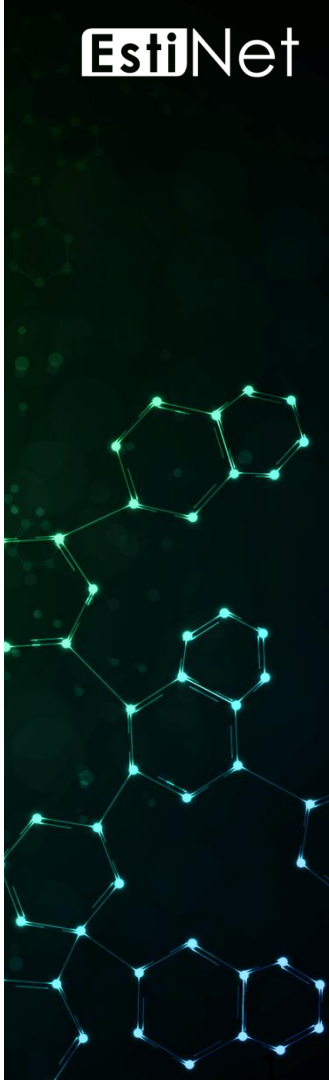
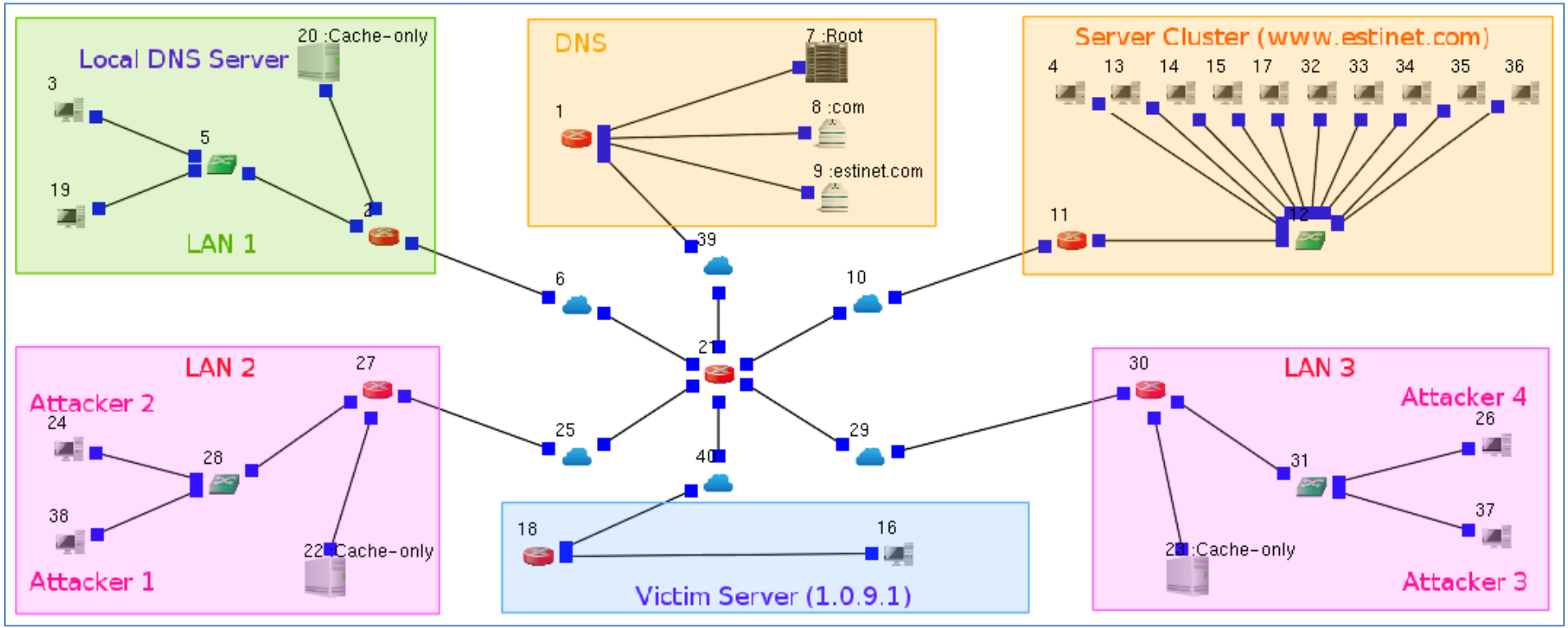
利用域名服务来进行放大式网络攻击



內容大綱

- 多服务器场域利用域名服务来达到负载均衡
- 利用域名服务来进行放大式网络攻击
- 利用防火墙来进行防御
- 总结

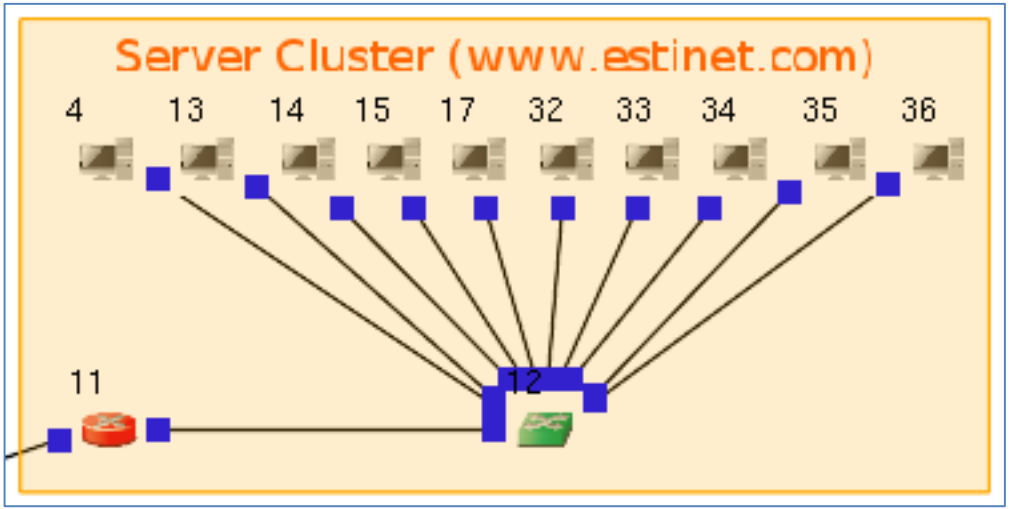
<仿真案例>
amplification_attack_using_dns_service.xtpl



多服务器场域利用域名服务来达到负载均衡

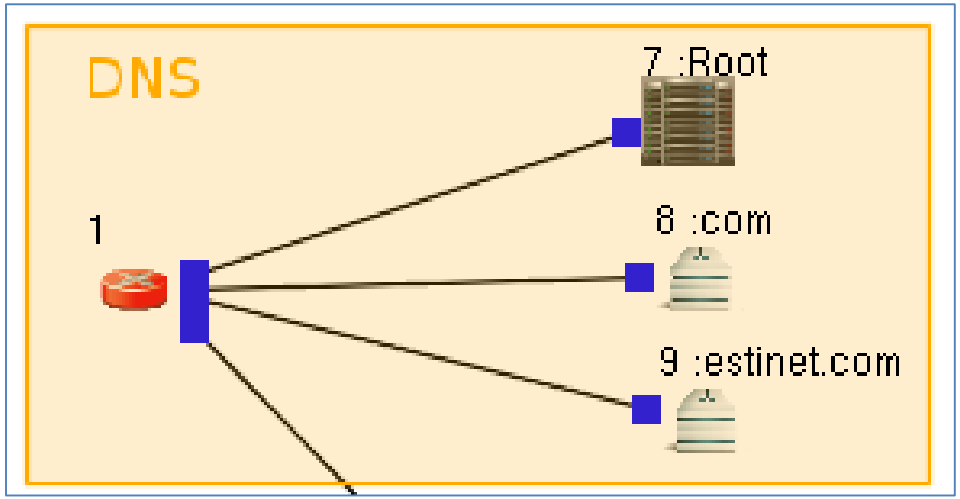
服务器群集

- 右图的服务器群集中，一共有 10 台服务器，它们一起提供相同的服务，可以达到分散负载的功用。
- 十台服务器的 IP 地址各自不同，但利用相同的域名 (www.estinet.com) 来对互联网上的用户提供服务。
- 换句话说，当互联网用户利用域名 www.estinet.com 来要求服务时，提供服务的机器可能是十台服务器中的任何一台。



