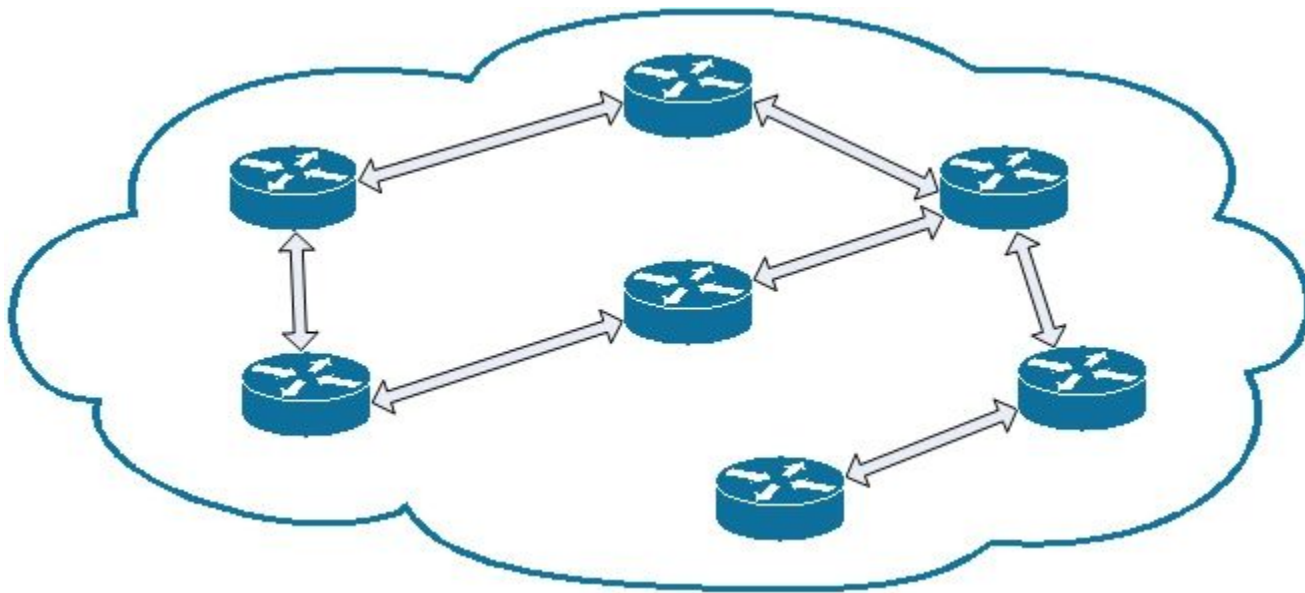
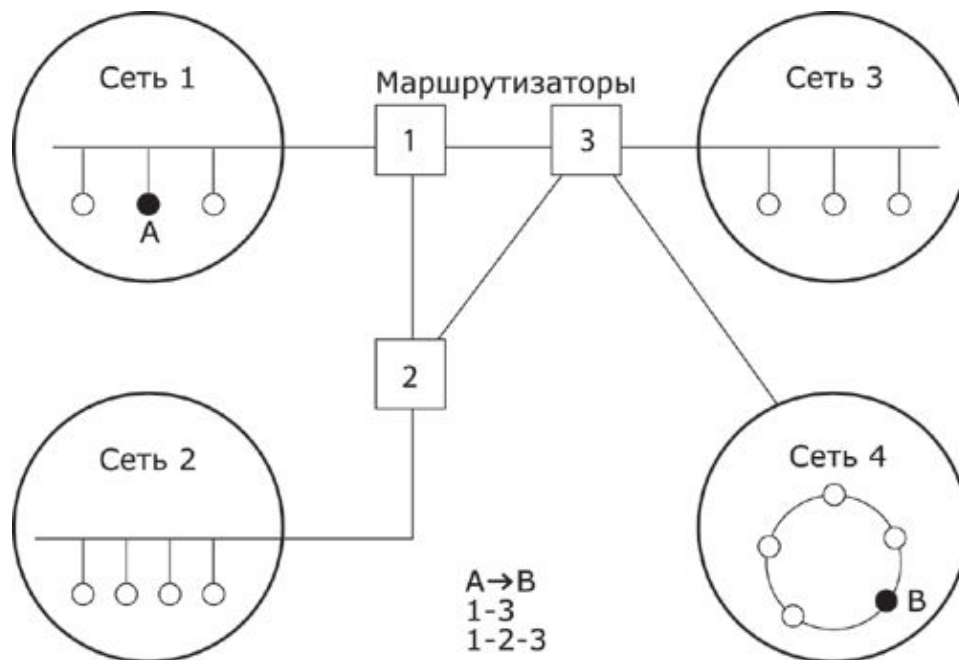


Безопасность на сетевом уровне

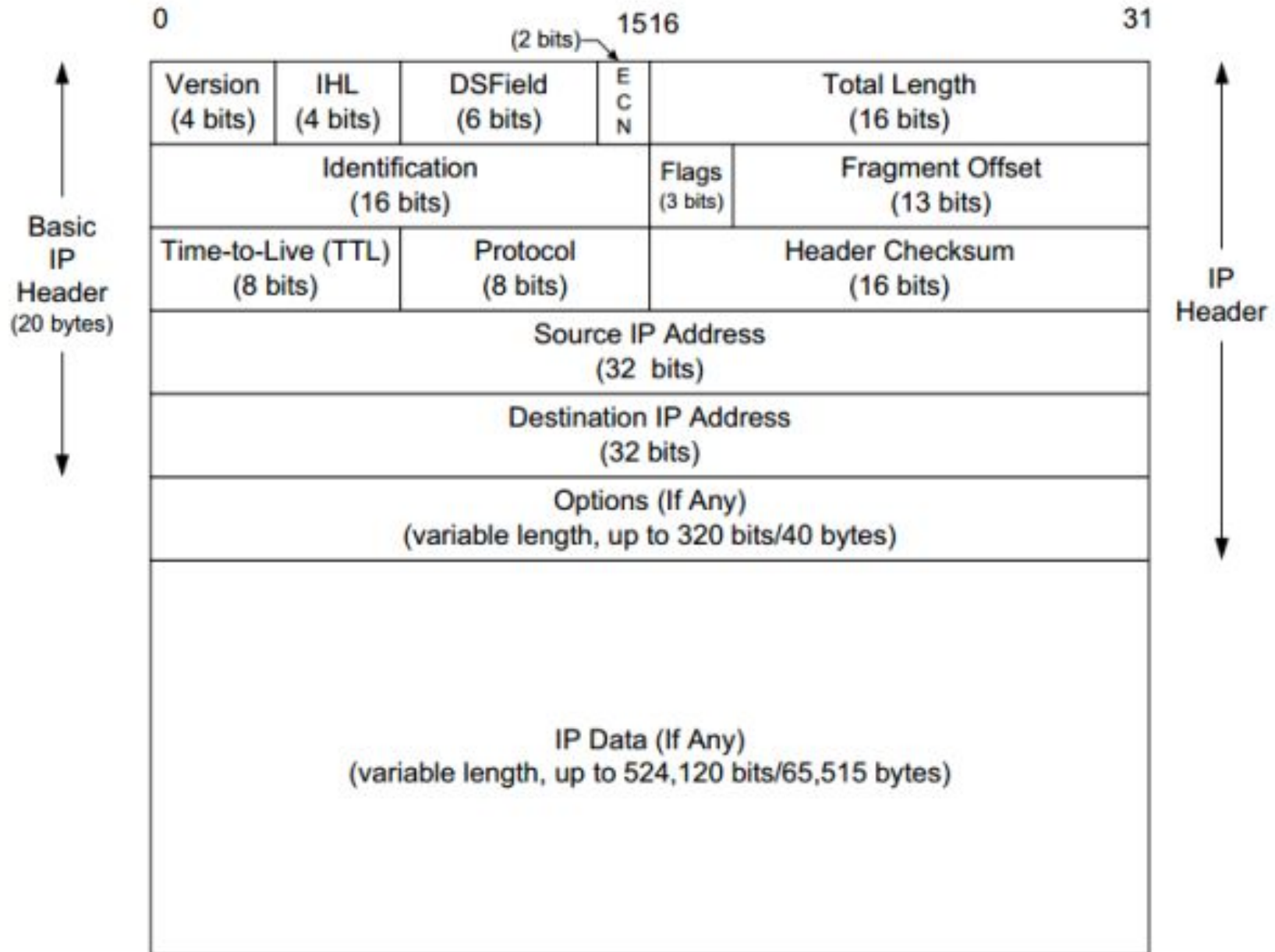


Функции сетевого уровня

- **Сетевой уровень** служит для образования единой системы, объединяющей несколько сетей.
 - Сети могут использовать различные принципы передачи сообщений между конечными узлами.
 - Сети обладают произвольной структурой связей.



