2			
DATA (VARIABLE LENGTH)			

TCP

0 4 8 16 24 Bits

SOURCE PORT:1027	DESTINATION PORT:80
SEQUENCE NUMBER:1	
ACKNOWLEDGEMENT NUMBER:1	

De vuelta:

PDU Information at Device: Jorge Router DMZ

OSI Model

Inbound PDU Details

Outbound PDU Details

At Device: Jorge Router DMZ
Source: JorgeULSA10.4.8.2
Destination: HTTP CLIENT

In Layers

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 10.7.8.2, Dest. IP: 10.4.8.2

Layer 2: Ethernet II Header
0001.636E.DD18 >> 00D0.FF23.6B01

Layer 1: Port GigabitEthernet0/0

Out Layers

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 10.7.8.2, Dest. IP: 10.4.8.2

Layer 2: Ethernet II Header
00D0.FF23.6B02 >> 0001.96B2.EB03

Layer 1: Port(s): GigabitEthernet0/1

1. The device looks up the destination IP address in the CEF table.

PDU Information at Device: Jorge Router DMZ

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

ID:0x000b

FLA
GS:0

FRAG OFFSET:0x000

TTL:127

PRO:0x06

CHKSUM

SRC IP:10.7.8.2

DST IP:10.4.8.2

DATA (VARIABLE LENGTH)

TCP

0

4

8

16

24

Bits

SOURCE PORT:80

DESTINATION PORT:1027

SEQUENCE NUMBER:1

ACKNOWLEDGEMENT NUMBER:111

Bloqueo de Firewall

Después de cambiar la IP de la PC de 10.4.8.2 a 10.10.8.2 e intentar establecer una conexión con el servidor, el firewall impide el tráfico porque el paquete de datos con la nueva IP no cumple con ninguno de los criterios establecidos en las listas de acceso configuradas.

PDU Information at Device: Firewall

OSI Model

Inbound PDU Details

At Device: Firewall

Source: JorgeULSA10.4.8.2

Destination: 10.7.8.2

In Layers

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 10.10.8.2, Dest. IP: 10.7.8.2

Layer 2: Ethernet II Header 000C.CFDA.5B02 >> 0001.96B2.EB02

Layer 1: Port GigabitEthernet1/2

Out Layers

Layer7

Layer6

Layer5

Layer4

Layer3

Layer2

Layer1

1. The receiving port has an inbound traffic access-list with an ID of ULSA. The device checks the packet against the access-list.

2. The packet does not match the criteria of any statement in the access-list. The packet is denied and dropped by default.

PDU Information at Device: Firewall

OSI Model Inbound PDU Details

PDU Formats

ID:0x0014		FLA GS:0	FRAG OFFSET:0x000
TTL:126	PRO:0x11	CHKSUM	
SRC IP:10.10.8.2			
DST IP:10.7.8.2			
DATA (VARIABLE LENGTH)			

UDP

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Bits

SOURCE PORT:1028	DESTINATION PORT:53
LENGTH:0x002d	CHECKSUM:0
DATA (VARIABLE LENGTH)	

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	JorgeULSA10.4.8.2	DNS
	0.004	--	JorgeULSA10.4.8.2	DNS
	0.005	JorgeULSA10.4.8.2	JorgeCoreULSA	DNS
	0.006	JorgeCoreULSA	RouterJorgeULSA	DNS
	0.007	RouterJorgeULSA	Firewall	DNS
Visible	15.001	--	JorgeULSA10.4.8.2	DNS

4 de noviembre del 2024