Архитектура компьютерных сетей

Останков Александр Иванович

План курса

1. Введение в компьютерные сети
2. Основные методы построения СПД
3. **Архитектура Internet Protocol Suite (TCP/IP)**
    - 3.1. Адресация в IP сетях
    - 3.2. Протокол IP (v4)
    - 3.3. Протокол ARP
    - 3.4. Служебный трафик и протокол ICMP
4. Архитектура модулей физического уровня
5. Технологии беспроводных сетей
6. Архитектура модулей канального уровня
7. Протоколы транспортного уровня
8. Технологии WWW

Internet Protocol Suite (IPS)

Internet Protocol Suite – совокупность средств и методов, посредством которых реализовано большинство современных компьютерных сетей, от маленьких домашних до глобальной сети Internet. TCP/IP – это просто альтернативное и менее точное название IPS.

IPS был создан в результате открытого процесса стандартизации, изобретенного в проекте ARPAnet, поэтому все документы, касающиеся устройства IPS бесплатно доступны в виде RFC (STF, FYI, BCP, Informational). Процесс стандартизации продолжается до сих пор. IETF (Internet Engineering Task Force) – это Standard Body Organization для IPS.

В рамках IPS разработано и стандартизовано множество различных протоколов (более 2800 STD RFC). Кроме того, в составе протокольных стеков IPS успешно функционирует множество протоколов и интерфейсов, стандартизованных другими Standard Bodies (IEEE, ITU, ISO, IEC…), поэтому **IPS** это больше чем набор протоколов - **это наиболее развитая глобальная сетевая архитектура**.

Центральную роль в архитектуре IPS играет **Internet Protocol (IP).**

Что такое Internet ?

- ✓ Всемирная компьютерная сеть общего пользования (Internet)
- ✓ Способ построения компьютерных сетей в виде inter-network (сокращенно internet): совокупность отдельных сетей (networks), объединенных друг с другом при помощи межсетевых устройств, функционирующая как единая сеть. Internet – это тоже internet (internetwork).
- ✓ Термин сеть (network) в IPS используется для обозначения звена передачи данных (link)

Что такое Network (с точки зрения IPS)

Коммуникационная система (среда), позволяющая двум или более узлам передавать напрямую друг другу пакеты(кадры).

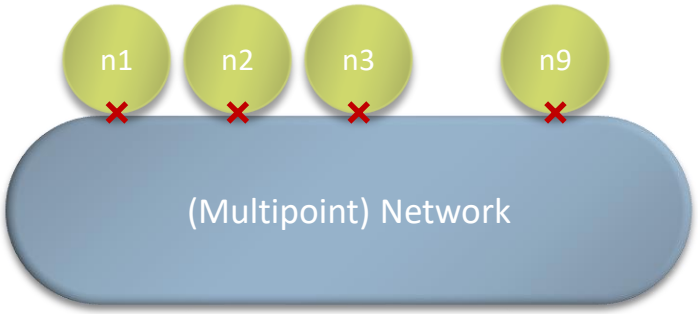
Простейший вариант: двухточечная сеть:

Интерфейс - точка **присоединения узла к сети**.

Все пакеты (кадры), отправляемые узлом n1, доставляются к интерфейсу узла n2 и наоборот.

Возможен дуплексный режим при котором прием пакета (кадра) от соседнего узла может вестись одновременно с передачей пакета (кадра) на соседний узел.

Многоточечная сеть и режимы передачи

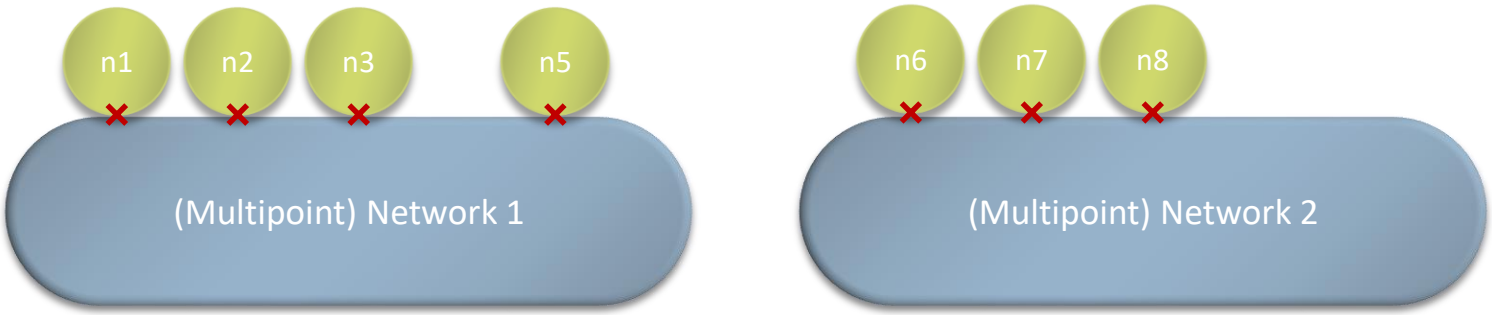


Любой из узлов многоточечной сети имеет возможность послать пакет (кадр) в сеть в одном из трех режимов:

- Широковещательном (broadcast) – такой пакет (кадр) должен быть доставлен к интерфейсам всех узлов, подключенных к сети в данный момент
- Однонаправленном (unicast) – такой пакет (кадр) должен быть доставлен лишь к интерфейсу одного конкретного узла.
- Групповом (multicast) – такой пакет должен быть доставлен некоторому подмножеству узлов, включенных в группу

В последних двух режимах отправитель должен обозначить адресата пакета (кадра), указав номер(адрес) узла-адресата, либо код группы узлов-получателей

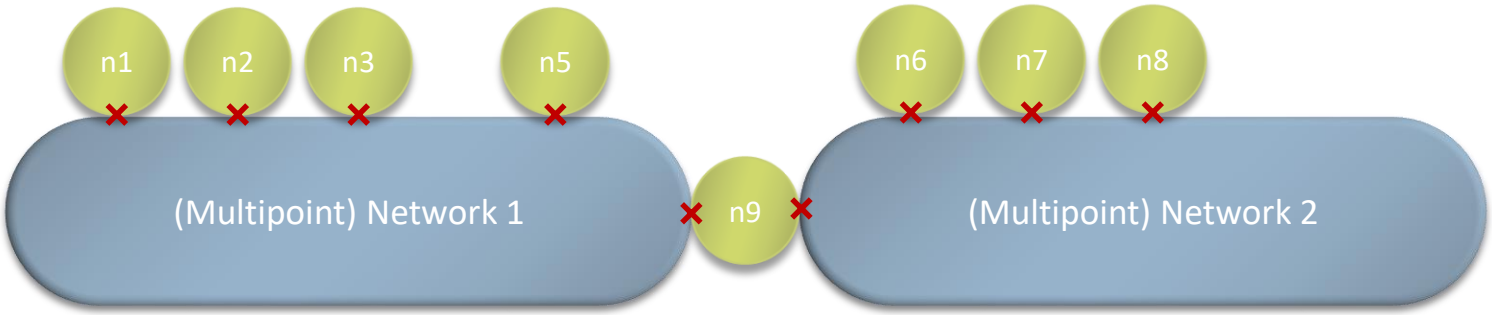
Объединение сетей (internetworking)



Сети *Network 1* и *Network 2* изолированы друг от друга и поэтому узел ***n3*** не имеет возможности общаться с узлами ***n6, n7*** и ***n8,*** поскольку они не являются соседями (neighbors).

Превратить две изолированные сети в одну большую сеть не всегда целесообразно/возможно, однако для обеспечения *connectivity* можно организовать internetwork.

Объединение сетей (internetworking)



- При организации *internetwork* объединяемые сети сохраняют свою изначальную изолированность: ***n3*** и ***n6*** по прежнему не могут отправлять пакеты напрямую друг другу и не становятся соседями (neighbors).
- Узел ***n9*** подключается по двум изолированным интерфейсам к обоим сетям.
- Возможность передачи пакетов (кадров) между узлами разных сетей не напрямую, а через шлюз (gateway) ***n9*** по маршруту:

n3 *->* *Network 1* *->* ***n9*** *->* *Network 2* *->* ***n6***

Термины, применяемые в IPS

Host (узел) – (ПК, сервер, гаджет и т.п.), подключенный к сети

Interface (интерфейс) – точка подключения **узла к сети**

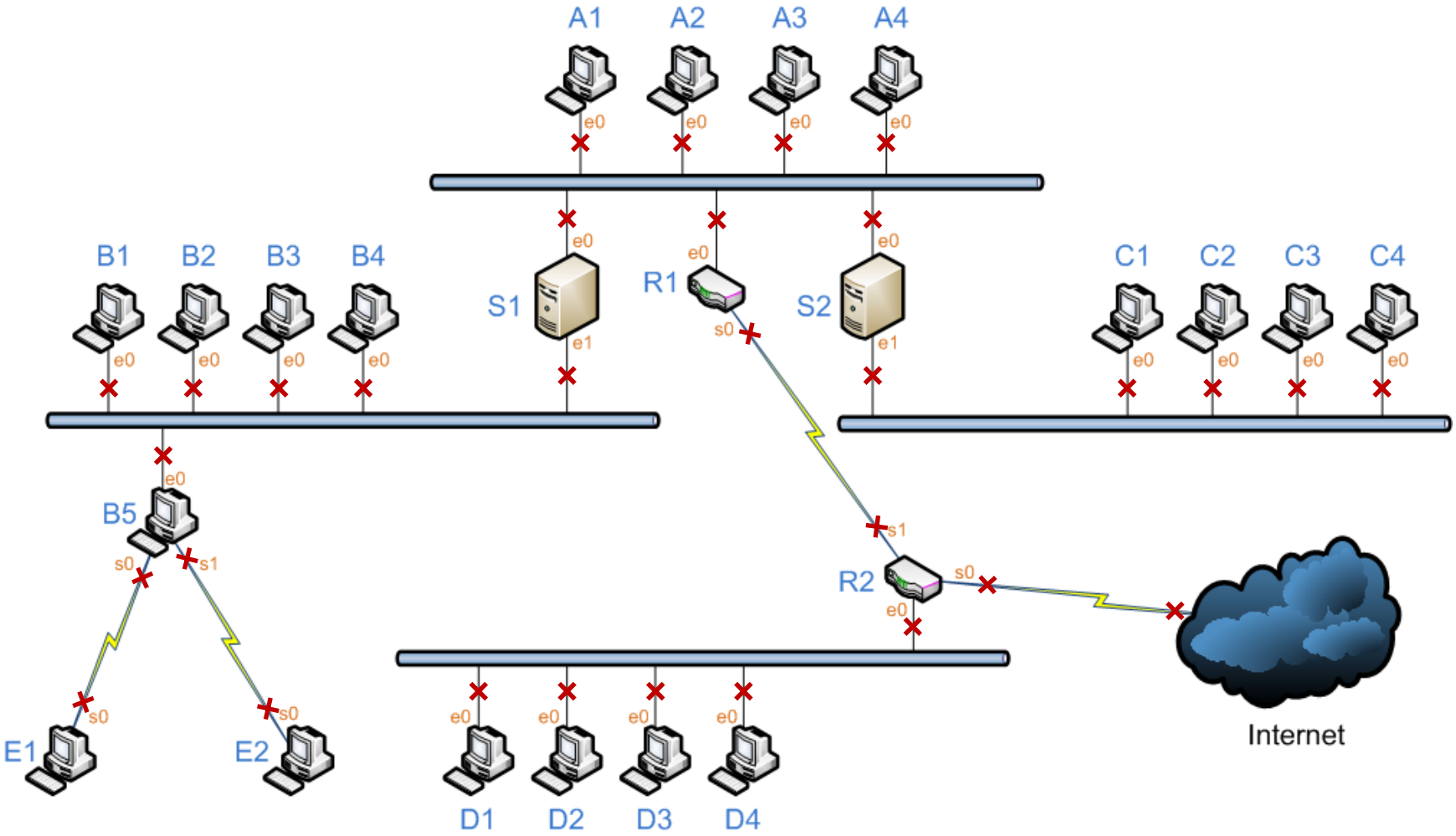
Multihomed host – узел сети, укомплектованный несколькими сетевыми интерфейсам

Gateway (шлюз) – multihomed host, подключенный к нескольким различным сетям и способный осуществлять транзит пакетов между своими интерфейсами

Neighbors (соседи) – множество узлов, непосредственно подключенных к сетям, в которых данный узел имеет интерфейсы

Hop (прыжок) – действие по прямой передаче пакета (кадра) между соседними узлами

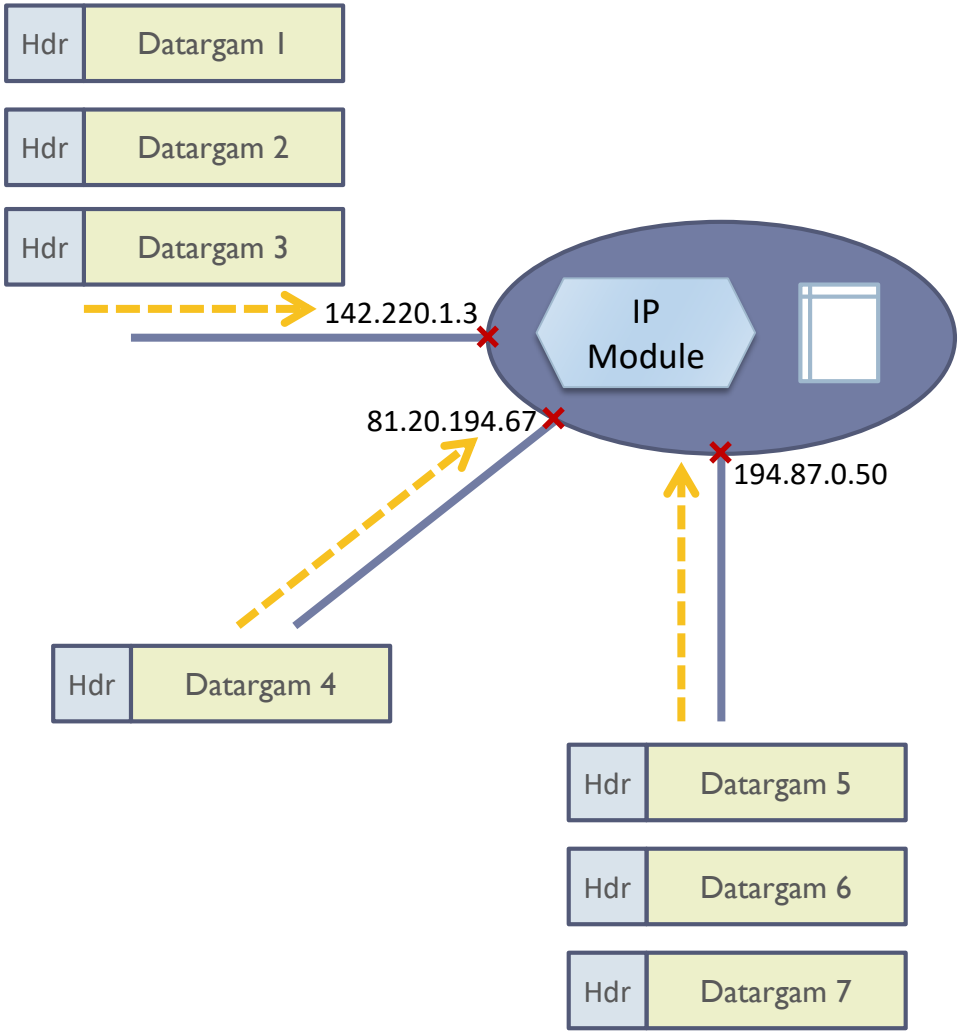
Пример интерсети



Основные принципы работы internetwork

- Трафик объединенной сети (internetwork) складывается из передачи множества отдельных пакетов - IP дейтаграмм.
- IP дейтаграмма – это порция произвольных данных (набор байтов), снабженная служебной этикеткой – IP заголовком.
- На каждом узле объединенной сети функционирует модуль протокола IP, которому по очереди доставляются все принятые узлом дейтаграммы. Анализируя служебные заголовки, IP модули определяют что следует сделать с очередной дейтаграммой: доставить на транспортный уровень, отправить на соседний узел или сбросить.
- Действие и направление передачи выбираются каждым IP модулем самостоятельно на основании значения адреса получателя (destination address), указанного узлом-отправителем в заголовке дейтаграммы. Таким образом, дейтаграммы «путешествуют» по сети от одного узла к другому.
- Для нормальной работы в объединенной сети **каждому интерфейсу** должен быть назначен **различимый IP адрес**.

Коммутация IP пакетов



IP модуль:

- Обрабатывает входящие пакеты друг за другом в порядке их поступления (по одному за раз)
- (для каждого пакета) определяет предпринимаемое действие по IP адресу назначения (Dst-IP) из заголовка пакета
  - Передать пакет вышестоящему протоколу (*адрес достигнут*)
  - Передать напрямую соседу (*адрес соседа*)
  - Перенаправить для дальнейшего принятия решения на сосед-шлюз

План курса

1. Введение в компьютерные сети
2. Основные методы построения СПД
3. **Архитектура Internet Protocol Suite (TCP/IP)**
    - **3.1. Адресация в IP сетях**
    - 3.2. Протокол IP (v4)
    - 3.3. Протокол ARP
    - 3.4. Служебный трафик и протокол ICMP
4. Архитектура модулей физического уровня
5. Технологии беспроводных сетей
6. Архитектура модулей канального уровня
7. Протоколы транспортного уровня
8. Технологии WWW

Структура IP адресов (версии 4)

IP адрес (v4) – это целое 32-битное двоичное число, например:

11000000101010000000000100000001 = 3232235777
10000001001000001100001001011010 = 2166407770

Всего существует 2^{32} возможных IP адресов или 4 GiB (4 294 967 296 комбинаций)

Для записи IP адресов применяют комбинированную октетно-десятичную нотацию: 32-битный код разбивают на 4 байта (октета) и содержимое каждого из них по отдельности переводят в десятичное число. В итоге получается:

11000000 10101000 00000001 00000001 = 192.168.1.1
10000001 00100000 11000010 01011010 = 81.20.194.90

Каждый байт по отдельности может содержать целое число от 0 до 255 (2^8-1), поэтому весь диапазон возможных IP адресов (от минимального адреса, состоящего из 32 двоичных нулей, до максимального адреса из 32 двоичных единиц) составляет: 0.0.0.0 ÷ 255.255.255.255

Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

0.0.0.0

Арифметика IP адресов (версии 4)

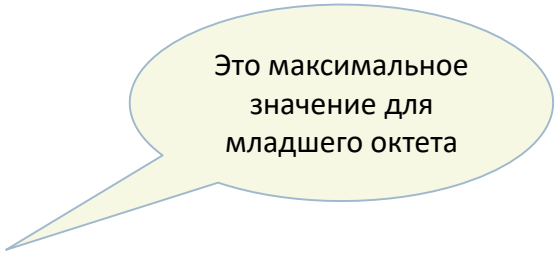
IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

0.0.0.0
0.0.0.1
0.0.0.2
……..

Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

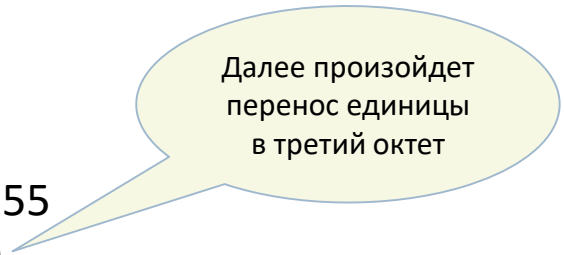
0.0.0.0
0.0.0.1
0.0.0.2
……..
0.0.0.255



Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

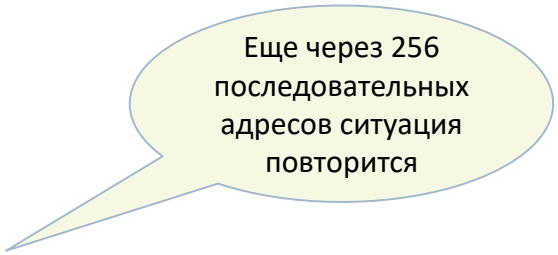
0.0.0.0
0.0.0.1
0.0.0.2
……..
0.0.0.255
0.0.1.0



Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

0.0.0.0
0.0.0.1
0.0.0.2
……..
0.0.0.255
0.0.1.0
0.0.1.1
……..
0.0.1.255



Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

0.0.0.0
0.0.0.1
0.0.0.2
……..
0.0.0.255
0.0.1.0
0.0.1.1
……..
0.0.1.255
0.0.2.0

Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

0.0.0.0
0.0.0.1
0.0.0.2
……..
0.0.0.255
0.0.1.0
0.0.1.1
……..
0.0.1.255
0.0.2.0
……..
0.0.255.255

После того, как заполнятся оба младших октета

Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

0.0.0.0
0.0.0.1
0.0.0.2
……..
0.0.0.255
0.0.1.0
0.0.1.1
……..
0.0.1.255
0.0.2.0
……..
0.0.255.255
0.1.0.0

Произойдет перенос единицы во второй октет

Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

0.0.0.0
0.0.0.1
0.0.0.2
…….
0.0.0.255
0.0.1.0
0.0.1.1
…….
0.0.1.255
0.0.2.0
…….
0.0.255.255
0.1.0.0
…….
0.1.255.255
0.2.0.0
0.2.0.1
…….
0.2.255.255
0.3.0.0
…….
0.255.255.255
1.0.0.0

Затем, через 16 миллионов адресов начнет заполняться 1 октет

Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

0.0.0.0
0.0.0.1
0.0.0.2
……..
0.0.0.255
0.0.1.0
0.0.1.1
……..
0.0.1.255
0.0.2.0
……..
0.0.255.255
0.1.0.0
……..
0.1.255.255
0.2.0.0
0.2.0.1
……..
0.2.255.255
0.3.0.0
……..
0.255.255.255
1.0.0.0
1.0.0.1
……..
1.255.255.255
2.0.0.0
…….
255.255.255.255

И постепенно получится самый максимальный адрес

Арифметика IP адресов (версии 4)

IP адреса – это целые числа, поэтому их можно записать по порядку возрастания:

0.0.0.0
0.0.0.1
0.0.0.2
……..
0.0.0.255
0.0.1.0
0.0.1.1
……..
0.0.1.255
0.0.2.0
……..
0.0.255.255
0.1.0.0
……..
0.1.255.255
0.2.0.0
0.2.0.1
……..
0.2.255.255
0.3.0.0
……..
0.255.255.255
1.0.0.0
1.0.0.1
……..
1.255.255.255
2.0.0.0
…….
255.255.255.255

Таким образом, изменение в третьем октете (1.2.3.4) возникает через 256 последовательных IP адресов.

Изменение во 2 октете (1.2.3.4) возникает через 256*256 = 65536 посл. адресов

А для изменения в 1 октете (1.2.3.4) необходимо уже 256*256*256 = 16777216 посл. адресов

Диапазоны IP адресов (версии 4)

Диапазон – это множество IP адресов содержащее все последовательные адреса от некоего начального адреса **a.b.c.d** до конечного адреса **e.f.g.h**. Например:

192.168.1.1 ÷ 192.168.2.15 (диапазон содержит ??? адресов)

Диапазоны IP адресов (версии 4)

Диапазон – это множество IP адресов содержащее все последовательные адреса от некоего начального адреса **a.b.c.d** до конечного адреса **e.f.g.h**. Например:

192.168.1.1 ÷ 192.168.2.15 (диапазон содержит **271** адрес)

В частном случае возможен диапазон из одного единственного адреса.

Диапазоны IP адресов (версии 4)

Диапазон – это множество IP адресов содержащее все последовательные адреса от некоего начального адреса **a.b.c.d** до конечного адреса **e.f.g.h**. Например:

192.168.1.1 ÷ 192.168.2.15 (диапазон содержит **271** адрес)

В частном случае возможен диапазон из одного единственного адреса.

Двоичный блок IP адресов – это диапазон, обладающий следующими свойствами:

- Количество адресов в диапазоне - 2^n
- Начальный адрес диапазона должен быть кратен 2^n

Примеры правильных двоичных блоков:

192.168.1.0 ÷ 192.168.1.255 (блок содержит 256 адресов)
192.168.2.64 ÷ 192.168.2.127 (блок содержит 64 адреса)
10.231.18.0 ÷ 10.231.19.255 (блок содержит ??? адреса)

Диапазоны IP адресов (версии 4)

Диапазон – это множество IP адресов содержащее все последовательные адреса от некоего начального адреса **a.b.c.d** до конечного адреса **e.f.g.h**. Например:

192.168.1.1 ÷ 192.168.2.15 (диапазон содержит **271** адрес)

В частном случае возможен диапазон из одного единственного адреса.

Двоичный блок IP адресов – это диапазон, обладающий следующими свойствами:

- Количество адресов в диапазоне - 2^n
- Начальный адрес диапазона должен быть кратен 2^n

Примеры правильных двоичных блоков:

192.168.1.0 ÷ 192.168.1.255 (блок содержит 256 адресов)
192.168.2.64 ÷ 192.168.2.127 (блок содержит 64 адреса)
10.231.18.0 ÷ 10.231.19.255 (блок содержит **512** адресов)

Свойства блоков IP адресов (версии 4)

Двоичное представление IP адресов, образующих правильный блок имеет характерную структуру:

11000000101010000000001001000000 – 192.168.2.64
11000000101010000000001001000001 – 192.168.2.65
11000000101010000000001001000010 – 192.168.2.66
11000000101010000000001001000011 – 192.168.2.67
. . . . . .
11000000101010000000001001111100 – 192.168.2.124
11000000101010000000001001111101 – 192.168.2.125
11000000101010000000001001111110 – 192.168.2.126
11000000101010000000001001111111 – 192.168.2.127

Свойства блоков IP адресов (версии 4)

Двоичное представление IP адресов, образующих правильный блок имеет характерную структуру:

11000000101010000000001001000000 – 192.168.2.64
11000000101010000000001001000001 – 192.168.2.65
11000000101010000000001001000010 – 192.168.2.66
11000000101010000000001001000011 – 192.168.2.67
. . . . . .
11000000101010000000001001111100 – 192.168.2.124
11000000101010000000001001111101 – 192.168.2.125
11000000101010000000001001111110 – 192.168.2.126
11000000101010000000001001111111 – 192.168.2.127

Префикс Суффикс

Для всех адресов блока значение битов префикса одинаковое, а значение суффикса «пробегает» все последовательные значения от 0..000 до 1..111

Для блока размером 2^n количество битов в суффиксе равно n, а количество битов в префиксе $(32-n)$

Способы записи блоков IP адресов

Каждый правильный блок полностью описывается двумя параметрами:

- Начальным (минимальным) адресом диапазона;
- Длиной префикса в битах.

Такая форма представления называется CIDR-нотацией. Например:

192.168.1.0/24 это диапазон 192.168.1.0 ÷ 192.168.1.255
10.231.18.0/23 это диапазон 10.231.18.0 ÷ 10.231.19.255

Альтернативной (и более старой) является форма, когда вместо длины префикса указывается маска сети (Netmask).

Маска сети – это *псевдо IP адрес*, представляющий собой 32-битный код (маску), у которого биты префикса блока установлены в 1, а биты суффикса равны 0.

Для 192.168.1.0/24 маска сети будет 255.255.255.0 или в двоичной форме:
11111111 11111111 11111111 00000000 (длина префикса – 24 бита)

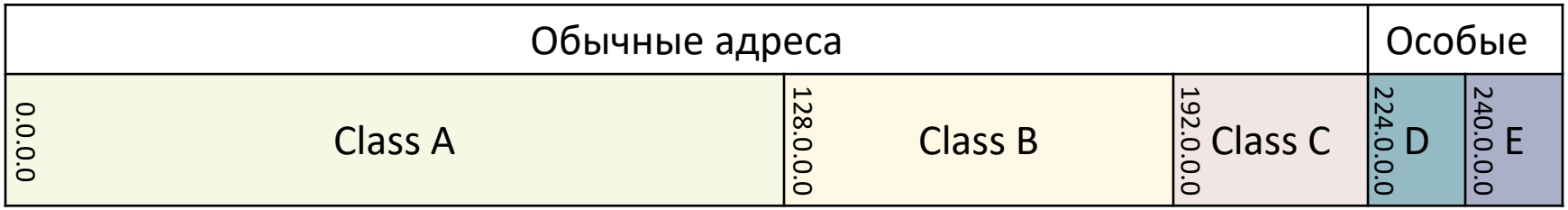
Для 10.231.18.0/23 маска сети будет 255.255.254.0 или в двоичной форме:
11111111 11111111 11111110 00000000 (длина префикса – 23 бита)

Зависимость префиксов, масок и блоков

Длина префикса/сетевая маска определяют размер блока (количество IP в блоке):

/n	Netmask	32-n	Размер	/n	Netmask	32-n	Размер
/32	255.255.255.255	0	1	/18	255.255.192.0	14	16384
/31	255.255.255.254	1	2	/17	255.255.128.0	15	32768
/30	255.255.255.252	2	4	/16	255.255.0.0	16	65536
/29	255.255.255.248	3	8	/15	255.254.0.0	17	131072
/28	255.255.255.240	4	16	/14	255.252.0.0	18	262144
/27	255.255.255.224	5	32	/13	255.248.0.0	19	524288
/26	255.255.255.192	6	64	/12	255.240.0.0	20	1 Mi
/25	255.255.255.128	7	128	/11	255.224.0.0	21	2 Mi
/24	255.255.255.0	8	256	/10	255.192.0.0	22	4 Mi
/23	255.255.254.0	9	512	/9	255.128.0.0	23	8 Mi
/22	255.255.252.0	10	1024	/8	255.0.0.0	24	16 Mi
/21	255.255.248.0	11	2048	/7	254.0.0.0	25	32 Mi
/20	255.255.240.0	12	4096	…	…….		
/19	255.255.224.0	13	8192	/0	0.0.0.0	0	4 Gi

Виды IP адресов



Обычные адреса могут назначаться на сетевые интерфейсы:

- Класс A: 128 сетей по 16777216 (0.0.0.0-127.255.255.255)
- Класс B: 64*256=16384 сетей по 65536 (128.0.0.0-191.255.255.255)
- Класс C: 32*256*256=2097152 сетей по 256 (192.0.0.0-223.255.255.255)

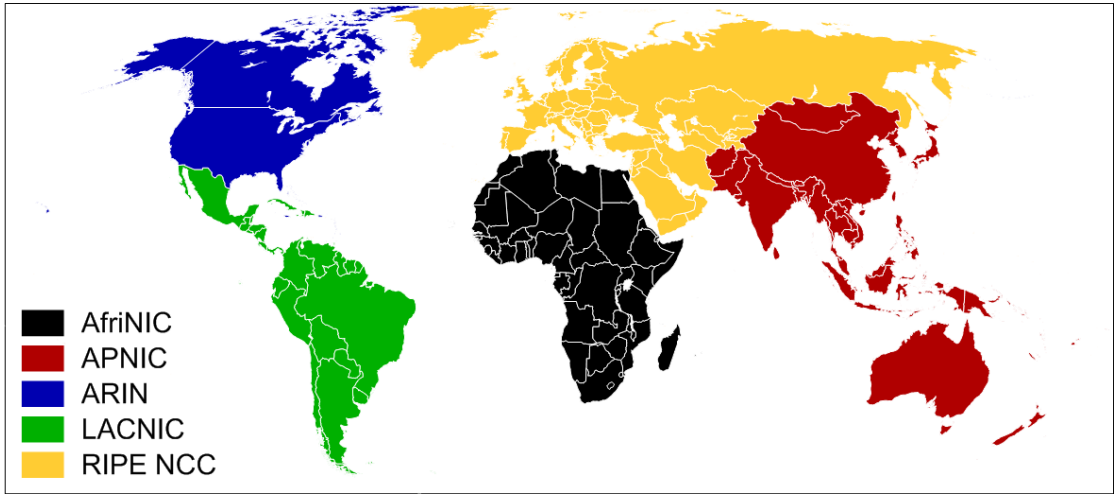
Особые адреса не могут использоваться для назначения интерфейсам:

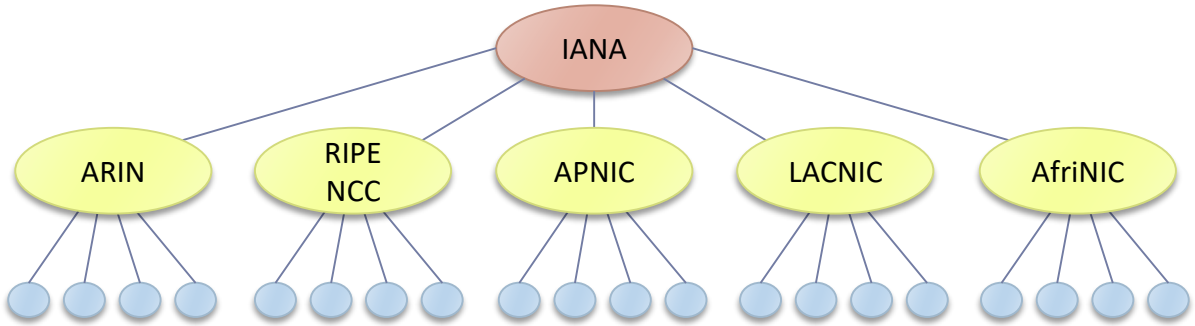
- Класс D: адреса для Multicast (групповые адреса) (224.0.0.0-239.255.255.255)
- Класс E: зарезервированные адреса (240.0.0.0-255.255.255.255)

В 1993 году (RFC-1518) деление на классы обычных адресов было упразднено и теперь весь диапазон 0.0.0.0-223.255.255.255 рассматривается как единый пул (массив ресурсов) из которого производится выделение (allocation) и назначение (assignment) блоков адресов.

Процесс распределения уникальных адресов

Так называемые «белые» IP адреса должны быть уникальными. Т.е. во всей сети Internet не должно быть более одного интерфейса с конкретным IP адресом.





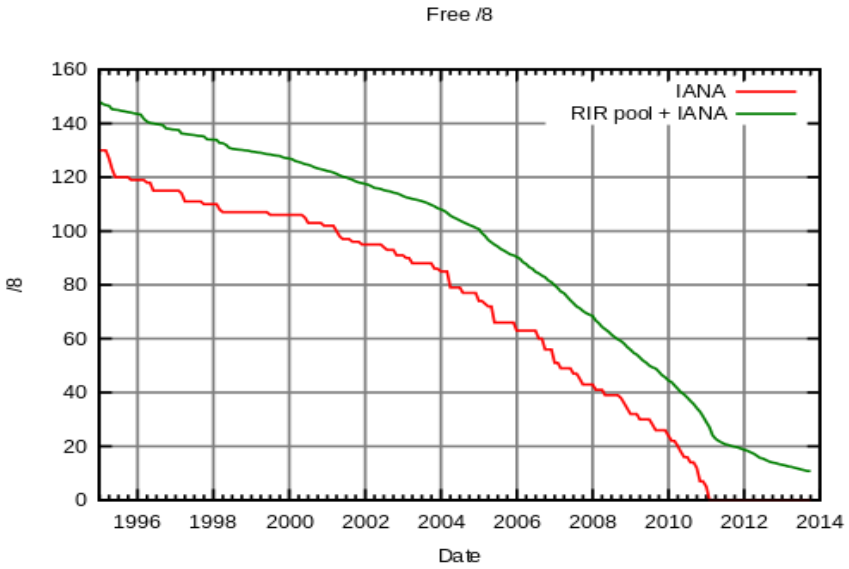
Regional Internet Registries (RIR)

Internet Service Providers (ISP)

Исчерпание IPv4 адресов и частные адреса

Всего существует около 3,7 млн. возможных уникальных («белых») IP адресов. Еще в 1991 году стало понятно, что их явно недостаточно и на сегодняшний момент этот ресурс **практически исчерпан**.