IP - основной протокол сетевого уровня



Классы IPv4 адресов

Класс	Диапазон значений 1 октета	Биты первого октета	Части адресов сети (N) и хоста (H)	Маска подсети по умолчанию	Число подсетей и хостов
A	1-127	00000000 – 01111111	N.H.H.H	255.0.0.0	128 сетей (2^7) 16777214 хостов в сети ($2^{24}-2$)
B	128-191	10000000 – 10111111	N.N.H.H	255.255.0.0	16 384 сетей (2^{14}) 65 534 хостов в сети ($2^{16}-2$)
C	192-223	11000000 – 11011111	N.N.N.H	255.255.255.0	2 097 150 сетей (2^{21}) 254 хоста в сети (2^8-2)
D	224-239	11100000 – 11101111	Мультикастовая адресация		
E	240-255	11110000 – 11111111	Экспериментальная адресация		

Адрес 127.0.0.1 – «локальная петля», локальный IP-адрес по-умолчанию

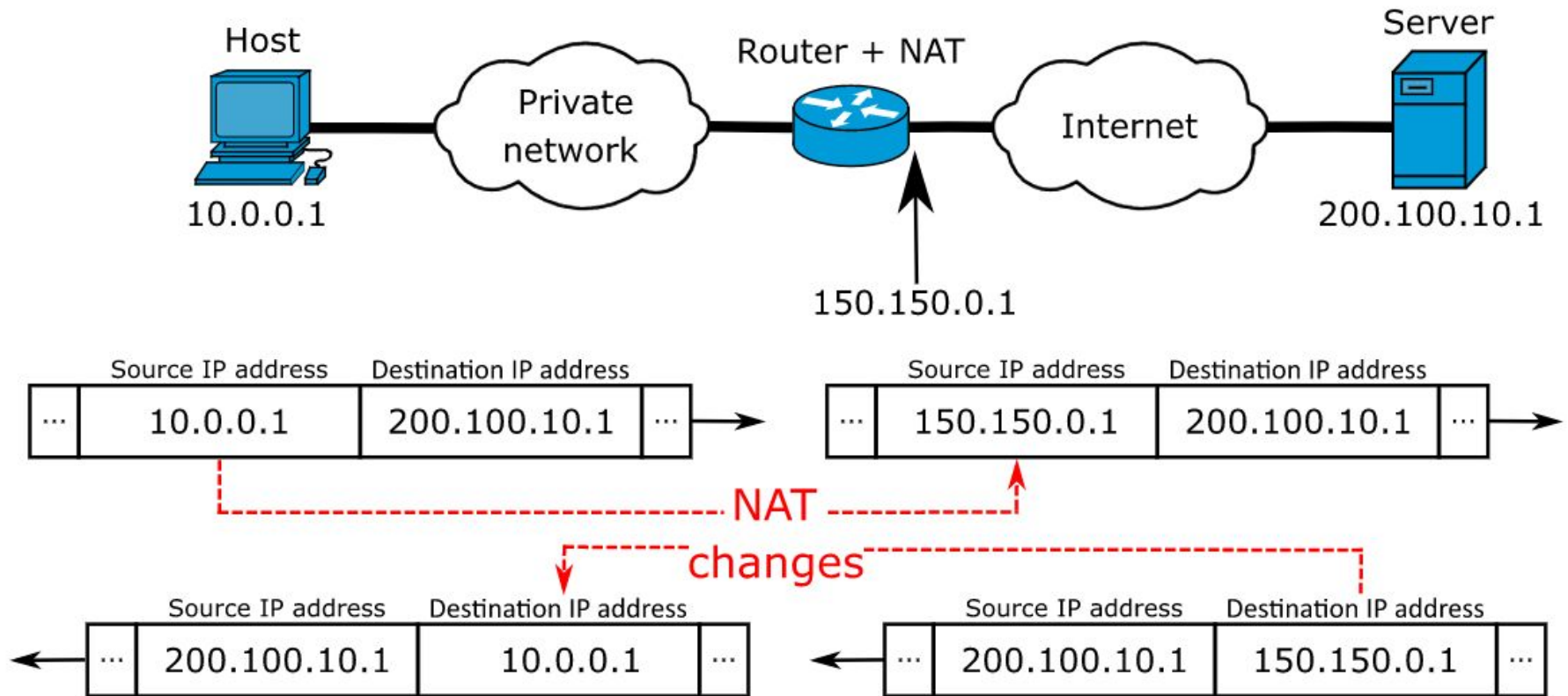
Бесклассовая адресация и маски подсети

				Subnets			Hosts		
	/	Netmask	Block Size	Class A	Class B	Class C	Class A	Class B	Class C
Class A Network	8	255.0.0.0	256	1			16777214		
	9	255.128.0.0	128	2			8388606		
	10	255.192.0.0	64	4			4194302		
	11	255.224.0.0	32	8			2097150		
	12	255.240.0.0	16	16			1048574		
	13	255.248.0.0	8	32			524286		
	14	255.252.0.0	4	64			262142		
	15	255.254.0.0	2	128			131070		
	16	255.255.0.0	256	256	1		65534	65534	
	17	255.255.128.0	128	512	2		32766	32766	
	18	255.255.192.0	64	1024	4		16382	16382	
	19	255.255.224.0	32	2048	8		8190	8190	
Class B Network	20	255.255.240.0	16	4096	16		4094	4094	
	21	255.255.248.0	8	8192	32		2046	2046	
	22	255.255.252.0	4	16384	64		1022	1022	
	23	255.255.254.0	2	32768	128		510	510	
	24	255.255.255.0	256	65536	256	1	254	254	254
	25	255.255.255.128	128	131072	512	2	126	126	126
Class C Network	26	255.255.255.192	64	262144	1024	4	62	62	62
	27	255.255.255.224	32	524288	2048	8	30	30	30
	28	255.255.255.240	16	1048576	4096	16	14	14	14
	29	255.255.255.248	8	2097152	8192	32	6	6	6
	30	255.255.255.252	4	4194304	16384	64	2	2	2

