

Условные обозначения



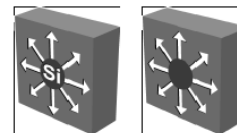
Router



Multiservice
Switch



Switch



Multilayer Switch



Workgroup
Switch



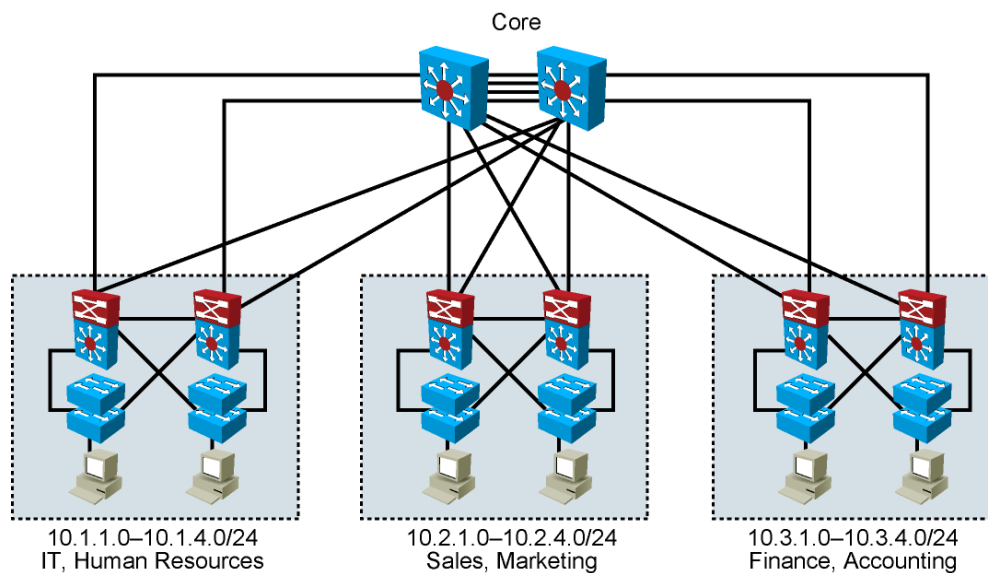
Workgroup
Switch:
Voice-Enabled



100BASE-T
Hub



Bridge



IP маршрутизация



Эволюция маршрутизаторов

