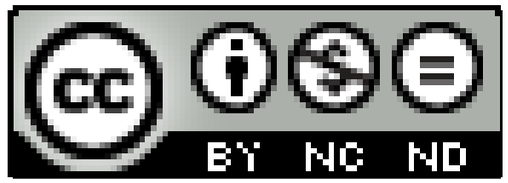
Мрежова сигурност I

http://training.iseca.org/

IP 3/7

ARP, ICMP, DHCP



Boyan Krosnov

Преговор и план на курса

- Увод в мрежовата сигурност
- Криптография
- Увод в мрежите
- Ethernet
- Wi-Fi
- IP

→ UDP, DHCP, ARP, Атаки върху IP

- IP routing protocols, IPv6
- TCP
- Лекция преговор
- Тест – 16-ти или 18-ти Ноември
- Демо
- …

Преговор 1/6 и 2/6

- История
- Стандартите
- IP service model
- Адресиране
  - основи
  - специални адреси
  - CIDR
  - алокиране на IP адреси
- The IPv4 protocol
  - header format
  - basic routing
  - fragmentation
  - options

План – 3/6

- ARP
  - Encapsulation
  - Нормална работа
  - Gratuitous ARP
- ICMP
  - Encapsulaiton
  - Ping
  - Error
  - Други
- DHCP
  - Encapsulation - UDP
  - DHCP exchange
  - Таймери
- 4/6 - Атаки върху IP

ARP

- Address Resolution Protocol
  - Resolve на MAC адрес по IP адрес

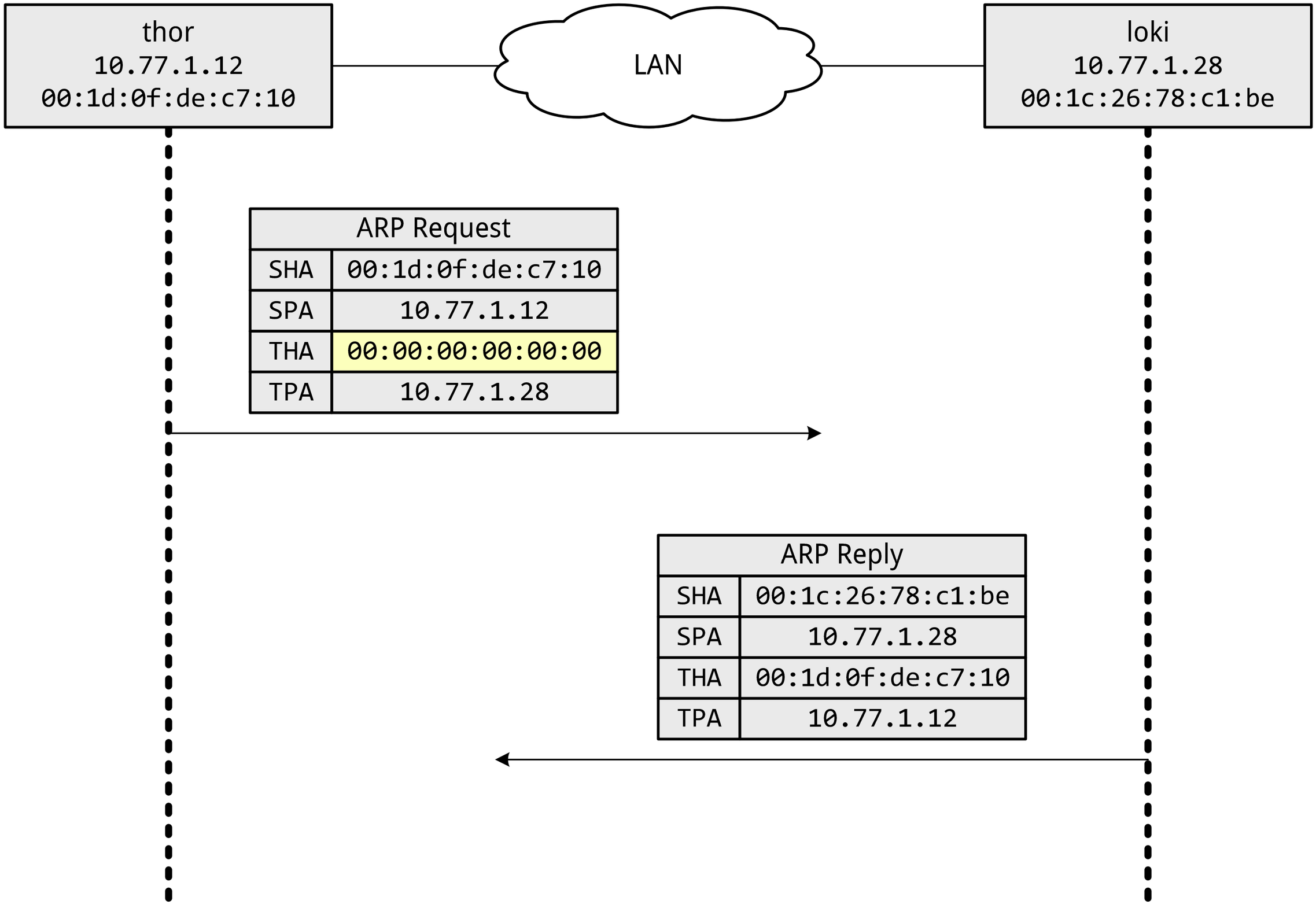
16	Hardware Type = 0x0001
16	Protocol Type = 0x0800
8	Hardware Address Length = 6
8	Protocol Address Length = 4
16	Operation = 1 or 2
48	Sender Hardware Address
32	Sender Protocol Address
48	Target Hardware Address
32	Target Protocol Address

