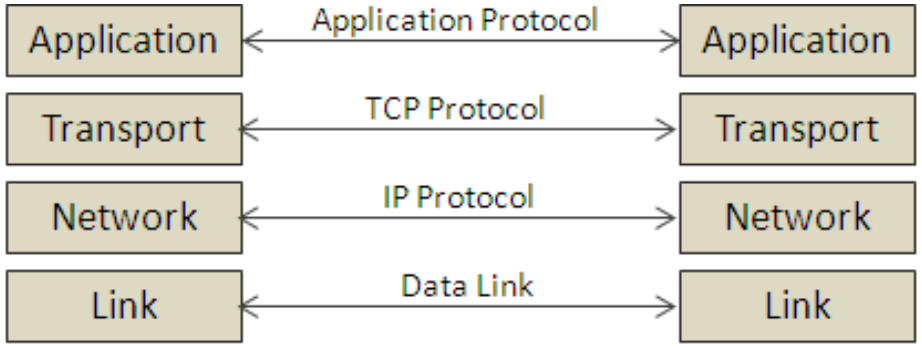
ELECS425F
Computer and Network Security

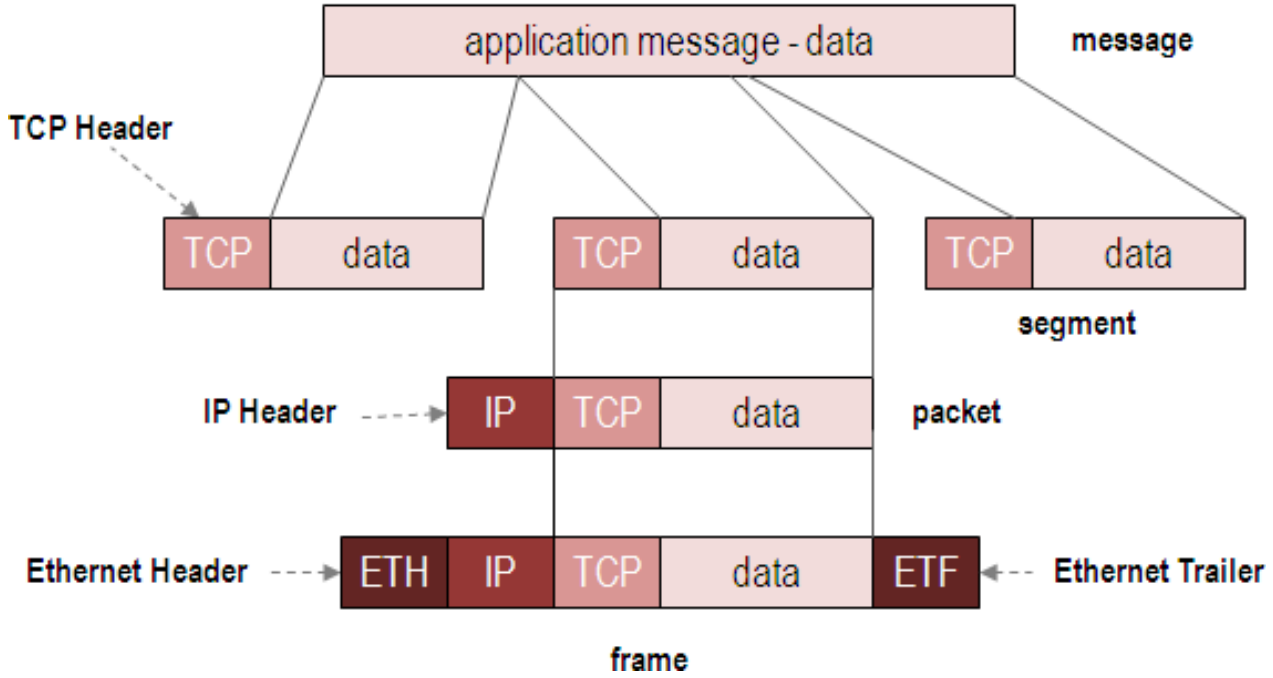
Lec 06

Review of TCP Protocol Stack

Ethernet is not the only layer 2 protocol

But we use Ethernet in this course. Because at our PC, it can get Ethernet frame easily.





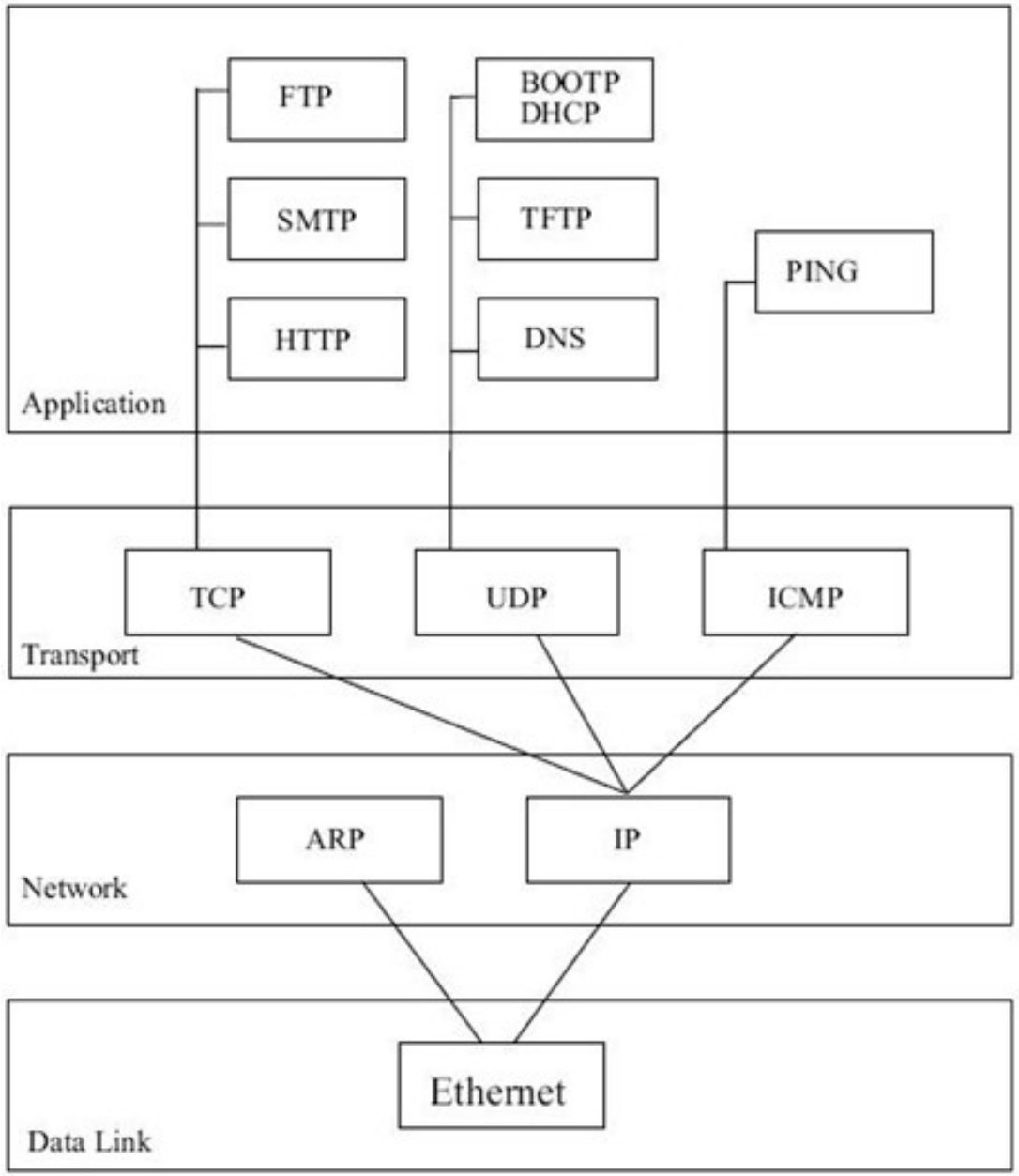
- Layered Model

- PDU (Protocol Data Unit) in the different layer
- PDU: Different data format in different layer
- Different Format => Different Header
- The operation of adding / removing head; Encapsulation / de-encapsulation when the data goes though different layer

Remember these terms: frame, packet, TCP segment, application data = message

Ethernet and WiFi Frame Format

Example protocols in different layers

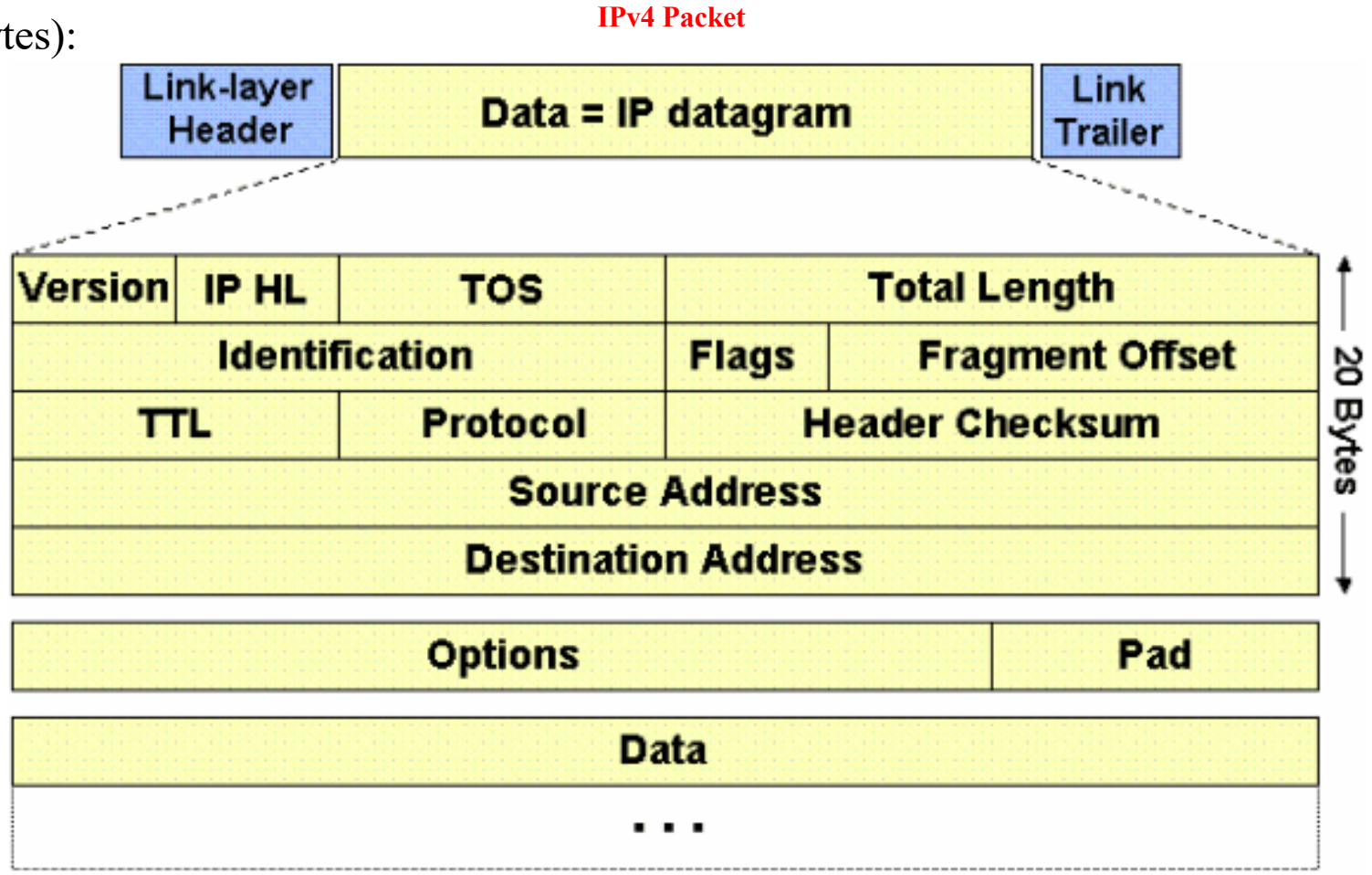


* Ping is not a protocol

It is a tool/command which useful and popular.

Summary of Internet Protocol (IP)

IP Header Structure (20+ Bytes):



The major function of IP protocol itself is addressing.

The routing function is provided by other routing protocols like OSPF, BGP, RIP.