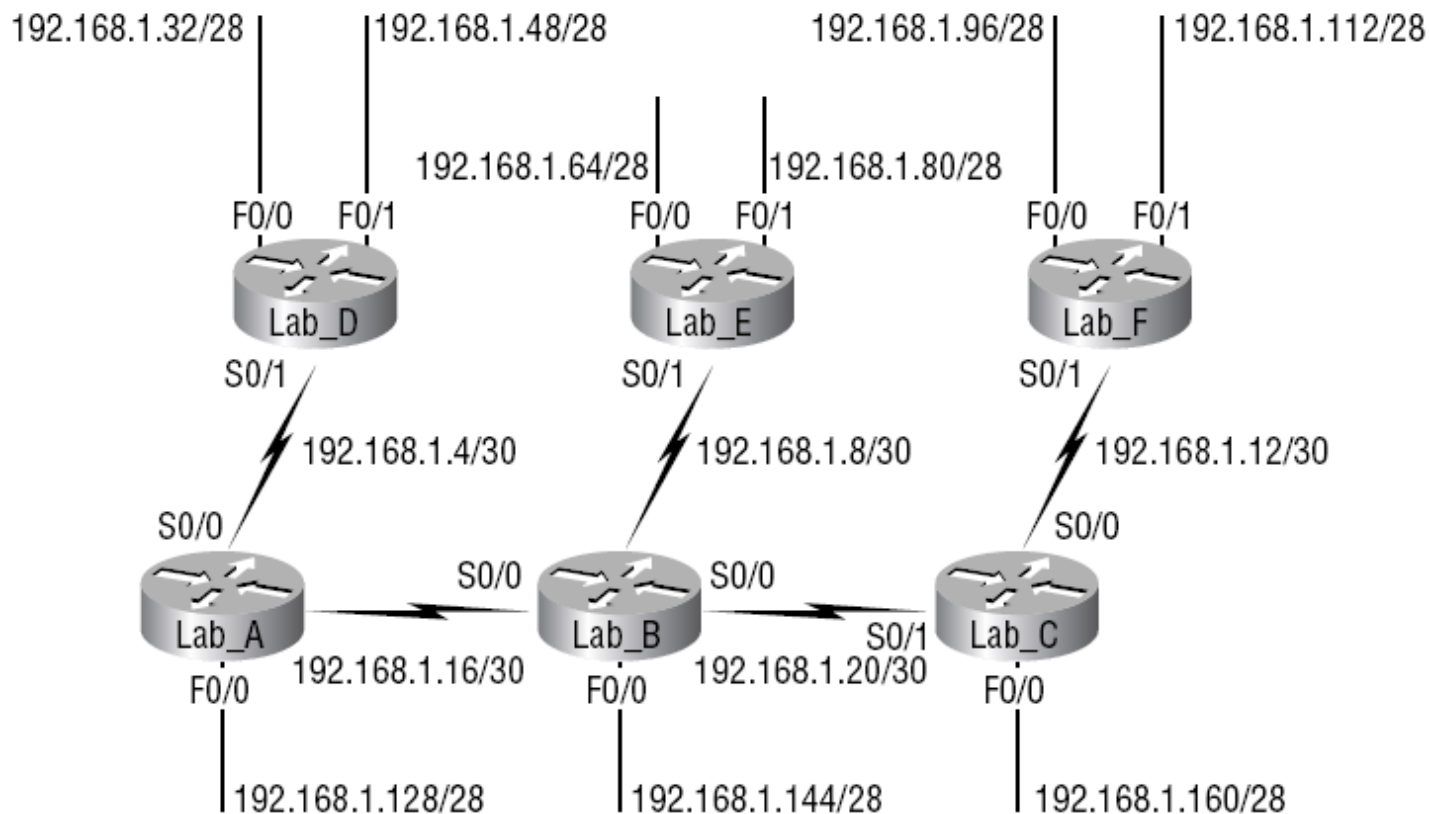


Обнаружение неисправностей, связанных с IP

- ping 127.0.0.1
- ping NIC's address
- ping the default gateway/ router
- ping the remote server.

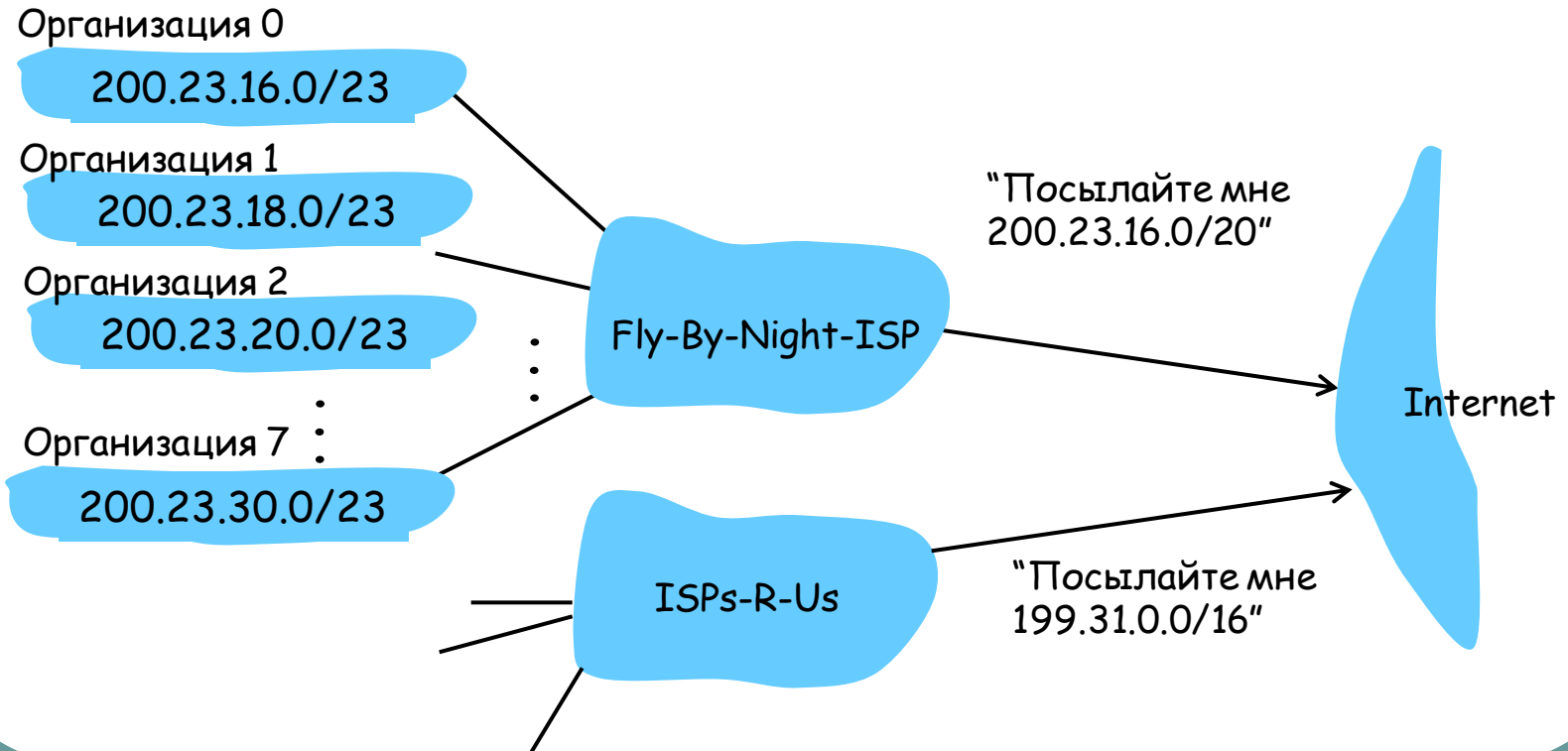
Variable Length Subnet Masks (VLSMs) - маски подсети переменной длины