ARP – Нормална работа

- ARP request
  - Ethernet broadcast – destination MAC FF:FF:FF:FF:FF:FF
  - ARP type 1
  - ARP Target MAC address is 00:00:00:00:00:00
  - Who has 10.22.33.42? Tell 10.22.33.44

- ARP response
  - Ethernet unicast
  - ARP type 2
  - Всички полета са попълнени
  - 10.22.33.42 is at 02:11:12:13:14:15

ARP – Нормална работа



Gratuitous ARP

- Отговор без въпрос
  - Моят адрес е следния
  - Clustering и HA
  - Router redundancy

- Въпрос за собствения адрес
  - Има ли някой друг на моя адрес?
  - Проверка за дуплицирани адреси

- “Stateless” ARP
  - повечето имплементации приемат ARP отговори безусловно

ARPing

- Broadcast request
- Unicast response

- Loop
  - Unicast request
  - Unicast response

Въпроси

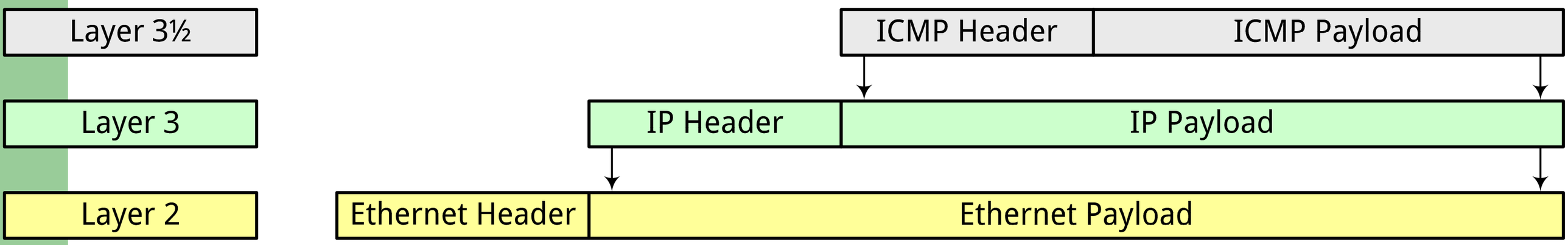
ICMP

- Internet Control Message Protocol (RFC792)
- Функции
  - Troubleshooting
    - Echo
  - Error reporting by routers and hosts
    - Destination Unreachable
    - Time Exceeded
    - Parameter Problem
    - Source Quench
    - Redirect
  - Други