До всеобщего перехода на IPv6, где используются 128-битные адреса (около 3,4 * 10^{38} возможных адресов) было предложено два решения:



- Отмена классов и переход на выделение адресов блоками нужного размера (Classless Inter-Domain Internet Routing – CIDR)
- Использование частных (RFC 1918) IP адресов там, где не требуется непосредственная связность (end to end connectivity):
  - 10.0.0.0-10.255.255.255: 16777216 адресов (1 сеть класса A)
  - 172.16.0.0-172.31.255.255: 1048576 адресов (16 сетей класса B)
  - 192.168.0.0-192.168.255.255: 65536 адресов (256 сетей класса C)

Частные vs уникальные IP адреса

Частные IP адреса	Уникальные IP адреса
Предназначены для использования внутри локальной (обособленной) сети	Предназначены для назначения на интерфейсы, напрямую адресуемые в глобальной сети Internet
Связь с другими узлами Internet возможна только через шлюз, имеющий уникальный IP адрес и оборудованный NAT или Proxy	Возможен непосредственный обмен пакетами с любым другим узлом Internet с уникальным IP
Могут назначаться без согласования из блоков, определенных в RFC 1918	Требуют предварительного получения у ISP блока адресов, назначенного для данного абонента
Большая свобода выбора из 17 млн. адресов RFC 1918	ISP выделяет лишь минимальное количество адресов – часто всего один

«Серые» IP адреса – как правило, частные IP адреса, которые могут выделяться ISP своим клиентам вместо уникальных IP адресов. Благодаря технологиям NAT с таких адресов возможна ограниченная связь с узлами Internet.

IP адреса специального назначения

Диапазон	Кол-во	Назначение
0.0.0.0 /8	16 Mi	Адрес отправителя из данного диапазона обозначает “Эта сеть”
127.0.0.0 /8	16 Mi	Внутренняя псевдо-сеть узла (Loopback)
10.0.0.0 /8	16 Mi	Диапазоны для частной адресации (Private network) в соответствие с RFC-1918
172.16.0.0 /12	1 Mi	
192.168.0.0 /16	64 Ki	
100.64.0.0 /10	4 Mi	Shared address space («серые» адреса для ISP NAT)
169.254.0.0 /16	64 Ki	Местные адреса для сегмента сети (Link-Local)
224.0.0.0 /4	64 Mi	Адреса вещательного режима (Multicast) [Class E]
240.0.0.0 /4	64 Mi	Зарезервированный диапазон [Class D]
255.255.255.255	1	Широковещательный адрес ограниченного действия

План курса

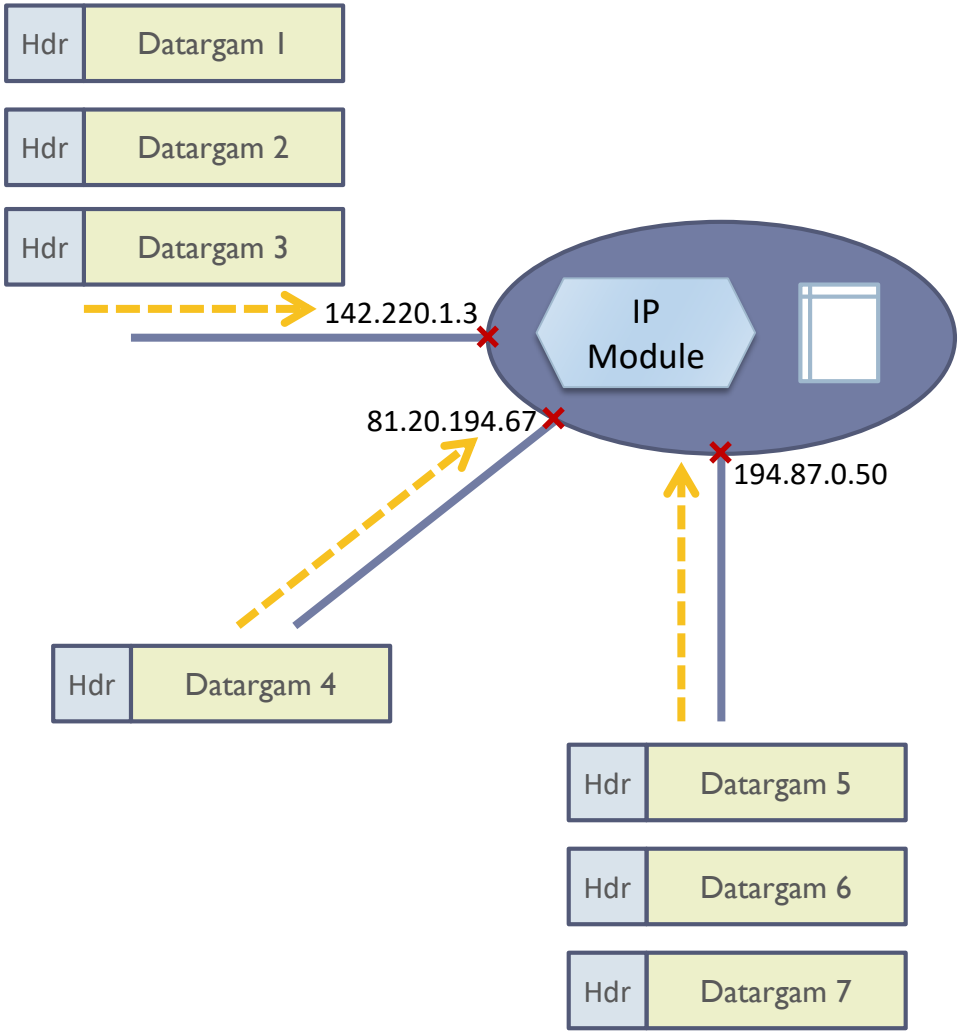
1. Введение в компьютерные сети
2. Основные методы построения СПД
3. **Архитектура Internet Protocol Suite (TCP/IP)**
    - 3.1. Адресация в IP сетях
    - **3.2. Протокол IP (v4)**
    - 3.3. Протокол ARP
    - 3.4. Служебный трафик и протокол ICMP
4. Архитектура модулей физического уровня
5. Технологии беспроводных сетей
6. Архитектура модулей канального уровня
7. Протоколы транспортного уровня
8. Технологии WWW

IP модули и выполняемые ими функции

IP модуль – часть IP протокола, выполняющаяся на одном узле. Собственно протокол IP это и есть совокупность совместно функционирующих IP модулей. Каждый узел Internet обязан иметь функционирующий IP модуль:

- ✓ Получение пакетов, поступающих:
  - С внешних интерфейсов (links)
  - От местных модулей протоколов (работающих на этом же узле)
- ✓ Коммутация пакетов - определение направления дальнейшего движения пакета:
  - Передача по внешнему интерфейсу
  - Передача на обработку местному модулю протокола
  - Сброс пакета
- ✓ Фрагментация/сборка пакетов
- ✓ (Опционально) Фильтрация пакетов (Packet Filter – Firewall)
- ✓ (Опционально) Управление очередями (QoS, Traffic Shaping, etc.)
- ✓ (Опционально) Преобразование IP адресов (NAT)

Коммутация IP пакетов

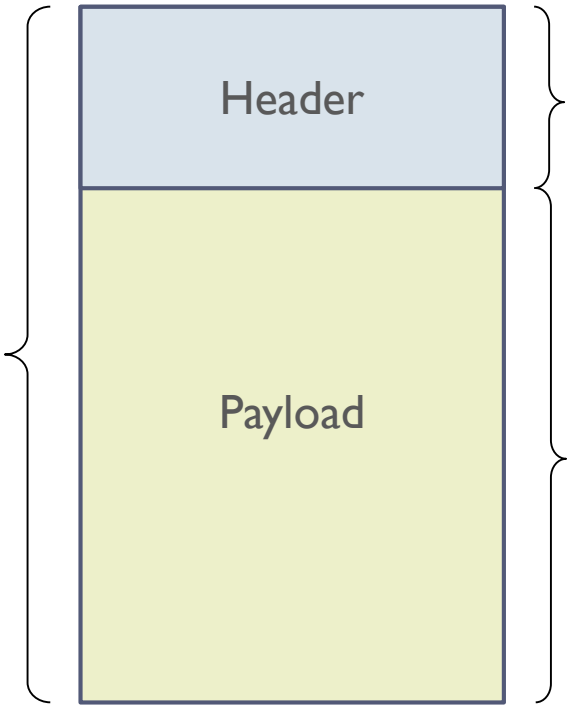


IP модуль:

- Обрабатывает входящие пакеты друг за другом в порядке их поступления (по одному за раз)
- (для каждого пакета) определяет предпринимаемое действие по IP адресу назначения (Dst-IP) из заголовка пакета
  - Передать пакет вышестоящему протоколу (*адрес достигнут*)
  - Передать напрямую соседу (*адрес соседа*)
  - Перенаправить для дальнейшего принятия решения на сосед-шлюз

Структура IP пакета

Пакет – порция данных переменной длины (содержит целое количество байтов).

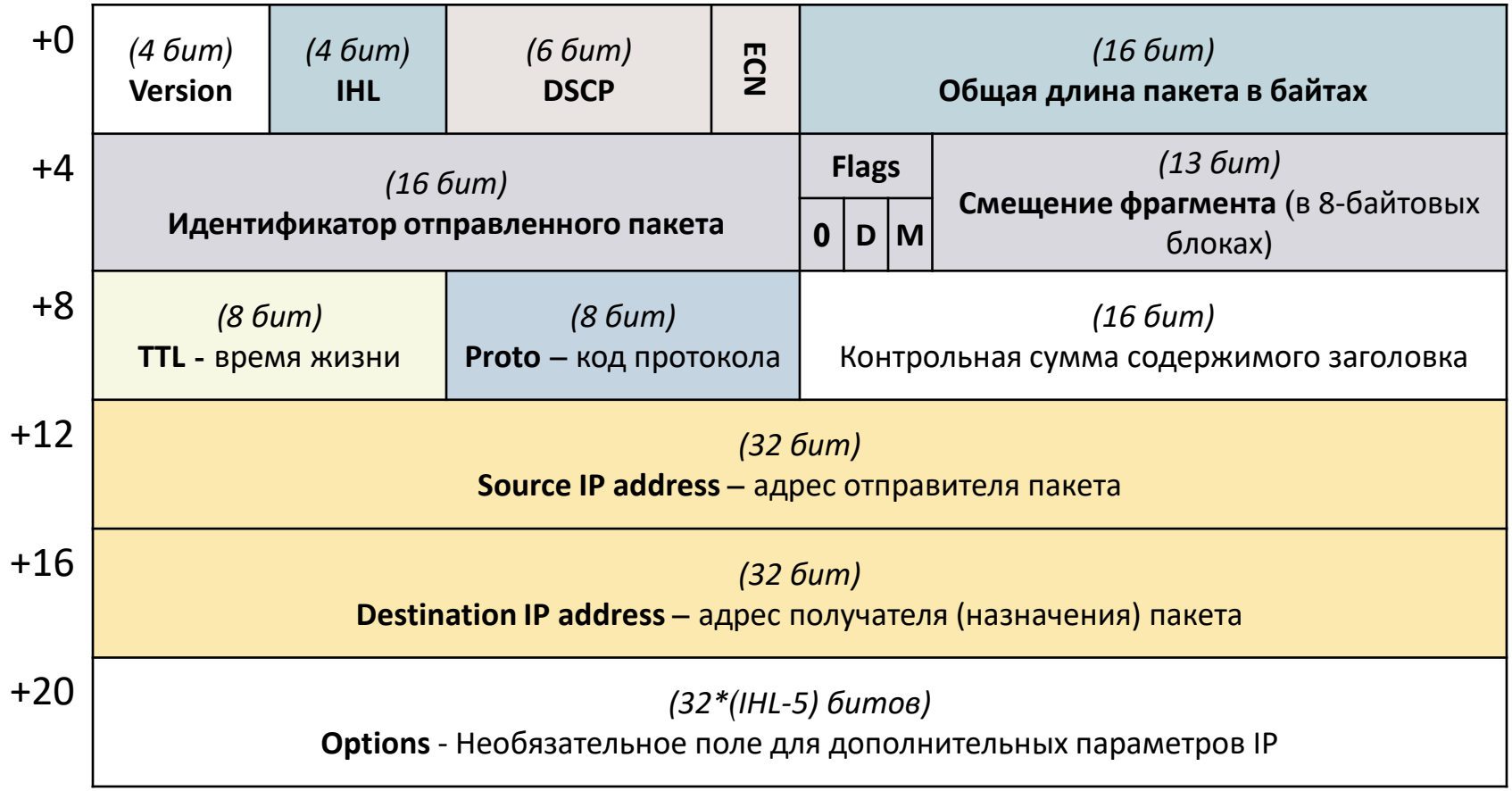


Заголовок пакета: 20+ байтов фиксированной структуры (присутствует всегда)

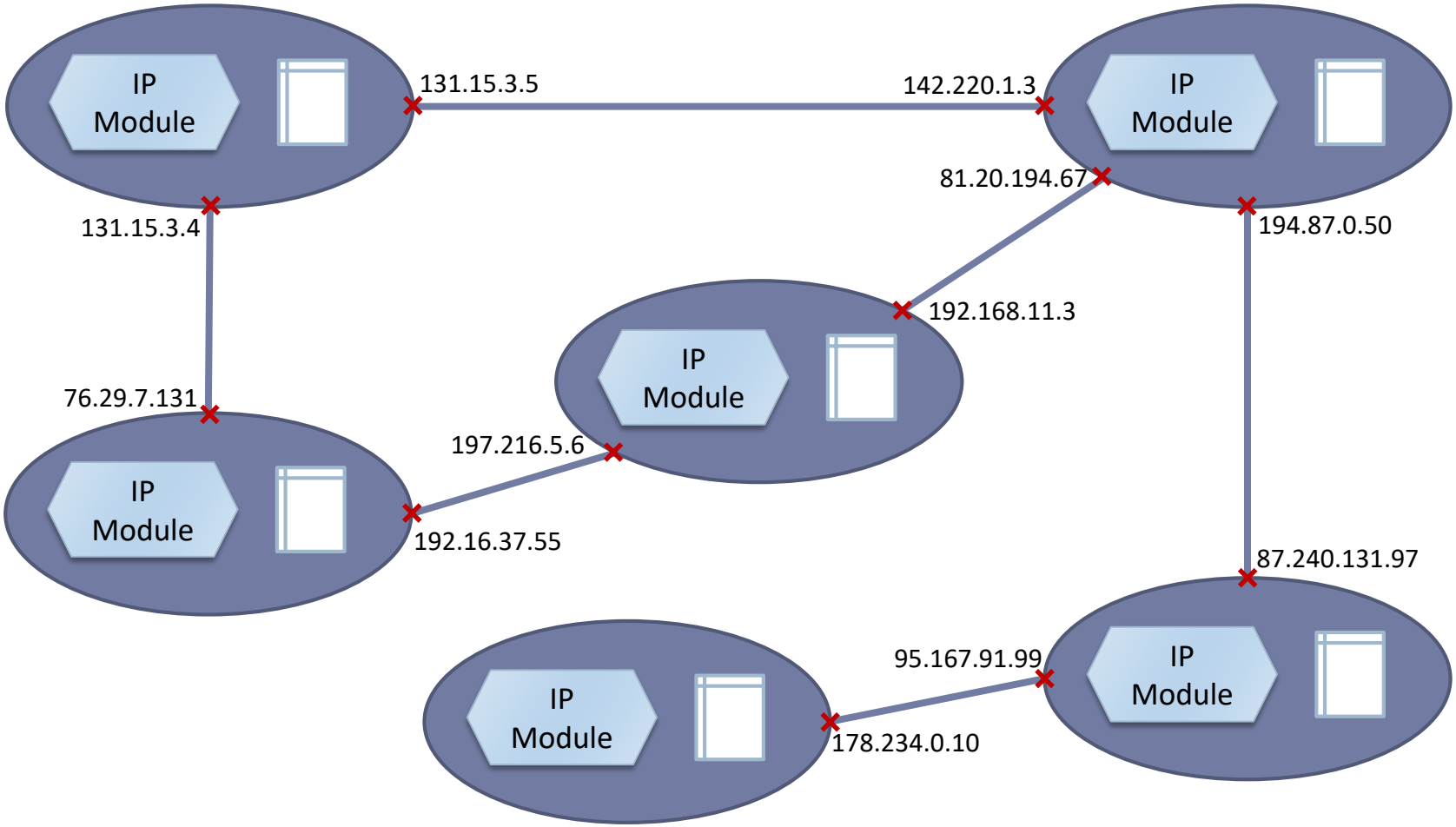
«Полезная нагрузка»: произвольные данные, которые IP передает «как есть» без анализа.
(в частных случаях может отсутствовать).

Общий размер пакета в байтах ограничен сверху параметром MTU (Maximum Transmission Unit). Он задается индивидуально для каждого сетевого интерфейса. Теоретически величина MTU может выбираться из диапазона 68…65535 байтов. На практике в большинстве случаев величина MTU=1500 байтов или чуть меньше. Однако иногда применяется MTU до 9000 байтов (Jumbo Frames).

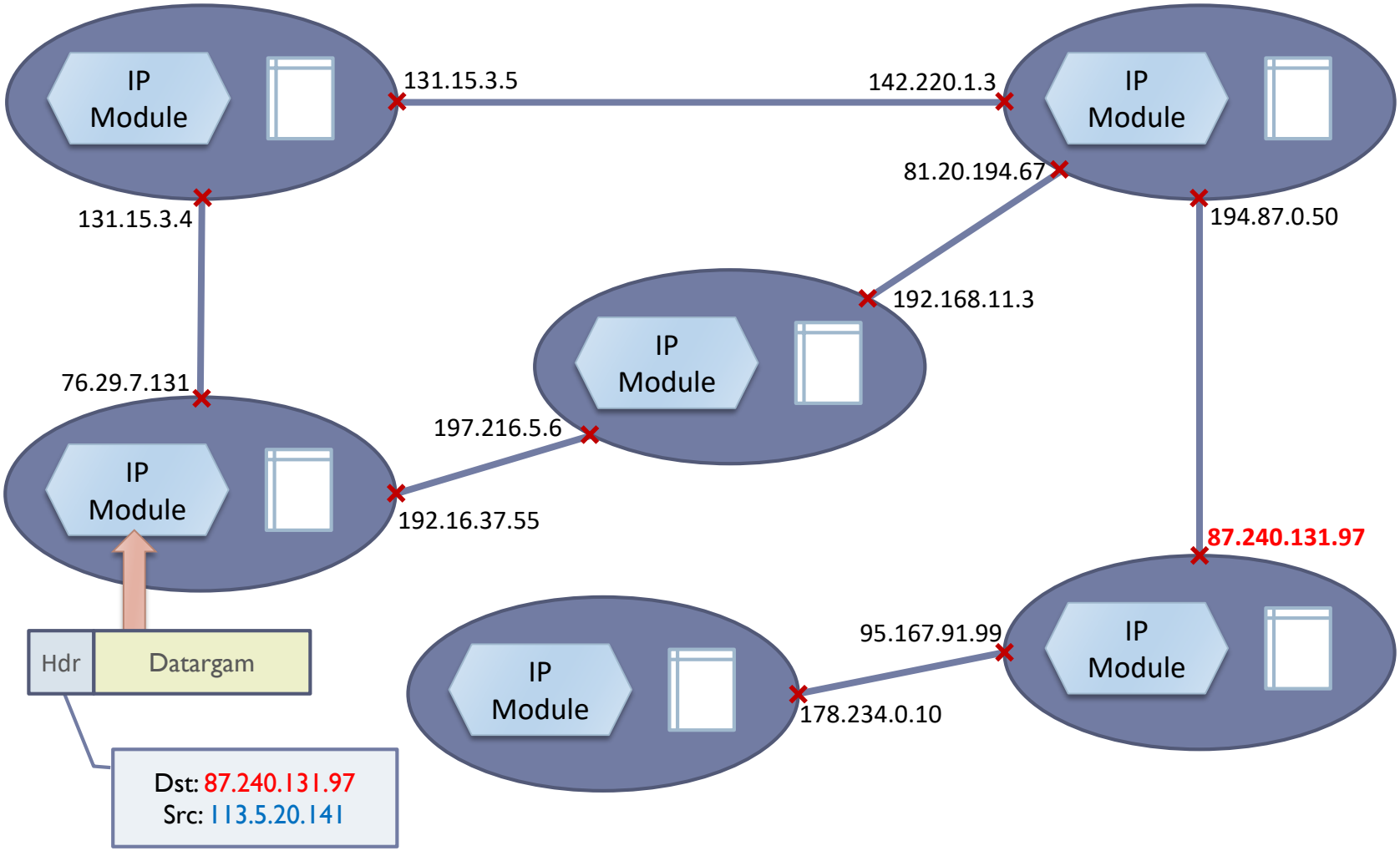
Структура заголовка IP пакета



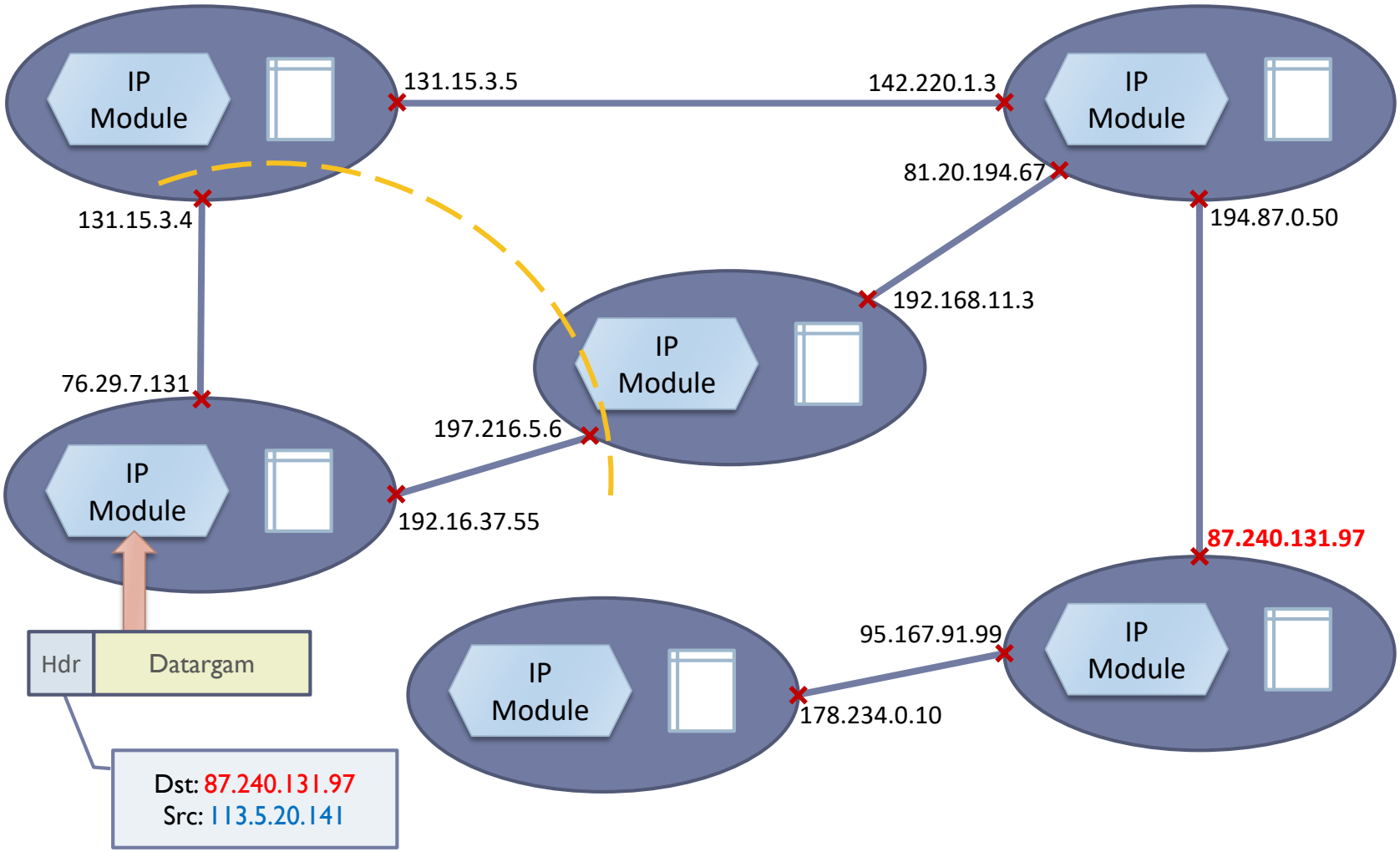
Коммутация IP пакетов



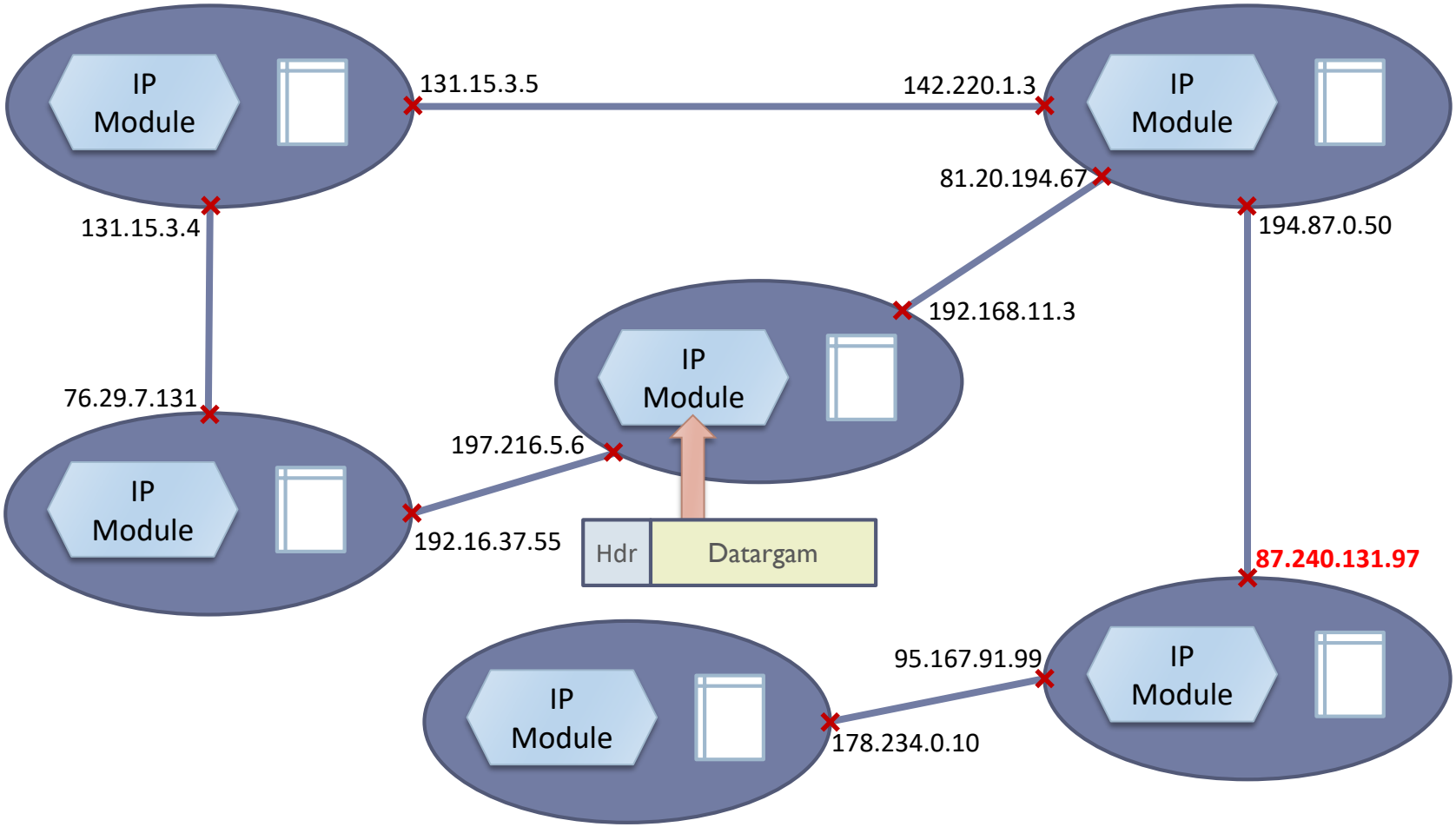
Коммутация IP пакетов



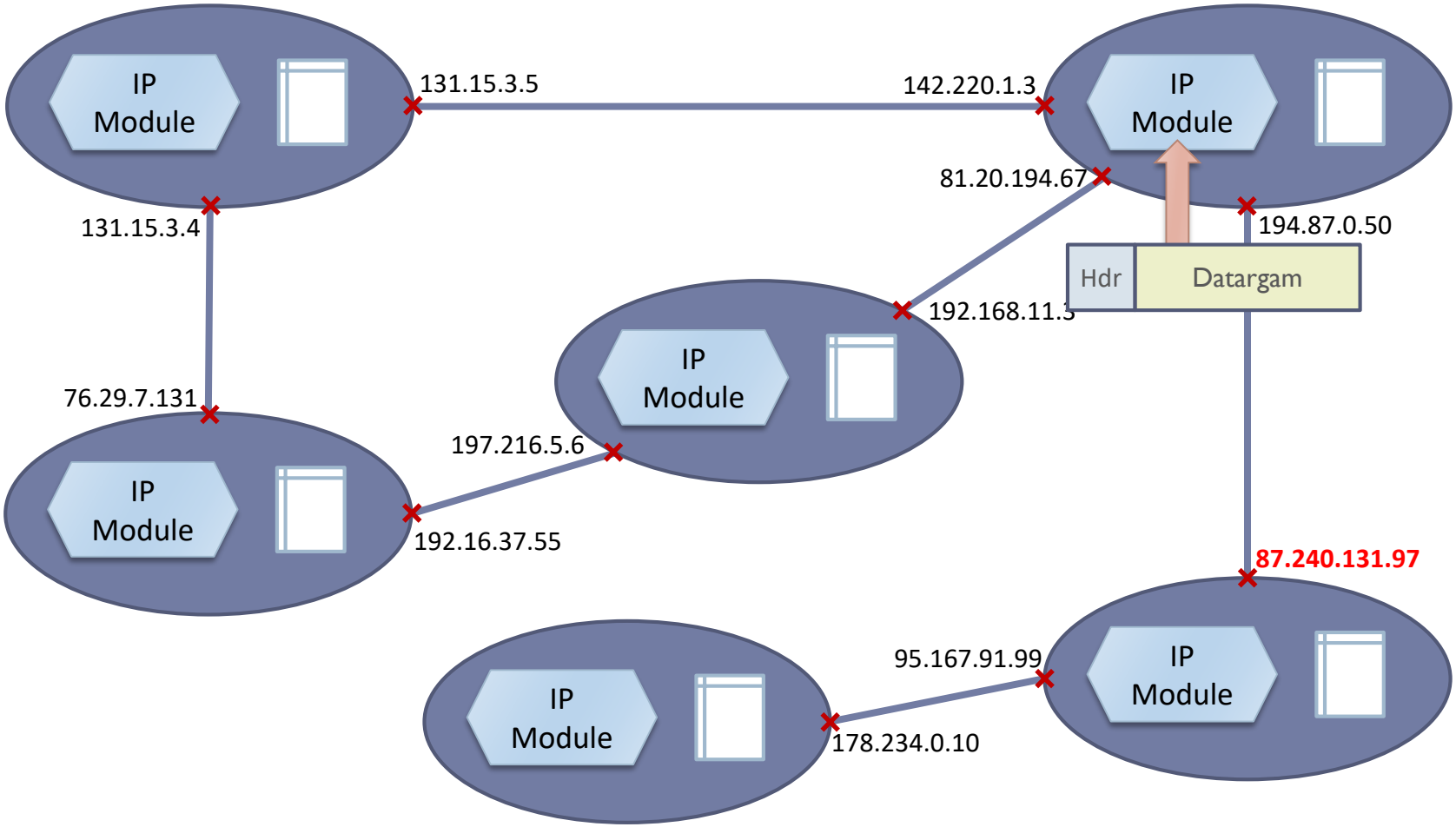
Коммутация IP пакетов



Коммутация IP пакетов



Коммутация IP пакетов



Коммутация IP пакетов

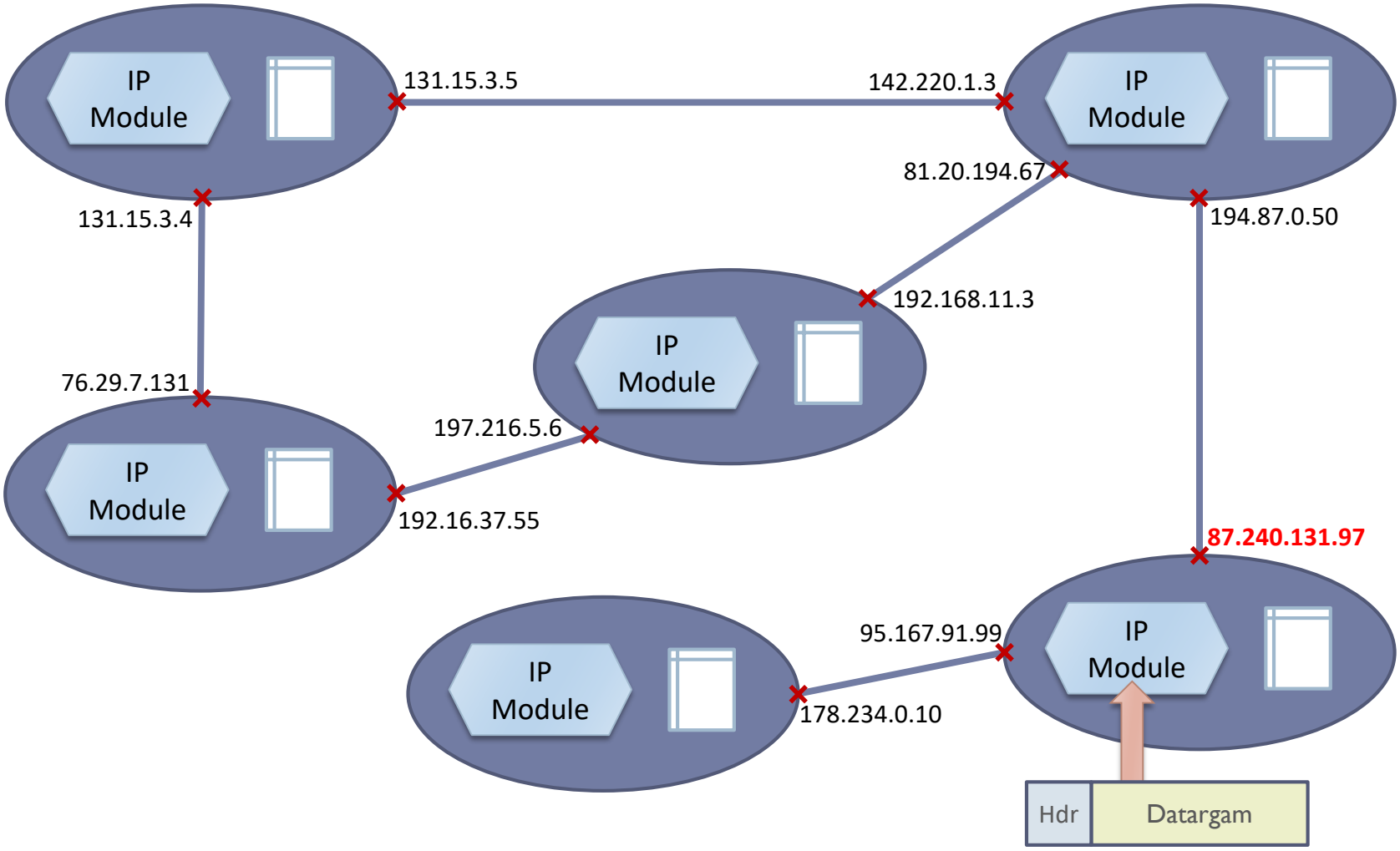


Таблица маршрутов

Работа коммутатора управляется содержимым таблицы маршрутов (routing table):

Destination	Type	If	Next-Hop	Metric
192.168.1.199/32	Local	lo0		1
192.168.1.0/24	U	Eth0		10
10.23.149.21/32	UH	Ser0		5
0.0.0.0/0	UG	Eth0	192.168.1.1	50

Destination: блок IP адресов к которому применима данная строка таблицы

Type: Тип действия, которое будет выполнено с пакетом, если сработает данная строка

If: Местное имя интерфейса, который будет использоваться для выполнения указанного в строке действия

Next-Hop: Адрес шлюза, которому будет направлен пакет (используется только для косвенных маршрутов типа UG)

Алгоритм коммутатора IP пакетов

Для каждого полученного пакета с адресом назначения Dst-IP:

1. Найти в таблице маршрутов все строки, у которых блок адресов указанный в колонке Destination включает (охватывает) Dst-IP
2. Если подходящих строк не нашлось – сбрасываем пакет
3. Если подходит несколько строк оставляем те, у которых наибольшая длина префикса
4. Если все еще осталось несколько строк оставляем те, у которых минимальное значение Metric
5. Если в результате отобрано более одной строки, то в зависимости от вида коммутатора может применяться одна из двух стратегий:
   - Всегда выбирается одна произвольная из оставшихся строк
   - Разные строки выбираются по очереди для каждого следующего пакета
6. Для пакета выполняется действие, указанное в выбранной строке

Действия выполняемые с пакетами

Type	Вид маршрута	Выполняемое действие
Local	Местный	*Пакет достиг адреса назначения*. IP модуль выполняет сборку фрагментированного пакета (если необходимо) и передает его на обработку модулю протокола, указанному в поле Proto IP заголовка
UH	Прямой	*Пакет предназначен соседнему узлу, подключенному по прямому двухточечному каналу*. IP модуль ставит пакет в очередь указанного интерфейса.
U	Прямой	*Пакет предназначен соседнему узлу, подключенному к общему многоточечному звену* (Ethernet). IP модуль: • Определяет канальный адрес требуемого узла по его IP адресу (преобразование IP→адрес в канале); • Ставит в очередь указанного интерфейса для доставки по найденному адресу в канале
UG	Косвенный	*Пакет должен быть передан другому узлу (шлюзу) для дальнейшей доставки.* IP модуль повторяет поиск по таблице маршрутов для указанного в колонке Next-Hop IP адреса шлюза.