- Classless (бесклассовые) протоколы маршрутизации должны передавать информацию и о маске
- Поддерживается RIPv2, EIGRP, OSPF



Иерархическая адресация: route aggregation (aka summarization)

Иерархическая адресация позволяет более эффективно анонсировать маршруты:



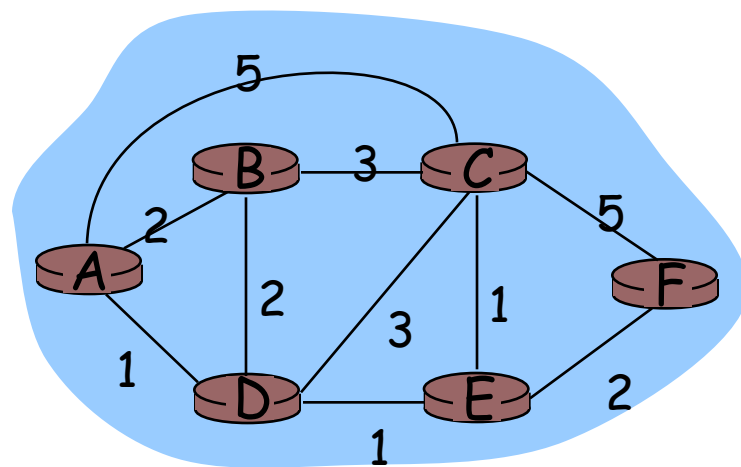
Маршрутизация (routing)

Протокол маршрутизации

Цель: определить «хороший» маршрут в сети между узлом-источником и приемником.

Методы задания маршрутизации:

- статическая (маршрутные таблицы задаются вручную)
- по-умолчанию (один маршрут для неизвестных сетей)
- динамическая, под управлением протокола маршрутизации



Протоколы маршрутизации

- IGP (Interior Gateway Protocols) - внутренние протоколы маршрутизации, распространяют маршрутную информацию внутри одной автономной системы. Примеры: RIP, OSPF, IGRP.
- RIP1,2 (Routing Information Protocol) - протокол передачи маршрутной информации, маршрутизаторы динамически создают маршрутные таблицы.
- IGRP, EIGRP – протоколы динамической маршрутизации CISCO
- OSPF (Open Shortest Path First) - протокол «Использовать кратчайший путь», является внутренним протоколом маршрутизации. Разработан после RIP, поддерживает маршрутизацию по нескольким путям, баланс их загрузки.
- EGP (Exterior Gateway Protocols) - внешние протоколы маршрутизации, распространяют маршрутную информацию между автономными системами. Примеры: EGP (Exterior Gateway Protocol, устарел), BGP.
- BGP (Border Gateway Protocol) - протокол граничных маршрутизаторов.