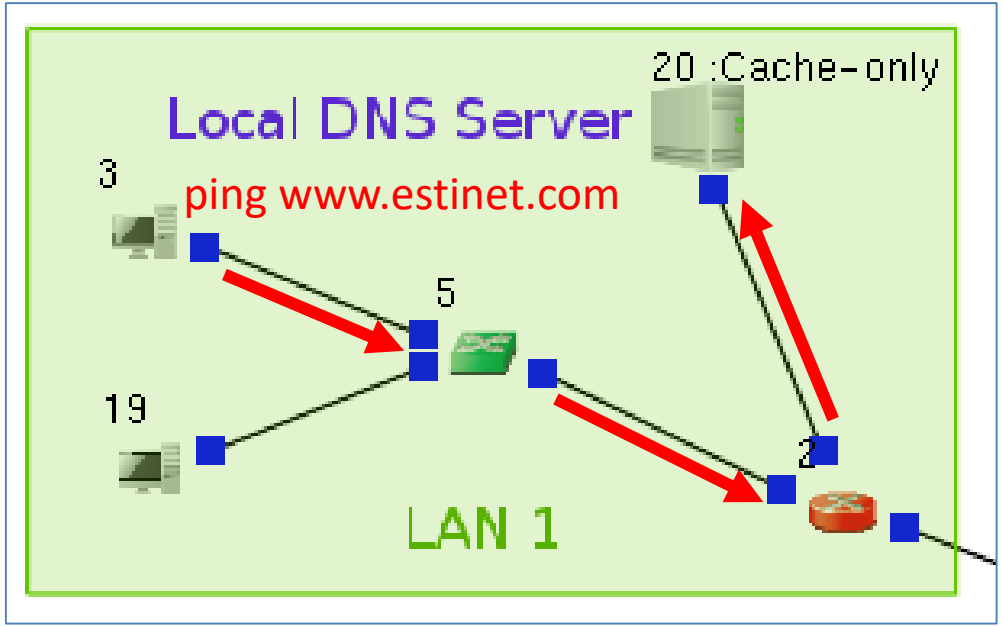
域名系统

- 右图的域名系统由三台服务器建置而成，由上而下构成分层架构。互联网用户来询问域名时，可能会由最上层的根服务器问起，若根服务器没有答案，则会依序往下层的服务器去询问。
- 先前所介绍的服务器群集所使用的域名 www.estinet.com，是注册在右图中最下方的服务器上面，它负责 estinet.com 这个域名。
- 互联网用户想要询问 www.estinet.com 所对应的 IP 地址为何时，就必须询问负责 estinet.com 域名的服务器才能得到答案。



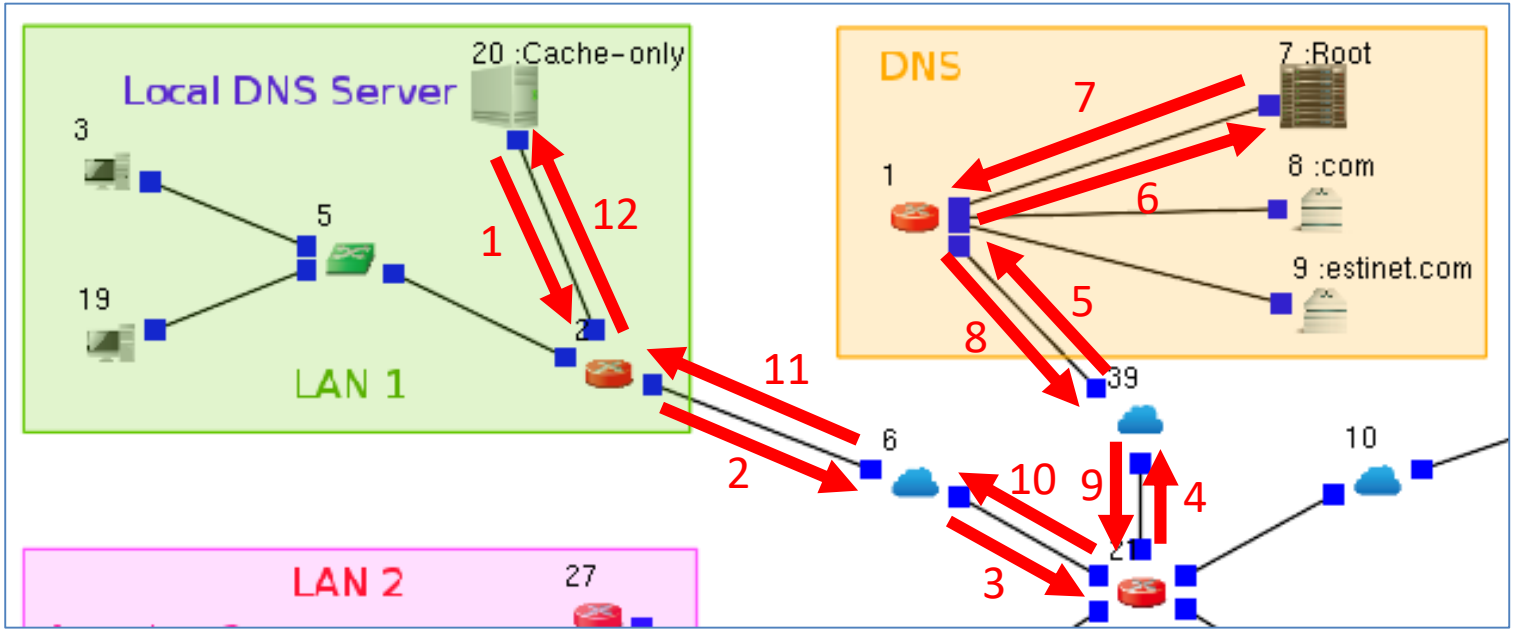
一号局域网 (LAN 1) 中的用户 3 要求服务器群集的回应服务

- 用户 3 执行 ping www.estinet.com 指令去跟服务器群集要求回应 (echo) 服务。
- 因为网络上的路由器设备是根据服务器的 IP 地址来转发信息包，不是根据服务器的域名 www.estinet.com，所以，用户 3 会先去跟局域网中的域名服务器 20（Local DNS Server）来询问 www.estinet.com 所对应的 IP 地址。



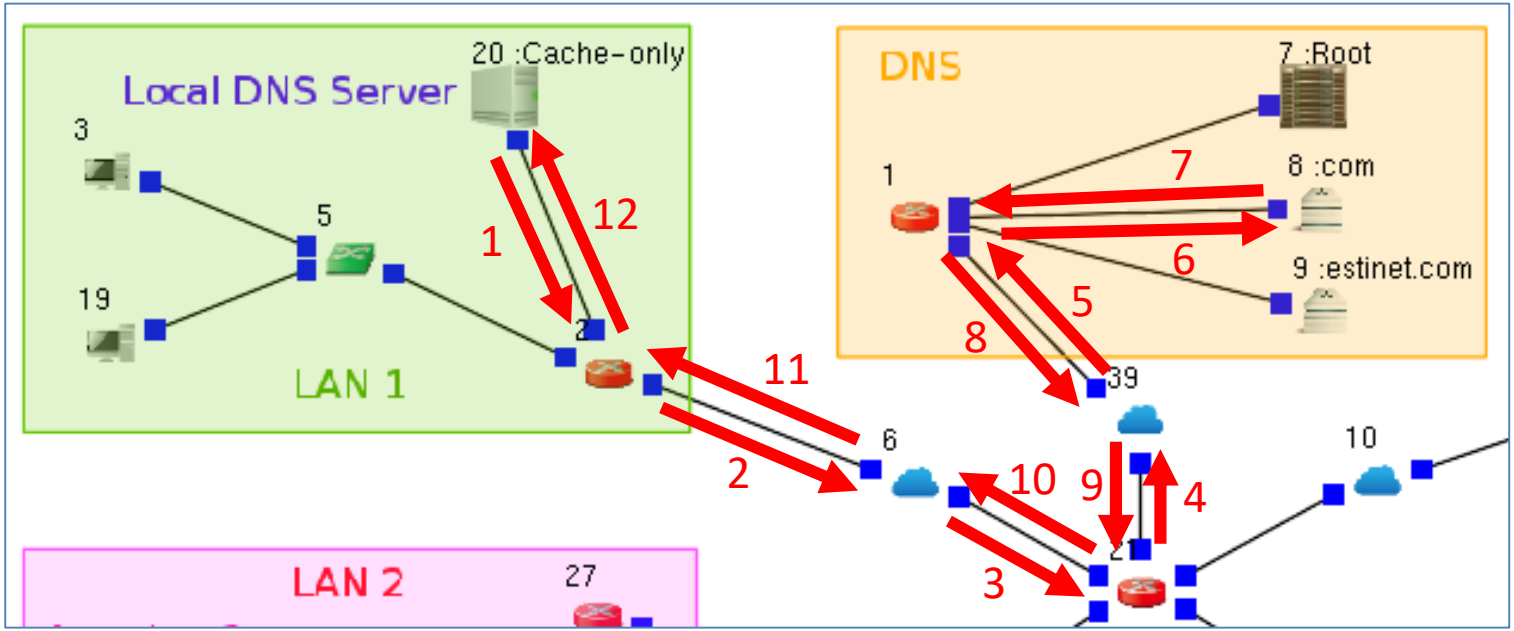
局域网中的域名服务器 20 去向域名系统中的根服务器 7 寻求答案

- 服务器 20 目前不知道 www.estinet.com 所对应的 IP 地址为何，所以向域名系统中的根服务器 7 寻求解答，但因为在服务器群集中的十台服务器都是跟 estinet.com 这台域名服务器 9 来注册 www.estinet.com 这个域名，所以根服务器 7 并不知道答案。于是，根服务器 7 回覆给服务器 20，请服务器 20 再去询问管理 ”com” 这个域名的服务器 8。



