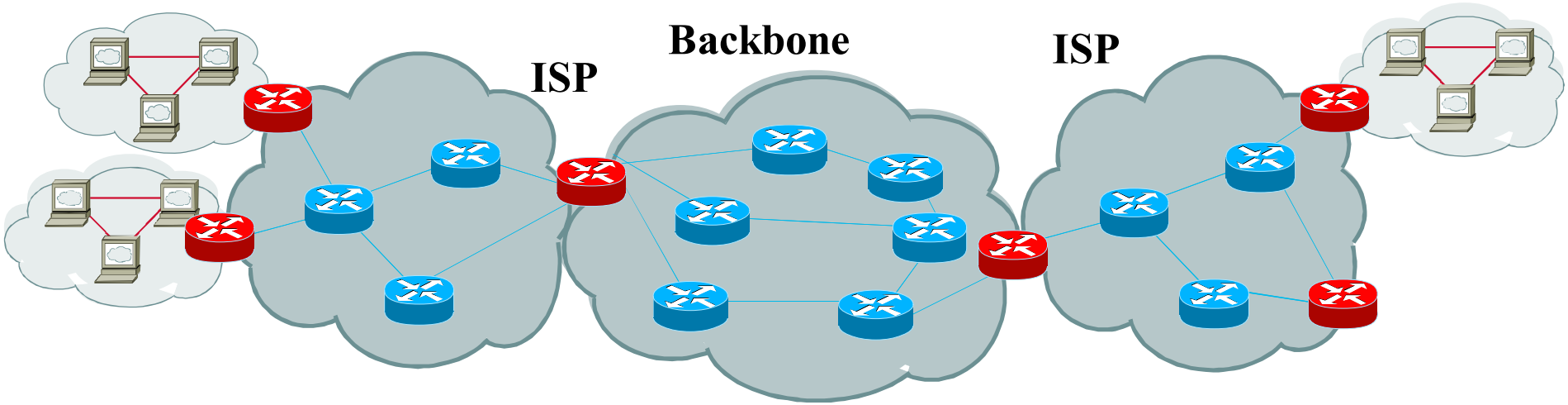
آسیب پذیری های شبکه
(Network Vulnerabilities)

رئوس مطالب

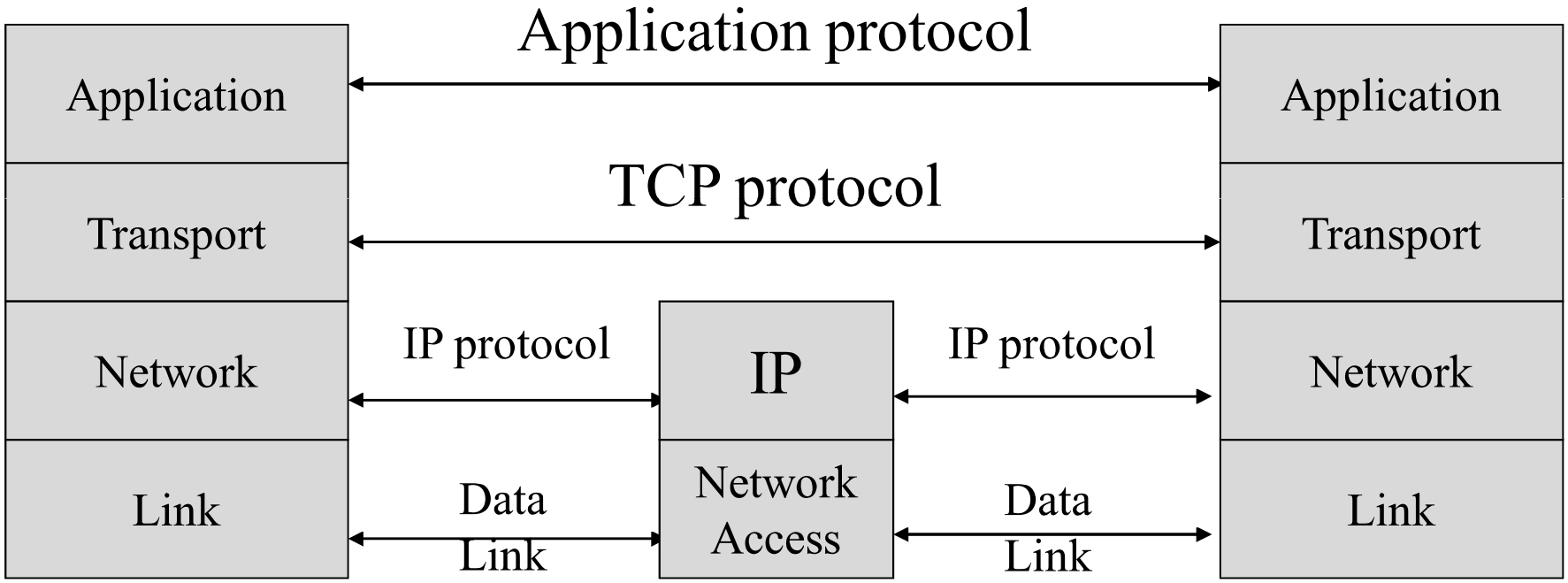
- اساس شبکه
  - نحوه کار اینترنت
  - مشکلات
- حملات شبکه
  - حملات مربوط به هاست
    - TCP Spoofing
  - حملات مربوط به زیرساخت شبکه
    - مسیریابی
    - Domain Name System (DNS)

زیرساخت اینترنت

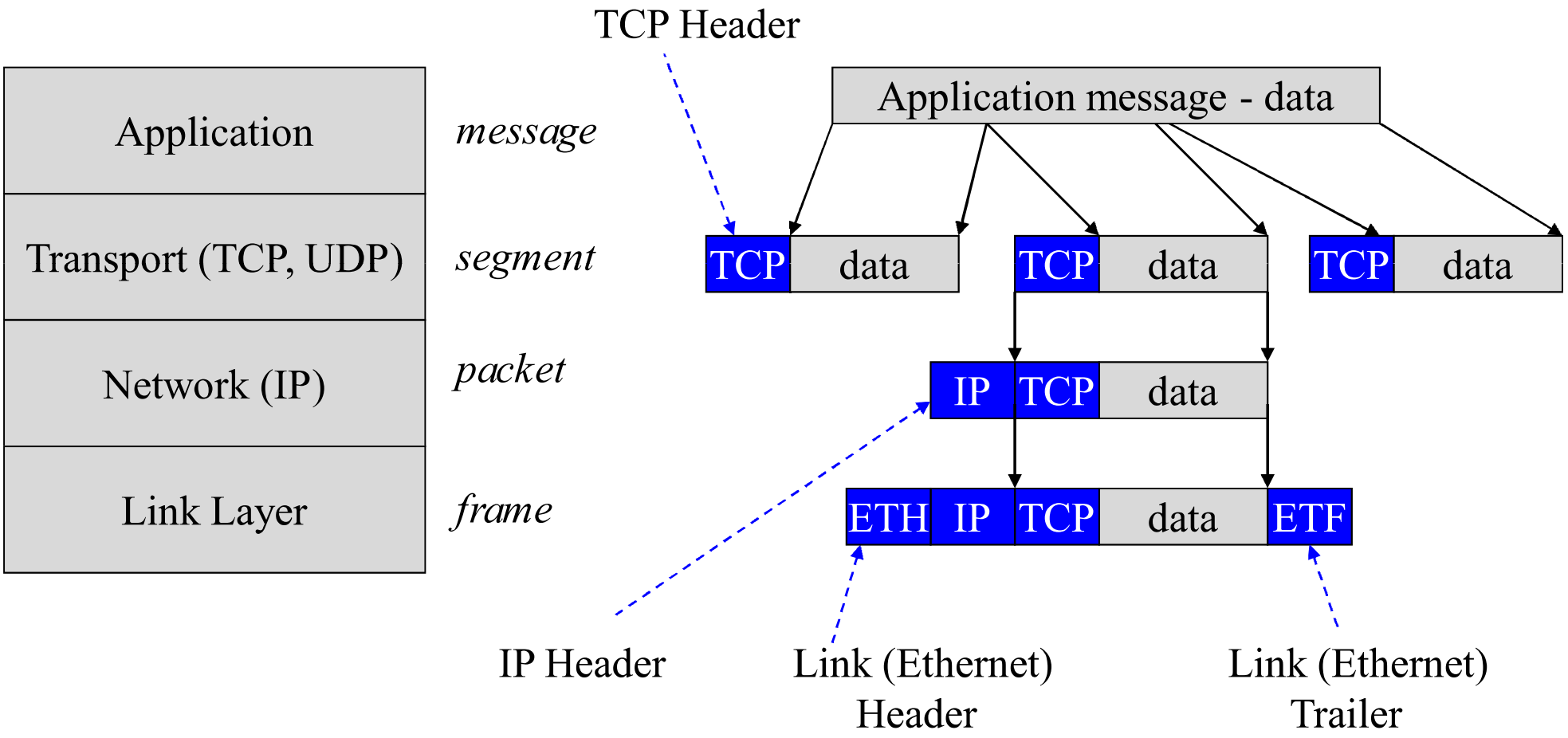
- مسیریابی
  - داخل ISP
  - بین ISPها
- DNS
  - پیدا کردن IP یک اسم (ece.sbu.ac.ir)