Пример заполненной таблицы маршрутов

Destination	Type	If	Next-Hop	Metric	
192.168.1.199/32	Local	lo0		1	Конфигурация сетевого интерфейса eth0
192.168.1.0/24	U	Eth0		10	
10.23.149.21/32	UH	Ser0		5	Конфигурация интерфейса ser0
0.0.0.0/0	UG	Eth0	192.168.1.1	50	Default gateway

Локальный маршрут: Описывает собственные IP адреса узла (адреса верхних уровней)

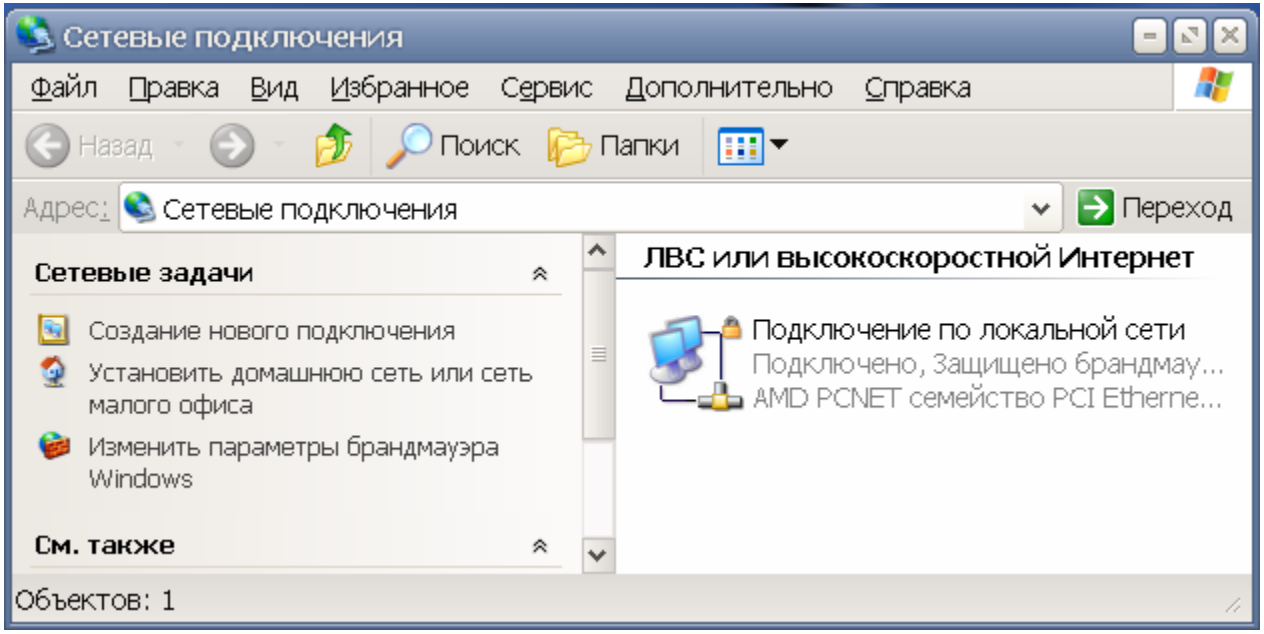
Прямой маршрут: Описывает адреса прямых соседей

Косвенный маршрут: Описывает адреса иных узлов и шлюз доступа к ним

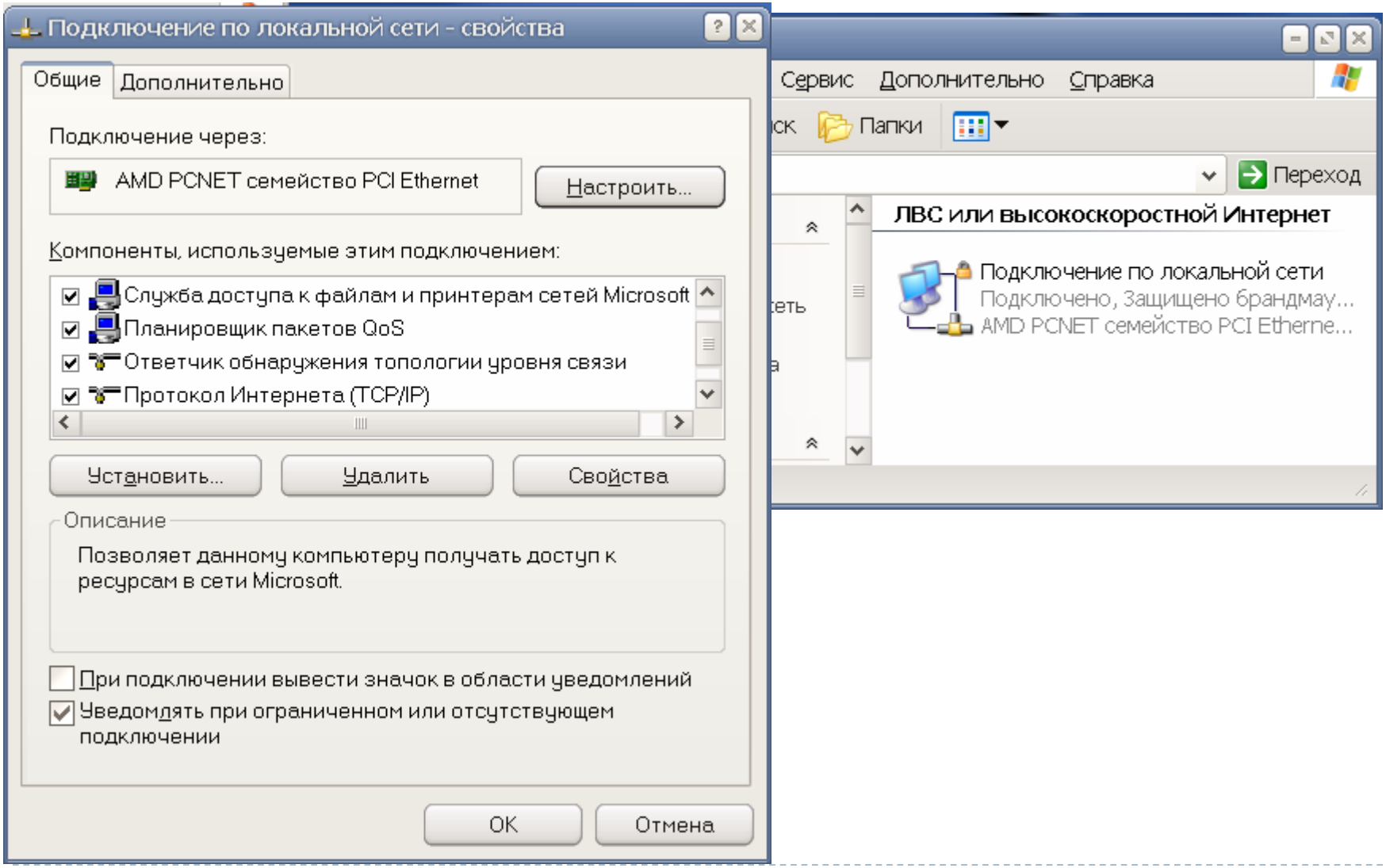
Заполнение таблиц маршрутов

- ✓ На каждом узле IP сети присутствует собственная таблица маршрутов (***netstat –r*** или ***route print***), которая требует корректного заполнения
- ✓ Главный источник данных для таблицы – конфигурация сетевых интерфейсов
  - Логический интерфейс loopback
    - ➢ Фиксированный IP адрес - 127.0.0.1
  - Многоточечный интерфейс (например, Ethernet):
    - ➢ IP адрес, присвоенный интерфейсу
    - ➢ Netmask или длина префикса, описывающие блок адресов подсети
  - Двухточечный интерфейс (например, PPP):
    - ➢ Локальный IP адрес
    - ➢ Противоположный (удаленный) IP адрес
- ✓ Шлюз по умолчанию (default gateway)
- ✓ Косвенные маршруты:
  - ➢ Заданные вручную (статические)
  - ➢ Определенные одним из автоматических протоколов маршрутизации

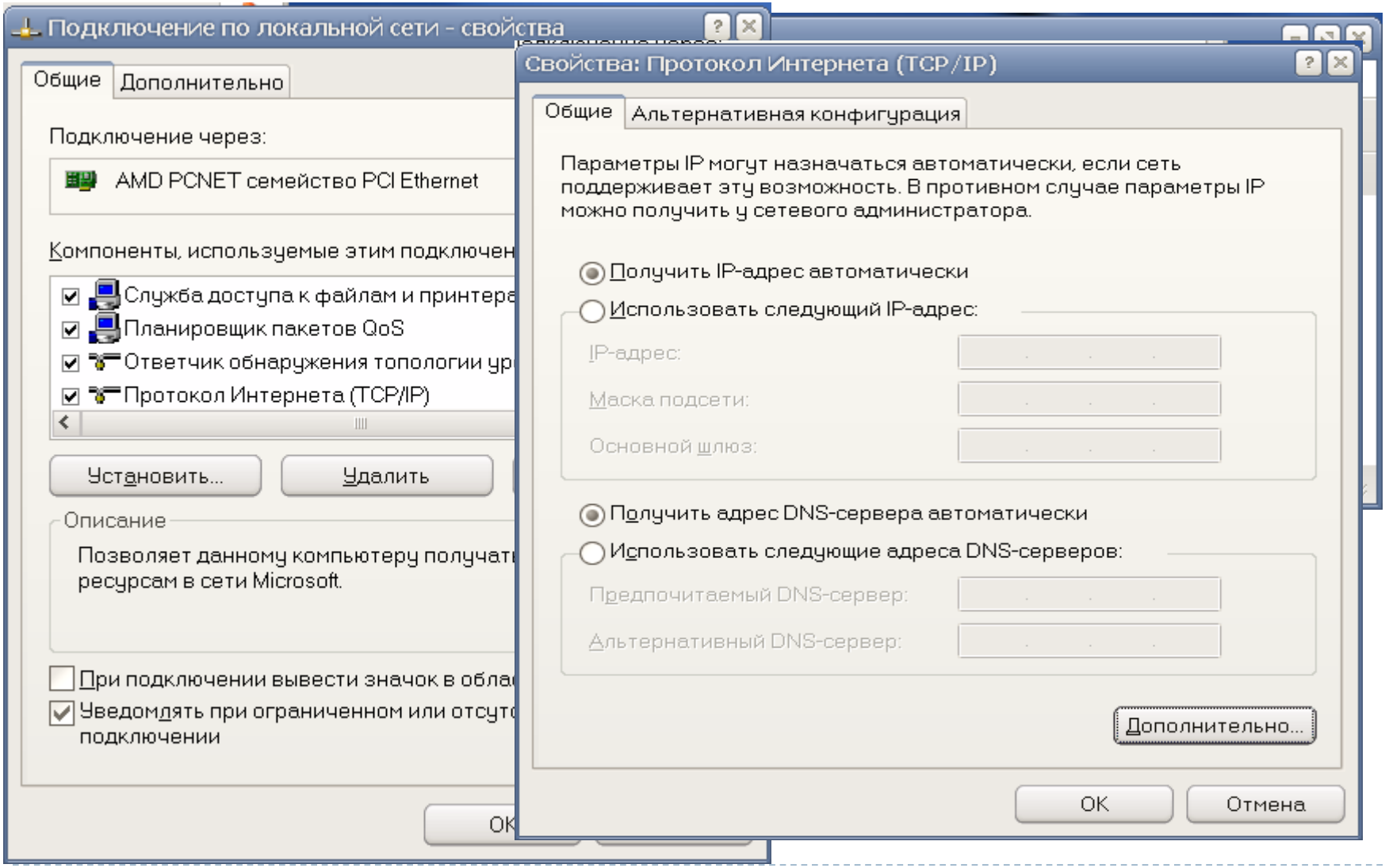
Конфигурация сетевых интерфейсов



Конфигурация сетевых интерфейсов



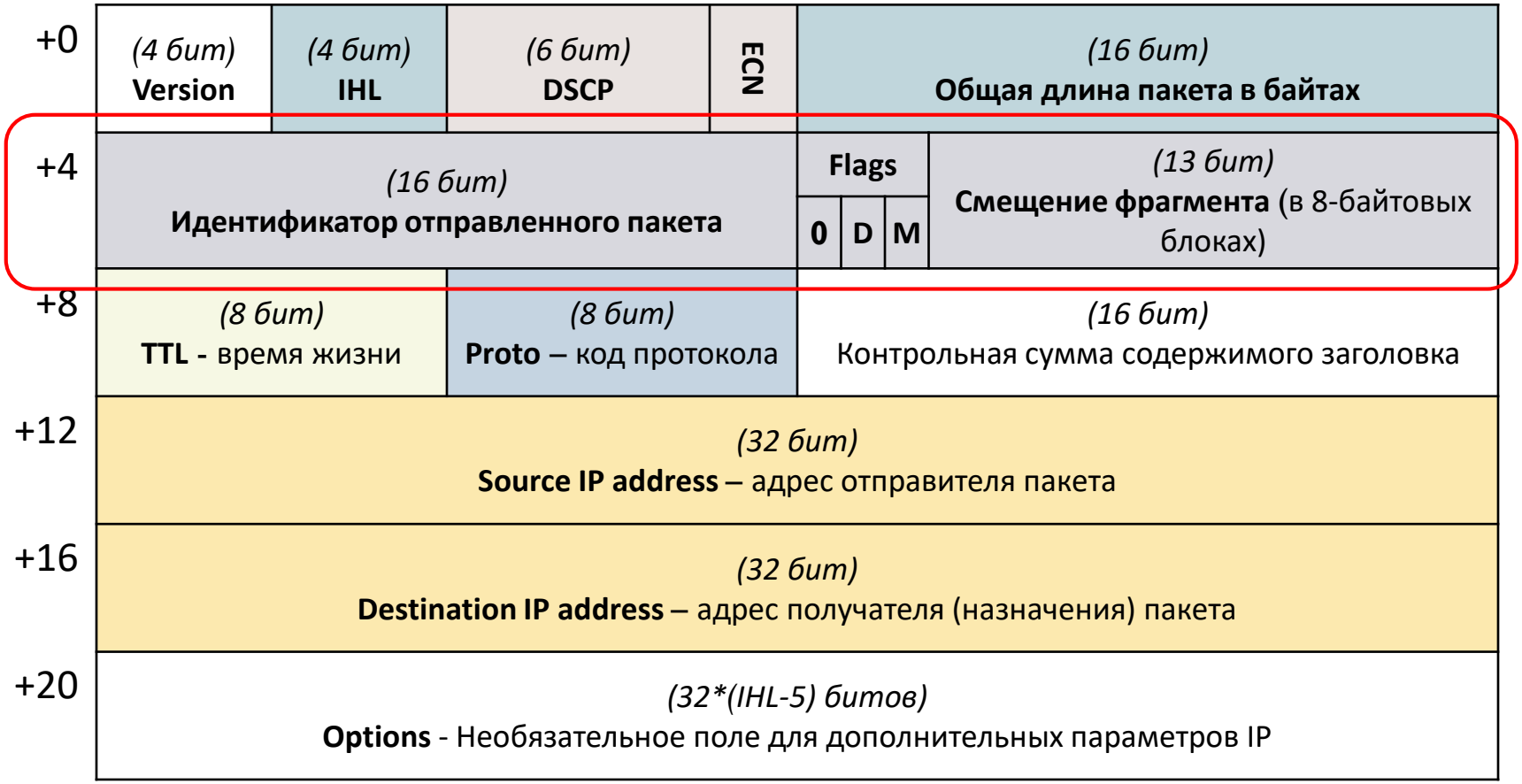
Конфигурация сетевых интерфейсов



Варианты задания конфигурации интерфейса

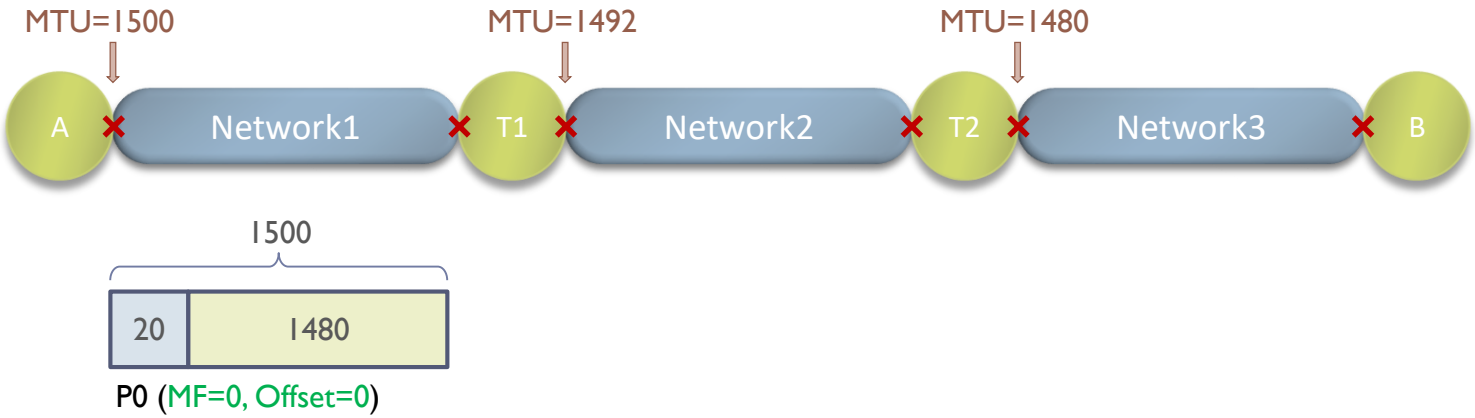
- ***"Автоматически"***- выполняется следующая процедура:
  1. Параметры конфигурации интерфейса (IP адрес, Netmask, Default gateway, адреса серверов DNS, адреса серверов WINS …) запрашиваются у сервера **DHCP** (RFC 2131).
  2. Если ответ от сервера DHCP не получен около минуты, то выполняется динамическое (псевдослучайное) назначение местного (link-local) адреса из диапазона ***169.254.1.0 - 169.254.254.255*** с последующей проверкой на отсутствие дублирования (RFC 3927).
- ***Использовать следующий IP адрес*** – пользователь должен вручную задать:
  1. IP адрес, назначенный на данный интерфейс – используется для создания маршрутов типа ***local***.
  2. Маску подсети (netmask) – определяет размер блока адресов, выделенных для данной сети и используется для вычисления префикса и создания прямых маршрутов типа ***U***.
  3. Основной шлюз – используется для создания маршрута по умолчанию (Default route с типом ***UG***).

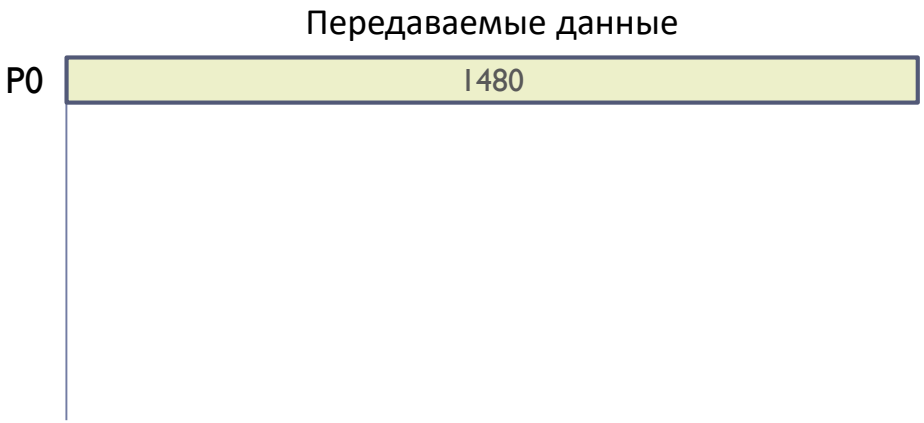
Структура заголовка IP пакета



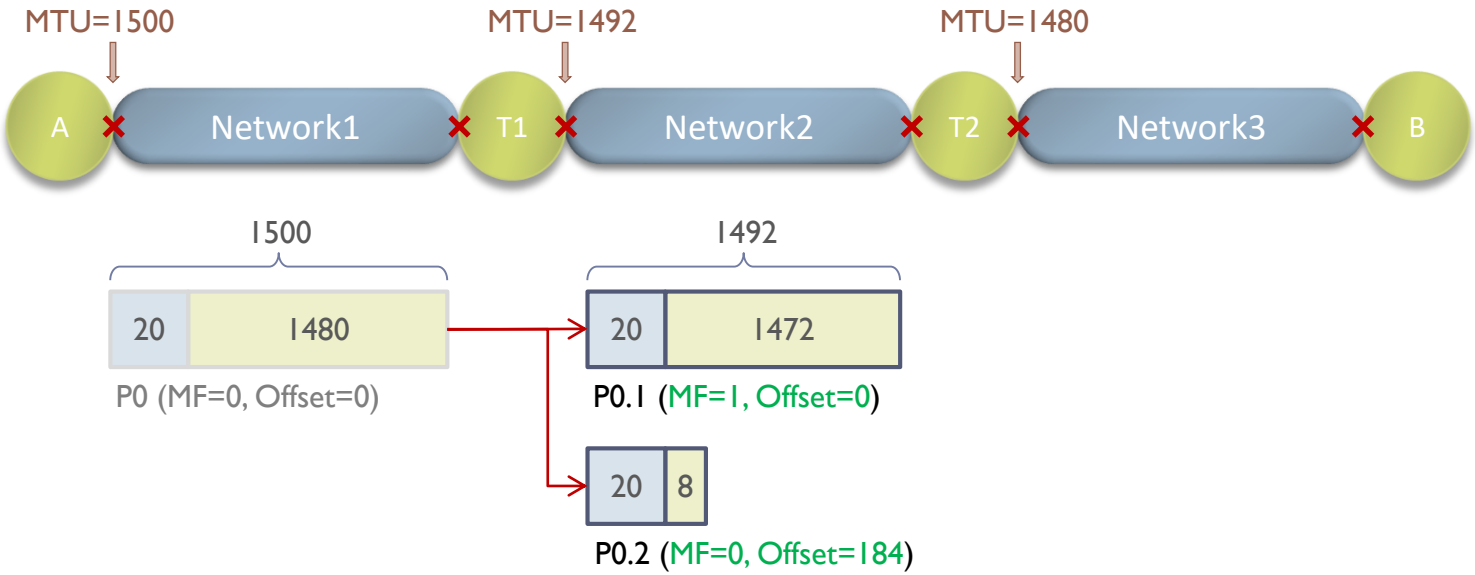
Механизм фрагментации пакетов

Механизм фрагментации пакетов

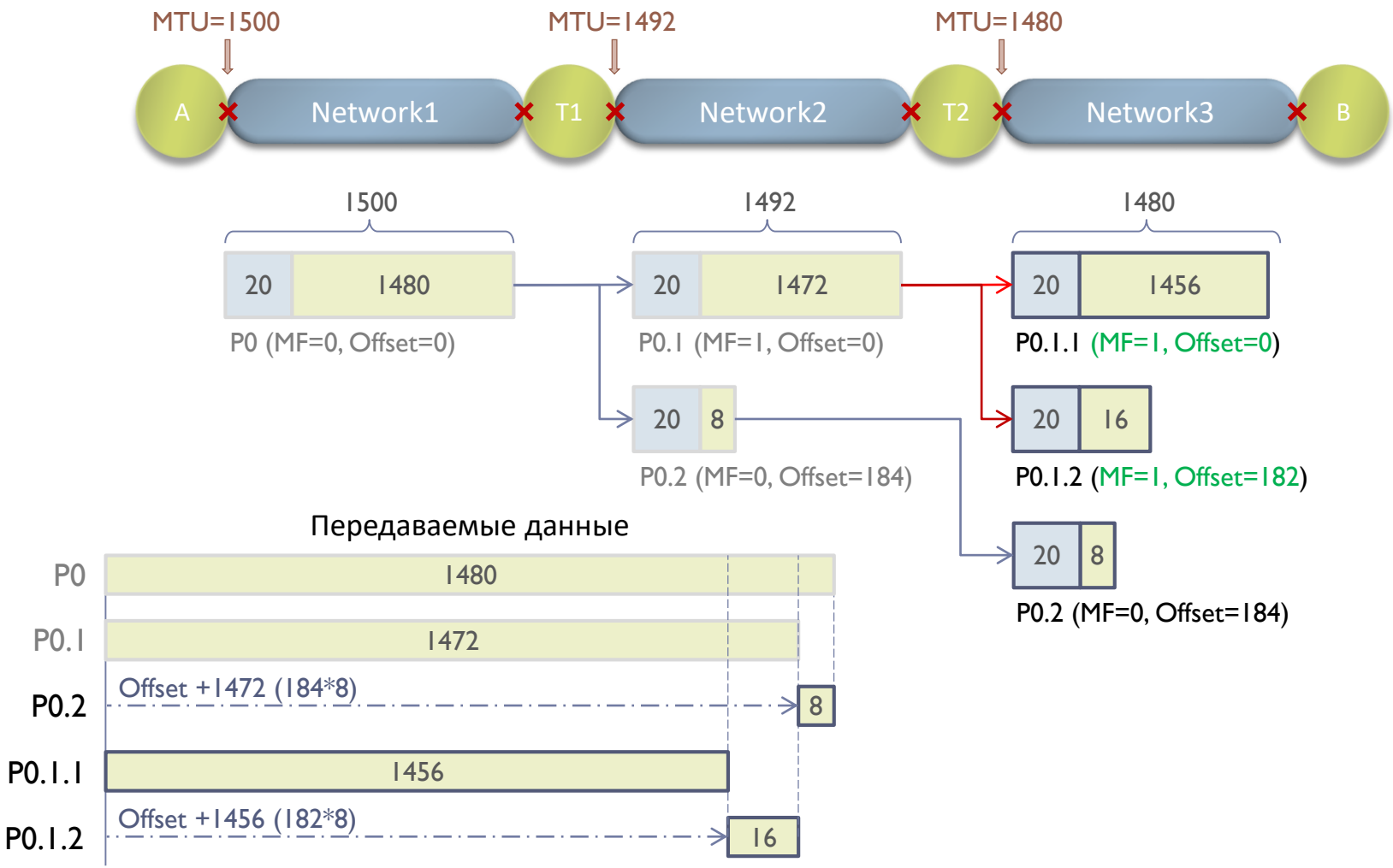




Механизм фрагментации пакетов



Механизм фрагментации пакетов



Замечания по фрагментации пакетов

Механизм фрагментации на практике показал свою низкую эффективность:

- Увеличивает объем служебного трафика, передаваемого по сети (размножение IP заголовков);
- Нагружает транзитные узлы;
- «Съедает» буферную память оконечных узлов;
- Увеличивает время задержки;
- Уменьшает эффективную скорость передачи;
- Способствует нарушению порядка приема пакетов;
- Создает почву для атак злоумышленников.

По этим причинам механизм фрагментации не включен в IP версии 6.

А как быть с различным значением MTU ?

Замечания по фрагментации пакетов

Механизм фрагментации на практике показал свою низкую эффективность:

- Увеличивает объем служебного трафика, передаваемого по сети (размножение IP заголовков);
- Нагружает транзитные узлы;
- «Съедает» буферную память оконечных узлов;
- Увеличивает время задержки;
- Уменьшает эффективную скорость передачи;
- Способствует нарушению порядка приема пакетов;
- Создает почву для атак злоумышленников.

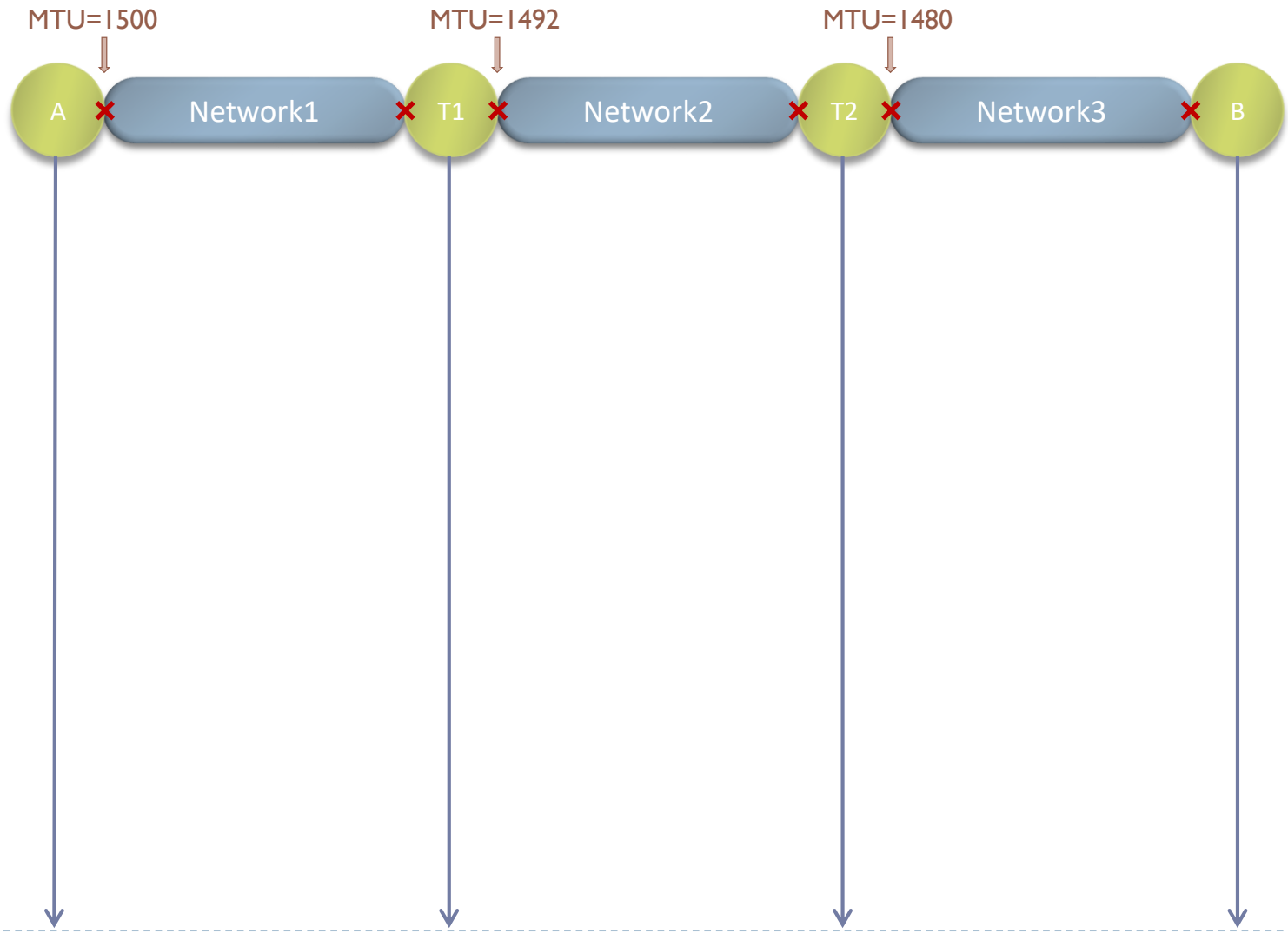
По этим причинам механизм фрагментации не включен в IP версии 6.