ICMP

- Internet Control Message Protocol

0								1								2								3							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Type								Code								Checksum															
Unused																															
IP Header + 64 bits of Original IP Payload																															



ICMP Echo/Echo reply

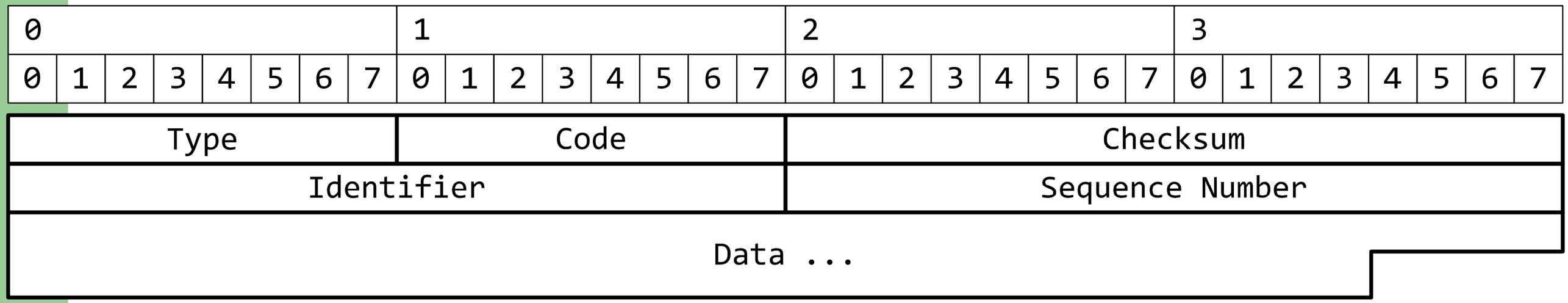
- ICMP Echo (type 8)
- ICMP Echo reply (type 0)

- Ping

```
boyan@gaia:~$ ping www.google.com -n
PING www.l.google.com (209.85.227.99) 56(84) bytes of data.
64 bytes from 209.85.227.99: icmp_seq=1 ttl=55 time=47.7 ms
64 bytes from 209.85.227.99: icmp_seq=2 ttl=55 time=47.5 ms
64 bytes from 209.85.227.99: icmp_seq=3 ttl=55 time=47.7 ms
^C
--- www.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 47.469/47.618/47.792/0.123 ms
```

ICMP Echo/Echo reply

- ICMP Echo (type 8)
- ICMP Echo reply (type 0)