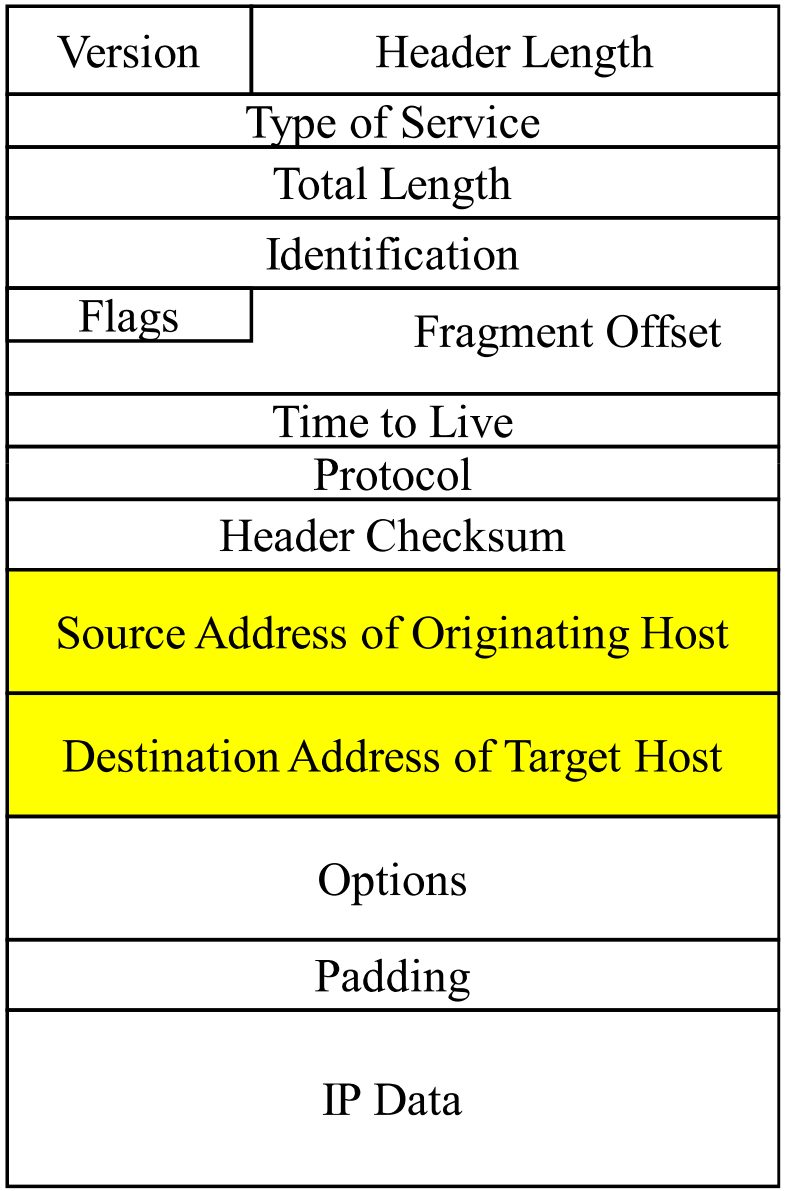
TCP/IP Protocol Stack



فرمت داده


Application
Transport (TCP, UDP)
Network (IP)
Link Layer
message
segment
packet
frame
TCP Header
Application message - data
TCP
data
TCP
data
TCP
data
IP
TCP
data
ETH
IP
TCP
data
ETF
IP Header
Link (Ethernet) Header
Link (Ethernet) Trailer

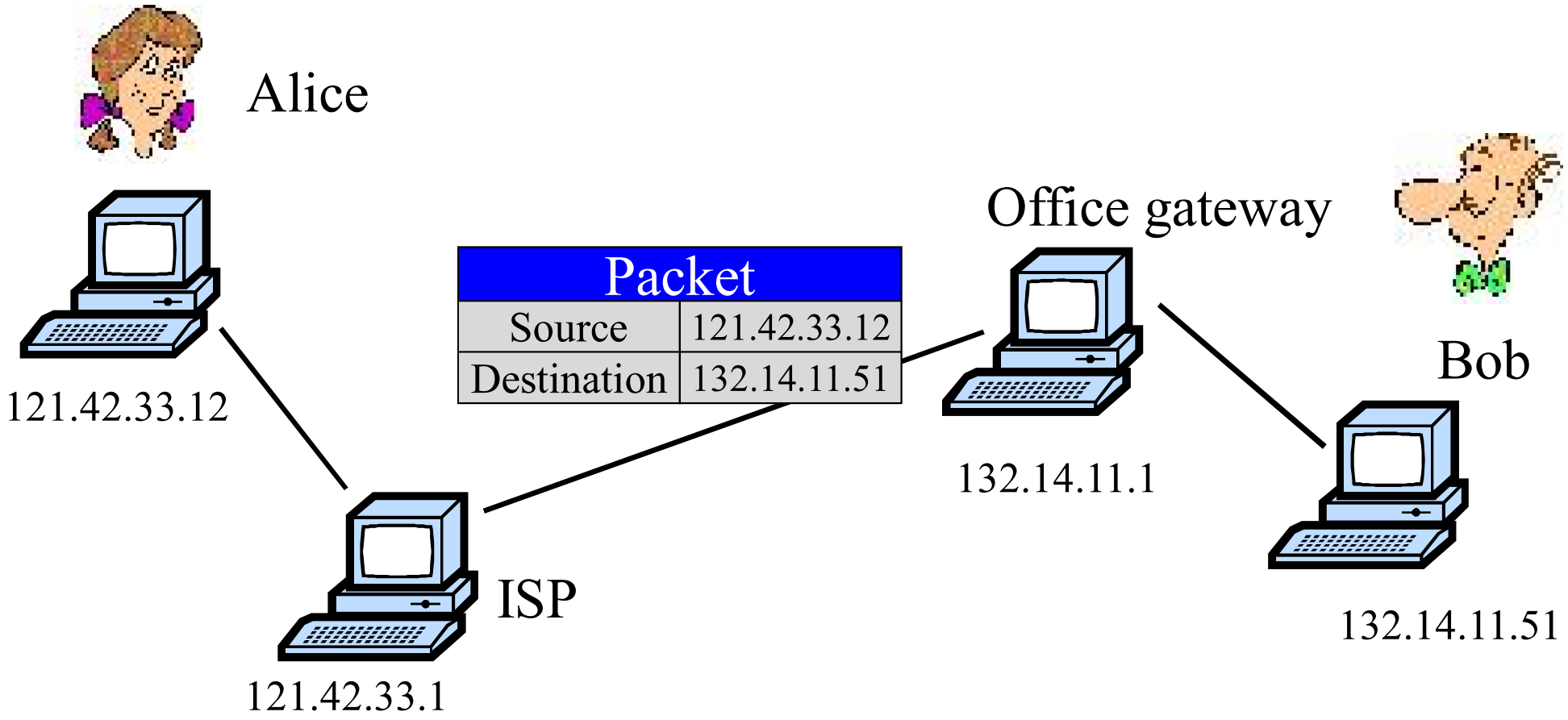
Internet Protocol (IP)



- Connection-less
  - غیر قابل اطمینان (Unreliable)
  - عدم تضمین در رساندن بسته به مقصد
  - حداکثر تلاش برای رساندن بسته به مقصد (Best Effort)
- پورت های مبدأ و مقصد در سربار IP وجود ندارند.

مسیریابی (Routing)

- مسیریابی از آدرس IP عددی استفاده می کند.
- معمولاً یک مسیر از چندین hop استفاده می کند.