А как быть с различным значением MTU ? → **Предотвращать фрагментацию !!!**

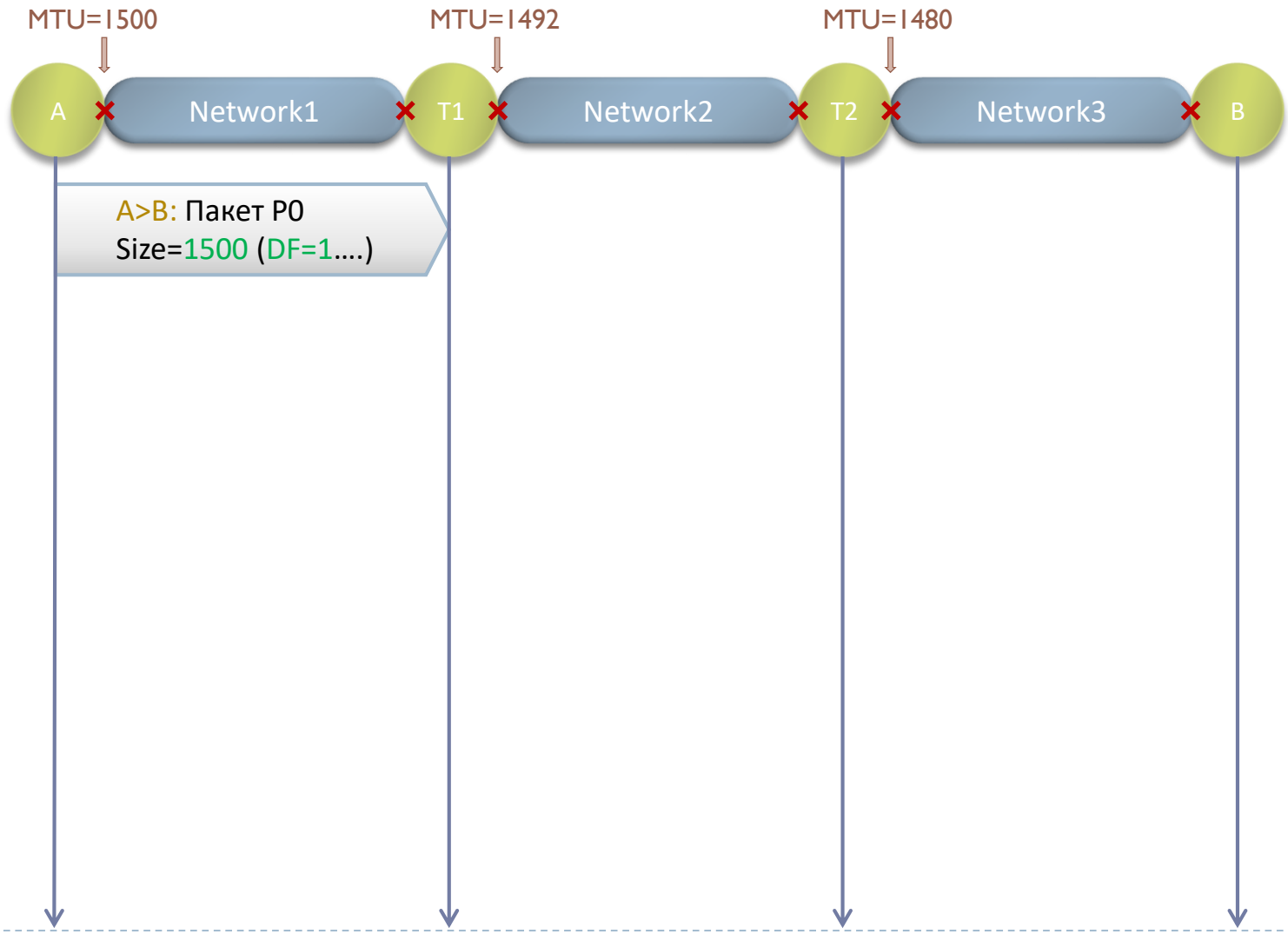
Узел-отправитель должен формировать пакеты размером не более *минимального значения MTU по всему пути доставки* пакетов (Path-MTU).

Для этого применяется метод автоматического обнаружения Path-MTU.

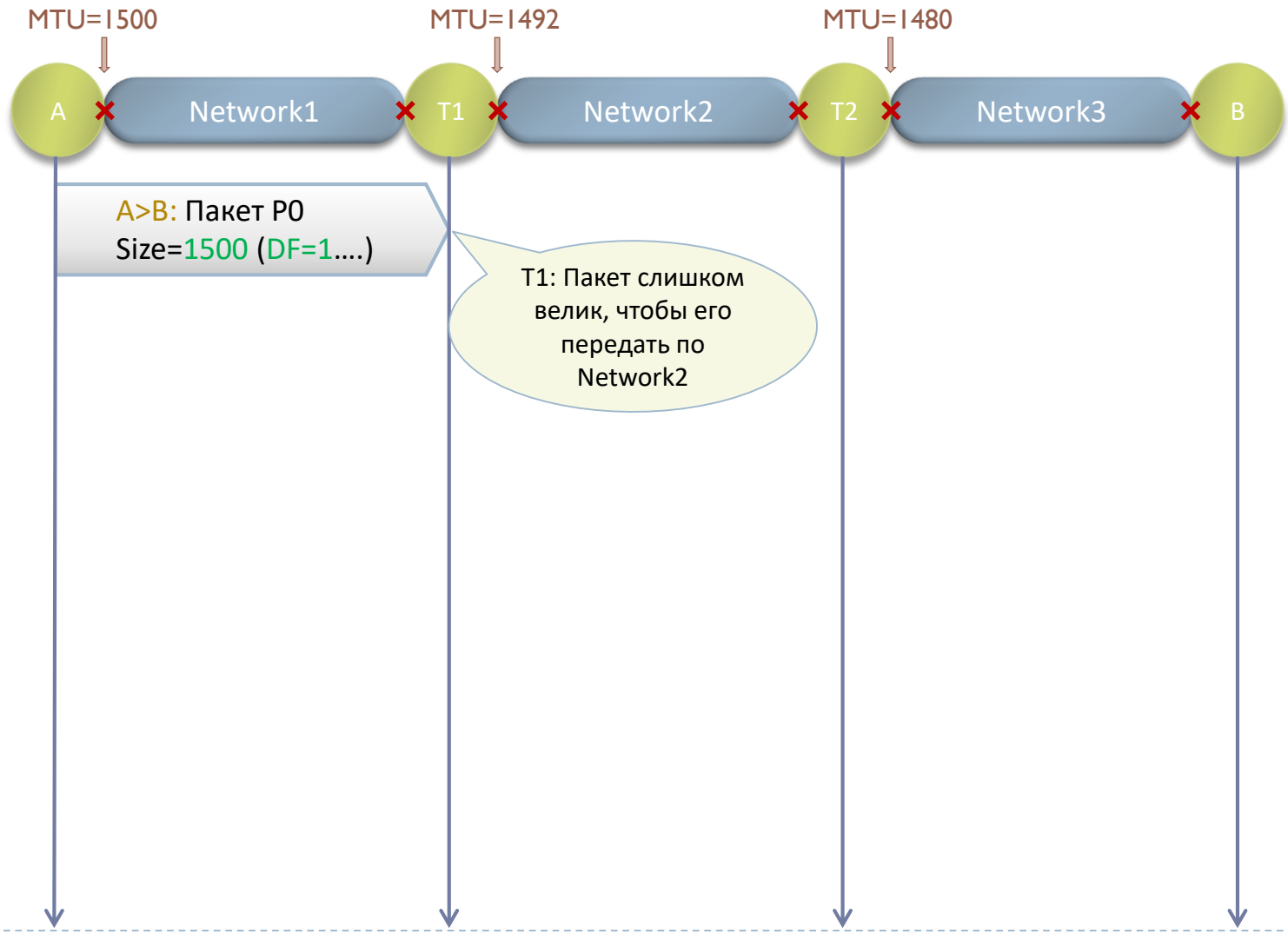
Path MTU Discovery



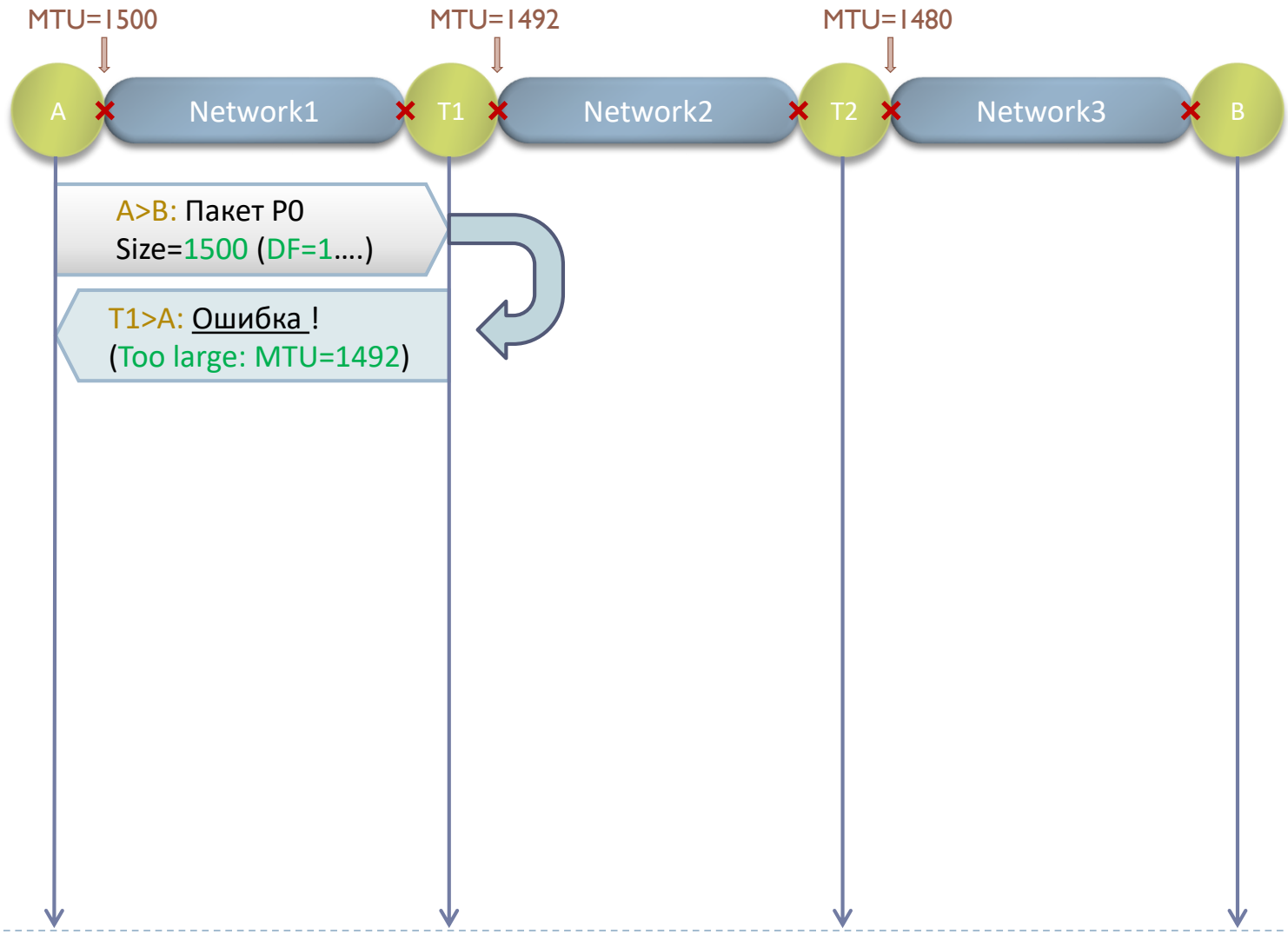
Path MTU Discovery



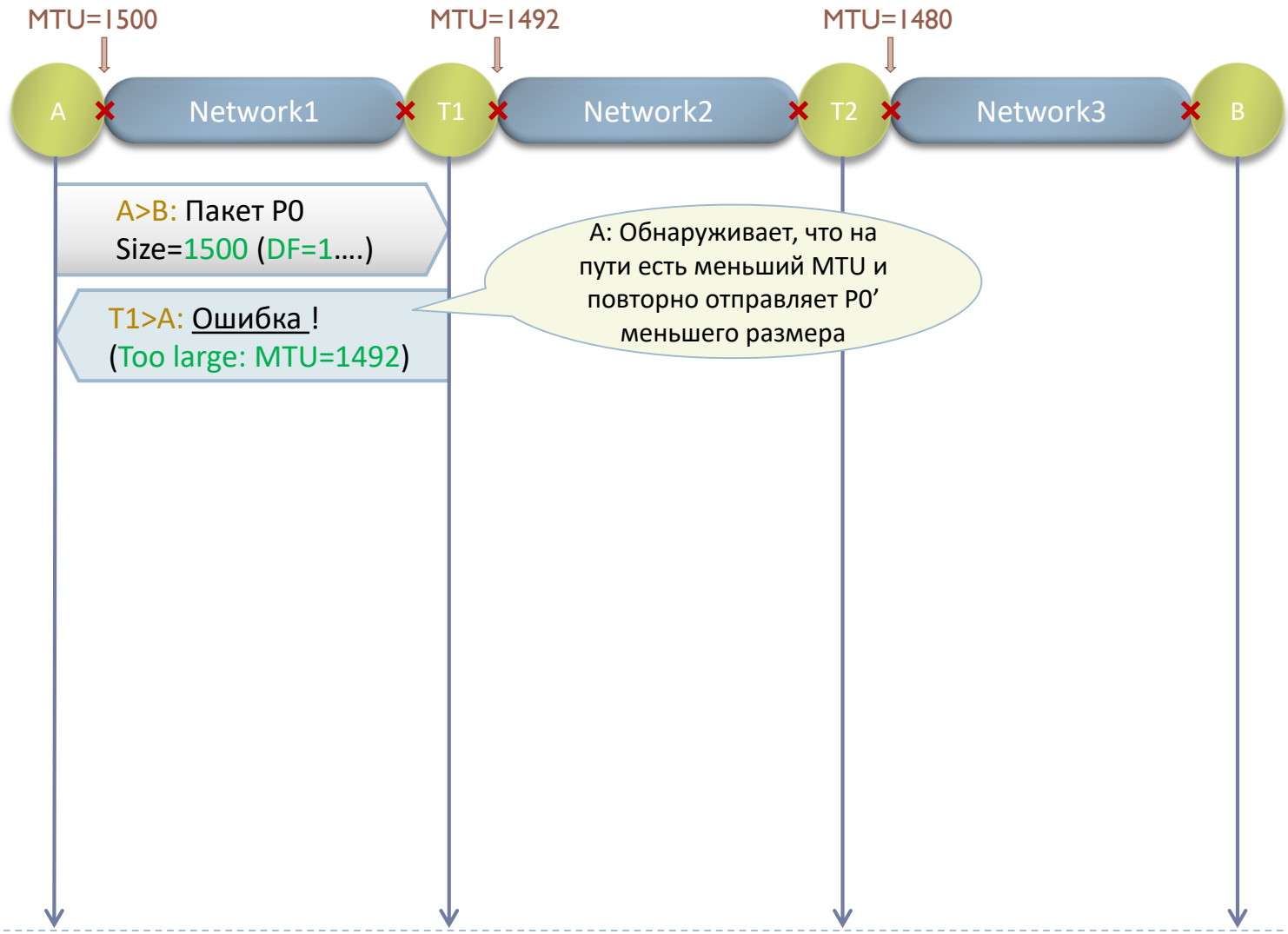
Path MTU Discovery



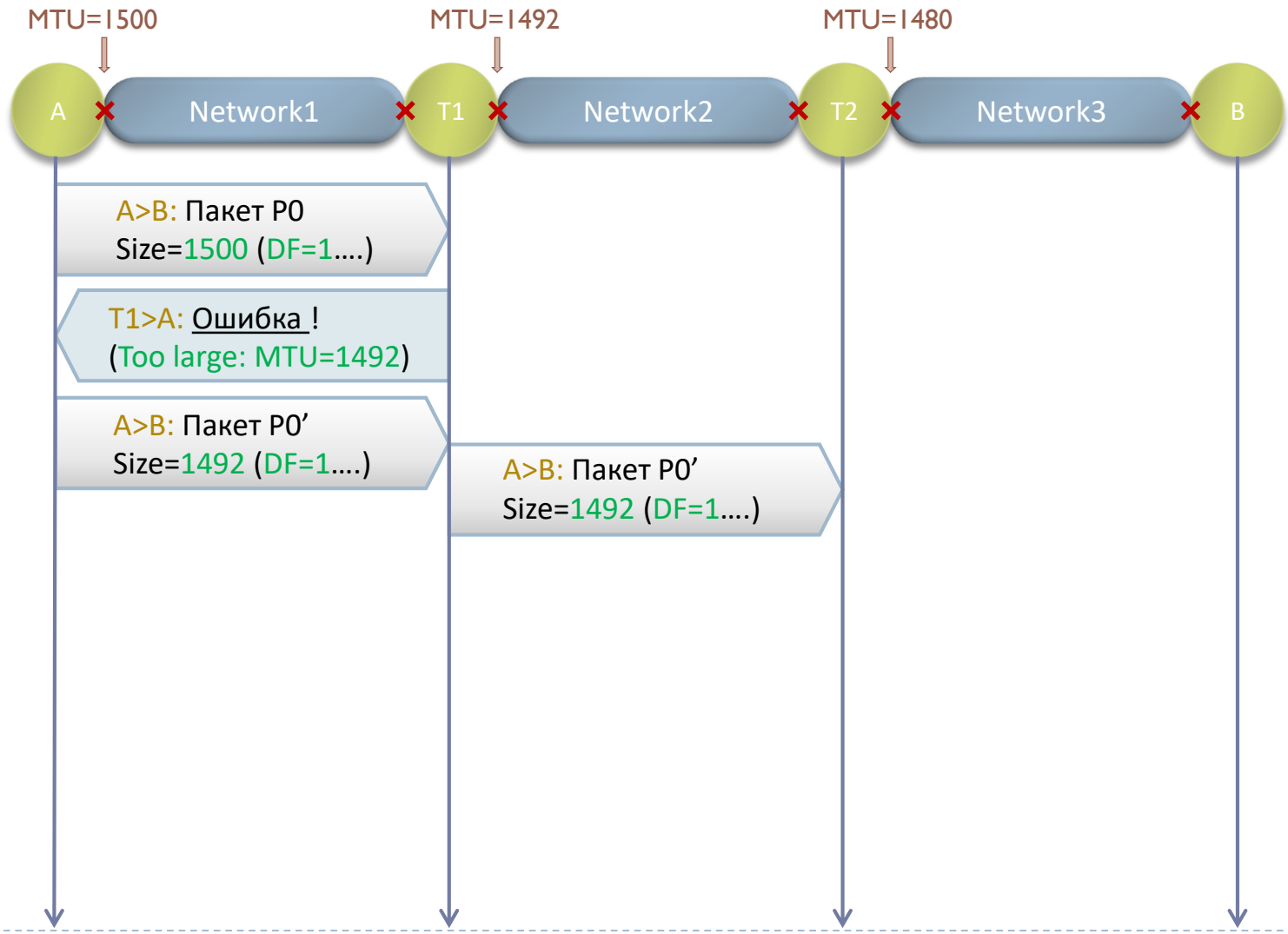
Path MTU Discovery



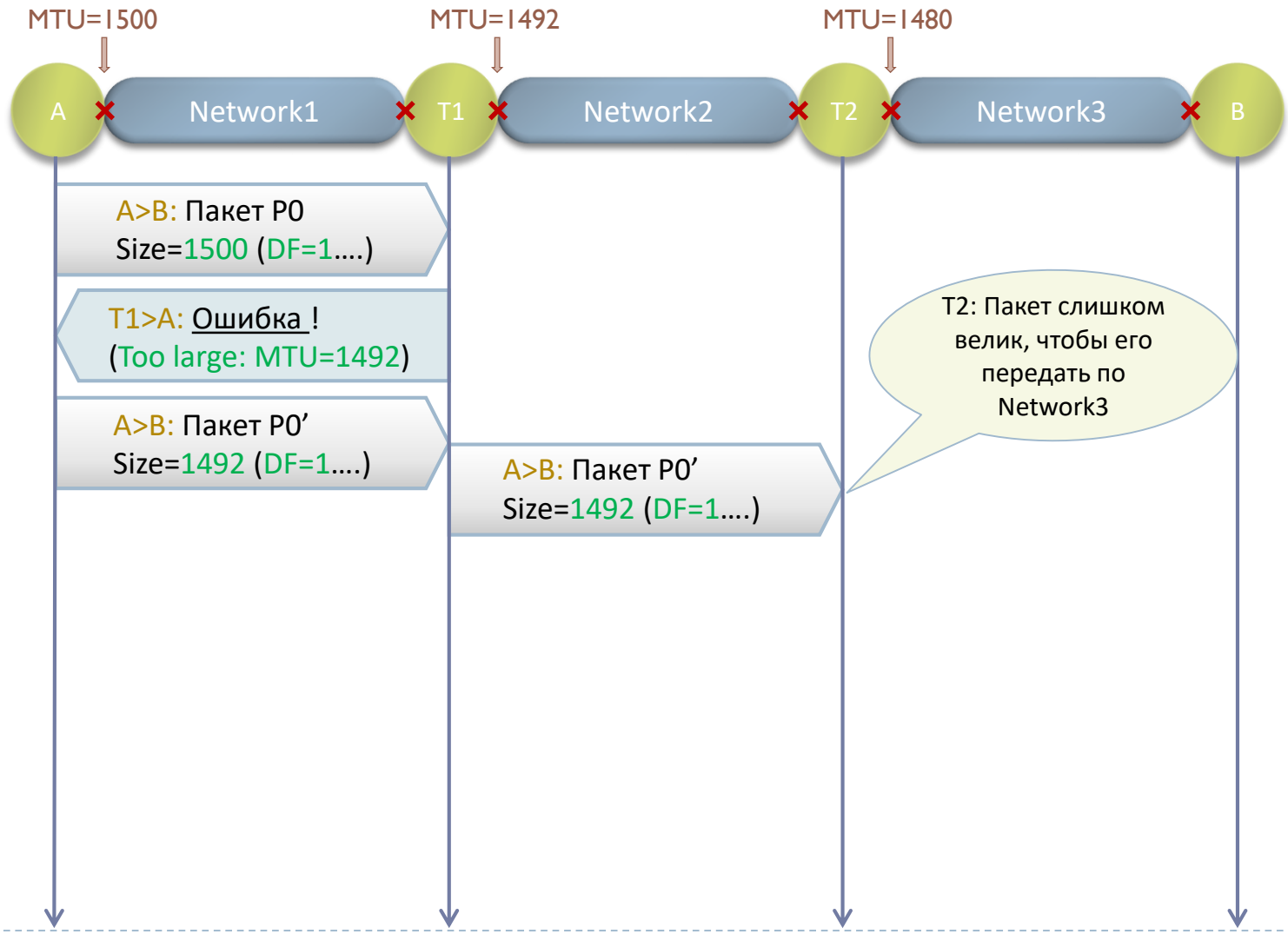
Path MTU Discovery



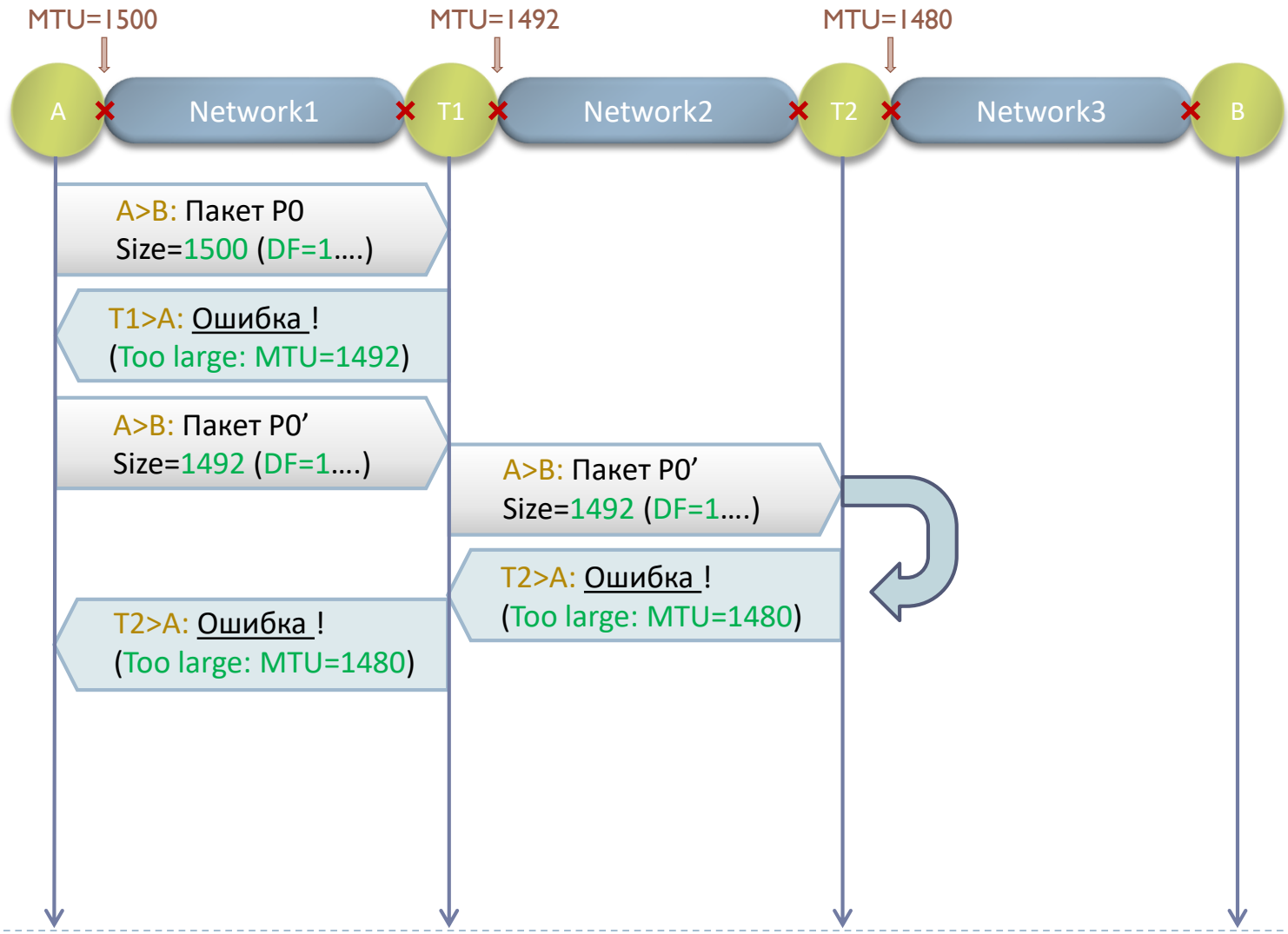
Path MTU Discovery



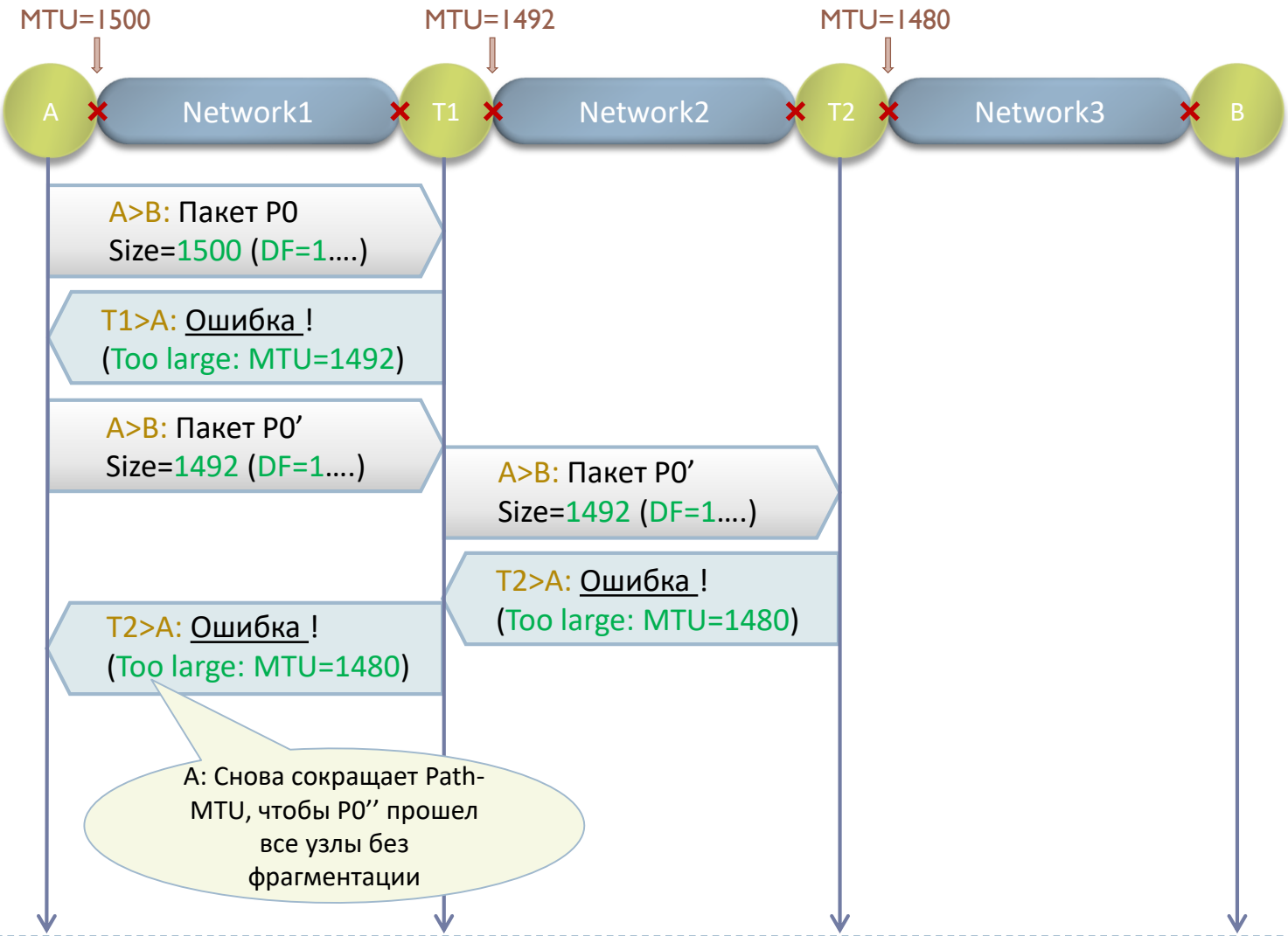
Path MTU Discovery



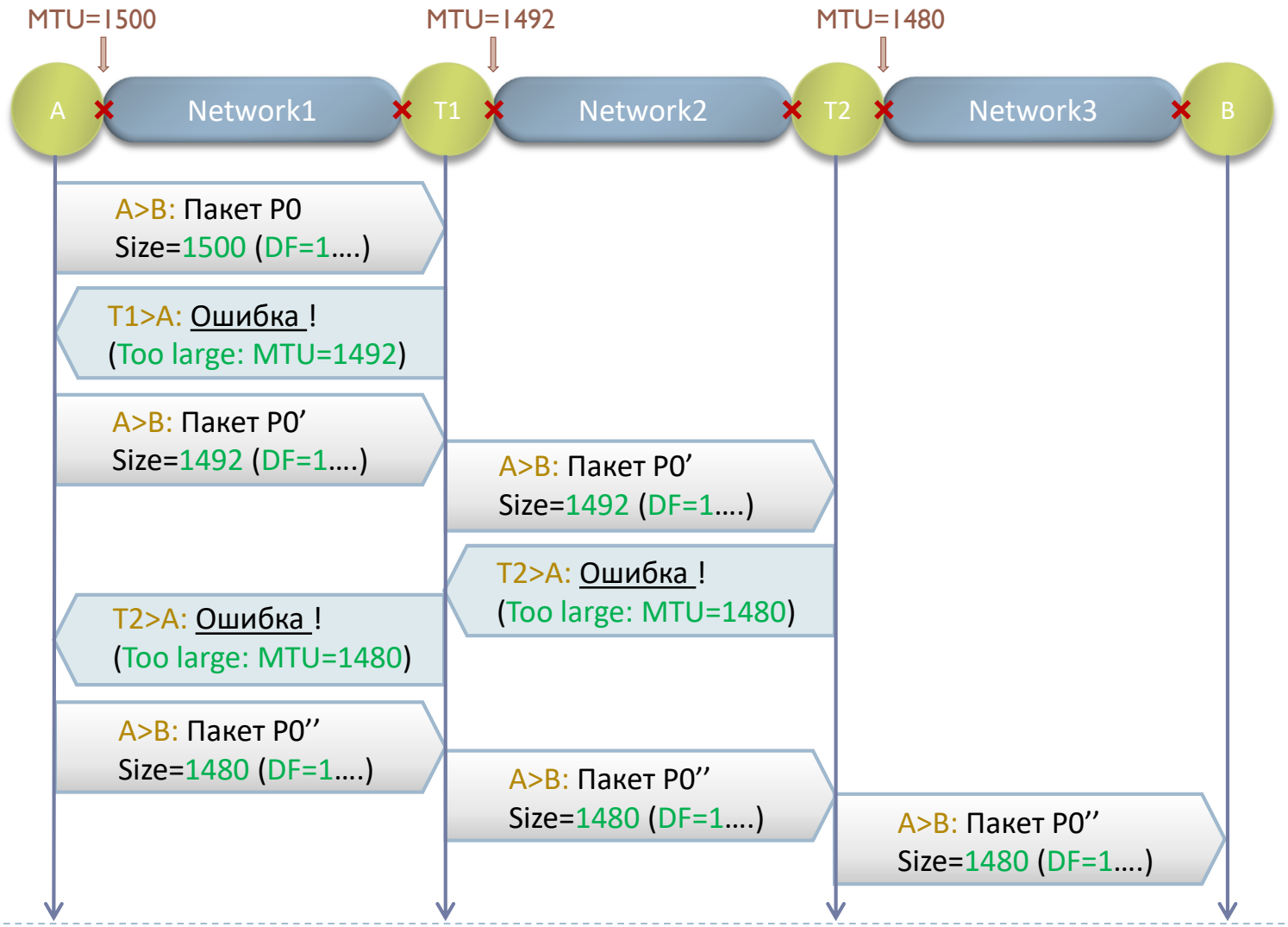
Path MTU Discovery



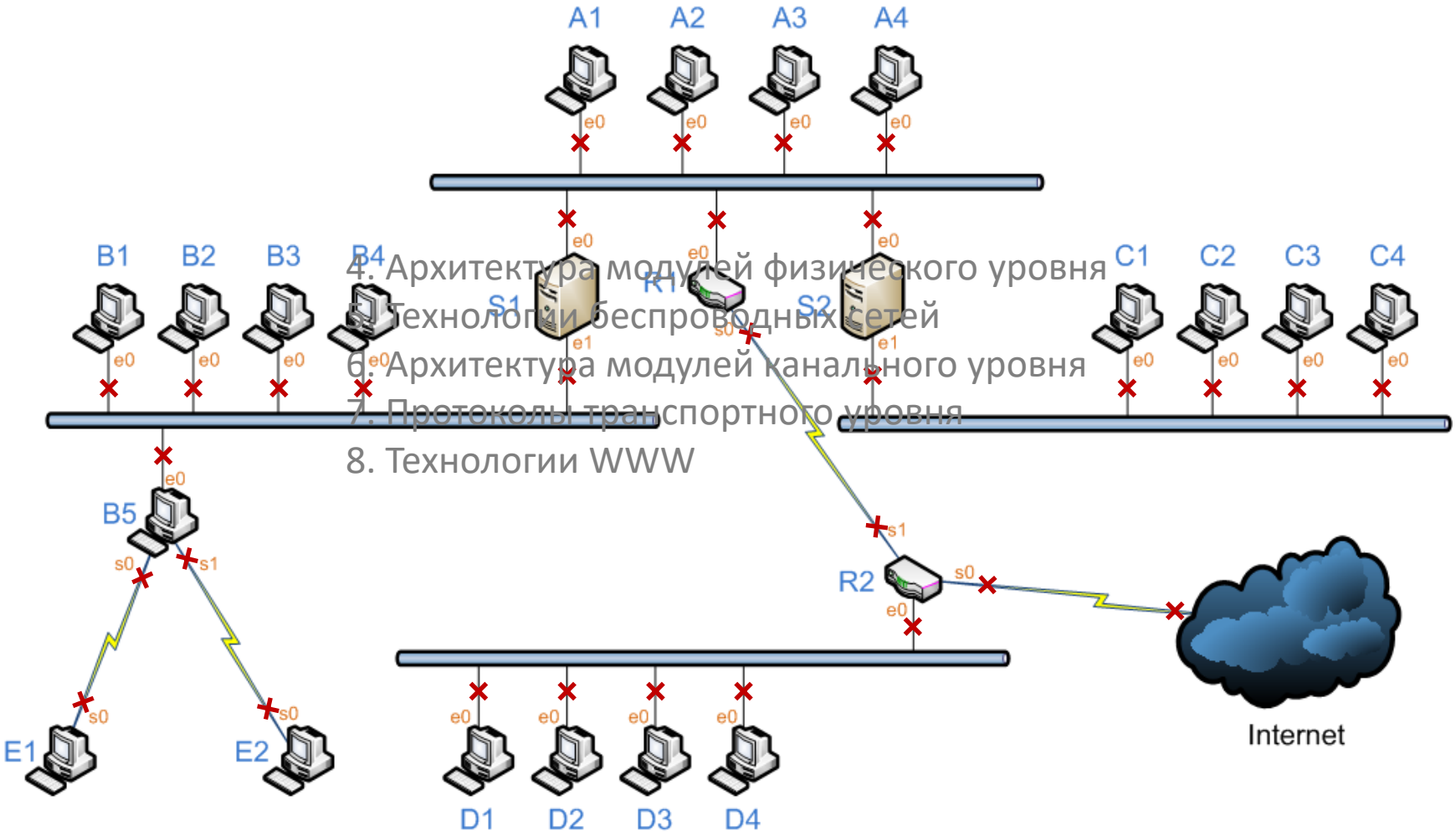
Path MTU Discovery



Path MTU Discovery



Пример интерсети

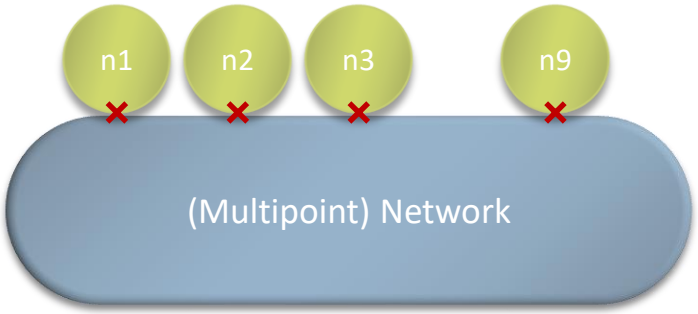


4. Архитектура модулей физического уровня
5. Технологии беспроводных сетей
6. Архитектура модулей канального уровня
7. Протоколы транспортного уровня
8. Технологии WWW