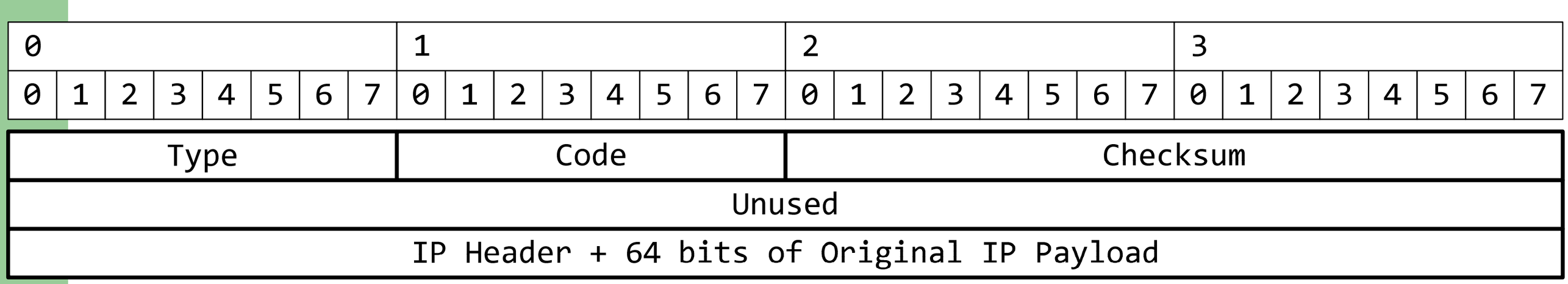


ICMP Destination Unreachable

- ICMP Destination Unreachable (type 3)
  - Router
    - Net Unreachable - адресът не е намерен в routing таблицата
    - Host Unreachable - адресът не е намерен в ARP таблицата
    - Fragmentation needed but DF set – PMTU-D
  - Филтър
    - Communication Administratively Prohibited
  - Host
    - Port Unreachable

ICMP Destination Unreachable

- ICMP Destination Unreachable (type 3)



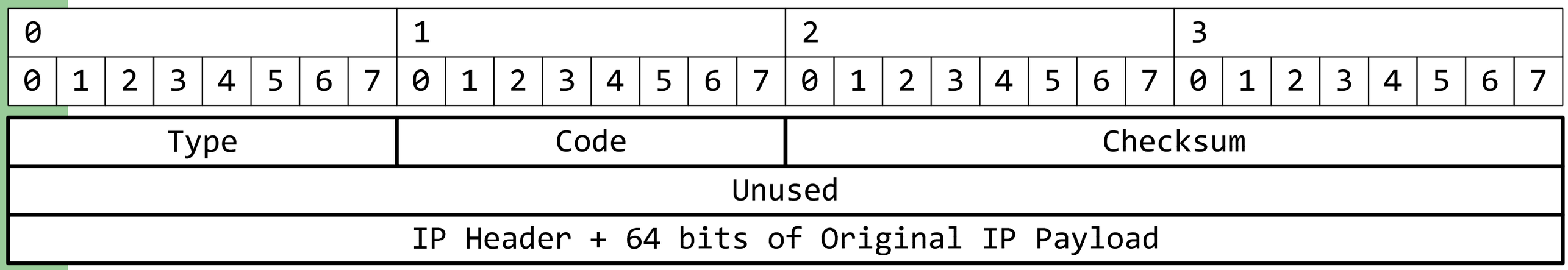
PMTU-D

- Path MTU Discovery (RFC 1191, Nov 1990)
  - ICMP type 3 code 4

0								1								2								3							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Type								Code								Checksum															
Unused																Next-Hop MTU															
IP Header + 64 bits of Original IP Payload																															

ICMP Source Quench

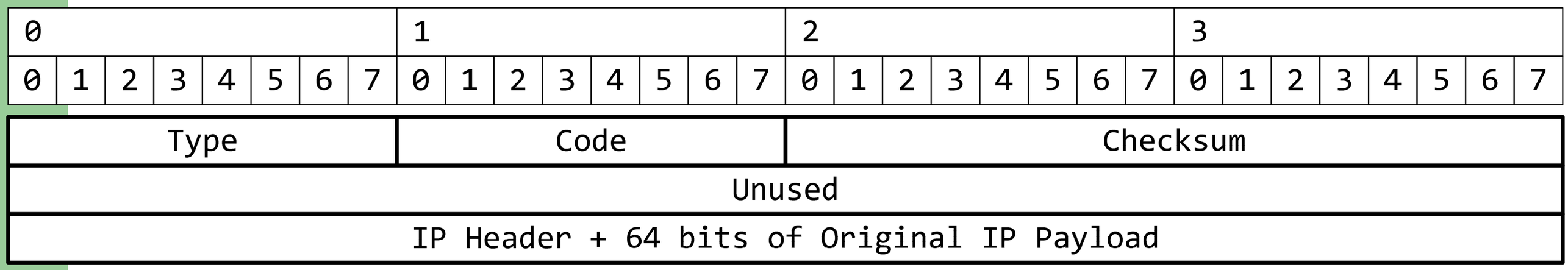
- ICMP Source Quench (type 4)
- Пакета е drop-нат, защото е нямало място в опашката