کارکردهای پروتکل IP

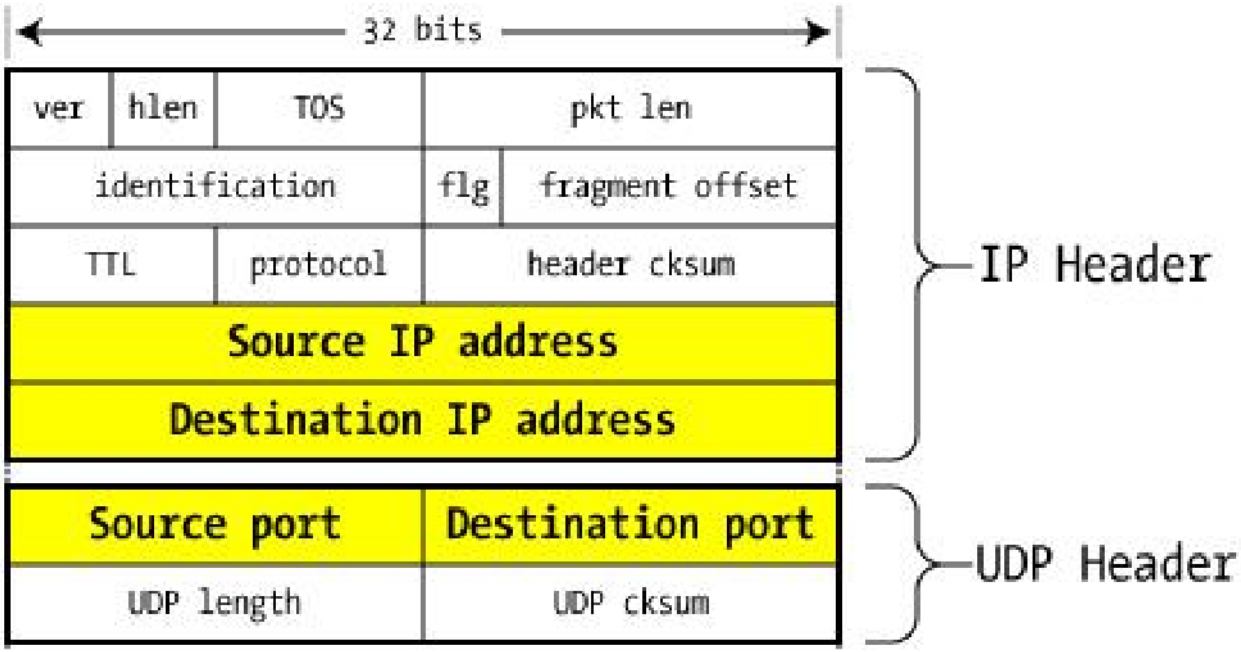
- مسیریابی
  - هاست ها آدرس درگاه (Gateway) را می دانند.
  - درگاه نحوه ارسال بسته ها به شبکه های دیگر را می داند.
- Fragmentation و Reassembly
  - داده کاربر از حداکثر اندازه مجاز بسته IP بزرگتر باشد.
- گزارش خطا
  - ارسال بسته ICMP در صورت دور انداخته شدن بسته در مقصد
- فیلد TTL
  - هر hop قبل از ارسال بسته، مقدار فیلد را یک واحد کاهش می دهد.
  - اگر مقدار فیلد صفر شود، بسته دور انداخته می شود.
    - جلوگیری از افتادن بسته در یک حلقه بی نهایت

مشکل: عدم تأیید هویت مبدأ

- فرض می شود که کلاینت IP مبدأ درست را قرار می دهد.
  - با از استفاده از raw socket می توان هر IP ای گذاشت.
  - Libnet: یک کتابخانه برای تولید بسته های دلخواه
- هر کسی می تواند بسته هایی با IP مبدأ دلخواه ارسال کند.
  - پاسخ به ماشینی که IP جعلی را در اختیار دارد، بر می گردد.
- کاربرد:
  - حملات DoS
    - عدم شناسایی هاست حمله کننده درست

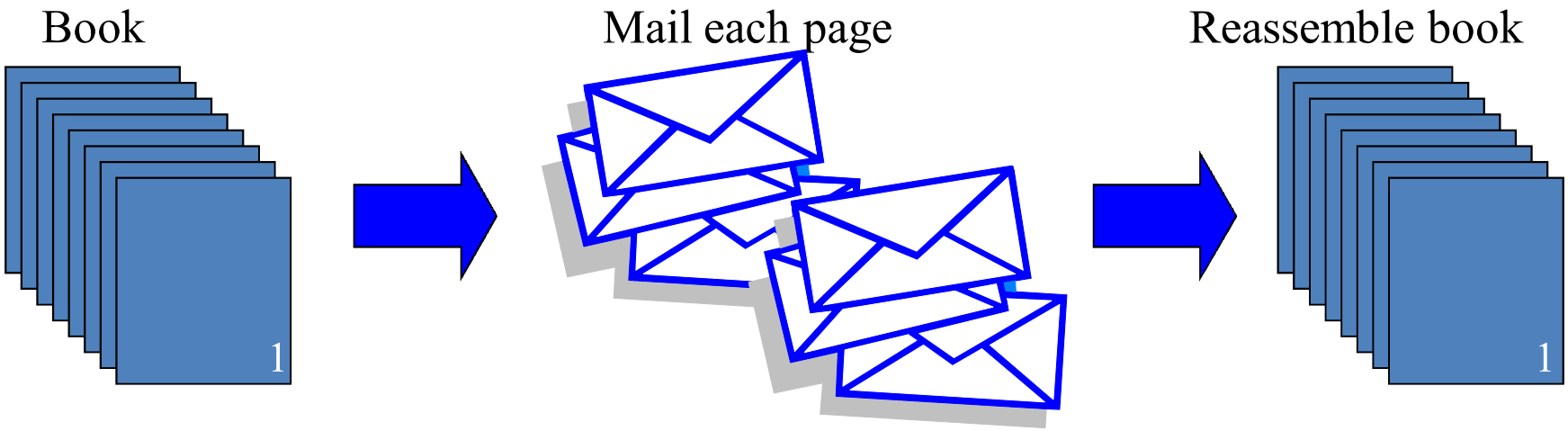
User Datagram Protocol (UDP)

- انتقال داده غیر قابل اطمینان
  - از IP استفاده می کند.
  - عدم ارسال Acknowledgement
  - عدم کنترل Congestion

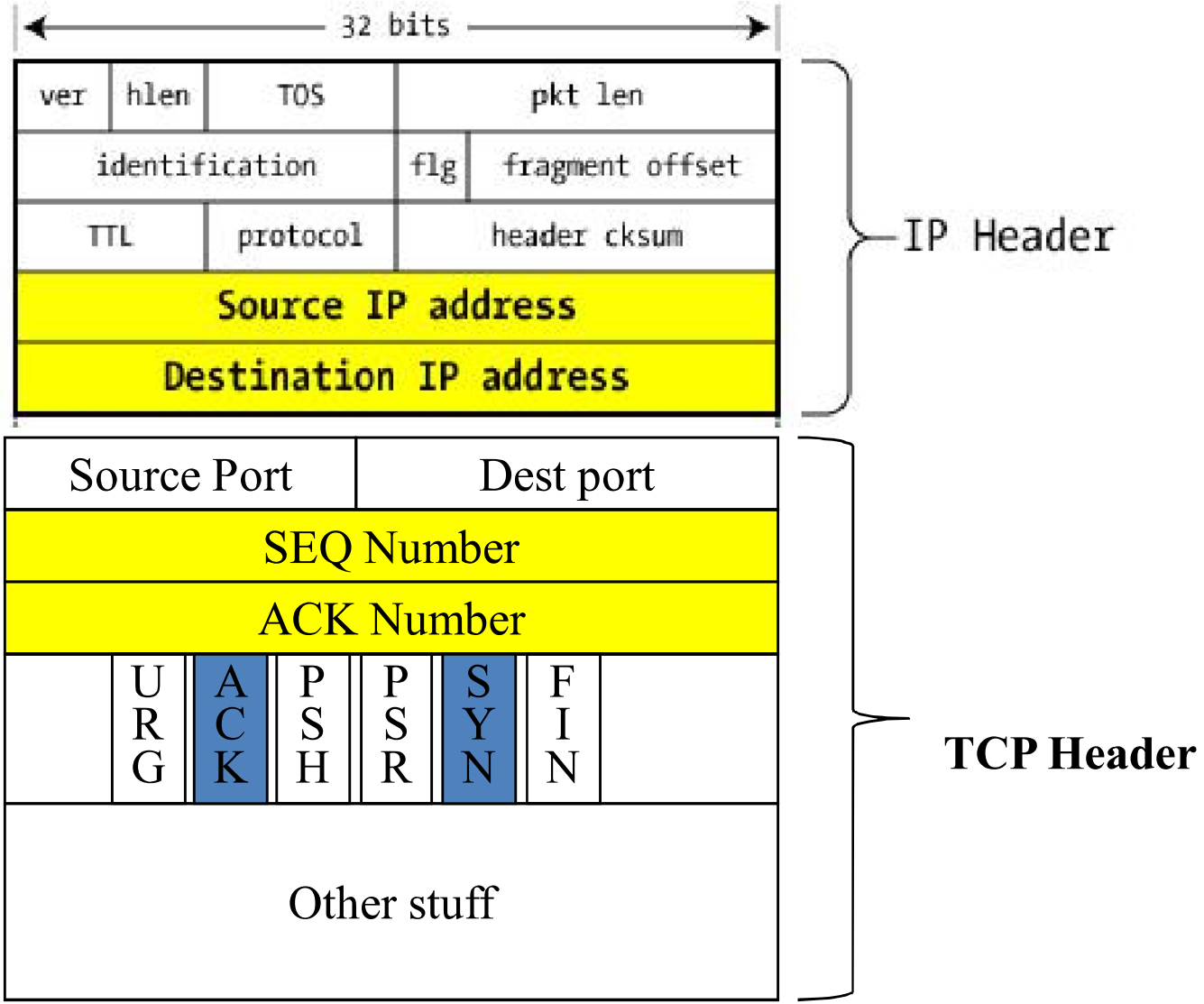


Transmission Control Protocol (TCP)