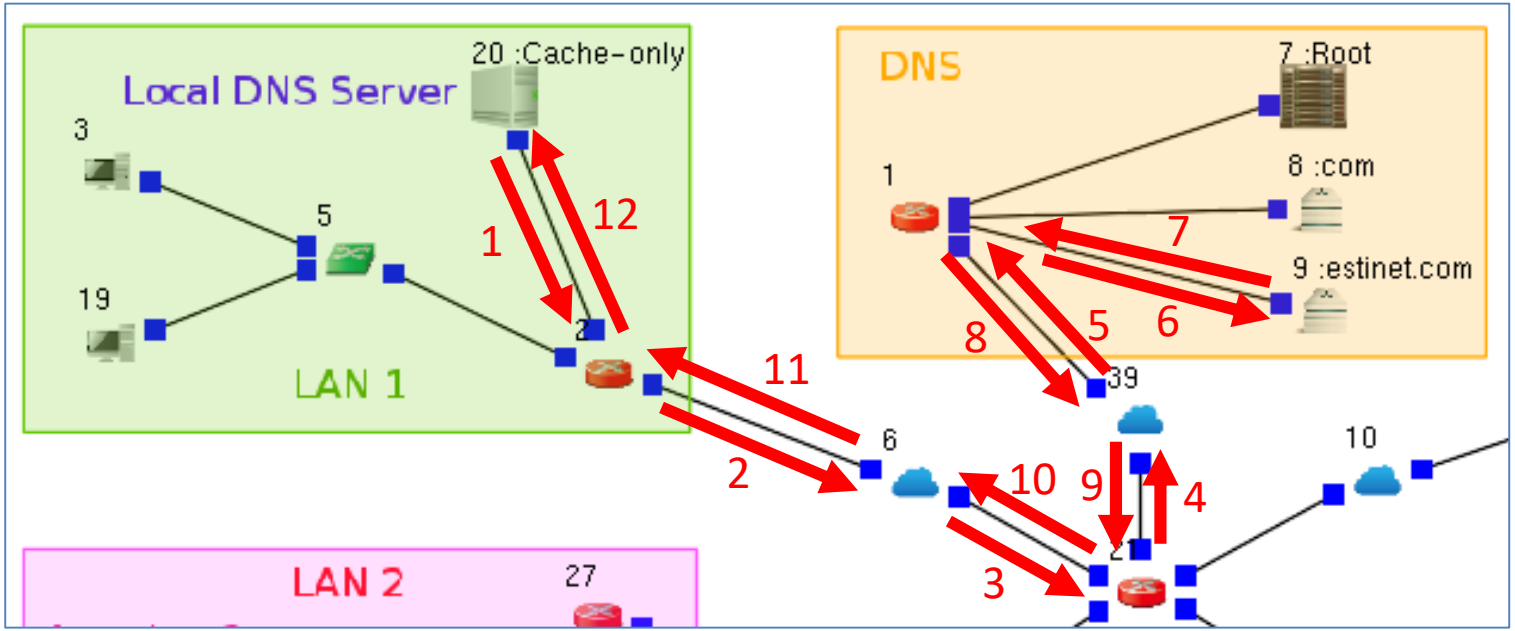
局域网中的域名服务器 20 再去询问管理 “com” 这个域名的服务器 8

- 因为服务器 8 也不知道答案，所以服务器 8 回覆给服务器 20，请服务器 20 再去询问管理 ”estinet.com” 这个域名的服务器 9。



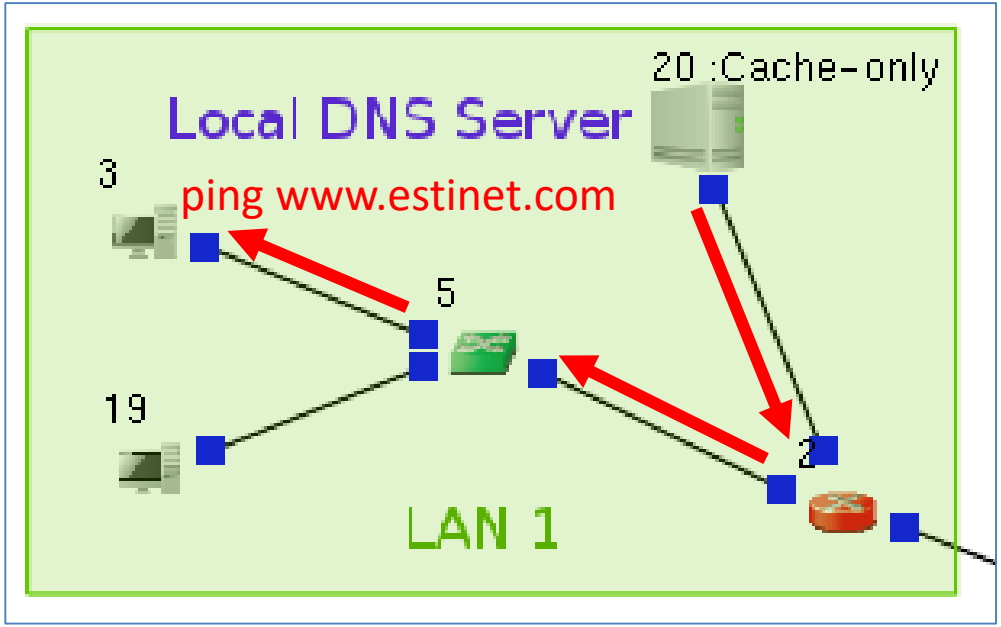
局域网中的域名服务器 20 再去询问管理 “estinet.com” 这个域名的服务器 9

- 最终，服务器 20 会由服务器 9 得知 www.estinet.com 所对应的 IP 地址为何。



局域网中的域名服务器 20 将答案回传给用户 3

- 服务器 20 会将答案记住一段时间（缓存），若这段时间内有其他用户来询问相同的问题，就可以将缓存的答案直接回覆给用户。



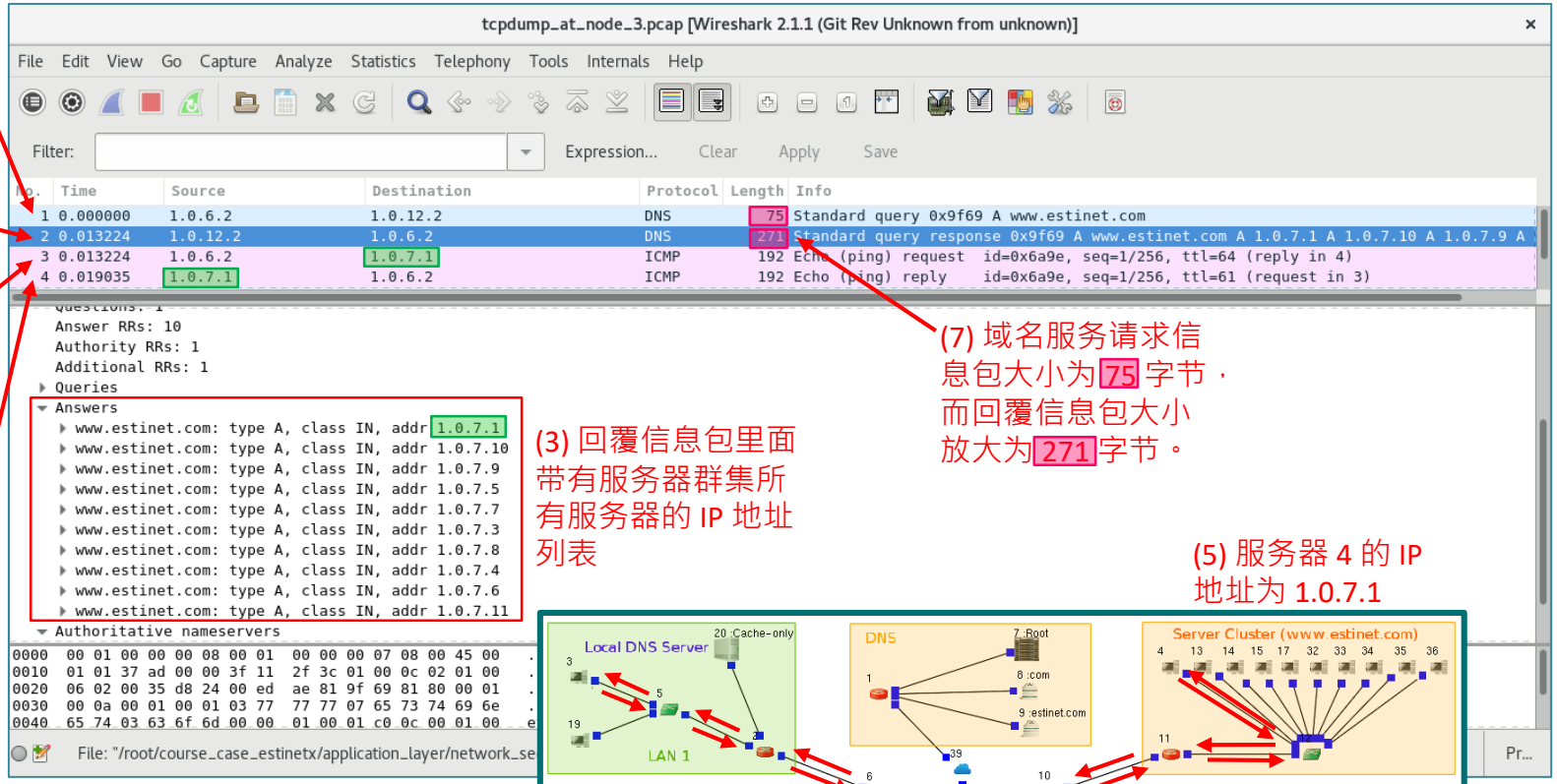
用户 3 会取得服务器群集中所有服务器的 IP 地址列表（利用 Wireshark 工具开启在用户 3 上面执行 tcpdump 指令所纪录到的信息包内容）