План курса

1. Введение в компьютерные сети
2. Основные методы построения СПД
3. **Архитектура Internet Protocol Suite (TCP/IP)**
    - 3.1. Адресация в IP сетях
    - 3.2. Протокол IP (v4)
    - **3.3. Протокол ARP**
    - 3.4. Служебный трафик и протокол ICMP
4. Архитектура модулей физического уровня
5. Технологии беспроводных сетей
6. Архитектура модулей канального уровня
7. Протоколы транспортного уровня
8. Технологии WWW

Особенности многоточечных сетей Layer2

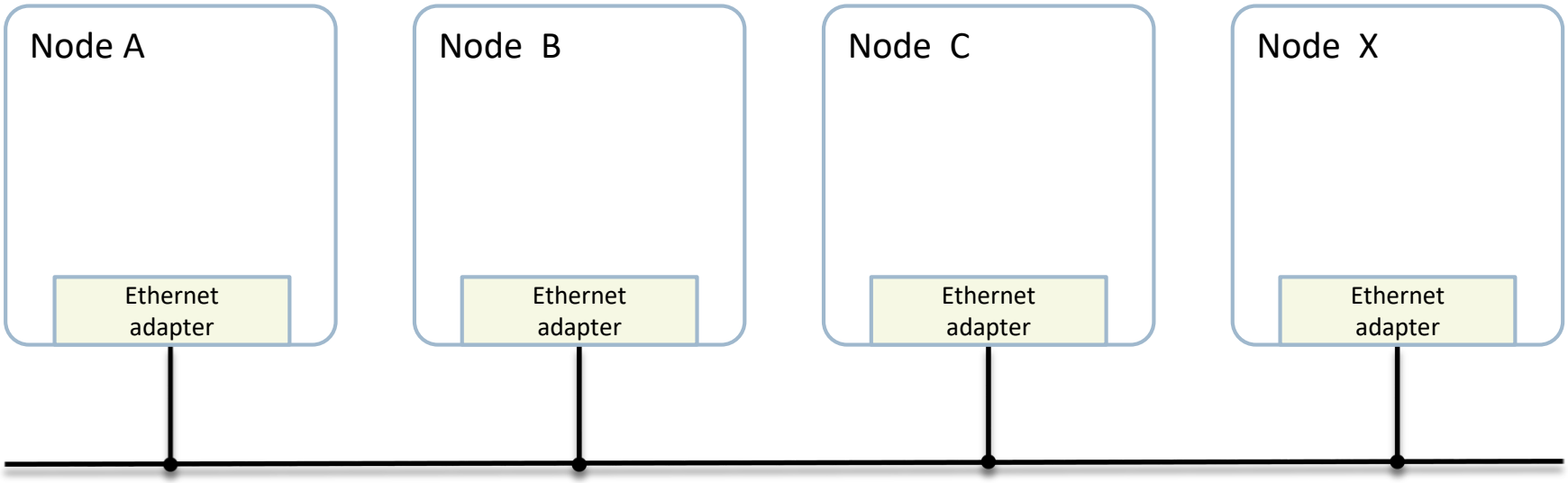


В многоточечной сети несколько станций подключены к общей среде передачи:

- широковещательный режим (broadcast mode) – сигнал, передаваемый одной станцией, могут воспринимать все остальные станции
- разделяемая среда (shared media) – станциям приходится делить друг с другом один общий тракт передачи сигнала и разговаривать по очереди
- логическая адресация станций (logical addressing) – каждая станция желает принимать только те кадры, которые предназначены для нее и игнорировать все остальные, для этого необходимы адреса уровня 2

Самыми распространенными в мире сетевыми технологиями канального уровня являются разновидности Ethernet (10/100/1000 Mbit/s, 10/25/40/100 Gbit/s, Wi-Fi)

Широковещательная сеть Ethernet



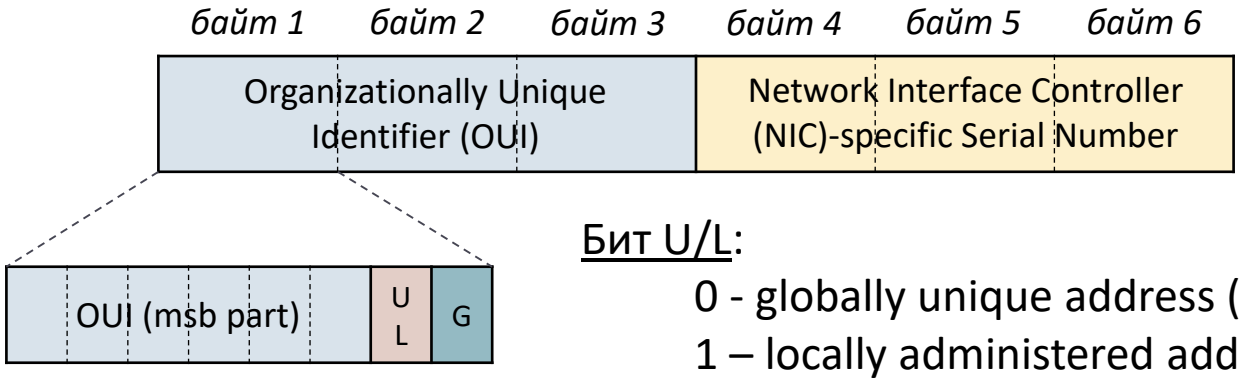
Широковещательная шина (broadcast bus)

(6 байт) **Destination MAC**	*(6 байт)* **Source MAC**	*(2 б)* **Ether Type**	*(64-1500 байтов)* **Данные кадра (Payload)**

Формат кадра (frame), передаваемого по шине

Что такое MAC-адрес

- ✓ 48-битовый (6-байтовый) двоичный код
- ✓ Потенциально обеспечивает 2^{48} = 281,474,976,710,656 уникальных значений
- ✓ Текстуально записывается в виде шестнадцатеричных чисел:
  - 01-23-45-67-89-ab или 01:23:45:67:89:ab или 0123.4567.89ab
- ✓ Имеет следующую внутреннюю структуру:



Бит U/L:

0 - globally unique address (OUI)

1 – locally administered address

Бит G:

0 – unicast address

1 – group address

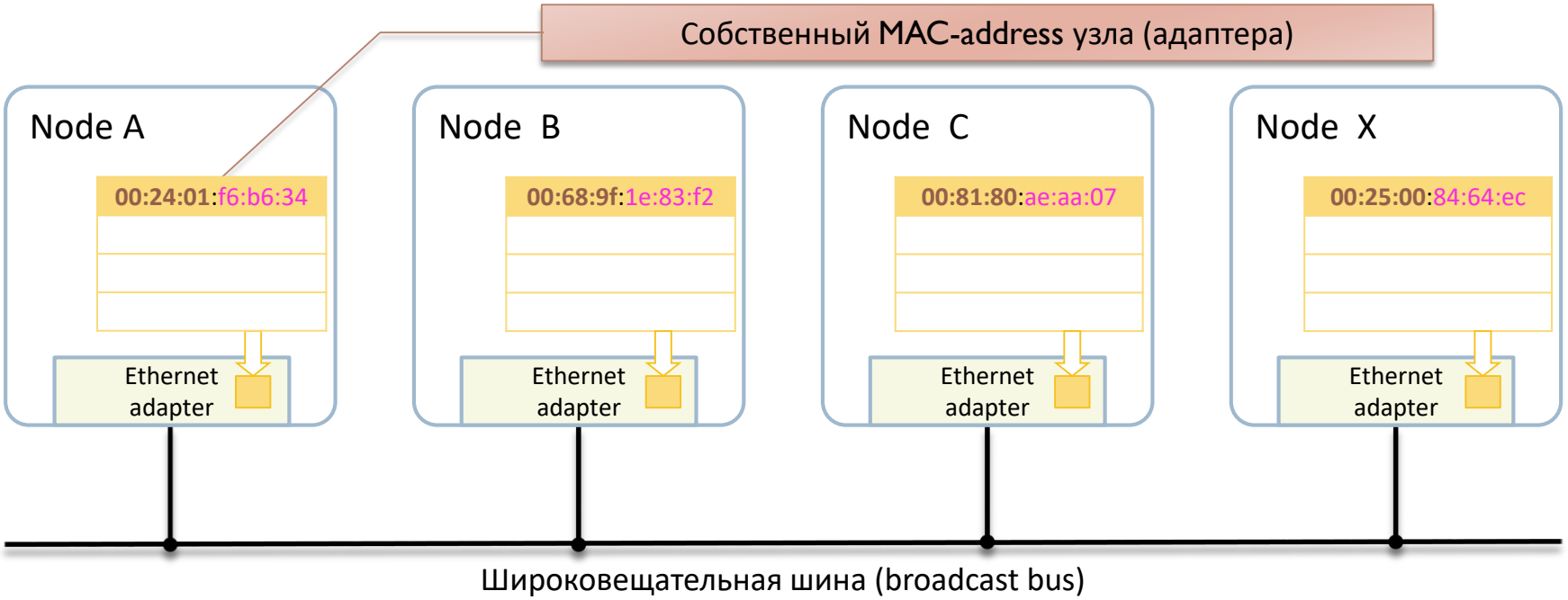
Применение MAC адресов

- ✓ MAC адреса используются в качестве адресов канального уровня для большинства сетевых технологий с многоточечной структурой, например:
  - Ethernet всех разновидностей (IEEE 802.3)
  - Wi-Fi (IEEE 802.11)
  - Bluetooth (IEEE 802.15*)
  - Token-Ring (IEEE 802.5)
  - Fibre Channel, Serial Attached SCSI (SAS)
  - ITU G.hn и др.
- ✓ Четыре разновидности MAC адресов:

U/L	G	Назначение	Структура адреса
0	0	Глобально уникальный индивидуальный	**Uu:UU:UU**:DD:DD:DD
0	1	Глобальный групповой	**Uu:UU:UU**:GG:GG:GG
1	0	Индивидуальный адрес местного назначения	Ss:SS:SS:SS:SS:SS
1	1	Групповой адрес местного назначения	Mm:MM:MM:MM:MM:MM

- ✓ MAC адрес ff:ff:ff:ff:ff:ff – опознается всеми адаптерами как broadcast

Широковещательная сеть Ethernet



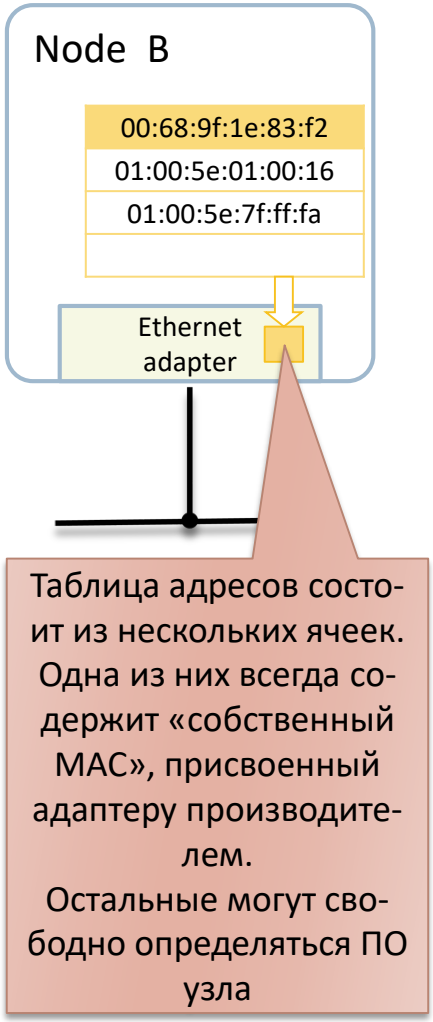
Собственные MAC адреса (глобально уникальные) присваиваются производителем оборудования при производстве:

00:24:01:f6:b6:34

OUI Серийный номер

OUI (Organization Unique Identifier) выделяется *IEEE* производителям сетевого оборудования по запросу

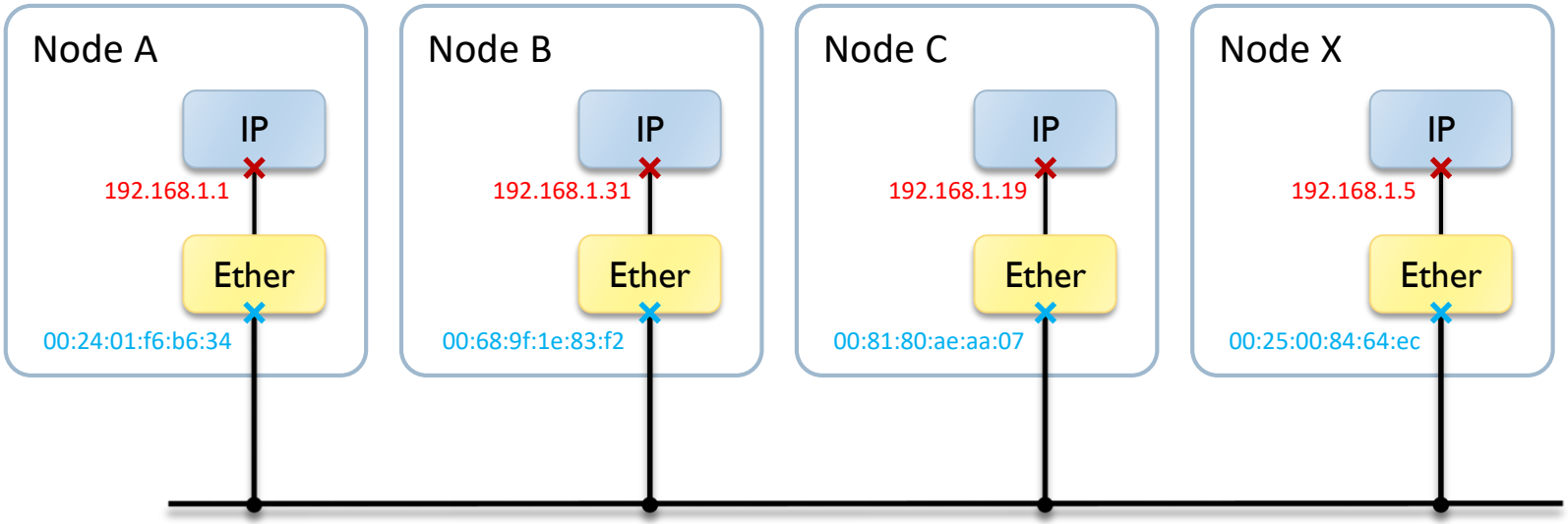
Принцип работы адаптера Ethernet



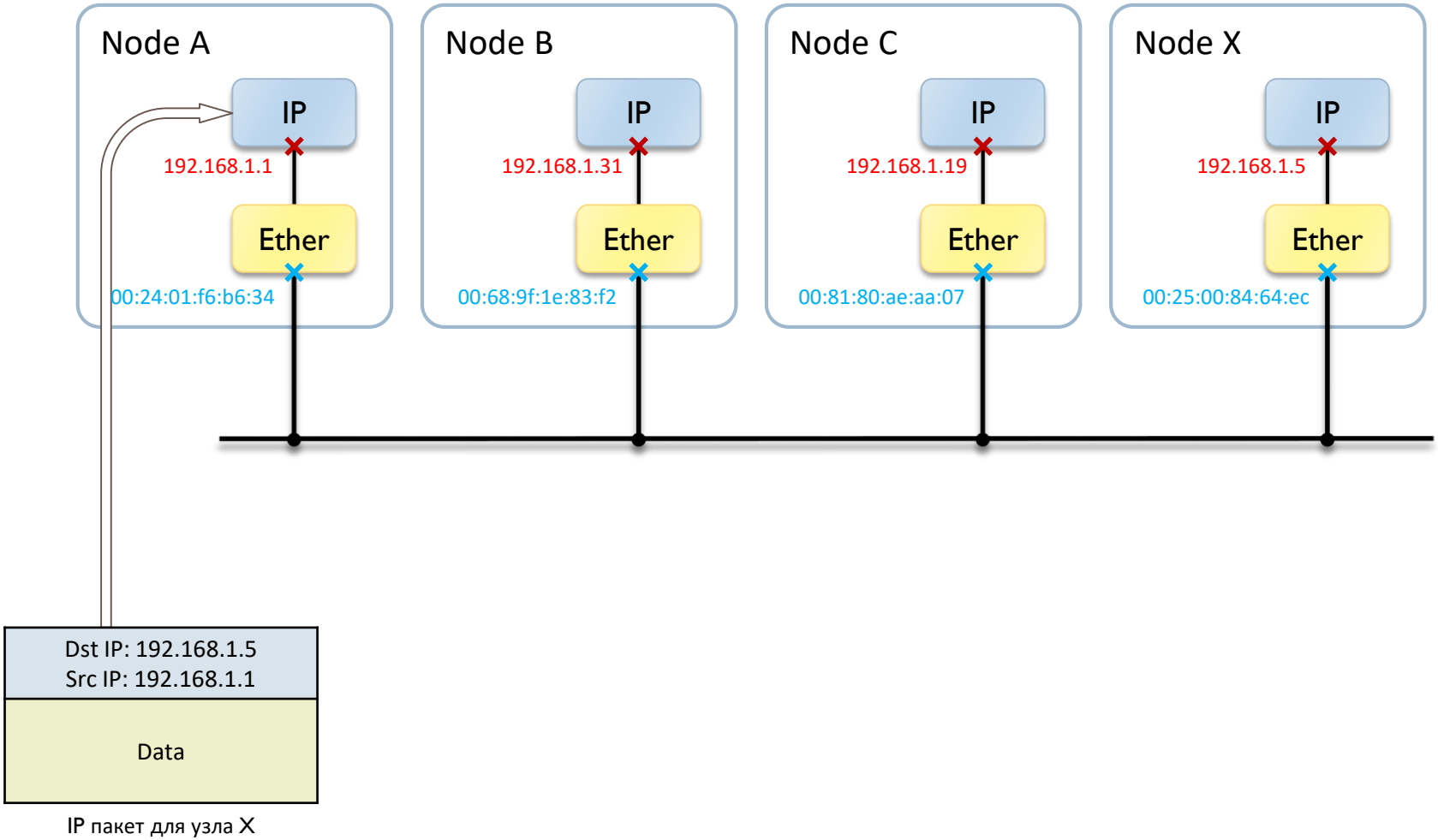
- Сетевой адаптер узла «слышит» и принимает в свой буфер все кадры, передаваемые по шине
- Для каждого принятого кадра анализируется поле заголовка *Destination MAC*
- Только в следующих случаях принятый кадр передается на обработку:
  - ✓ Содержимое *Destination MAC* совпало с одной из ячеек **таблицы адресов** адаптера
  - ✓ *Destination MAC* = ***ff:ff:ff:ff:ff:ff*** – специальный broadcast MAC address **«слушайте все»**
  - ✓ Адаптер переведен в promiscuous mode (режим «всеядности»)

Если ни одно из условий не выполнилось – кадр сбрасывается адаптером и ПО узла его «не видит»

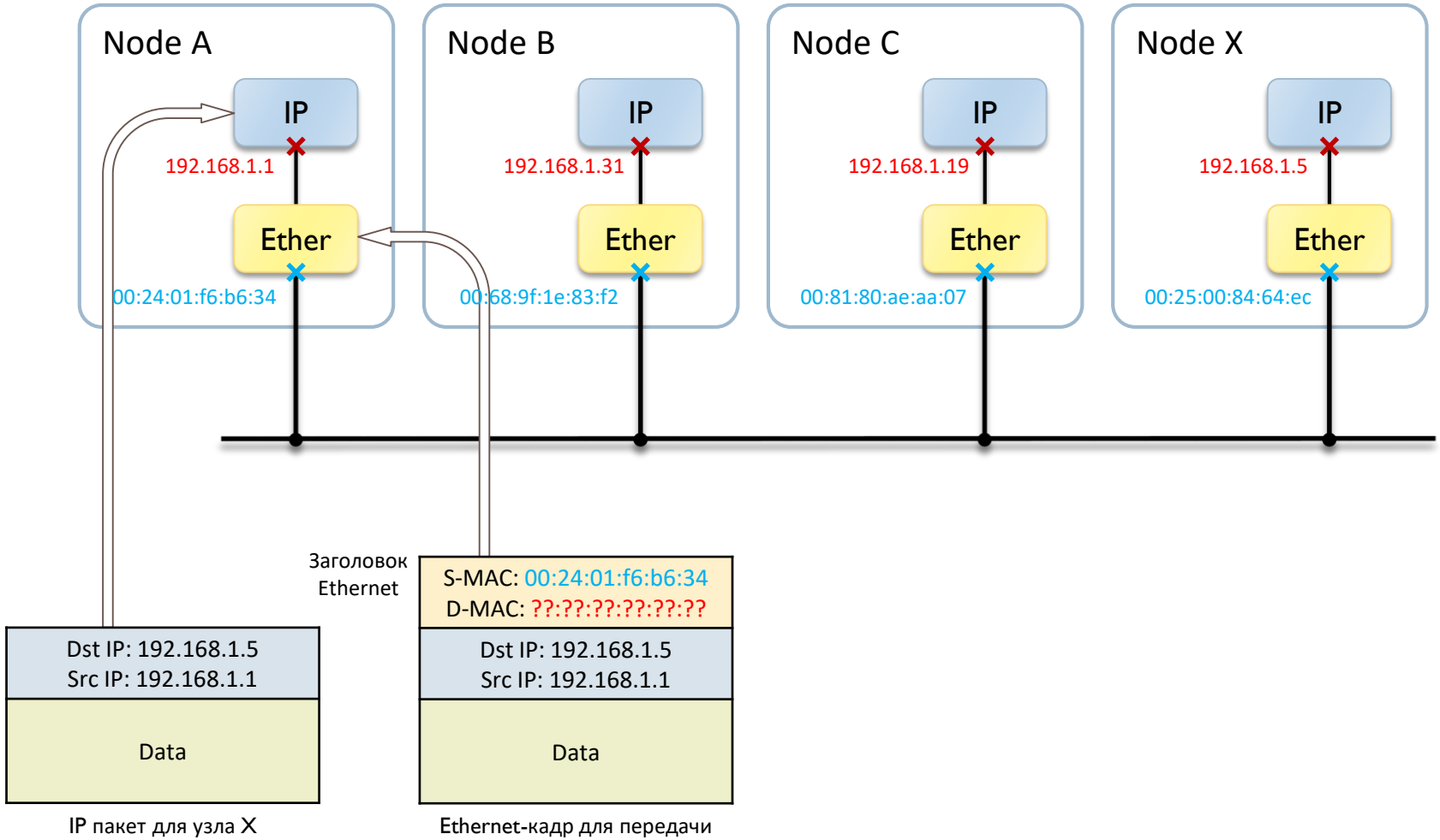
Проблема IP адресации в Ethernet



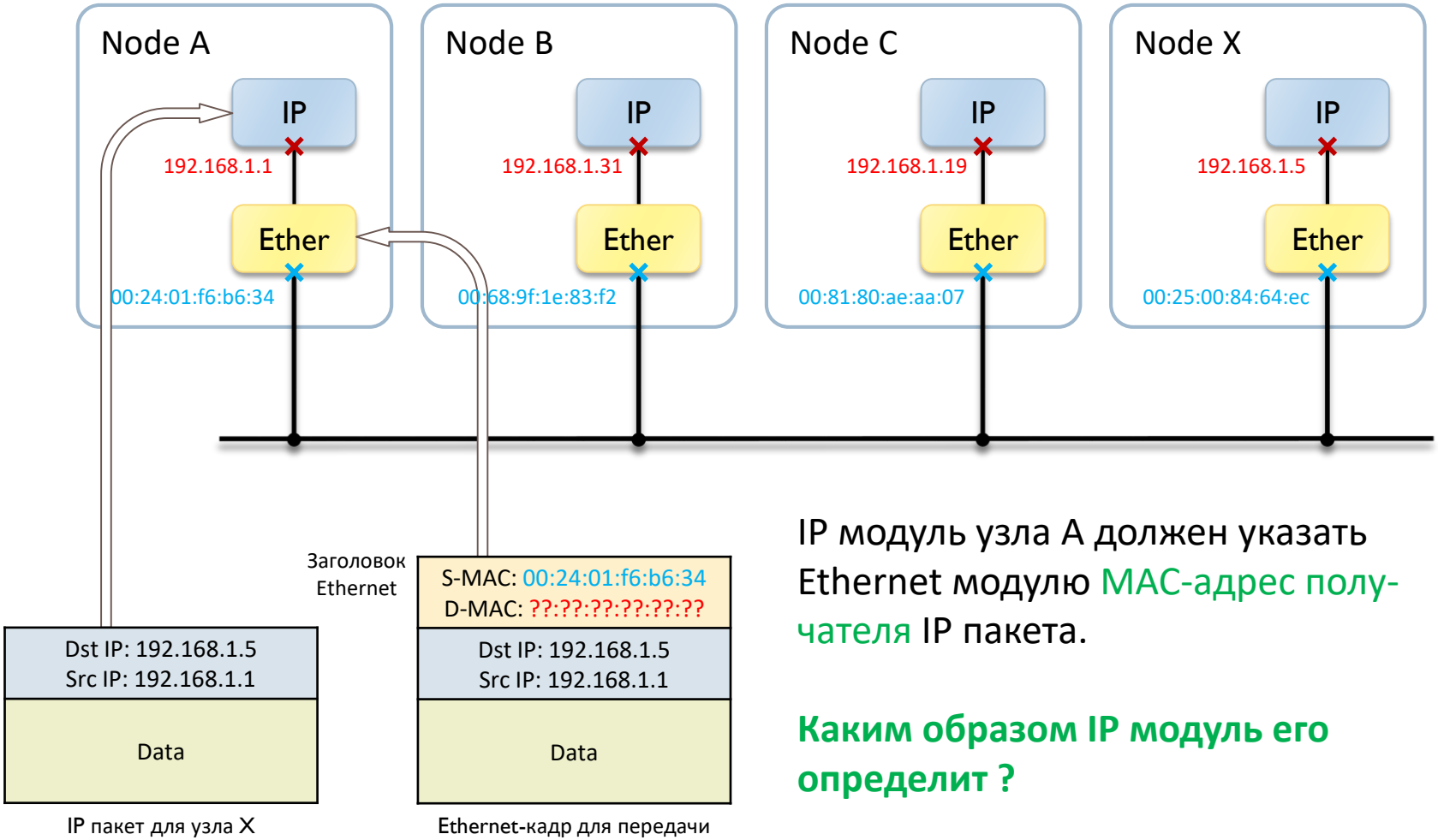
Проблема IP адресации в Ethernet



Проблема IP адресации в Ethernet



Проблема IP адресации в Ethernet

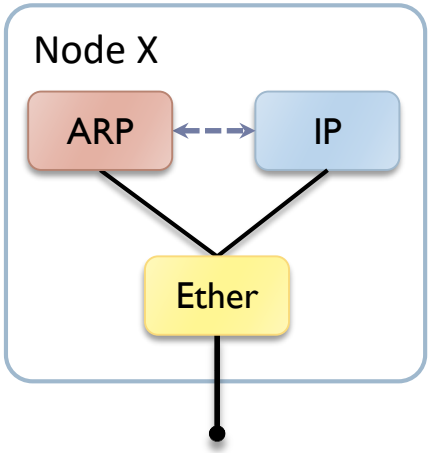


IP модуль узла A должен указать Ethernet модулю MAC-адрес получателя IP пакета.

Каким образом IP модуль его определит ?