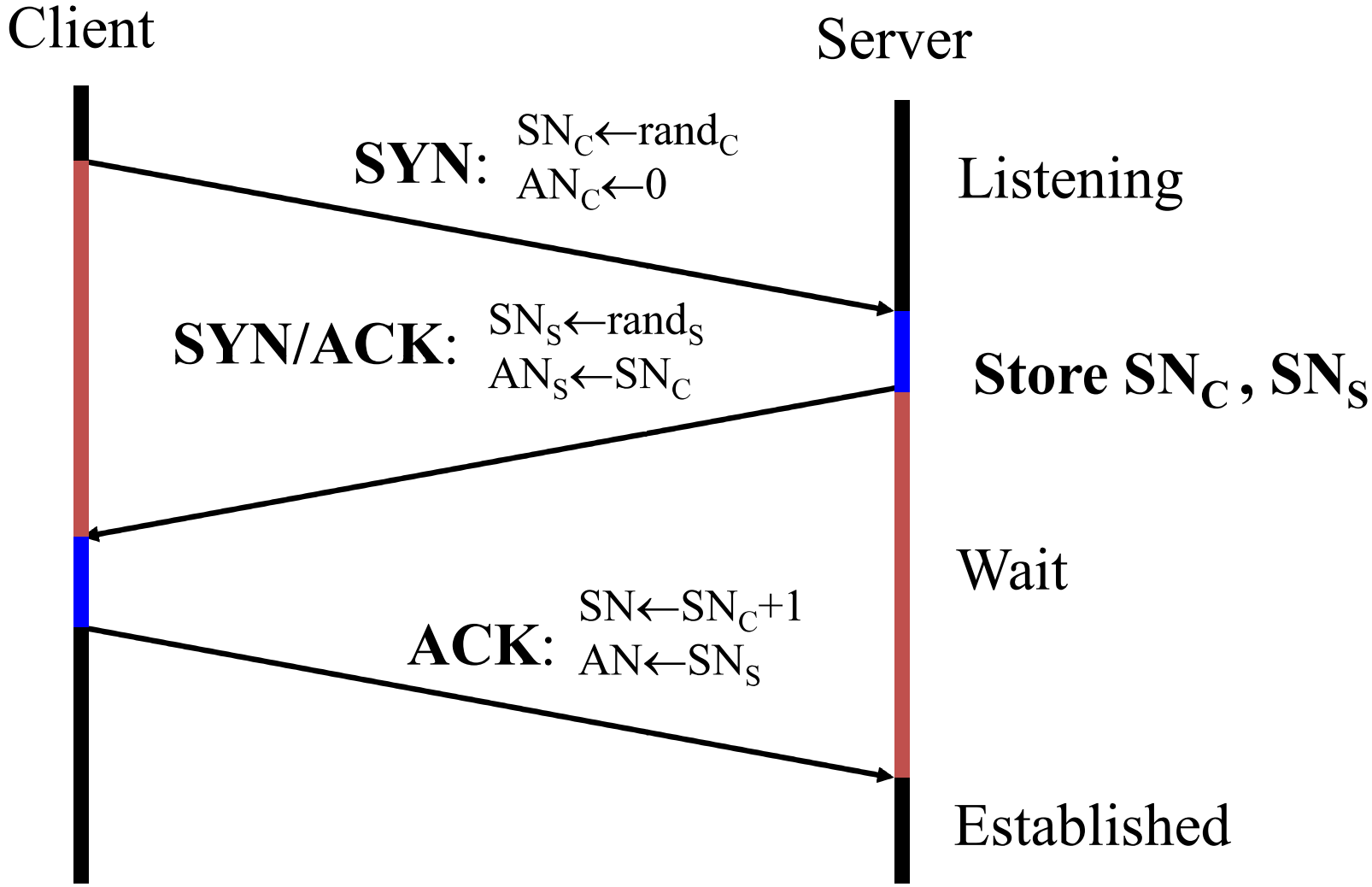
- Connection-oriented: ترتیب بسته ها رعایت می شود.
  - فرستنده:
    - داده را به بسته هایی می شکند و به هر بسته یک عدد اختصاص می دهد.
  - گیرنده:
    - ack بسته ها را می فرستد. (بسته های گم شده دوباره ارسال می شوند)
    - ترتیب بسته ها درست می کند و داده را به کاربر می فرستد.



TCP Header


32 bits
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
Source IP address
Destination IP address
IP Header
Source Port
Dest port
SEQ Number
ACK Number
URG
ACK
PSH
PSR
SYN
FIN
Other stuff
TCP Header

TCP Handshake

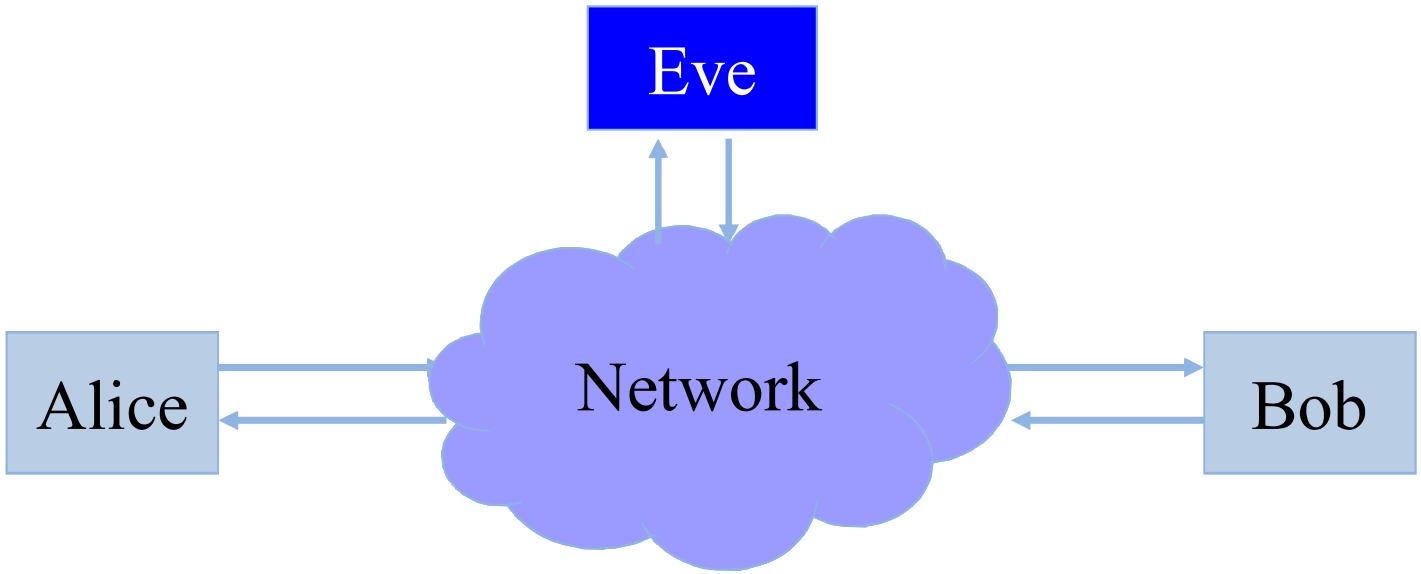


مشکلات امنیتی

- بسته ها از درون هاست های غیر قابل اعتماد عبور می کنند.
  - استراق سمع (Eavesdropping)
  - Packet Sniffing
- جعل هویت
  - Arp Spoofing
- حالت TCP به راحتی قابل حدس زدن است.
  - Spoofing
  - Session Hijacking
- حملات Denial of Server (DoS)

Packet Sniffing

- کارت شبکه در مد Promiscuous تمام بسته ها را می خواند
  - تمام اطلاعات رمز نشده قابل خواندن هستند (wireshark)
  - پروتکل های ftp و telnet پسوردها را رمز نشده می فرستند.
- رمزنگاری یکی از راه های مؤثر برای جلوگیری از sniffing

