Trama 1

Trama 1

SOURCE MAC --> **MAC:** 00:01:5c:31:bb:c1

Trama 1

SOURCE MAC --> **MAC:** 00:01:5c:31:bb:c1

SOURCE IP --> **IP:** fe80::201:5cff:fe31:bbc1

Trama 1

SOURCE MAC --> **MAC:** 00:01:5c:31:bb:c1

SOURCE IP --> **IP:** fe80::201:5cff:fe31:bbc1

Protocolo ICMP , indica es un router-->

Trama 2

source mac --> **MAC:** 00:01:5c:31:bb:c1

source ip --> **IP:** fe80::201:5cff:fe31:bbc1

Trama 2

Es una solicitud ARP

source MAC --> **MAC:** 00:01:5c:31:bb:c1

Ya no aparece esta SOURCE IP --> **IP:** fe80::201:5cff:fe31:bbc1

Vemos esta nueva IP --> ya que los routers tienen 'n' direcciones IP y está usando ahora esta source IP.

IP_2: 24.6.168.1

Trama 2

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1

Target IP adress de la que solicita la MAC con esta solicitud ARP

IP: 24.6.175.56

Trama 3

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1

IP: 24.6.175.56

Trama 3

El PC estará usando la puerta de enlace del router, para comunicarse con otras subredes.
MAC DESTINO ----> (la de lRouter)

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1

Sabemos con la OUI(3 primeros octetos de la MAC) origen, que se trata de la tarjeta de red de un PC Hewlett Packard

MAC: d4:85:64:a7:bf:a3

IP: 24.6.175.56

Trama 3

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1

MAC: d4:85:64:a7:bf:a3

SOURCE IP --> **IP:** 24.6.173.220

IP: 24.6.175.56

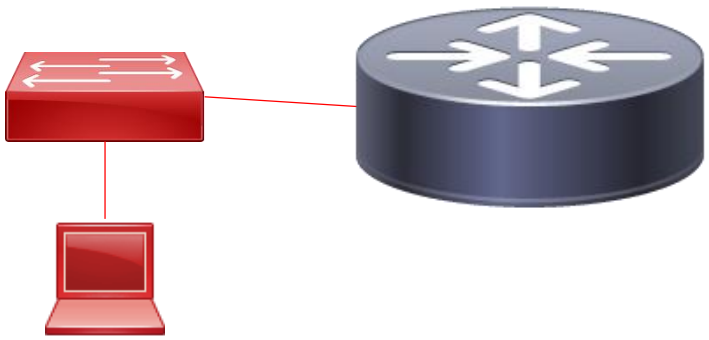
Trama 3

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1

Asumimos que por logica, hay un switch intermedio entre el router y el PC. --->



MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

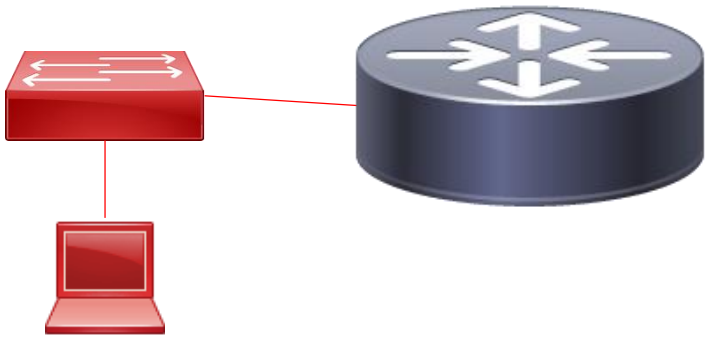
IP: 24.6.175.56

Trama 3

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

IP de destino,
vemos que este segmento
termina con un protoclo de
capa de transporte TCP
donde nos fijamos
en el puerto de destino (80)
probablemente estara
tratando de iniciar comunicación con
un servidor http.

Vemos que este paquete es un SYN
y los 2 siguientes SYN/ACK y ACK
por lo que podemos asumir que
se trata de un three hand shake
para esdtablecer una conexión
HTTP.