(1) 用户 3 送出的域名服务请求信息包

(2) 用户 3 收到的域名服务回覆信息包

(4) 用户 3 向 IP 地址是 1.0.7.1 的服务器发出回应请求

(6) 用户 3 收到 IP 地址是 1.0.7.1 的服务器所回传的回应



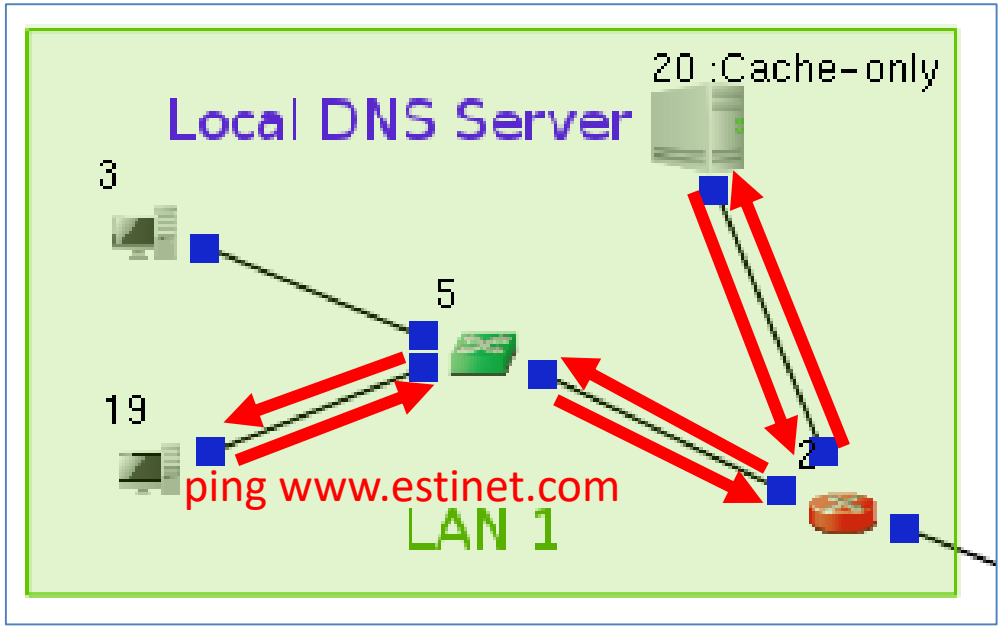
(3) 回覆信息包里面带有服务器群集所有服务器的 IP 地址列表

(7) 域名服务请求信息包大小为 75 字节，而回覆信息包大小放大为 271 字节。

(5) 服务器 4 的 IP 地址为 1.0.7.1

一号局域网 (LAN 1) 中的用户 19 要求服务器群集的回应服务

- 用户 19 执行 ping www.estinet.com 指令去跟服务器群集要求回应 (echo) 服务。
- 用户 19 会先去跟局域网中的域名服务器 20（ Local DNS Server ）来询问 www.estinet.com 所对应的 IP 地址。
- 因为域名服务器 20 先前已经记住了 www.estinet.com 所对应的 IP 地址有哪些，因此服务器 20 直接将答案回覆给用户 19。



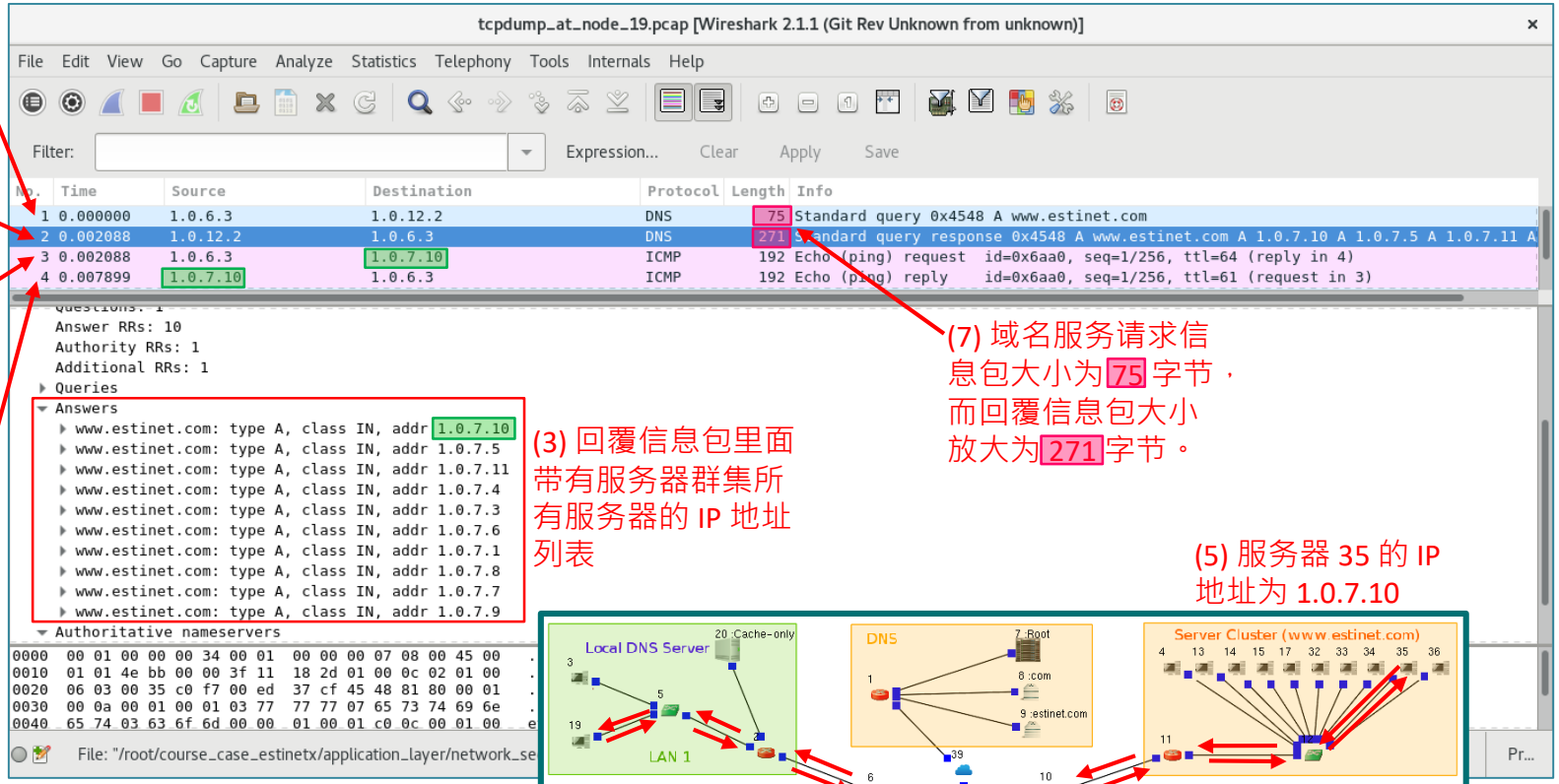
用户 19 会取得服务器群集中所有服务器的 IP 地址列表（利用 Wireshark 工具开启在用户 19 上面执行 tcpdump 指令所纪录到的信息包内容）