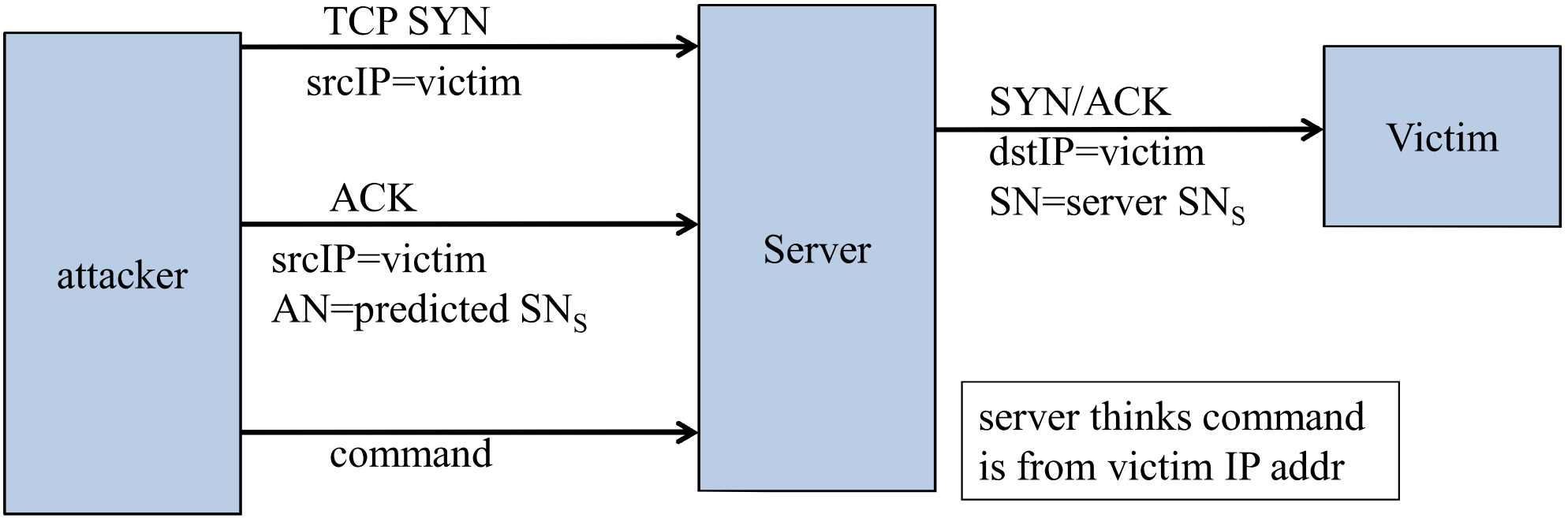


ARP Spoofing

- پروتکل ARP برای پیدا کردن آدرس Ethernet یک آدرس IP استفاده می شود.
- ماشین حمله کننده می تواند به درخواست های ARP پاسخ دهد و بسته های ماشین قربانی را به سمت خود منحرف کند.
- پیشگیری
  - مطابقت دادن درخواست ها و پاسخ های ARP

TCP Connection Spoofing

- اگر شمارنده توالی اولیه قابل پیشبینی باشد:
  - مهاجم می تواند IP مبدأ جعل کرده و به سرور دستور بفرستد.
    - دور زدن تأیید هویت مبتنی بر IP



حدس زدن ISN

- X برای یاد گرفتن ISN_S یک اتصال برقرار می کند:

$$X \to S: \quad SYN(ISN_X)$$

$$S \to X: \quad SYN(ISN_S), ACK(ISN_X)$$

- سپس X هویت T را جعل می کند:

$$X \to S: \quad SYN(ISN_X), SRC = T$$

$$S \to T: \quad SYN(ISN_S + k), ACK(ISN_X)$$

$$X \to S: \quad ACK(ISN_S + k), SRC = T$$

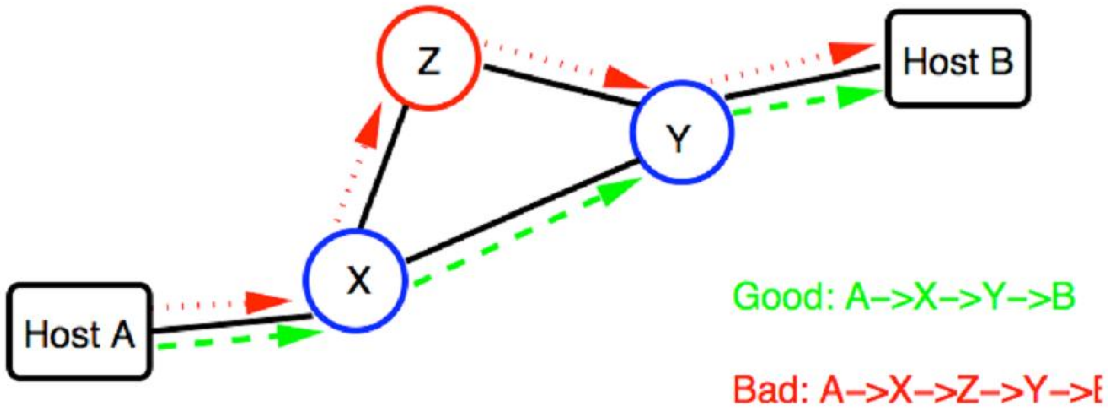
$$X \to S: \quad ACK(ISN_S + k), SRC = T, nasty\ data$$

پیشگیری

- N بار افزایش ISN به اندازه یک واحد در هر ثانیه
- افزایش تصادفی ISN بعد از هر اتصال
- ایجاد ISN تصادفی بعد از هر اتصال
- استفاده از تابع در همسازی (Hash) برای تولید ISN برای هر اتصال به صورت جداگانه
  - <IP مبدأ، پورت مبدأ، IP مقصد، پورت مقصد>
- استفاده از تابع رمزنگاری برای رمز کردن شمارنده ISN و ارسال خروجی رمز شده به عنوان ISN

Routing Information Protocol (RIP) حملات

- اطلاعات مسیریابی بدون تأیید هویت استفاده می شوند.
- مهاجم (Z) با ارسال اطلاعات مسیریابی نادرست، ترافیک هاست B را به سمت خود تغییر جهت می دهد.
  - هاست B موجود باشد: استراق سمع اطلاعات
  - هاست B موجود نباشد: ارسال اسپم با IP هاست B



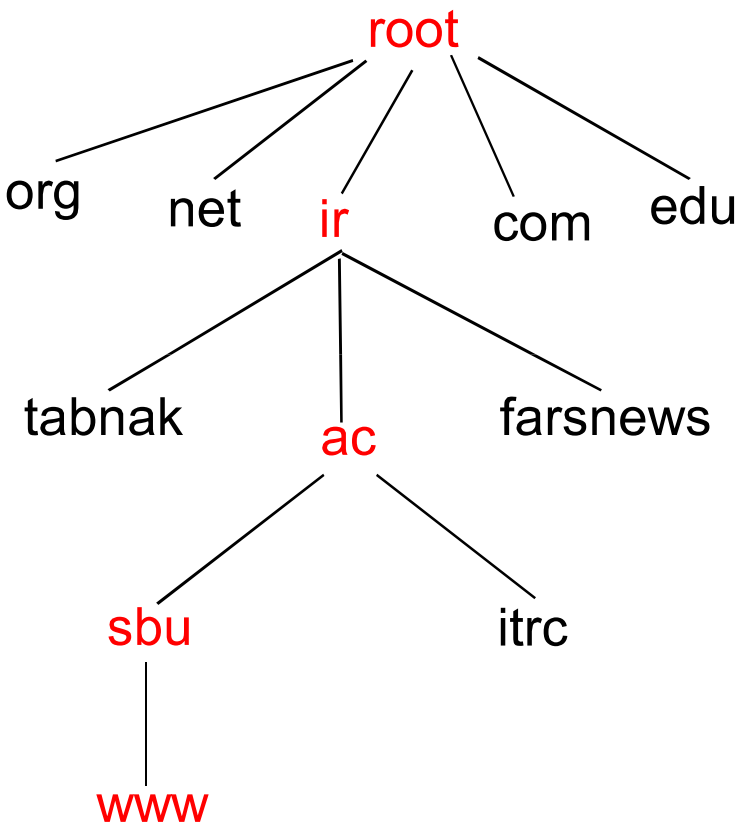
Internet Control Message Protocol (ICMP) حملات

- قطع اتصالات TCP
  - ICMP Destination Unreachable –
  - ICMP Time to Live Exceeded –
- حمله DOS با استفاده از ICMP
  - حملات از کار انداختن سرویس
- تغییر جدول مسیریابی با ICMP Redirect
-

پیشگیری

- قطع اتصالات TCP
  - چک کردن sequence number موجود در بسته ICMP و مطابقت آن با sequence number بسته TCP مورد نظر
- تغییر جدول مسیریابی با ICMP Redirect
  - نادیده گرفتن بسته های ICMP Redirect و عدم تغییر جدول مسیریابی