Can we capture some routing protocol data/packet?
Usually we cannot get at PC side

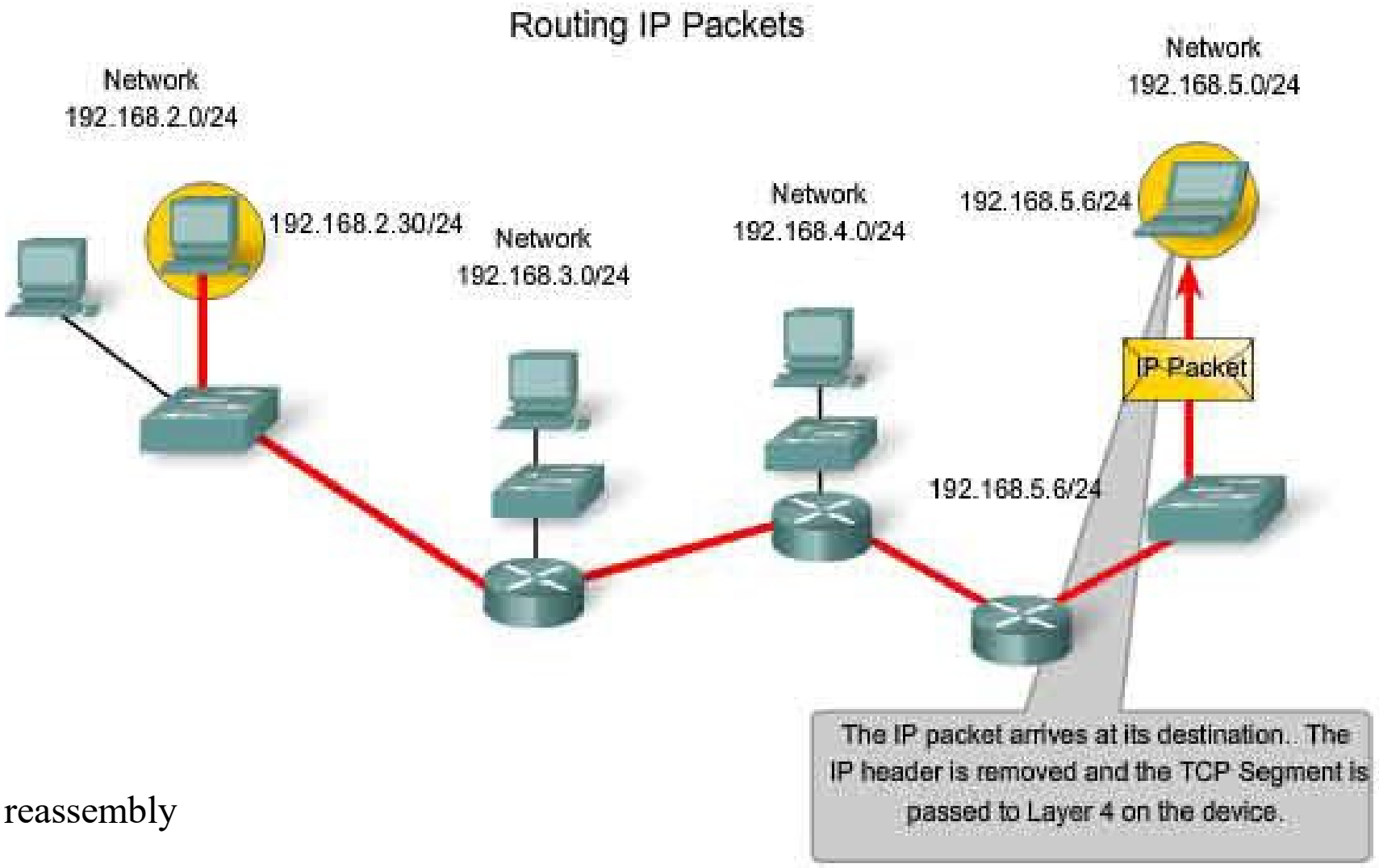
- Connectionless: unreliable, best effort
- Routing: IP host knows location of router (gateway); IP gateway knows route to other networks.
- Routing IP Packets: many routers/hops along the way may process the packet before reaching the destination.

IPv4 has fragmentation and reassembly.
Fragmentation happens in the middle of paths. But reassembly only happens at the destination.

The performance of fragmentation is not good.

So in IPv6, there is not fragmentation.

Original design of TTL is used to prevent loop in the network; Later ICMP makes use of it to analyse the network.



- Fragmentation and reassembly
- TTL field: decremented after each hop, packet will be dropped if TTL is zero.
- Error reporting: ICMP packet to source if packet is dropped.

Recap: The ICMP is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

Security Problems in IP, ICMP

Contents of an ICMP packet:

1. Not authenticated. Everyone can send IP address.
2. Easy to override. People can easily created fake packet from a sources.

Solution to prevent:
If you are in the organization. Internal firewall can find these problem.

ICMP packet

	Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Payload (8+ bytes)	Type of message	Code	Checksum	
	Quench			
	Data (*optional*)			

ICMP types and codes: https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

- Source IP (in IP headers) is not authenticated
- Easy to override using raw socket: anyone with their own machine can send packets with arbitrary source IP.

Common tools of TCP/IP packet assembler

hping3 (http://tools.kali.org/information-gathering/hping3)
Scapy (http://resources.infosecinstitute.com/what-is-scapy/)

- **IP address spoofing** or IP spoofing is the creation of IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system.

- **Implications of IP address spoofing**
  - **Anonymous DDoS Attacks**
  - **Reflection DDoS Attacks**

In a reflection DDoS attack, the attacker imitates ("spoofs") the victim's IP address and sends a request for information via UDP to servers ("reflectors") known to respond to that type of request. The servers answer the request and send ("reflect") the response to the victim's IP address. Thus, from the servers' perspective, the victim sent the original request.

Waste, consume victim's resources.
Like interface buffer, processors, etc.
Other valid user will not able to access the server.

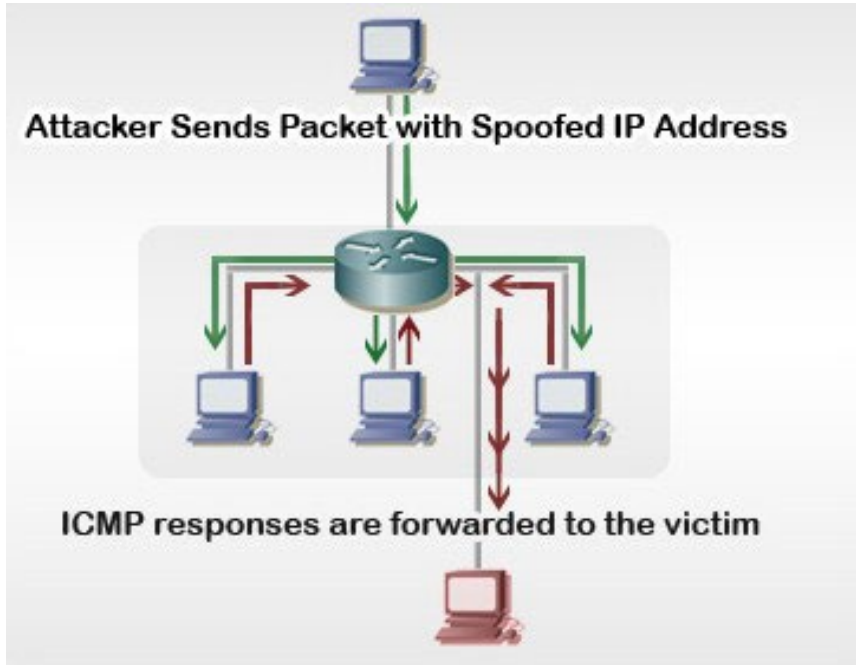
Reflection DDoS Attack by NTP

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2017-03-05 21:33:50.456	119.464	17	39.110.63.180:123	180.235.[redacted]:52352	633465	296461620	2
2017-03-05 21:33:50.000	119.752	17	14.136.204.60:123	180.235.[redacted]:52352	517198	242048664	2
2017-03-05 21:33:49.208	120.520	17	203.151.93.84:123	180.235.[redacted]:52352	282003	129721788	2
2017-03-05 21:33:49.148	120.584	17	157.7.131.233:123	180.235.[redacted]:52352	279983	131032044	2
2017-03-05 21:33:49.720	119.756	17	1.9.116.229:123	180.235.[redacted]:52352	193600	90604800	2
2017-03-05 21:33:49.776	120.028	17	204.2.129.243:123	180.235.[redacted]:52352	183814	86024952	2
2017-03-05 21:33:49.192	120.592	17	81.175.103.28:123	180.235.[redacted]:52352	180093	84283524	2
2017-03-05 21:33:50.044	119.532	17	86.35.5.182:123	180.235.[redacted]:52352	176464	82296720	2
2017-03-05 21:33:49.680	119.912	17	89.115.124.63:123	180.235.[redacted]:52352	155900	72961200	2
2017-03-05 21:33:50.112	119.628	17	185.154.20.144:123	180.235.[redacted]:52352	155194	72630792	2
2017-03-05 21:33:49.124	120.672	17	66.147.51.82:123	180.235.[redacted]:52352	153754	71681040	2
2017-03-05 21:33:49.752	119.952	17	220.224.145.19:123	180.235.[redacted]:52352	140700	65847600	2
2017-03-05 21:33:50.076	119.644	17	213.42.30.90:123	180.235.[redacted]:52352	130368	61012224	2
2017-03-05 21:33:49.248	120.572	17	23.253.58.144:123	180.235.[redacted]:52352	129870	58909032	2
2017-03-05 21:33:50.000	119.788	17	147.178.198.7:123	180.235.[redacted]:52352	122222	55887768	2
2017-03-05 21:39:01.784	49.992	17	8.254.74.6:123	180.235.[redacted]:2690	115195	59440620	1
2017-03-05 21:33:50.104	119.820	17	121.234.106.132:123	180.235.[redacted]:52352	112442	52622856	2
2017-03-05 21:39:01.780	50.056	17	217.66.226.23:123	180.235.[redacted]:2690	111903	57741948	1
2017-03-05 21:39:01.824	50.000	17	213.139.189.26:123	180.235.[redacted]:2690	111847	57713052	1
2017-03-05 21:39:01.784	50.052	17	217.66.226.24:123	180.235.[redacted]:2690	111649	57610884	1
2017-03-05 21:33:49.136	120.660	17	122.155.190.84:123	180.235.[redacted]:52352	111455	50656500	2
2017-03-05 21:33:50.524	119.460	17	116.86.70.22:123	180.235.[redacted]:52352	110900	51901200	2
2017-03-05 21:33:49.728	119.848	17	213.42.30.91:123	180.235.[redacted]:52352	106193	49698324	2
2017-03-05 21:39:01.784	49.992	17	8.254.74.6:123	180.235.[redacted]:61391	104659	54004044	1
2017-03-05 21:33:50.760	119.432	17	118.69.68.34:123	180.235.[redacted]:52352	104658	48979944	2

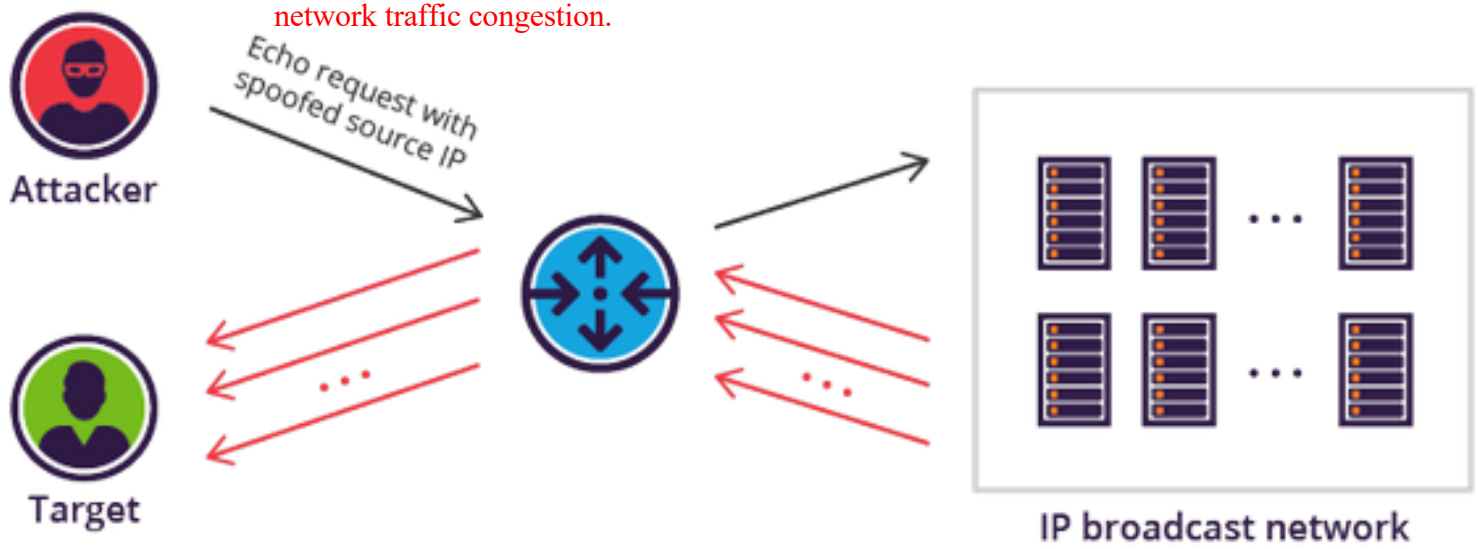
ICMP Attacks

Ping Flood - The attacker overwhelms the victim with ICMP Echo Request (ping) packets. This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies. To prevent ping flood. Some network devices or server may disable PING reply.

