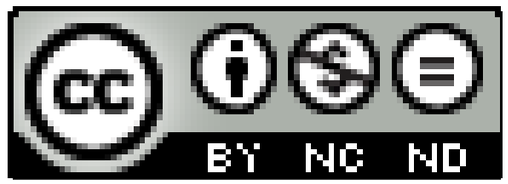
Мрежова сигурност I

http://training.iseca.org/

IP 5/7, 6/7

IP Routing Protocols



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

Преговор 3/6

- ARP
  - Нормална работа
  - Gratuitous ARP
- ICMP
  - Ping, Traceroute
  - Errors, PMTU-D
  - Redirect
- DHCP
  - Нормална работа
  - DHCP state machine & timers
- 4/6 - Атаки върху IP

Преговор 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

4/6 – Довършваме този час

- 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

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

План 5/6

- Рутиране на IP пакети
- ARP и Redirects
- Address Redundancy
  - VRRP
  - Други HSRP, GLBP, CARP
- Distance vector vs. Link state
- RIP
- OSPF
- BGP
- други

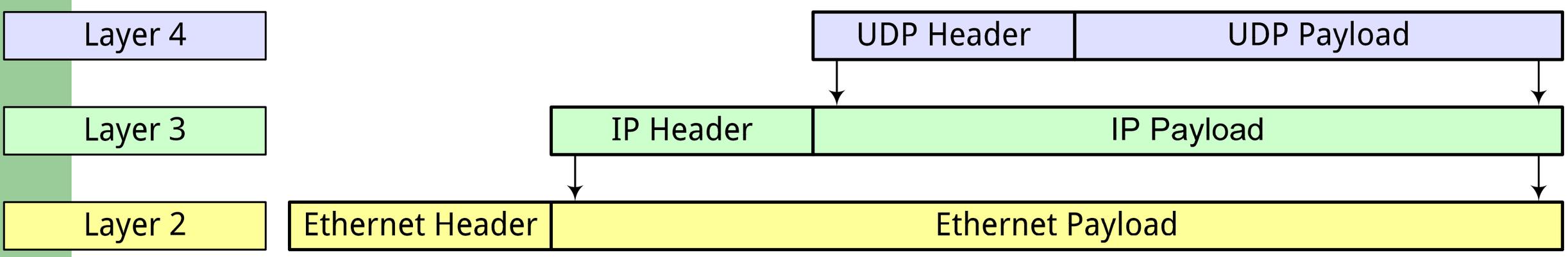
UDP

- User Datagram Protocol

UDP Header Format

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

Source Port	Destination Port
Length	Checksum
Data...	



Рутиране на IP пакети

- Routing table
  - Longest prefix match
  - Recursive lookup
- Static routing
  - таблицата се попълва от администратора
- Dynamic routing
  - таблицата се попълва от routing protocol