ICMP Time Exceeded

- ICMP Time Exceeded (type 11)
  - Router: TTL exceeded
  - Host: Fragment reassembly time exceeded

- Traceroute



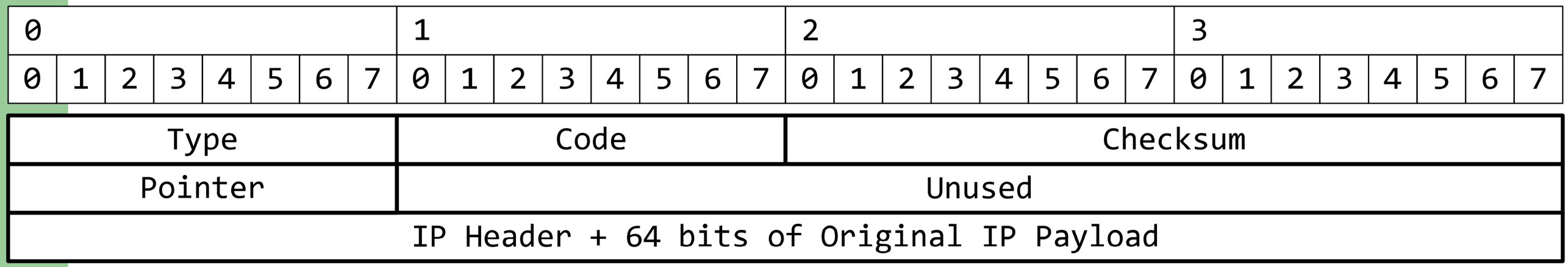
Traceroute

```
marla:~$ traceroute -n www.google.com
traceroute to www.l.google.com (209.85.135.147), 64 hops max, 52 byte packets
 1  194.12.255.249  1 ms  2 ms  4 ms
 2  85.14.2.2  0 ms  0 ms  0 ms
 3  80.81.192.108  30 ms  30 ms  32 ms
 4  209.85.255.172  40 ms (TOS=128!)  33 ms  31 ms
 5  209.85.248.248  38 ms 72.14.238.128  39 ms  38 ms
 6  209.85.241.189  43 ms  38 ms  42 ms
 7  209.85.253.22  42 ms 72.14.239.58  42 ms *
 8  209.85.135.147  42 ms (TOS=0!)  42 ms  42 ms
```

ICMP Parameter Problem

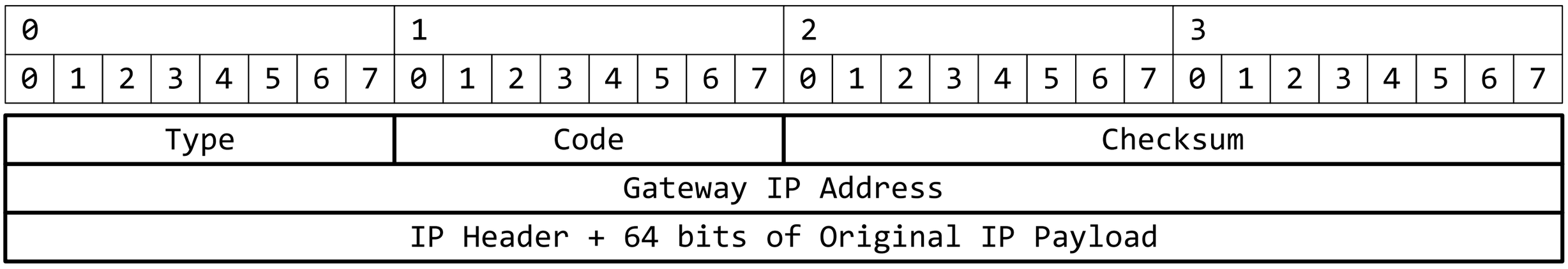
- ICMP Parameter Problem (type 12)