(1) 用户 19 送出的域名服务请求信息包

(2) 用户 19 收到的域名服务回覆信息包

(4) 用户 19 向 IP 地址是 1.0.7.10 的服务器发出回应请求

(6) 用户 19 收到 IP 地址是 1.0.7.10 的服务器所回传的回应



(3) 回覆信息包里面带有服务器群集所有服务器的 IP 地址列表

(7) 域名服务请求信息包大小为 75 字节，而回覆信息包大小放大为 271 字节。

(5) 服务器 35 的 IP 地址为 1.0.7.10

利用域名服务来进行放大式网络攻击

为何可以利用域名服务来对其它服务器发动攻击？

- 一个服务器群集的域名，实际上是由多个服务器同时来提供服务，因此，当互联网用户发出域名服务请求时，会得到一串服务器的 IP 地址列表，换句话说，互联网用户送出一个小信息包 (域名服务要求) 后，会收到一个相对较大的信息包 (域名服务回覆)。
- 如果，一个攻击者想攻击互联网上一台正在提供服务的服务器 S，攻击者可假冒服务器 S 来发出域名服务要求，如此，放大后的域名服务回覆就会送回到服务器 S 上 (反射式攻击)，若这样的回覆信息包太多的话，就会影响到服务器 S 的运作，造成拒绝服务 (Denial of Service, DoS) 的情况。
- 单一攻击者有时无法对攻击的对象造成拒绝服务的情况，所以通常会由多个攻击者同时发动拒绝服务的攻击，这样的方式称为分布式拒绝服务 (Distributed Denial of Service, DDoS) 攻击。

用户 38 第一个发动攻击，它执行了一个攻击程序来假冒他人发出域名服务请求

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)

指令说明：

(1) 用 python 语言编程的攻击程序

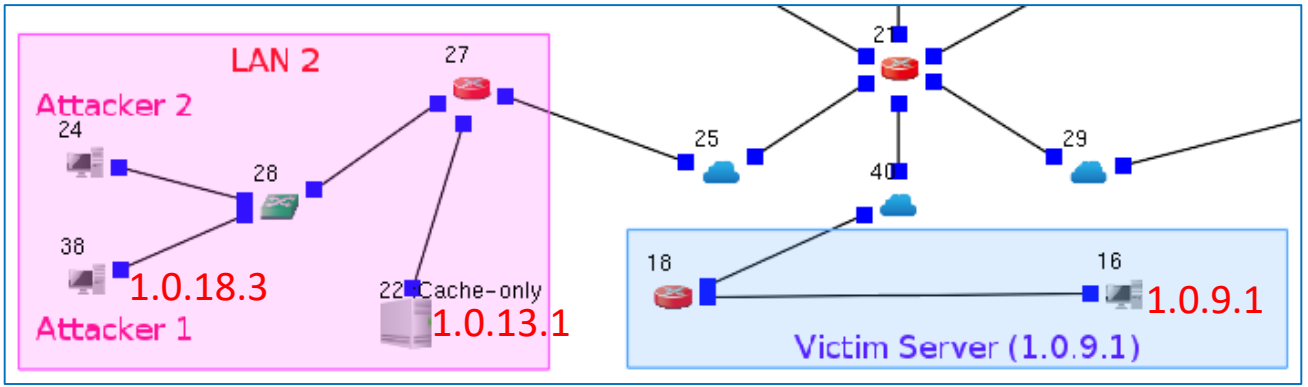
(2) 攻击对象的 IP 地址 (服务器 16)

(3) 透过哪一台域名服务器来进行反射式攻击 (局域网的域名服务器 22)

(4) 所要询问的域名 (有放大式效果)

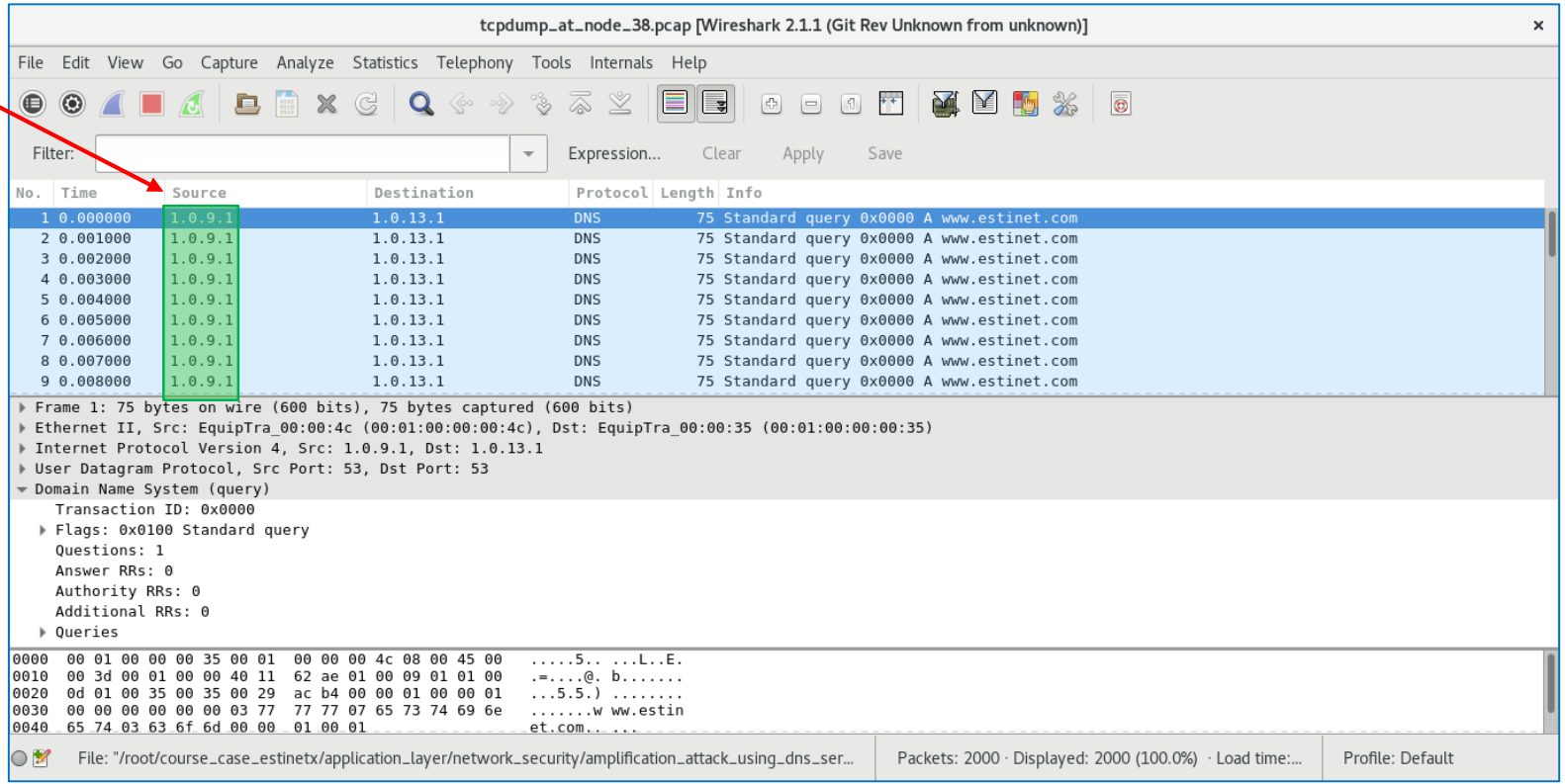
(5) 攻击持续的时间

(6) 连续发出域名服务请求的间隔 (秒)

