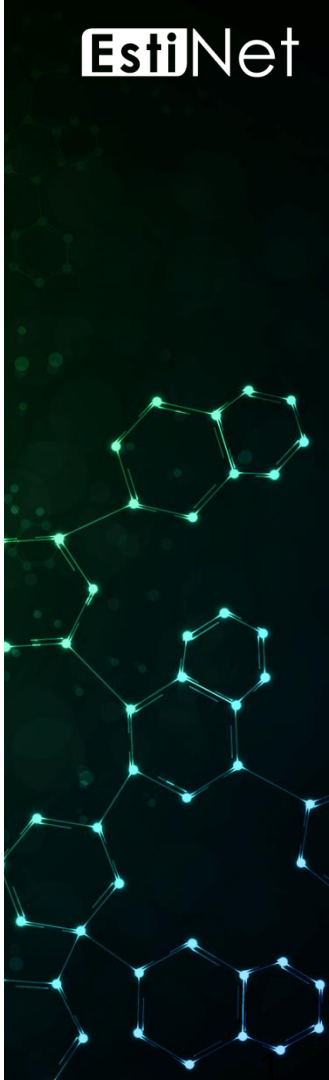
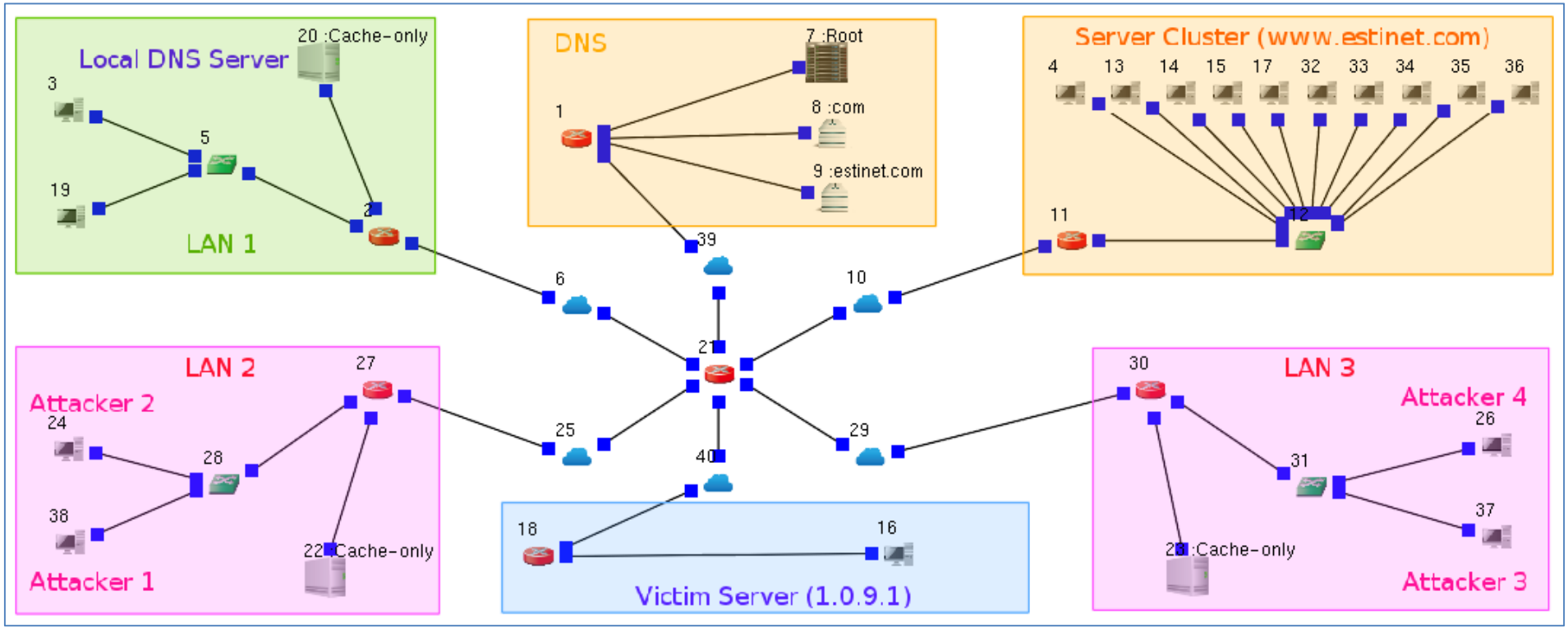
Using DNS Service for Amplification Attack



Outline

- Use DNS service to achieve load balancing for a server cluster
- Carry out an amplification attack by taking advantage of DNS service
- Enforce firewall rules to block the attack
- Summary

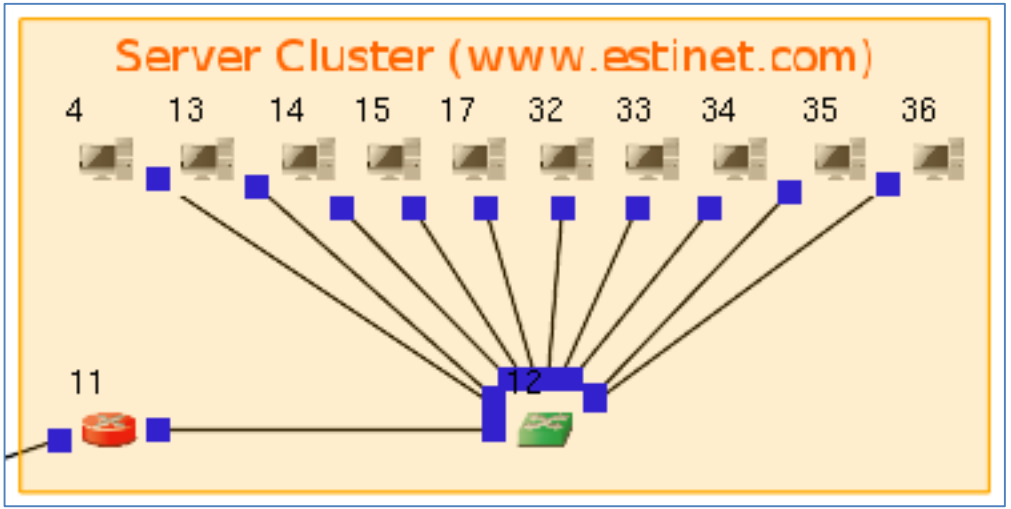
<Simulation Case>
amplification_attack_using_dns_service.xtpl



Use DNS service to achieve load balancing for a server cluster

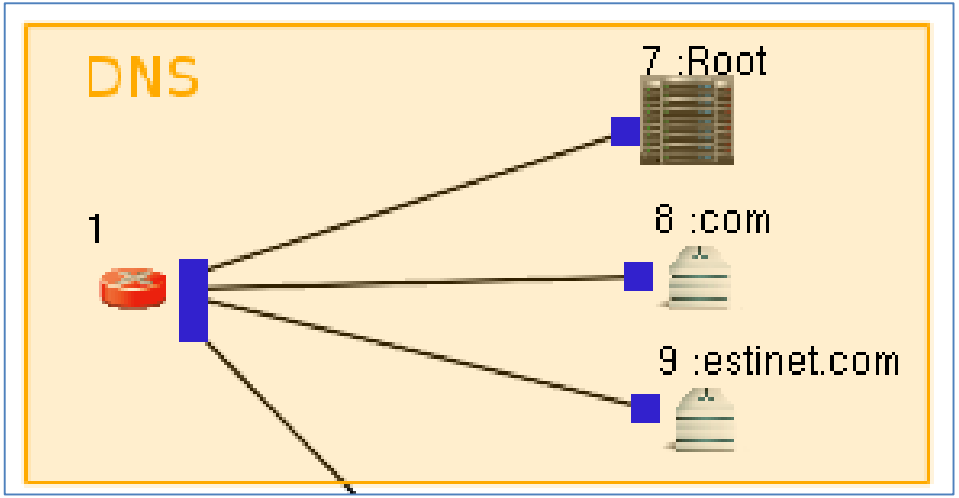
Server Cluster

- The graph on the right-hand side shows a server cluster. Ten servers join together to provide the same services. In this way, the service requests from Internet users are distributed among servers to achieve load balancing.
- The ten servers' IP addresses are different. However, only one single domain name (www.estinet.com) is provided for Internet users to request services.
- In other words, when an Internet user uses the domain name (www.estinet.com) to request a service, it could be anyone of the ten servers which is responsible for serving the user.



