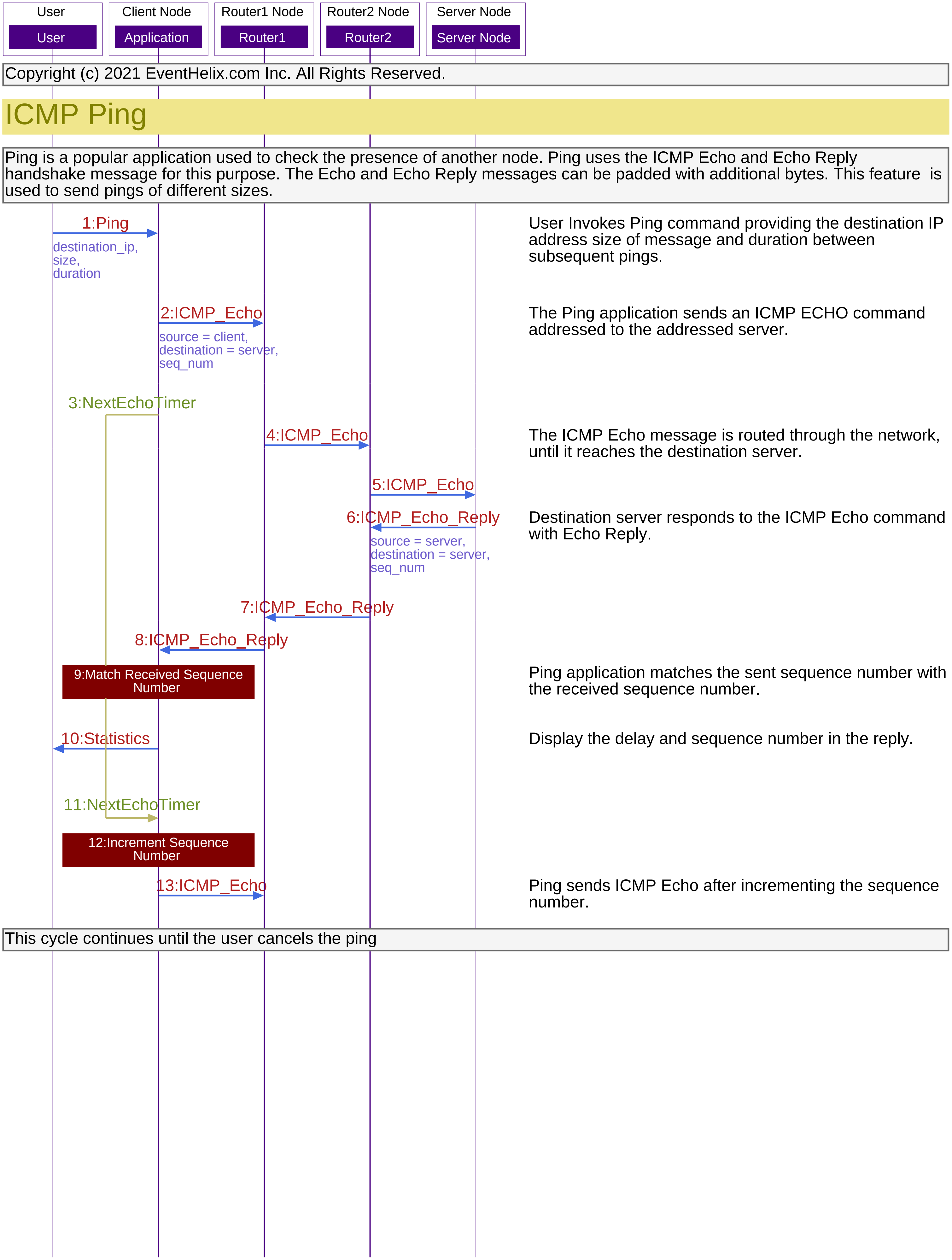
ICMP Ping

Ping is a popular application used to check the presence of another node. Ping uses the ICMP Echo and Echo Reply handshake message for this purpose. The Echo and Echo Reply messages can be padded with additional bytes. This feature is used to send pings of different sizes.