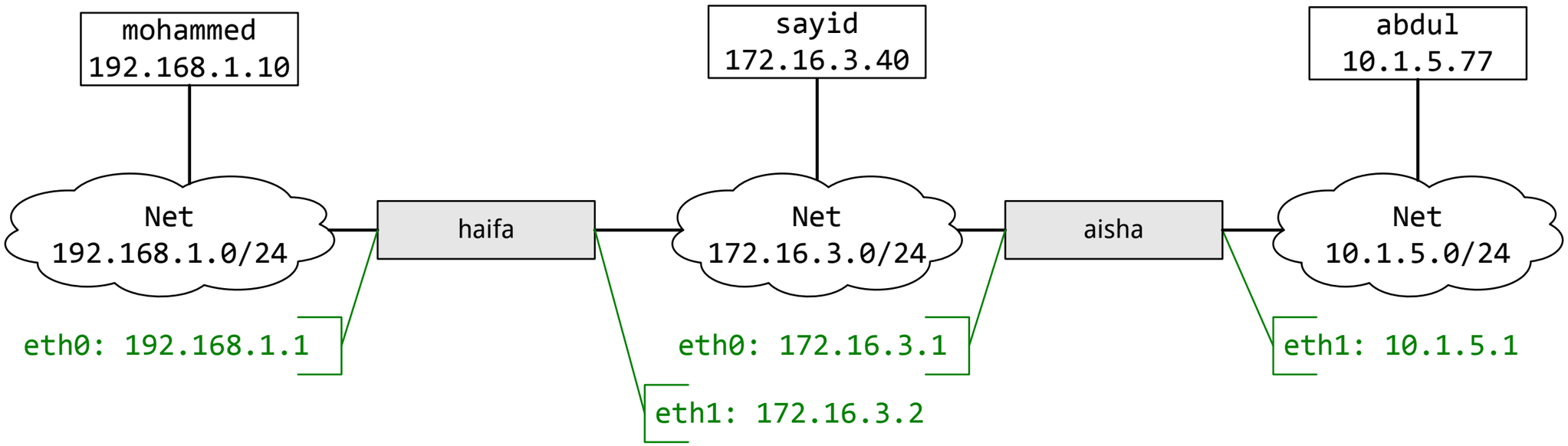
Рутиране на IP пакети

directly connected

indirect

haifa routing table	
Network	Trough
192.168.1.0/24	eth0
172.16.3.0/24	eth1
10.1.5.0/24	172.16.3.1

aisha routing table	
Network	Trough
10.1.5.0/24	eth1
172.16.3.0/24	eth0
192.168.1.0/24	172.16.3.2



mohammed routing table	
Network	Trough
192.168.1.0/24	-
172.16.3.0/24	192.168.1.1
10.1.5.0/24	172.16.3.1

sayid routing table	
Network	Trough
172.16.3.0/24	-
192.168.1.0/24	172.16.3.2
10.1.5.0/24	172.16.3.1

abdul routing table	
Network	Trough
10.1.5.0/24	-
172.16.3.0/24	10.1.5.1
192.168.1.0/24	172.16.3.2

ARP и Redirects

- “Рутиране” с ARP – arp proxy
  - host: 10.0.0.2/16, default route 0/0 -> 10.0.0.1
  - router: 10.0.0.1/24
  - host:~# ping 10.0.1.2
  - Какво ще се случи?
- “Рутиране” с ICMP Redirects
  - host: 10.0.0.3/24, default route 0/0 -> 10.0.0.1
  - router1: 10.0.0.1/24, 192.168.1.1/24
  - router2: 10.0.0.2/24, 192.168.2.1/24
  - host:~# ping 192.168.2.1
  - Какво ще се случи?

Въпроси

Address Redundancy

- VRRP – Virtual Router Reduncancy Protocol

- Други
  - HSRP – Hot Standby Redundancy Protocol
  - GLBP – Gateway Load Balancing Protocol
  - CARP – Common Address Reduncancy Protocol

VRRP

- VRRP Version 3 за IPv4 и IPv6 - RFC5798
- States
  - Initializing
  - Master
  - Backup
- VRRP Priority