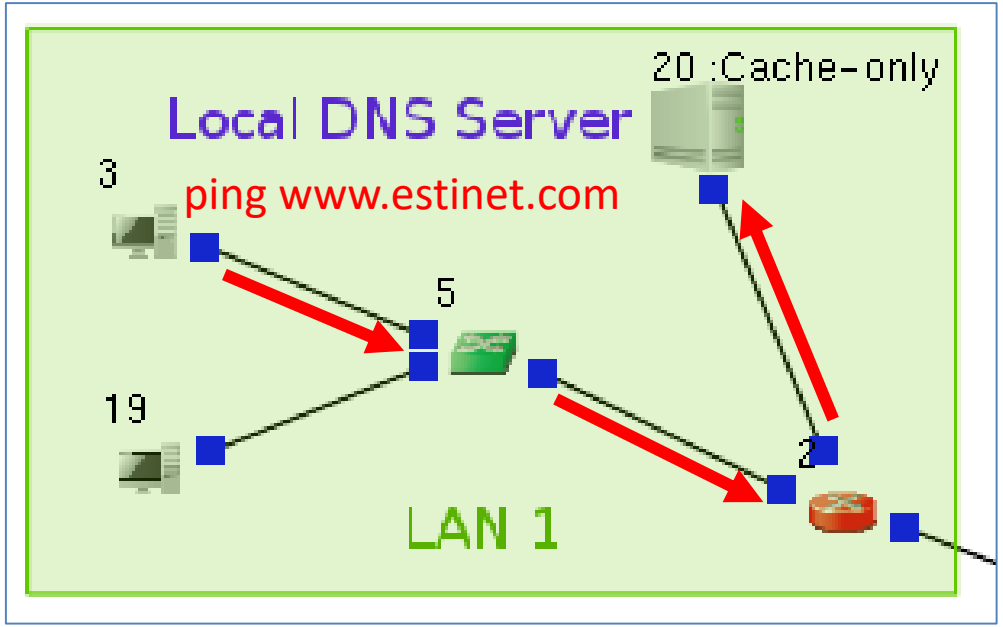
Domain Name System (DNS)

- The graph on the right-hand side shows a domain name system (DNS) that is composed of three servers. When an Internet user queries a domain name's corresponding IP address(es), the user may query the root server first. If the root server has no answer, it asks the down-level servers in turn for the answer. A DNS has a hierarchy architecture.
- The domain name of the aforementioned server cluster is registered on the server 9. It is responsible for the domain "estinet.com".
- If an Internet user wants to query the corresponding IP address(es) of domain name www.estinet.com, the answer is originally stored on the server 9.



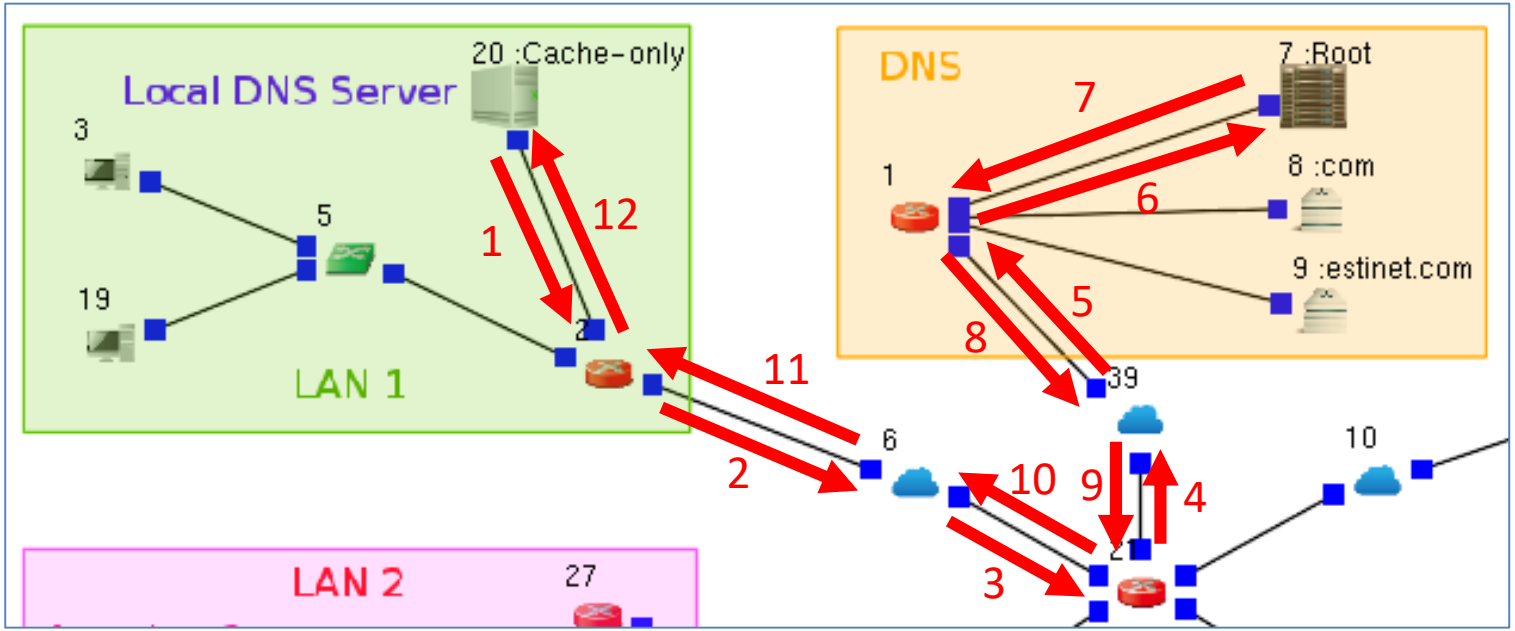
Host 3 within LAN 1 requests the echo service from the server cluster.

- Host 3 executes the command “ping www.estinet.com” to request the echo service from the server cluster whose domain name is www.estinet.com.
- Because network routers forward packets according to IP address instead of domain name, Host 3 queries the local DNS server 20 for the corresponding IP address of www.estinet.com.



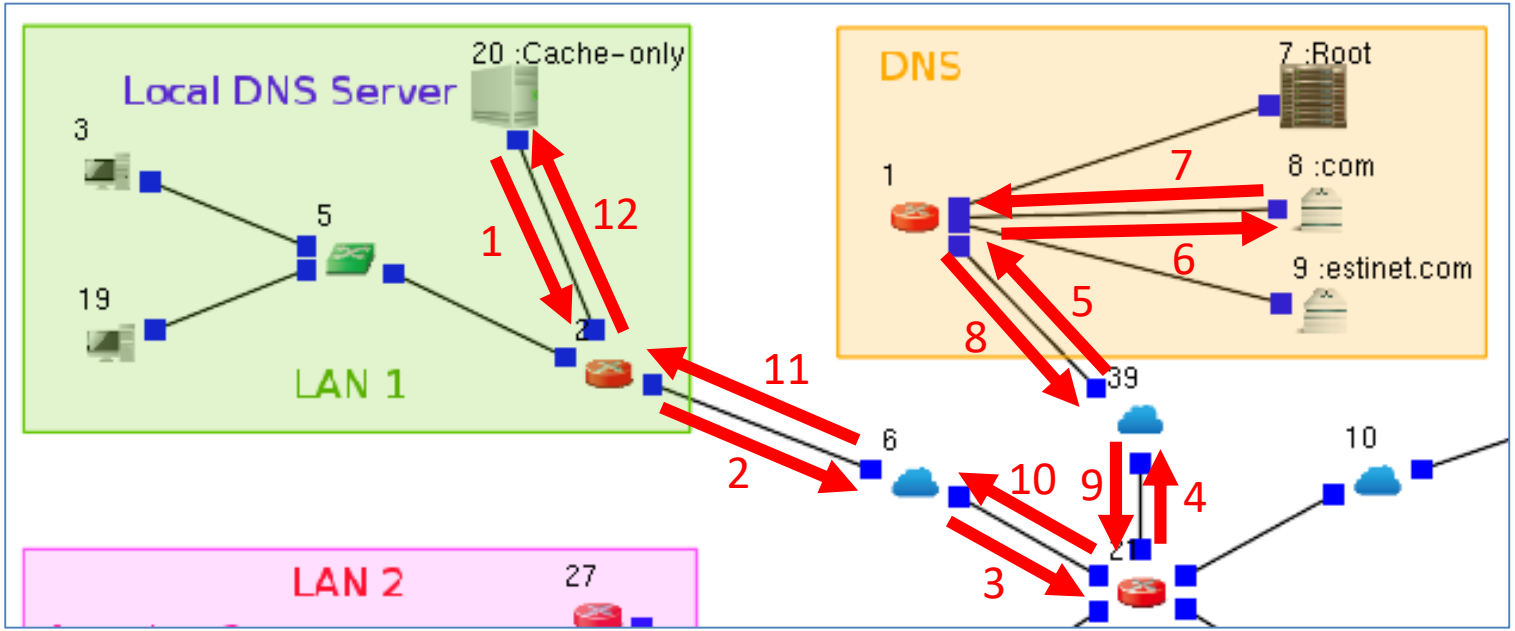
The local DNS server 20 queries the DNS root server 7 for the answer.