User Invokes Ping command providing the destination IP address size of message and duration between subsequent pings.

The Ping application sends an ICMP ECHO command addressed to the addressed server.

The ICMP Echo message is routed through the network, until it reaches the destination server.

Destination server responds to the ICMP Echo command with Echo Reply.

Ping application matches the sent sequence number with the received sequence number.

Display the delay and sequence number in the reply.

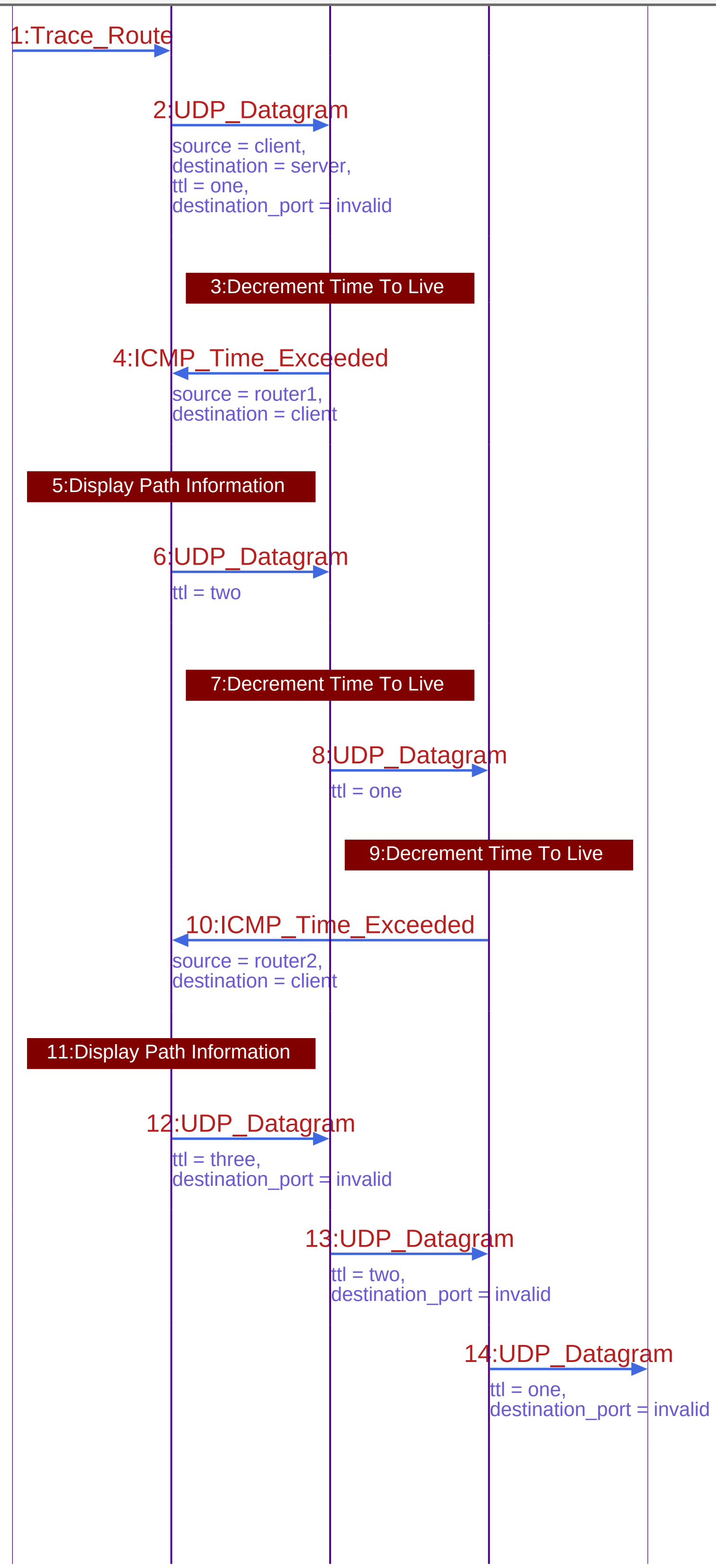
Ping sends ICMP Echo after incrementing the sequence number.