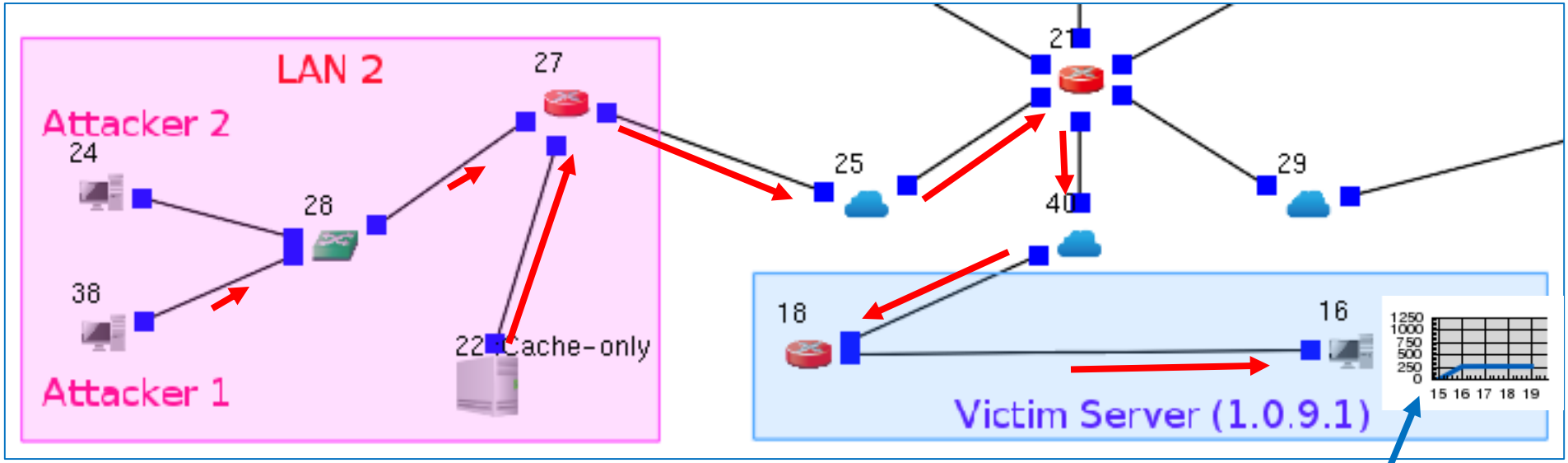


利用 Wireshark 工具开启在用户 38 上面执行 tcpdump 指令所纪录到的信息包内容

在信息包中，传送者的内容填的是服务器 16 的 IP 地址 (1.0.9.1)，而不是用户 38 自己的 IP 地址 (1.0.18.3)，因为这些信息包是用户 38 假冒服务器 16 所送出的。



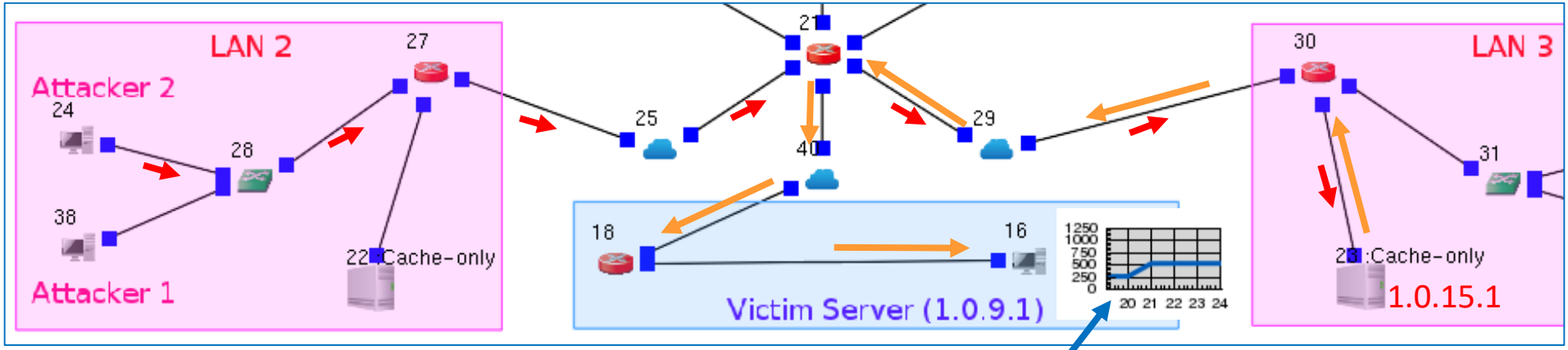
用户 38 透过局域网的域名服务器 22 来对互联网上的另外一台服务器 16 进行反射式与放大式的攻击



但是攻击力道仅消耗了服务器 16 可用网络流量的 1/5 左右。

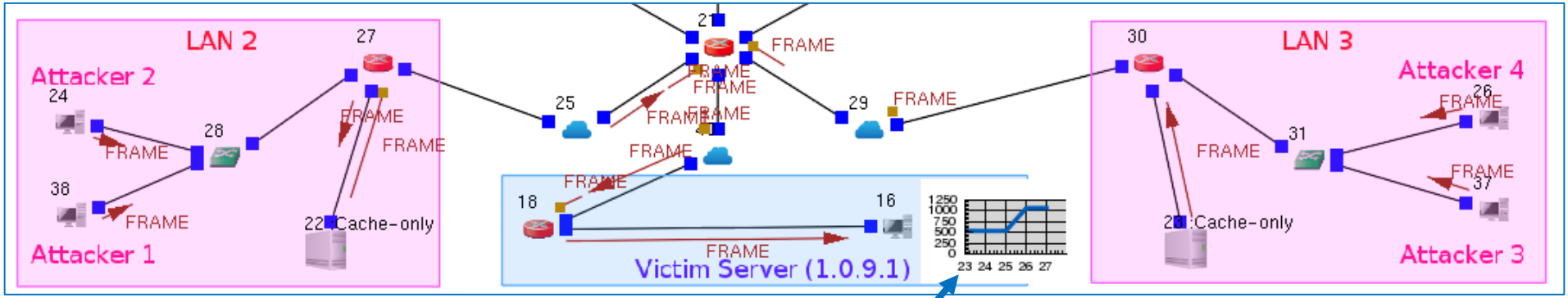
用户 24 透过外部的域名服务器 23 来对互联网上的另外一台服务器 16 进行反射式与放大式的攻击

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



結合用户 38 与用户 24 两者的攻击力道，消耗了服务器 16 可用网络流量的 2/5 左右。

最后，在局域网 3 里面的用户 37 与用户 26 也加入攻击行列，用户 37 是透过局域网内的域名服务器 23 来攻击，用户 26 是透过外部的域名服务器 22 来攻击。