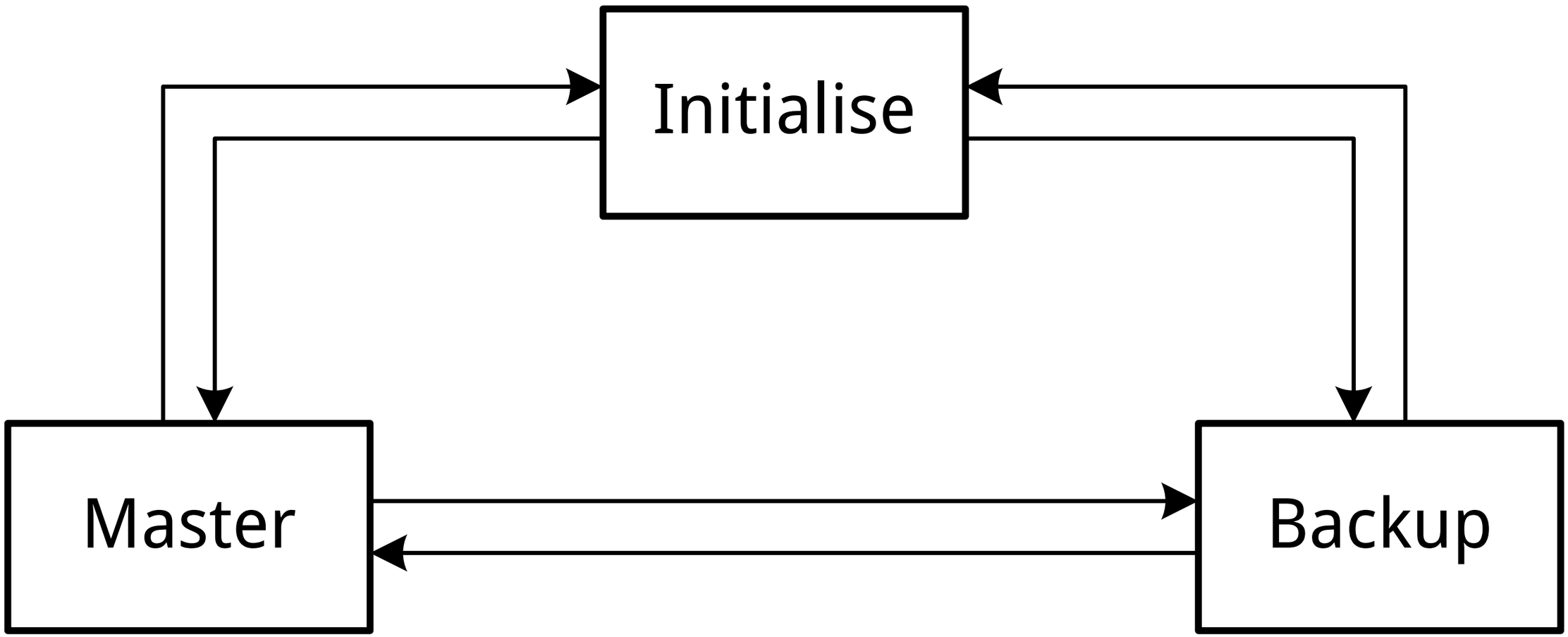
- RFC-то - Задължителен материал към курса
  - Прочетете внимателно Security Considerations секцията

VRRP

- VRRP Version 3 за IPv4 и IPv6 - RFC5798
- States
  - Initializing
  - Master
  - Backup
- VRRP Priority

- RFC-то - Задължителен материал към курса
  - Прочетете внимателно Security Considerations секцията

VRRP States



Въпроси

Routing Protocols

Distance vector

- Всеки router изпраща на съседите си списък с достъпните му мрежи и разстоянието до тях
- Разстояние традиционно се мери в hop count
    - но не във всички distance vector протоколи
- Пример за distance vector таблица