This cycle continues until the user cancels the ping

User	Client Node	Router1 Node	Router2 Node	Server Node
User	Application	Router1	Router2	Server Node

ICMP Trace Route

Trace Route utility relies on the ICMP Time Exceeded message to trace the route from the source to the destination. A UDP message with low time to live (TTL) value is used to trace the route from the source to destination. Client starts with a TTL value of 1, this results in the first router dropping the packet and responding with ICMP Time Exceeded. This identifies the router that rejected the message. Client then increases the TTL value incrementally until the complete path has been identified.



1:Trace_Route

User issues the Trace Route command

2:UDP_Datagram
source = client,
destination = server,
ttl = one,
destination_port = invalid

Trace Route then prepares a UDP datagram destined for the requested node. The time to live field is set to 1. This will ensure that the first node to receive this datagram will reject it. An invalid destination port number is used in detecting reached destination (more about this later).

3:Decrement Time To Live

Router receives the UDP packet and decrements the time to live field from 1 to 0

4:ICMP_Time_Exceeded
source = router1,
destination = client

Since TTL has reached a value of 0, Router1 drops the datagram and responds back to the sender of the message with ICMP Time Exceeded message.

5:Display Path Information

Display the information about Router1.

6:UDP_Datagram
ttl = two

Trace Route then sends the UDP message again. Now time to live field is set to 2. This will ensure that the second node to receive this datagram will reject it.

7:Decrement Time To Live

Router receives the UDP packet and decrements the time to live field from 2 to 1.

8:UDP_Datagram
ttl = one

The UDP datagram is forwarded to the next node in the path.

9:Decrement Time To Live

Router receives the UDP packet and decrements the time to live field from 1 to 0.

10:ICMP_Time_Exceeded
source = router2,
destination = client

Since TTL has reached a value of 0, Router2 drops the datagram and responds back to the sender of the message with ICMP Time Exceeded message.

11:Display Path Information

Display the information about Router2.

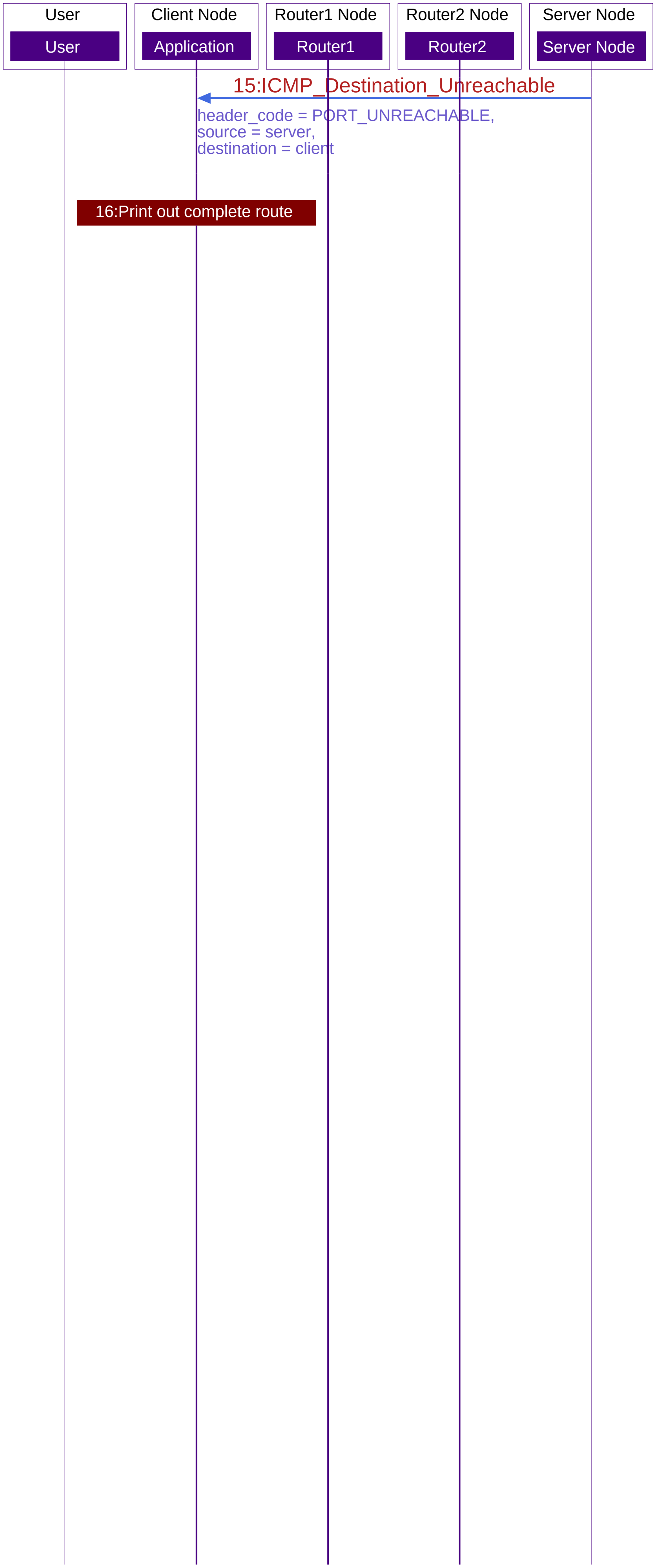
12:UDP_Datagram
ttl = three,
destination_port = invalid