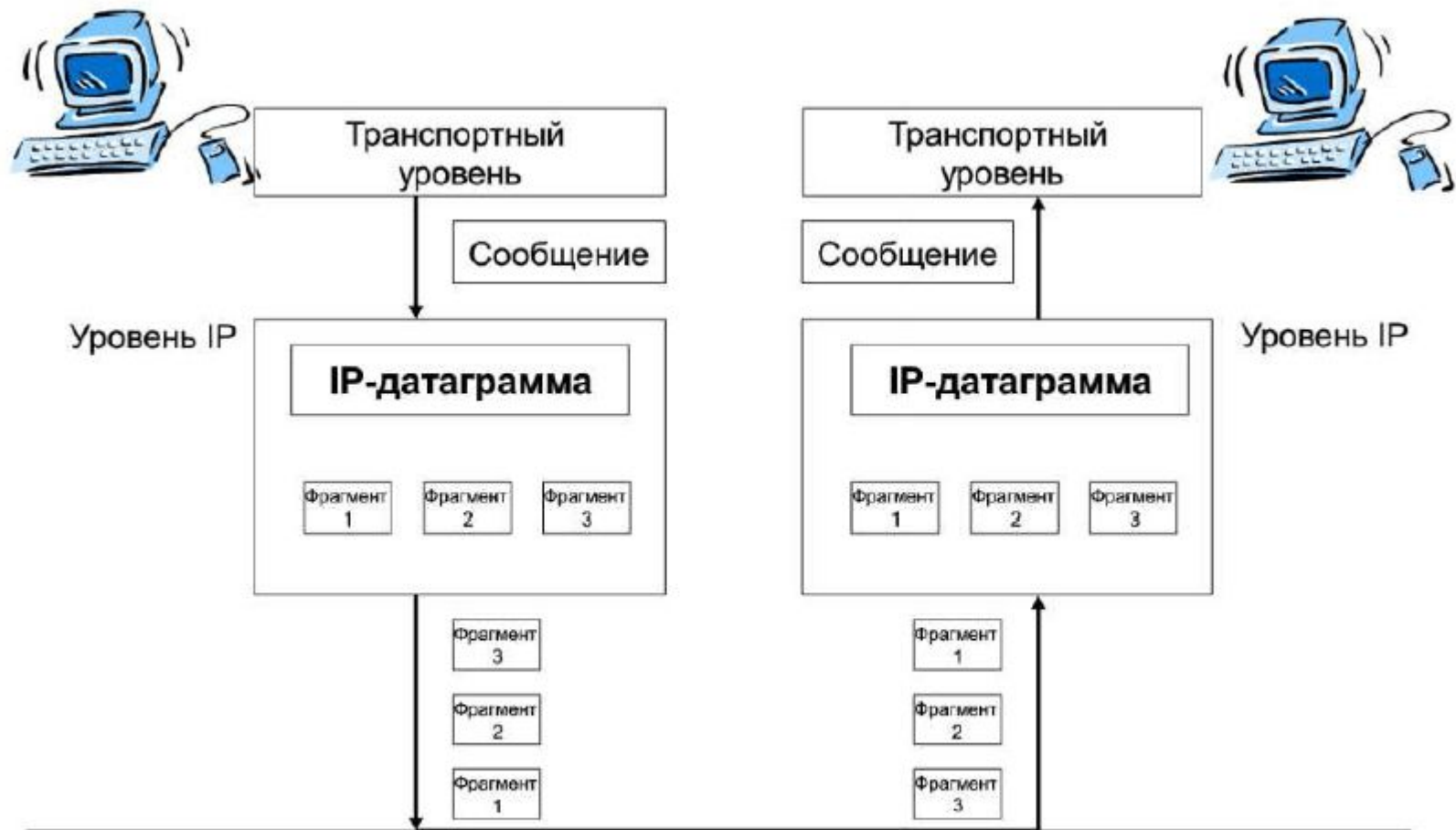
Зарезервированные IP адреса (IANA IPv4 Special-Purpose Address Registry)

Address block	Number of addresses	Description
0.0.0.0/8	16777216	Current network
10.0.0.0/8	16777216	Used for local communications within a private network.
100.64.0.0/10	4194304	Shared address space for communications between a service provider and its subscribers when using a carrier-grade NAT.
127.0.0.0/8	16777216	Used for loopback addresses to the local host.
169.254.0.0/16	65536	Used for link-local addresses between two hosts on a single link when no IP address is otherwise specified, such as would have normally been retrieved from a DHCP server.
172.16.0.0/12	1048576	Used for local communications within a private network.
192.0.0.0/24	256	IETF Protocol Assignments.
192.0.2.0/24	256	Assigned as TEST-NET-1, documentation and examples.
192.88.99.0/24	256	Reserved. Formerly used for IPv6 to IPv4 relay
192.168.0.0/16	65536	Used for local communications within a private network.
198.18.0.0/15	131072	Used for benchmark testing of inter-network communications between two separate subnets.
198.51.100.0/24	256	Assigned as TEST-NET-2, documentation and examples.
203.0.113.0/24	256	Assigned as TEST-NET-3, documentation and examples.
224.0.0.0/4	268435456	In use for IP multicast. (Former Class D network.)
233.252.0.0/24	256	Assigned as MCAST-TEST-NET, documentation and examples.
240.0.0.0/4	268435455	Reserved for future use. (Former Class E network.)
255.255.255.255/32	1	Reserved for the "limited broadcast" destination address

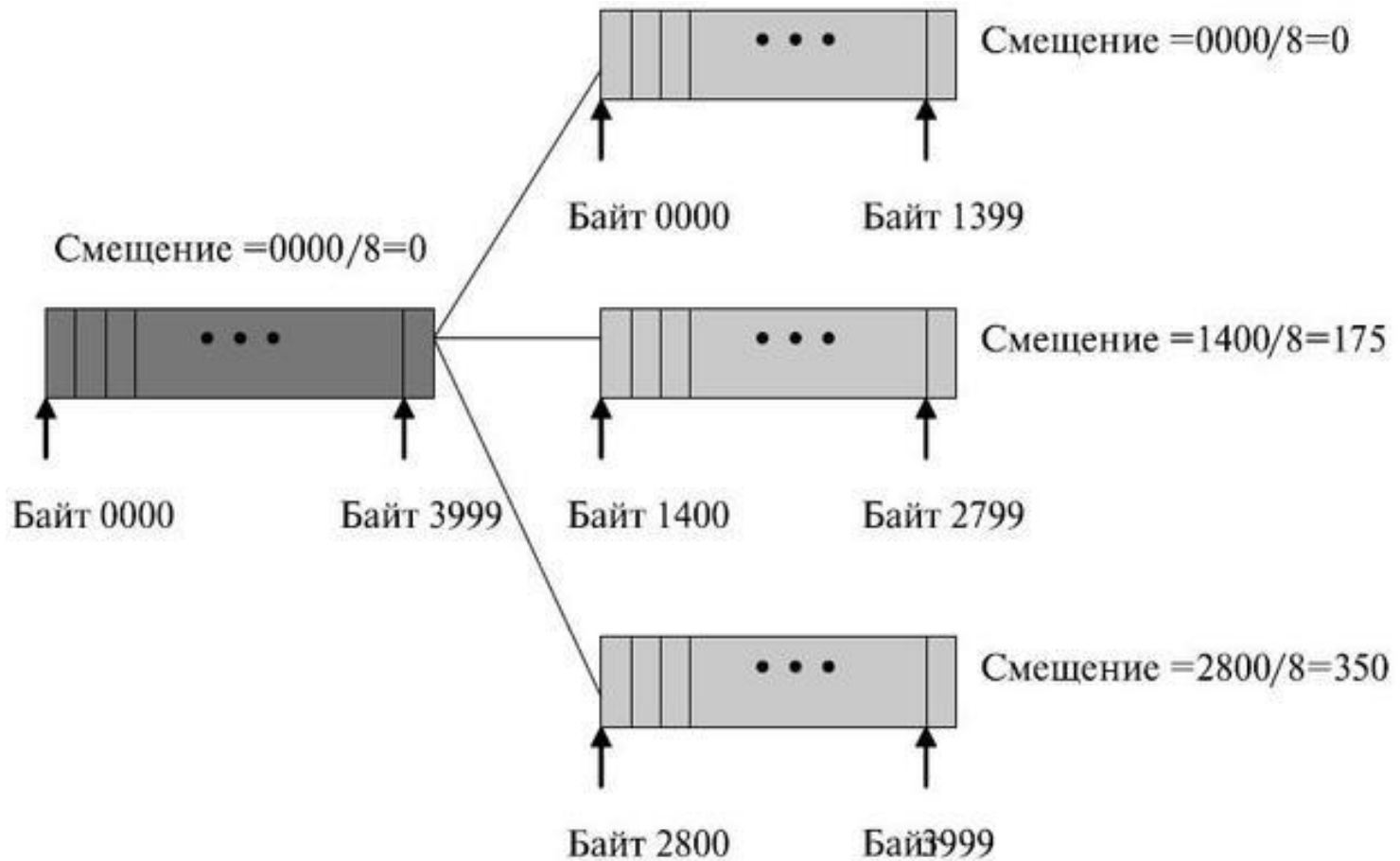
Механизм трансляции адресов NAT



Фрагментация IP пакетов



Пример фрагментации



Заголовки IPv4 и IPv6





IPv4 Header

Version	IHL	Type of Service	Total Length	
Indentification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options			Padding	

IPv6 Header

Version	Traffic Class	Flow Label		
Payload Length			Next Header	Hop Limit
Source Address				
Destination Address				