IP: 24.6.175.56

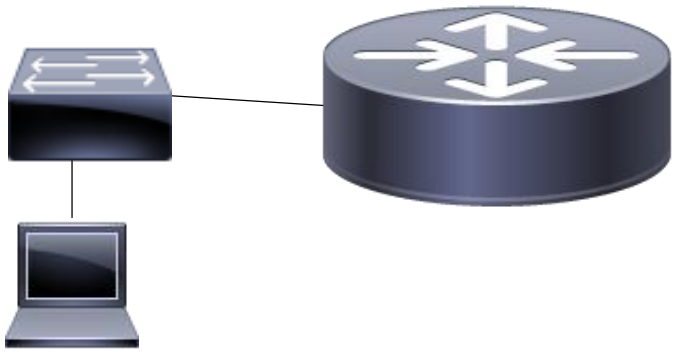
IP: 216.168.252.157

Trama 4

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

IP: 24.6.175.56

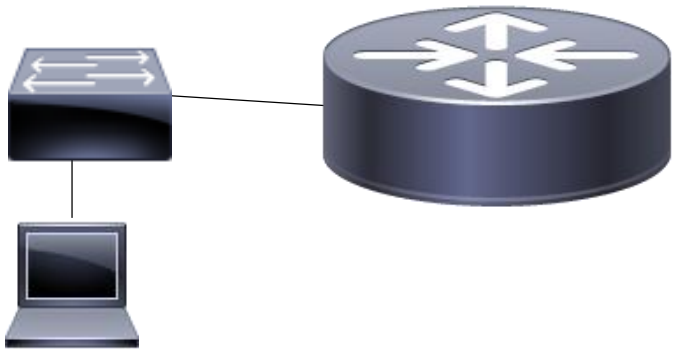
IP: 216.168.252.157

Trama 4

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

IP de destino,
vemos que este segmento

termina con un protoclo de
capa de transporte TCP
donde nos fijamos
en el puerto de destino (80)
probablemente estara
tratando de iniciar comunicación con
un servidor http.

Vemos que este paquete es un SYN
y los 2 siguientes SYN/ACK y ACK
por lo que podemos asumir que
se trata de un three hand shake
para esdtablecer una conexión
HTTP.

IP: 24.6.175.56

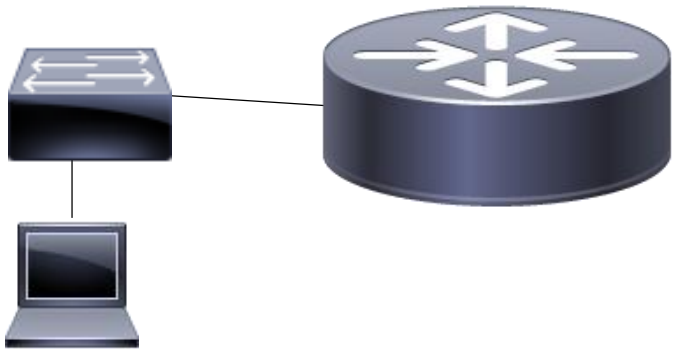
IP: 216.168.252.157

Trama 6

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

IP: 24.6.175.56

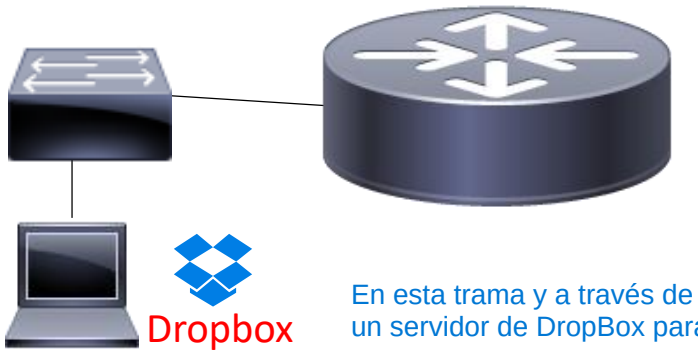
IP: 216.168.252.157

Trama 6

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



En esta trama y a través de la info del protocolo UDP podemos deducir que se está tratando de comunicar con un servidor de DropBox para subir alguna info o etc....

MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

IP: 24.6.175.56

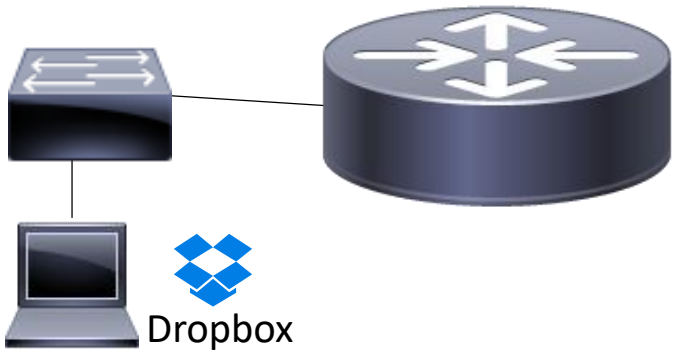
IP: 216.168.252.157

Trama 7

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

IP: 24.6.175.56

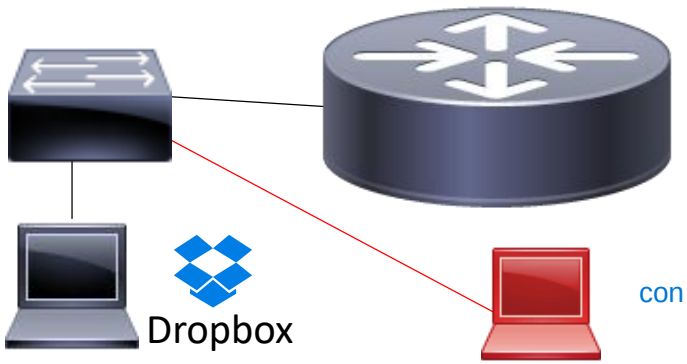
IP: 216.168.252.157

Trama 7

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



con esta OUI sabemos que es una tarjeta de red de una laptop personal de tipo ASUS

MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

MAC: c8:60:00:19:9e:19

IP: 24.6.175.56

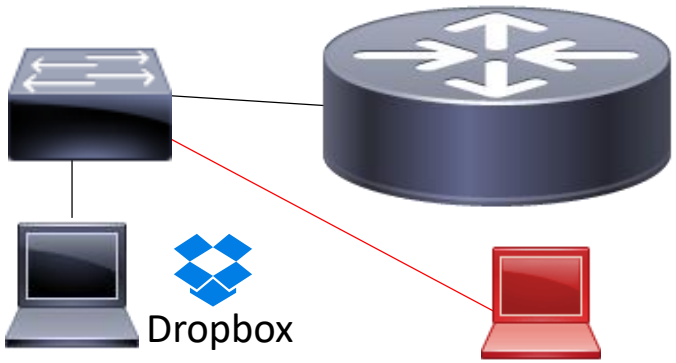
IP: 216.168.252.157

Trama 7

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

MAC: c8:60:00:19:9e:19

IP: 24.6.169.43

IP: 24.6.175.56

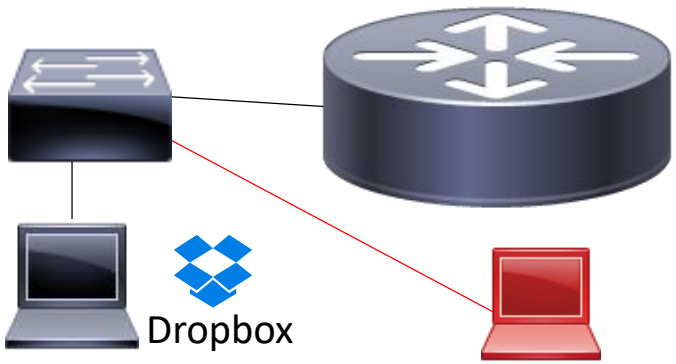
IP: 216.168.252.157

Trama 7

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



ip de destino de esta trama

?