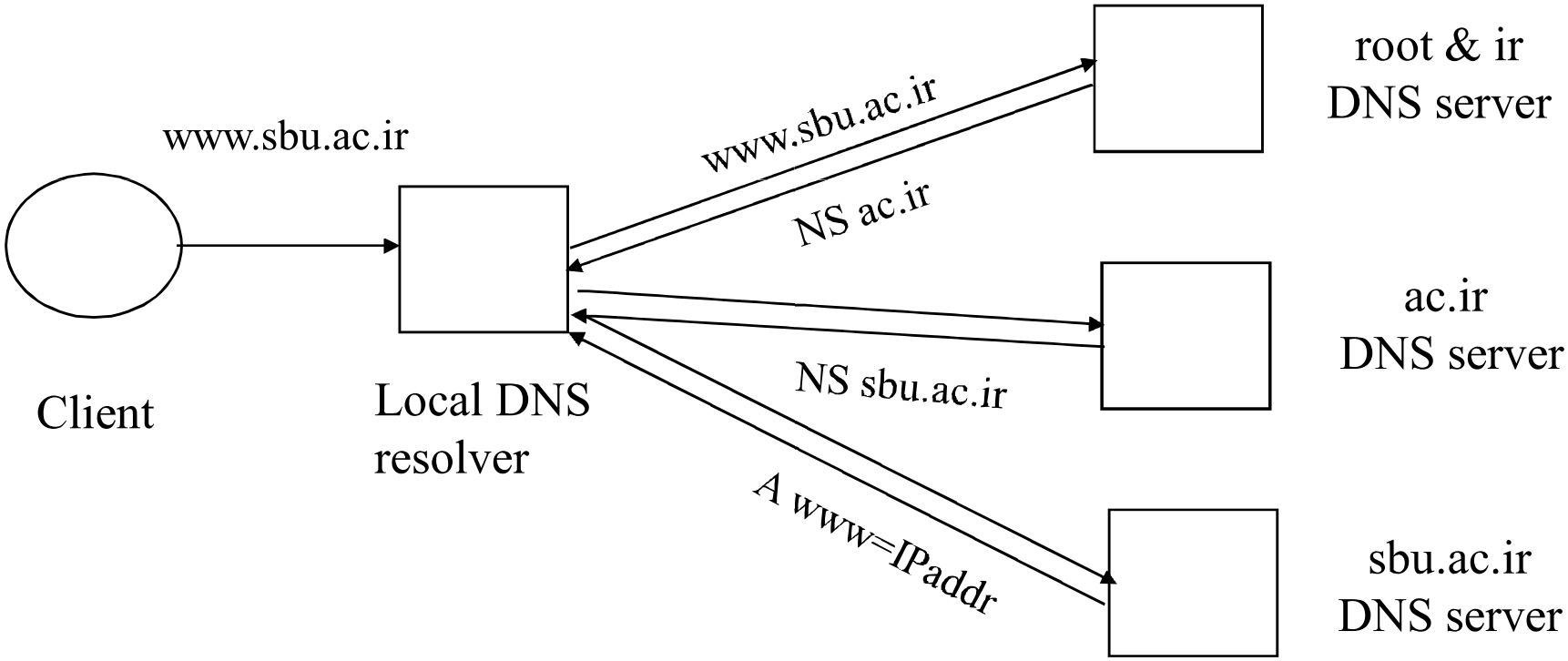
Domain Name System (DNS)