Smurf Attack - an attacker will spoof the source address of the ICMP packet and send a broadcast to all computers on that network. If networking devices do not filter this traffic, then they will be broadcasted to all computers in the network. The victim's network gets congested by this much traffic, which brings down the productivity of the entire network.



Send a "broadcast" attack by default, switches will transfer all broadcast. It may cause network traffic congestion.



Demo: `ping -b 255.255.255.255`

ICMP Attacks

The design of ICMP is simple; It is easy to use, to implement; That's may be the reason why ICMP is popular. But it also makes many ppl to make use of ICMP to get others' information and to launch some attacks.

Can we disable ICMP? No, we need to to do something like test connectivity or SNMP connectivity test. (Sol: Disable unused port; Update OS)

ICMP Tunnelling - ICMP tunneling works by injecting arbitrary data into an echo packet sent to a remote computer. The remote computer replies in the same manner, injecting an answer into another ICMP packet and sending it back. The client performs all communication using ICMP echo request packets, while the proxy uses echo reply packets.

Information Gathering - Under the information gathering attack, one can use different methods within the ICMP to find out live host, network topology, OS fingerprinting, ACL detection, and so on.

Trace Route - The trace route command is used to discover the routes that packets actually take when traveling to their destination.

Port Scan - ICMP Error Messages (Protocol/Port Unreachable) can be used to find out the open ports to an IP address or a LAN segment.

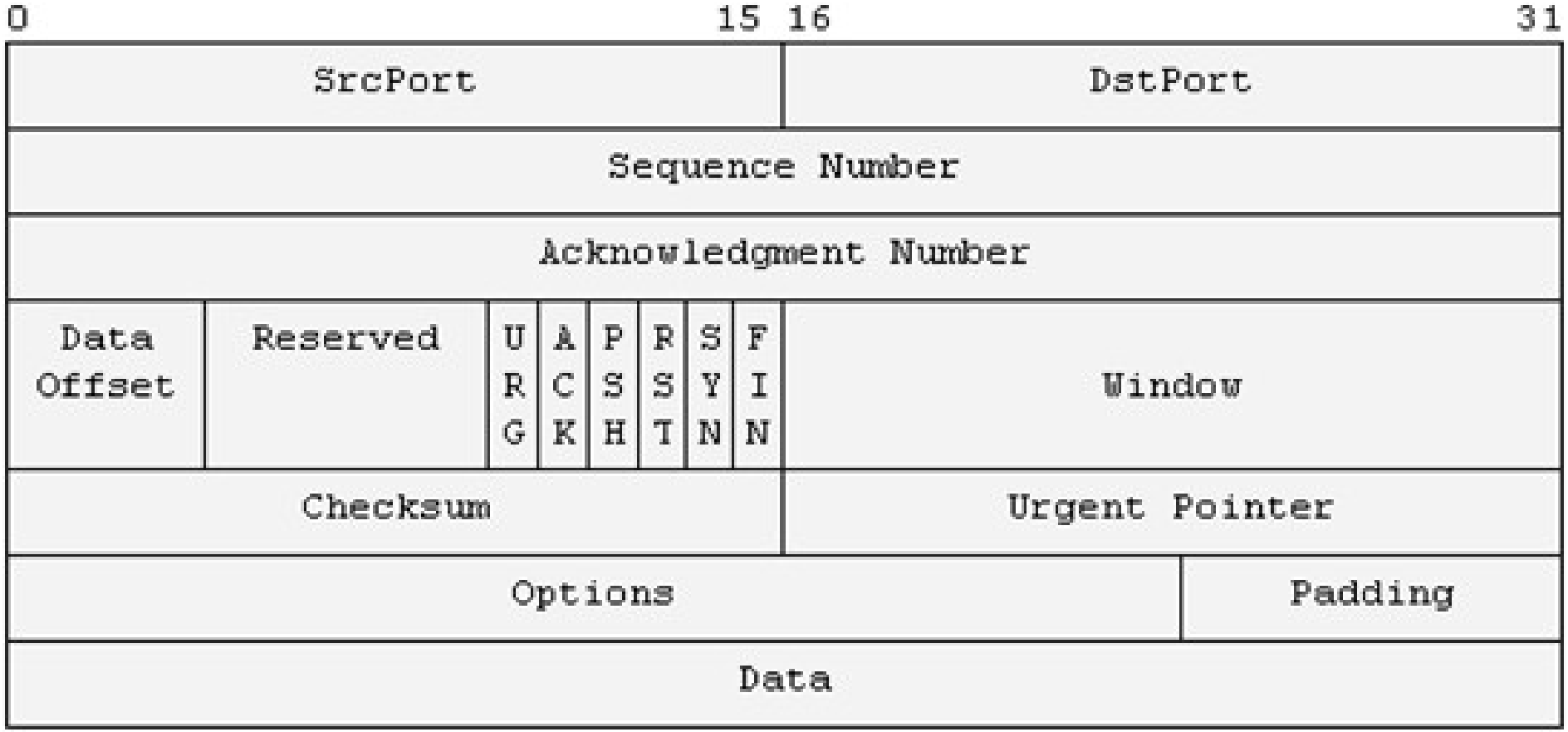
OS fingerprinting - Fingerprinting is a technique to find out what kind of OS the server is running by looking at the response of the ICMP packet.

ICMP Router Discovery - The ICMP router discovery protocol will discover the IP address of the neighbouring routers.

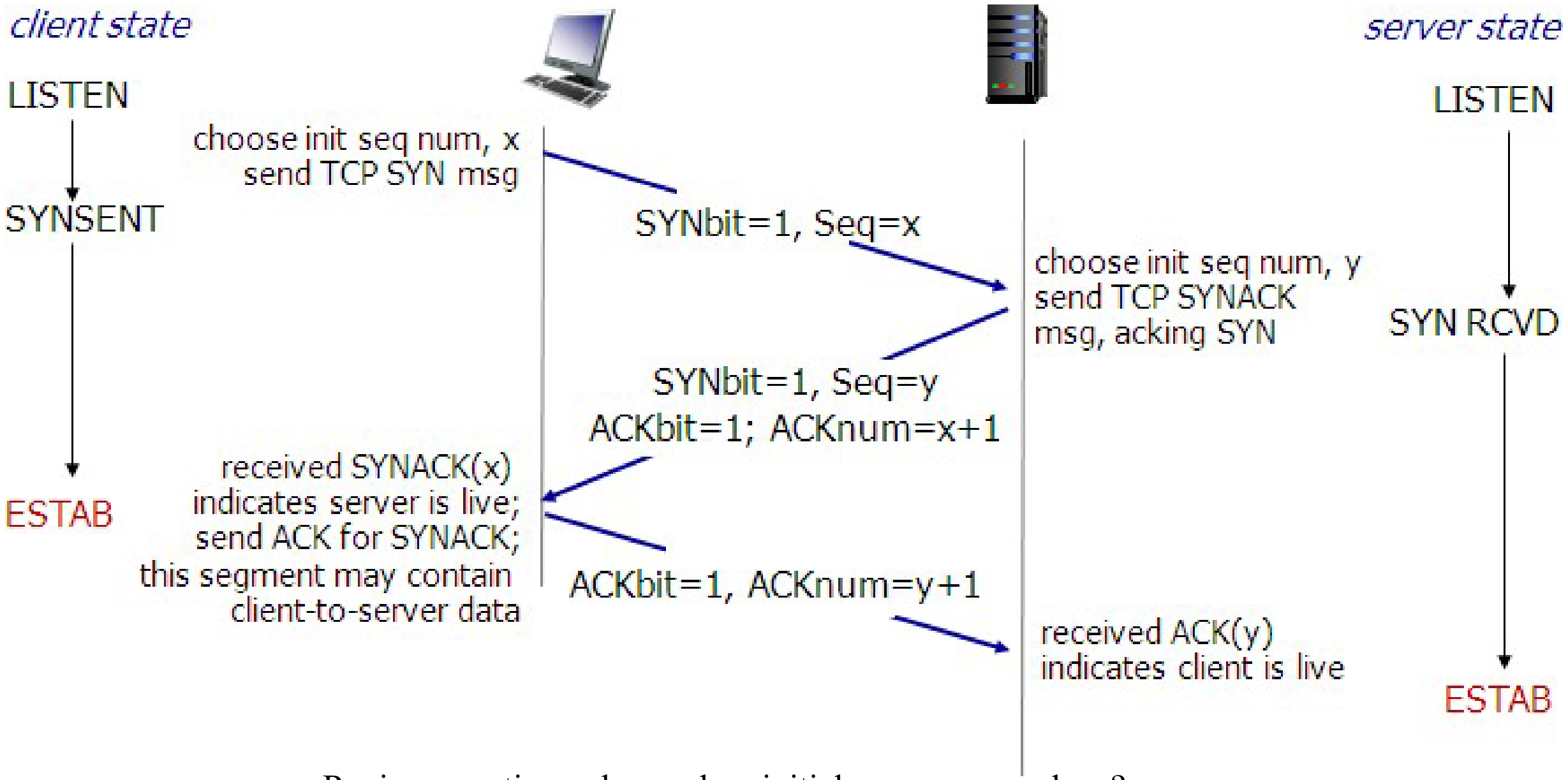
Security Issues of TCP

Summary of TCP

TCP Header Structure (20+ bytes):



- Connection-oriented
- Sender: break data into packets, attach packet numbers
- Receiver: acknowledge receipt, lost packets are resent, reassemble packets in correct order
- TCP connection set-up



Review question: why random initial sequence numbers?