Протокол ARP

- ✓ ARP (Address Resolution Protocol, RFC 826) – вспомогательный протокол, определяющий MAC адрес соседнего узла по IP адресу(*)
- ✓ ARP функционирует на одном уровне с IP:
- ✓ Модуль IP обращается к модулю ARP каждый раз, когда пакет должен доставляться через многоточечное звено (тип маршрута – **U**)
- ✓ Модуль ARP ведет у себя таблицу примерного вида:



If	IP addr	MAC addr	Type
Eth0	192.168.1.1	00:24:01:f6:b6:a4	C
Eth0	192.168.1.199	00:1c:26:ac:5c:2f	C
Eth0	192.168.1.23	00:00:00:00:00:00	
Eth0	192.168.1.255	ff:ff:ff:ff:ff:ff	M

Type:
C – completed
M – manual (static)

Операции протокола ARP

- ARP-Resolve – определить MAC адрес по указанному IP адресу
- ARP-Probe – проверить не занят ли указанный IP адрес
- ARP-Announcement (Gratuitous-ARP) – оповестить о MAC адресе указанного IP адреса с целью обновления кэша

Общая структура ARP-пакета

(2 б.) **HTYPE**	*(2 б.)* **PTYPE**	*(1 б.)* **HLEN**	*(1 б.)* **PLEN**	*(2 б.)* **OPER**	*(6 байт)* **SHA**	*(4 байт)* **SPA**	*(6 байт)* **THA**	*(4 байт)* **TPA**
0001	0800	06	04	nnnn	ss:ss:ss:ss:ss:ss	s.s.s.s	tt:tt:tt:tt:tt:tt	t.t.t.t

OPER – operation:
0001 – ARP-request
0002 – ARP-response

SHA – sender hardware (MAC) address
SPA – sender protocol (IP) address
THA – target hardware (MAC) address
TPA – target protocol (IP) address

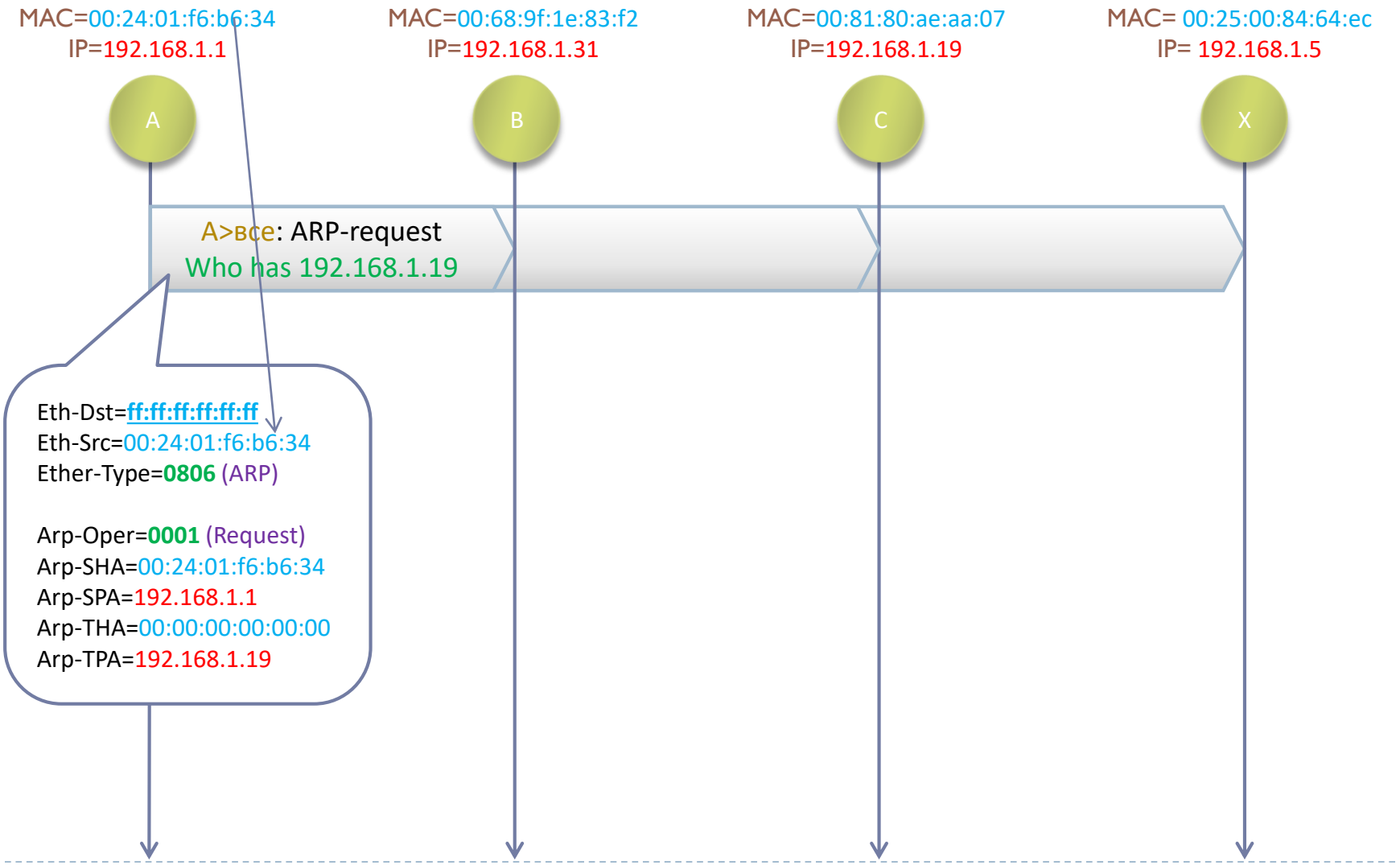
Содержимое ARP пакетов

Виды операций ARP:

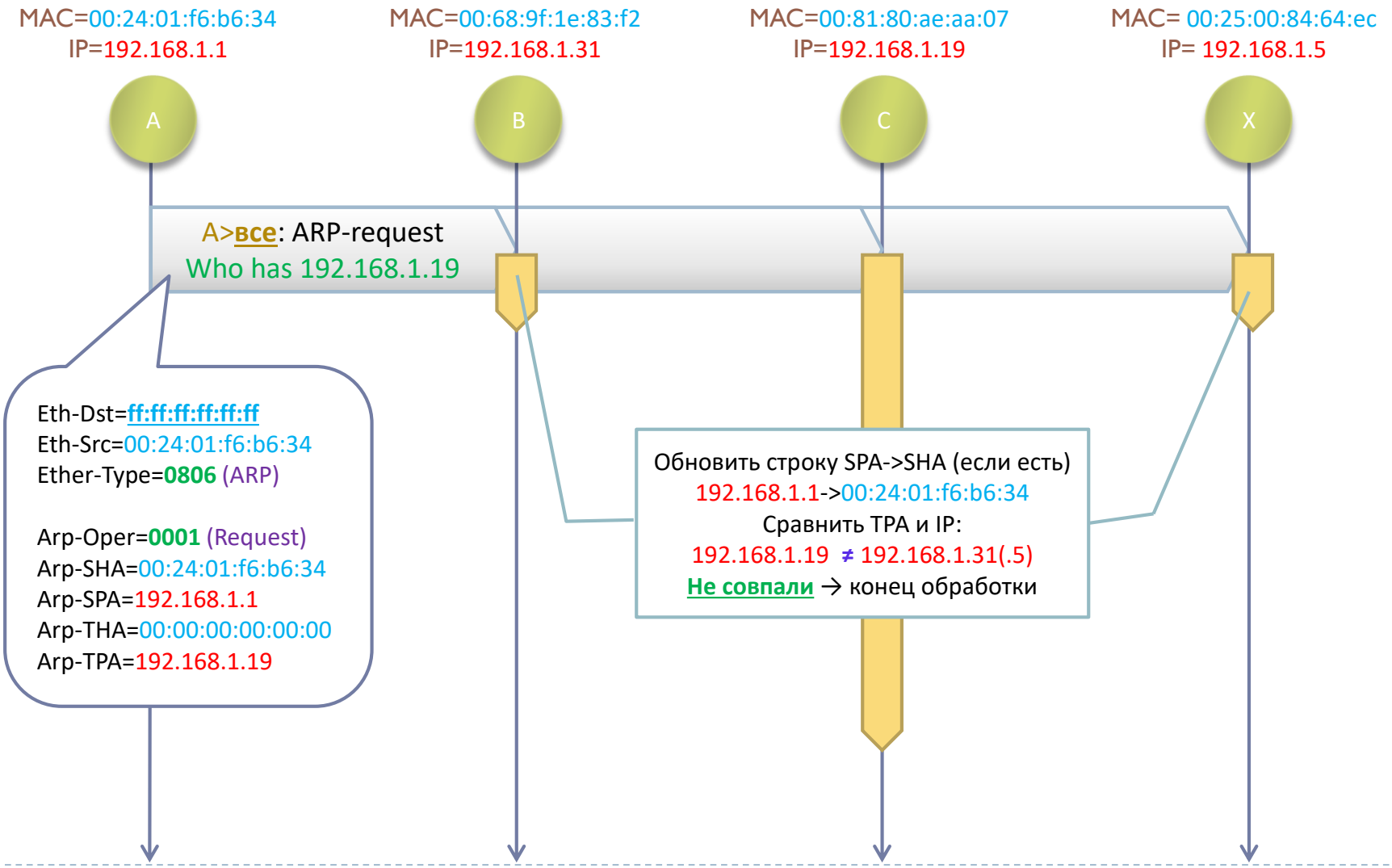
- Определение IP адреса (ARP-Resolve)
- Проверка занятости IP адреса (ARP-Probe)
- Оповещение о назначении/переназначении IP адреса (Gratuitous-ARP)

(6 байтов) **HTYPE-PTYPE**	*(2 байта)* **OPER**	*(6 байтов)* Sender HW Addr (**SHA**)	*(4 байта)* Sender Paddr (**SPA**)	*(6 байтов)* Target HW Addr (**THA**)	*(4 байта)* Target Paddr (**TPA**)
000108000604	0001 (Request)	MAC запрашивающего	IP запраши-вающего	00:00:00:00:00	искомый IP
	0002 (Response)	MAC узла с искомым IP	искомый IP	MAC запрашивающего	IP запраши-вающего
	0001 (Probe)	MAC проверяющего	0.0.0.0	00:00:00:00:00	проверяе-мый IP
	0001 (Announce)	MAC оповещающего	IP опове-щающего	00:00:00:00:00	IP опове-щающего
	0002 (Announce)	MAC оповещающего	IP опове-щающего	MAC оповещающего	IP опове-щающего

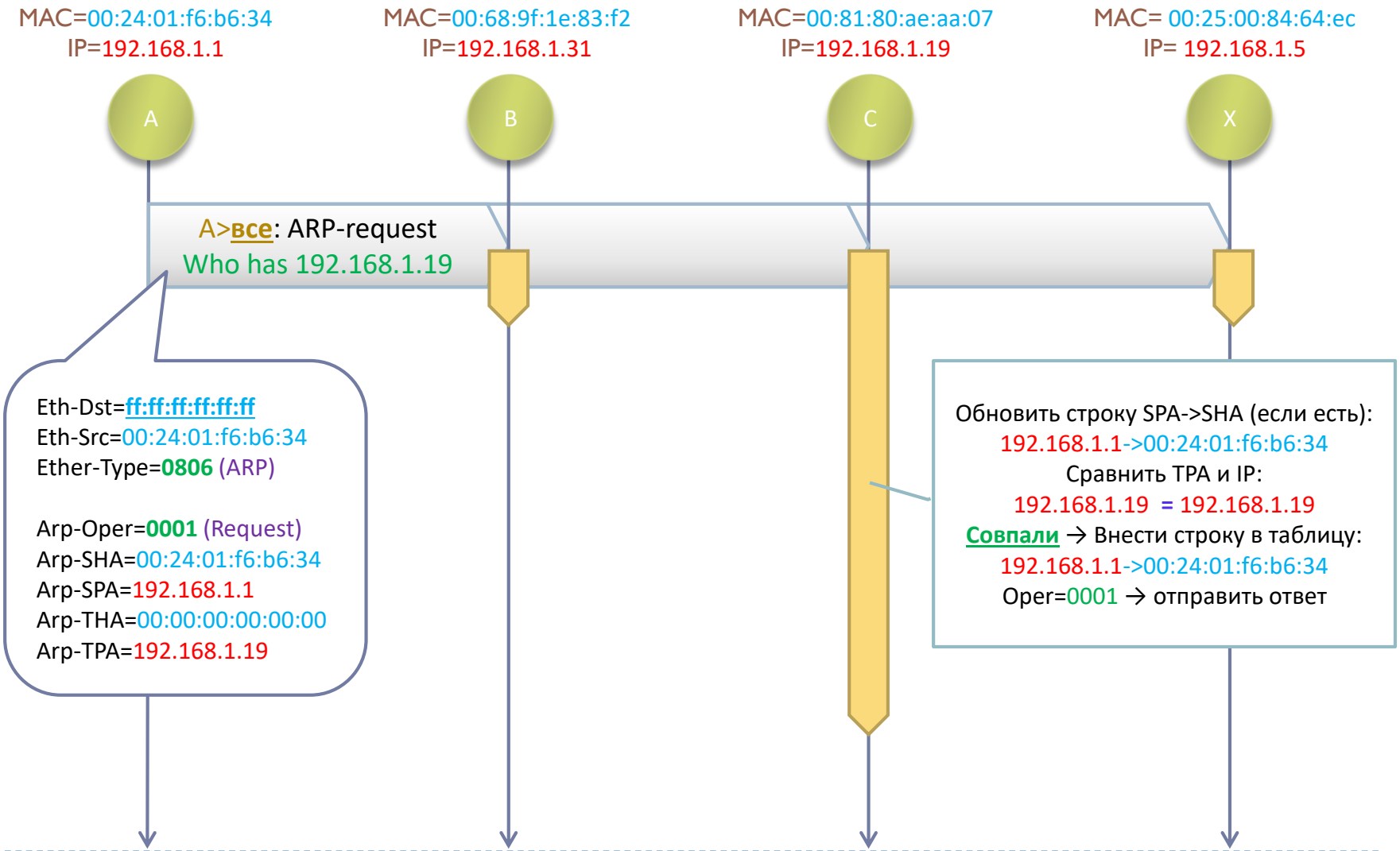
Процедура ARP-Resolve



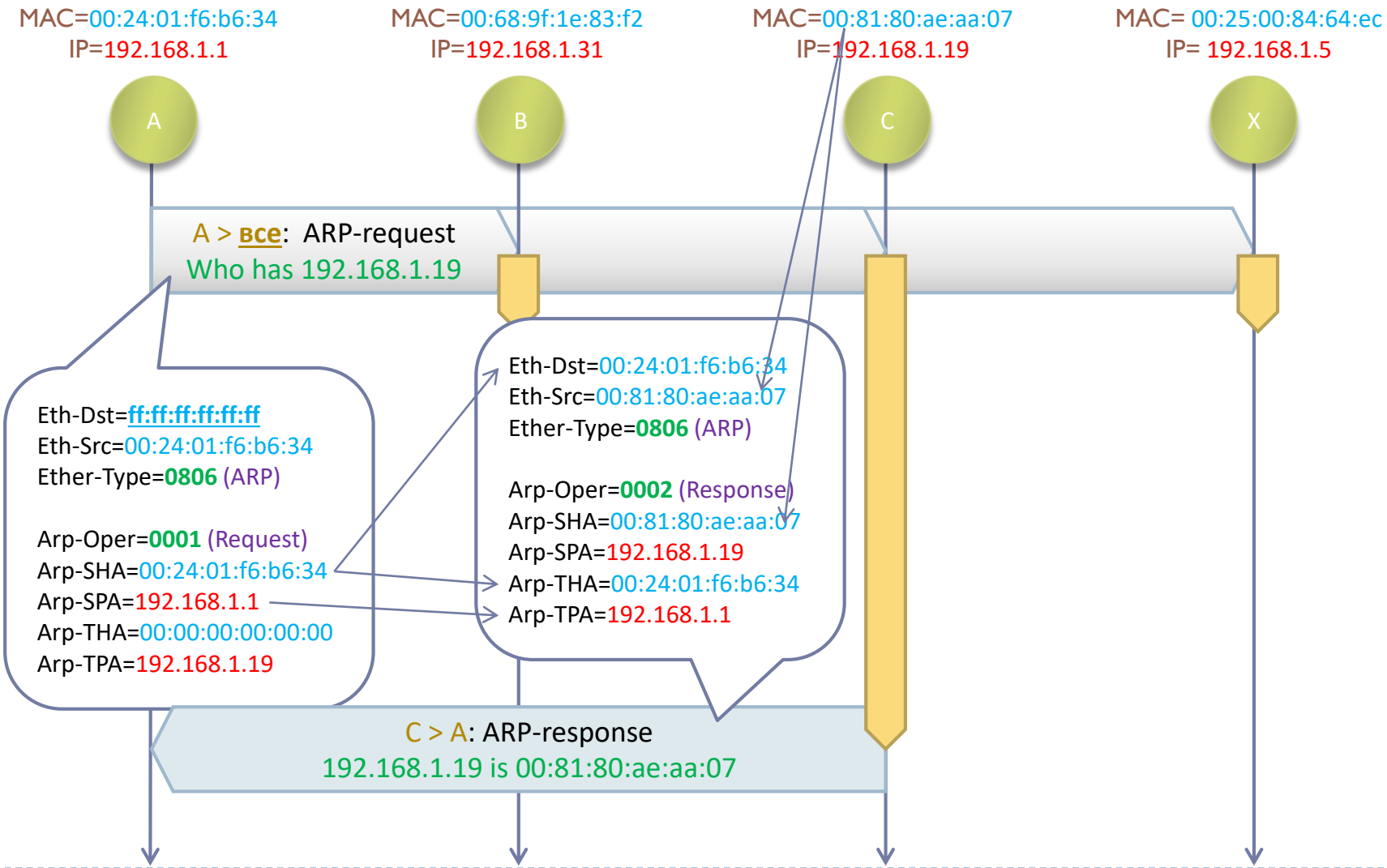
Процедура ARP-Resolve



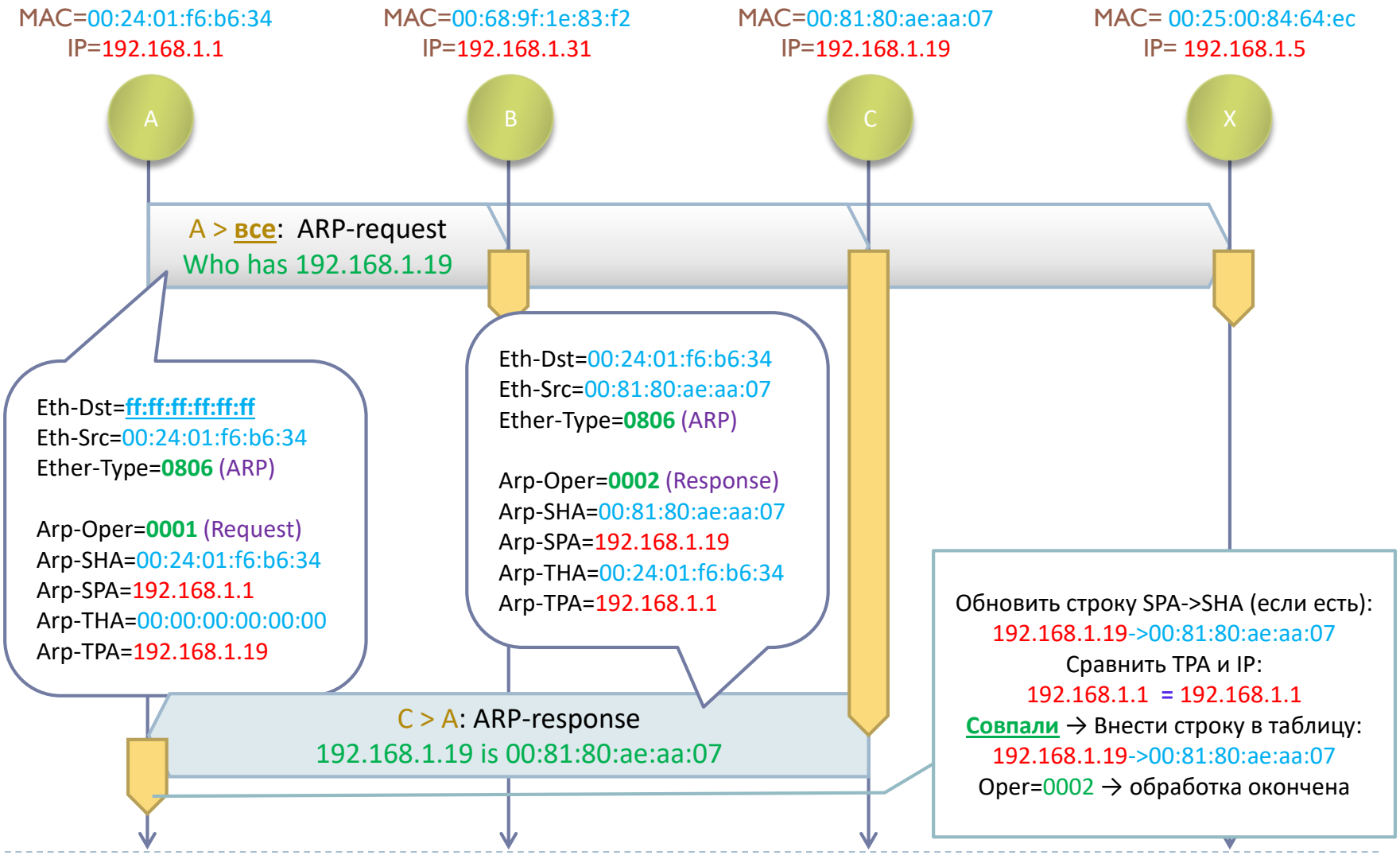
Процедура ARP-Resolve



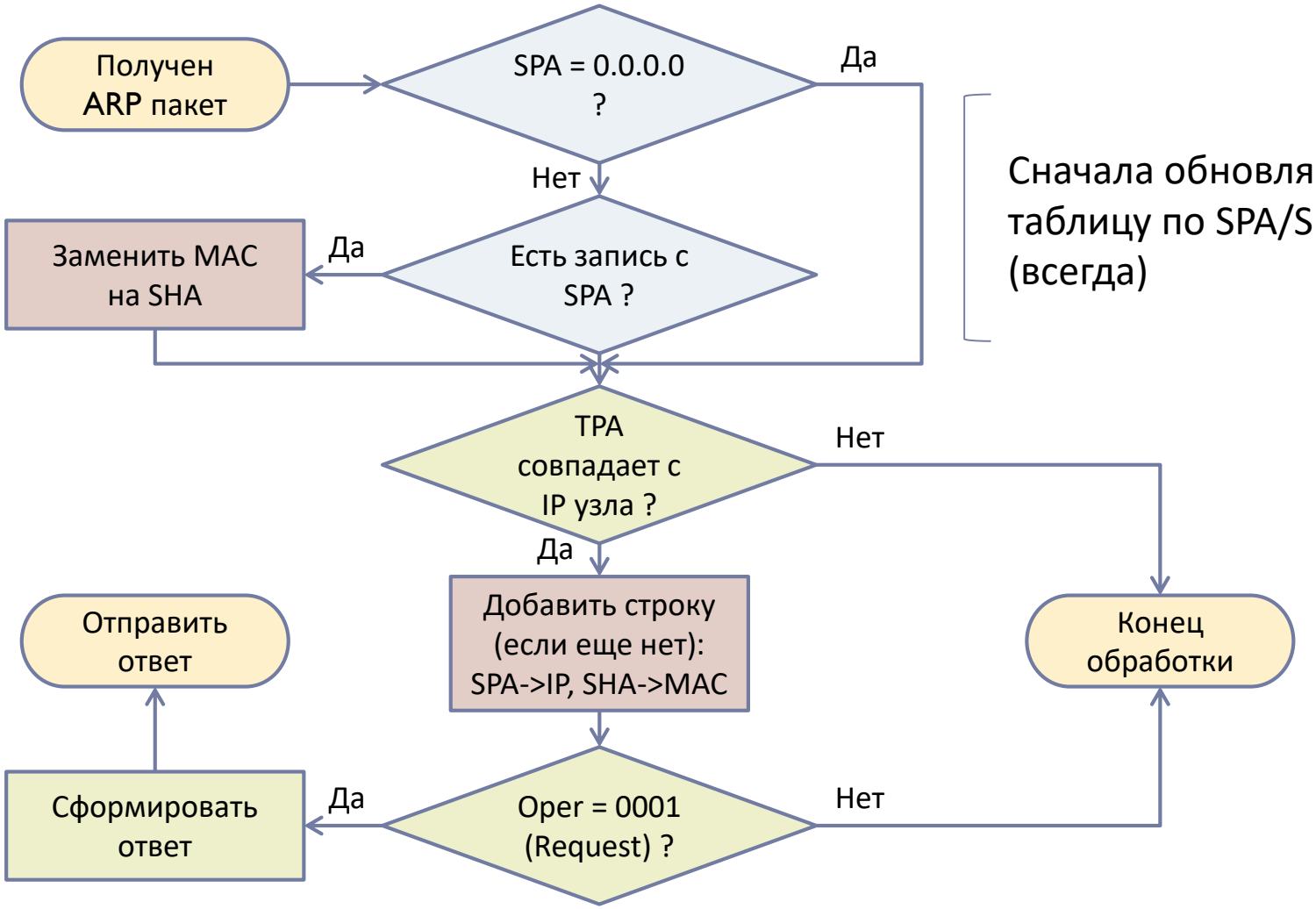
Процедура ARP-Resolve



Процедура ARP-Resolve



Алгоритм обработки ARP-пакета



План курса

1. Введение в компьютерные сети
2. Основные методы построения СПД
3. **Архитектура Internet Protocol Suite (TCP/IP)**
    - 3.1. Адресация в IP сетях
    - 3.2. Протокол IP (v4)
    - 3.3. Протокол ARP
    - **3.4. Служебный трафик и протокол ICMP**
4. Архитектура модулей физического уровня
5. Технологии беспроводных сетей
6. Архитектура модулей канального уровня
7. Протоколы транспортного уровня
8. Технологии WWW

Обмен служебным трафиком

Для реализации некоторых функций (например Path-MTU Discovery) IP модулям необходимо передавать друг другу служебные сообщения (например сообщение о том, что пакет слишком велик для последующей передачи).

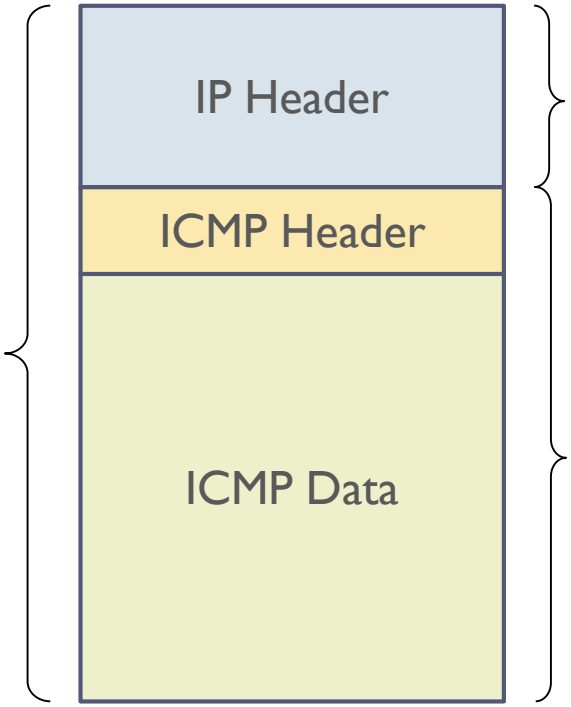
IP протокол использует несколько видов служебных сообщений:

- Уведомления об ошибках при коммутации пакетов – отправляются IP модулем, который обнаружил ошибку модулю-отправителю пакета (по Src-IP);
- Диагностические сообщения – используются служебными программами-утилитами (*ping, traceroute*) для проверки корректности работы сети и обнаружения неисправностей;
- Управление маршрутами на уровне канала – используются для “временной корректировки” маршрутных таблиц узлов-соседей при наличии необходимости
- Управление темпом передачи данных – данная функция уже не рекомендуется к применению
- и другие.

Протокол ICMP и структура сообщения

ICMP (Internet Control Message Protocol) предназначен для обмена служебными сообщениями между IP модулями разных. По сути, ICMP является частью протокола IP, однако по форме – это отдельный протокол, работающий “поверх IP”:

Сообщение ICMP представляет собой стандартный IP пакет, который передается по Internet обычным образом по указанному в пакете IP адресу назначения



Стандартный IP заголовок. Поле Proto = 1 (код ICMP)

Поле данных начинается с фиксированного заголовка ICMP (8 байтов) за которым *могут* следовать уточняющие данные переменной длины

Виды сообщений ICMP

ICMP позволяет IP модулям обмениваться служебными сообщениями из предопределенного набора. Они имеют различный формат и переменную длину, однако в любом случае первые два байта определяют вид сообщения:

Поле Type определяет функциональную группу, к которой относится сообщение, а поле Code конкретизирует (детализирует) внутри группы вид сообщения.

Наиболее значимыми для функционирования IP сети являются ICMP сообщения типа 3 (Destination unreachable) уведомляющие отправителя о невозможности доставки пакета по указанному назначению.

ICMP сообщения о недоступности адресата

(8 бит) **Type** = 3	*(8 бит)* **Code** (причина ошибки)	*(16 бит)* Контрольная сумма содержимого заголовка
(16 бит) Не используется (нули)		(16 бит) Next-Hop MTU (ограничение следующего по маршруту канала для Code=4)
(переменная длина 20+ байтов) Заголовок IP пакета, который не удалось доставить		
(N байтов, не менее 8) Первые N байтов идущие после заголовка в исходном IP пакете		

Перечень некоторых кодов

0	Сеть недоступна (временно)	7	Узел назначения не известен
1	Узел недоступен (временно)	9	Связь с сетью запрещена администратором
2	Указанный протокол не поддерживается	10	Связь с узлом запрещена администратором
3	Порт недоступен	11	Сеть недоступна с указанным типом обслуживания
4	Размер пакета больше MTU и флаг DF=1	12	Узел недоступен с указанным типом обслуживания
6	Сеть назначения не известна	13	Связь запрещена администратором

Другие виды ICMP сообщений

Функция	Type	Code	Описание
Индикация ошибок при обработке пакета	12 – Некорректный IP заголовок	0	Ошибка в параметре заголовка
		1	Ошибка в опциях
		2	Ошибка длины
	11 – Превышение времени	0	В процессе передачи пакета TTL стал =0
		1	Таймаут при сборке фрагментов пакета
Диагностика	8 – Эхо запрос	0	Запрос на эхо-повтор данных от получателя
	0 – Эхо ответ	0	Эхо-повтор полученных в запросе данных
Управление маршрута-ми на уровне местной сети	5 – Redirect (перенап-равление)	0	Используй другой (лучший) шлюз для сети
		1	Используй другой (лучший) шлюз для узла
	9 – Анонс шлюза	0	Оповещение в сеть о наличии шлюза
	10 – Запрос шлюза	0	Запрос оповещения о шлюзе
Управление темпом передачи данных	4 – Замедление (source quench)	0	Запрос к источнику трафика замедлить темп передачи

Методы элементарной диагностики IP сетей

Как любое сложное устройство IP сеть может функционировать некорректно. Этот эффект может быть вызван массой различных элементарных причин:

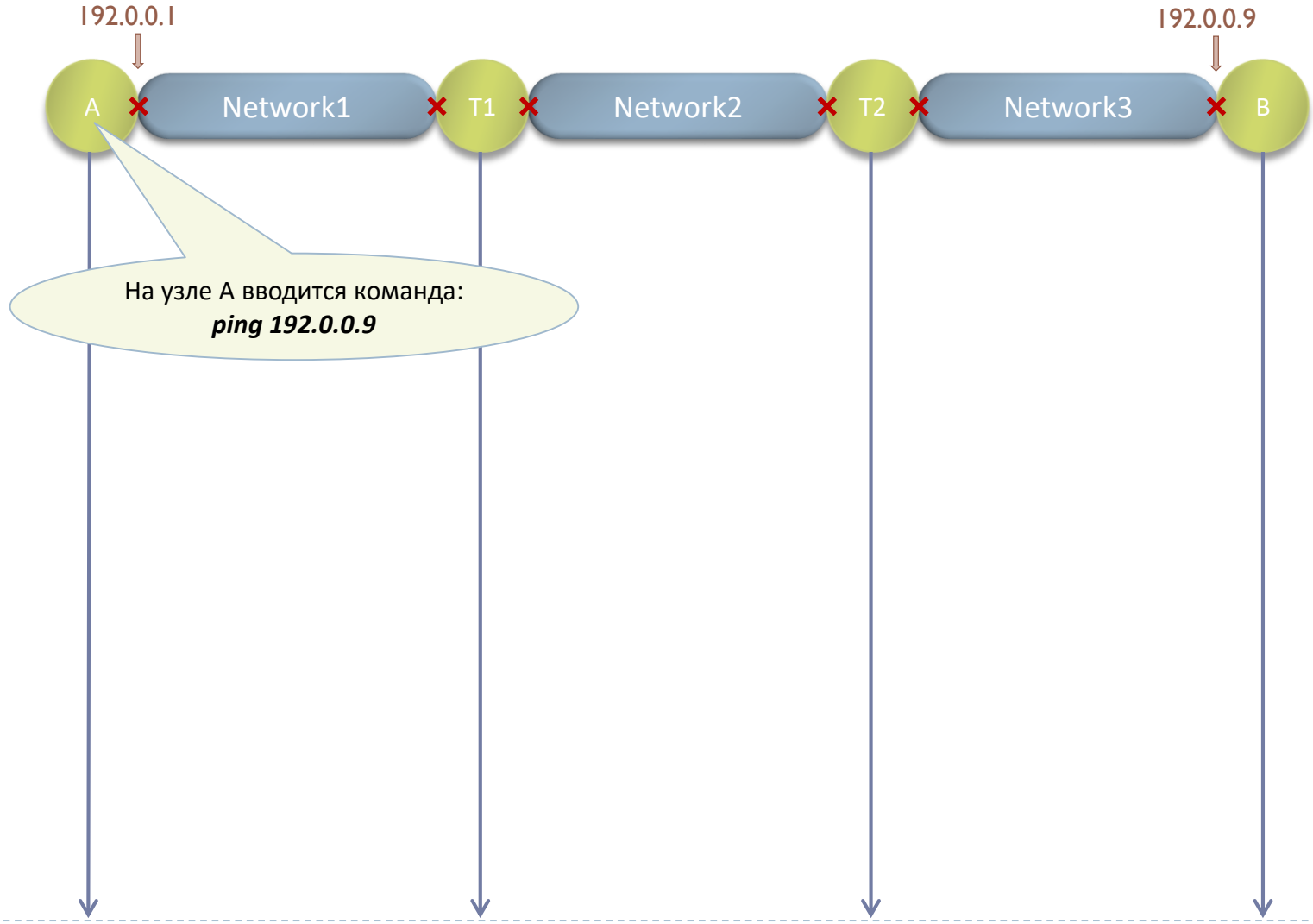
- не функционирует какой-либо канал (link);
- канал плохо работает (высокий процент ошибок);
- таблица маршрутов на каком-либо узле настроена некорректно;
- канал или узел перегружены (слишком большой трафик);
- и т.п.

Зачастую, устранить неисправность бывает нетрудно (например вставить в гнездо выпавший сетевой кабель или добавить в таблицу пропущенный маршрут). Однако, основная проблема заключается в том, как найти (локализовать) точное место и причину неисправности. К сожалению, метод «научного тыка» в данных случаях работает плохо.

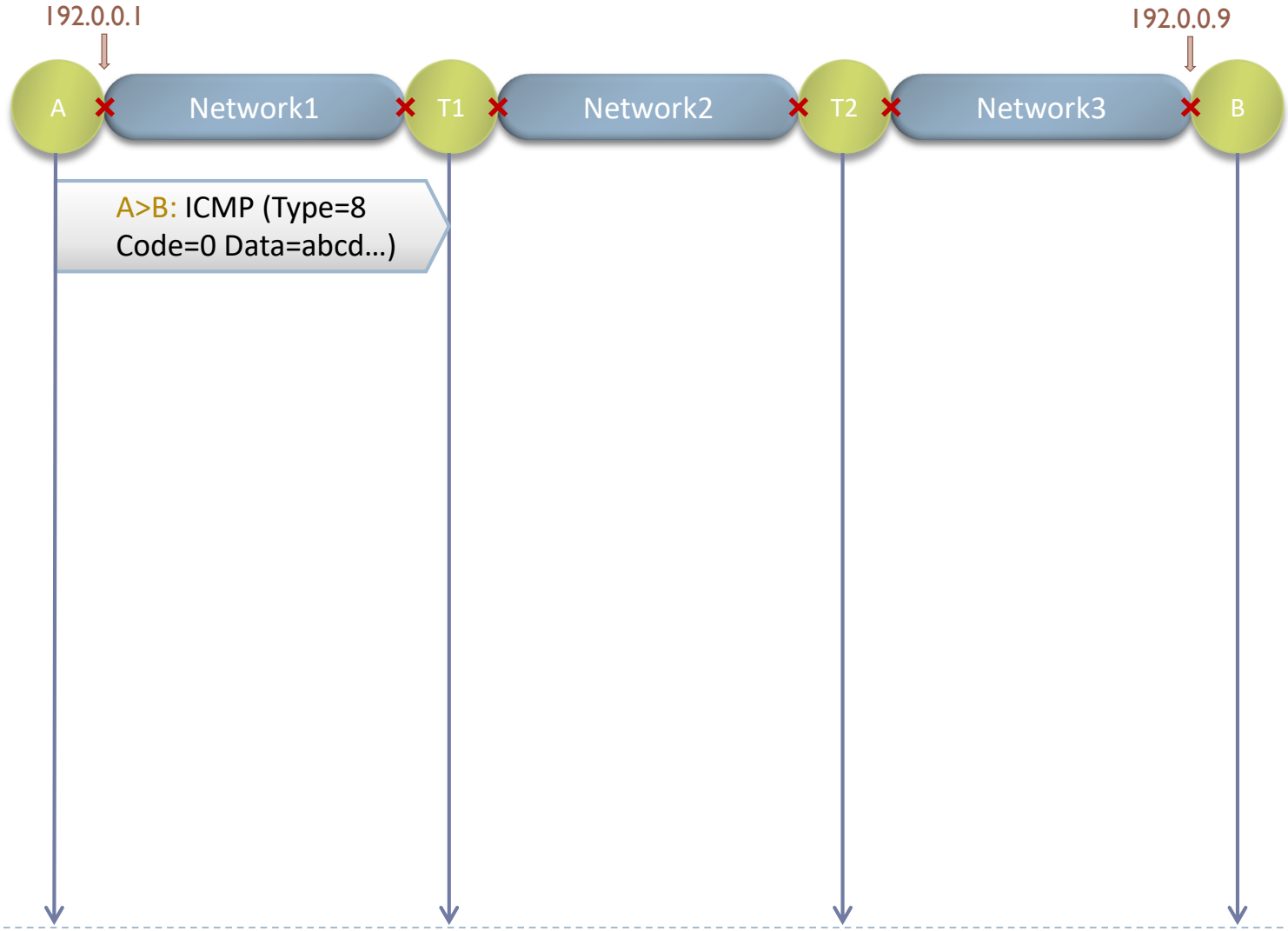
К счастью, IP сети имеют встроенные средства диагностики:

- Команда ***ping*** – позволяет проверить прохождение IP пакетов по замкнутому пути «туда-обратно» до указанного узла (IP адреса);
- Команда ***traceroute*** (tracert) – отображает маршрут прохождения пакетов.