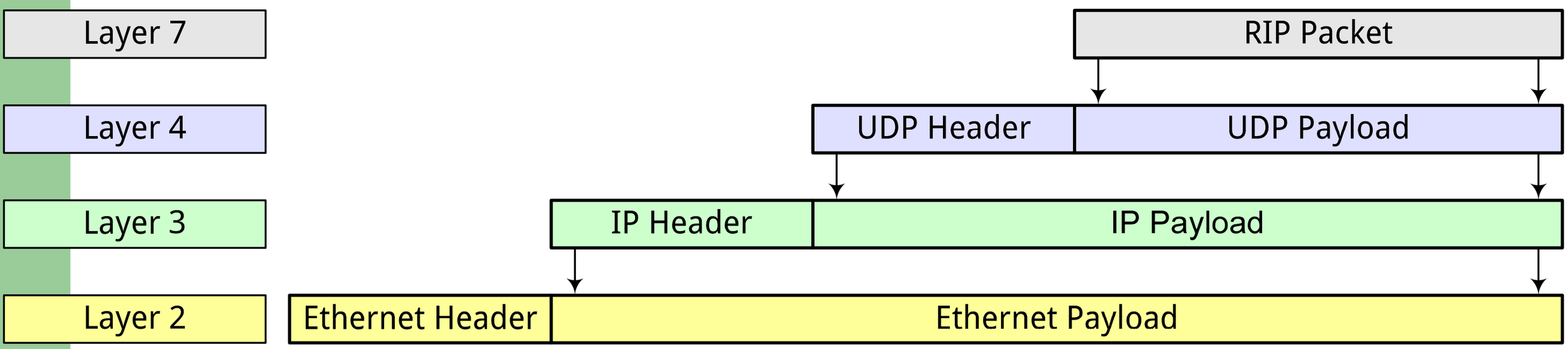
prefix	hop count
10.0.0.0/24	1
192.168.0.0/16	2
0.0.0.0/0	5

Link state

- Всеки router изпраща на всички рутери в мрежата списък с интерфейсите си и директно закачените си мрежи
- Всеки рутер построява граф на мрежата и намира оптималните пътища от себе си до всяка мрежа (Dijkstra’s algorithm)
- Пример за link state advertisement
  - router id 10.0.0.1
    - interface 10.0.0.1, 10.0.1.1, 10.0.2.1
  - network 10.0.0.0/24
  - network 10.0.1.0/24
  - network 10.0.2.0/24

RIP

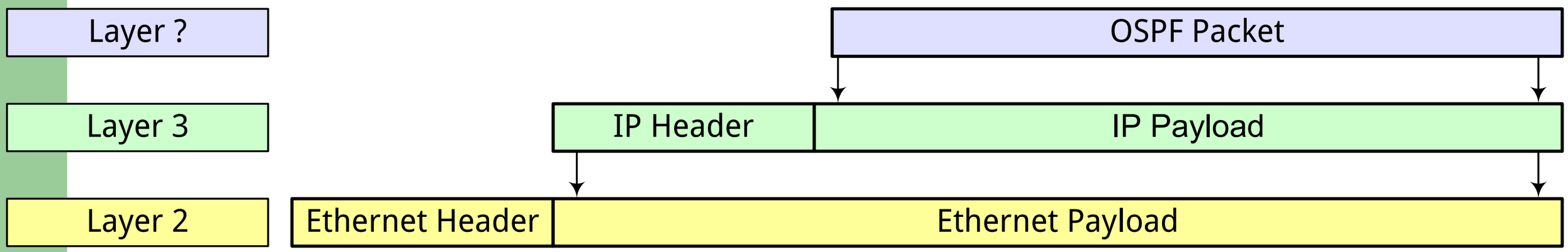
- Routing Information Protocol version 2
  - RFC2453 и RFC1722
- Distance Vector
- RIPng
- UDP енкапсулация
- Authentication