- Неправилно формиран IP пакет
- Грешна дължина или неправилна стойност в някое поле

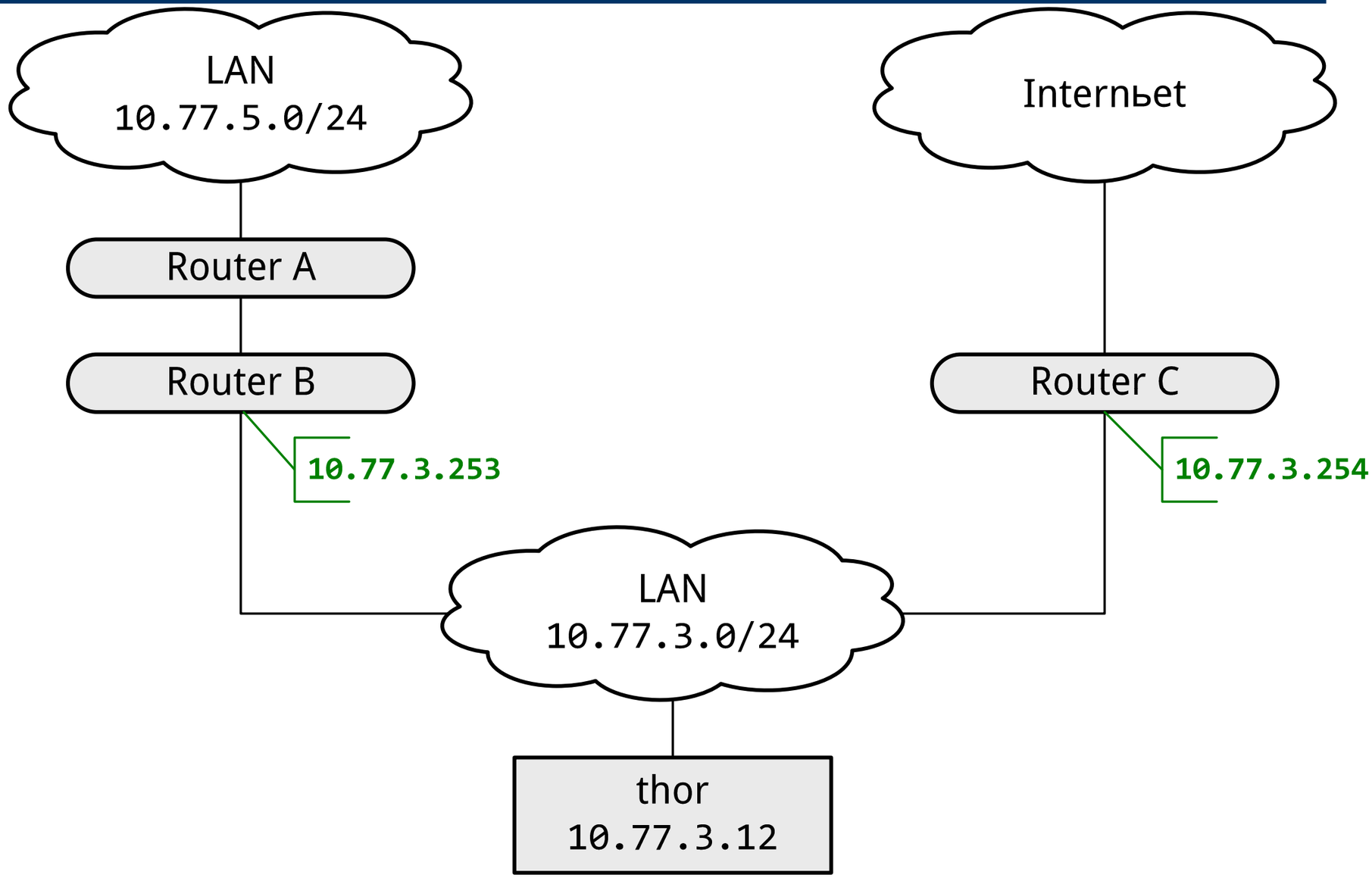


ICMP Redirect

- ICMP Redirect (type 5)
- Изпраща се от рутери, когато рутират пакет обратно през интерфейс ,през който е пристигнал
- Хостовете поддържат routing кеш за активните редиректи



ICMP Redirect



0								1								2								3							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Type								Code								Checksum															
Gateway IP Address																															
IP Header + 64 bits of Original IP Payload																															

Други ICMP

- Router advertisement/solicitation