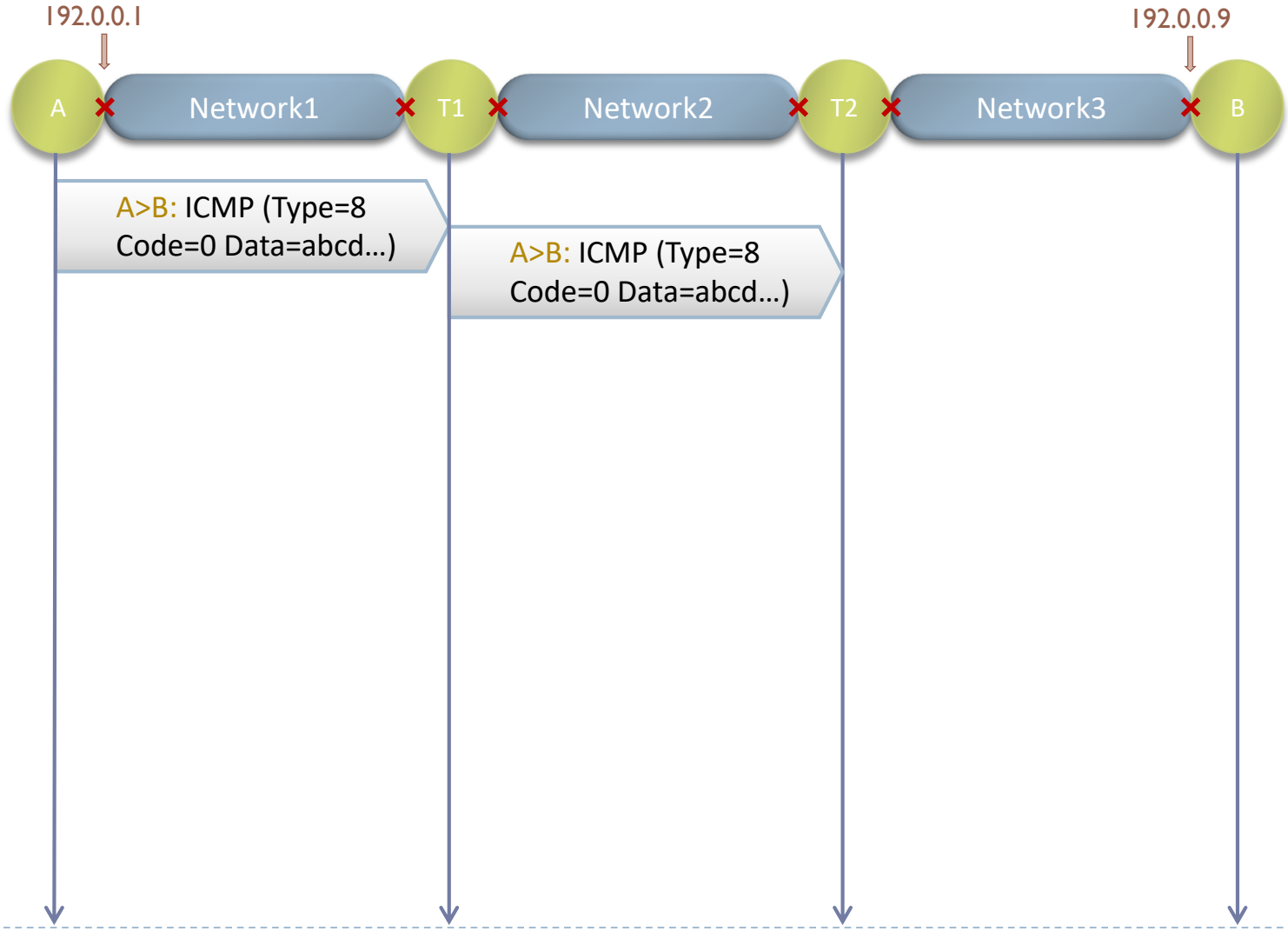
Принцип действия Ping



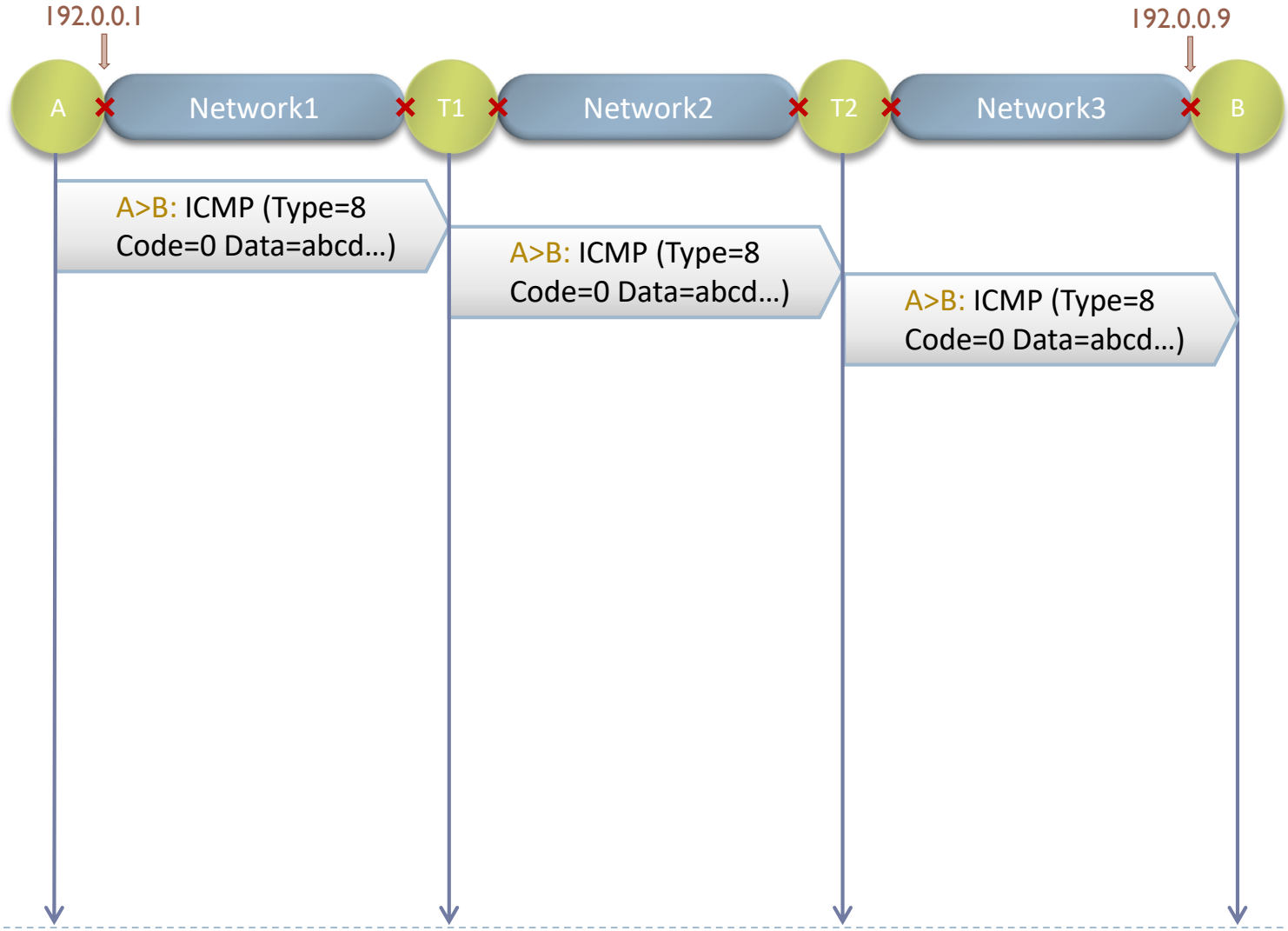
Принцип действия Ping



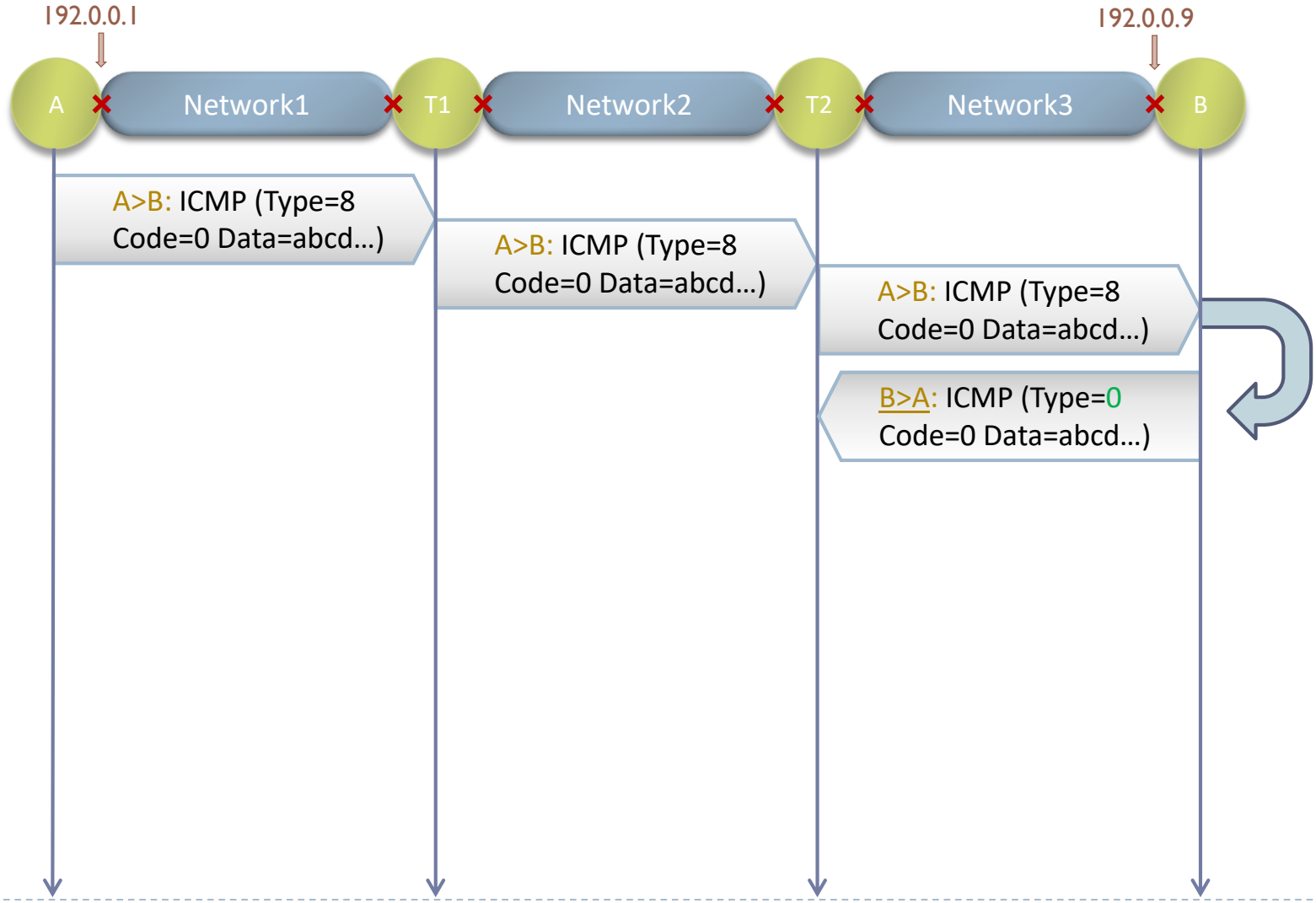
Принцип действия Ping



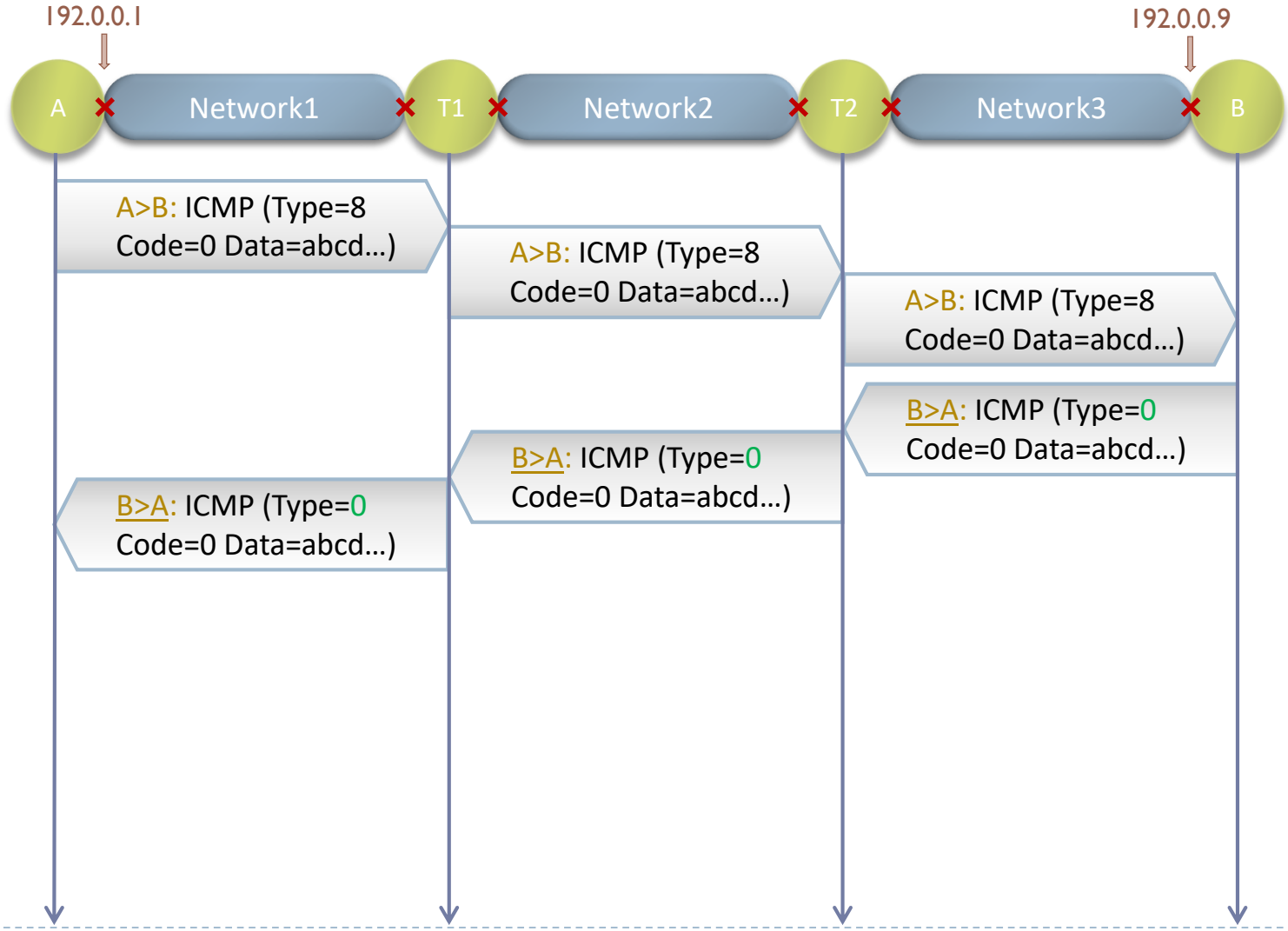
Принцип действия Ping



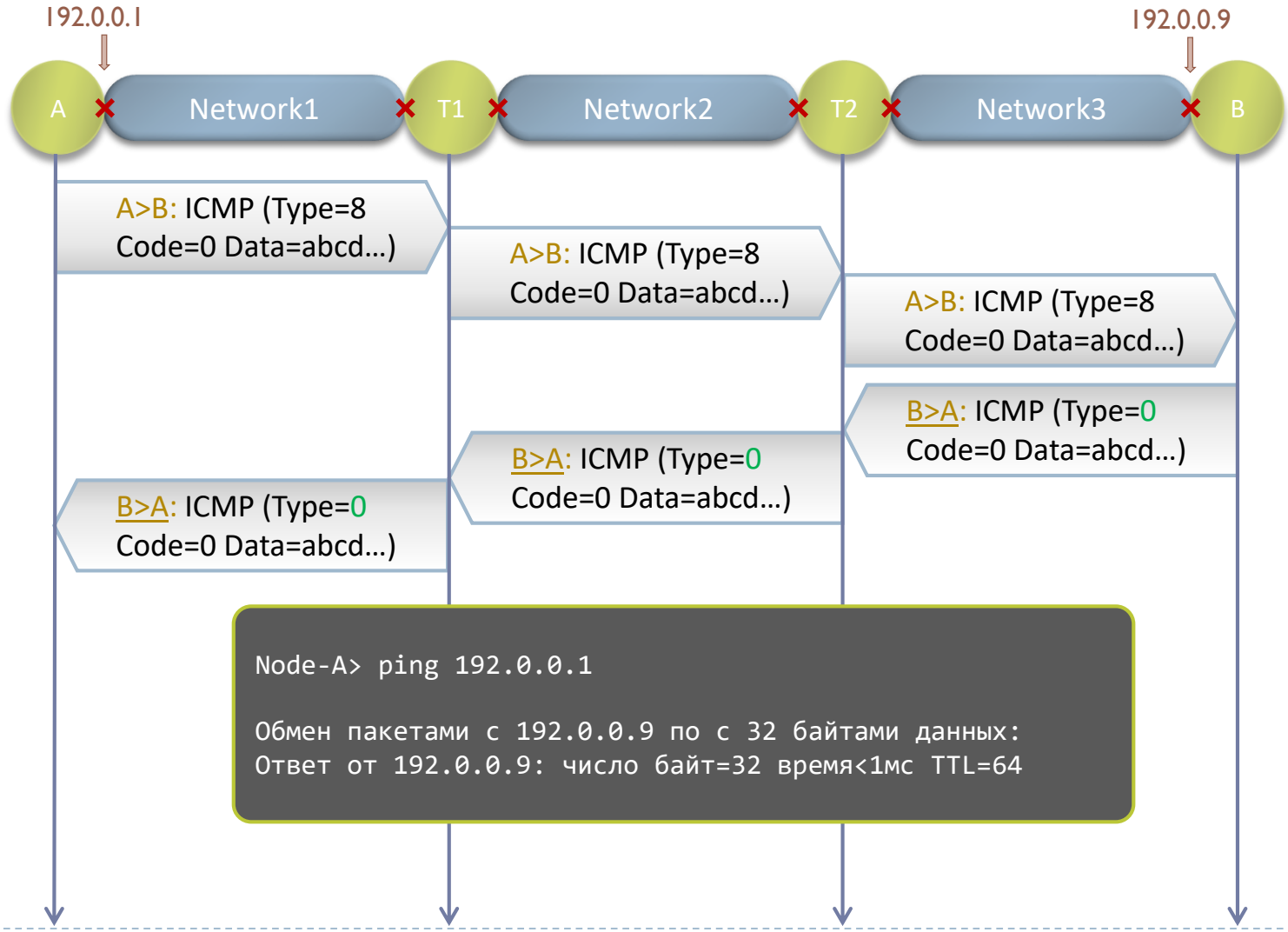
Принцип действия Ping



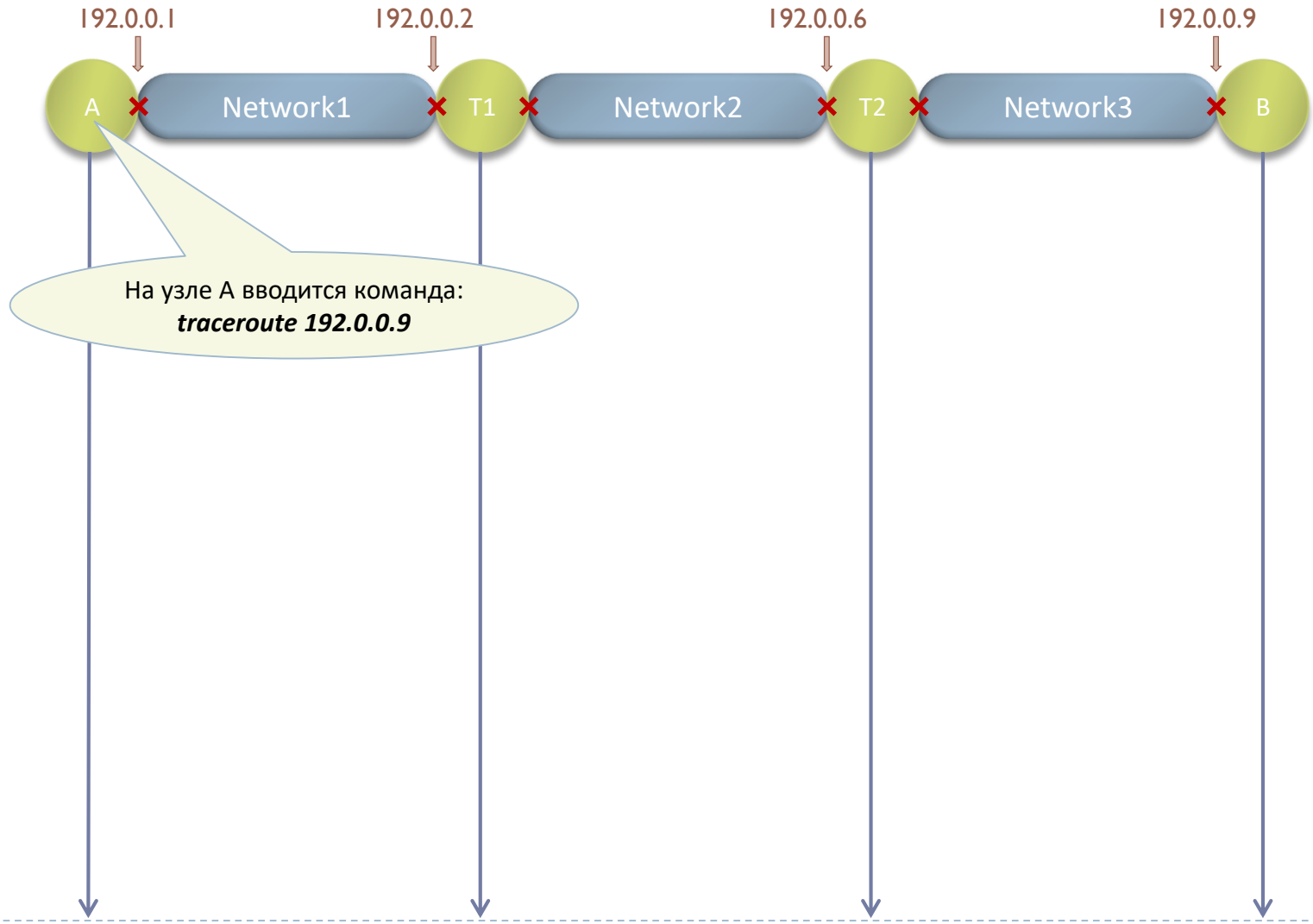
Принцип действия Ping



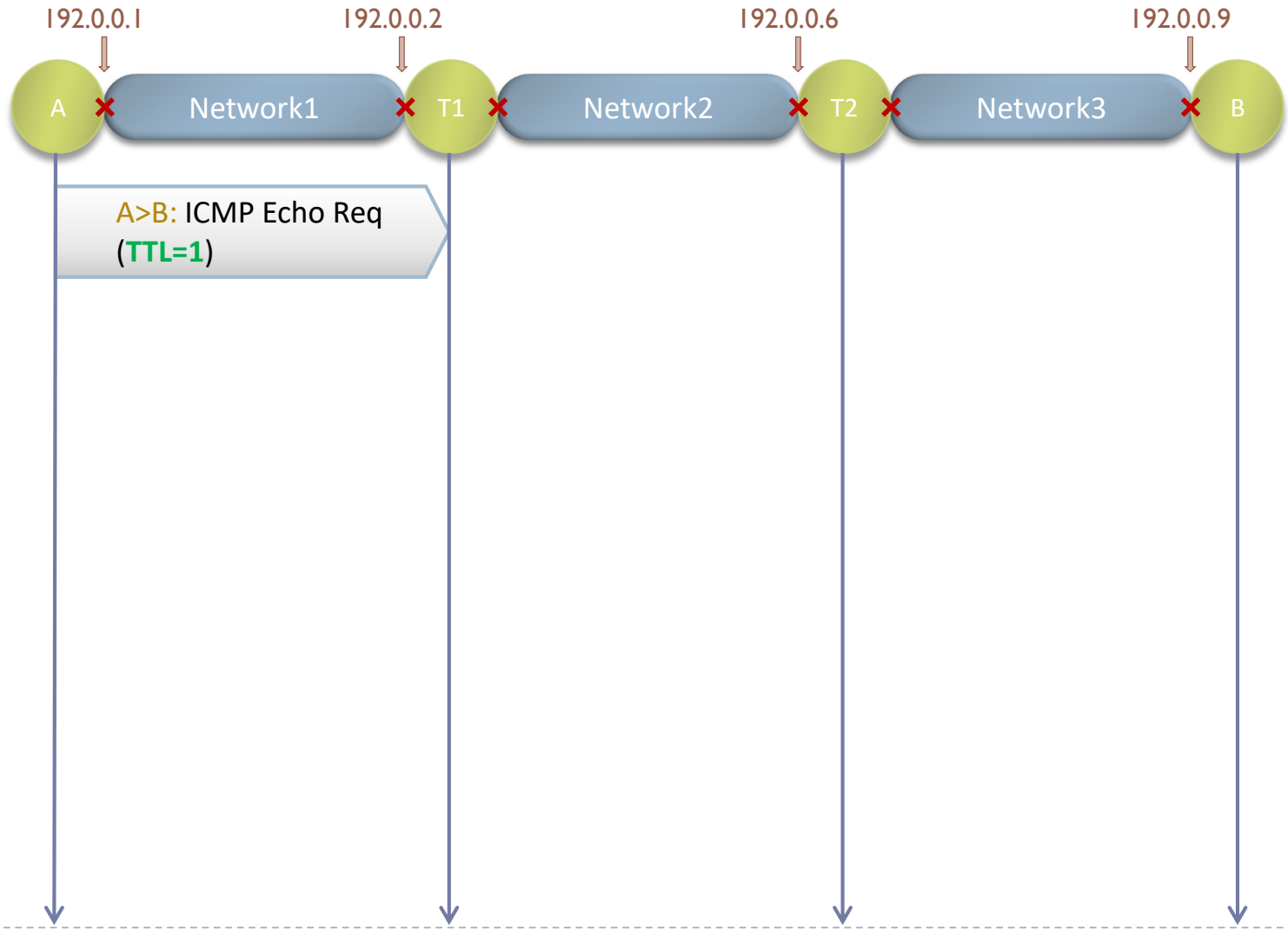
Принцип действия Ping



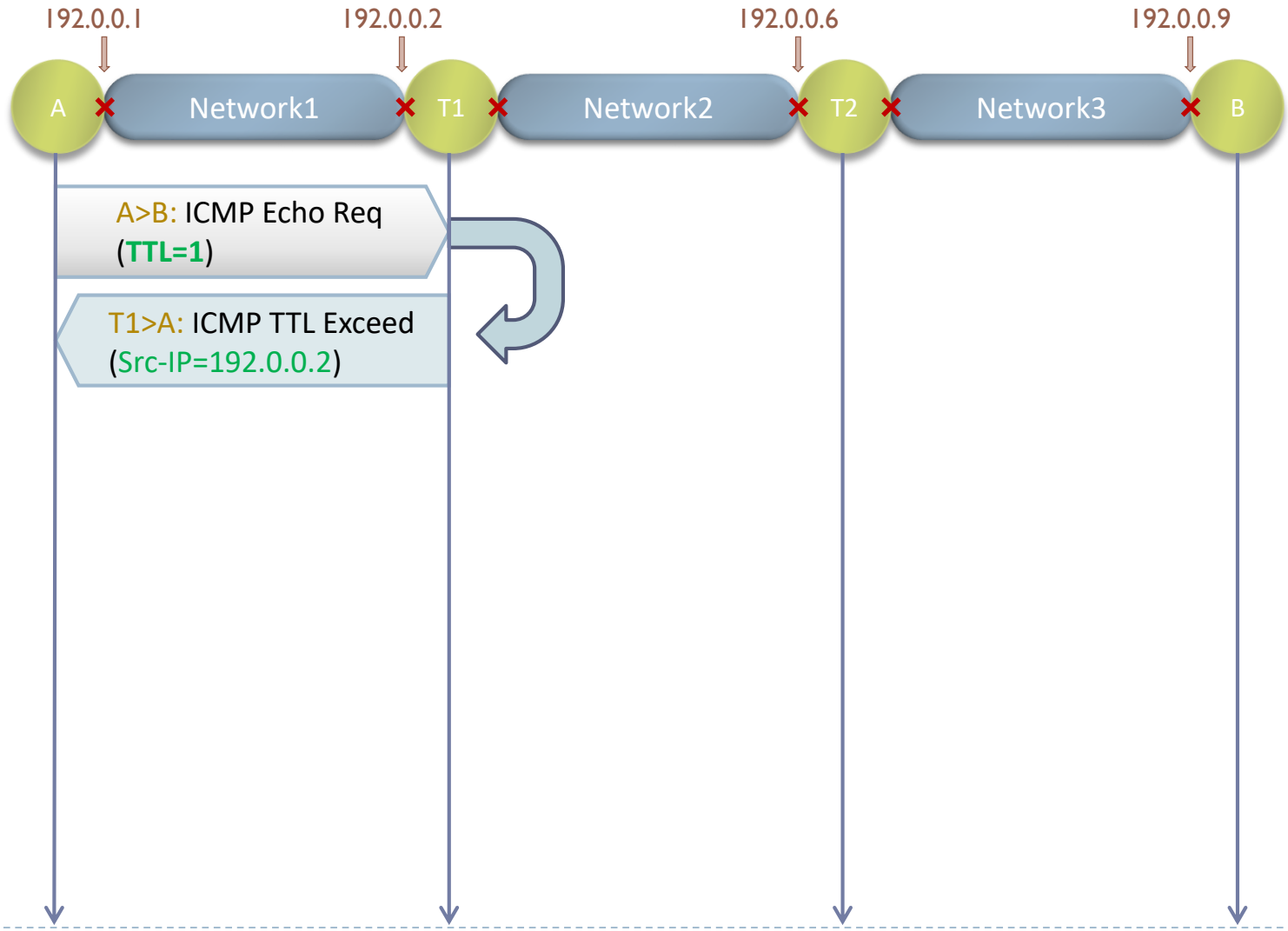
Принцип действия Traceroute



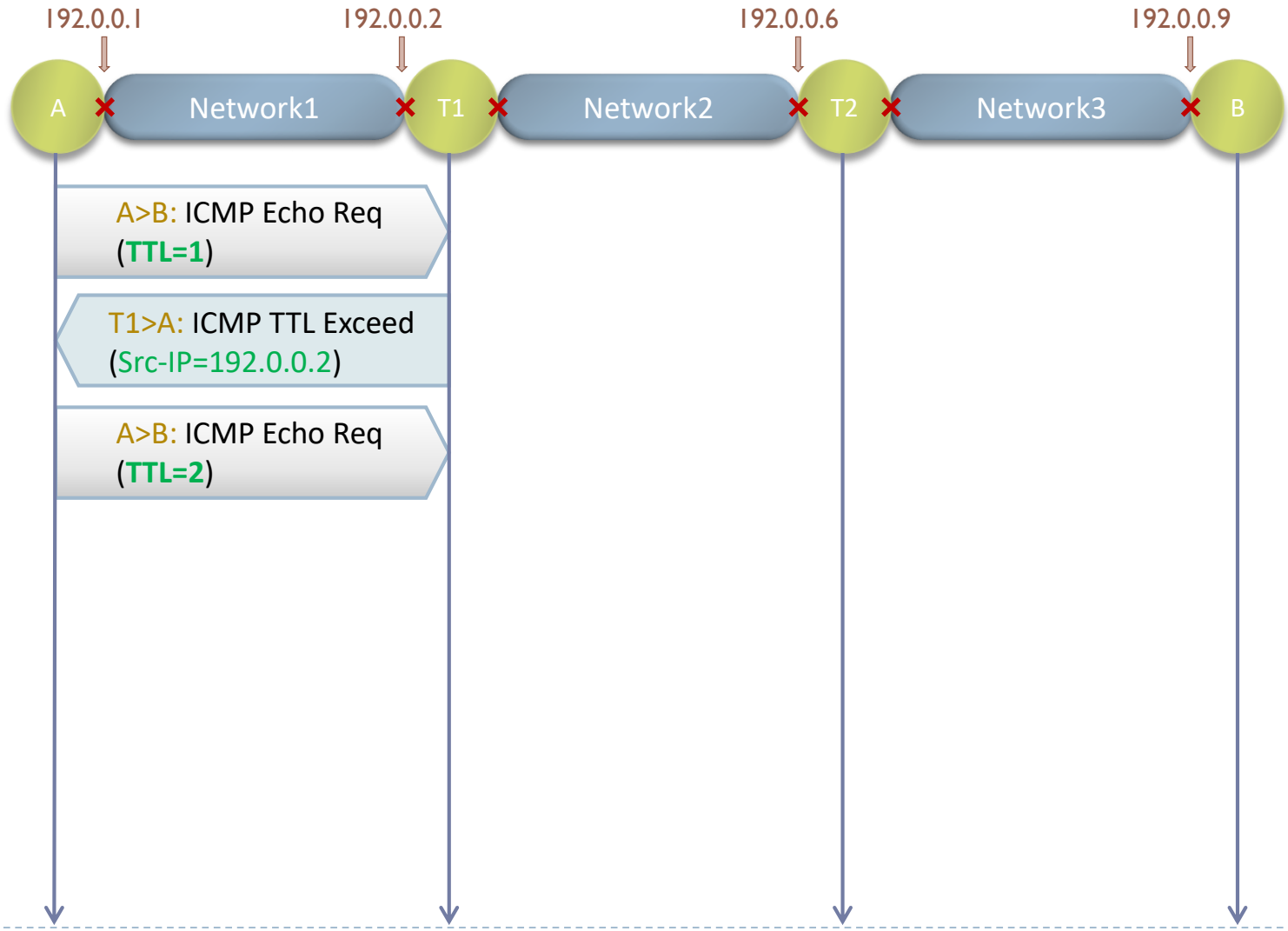
Принцип действия Traceroute



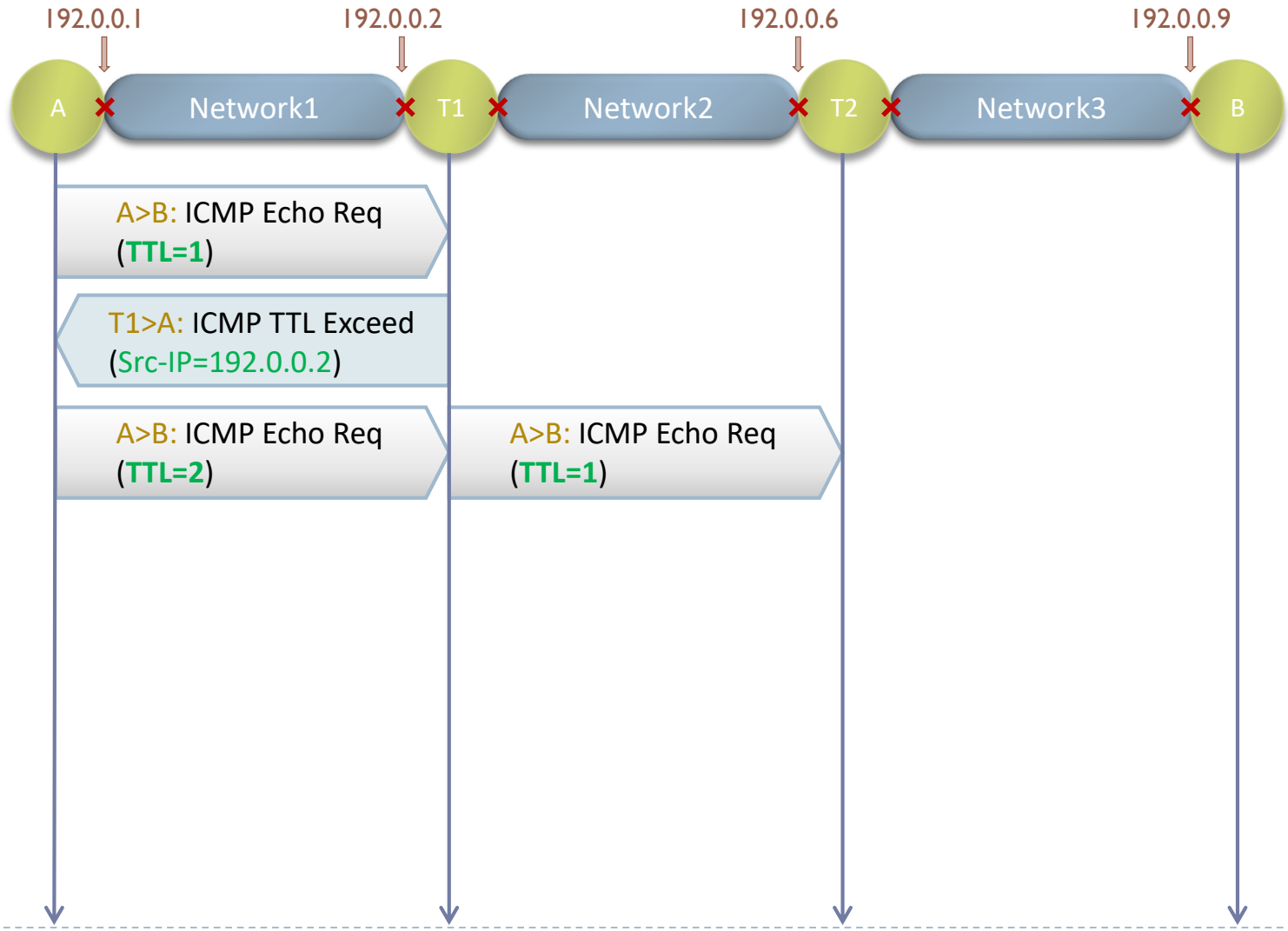
Принцип действия Traceroute