- ساختار سلسله مراتبی
- Zone
- Nameserver
- Authoritative Nameserver
- Resolver

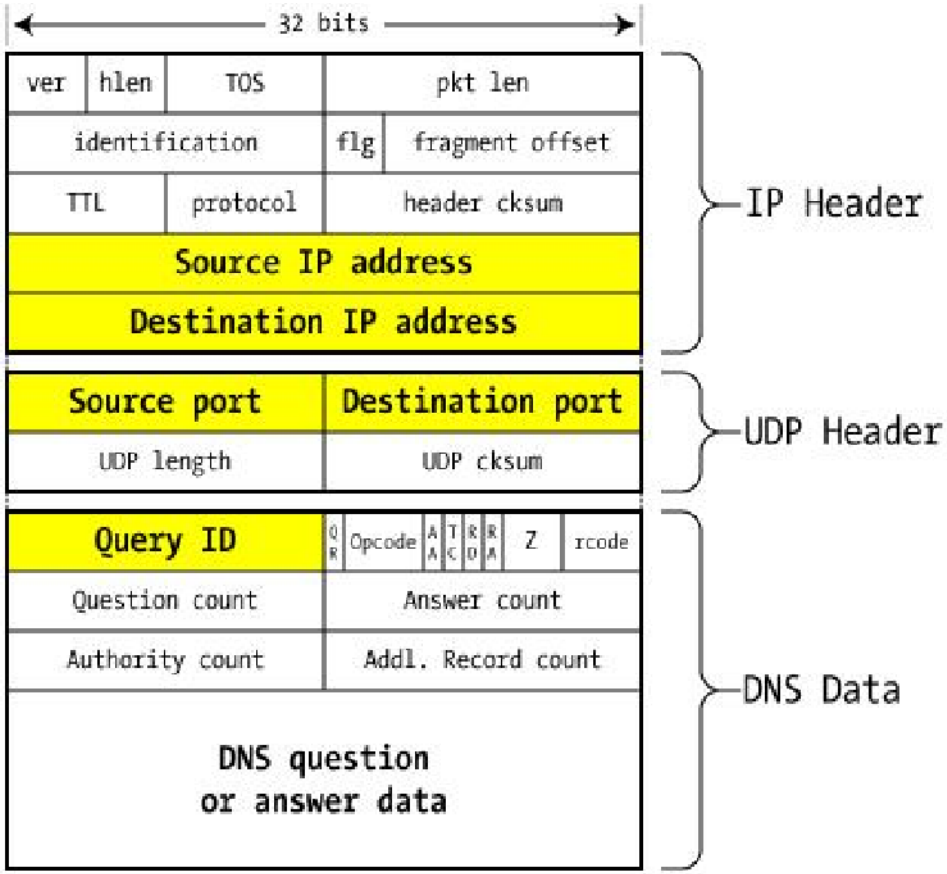
DNS Lookup

- استفاده از Caching برای افزایش کارایی

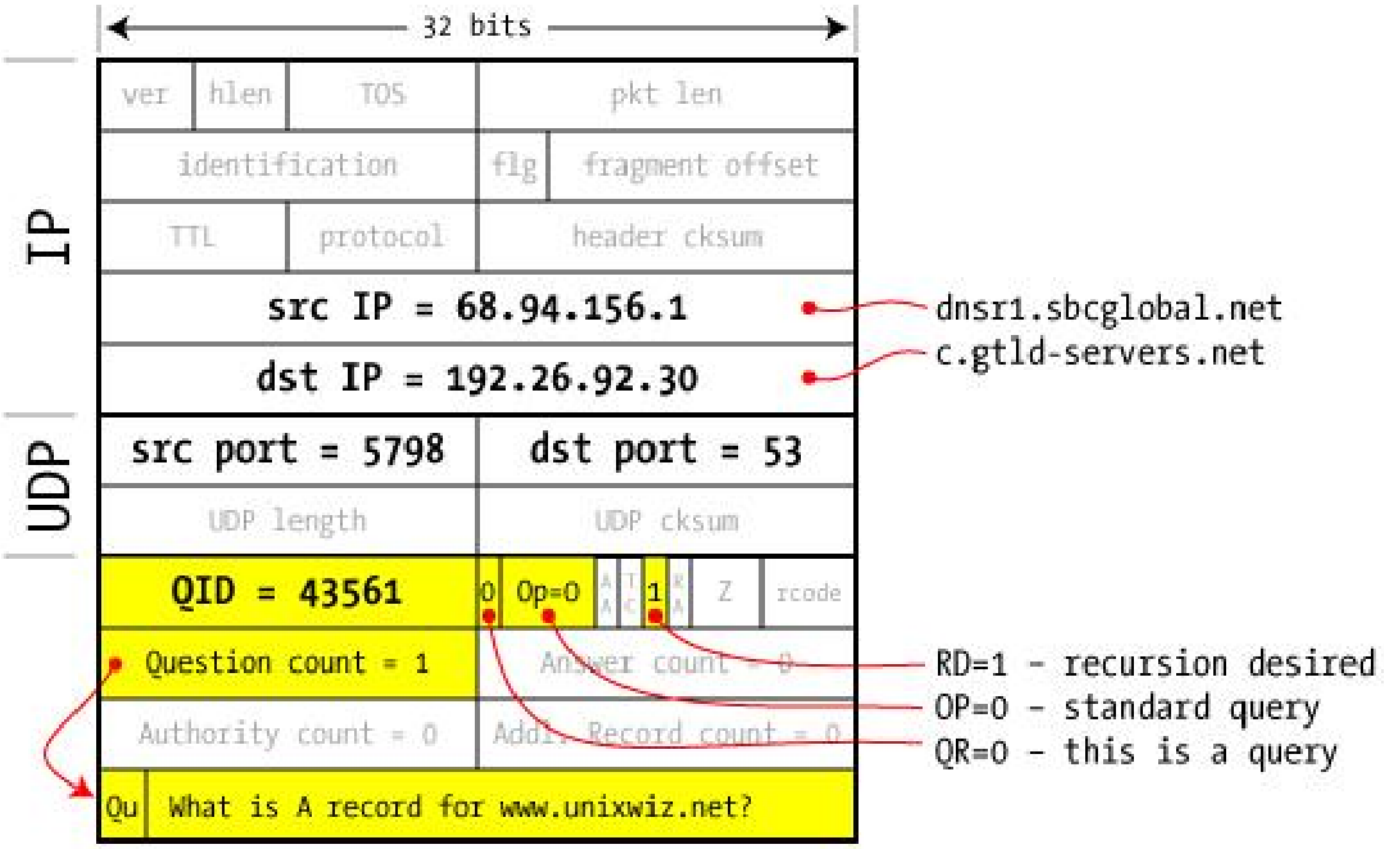


بسته DNS

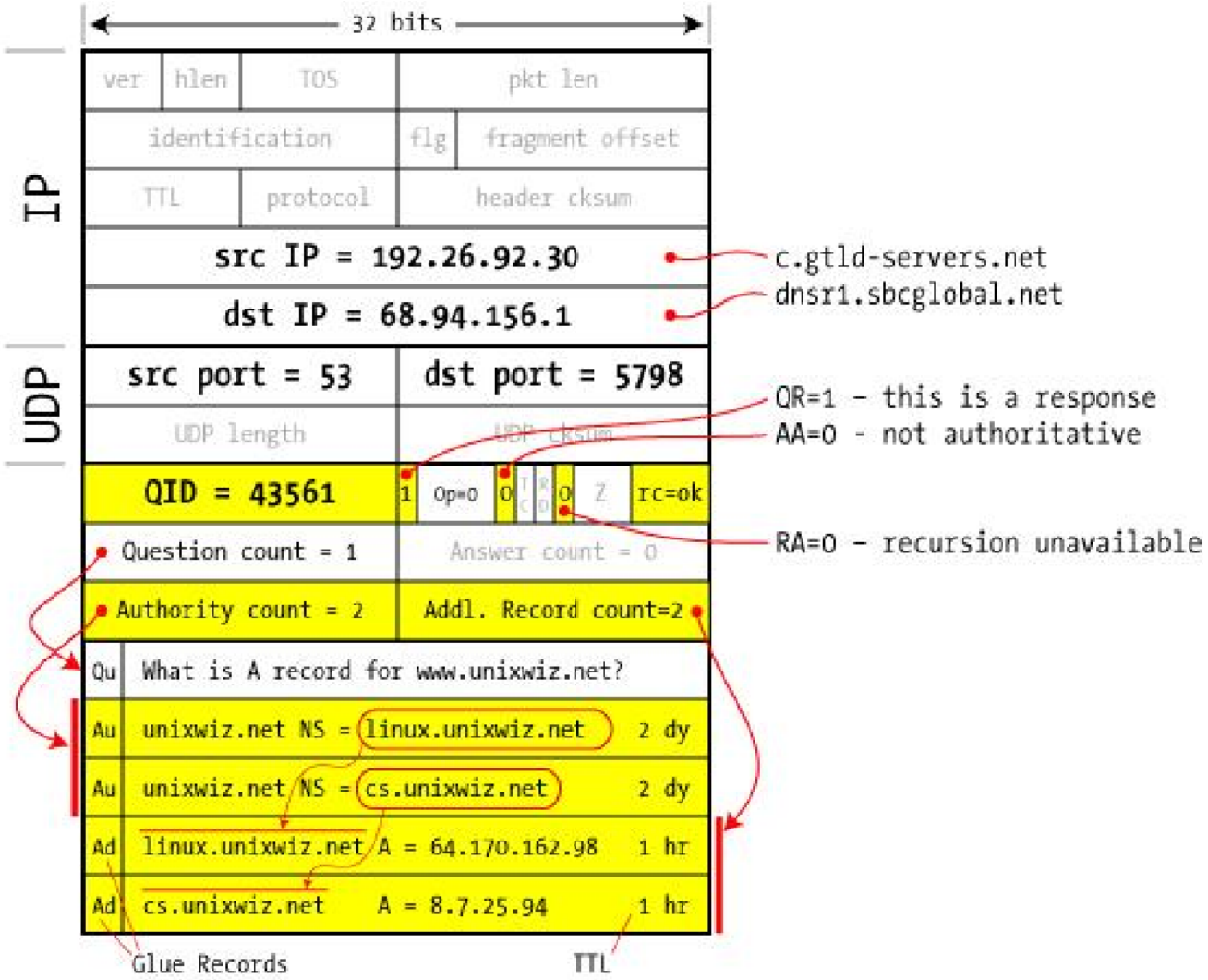
- شناسه پرس و جو
  - عدد ۱۶ بیتی
  - مطابقت پاسخ با پرس و جو



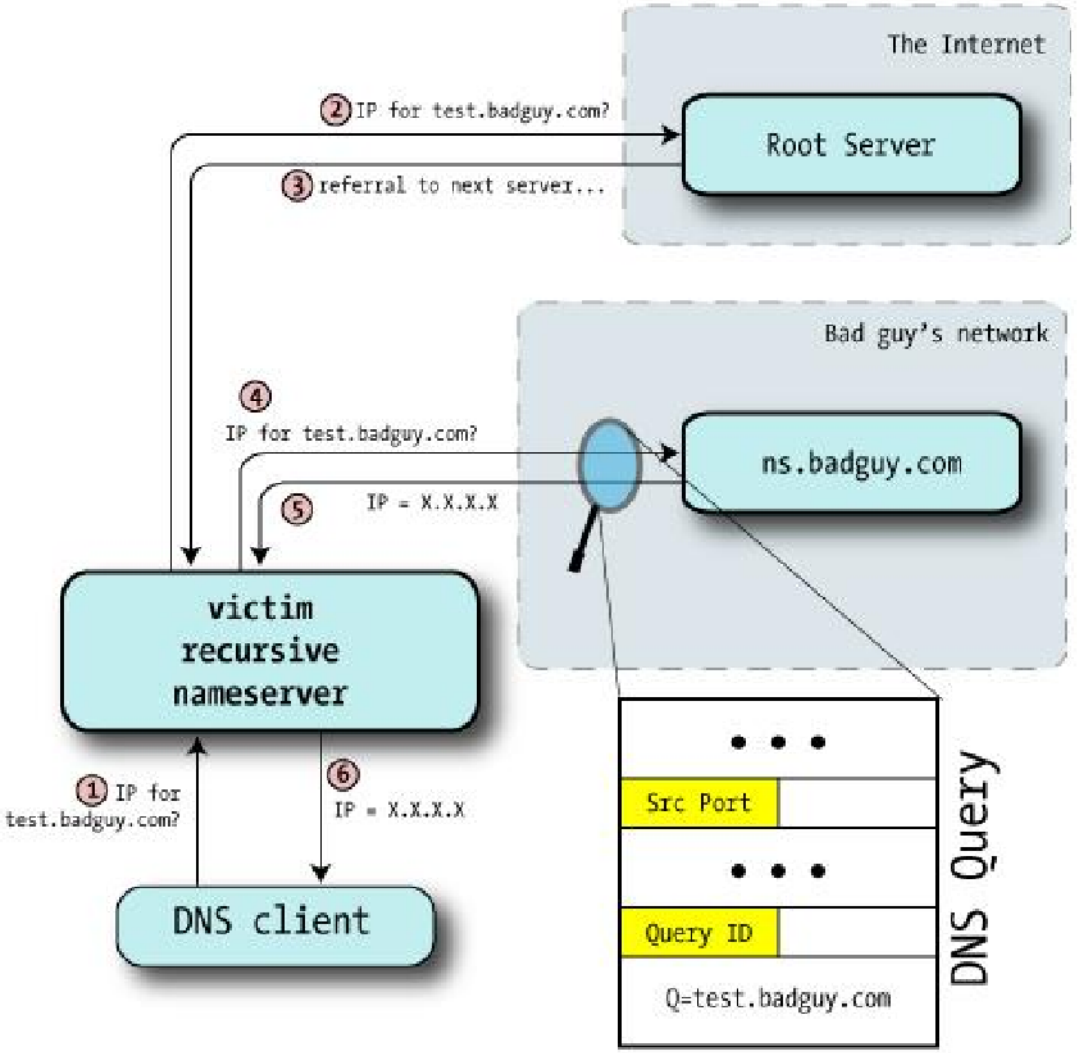
DNS Query


32 bits
IP
UDP
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
src IP = 68.94.156.1
dst IP = 192.26.92.30
src port = 5798
dst port = 53
UDP length
UDP cksum
QID = 43561
0
Op=0
1
Z
rcode
Question count = 1
Authority count = 0
Qu
What is A record for www.unixwiz.net?
dnsr1.sbcglobal.net
c.gtld-servers.net
RD=1 - recursion desired
OP=0 - standard query
QR=0 - this is a query