Now a new UPD Datagram is sent with a TTL value of 3.

13:UDP_Datagram
ttl = two,
destination_port = invalid

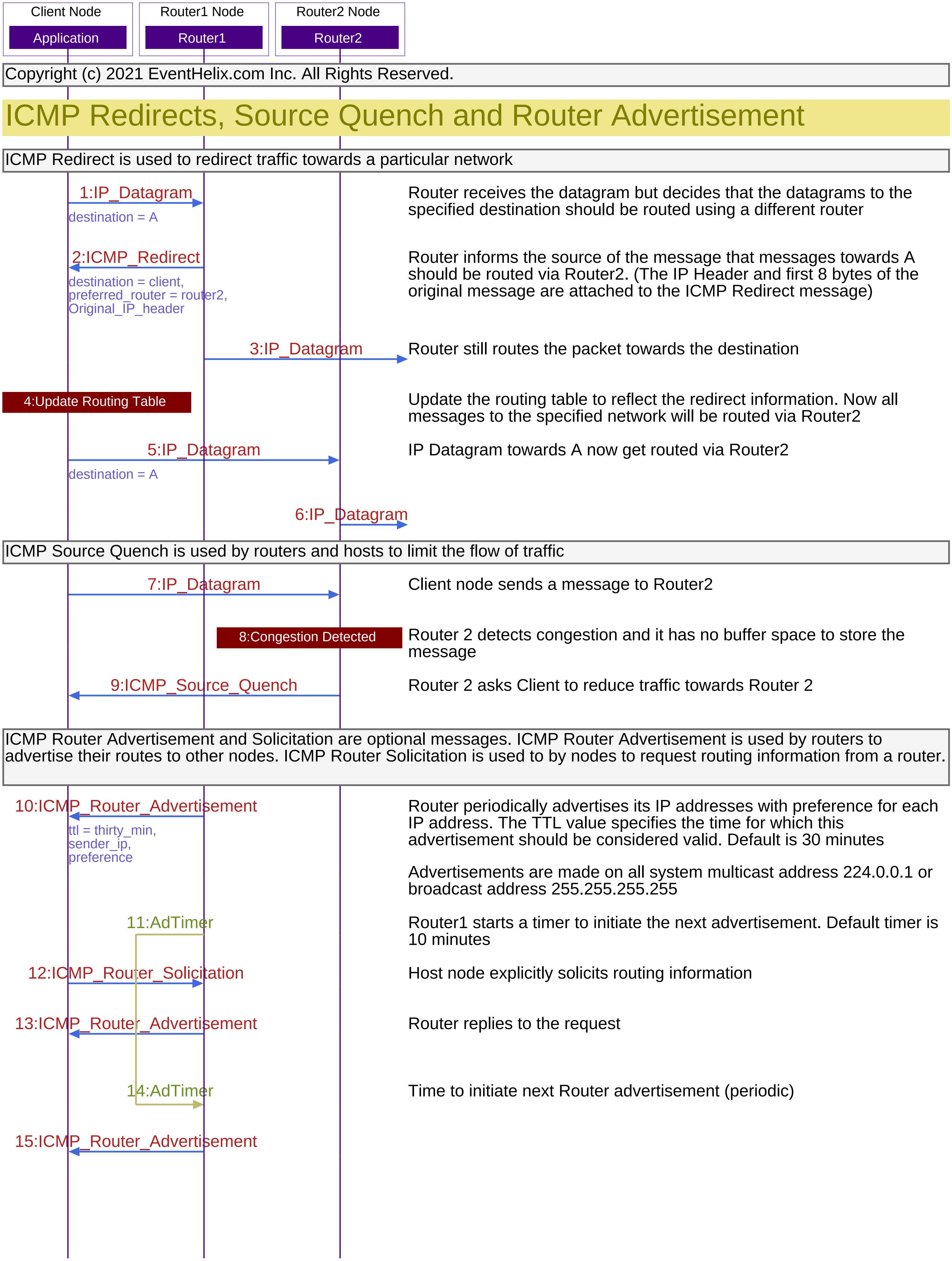
14:UDP_Datagram
ttl = one,
destination_port = invalid