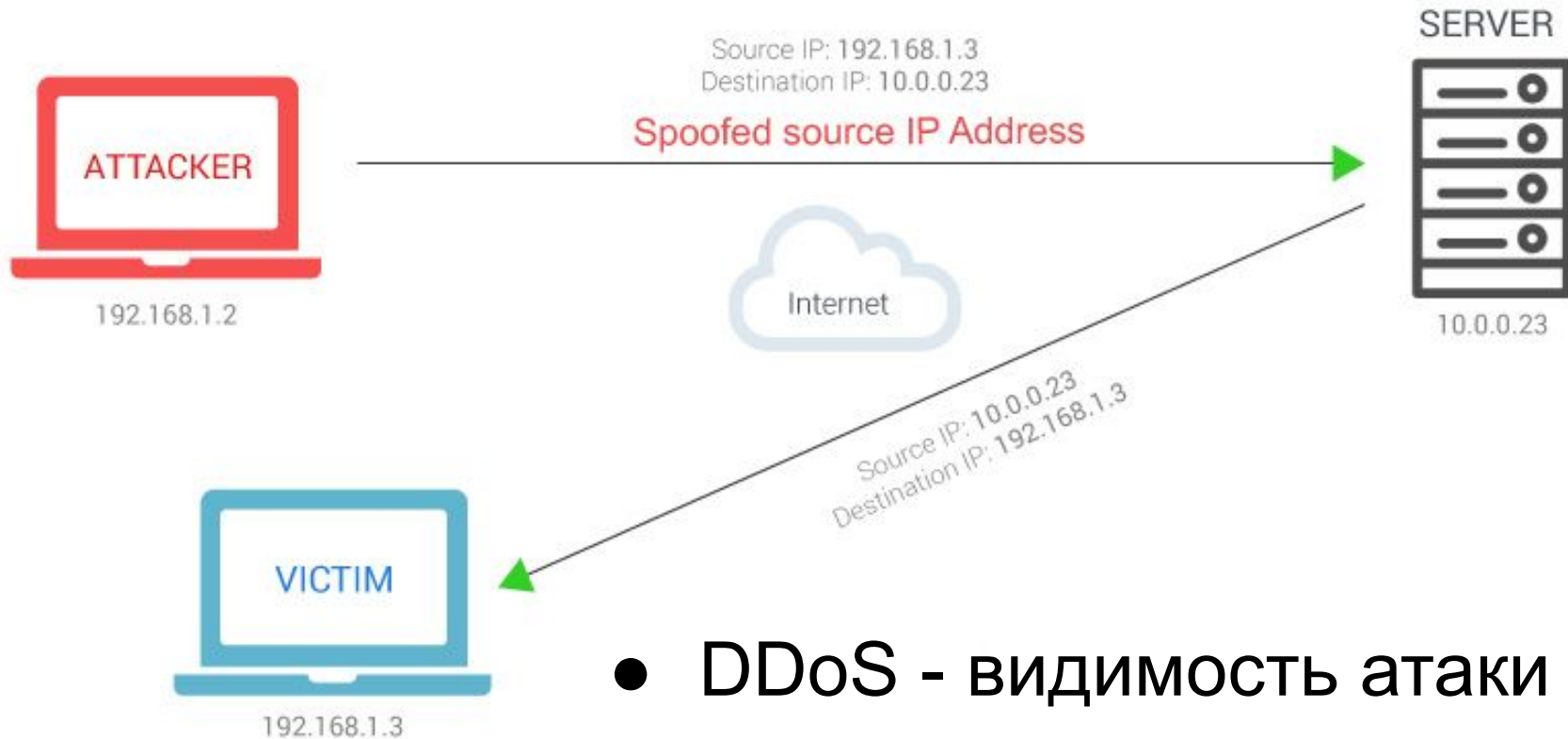
Legend

	- Field names kept from IPv4 to IPv6
	- Fields not kept in IPv6
	- Name & position changed in IPv6
	- New field in IPv6

Сравнение версий протокола IP

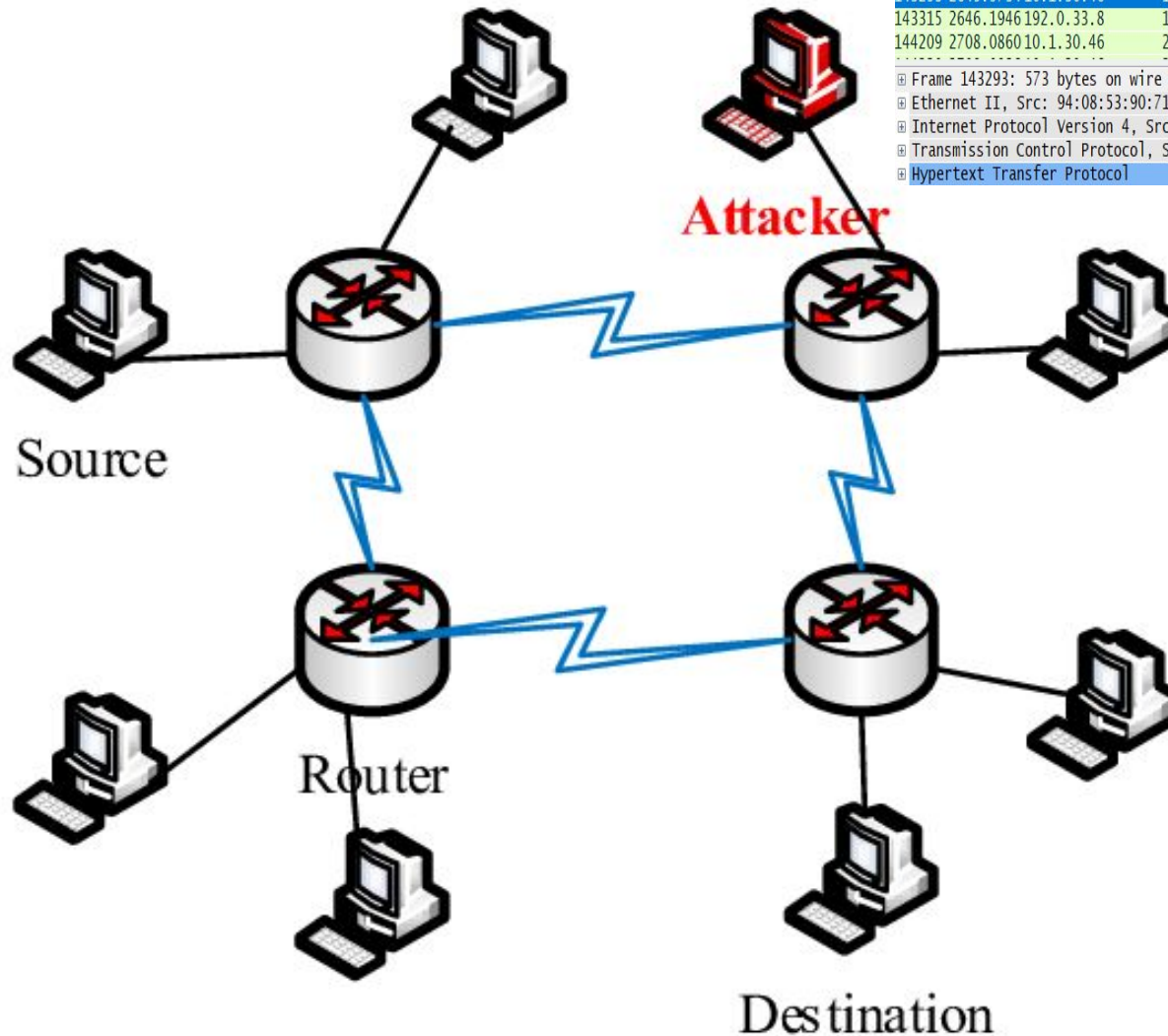
Критерий сравнения	IPv4	IPv6
Адресное пространство	Адрес - 32 бит $2^{32} = 4\,294\,967\,296$ адресов	Адрес - 128 бит $2^{128} = 3,4 \cdot 10^{38}$ адресов
Формат адреса	Десятичный: 192.168.1.1	Шестнадцатеричный: : 2001:0db8:85a3:0000:0000:8a2e:0370:7334 или 2001:db8:85a3::8a2e:370:7334
Конфигурация интерфейса	Необходима настройка (вручную или по DHCP)	Автоконфигурация SLAAC (возможна конфигурация по DHCPv6)
Фрагментация	Возможна на любом узле на маршруте пакета	Возможна только на отправителе (поля вынесены в расширенный заголовок)
Типы адресов	Unicast, Multicast, Broadcast	Unicast, Multicast, Anycast (адресует любого члена группы)
NAT (трансляция сетевых адресов)	Применяется повсеместно для экономии адресов	Необходимость в NAT отсутствует
Безопасность	Не поддерживает шифрование и аутентификацию	IPSEC встроен: шифрование доступно без стороннего ПО

IP-spoofing



- DDoS - видимость атаки из разных источников.
- Обход аутентификации на основе IP.