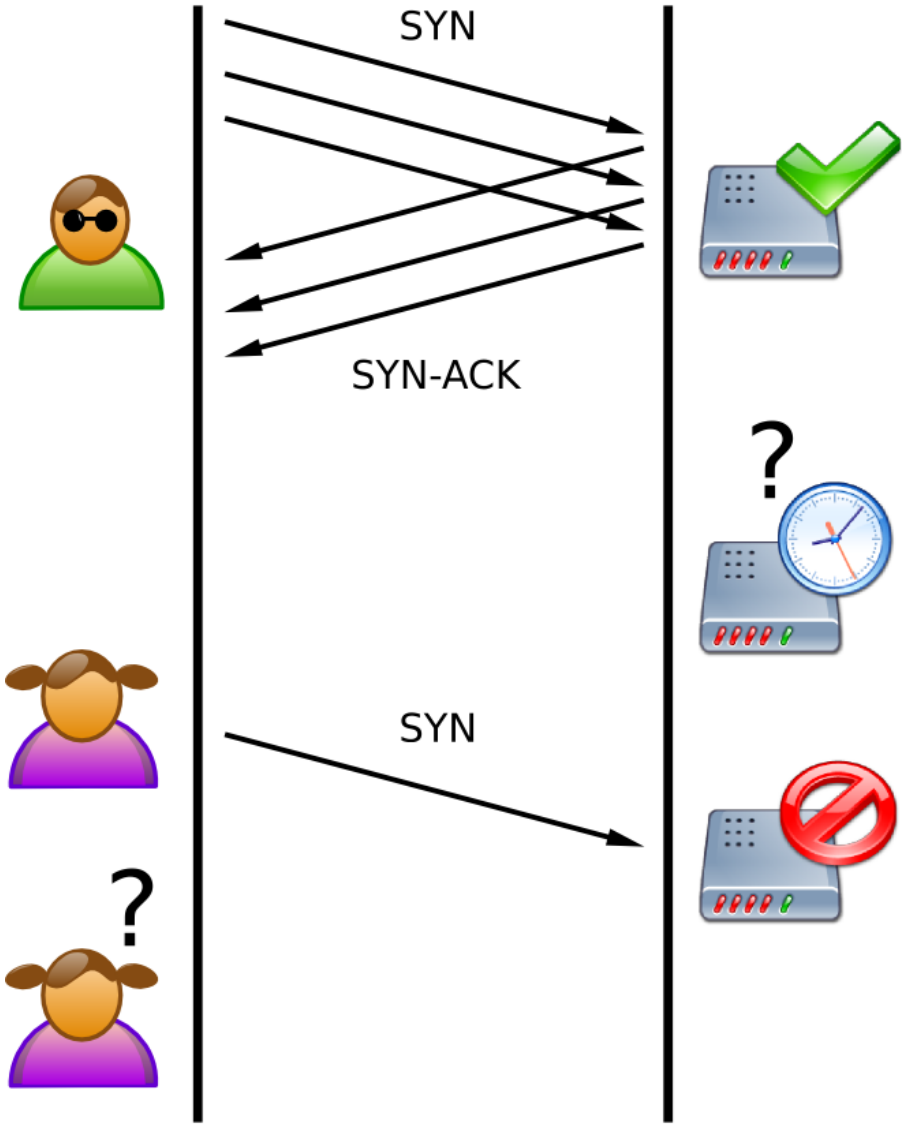
Security Problems in TCP

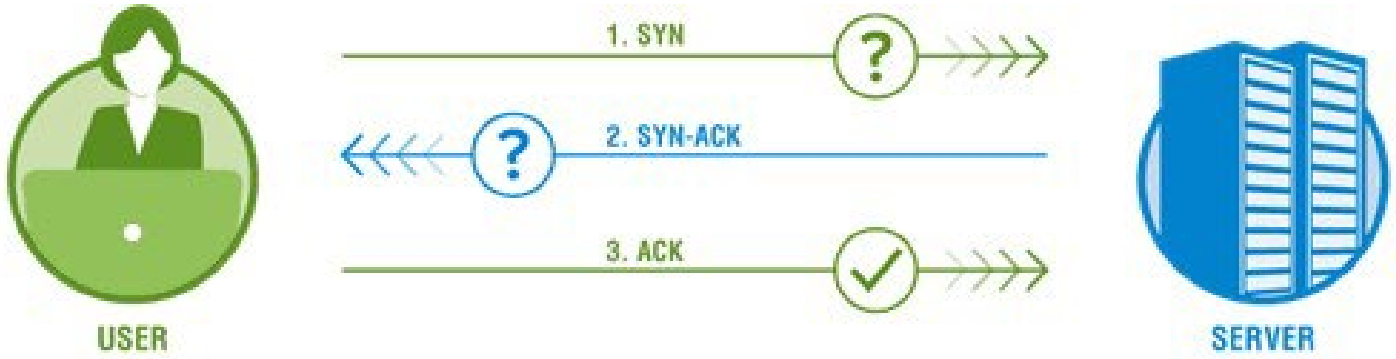
The attacker sends many SYN packets to the server
The server will become very busy with reply and keep those connections, waiting for reply.

It is not preventable as the server is hard to know which packet is valid.

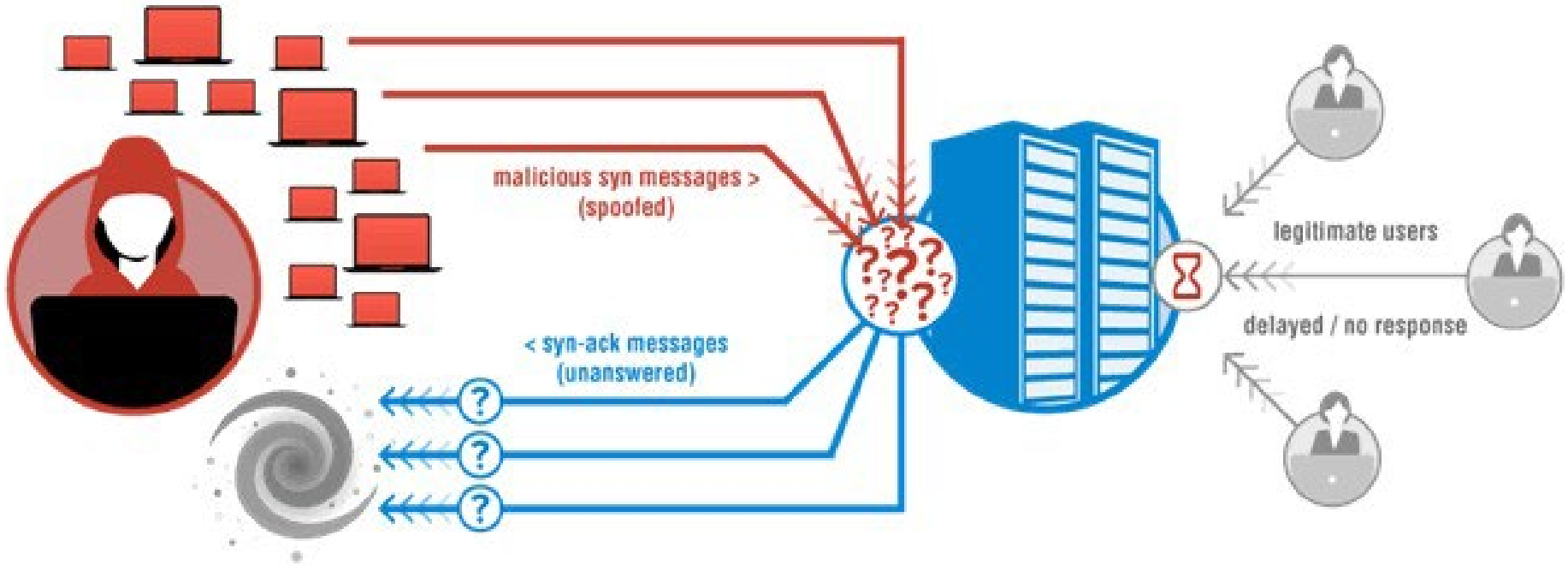
- Network packets can be easily sniffed.
- TCP state easily obtained by eavesdropping.
- Threats: spoofing and session hijacking
- Implications: denial of service (DoS) vulnerabilities
- Attack Example

TCP SYN Flooding: The host conducting the attack, sends TCP/SYN packets to the server often with a fake sender address. The server handles those requests, allocate memory and respond with a TCP/SYN ACK packet. The server is waiting for the client to accept that last packet in order to create a connection between the two hosts. However, the hostile host will never answer back, leaving a half-opened connection, until it timeout.





Normal TCP Connection Set-up



TCP SYN Flood

Demo: Use hping3 to launch TCP SYN flooding:

Host A:

```
hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source lab.ouhk.edu.hk
hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood -a 202.40.219.234
lab.ouhk.edu.hk hping3 -S --flood -V lab.ouhk.edu.hk
```

Host B: netstat -ant to view the TCP connection

TCP reset attack

An attacker sends a forge Reset (RST) TCP packet to an open socket.

If correct TCP sequence number, then the connection will be closed.

(While the range of TCP sequence numbers is quite large, the ability to use the TCP window size greatly decreases the number of guesses needed by the attacker.)

Security Issues of ARP

Summary of ARP

- The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol.

- ARP consists of the following 4 basic messages:

  1) ARP request : Computer A asks on the network, "who has this IP?"

  2) ARP reply : All the other computers ignore the request except the computer which has the requested IP. This computer, lets say B says, I have the requested IP address and here is my MAC address.

  3) RARP request : This is more or less same as ARP request, the difference being that in this message a MAC address is broad-casted on network.

  4) RARP reply : Same concept. Computer B tells that the requested MAC is mine and here is my IP address.

ARP Cache Poisoning

Reasons why ARP is insecure

1) There is no way to authenticate the IP to MAC address mapping in the ARP reply.
2) The host does not check whether it sent an ARP request for which it is receiving ARP reply message.

- ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network.

ARP Cache Poisoning Consequences

Denial of service

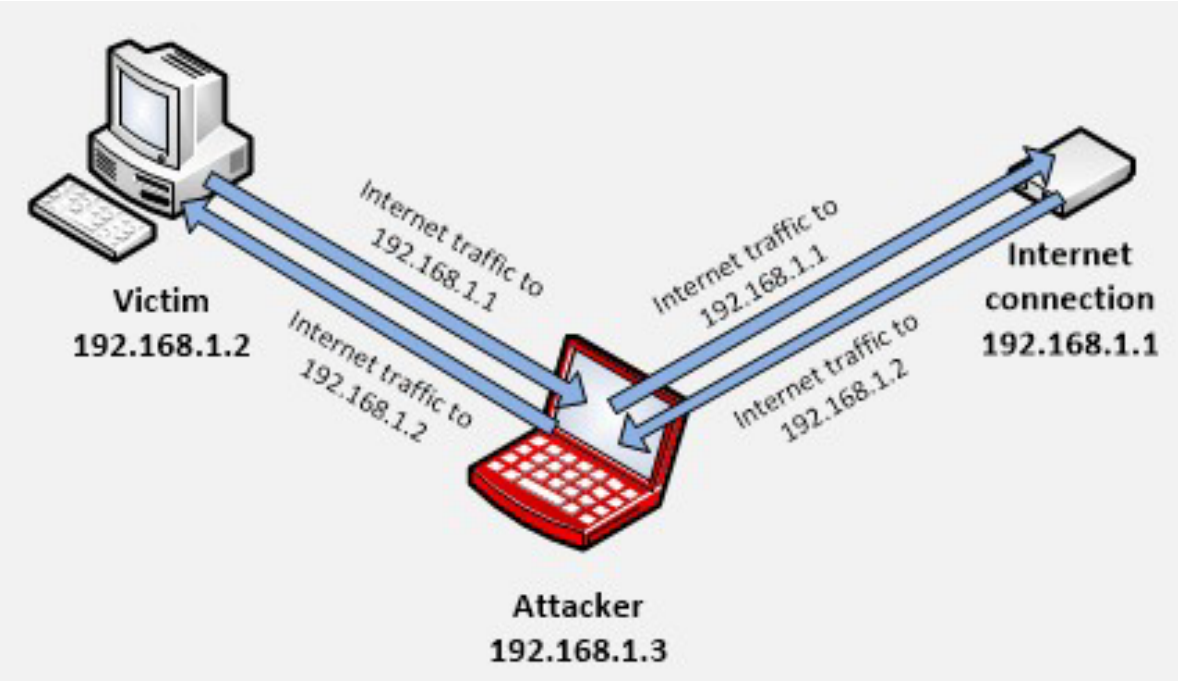
A hacker can send an ARP reply mapping an IP address on network with a wrong or non-existent MAC address. For example, a fake ARP reply mapping the network's router IP with a non-existent MAC will bring down the connectivity of the whole network with the outer world as now any packet sent to IP of router will be sent to a machine with a MAC address that does not exist.

Try it yourself exercise: **Disable other people Wi-Fi connection**

ARP Cache Poisoning Consequences

Man in Middle

A hacker can make his machine sit right in between of the communication between your system and any other system on network. This way the hacker can sniff all the traffic to and from from both the machines.



Try it yourself exercise: **Perform Man-in-the-middle Attack with ettercap**

ARP Cache Poisoning Consequences

MAC Flooding

For switches on network, MAC flooding is an ARP cache poising technique that is used.

Many network switches when overloaded can start acting like a hub and start broadcasting all the network traffic to all the hosts connected to network. So a hacker can flood a switch with fake ARP replies and can make the switch to start behaving like a hub.

In this role, the switch does not enable its ‘port security’ feature due to which it broadcast all the network traffic and taking advantage of this, the hacker can packet sniff the network.