- Mask request/reply
- Timestamp request/reply
- Information request/reply
- (другия) Traceroute

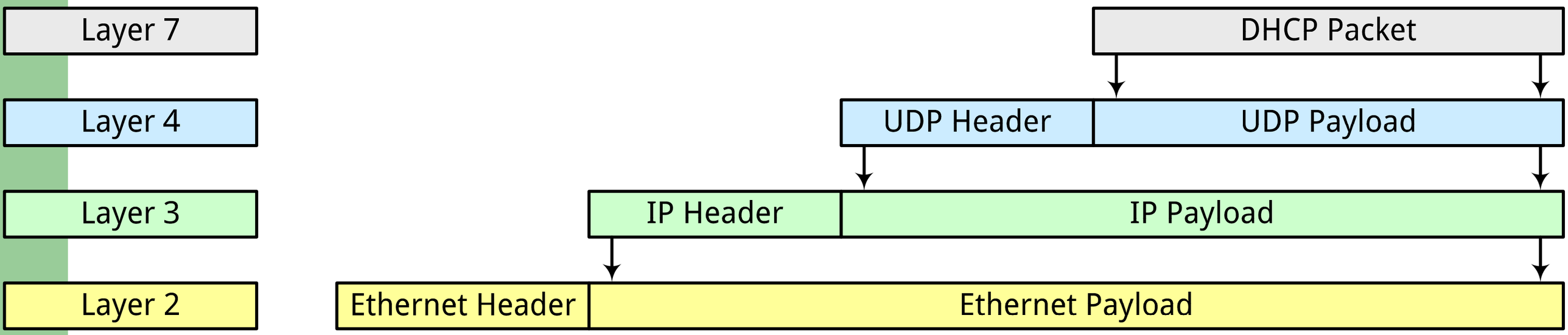
Въпроси

DHCP

- Dynamic Host Configuration Protocol
  - Наследник на BOOTP + опции
  - RFC2131 – първа версия 1993-та година
- Динамично конфигуриране на хостовете с
  - IP адрес, маска
  - default route
  - адреси на DNS сървърите
  - и
    - domain name
    - адрес на NTP сървъра
    - адрес на boot сървъра и име на boot файла
    - и т.н.

DHCP Encapsulation

- DHCP върху UDP върху IP
  - Неизвестен IP адрес: 0.0.0.0
  - Broadcast IP адрес: 255.255.255.255
  - UDP ports 67/68