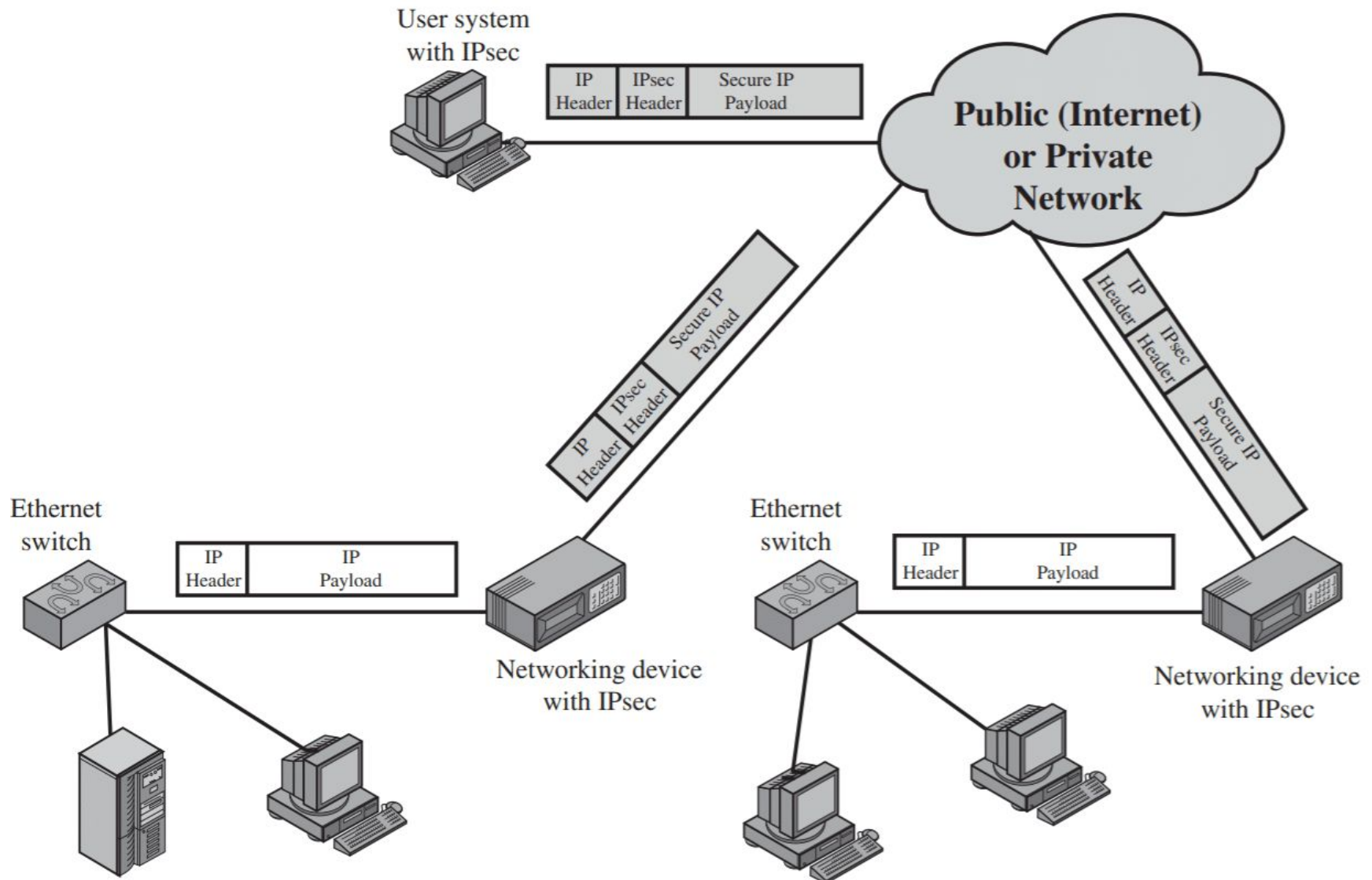
Перехват трафика на сетевом уровне



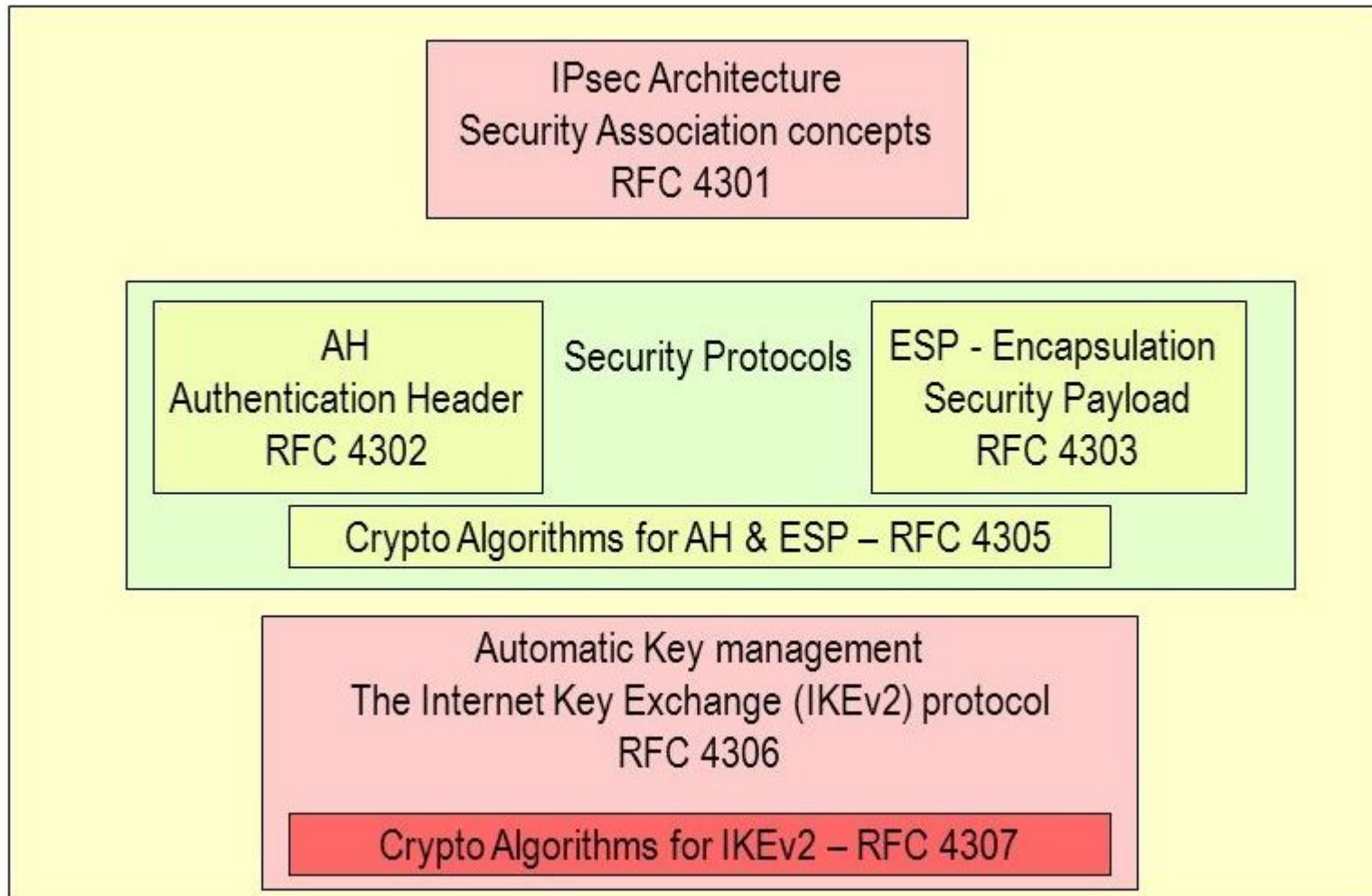
Filter: http		Expression...		Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info
142749	2590.1031	10.1.30.46	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
142750	2591.1036	10.1.30.46	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
143293	2645.9734	10.1.30.46	192.0.33.8	HTTP	573	GET /assignments/service-names-pd
143315	2646.1946	192.0.33.8	10.1.30.46	HTTP	1386	HTTP/1.1 200 OK (text/html)
144209	2708.0860	10.1.30.46	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 143293: 573 bytes on wire (4584 bits), 573 bytes captured (4584 bits) on interface 0
Ethernet II, Src: 94:08:53:90:71:0b (94:08:53:90:71:0b), Dst: 50:ff:20:1d:17:6c (50:ff:20:1d:17:6c)
Internet Protocol Version 4, Src: 10.1.30.46 (10.1.30.46), Dst: 192.0.33.8 (192.0.33.8)
Transmission Control Protocol, Src Port: 50264 (50264), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 519
Hypertext Transfer Protocol