- The local DNS server 20 doesn't know the answer of the corresponding IP address of www.estinet.com. It turns to ask the DNS root server 7 for the answer. Because the ten servers of server cluster register their domain name on the DNS server 9, the DNS root server 7 doesn't know the corresponding IP address of www.estinet.com. The DNS root server 7 replies to the DNS server 20 and tells it to query the DNS server 8 which is in charge of the domain name "com".



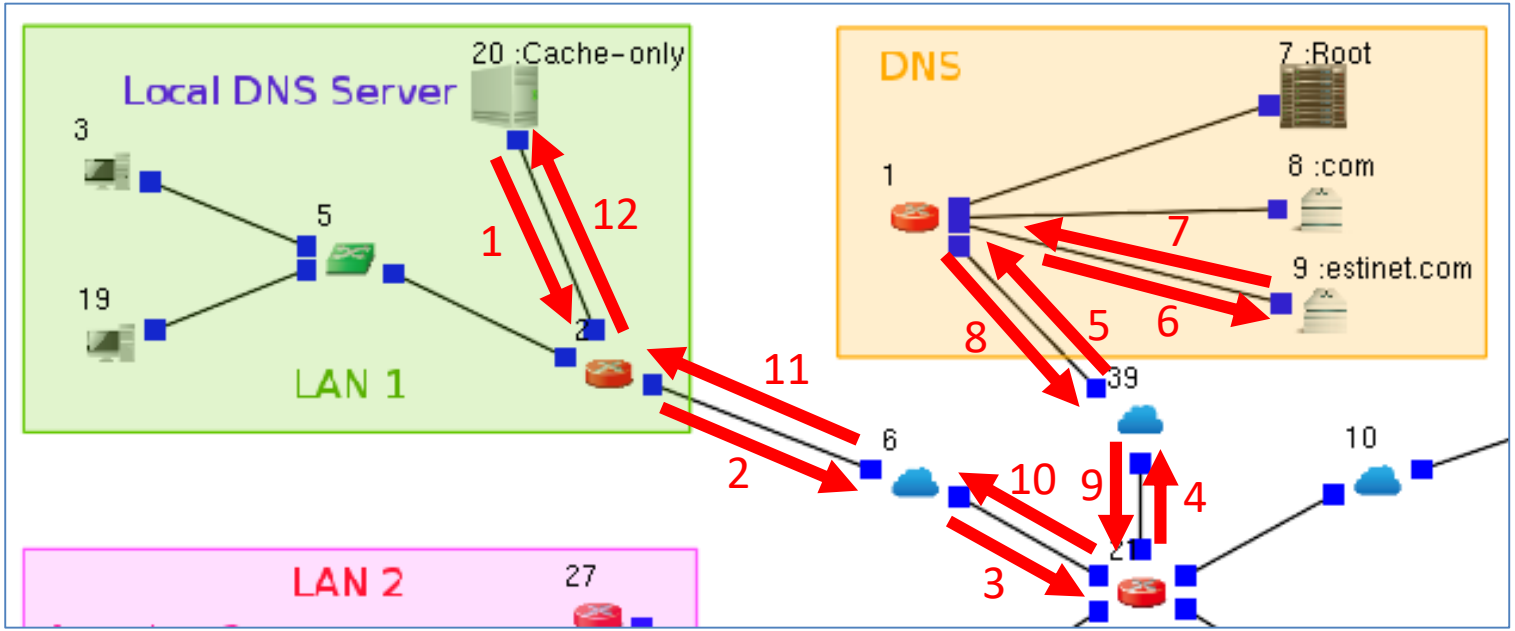
The local DNS server 20 queries the DNS server 8 for the answer.

- Because the DNS server 8 also doesn't know the answer, it replies to the DNS server 20 and tells it to query the DNS server 9 which is in charge of the domain name "estinet.com".



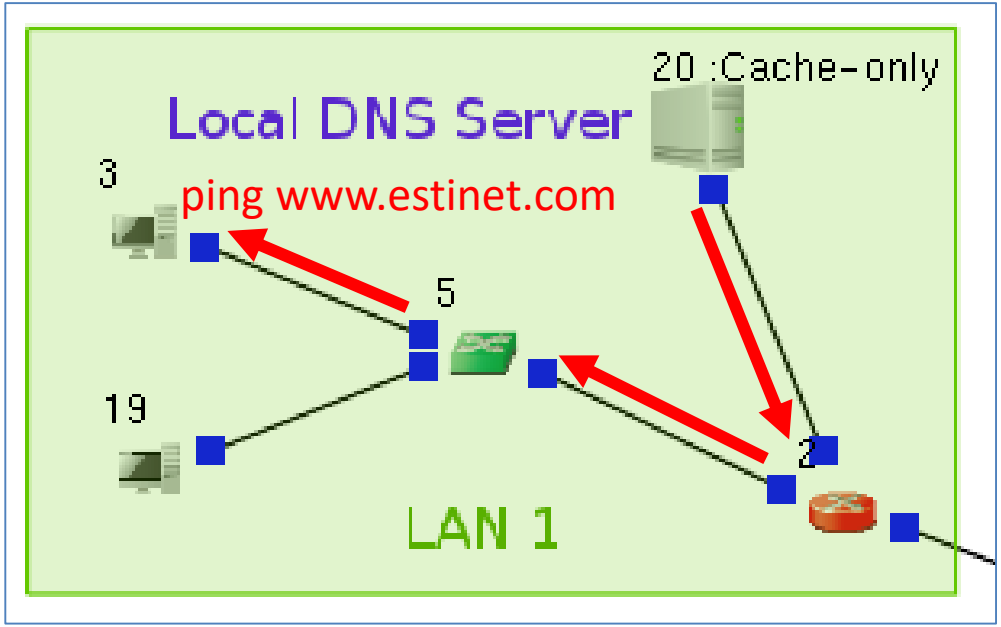
The local DNS server 20 queries the DNS server 9 for the answer.

- Eventually, the local DNS server 20 gets the corresponding IP address of www.estinet.com from the DNS server 9.



The local DNS server 20 sends the answer back to Host 3.

- The server 20 remembers/caches the answer for a period of time. If other hosts ask the same question later, the server replies the answer directly.