The message has been delivered to the destination node. IP layer passes the message to the UDP layer.



UDP does not find the destination port. (Trace Route had used an invalid destination port to force this condition). ICMP then sends Destination Unreachable message to the source of the message.

Receipt of "Destination Unreachable" signals completion of route tracing from the source to the destination.



Client Node: Application | Router1 Node: Router1 | Router2 Node: Router2

ICMP Redirects, Source Quench and Router Advertisement

ICMP Redirect is used to redirect traffic towards a particular network

1:IP_Datagram
destination = A

Router receives the datagram but decides that the datagrams to the specified destination should be routed using a different router

2:ICMP_Redirect
destination = client,
preferred_router = router2,
Original_IP_header

Router informs the source of the message that messages towards A should be routed via Router2. (The IP Header and first 8 bytes of the original message are attached to the ICMP Redirect message)

3:IP_Datagram

Router still routes the packet towards the destination

4:Update Routing Table

Update the routing table to reflect the redirect information. Now all messages to the specified network will be routed via Router2

5:IP_Datagram
destination = A

IP Datagram towards A now get routed via Router2

6:IP_Datagram

ICMP Source Quench is used by routers and hosts to limit the flow of traffic

7:IP_Datagram

Client node sends a message to Router2

8:Congestion Detected

Router 2 detects congestion and it has no buffer space to store the message

9:ICMP_Source_Quench

Router 2 asks Client to reduce traffic towards Router 2

ICMP Router Advertisement and Solicitation are optional messages. ICMP Router Advertisement is used by routers to advertise their routes to other nodes. ICMP Router Solicitation is used to by nodes to request routing information from a router.

10:ICMP_Router_Advertisement
ttl = thirty_min,
sender_ip,
preference

Router periodically advertises its IP addresses with preference for each IP address. The TTL value specifies the time for which this advertisement should be considered valid. Default is 30 minutes

Advertisements are made on all system multicast address 224.0.0.1 or broadcast address 255.255.255.255

11:AdTimer

Router1 starts a timer to initiate the next advertisement. Default timer is 10 minutes

12:ICMP_Router_Solicitation

Host node explicitly solicits routing information

13:ICMP_Router_Advertisement

Router replies to the request

14:AdTimer

Time to initiate next Router advertisement (periodic)

15:ICMP_Router_Advertisement