OSPF

- Open Shortest Path First version 2 – RFC2328
- Version 3 – RFC5340

- LSA flooding
- Authentication

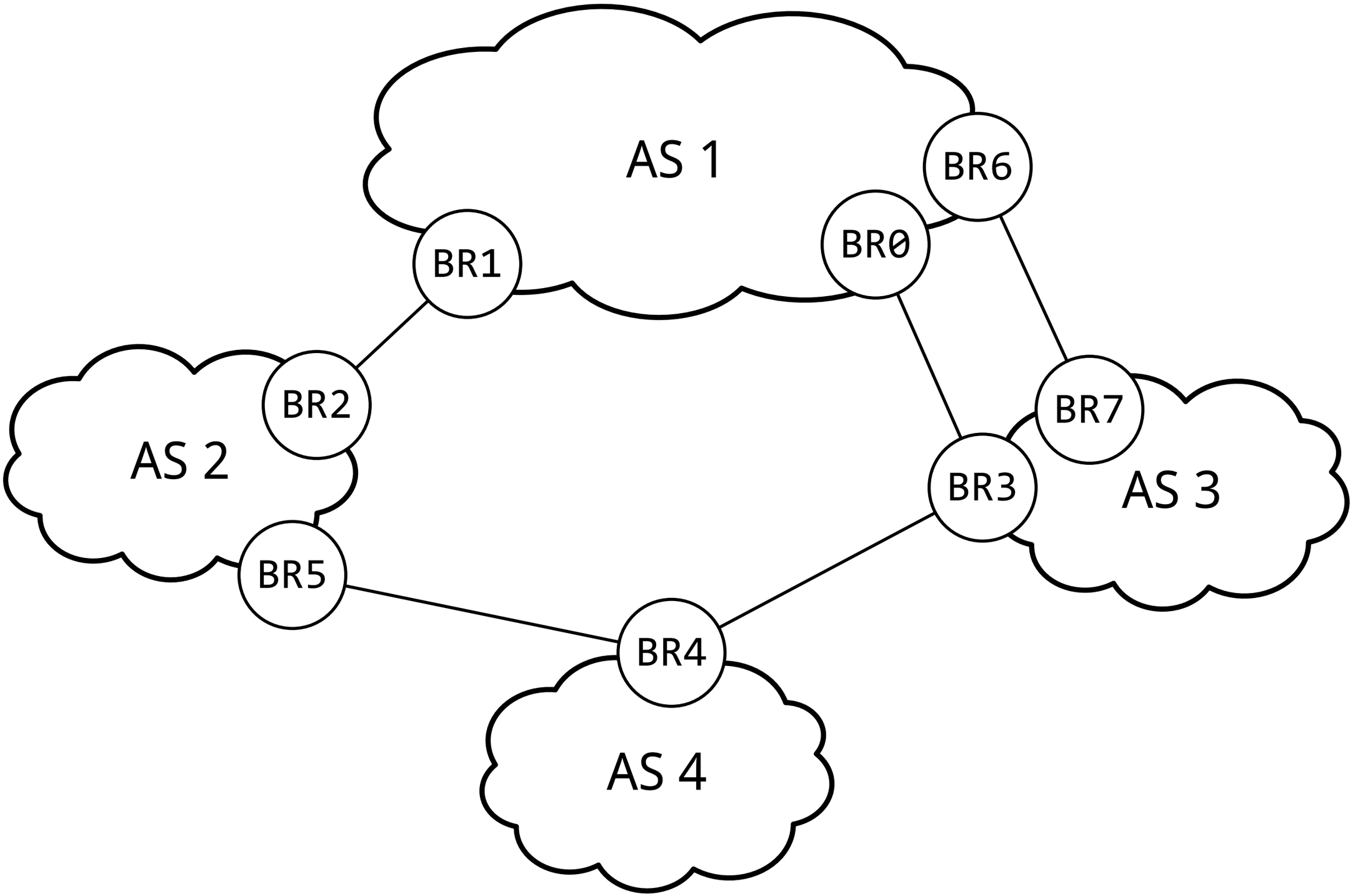


Въпроси

BGP

- Border Gateway Protocol – RFC 4271
- Префикси и пътища
- Автономни системи
  - loop avoidance
- Разликата между interior routing и exterior routing
- Inter-domain routing
- Default-free zone (DFZ)

BGP



BGP

- AS-path
  - from BR3: 203.0.113.0/24 through AS3 AS1 AS2
  - from BR5: 203.0.113.0/24 through AS2

- Best path-selection

- Policies
  - Customer, Peering, Transit

Атаки върху BGP

- Проверка на данните
  - Youtube/pakistani telecom случая
  - leakage
  - SBGP
- DoS върху BGP сесията
- DoS върху рутера

Други

- IS-IS
- EIGRP

Въпроси