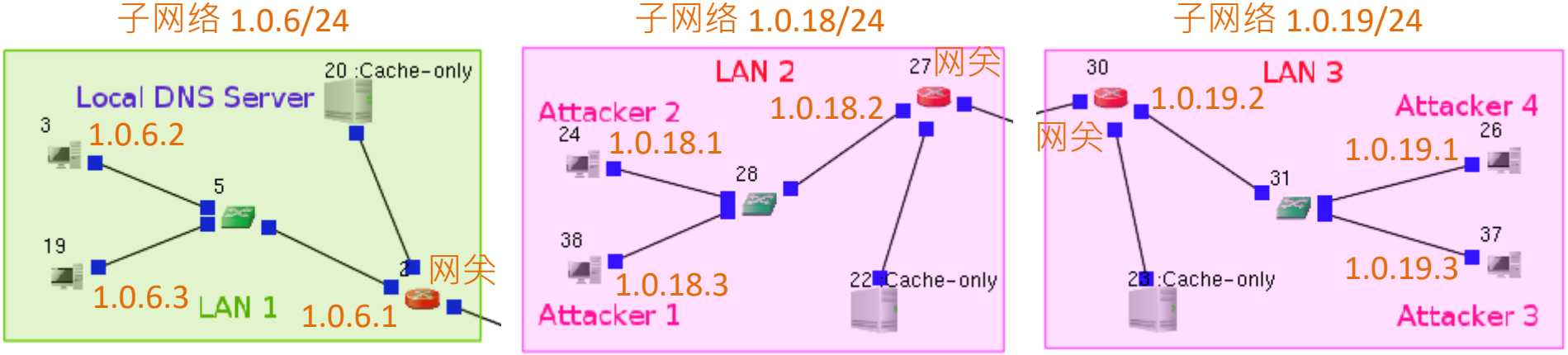


结合四个攻击者的攻击力道，消耗了服务器 16 可用网络流量超过 4/5，已对服务器 16 的运作造成显著影响。

利用防火墙来进行防御

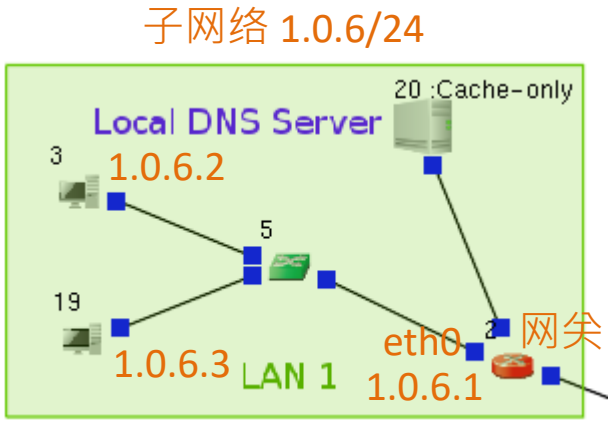
防御的方法之一：找出假冒传送者的信息包

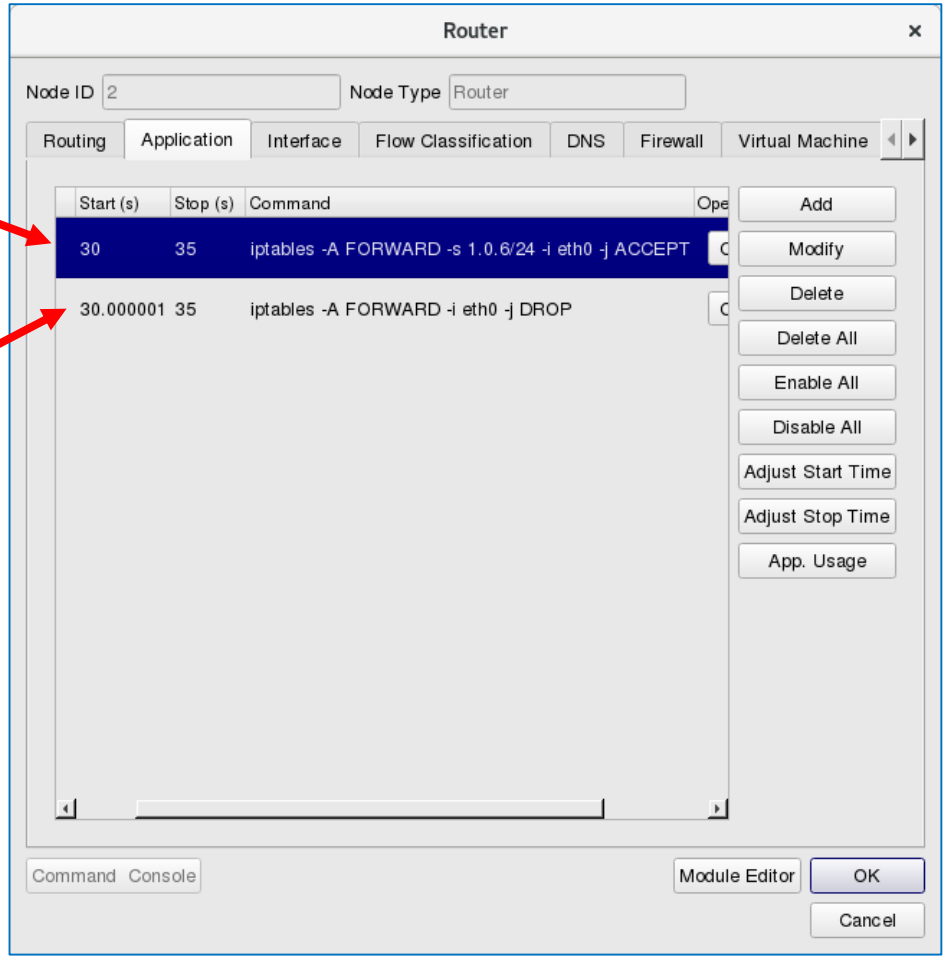
- 在互联网协议的规范下，同一个子网络下的 IP 地址是有规则性的。例如在子网络 1.0.6/24 下的 IP 地址就会是 1.0.6.1, 1.0.6.2, 1.0.6.3, … , 1.0.6.254。
- 一旦攻击者在所发出的信息包中，将传送者填写为其它子网络下的某个 IP 地址时，当这个信息包通过网关的时候，就可以被找出来并过滤掉，如此，假冒传送者的攻击行为就可以被阻挡下来。