IP: 199.59.150.9

MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

MAC: c8:60:00:19:9e:19

IP: 24.6.169.43

?

IP: 24.6.175.56

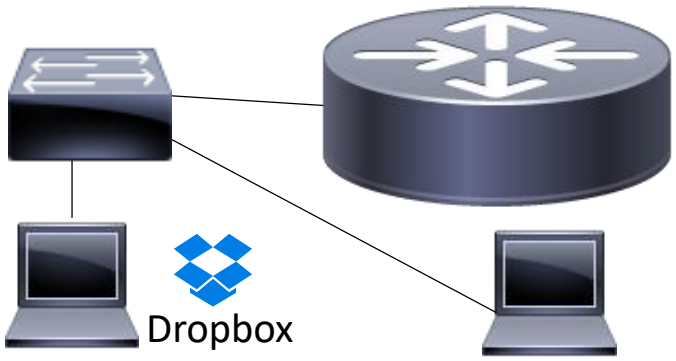
IP: 216.168.252.157

Trama 8

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

MAC: c8:60:00:19:9e:19

IP: 24.6.169.43

IP: 199.59.150.9

IP: 24.6.175.56

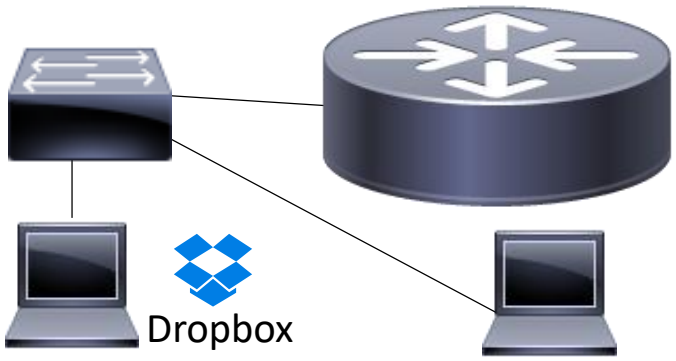
IP: 216.168.252.157

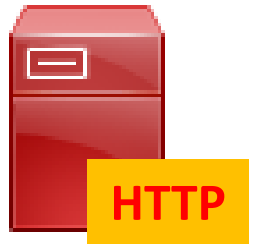
Trama 8

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1





IP: 199.59.150.9

MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

MAC: c8:60:00:19:9e:19

IP: 24.6.169.43

IP: 24.6.175.56

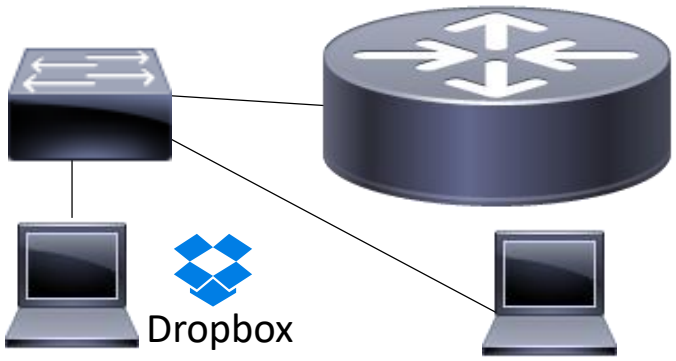
IP: 216.168.252.157

Trama 10

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



IP: 199.59.150.9

MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

MAC: c8:60:00:19:9e:19

IP: 24.6.169.43

IP: 24.6.175.56

IP: 216.168.252.157

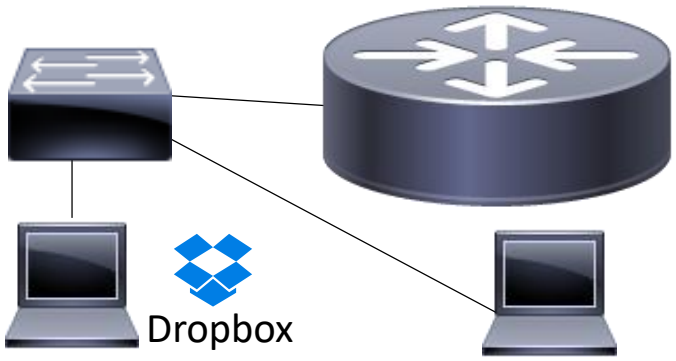
Trama 10

IP: 107.21.109.41

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