Security Issues of DNS

Summary of DNS

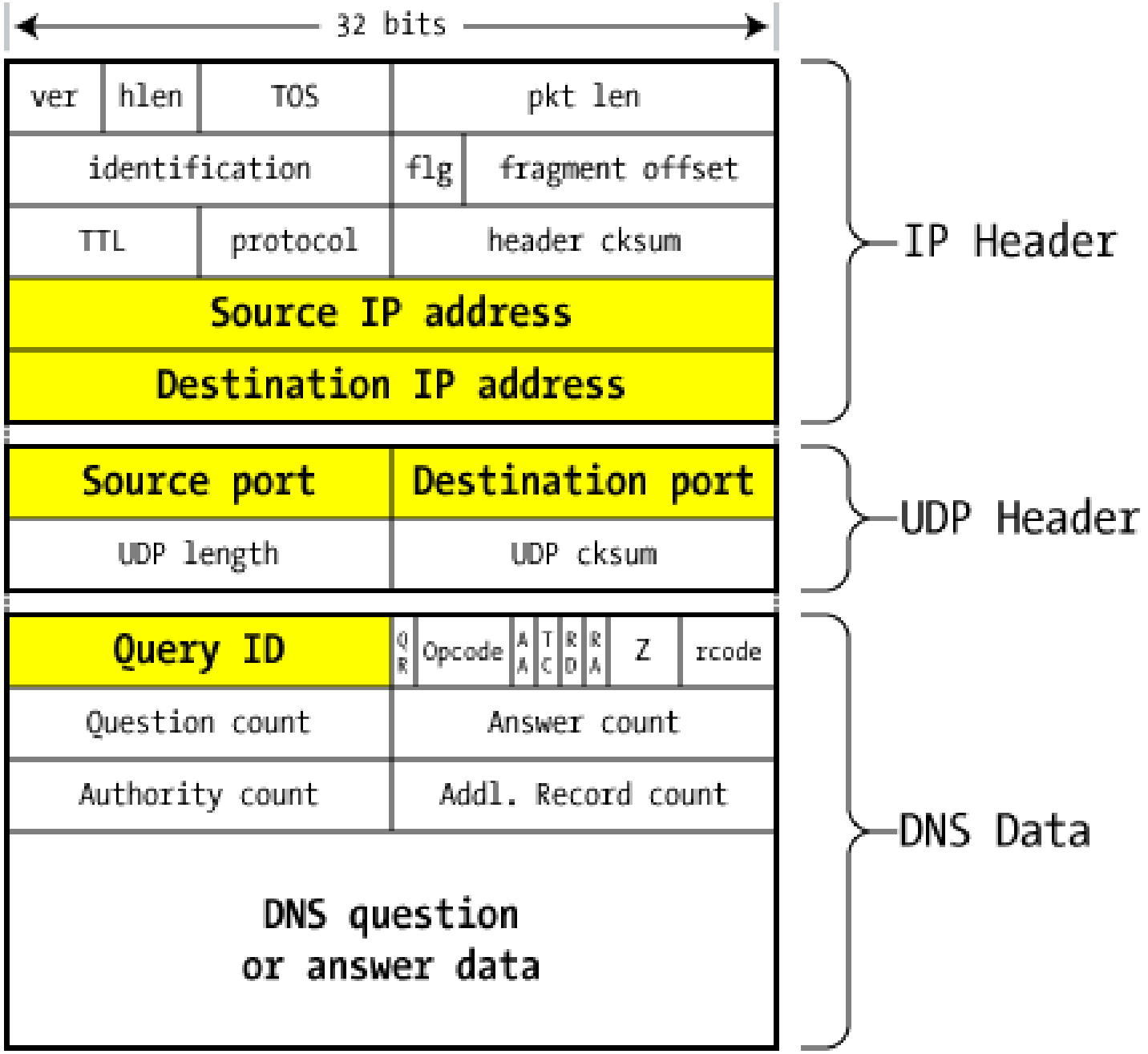
DNS working

Run the following commands and observe the DNS packets/responses.

```
dig +trace stepwise.hk
dig stepwise.hk
dig any stepwise.hk
dig stepwise.hk @8.8.8.8
```

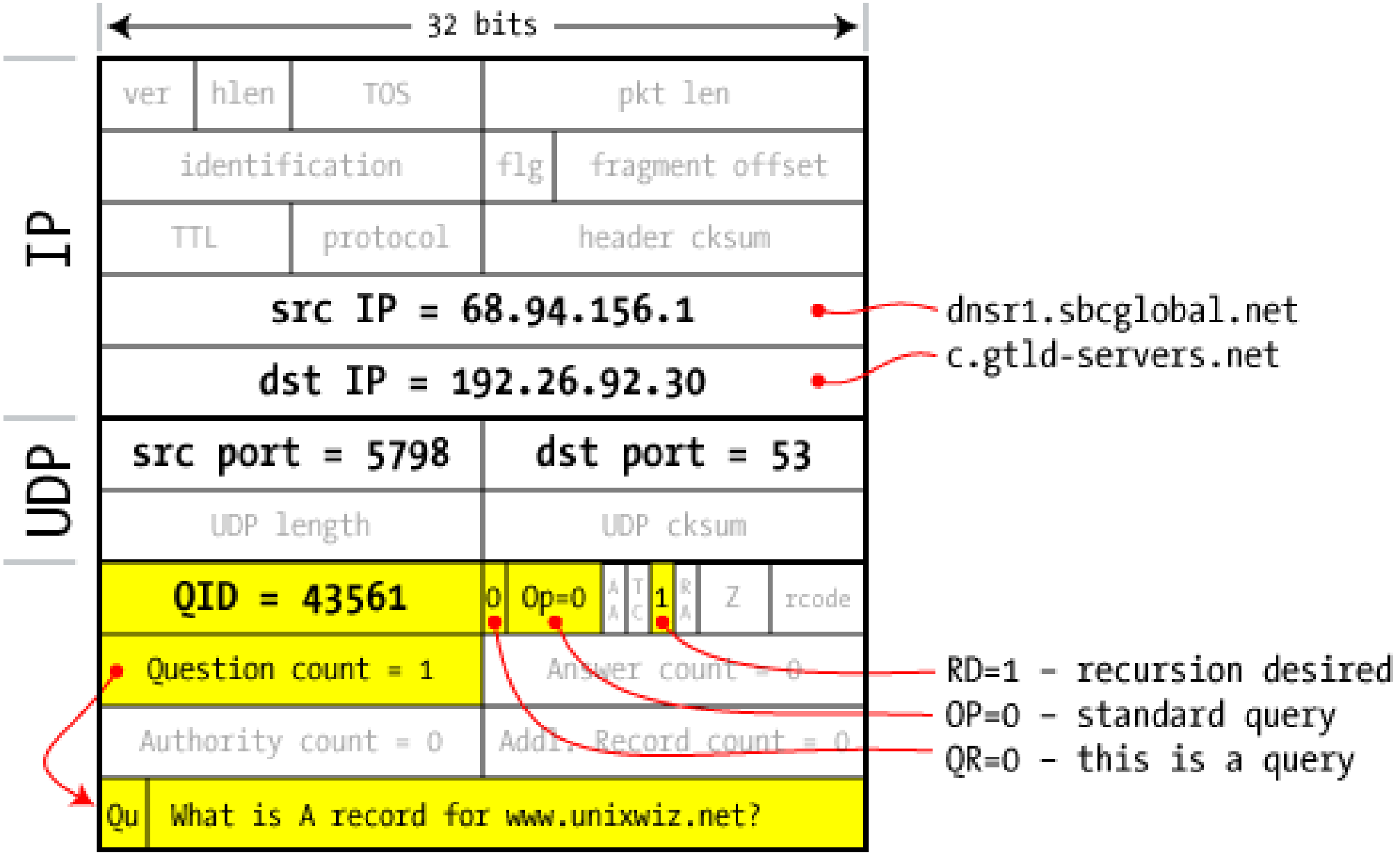
In Windows, the corresponding command is `nslookup`.

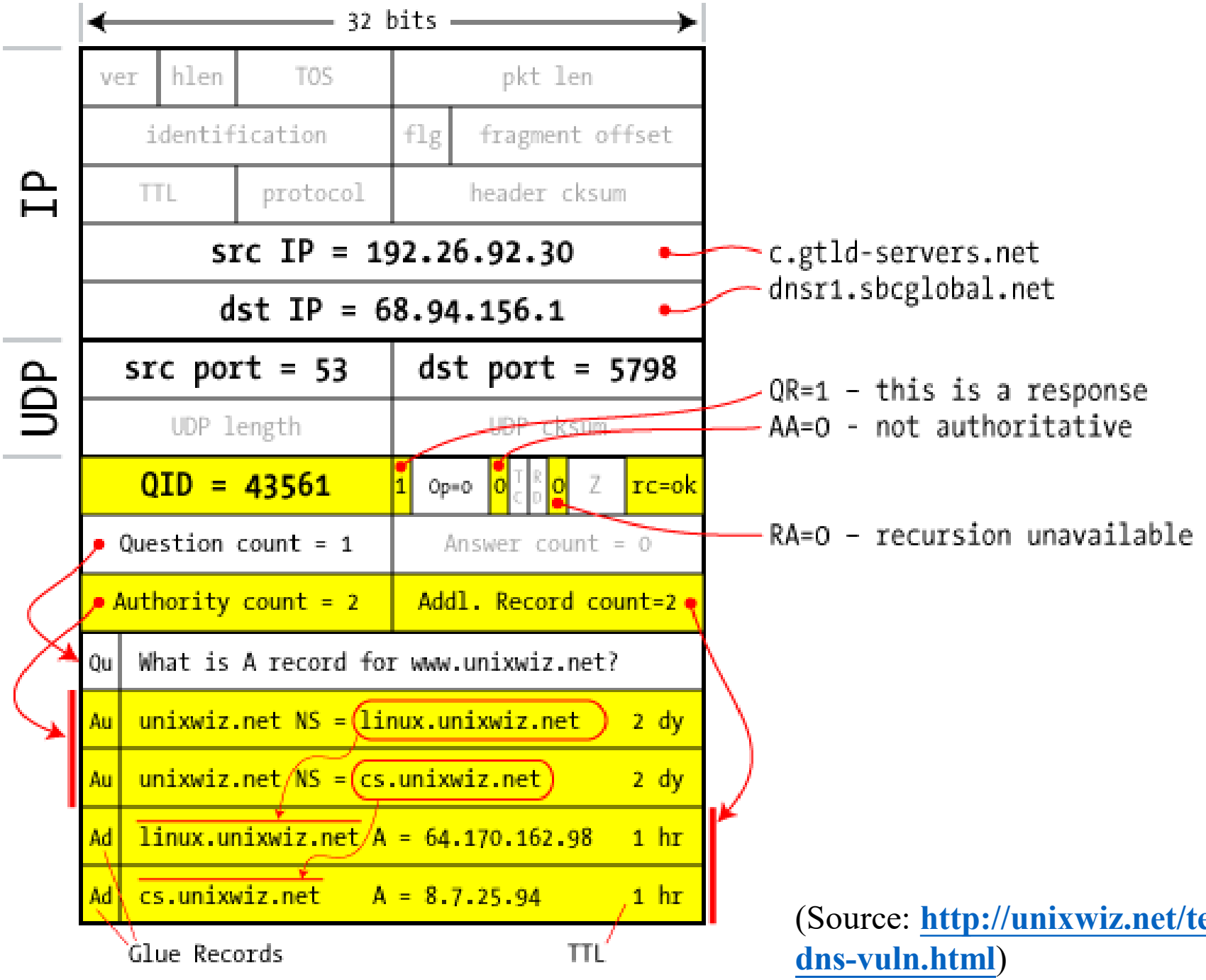
DNS Packet on the wire



Query ID is a 16 bit value that is used to link response to query.

Example query and answer packets





(Source: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html)

- DNS Caching
  - DNS responses are cached - quick response for repeated translations
  - Cached data periodically times out - Lifetime (TTL) of data controlled by owner of data