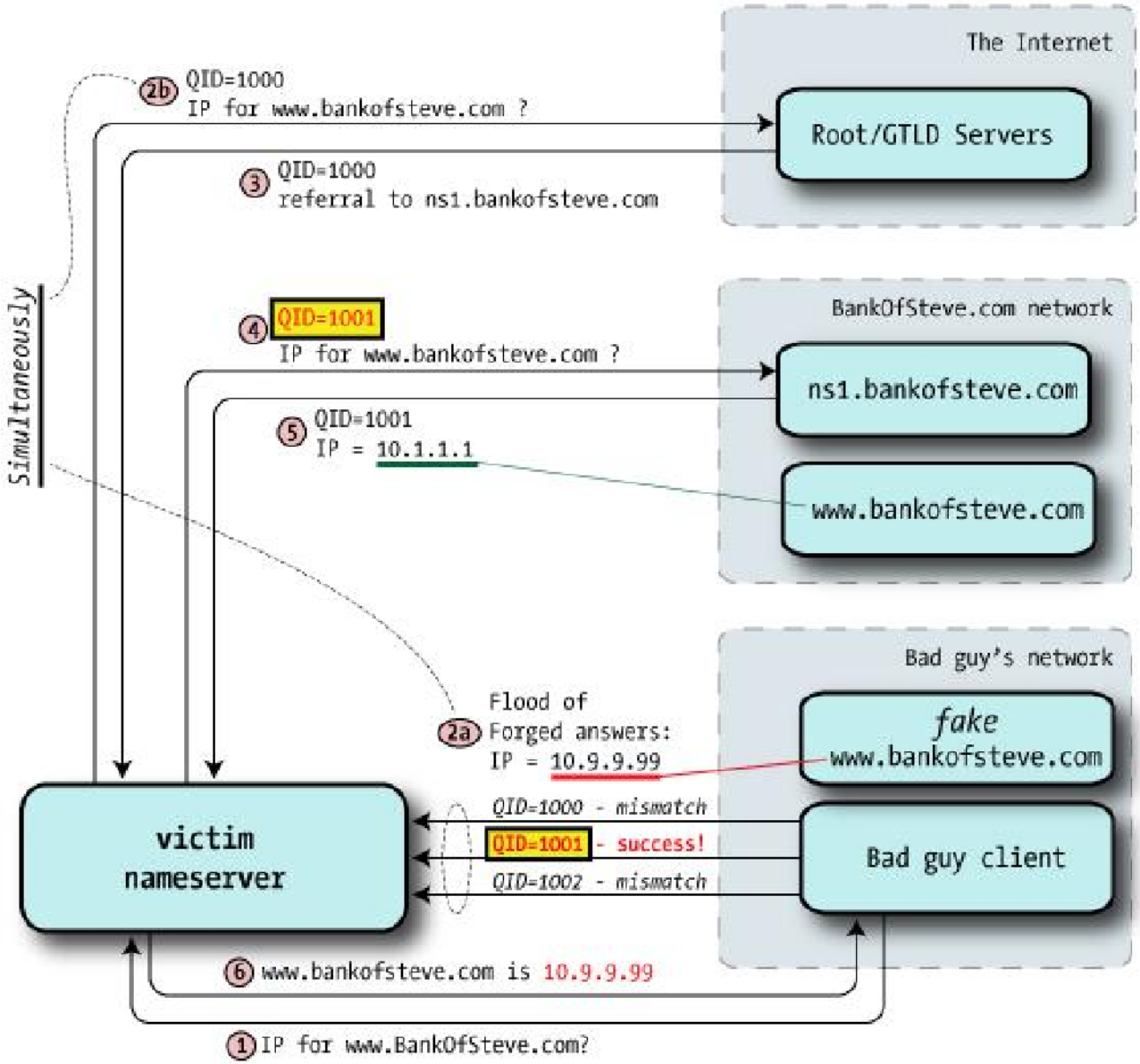
DNS Response



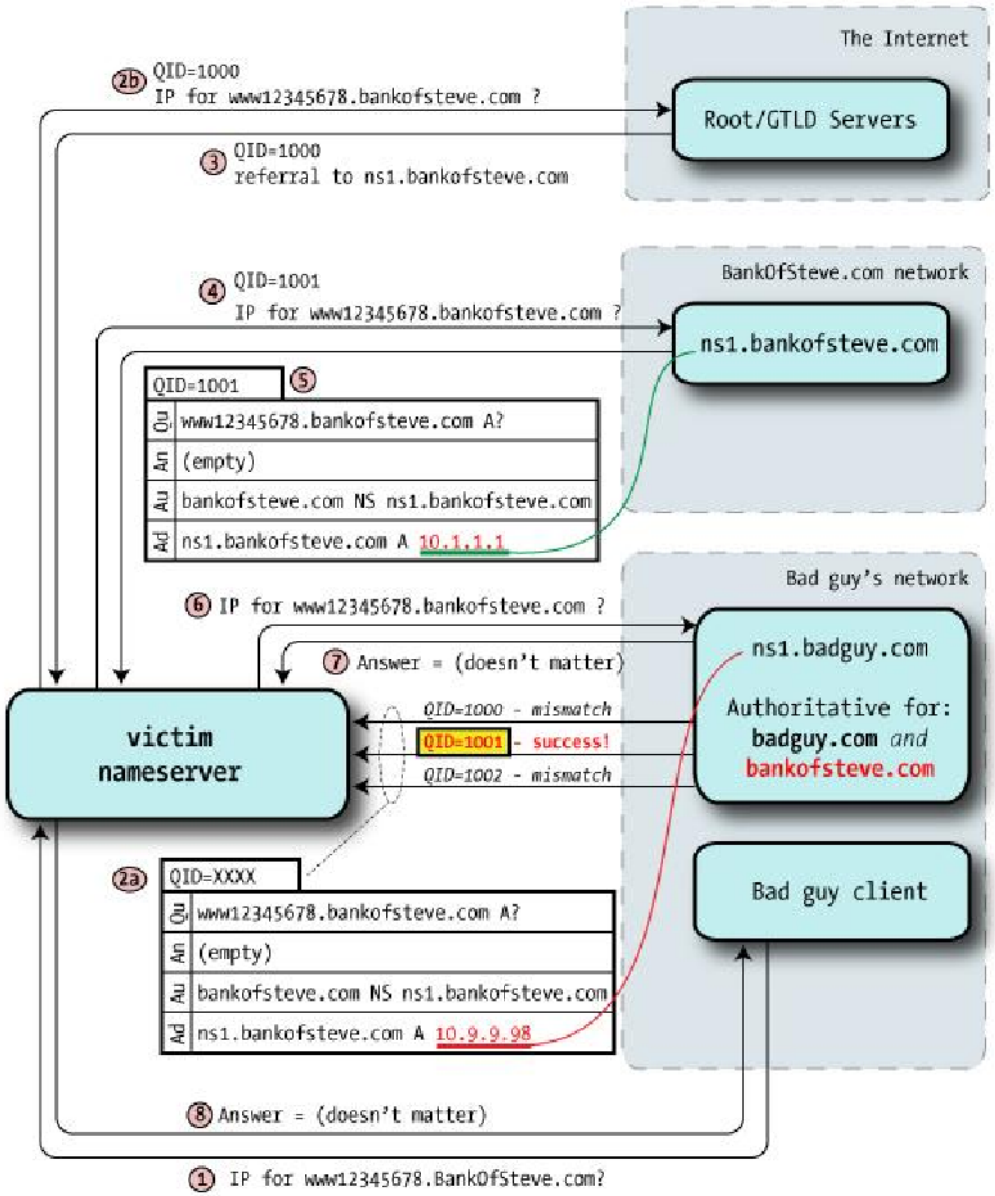
حدس زدن شناسه پرس و جو



DNS Cache poisoning (Hostname)



DNS Cache Poisoning (Nameserver)



منابع

- A look back at Security Problems in the TCP/IP Protocol Suite
- A survey of BGP security
- DNS Cache Poisoning
- DNS Cache Poisoning (BIND Birthday Attack)