DHCP

- DISCOVER, OFFER, REQUEST, ACK
- Други DHCP съобщения
  - NAK, DECLINE, RELEASE, INFORM
  - LEASEQUERY

DHCP Таймери

- T1 – Renew timer
- T2 – Rebind timer
- Lease expires time

- T1 << T2 << Lease Time

INIT - REBOOT

-
DHCPREQUEST

REBOOTING

DHCPNAK
Restart

DHCPNAK
Discard offer

INIT

DHCPACK
DHCPDECLINE

-
DHCPDISCOVER

DHCPNAK, Lease expired
Halt network

SELECTING

DHCPOFFER
Collect replies

Select offer
DHCPREQUEST

DHCPOFFER
Discard

REQUESTING

REBINDING

DHCPACK
Record lease, set T1, T2

DHCPACK
Record lease, set T1, T2

DHCPACK
Record lease, set T1, T2

BOUND

T2 expires
Broadcast DHCPREQUEST

DHCPACK
Record lease, set T1, T2

DHCP{OFFER,ACK,NAK}
Discard

T1 expires
DHCPREQUEST

RENEWING

DHCPNAK
Halt network

DHCP Relay

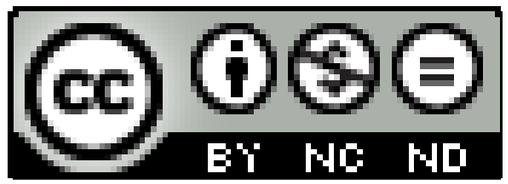
Въпроси

Мрежова сигурност I

http://training.iseca.org/

IP 4/7

Атаки върху IP



Boyan Krosnov

Атаки върху IP – 4/6

- Resource exhaustion
- Bottlenecks
- Бъгове и грешки в конфигурацията на рутери
- Бъгове и грешки в конфигурацията на хостове

- Source Routing
- IP spoofing
- ICMP attacks
- Flood, Amplification attacks
- ARP атаки
- DHCP атаки

Resource exhaustion

- ARP таблици с ограничен размер
- Буфери в рутери и хостове
  - Bursts
  - Fragment reassembly buffers

Bottlenecks

- Бавни връзки
- Бавни карти
- Бавни хостове
- Бавни процесори на рутери
  - Fast path vs. Slow Path

Бъгове в рутери

- Софтуер на типичен рутер
  - Router stack: IP, ARP
  - Routing protocols: RIP, OSPF, BGP
  - ICMP generation
- ... но и
  - DHCP server, DHCP relay agent, DHCP client
  - SSH, Telnet
  - SNMP
  - HTTP/HTTPS server
  - RADIUS client
  - и боклук от типа на echo, chargen, finger, etc.

Грешни конфигурации на рутери

- Цикли в мрежите
- IP Directed Broadcast
- IP Redirects

Бъгове в хостове

Грешни конфигурациите на хостове

Въпроси

Source Routng

- IP Option Strict/Loose Source Routing

IP spoofing

- IP Spoofing

- Unicast Reverse Path Forwarding/Filtering (URPF)
  - strict
  - loose

- Edge filtering
  - RFC1918
  - + more

ICMP attacks

- ICMP Redirect
  - Man-in-the-middle (MITM)
- ICMP Unreachable
  - Убива сесия от 4-ти слой
- ICMP Source Quench
  - Забавя сесия от 4-ти слой
- ICMP PMTU-D
  - Забавя сесия от 4-ти слой

- Informational RFC5927 July 2010 – ICMP Attacks against TCP
  - задължително четиво на курса

Flood и Amplification

- Flood
- Amplification
  - IP Directed Broadcast
    - Smurf
  - ICMP-та по-големи от оригиналния IP пакет

Въпроси

ARP атаки

- ARP spoofing/poisoning
  - MITM / DoS
- Да станем рутер

- Да станем избран от нас хост

DHCP атаки

- Да станем DHCP сървър
- Resource exhaustion върху броя на IP адресите от pool-a

Въпроси

Следващия път

- Увод в мрежовата сигурност
- Криптография
- Увод в мрежите
- Ethernet
- Wi-Fi
- IP
- UDP, DHCP, ARP, Атаки върху IP

→ IP routing protocols, IPv6

- TCP
- Лекция преговор – подготовка за теста
- Тест – 16-ти или 18-ти Ноември
- Демо
- …