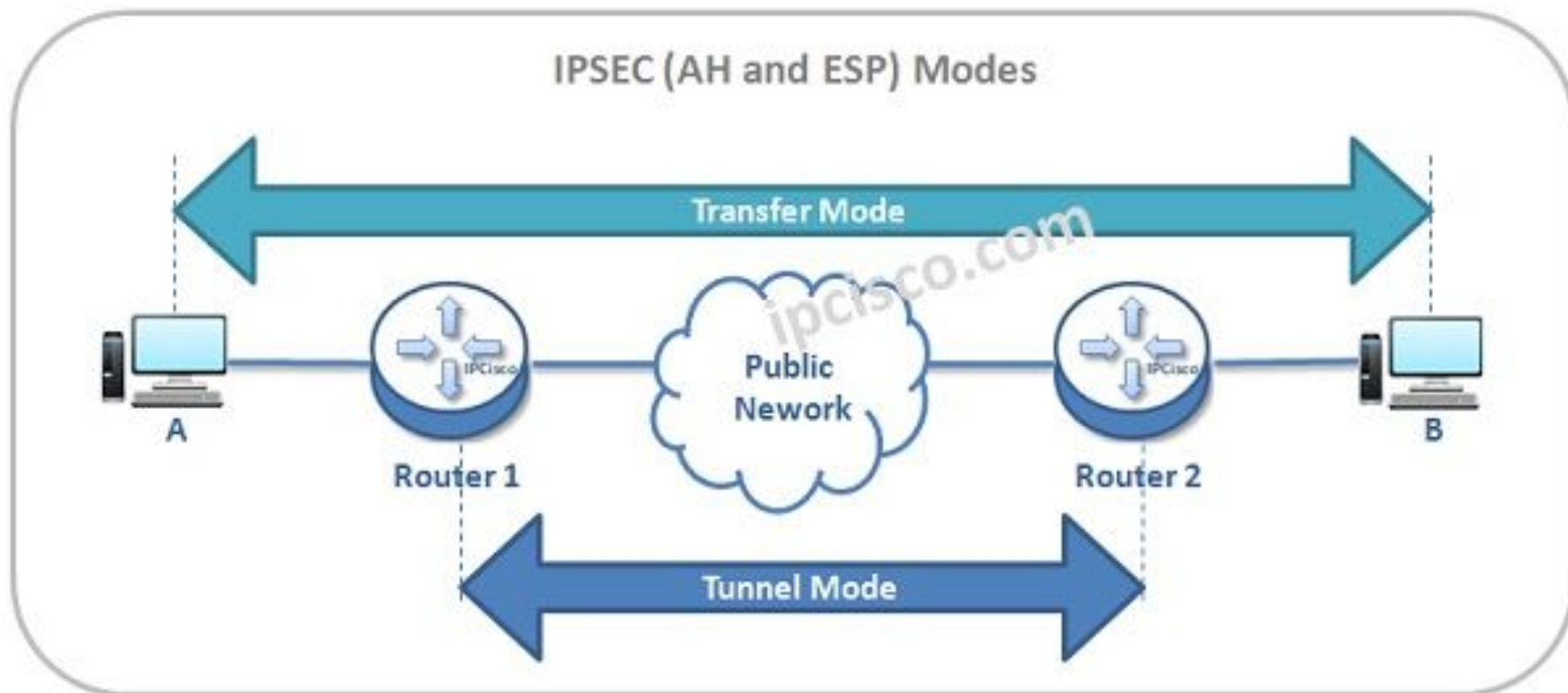
Защищенное сетевое взаимодействие на примере IPsec