Значения административного расстояния AD

Route Source	Default AD
Connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown	255 (this route will never be used)

AD определяет степень доверия к информации о маршрутизации, полученной маршрутизатором от соседнего устройства.

Просмотр содержимого таблицы маршрутов (IP-таблицы)

```
RouterC#sh ip route
```

```
[...]
```

```
R 192.168.215.0 [120/2] via 192.168.20.2, 00:00:23, Serial0/0
```

```
R 192.168.115.0 [120/1] via 192.168.20.2, 00:00:23, Serial0/0
```

```
R 192.168.30.0 [120/1] via 192.168.20.2, 00:00:23, Serial0/0
```

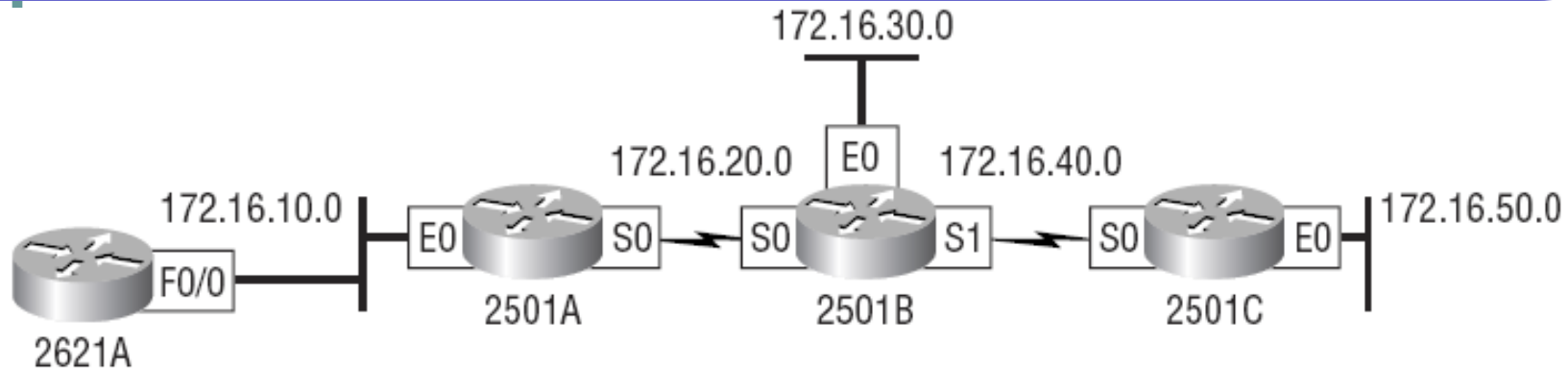
```
C 192.168.20.0 is directly connected, Serial0/0
```

```
C 192.168.214.0 is directly connected, FastEthernet0/0
```

Три класса протоколов маршрутизации intra-AS/IGP

- **Вектора расстояния (протоколы M по вектору расстояния, Distance vector)**
 - Каждое перенаправление пакета маршрутизатором называется участком (**hop**)
 - Наилучшим считается путь к удаленной сети с наименьшим количеством участков, это и есть **вектор**.
 - Посылает соседям полную таблицу
 - Примеры – RIP, IGRP.
- **Состояния связи (Link state)**
 - Постоянно проверяют состояние соседей с помощью HELLO протоколов
 - Поддерживают, обычно, 3 таблицы:
 1. соседей
 2. топологии всей сети
 3. таблица маршрутов.
 - Пример – OSPF, "первым - кратчайший путь" (open shortest path first).
- **Гибридные (Hybrid)**
 - Используют отдельные характеристики протоколов состояния связи и вектора расстояния. Пример – EIGRP.