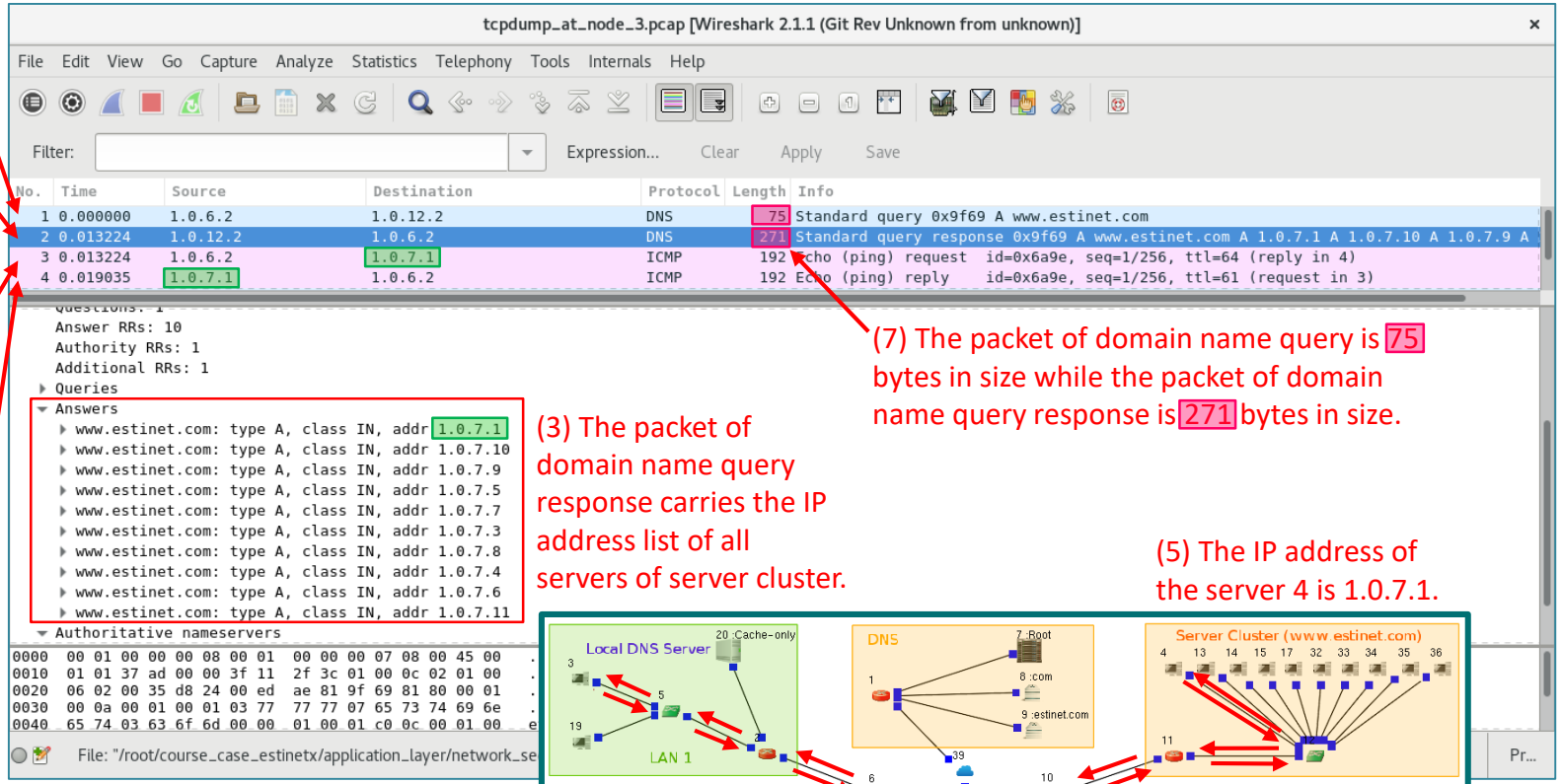
Host 3 gets the IP address list of all servers of server cluster. (use Wireshark utility to open the tcpdump file that records the incoming/outgoing packets on Host 3)

(1) Host 3 sends the packet of domain name query.

(2) Host 3 receives the packet of domain name query response.

(4) Host 3 sends the packet of echo request to the destination with IP 1.0.7.1.

(6) Host 3 receives the packet of echo reply from the source with IP 1.0.7.1.



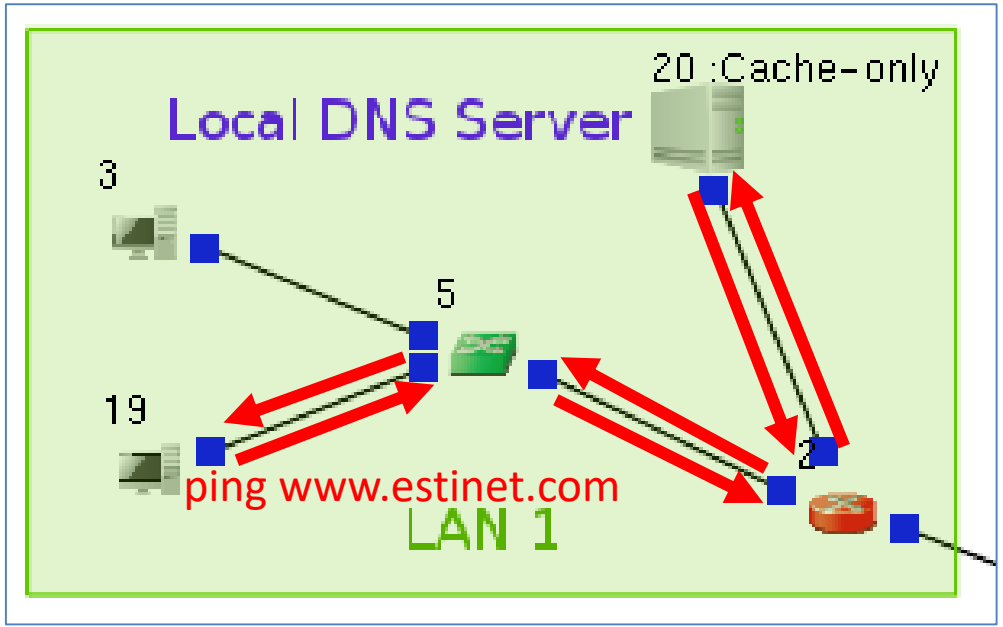
(7) The packet of domain name query is 75 bytes in size while the packet of domain name query response is 271 bytes in size.

(3) The packet of domain name query response carries the IP address list of all servers of server cluster.

(5) The IP address of the server 4 is 1.0.7.1.

Host 19 within LAN 1 requests the echo service from the server cluster.

- Host 19 executes the command “ping www.estinet.com” to query the echo service from the server cluster whose domain name is www.estinet.com.
- Host 19 queries the local DNS server 20 for the corresponding IP address of www.estinet.com.
- Because the server 20 has remembered the answer while Host 3 issued the same query before, it directly sends back the answer to Host 19.



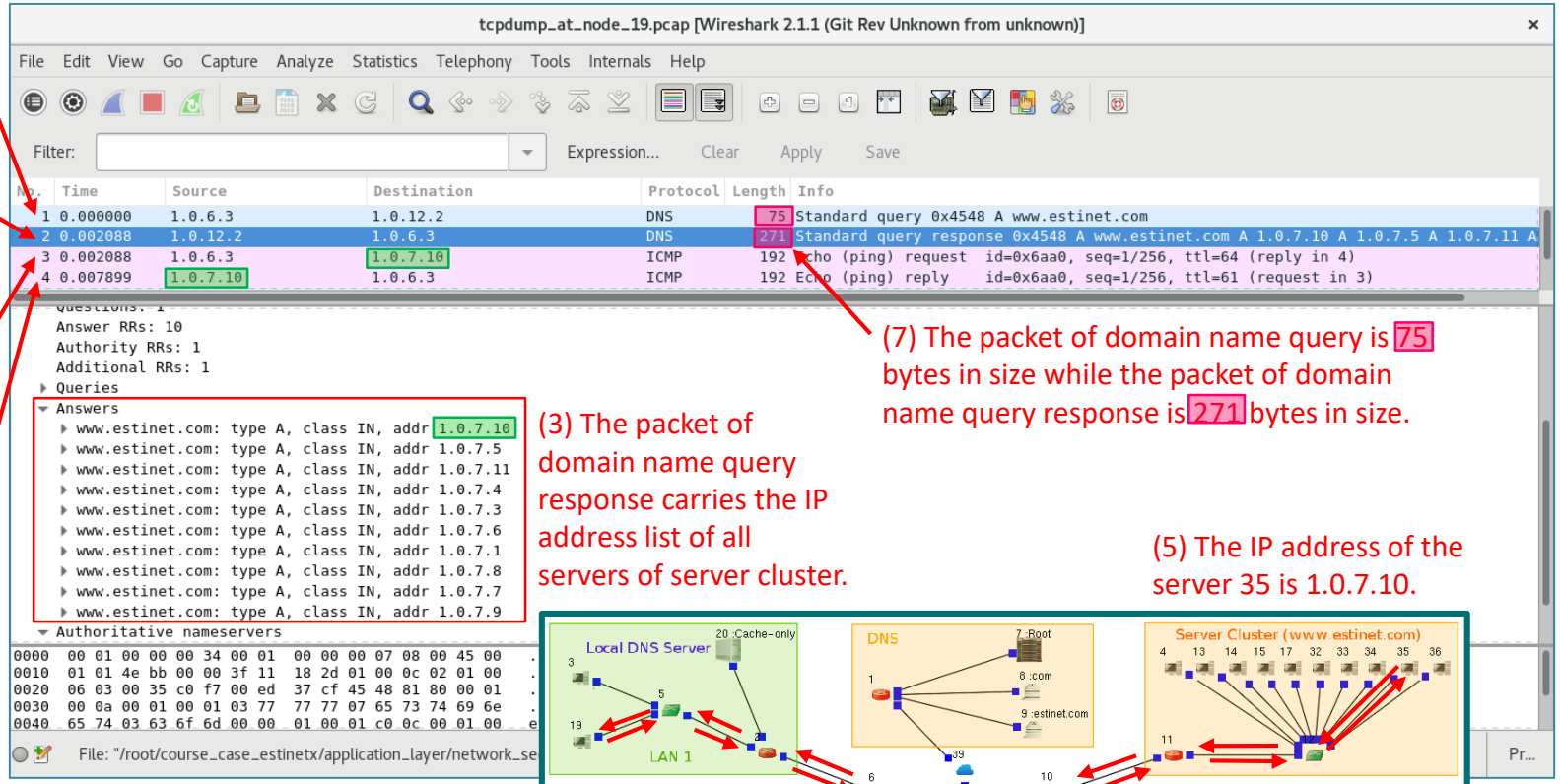
Host 19 gets the IP address list of all servers of server cluster. (use Wireshark utility to open the tcpdump file that records the incoming/outgoing packets on Host 19)

(1) Host 19 sends the packet of domain name query.