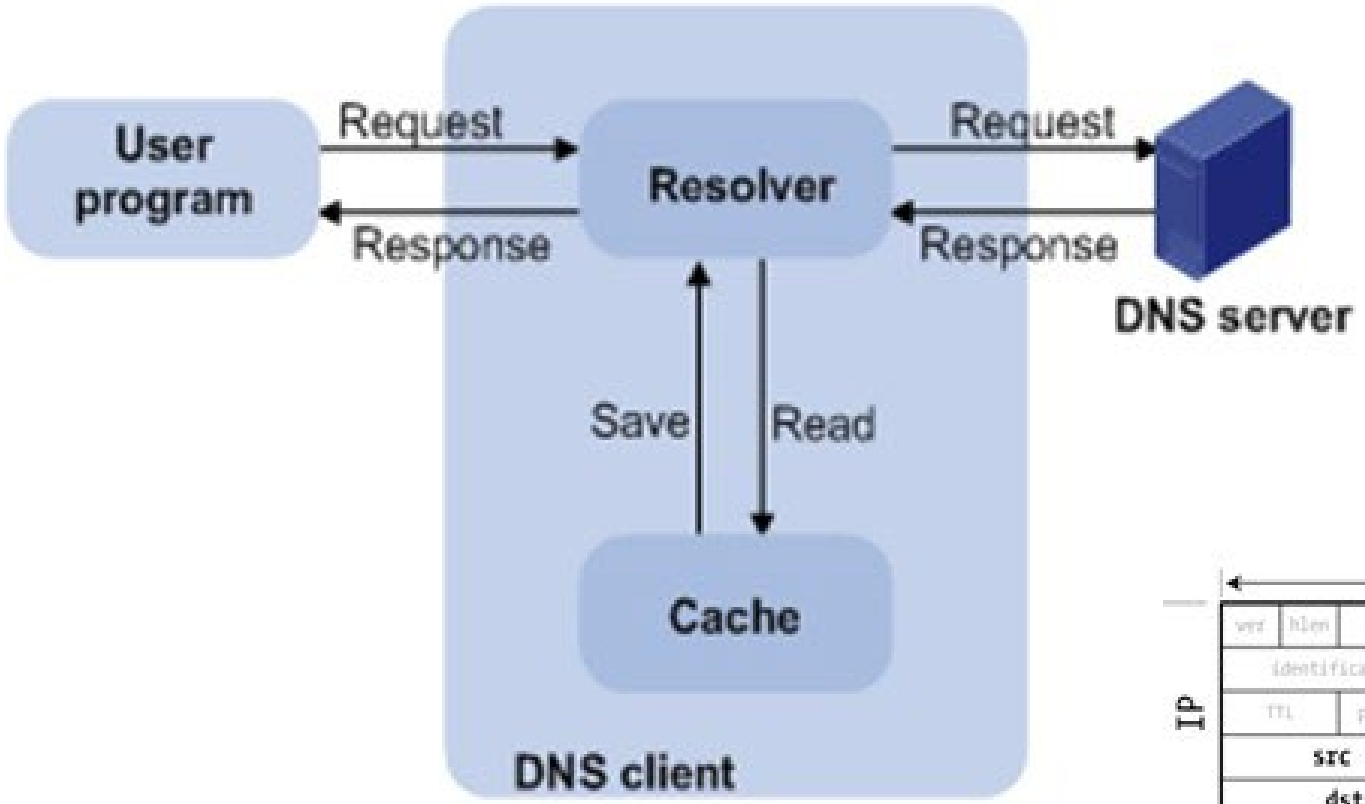
- Class demonstration on DNS Caching

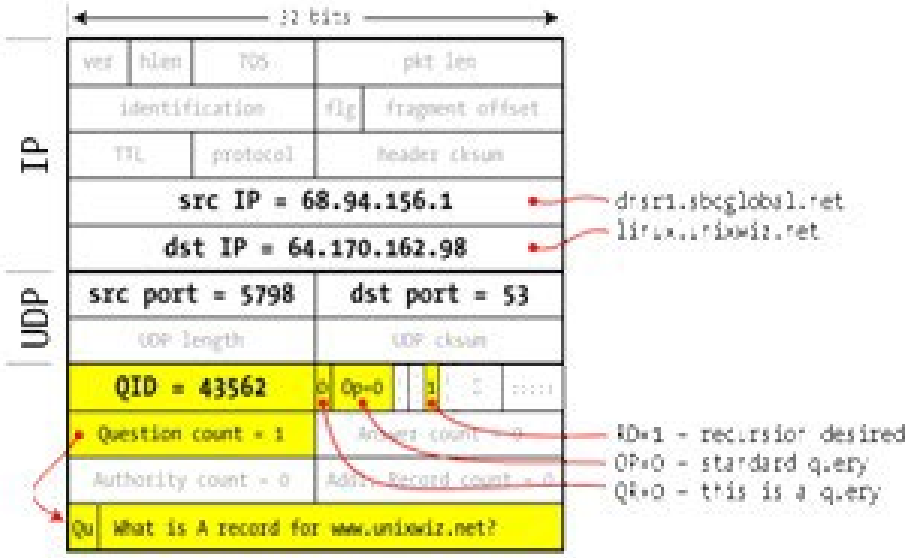
1) Create a A record of a domain in DNS server.
2) Use some commands such as ping, dig, host to find the IP address of that domain.
3) Go to the DNS server to change the A record.
4) Use some commands to find the IP address of that domain. Does the IP update?

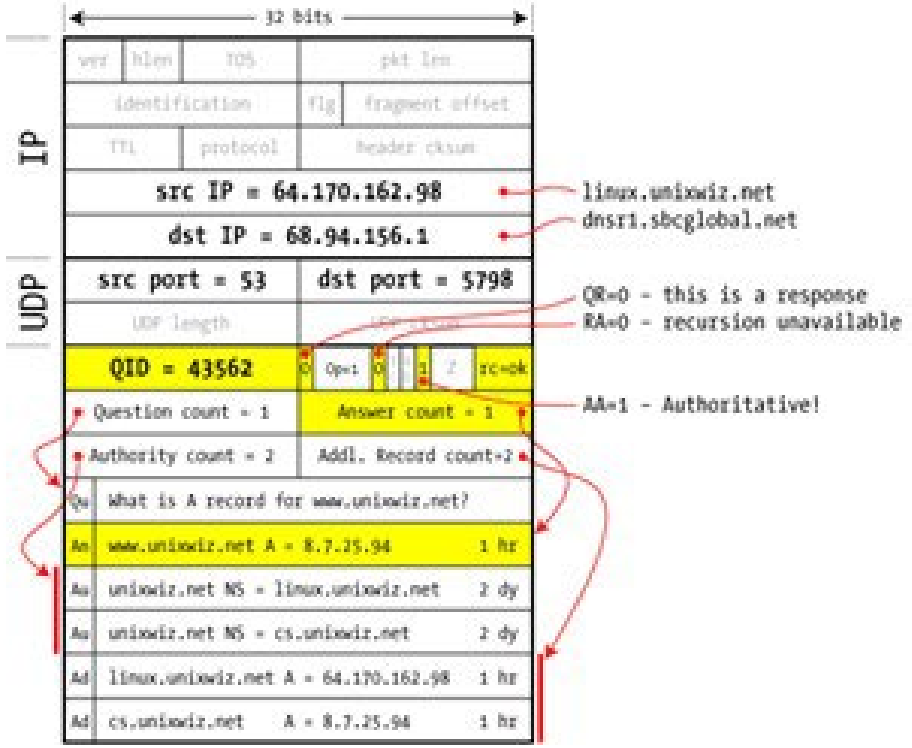
Security Problems in DNS

- Users/hosts trust the host-address mapping provided by DNS.

- **Reasons why DNS is insecure**
  Packets over UDP (less than 512 bytes)
  Only 16-bit Query ID and UDP source port form the security door
  Resolver accepts packet if above two match
  Resolver never asks packet from whom or was it manipulated

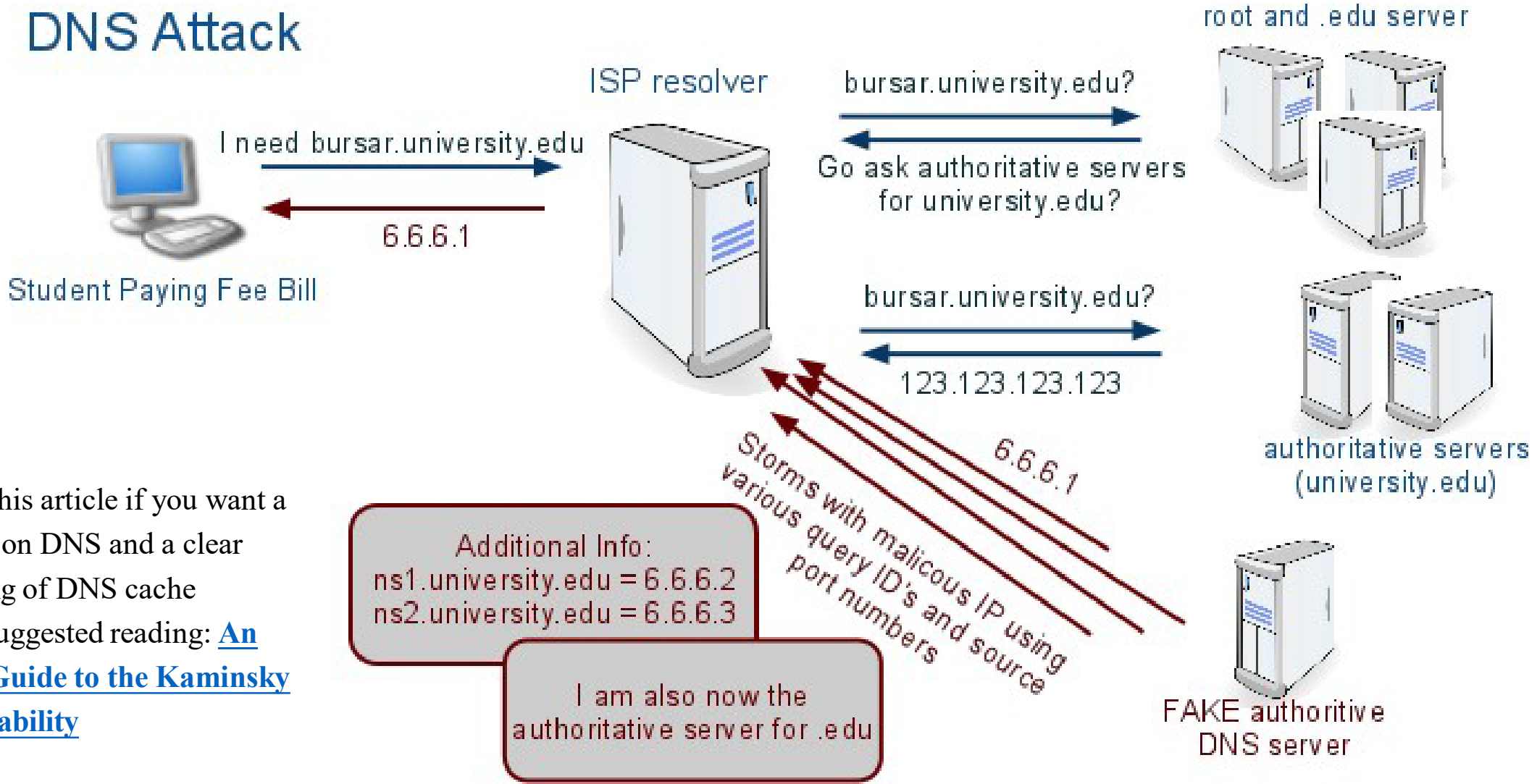

User program
Request
Response
Resolver
Request
Response
DNS server
Save
Read
Cache
DNS client


32 bits
IP
UDP
src IP = 68.94.156.1
dst IP = 64.170.162.98
src port = 5798
dst port = 53
QID = 43562
Question count = 1
Authority count = 0
Qu What is A record for www.unixwiz.net?
RD=1 - recursion desired
OP=0 - standard query
QR=0 - this is a query


32 bits
IP
UDP
src IP = 64.170.162.98
dst IP = 68.94.156.1
src port = 53
dst port = 5798
QID = 43562
Question count = 1
Answer count = 1
Authority count = 2
Addl. Record count=2
Qu What is A record for www.unixwiz.net?
An www.unixwiz.net A = 8.7.25.94 1 hr
Au unixwiz.net NS = linux.unixwiz.net 2 dy
Au unixwiz.net NS = cs.unixwiz.net 2 dy
Ad linux.unixwiz.net A = 64.170.162.98 1 hr
Ad cs.unixwiz.net A = 8.7.25.94 1 hr
linux.unixwiz.net
dnsri.sbcglobal.net
QR=0 - this is a response
RA=0 - recursion unavailable
AA=1 - Authoritative!