IPSEC – архитектура



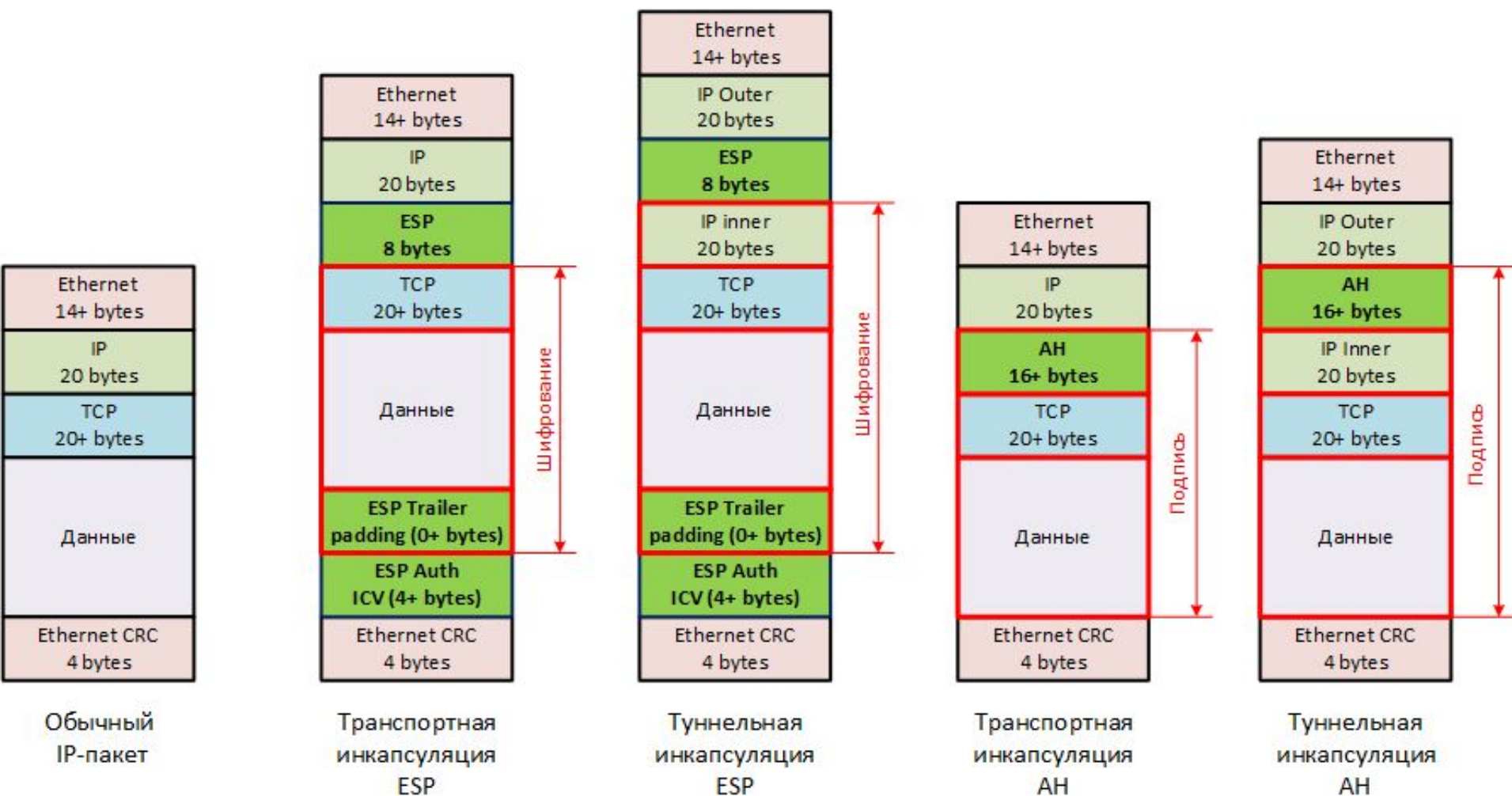
Режимы работы IPSEC



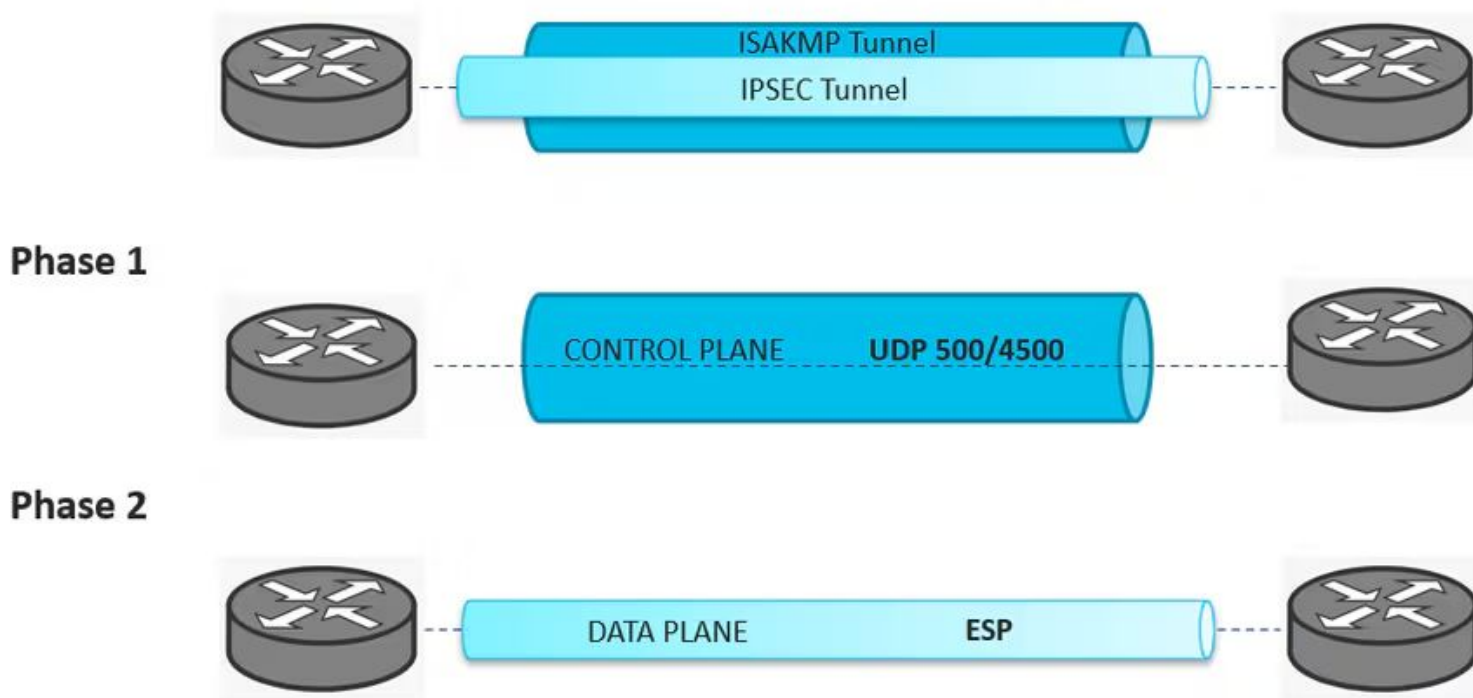
Транспортный режим - шифрует только данные. Используется для соединения между хостами, либо для защиты других туннельных протоколов (L2TP)

Туннельный режим - шифрует пакет целиком. Используется для организации виртуальных частных сетей (VPN)