(2) Host 19 receives the packet of domain name query response.

(4) Host 19 sends the packet of echo request to the destination with IP 1.0.7.10.

(6) Host 19 receives the packet of echo reply from the source with IP 1.0.7.10.



(7) The packet of domain name query is 75 bytes in size while the packet of domain name query response is 271 bytes in size.

(3) The packet of domain name query response carries the IP address list of all servers of server cluster.

(5) The IP address of the server 35 is 1.0.7.10.

Carry out an amplification attack by taking advantage of DNS service

Why can an attacker take advantage of DNS service to attack a server on Internet?

- The domain name of a server cluster represents a group of servers that provide services simultaneously. When an Internet user issues a domain name query, the user gets a response with an IP address list. In other words, the user sends a small query packet and gets a relatively larger response packet.
- If an attacker wants to attack one working server V, the attacker can fake the source IP address with the server V's IP address while it sends out the packets of domain name query. In this way, the amplified packets of domain name query response are sent to the server A (a reflection attack) instead of the attacker. Too many of the amplified packets will affect the normal operation of the server A. It could cause the situation of denial of service (DoS) on the server A.
- Sometimes, a single attacker is not able to cause the situation of DoS. Thus, an effective attack is usually carried out by multiple attackers simultaneously. It is called distributed denial of service (DDoS) attack.

Host 38 starts the attack first. It executes a program to send domain name queries in the name of other Host.

amplification_attack_using_dns_service.py	1.0.9.1	1.0.13.1	www.estinet.com	100	0.001
(1)	(2)	(3)	(4)	(5)	(6)

Command Line Statement:

(1) An attack python program

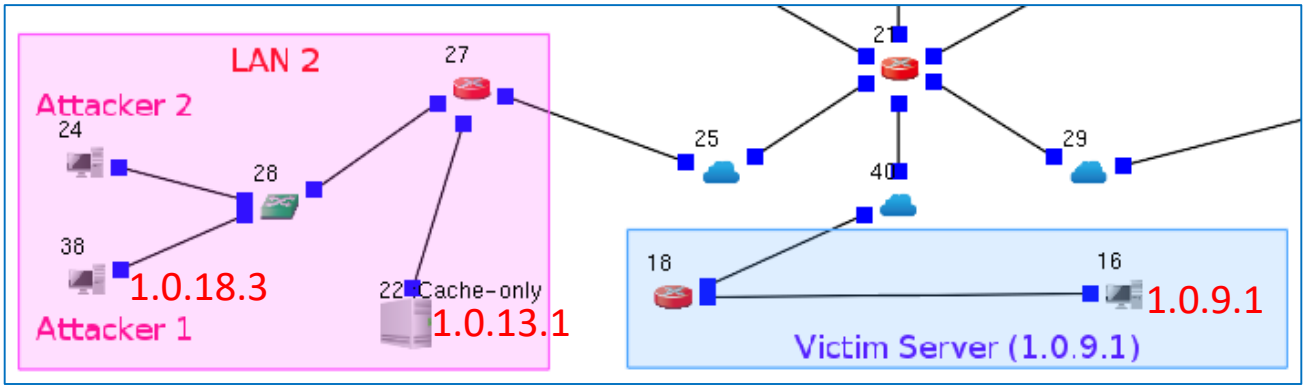
(2) The IP address of attack target (Server 16)

(3) Through which DNS server to carry out reflection attack (local DNS Server 22)

(4) The domain name to query (with amplification effect)

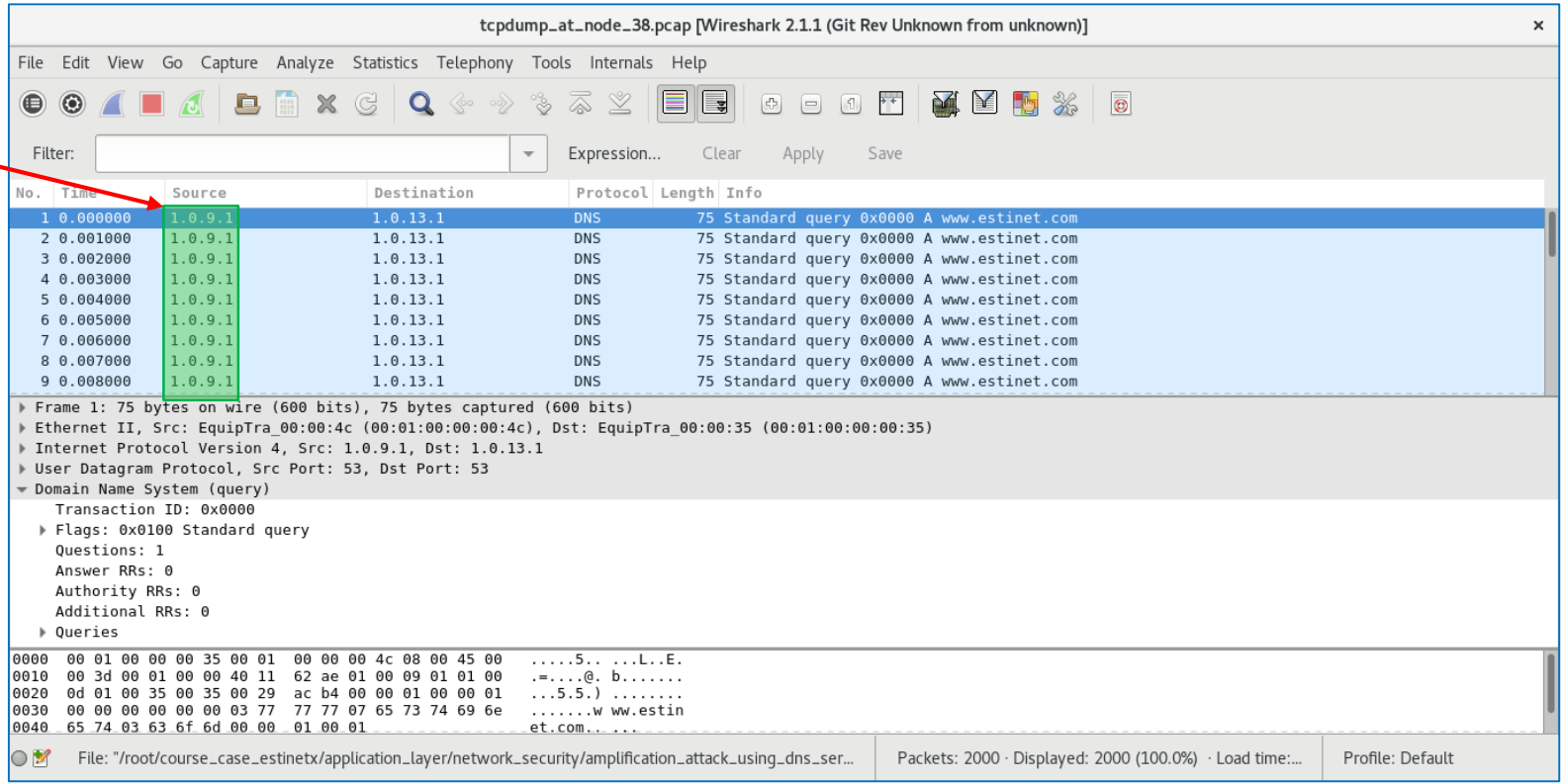
(5) The lasting time of attack

(6) The interval between two adjacent domain name queries (sec)