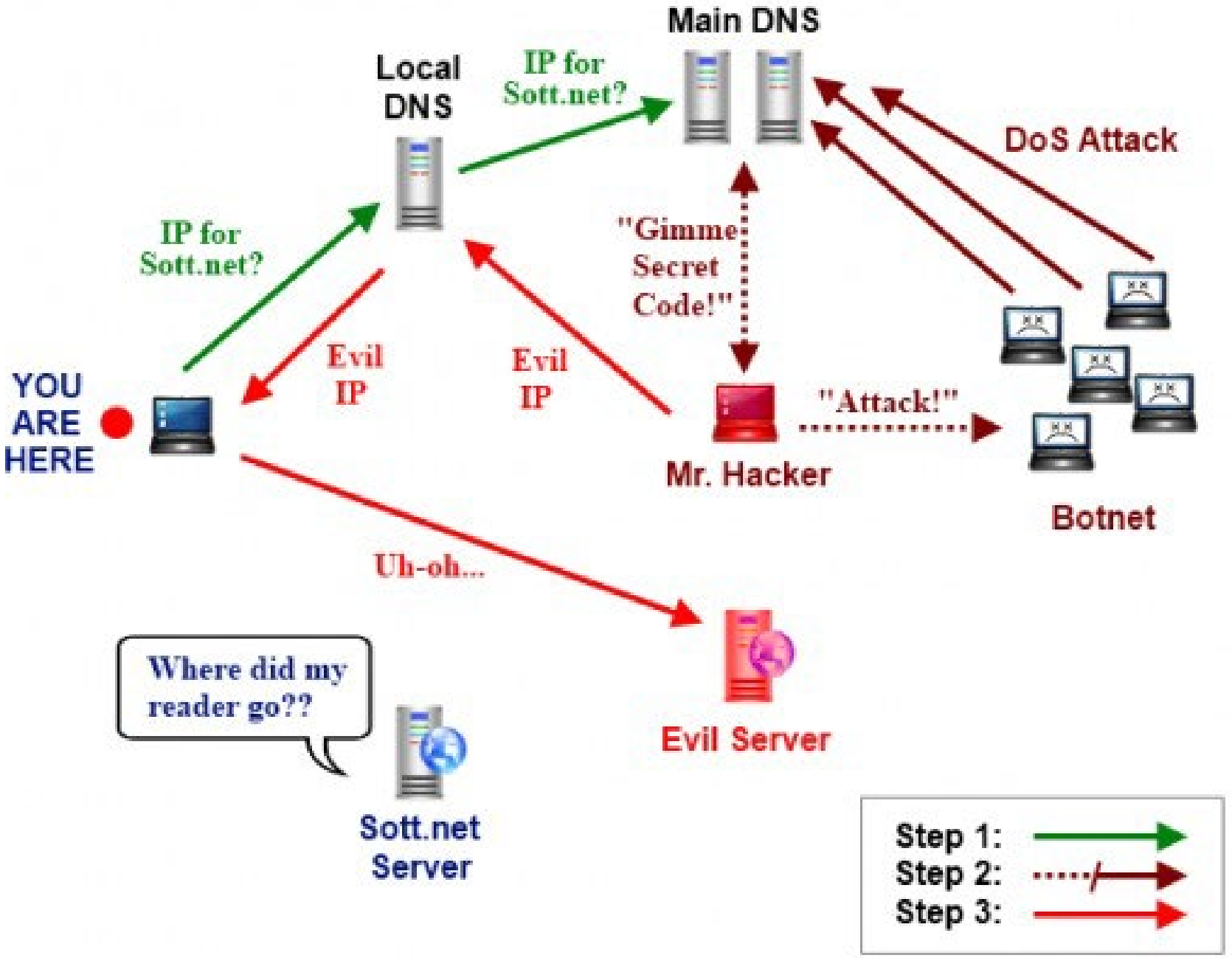
DNS Cache Posioning Attack

DNS cache poisoning, also known as DNS spoofing, is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones.



Please read this article if you want a good review on DNS and a clear understanding of DNS cache posioning. Suggested reading: **An Illustrated Guide to the Kaminsky DNS Vulnerability**

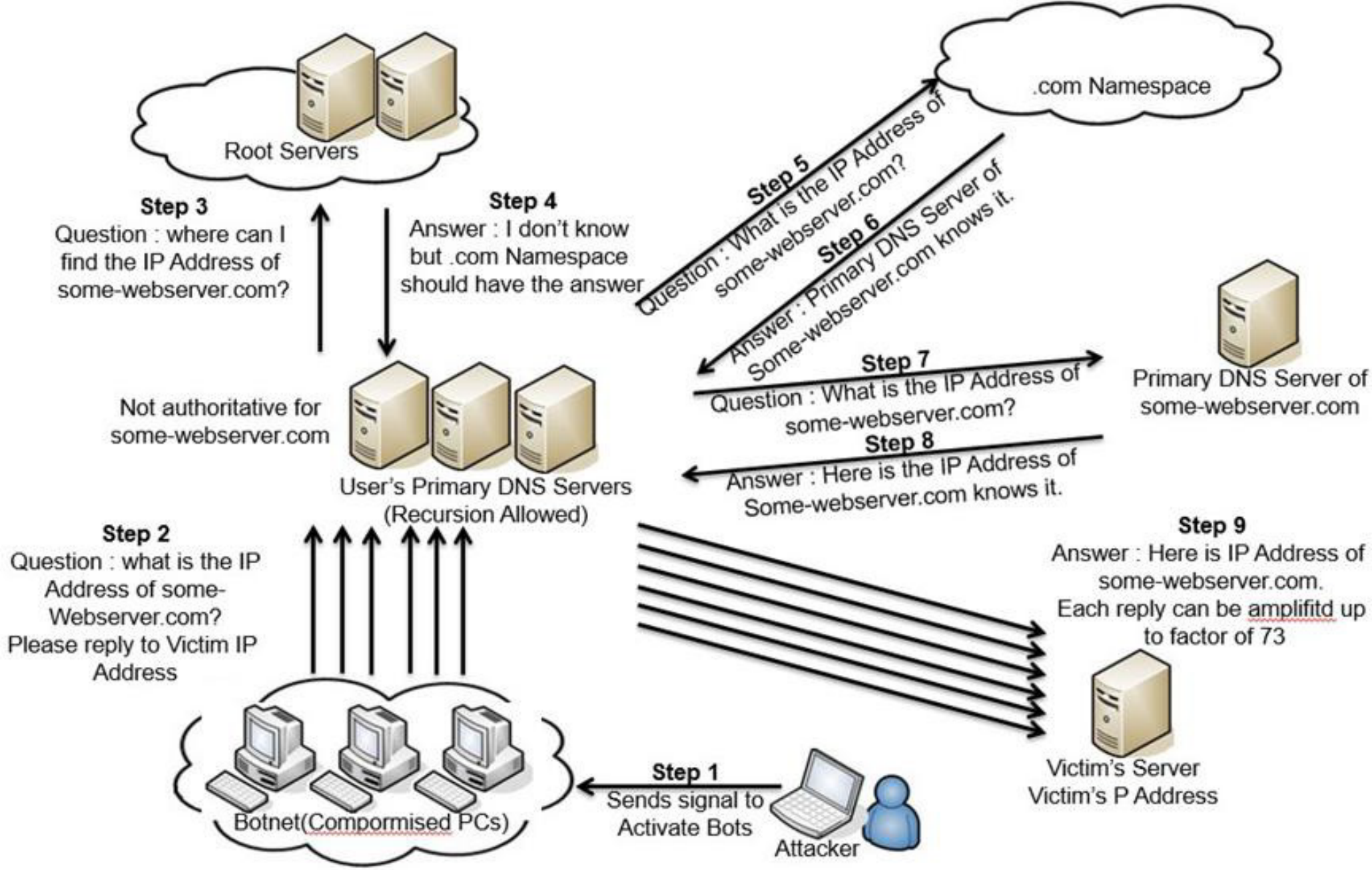
DNS poisoning attacks example:



DNS Amplification Attack

DNS amplification is a Distributed Denial of Service (DDoS) attack in which the attacker exploits vulnerabilities in domain name system (DNS) servers to turn initially small queries into much larger payloads, which are used to bring down the victim's servers.

During a DNS amplification attack, the perpetrator sends out a DNS query with a forged IP address (the victim's) to an open DNS resolver, prompting it to reply back to that address with a DNS response. With numerous fake queries being sent out, and with several DNS resolvers replying back simultaneously, the victim's network can easily be overwhelmed by the sheer number of DNS responses.



Why it is a type of amplification attacks?

Why it is a type of amplification attacks?

There are two senses of amplifications:
1) A small packet of query -> large packet of response
2) A single query -> responses from multiple DNS servers

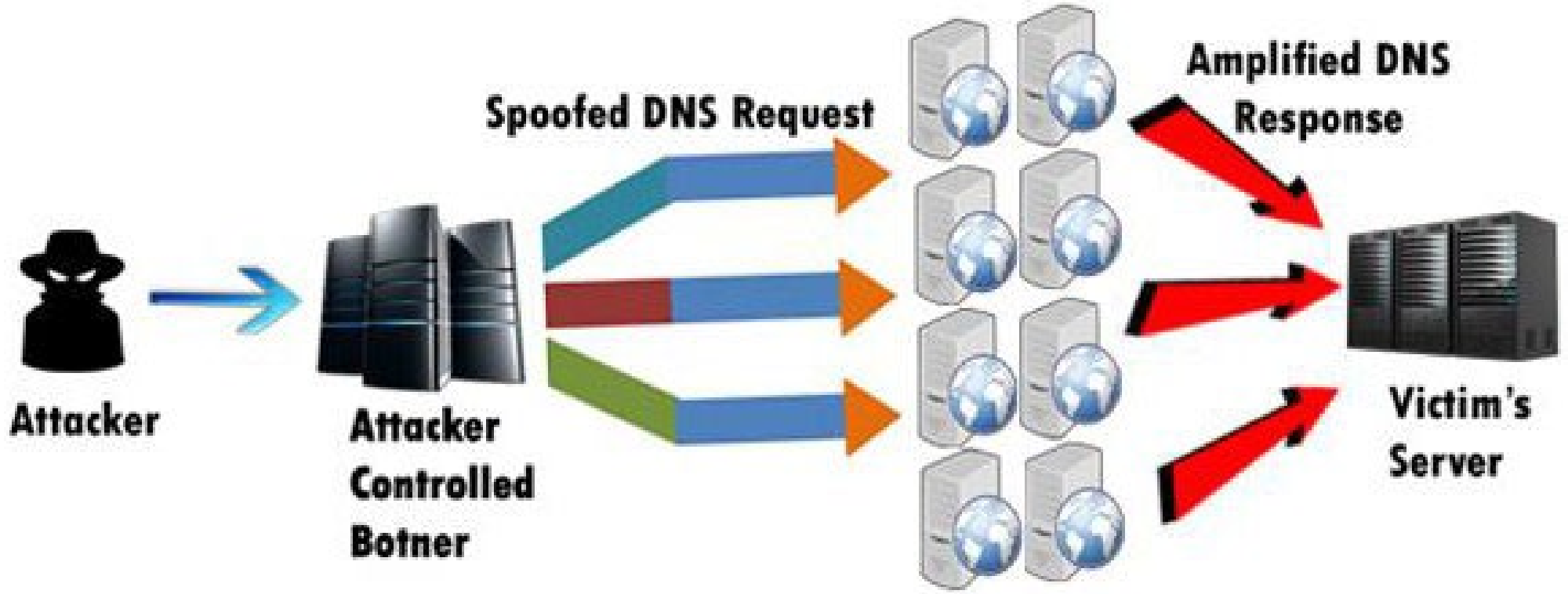
Video : **DNS Amplification Attack**

DNS Amplification Attack Tool: **Tsunami**
http://samiux.blogspot.hk/2014/07/tsunami-dns-amplification-attack-tool.html

To perform DNS Amplification attack :
python amplfiy.py -t 1.2.3.4 -s open_dns.txt -a domain_name.txt -c -1 --verify -v --threads=1000
(where 1.2.3.4 is the victim's IP address)

Open recursive DNS resolver test: **http://openresolver.com/**

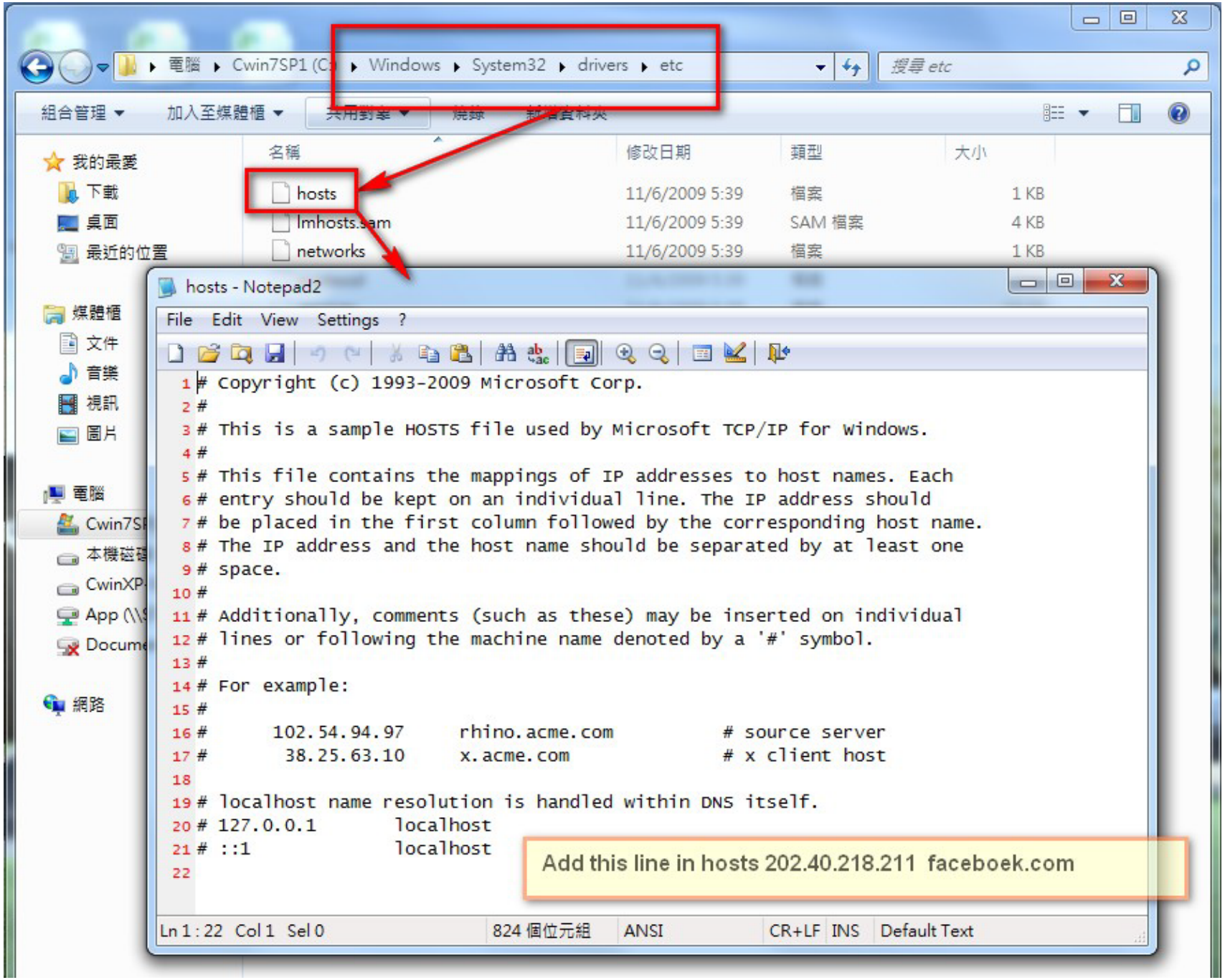
Summary: A DNS amplification attack exploits open DNS resolvers by performing a spoofed query of all record types for a given domain. The effectiveness of this attack can be increased by employing a DDoS component as well by sending requests to multiple open resolvers simultaneously.