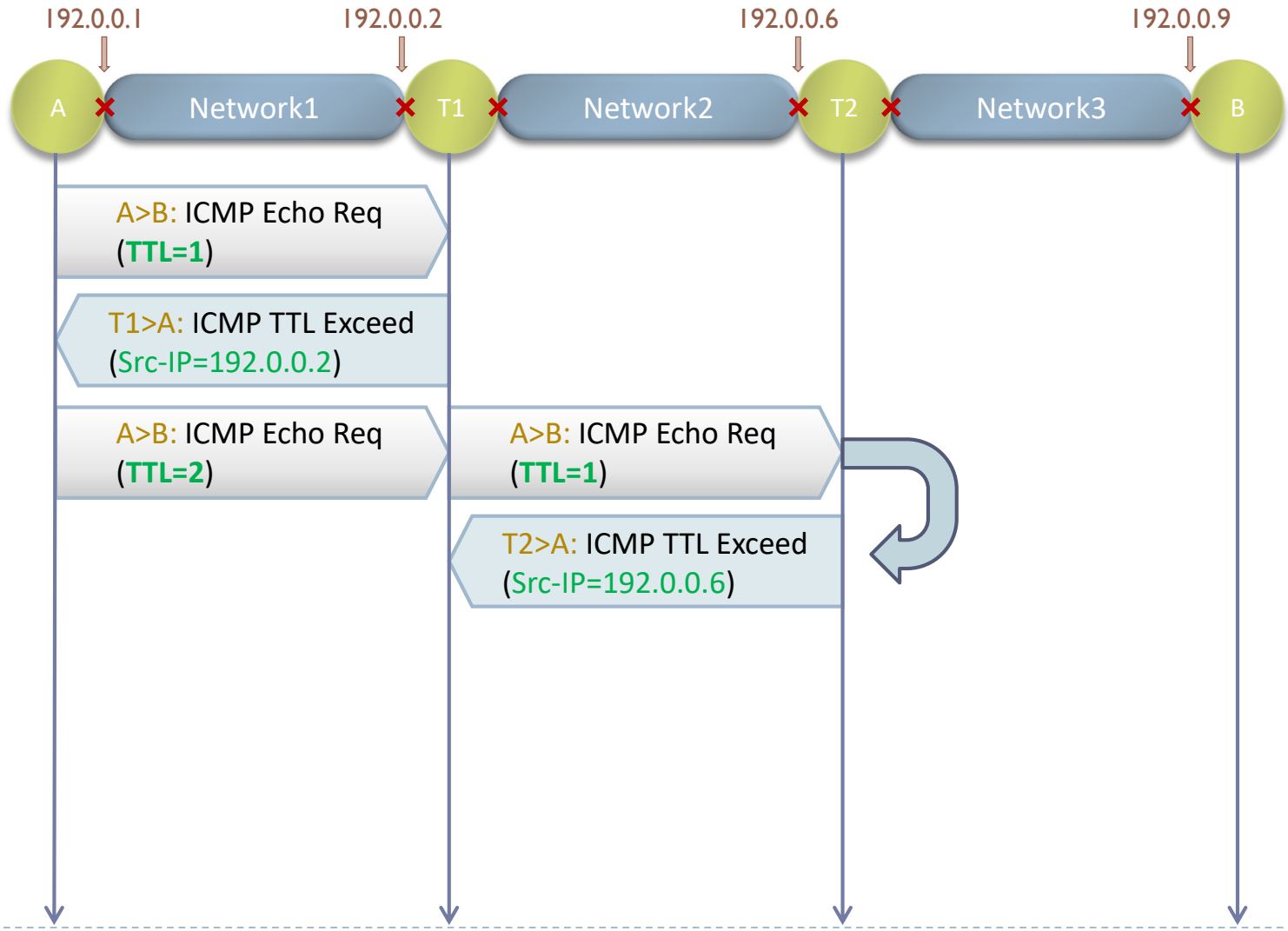
Принцип действия Traceroute



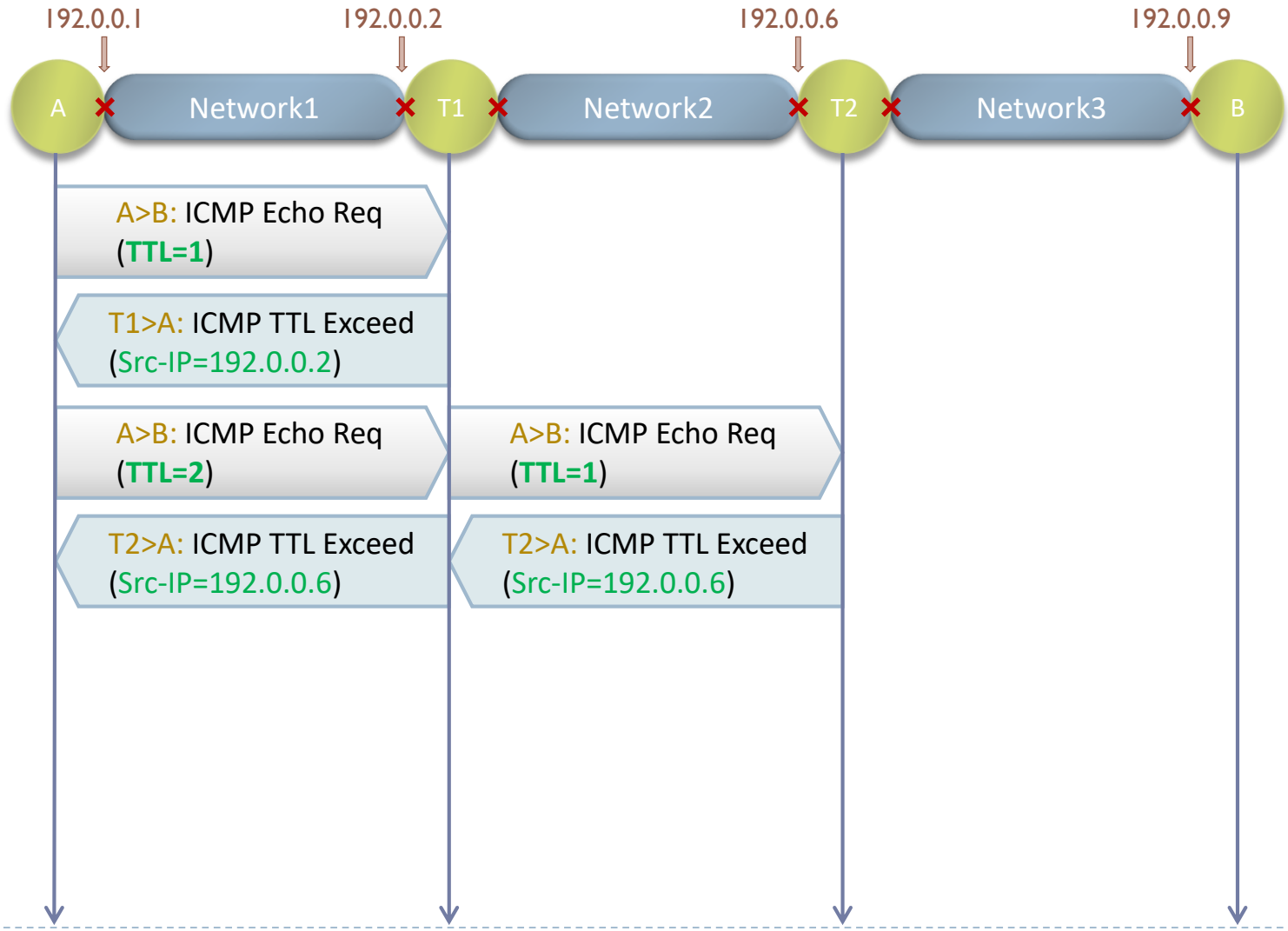
Принцип действия Traceroute



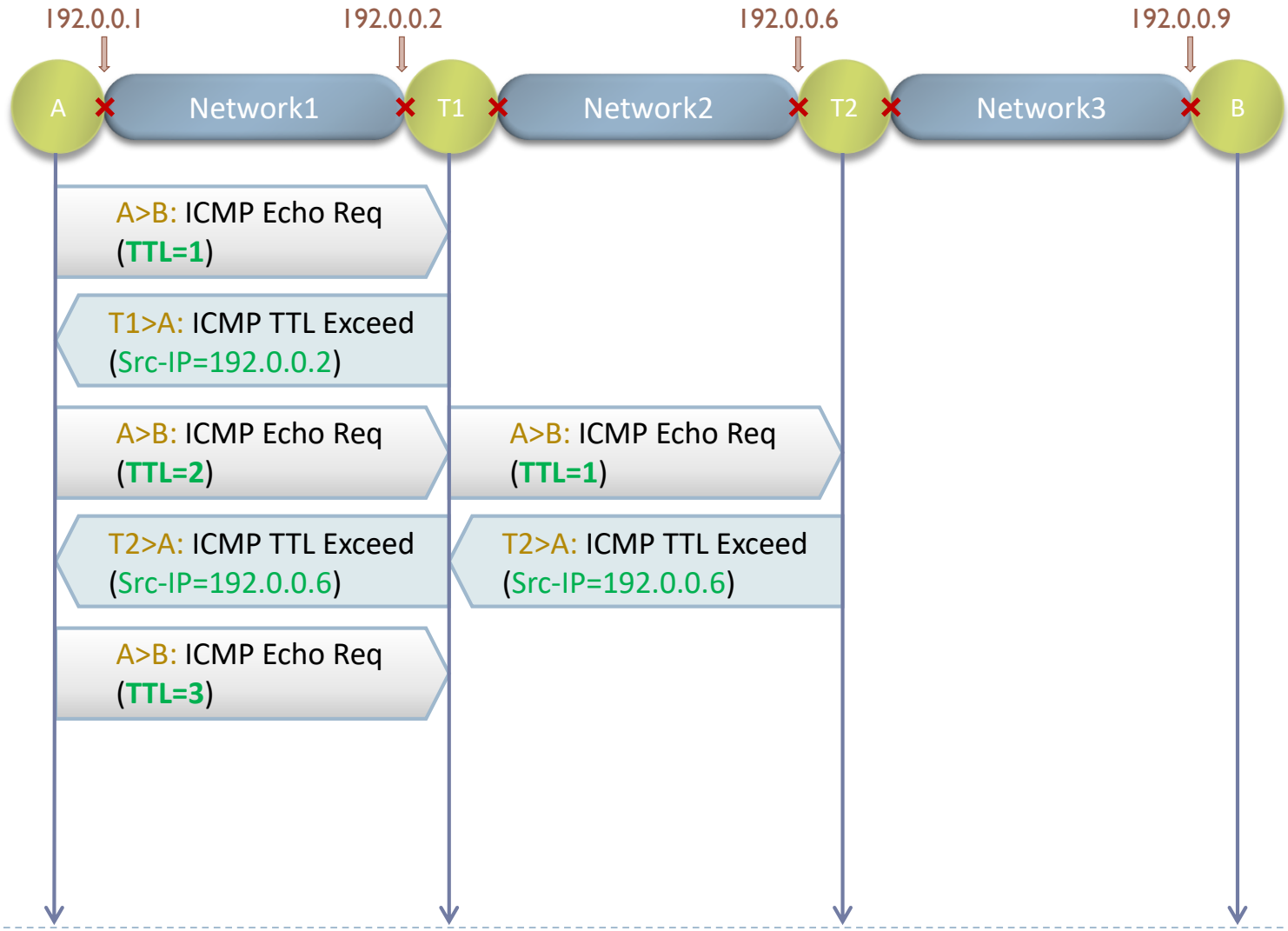
Принцип действия Traceroute



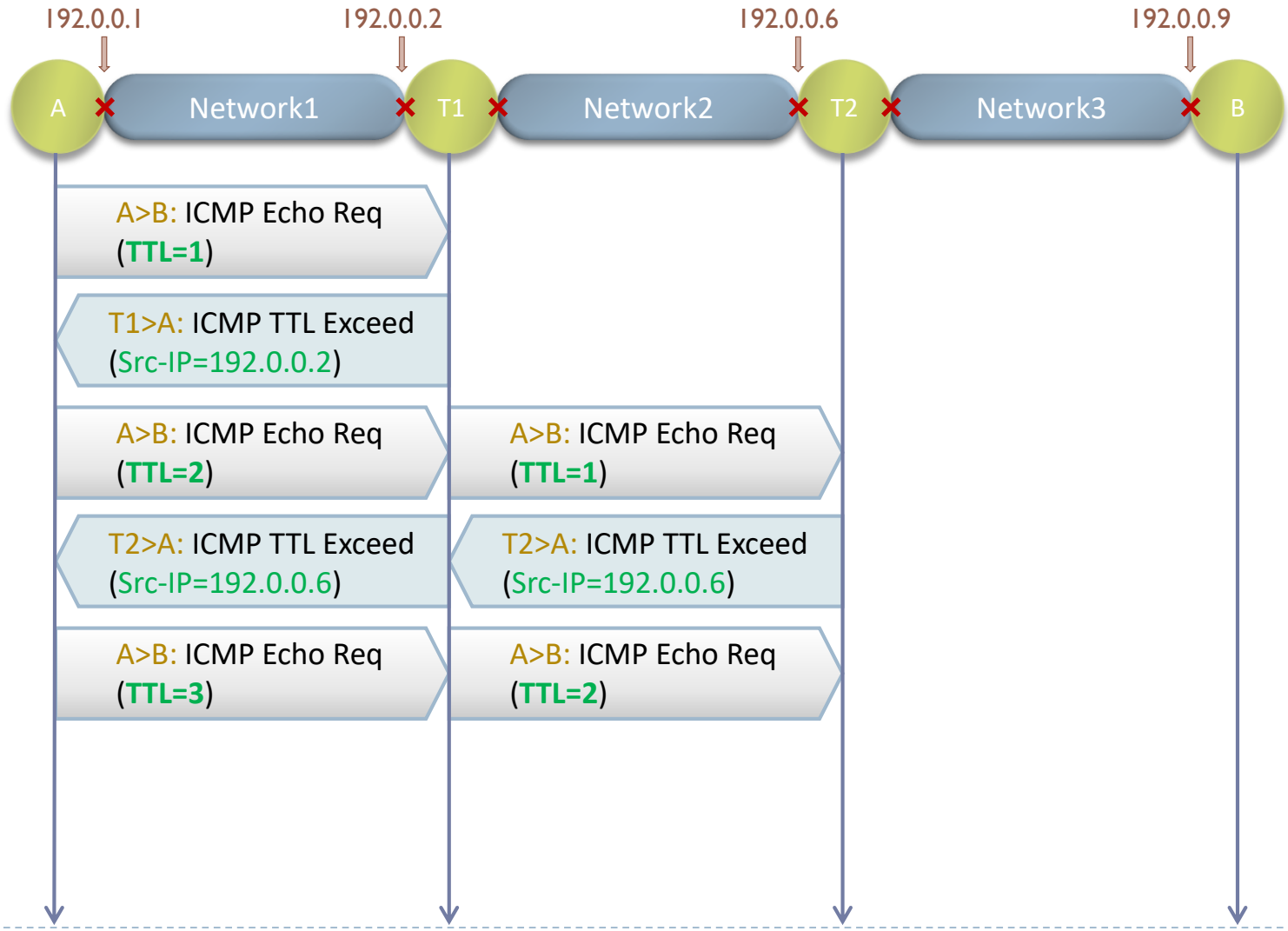
Принцип действия Traceroute



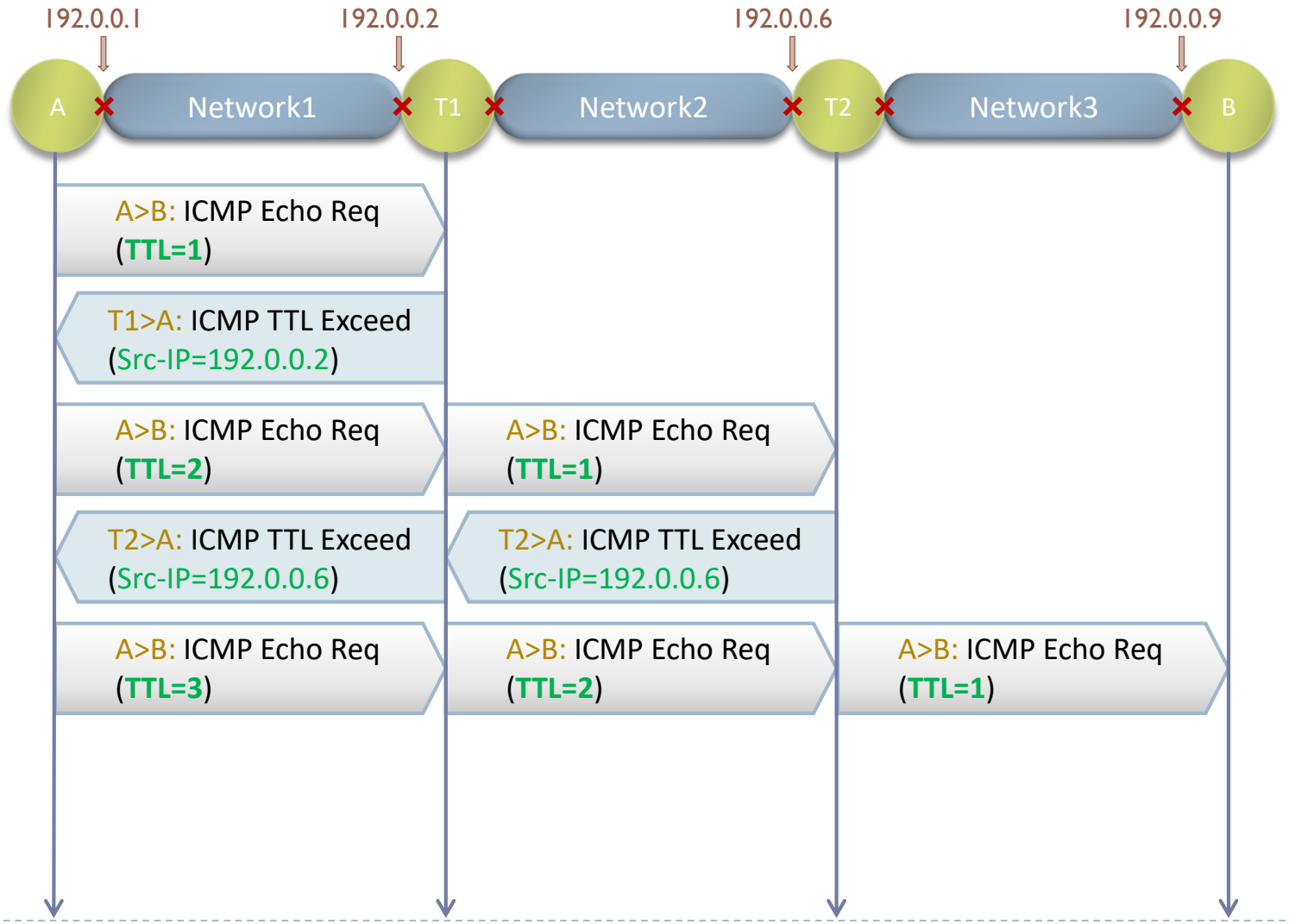
Принцип действия Traceroute



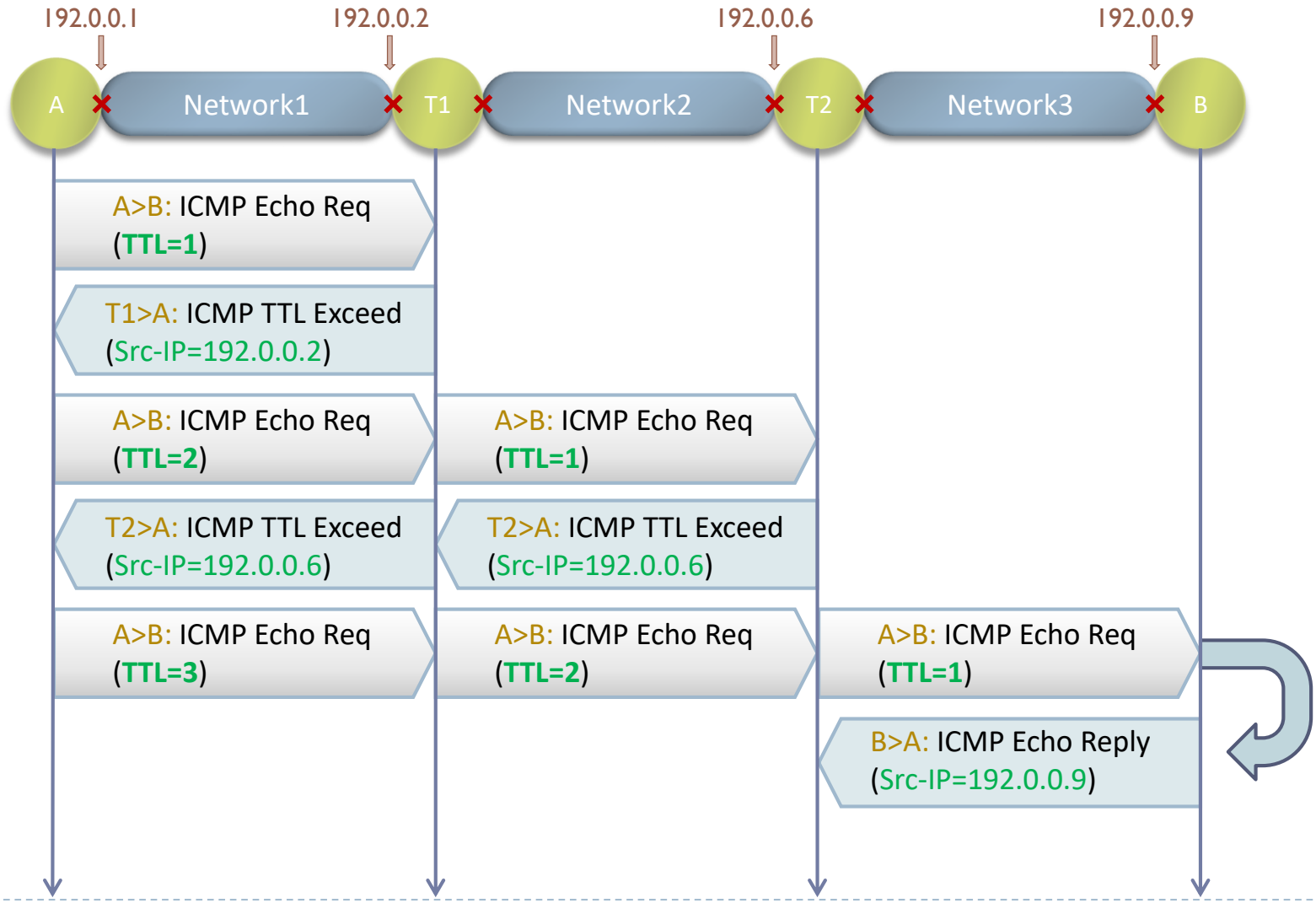
Принцип действия Traceroute



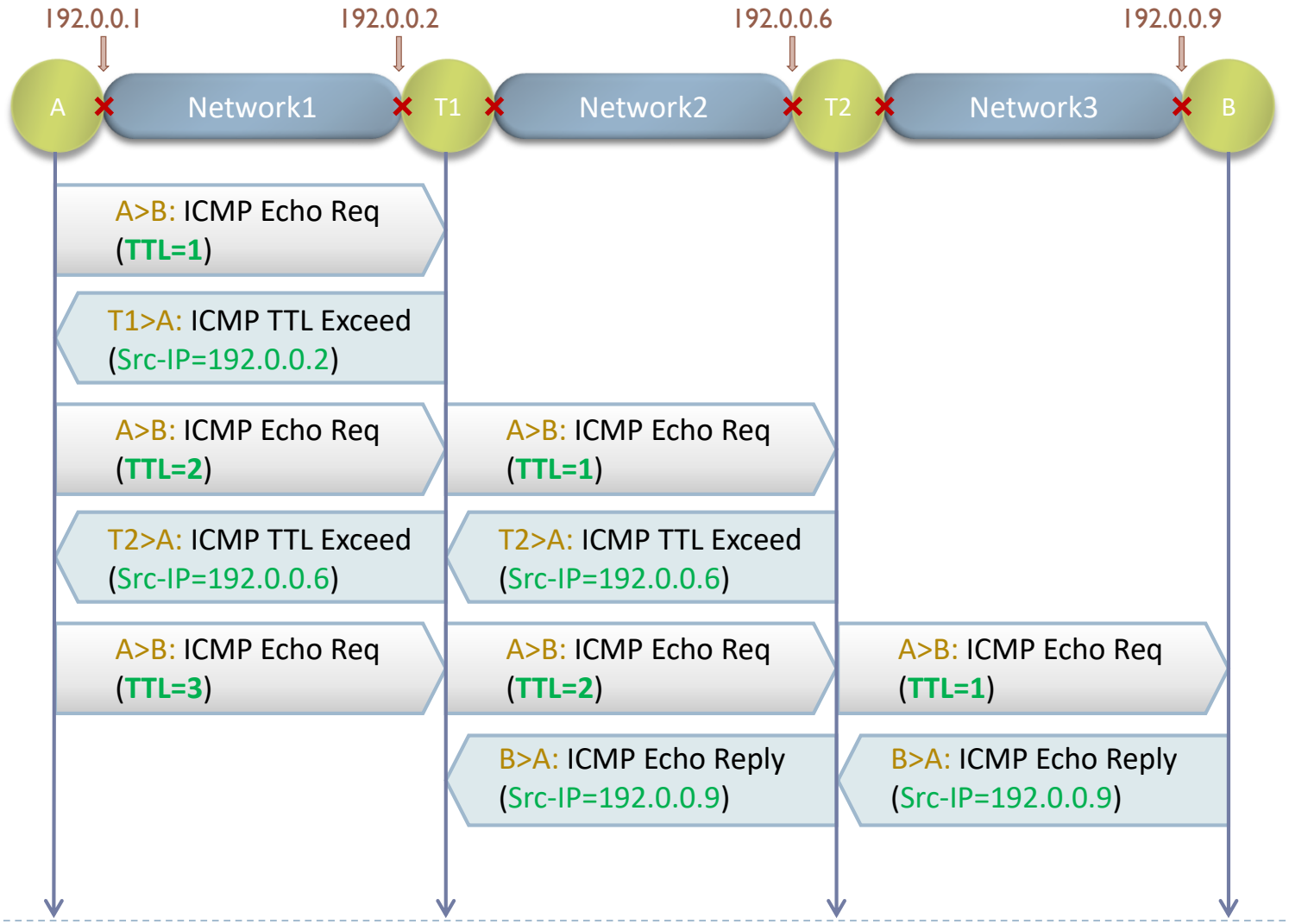
Принцип действия Traceroute



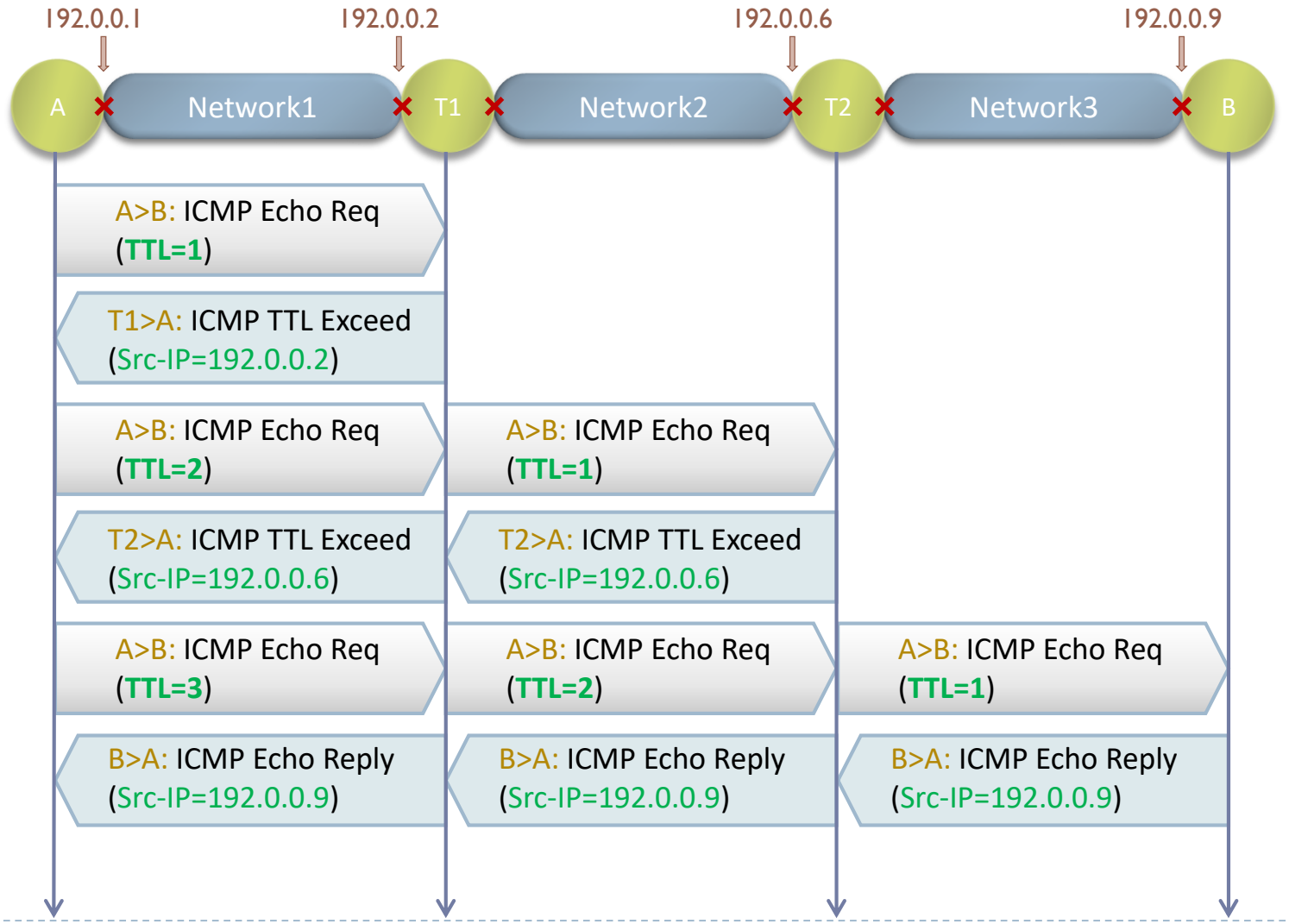
Принцип действия Traceroute



Принцип действия Traceroute



Принцип действия Traceroute



Принцип действия Traceroute