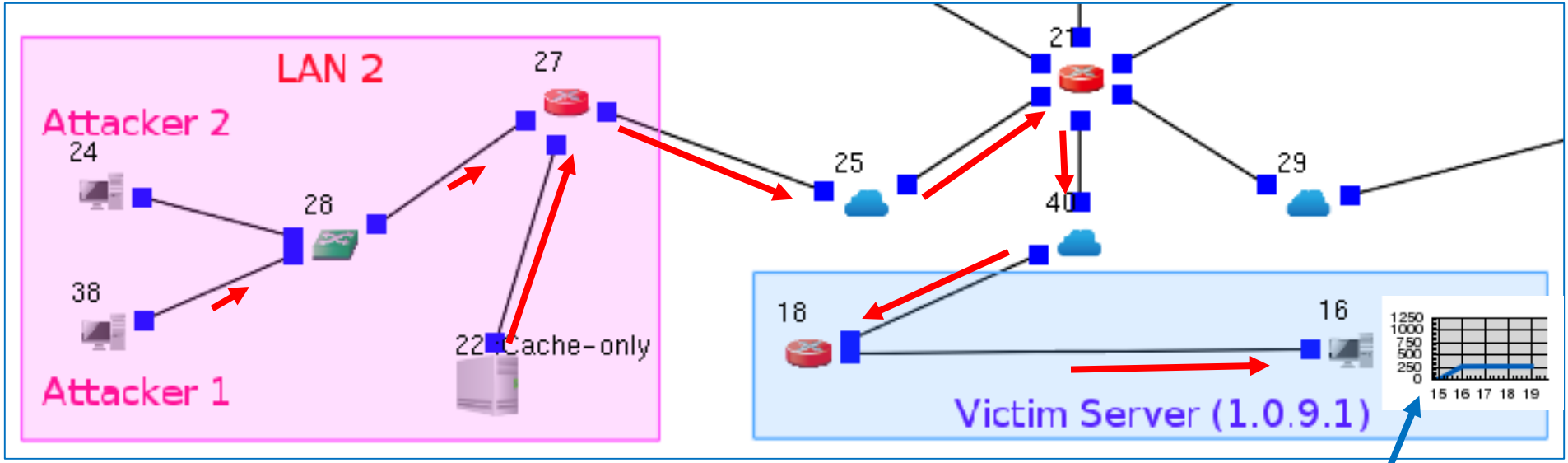


Use Wireshark utility to open the tcpdump file that records the incoming/outgoing packets on Host 38

In the recorded packets, the source IP address is the server 16's IP address (1.0.9.1), not the Host 38's IP address (1.0.18.3). Because Host 38 fakes the source IP address in the outgoing packets of domain name query.



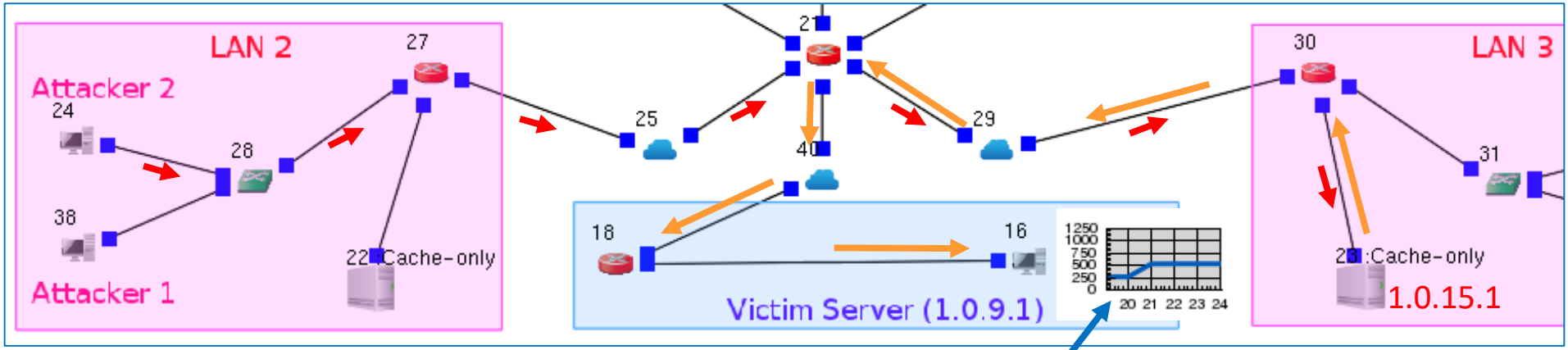
Host 38 carries out a reflection and amplification attack on Server 16 through the local DNS server Server 22.



However, the attack only consumes 1/5 the available network bandwidth of Server 16.

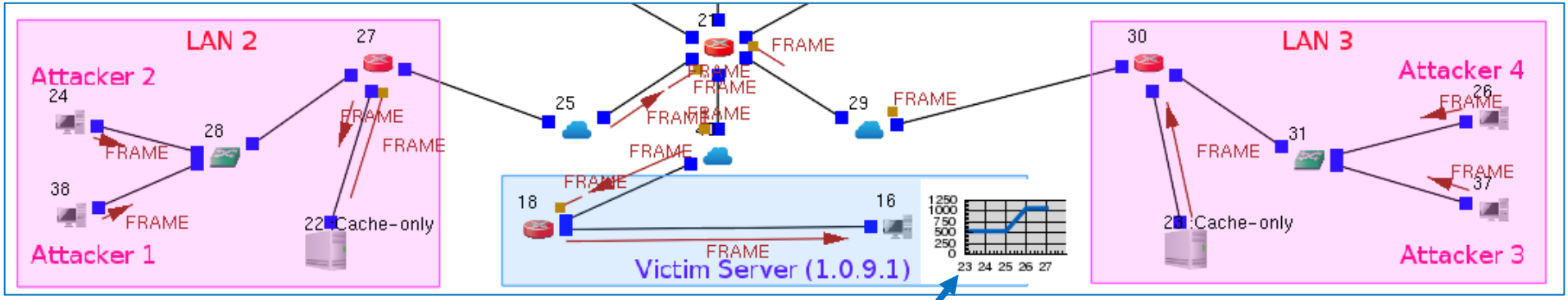
Next, Host 24 carries out a reflection and amplification attack on Server 16 through the outside DNS server Server 23.

amplification_attack_using_dns_service.py | 1.0.9.1 | 1.0.15.1 | www.estinet.com | 100 | 0.001



The union attack consumes 2/5 the available network bandwidth of Server 16.

Finally, in LAN 3, Host 37 and Host 26 join to attack Server 16. Host 37 carries out attack through the local DNS server Server 23 while Host 26 carries out attack through the outside DNS server Server 22.

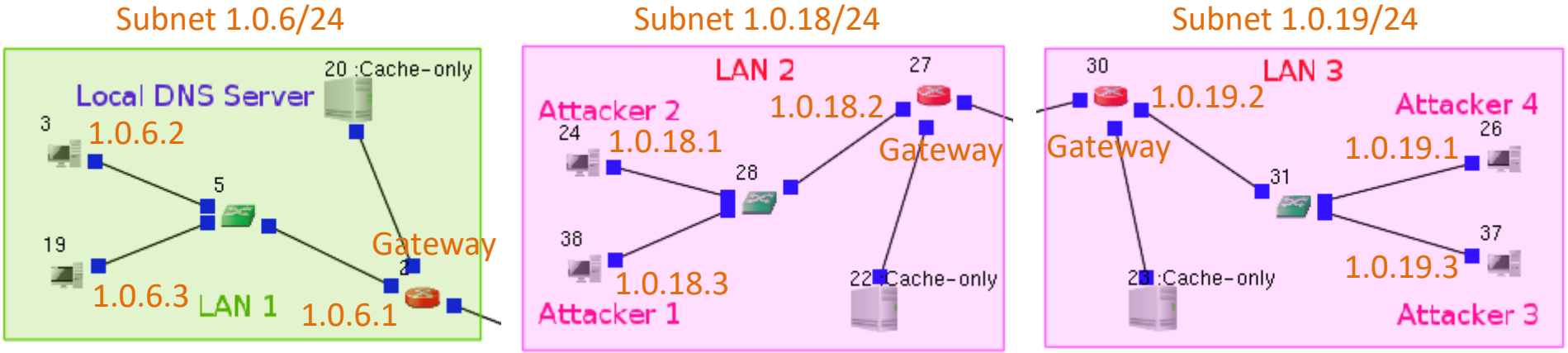


Eventually, the union attack consumes more than 4/5 the available network bandwidth of Server 16. It significantly affects the normal operation of Server 16.