Заголовки IPSEC



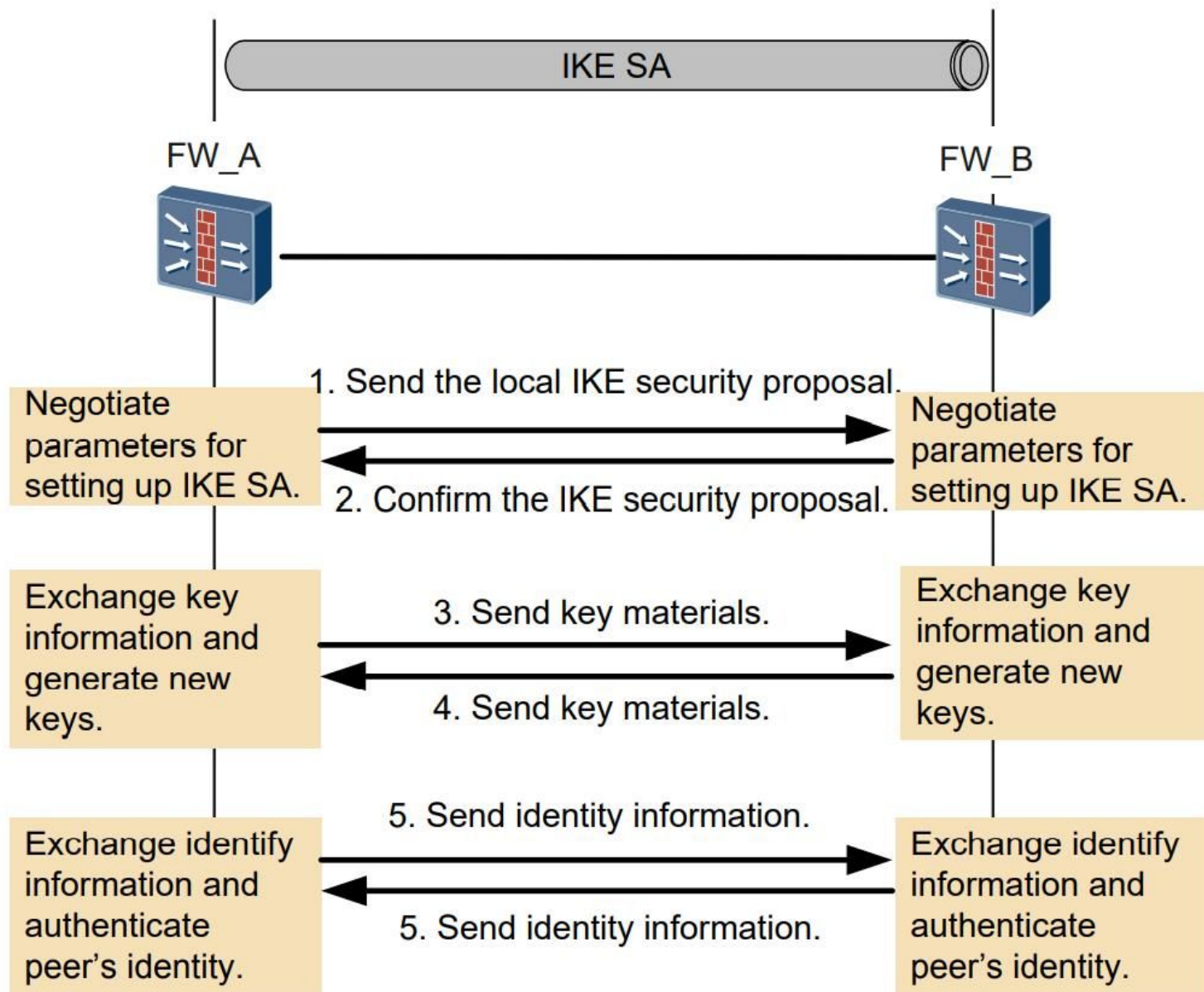
Фазы обмена данными IKE



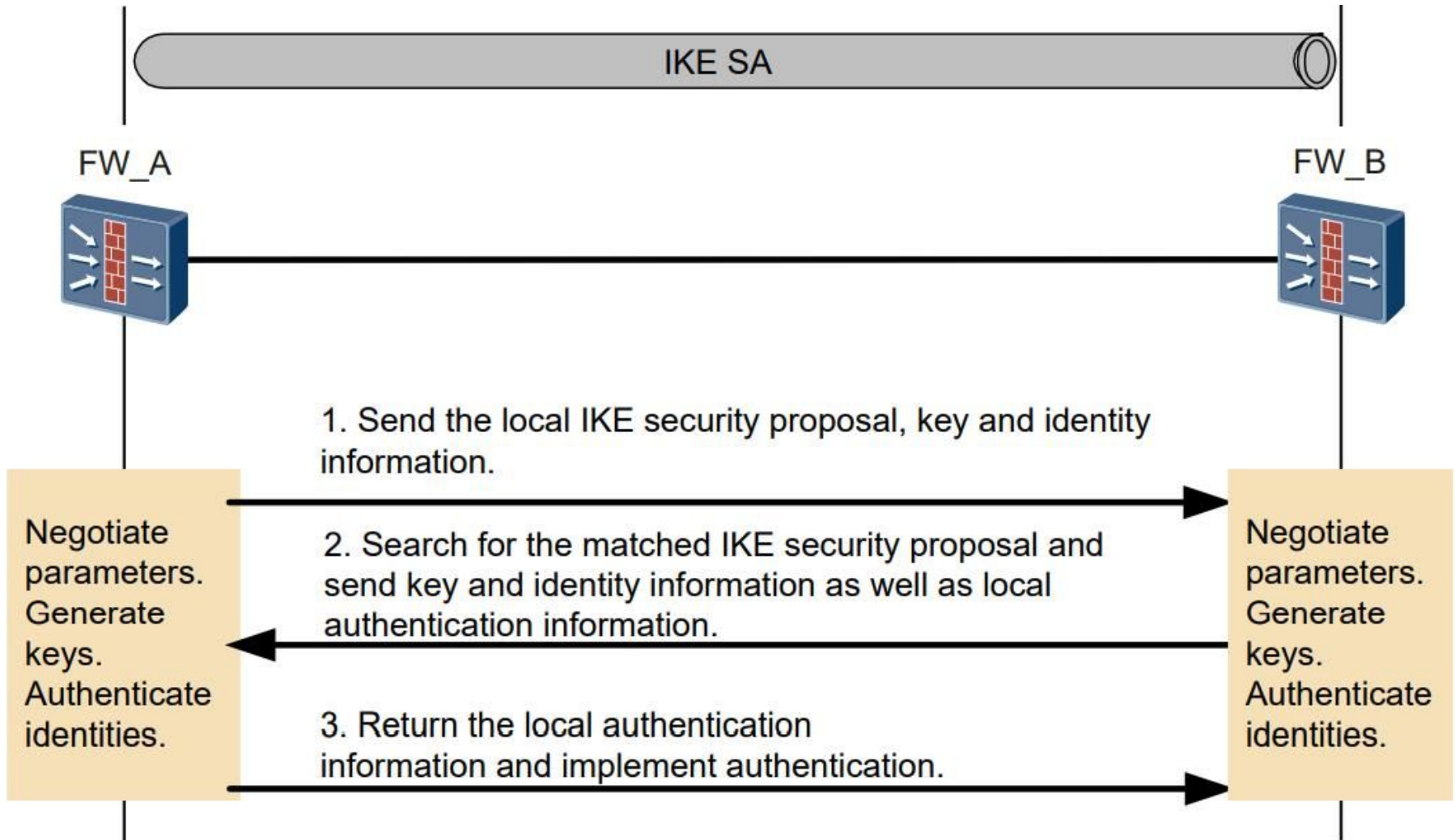
Phase-1: Согласовывается защита самого IKE (ISAKMP tunnel)

Phase-2: Согласовывается защита IPsec. Получение данных из первой фазы для формирования ключей сессии

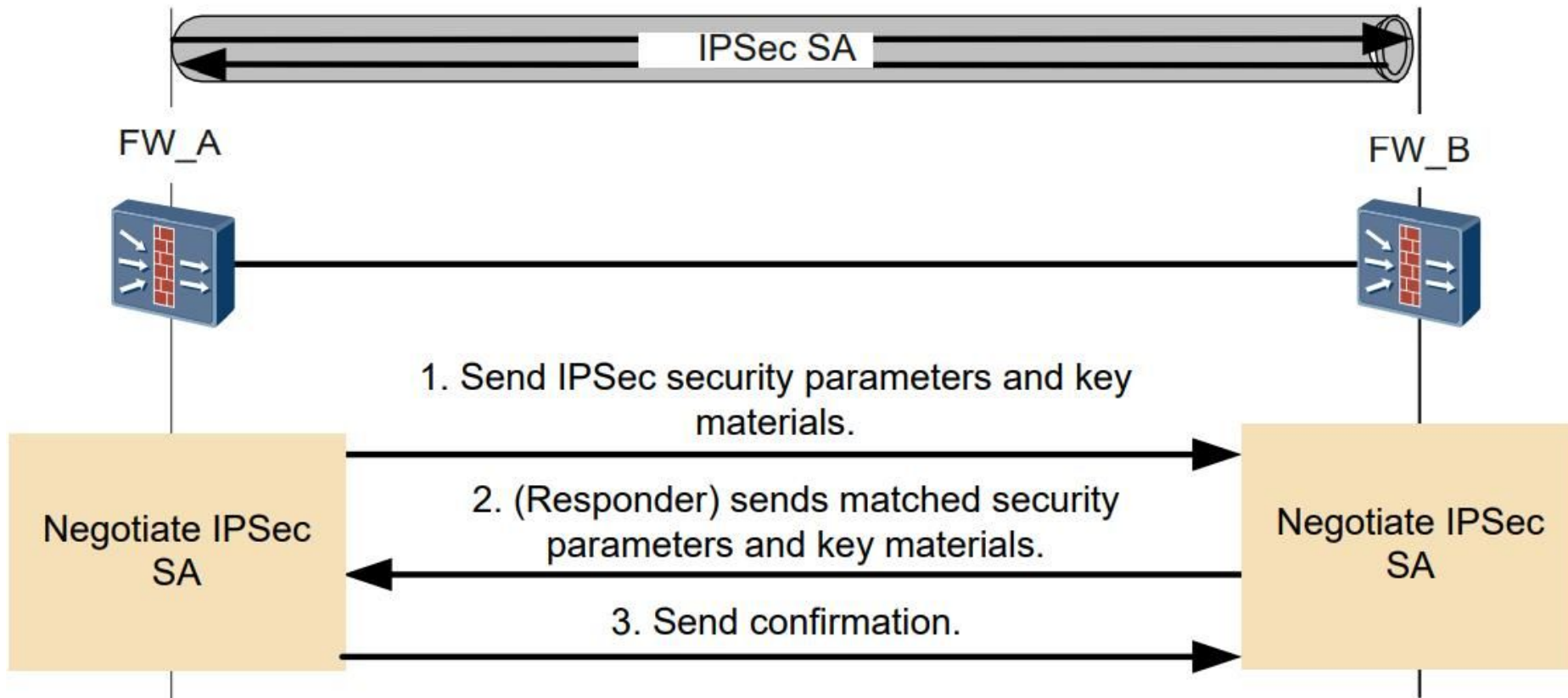
IKE Фаза 1 (Main mode)



IKE Phase 1 (Aggressive mode)



IKE Фаза 2 (Quick mode)



Определение трафика для туннелирования



```
access-list 101 permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

Access lists determine traffic to encrypt

- Permit—traffic must be encrypted
- Deny—traffic sent unencrypted

Протокол ICMP

- **ICMP** – протокол межсетевых управляющих сообщений
- Используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных

IP-датаграмма

	Биты 0-7	Биты 8-15	Биты 16-23	Биты 24-31
IP-заголовок (20 байт)	Версия/IHL	Тип сервиса	Длина	
	Идентификация		флаги и смещение	
	Time To Live (TTL)	Протокол	Контрольная сумма	
	IP-адрес источника			
	IP-адрес получателя			
ICMP-заголовок (8 байт)	Тип сообщения	Код	Контрольная сумма	
	Данные заголовка			
Полезная нагрузка ICMP (опционально)	Данные полезной нагрузки			

Т	К	Назначение
0	0	Эхо-ответ
3	1	Хост недоступен
	2	Сеть недоступна
	3	Порт недоступен
5	0	Перенаправление в сеть
	1	Перенаправление к узлу
8	0	Эхо-запрос
11	0	TTL истекло при передаче
12	0	Ошибка в заголовке
	1	Отсутствует опция
	2	Неверная длина

Smurf attack



Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol=ICMP		Header Checksum	
Адрес объекта атаки				
Адрес сети или широковещательный				
Options				Padding

Атака ICMP redirect (навязывание маршрута)