IP: 199.59.150.9

MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

MAC: c8:60:00:19:9e:19

IP: 24.6.169.43

IP: 24.6.175.56

IP: 216.168.252.157

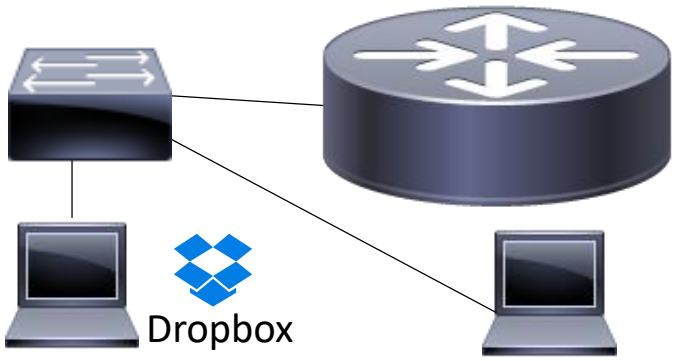
Trama 11

IP: 107.21.109.41

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



IP: 199.59.150.9

MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

MAC: c8:60:00:19:9e:19

IP: 24.6.169.43

IP: 24.6.175.56

IP: 216.168.252.157

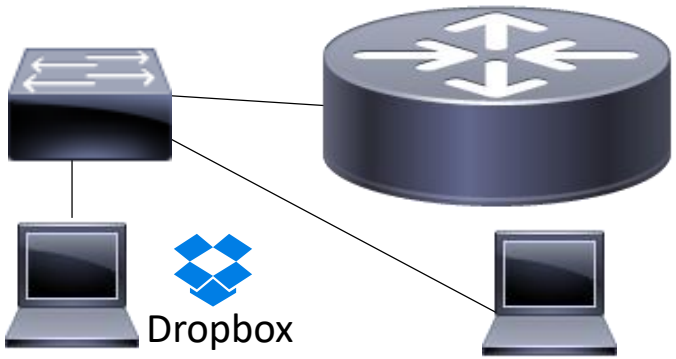
Trama 11

IP: 107.21.109.41

MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1



IP: 199.59.150.9

MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

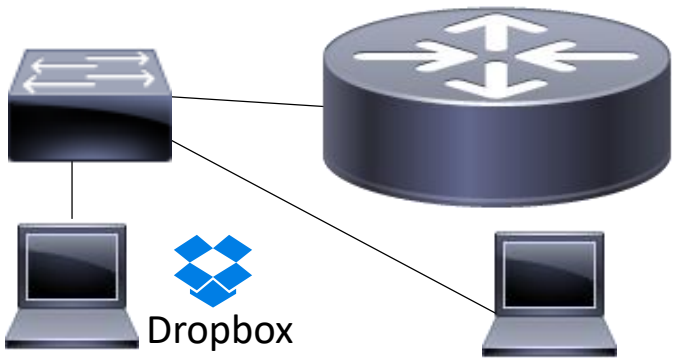
MAC: c8:60:00:19:9e:19

IP: 24.6.169.43

IP: 24.6.175.56

IP: 216.168.252.157

Topologia Final



MAC: 00:01:5c:31:bb:c1

IP: fe80::201:5cff:fe31:bbc1

IP_2: 24.6.168.1

MAC: d4:85:64:a7:bf:a3

IP: 24.6.173.220

MAC: c8:60:00:19:9e:19

IP: 24.6.169.43

IP: 107.21.109.41

IP: 199.59.150.9

IP: 24.6.175.56

IP: 216.168.252.157