Enforce firewall rules to block the attack

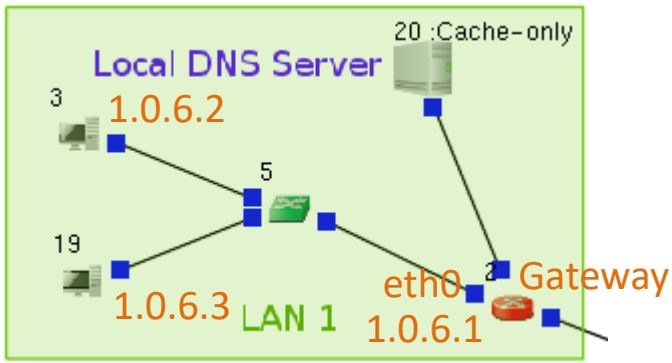
Defense Method 1: finding out the packets with fake source IP address

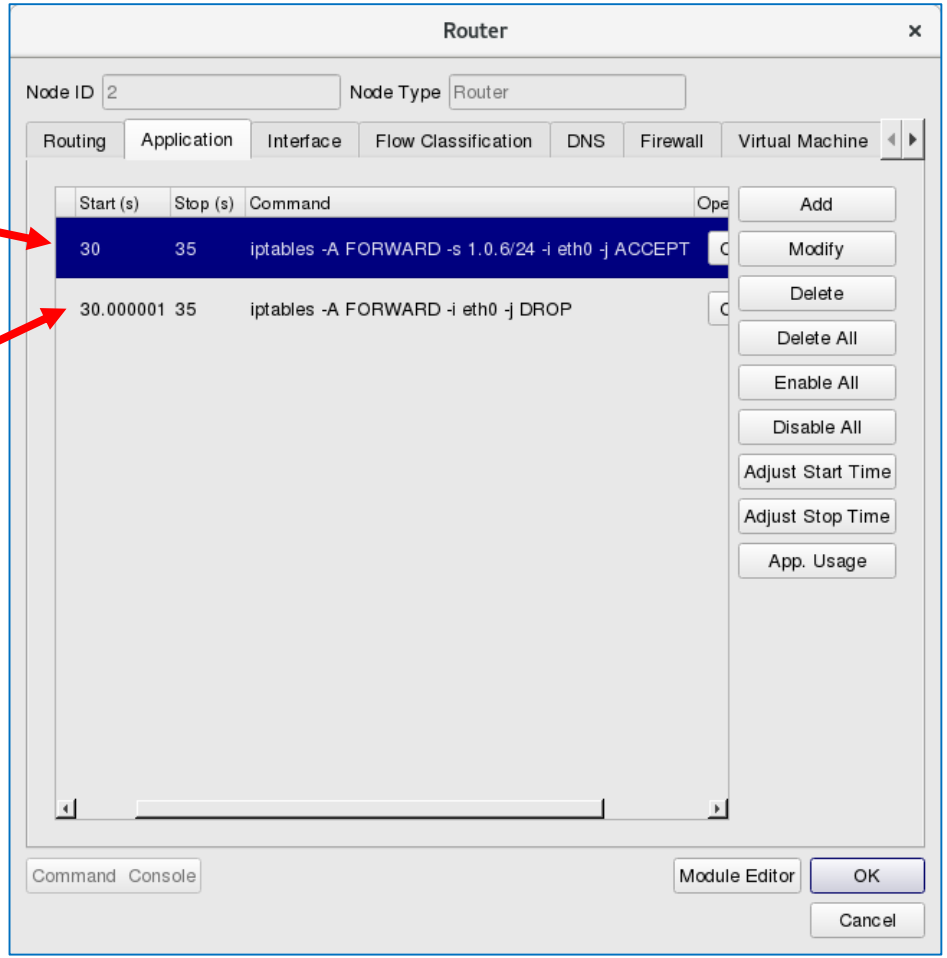
- Under the norm of Internet protocol, the workable IP addresses within a subnet are regulative. For example, within the subnet 1.0.6/24, the workable IP addresses are 1.0.6.1, 1.0.6.2, 1.0.6.3, … , and 1.0.6.254。
- Once a packet's source IP address is faked, this packet is dropped by firewall when it tries to pass through a subnet's gateway. Hence, the attack is blocked.



In LAN 1, Gateway 2 sets firewall rules to filter fake packets.

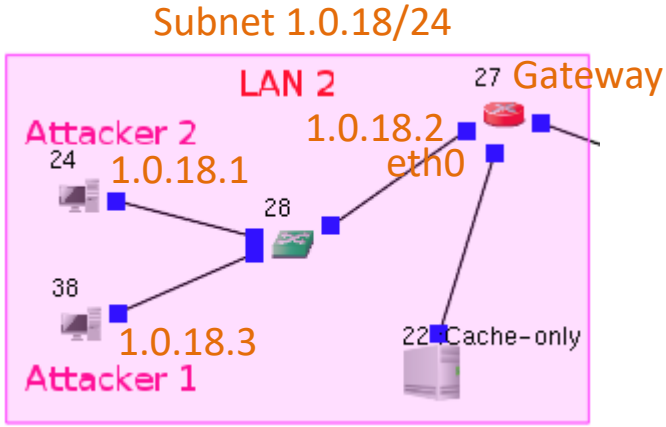
- The first rule allows a packet pass through the firewall only when its source IP address conforms to the regulation.
- The second rule filters out the packets that do not conform to the first rule.

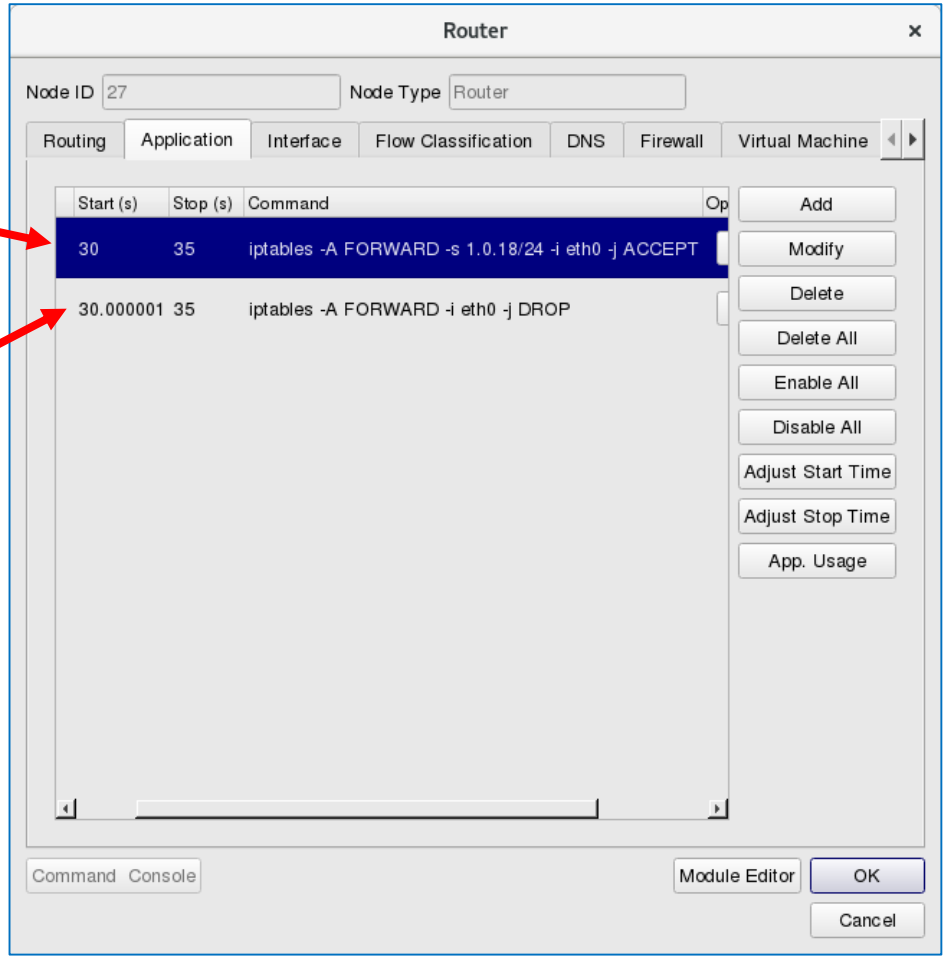




In LAN 2, Gateway 27 sets firewall rules to filter fake packets.

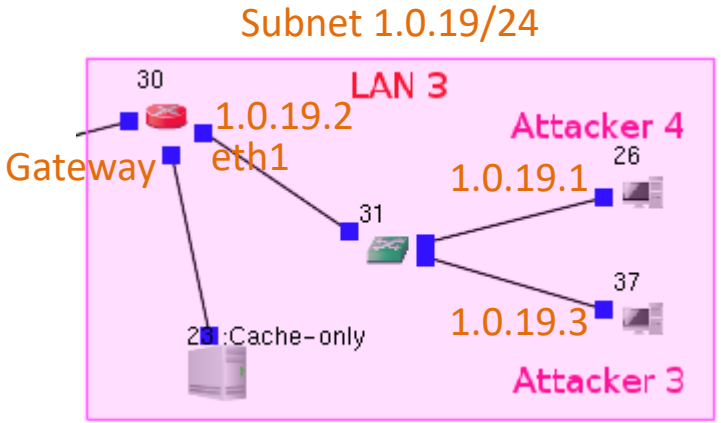
- The first rule allows a packet pass through the firewall only when its source IP address conforms to the regulation.
- The second rule filters out the packets that do not conform to the first rule.