在局域网 1 的网关 2 上设定防火墙规则来过滤假冒的信息包

- 第一条规则检查当信息包中的传送者 IP 地址是属于这个子网络所有时，才允许这个信息包通过网关。
- 第二条规则过滤掉所有不符合第一条规则的所有信息包。

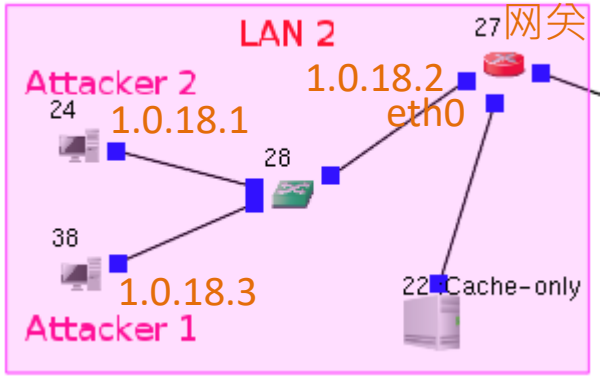


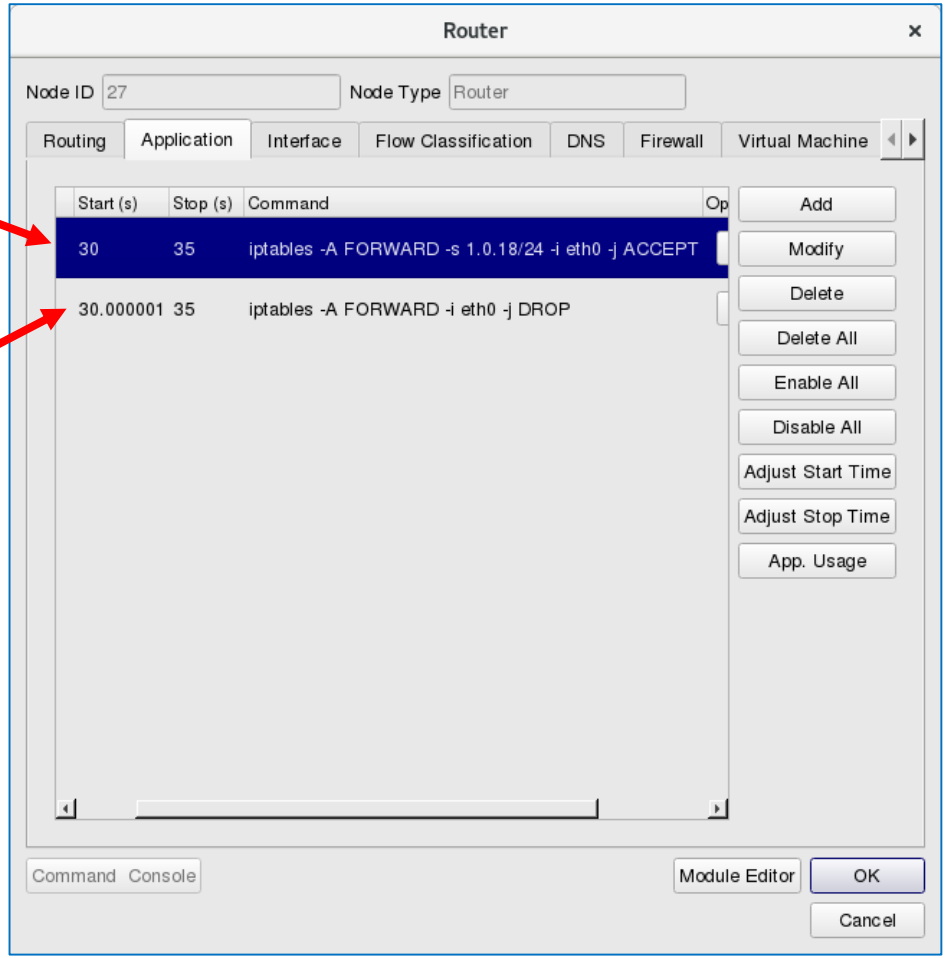


在局域网 2 的网关 27 上设定防火墙规则来过滤假冒的信息包

- 第一条规则检查当信息包中的传送者 IP 地址是属于这个子网络所有时，才允许这个信息包通过网关。
- 第二条规则过滤掉所有不符合第一条规则的所有信息包。

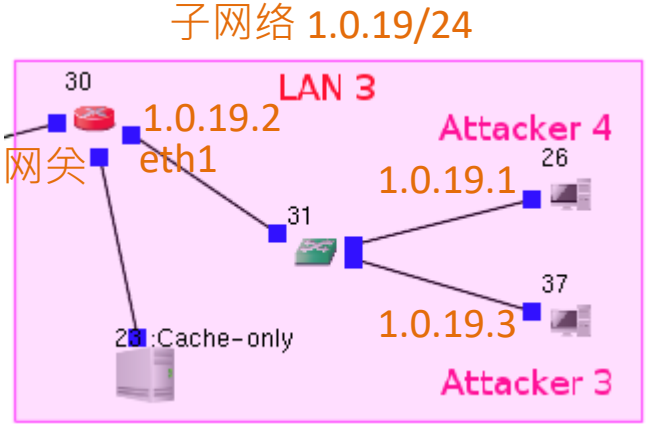
子网络 1.0.18/24

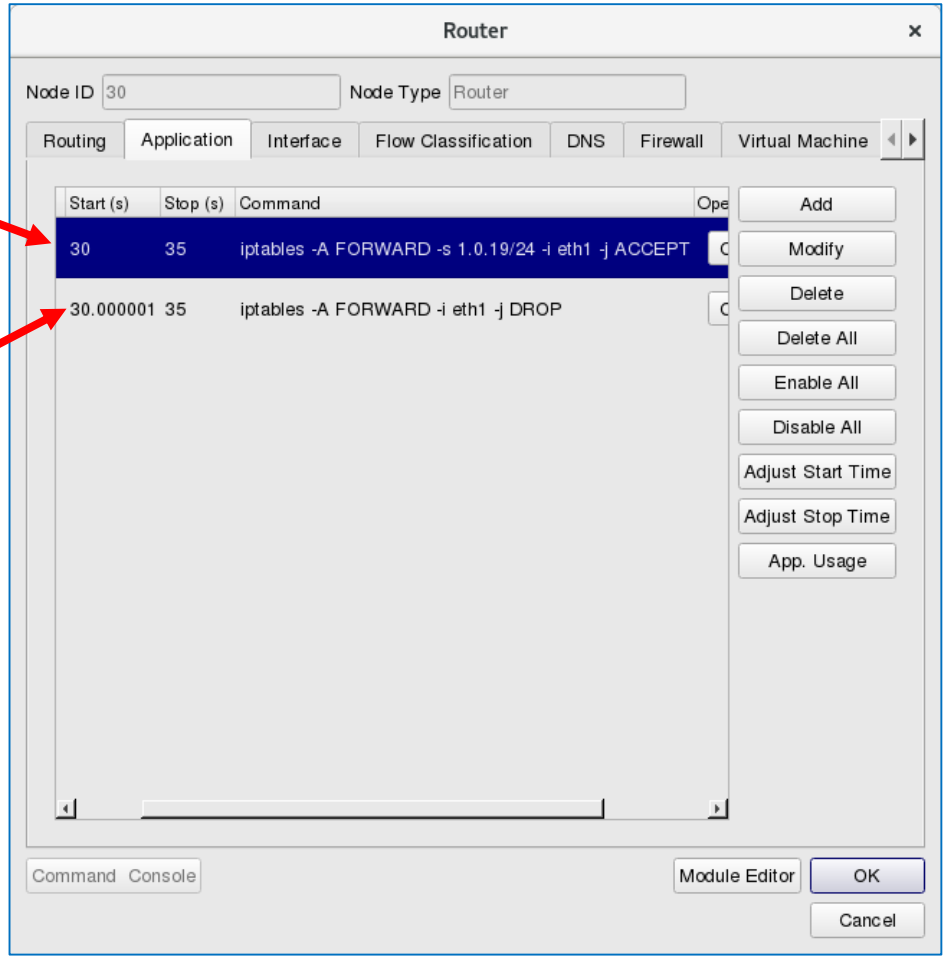




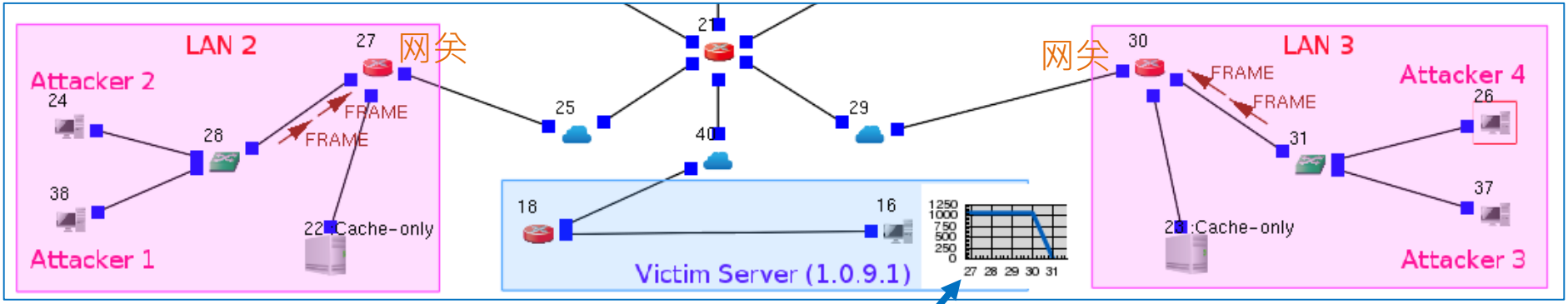
在局域网 3 的网关 30 上设定防火墙规则来过滤假冒的信息包

- 第一条规则检查当信息包中的传送者 IP 地址是属于这个子网络所有时，才允许这个信息包通过网关。
- 第二条规则过滤掉所有不符合第一条规则的所有信息包。



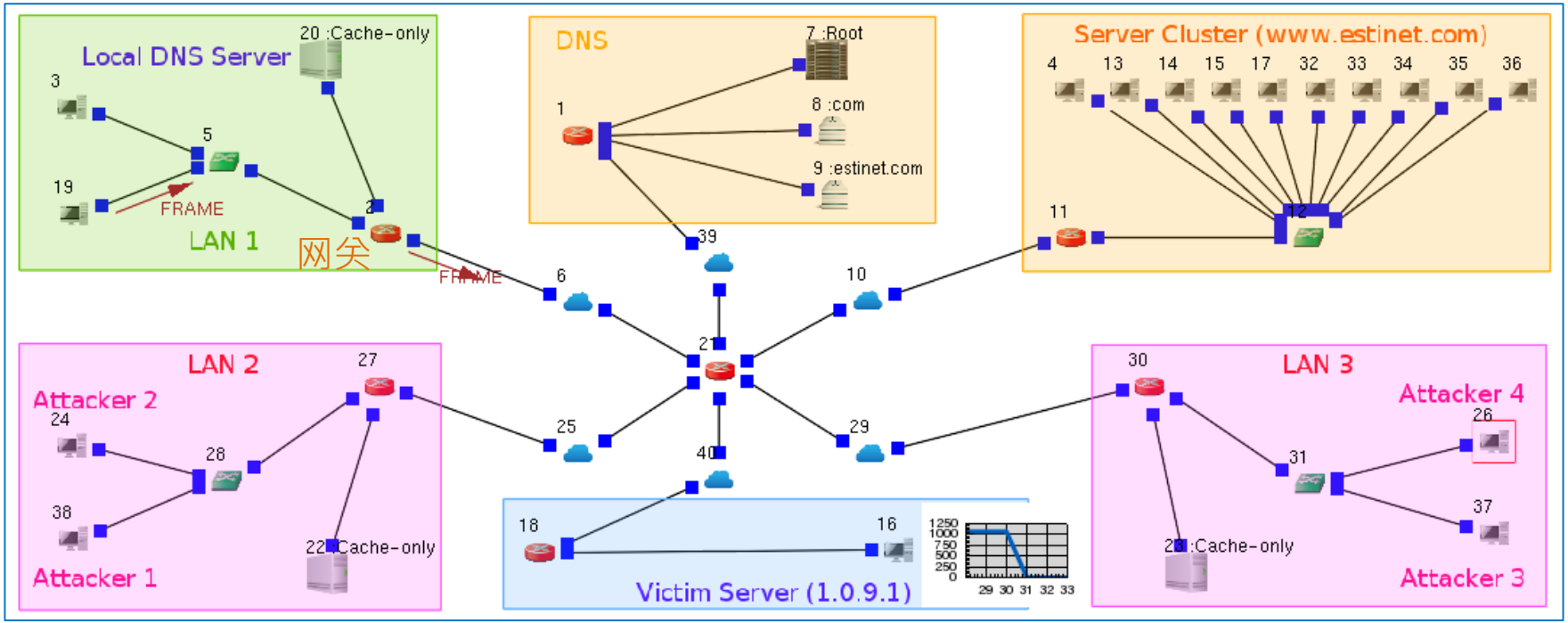


在网关上的防火墙将假冒传送者的信息包给过滤掉了，因此，被攻击的服务器就不再收到域名服务回覆信息包。



服务器 16 的运作恢复正常。

局域网 1 中，正常的信息包仍可通过网关上的防火墙



总结

重点回顾

- 为了同时服务互联网上众多的用户，服务器群集如何利用一个域名来对应多个服务器并且达到负载均衡？
- 相对于域名服务的请求信息包来说，回覆信息包的大小在什么情况下会变大？
- 如何利用域名服务来进行反射式攻击？
- 要如何阻挡假冒传送者的信息包？