DNS Spoofing with the Hosts file and in LAN

- A simple method of DNS spoofing is updating `hosts` file.

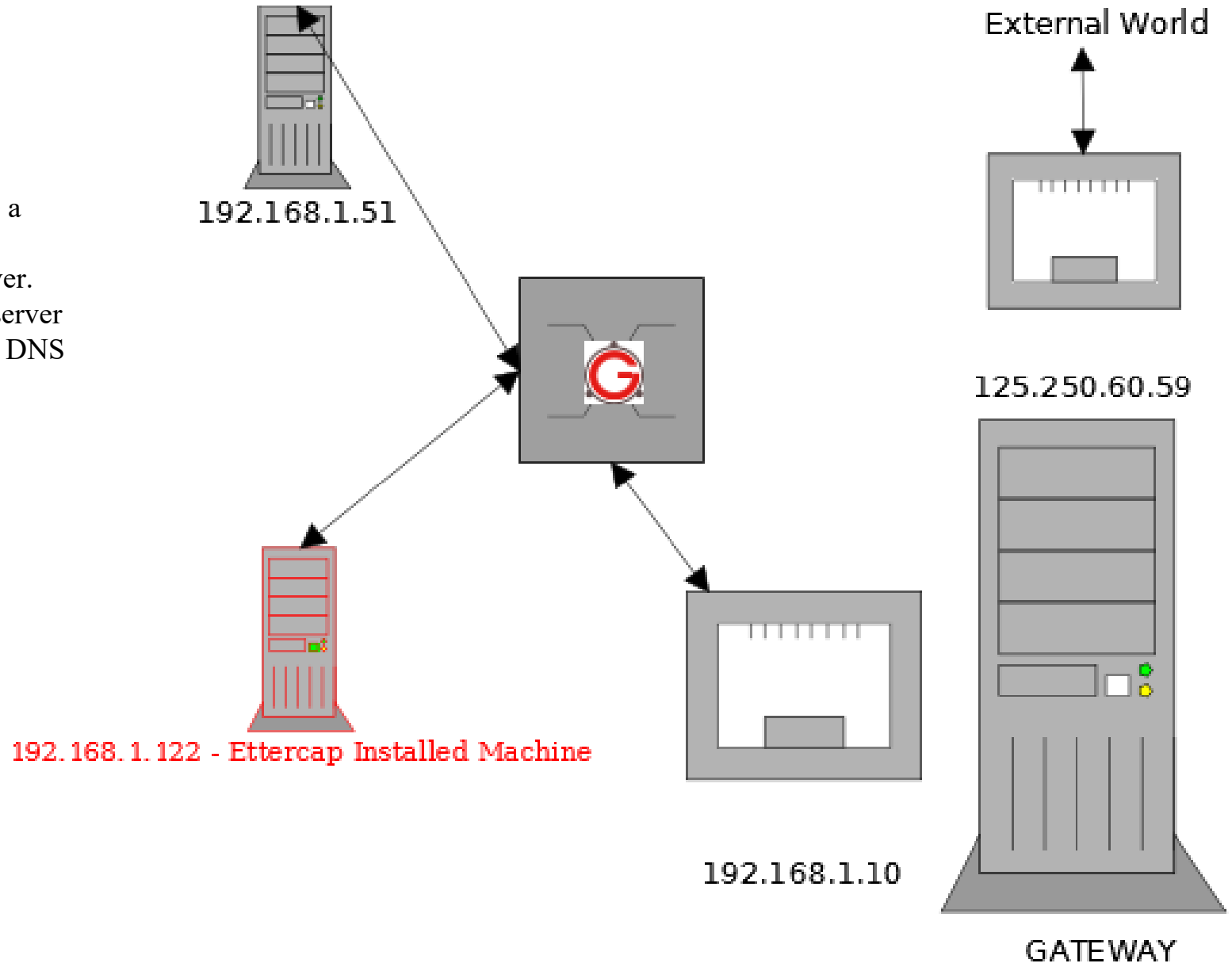
  A hosts file is an important system file which will store the information about where to find or locate a particular PC on a network.In Other words it maps the Domain or host names to the IP addresses. So we can consider the hosts file as a local system version of the DNS.


電腦 ▸ Cwin7SP1 (C:) ▸ Windows ▸ System32 ▸ drivers ▸ etc
搜尋 etc
組合管理
加入至媒體櫃
共用對象
燒錄
新增資料夾
我的最愛
下載
桌面
最近的位置
媒體櫃
文件
音樂
視訊
圖片
電腦
網路
名稱
修改日期
類型
大小
hosts
11/6/2009 5:39
檔案
1 KB
lmhosts.sam
11/6/2009 5:39
SAM 檔案
4 KB
networks
11/6/2009 5:39
檔案
1 KB
hosts - Notepad2
File Edit View Settings ?
Copyright (c) 1993-2009 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97   rhino.acme.com   # source server
38.25.63.10   x.acme.com   # x client host
localhost name resolution is handled within DNS itself.
127.0.0.1   localhost
::1   localhost
Add this line in hosts 202.40.218.211 faceboek.com
Ln 1 : 22 Col 1 Sel 0
824 個位元組
ANSI
CR+LF
INS
Default Text

- DNS Spoofing Attack in LAN with ARP poisoning
  Reference: **http://www.thegeekstuff.com/2012/05/ettercap-tutorial/**

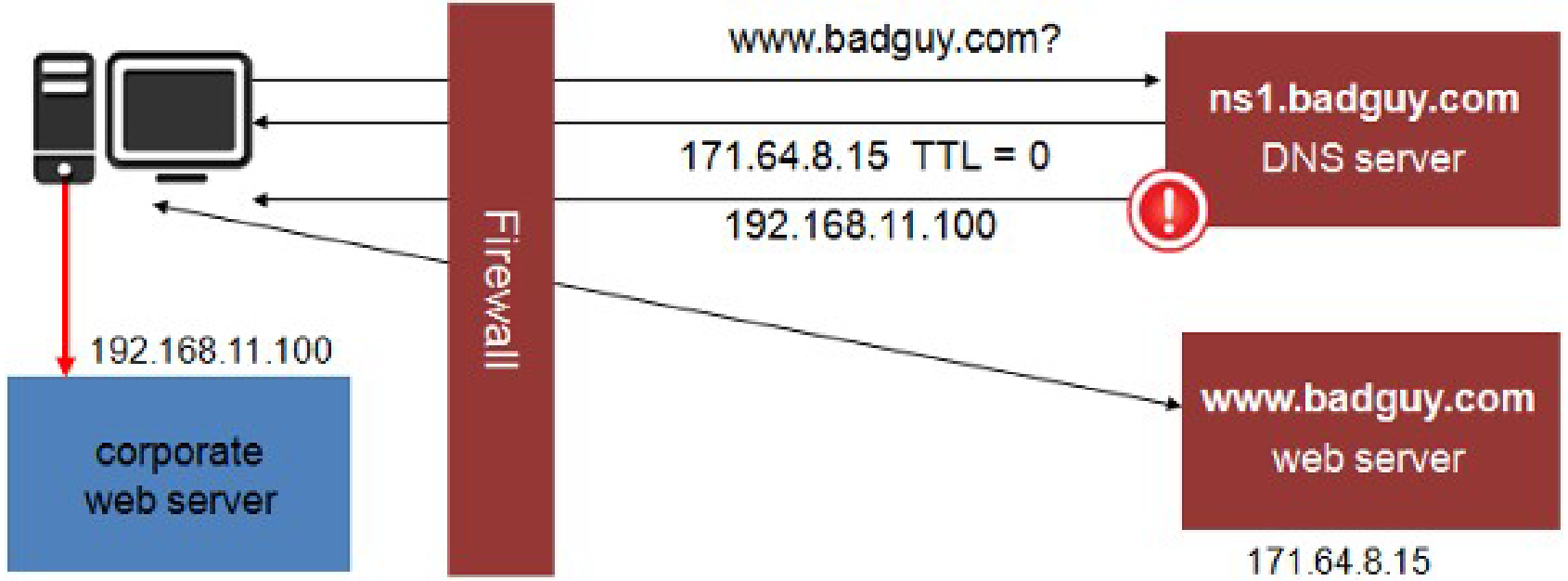
Two types of attack

1. DNS Spoofing
2. ARP Poisoning: Give a wrong (malicious) IP address for DNS Server.
3. The Malicious DNS server will reply 'malicious" DNS record



DNS Rebinding Attacks

- DNS rebinding attacks subvert the same-origin policy and convert browsers into open network proxies.



General scenario of DNS rebinding attack:

"To mount a DNS rebinding attack, the attacker need only register a domain name, such as attacker.com, and attract web traffic, for example by running an advertisement. In the basic DNS rebinding attack, the attacker answers DNS queries for attacker.com with the IP address of his or her own server with a short time-to-live (TTL) and serves visiting clients malicious JavaScript. To circumvent a firewall, when the script issues a second request to attacker.com, the attacker rebinds the host name to the IP address of a target server that is inaccessible from the public Internet. The browser believes the two servers belong to the same origin because they share a host name, and it allows the script to read back the response. The script can easily exfiltrate the response, enabling the attacker to read arbitrary documents from the internal server".

(Source: Protecting Browsers from DNS Rebinding Attacks - **https://crypto.stanford.edu/dns/dns-rebinding.pdf**)

Another scenario of DNS rebinding attack:

1) You connect to abcde.badsite.com, which resolves to IP 1.2.3.4 with a very short TTL
2) 1.2.3.4 delivers some Javascript code (malicious code) to your browser to execute in 15 seconds
3) The DNS server in control of *.badsite.com immediately points abcde.badsite.com to 10.0.0.1 (Internal Server)
4) 15 seconds later, the Javascript on your browser connects to abcde.badsite.com, in compliance with the same origin policy, and retrieves a web page from your internal server at 10.0.0.1
5) The DNS server resets abcde.badsite.com to 1.2.3.4 and after some period of time, your browser reconnects and sends 1.2.3.4 its findings

Yet another scenario of DNS rebinding attack (20 Apr 2015)
https://miki.it/blog/2015/4/20/the-power-of-dns-rebinding-stealing-wifi-passwords-with-a-website/

How your ethereum can be stolen through DNS rebinding (19 Jan 2018)
https://blog.hacker.af/how-your-ethereum-can-be-stolen-using-dns-rebinding

Solution for solving DNS attack:

1. Audit the DNS zone
2. Keep the DNS server up-to-date
3. Hide BIND version
4. Restrict Zone transfer
5. DNSSEC (DNS security extension)

Readings and References

Denial Of Service Methods : ICMP, SYN, teardrop, botnets

ICMP IP Tunnel: ICMPTunnel

An Illustrated Guide to the Kaminsky DNS Vulnerability - by Steve Friedl.

DDoS Attack Types by Paul C Dwyer Security GRC & Cyber Crime Advisor - 7 min video

ARP Cache Poisoning Fundamentals Explained

DNS rebinding: how an attacker can use your web browser to bypass a firewall

ICMP Attacks - Infosec Institute

Kali - Scapy Basics - Youtube Video (7 min)

Attacking Private Networks from the Internet with DNS Rebinding

A Case Study: **http://security.tencent.com/index.php/blog/msg/98**