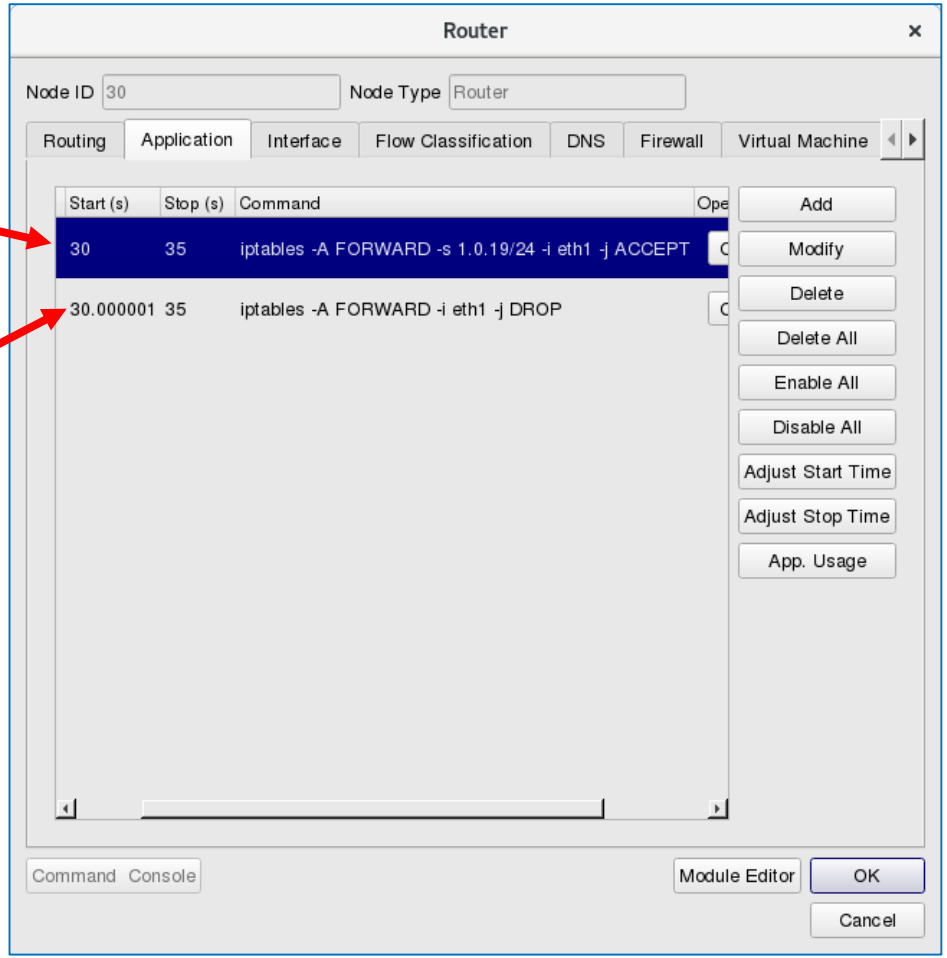




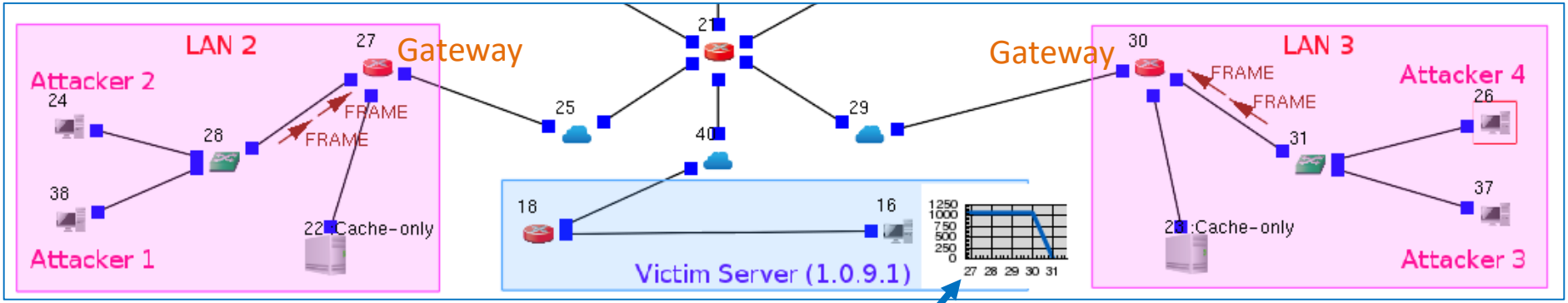
In LAN 3, Gateway 30 sets firewall rules to filter fake packets.

- The first rule allows a packet pass through the firewall only when its source IP address conforms to the regulation.
- The second rule filters out the packets that do not conform to the first rule.



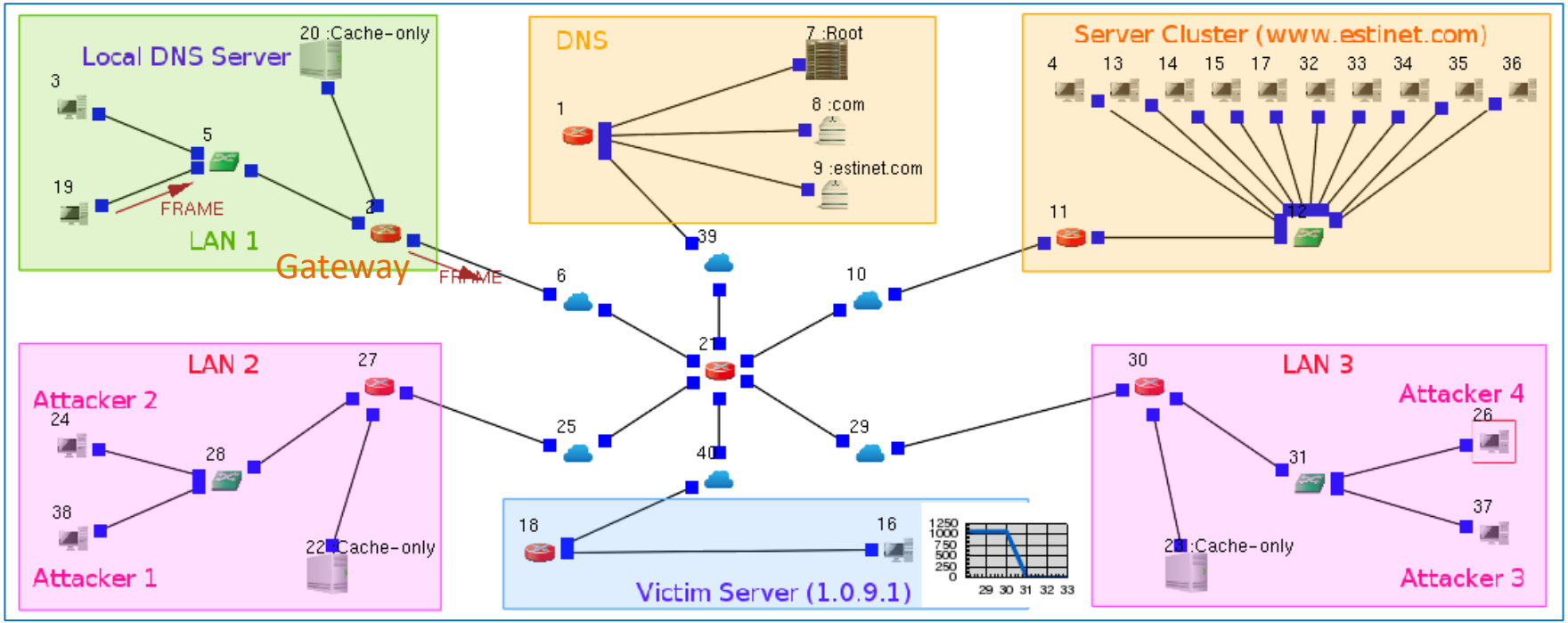


Because the fake packets are filtered out by the firewall on the gateways, no amplified domain name query response is sent to Server 16.



Server 16 is restored.

In LAN 1, normal packets can pass through the firewall on the gateway.



Summary

Review of Points

- In order to simultaneously serve many Internet users, how can a server cluster use a single domain name to achieve load balancing among a group of servers?
- Comparing to the packet of domain name query, why does the packet of domain name query response become relatively larger in size?
- How to take advantage of DNS service to carry out a reflection attack?
- How to block the packets with fake source IP address?