Distance-vector маршрутизация



Routing Table		
172.16.10.0	F0/0	0

Routing Table		
172.16.10.0	E0	0
172.16.20.0	S0	0

Routing Table		
172.16.20.0	S0	0
172.16.30.0	E0	0
172.16.40.0	S1	0

Routing Table		
172.16.40.0	S0	0
172.16.50.0	E0	0

Starting ...

Routing Table		
172.16.10.0	F0/0	0
172.16.20.0	F0/0	1
172.16.30.0	F0/0	2
172.16.40.0	F0/0	2
172.16.50.0	F0/0	3

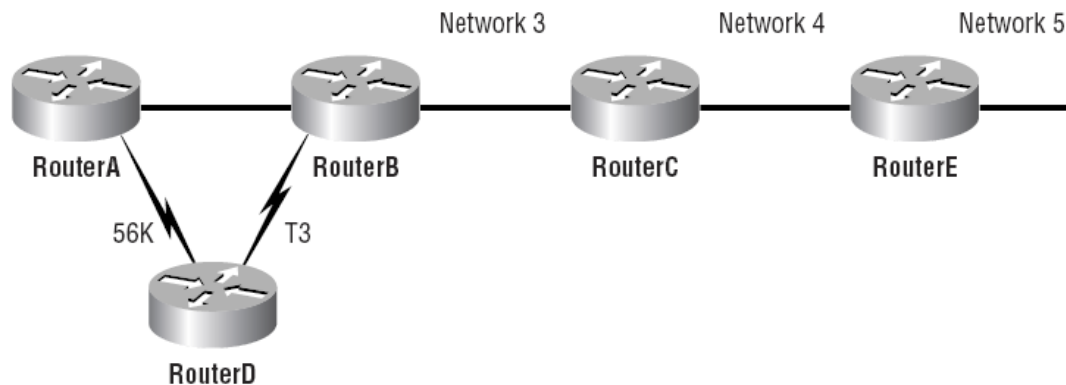
Routing Table		
172.16.10.0	E0	0
172.16.20.0	S0	0
172.16.30.0	S0	1
172.16.40.0	S0	1
172.16.50.0	S0	2

Routing Table		
172.16.20.0	S0	0
172.16.30.0	E0	0
172.16.40.0	S1	0
172.16.10.0	S0	1
172.16.50.0	S1	1

Routing Table		
172.16.40.0	S0	0
172.16.50.0	E0	0
172.16.10.0	S0	2
172.16.20.0	S0	1
172.16.30.0	S0	1

converged

Routing loop (петли маршрутизации и борьба с ними)



- Maximum Hop Count (максимальное число участков/хопов)
 - Ограничение на кол-во участков (хопов).
- Split Horizon (деление/расщепление горизонта)
 - Не анонсировать маршрут обратно через интерфейс, через который он получен
- Route Poisoning (порча пути)
 - Анонс недоступной сети, как сети с плохой метрикой (для RIP - 16, unreachable)
- Holddown (удержание)
 - не изменять маршрутную таблицу сразу за «подъемом» интерфейса, только в случае улучшившейся метрики

RIP

- Distance vector (протокол M по вектору расстояния)
- Открытый стандарт
- BSD-UNIX, 1982
- Обменивается с соседями полной таблицей каждые 30 секунд через Response Message (**advertisement, анонс**)
- Метрика: # хопов, максимальное число хопов - 15
- Версии: RIP1, RIP2, RIPng
- AD=120
- load balancing 4/6 линий с равной полосой
- RIPng поддерживает IPv6
- Дополнительные возможности вер. 2:
 - classless,
 - VLSMs
 - summarization,
 - authentication,
 - multicast вместо broadcasts в ver.1
 - discontinuous .
- Aka R.I.P.

Таймеры RIP

- Route update (обновления) timer
 - 30
- Route invalid (некорректного пути) timer
 - 180
- Holddown (удержание, если не получен маршрут с лучшей метрикой) timer
 - 180
- Route flush (очистки/удаления пути) timer
 - 240
- load balancing до 6 линий (4 - default)

Настройка RIP, основные команды

Lab(config)#router rip (далее указываются непосредственно подключенные анонсируемые сети)

Lab(config-router)#network 192.168.20.0

Lab(config-router)#network 192.168.30.0

Lab(config-router)#network 192.168.40.0

Lab(config-router)#network 192.168.50.0

?Lab(config-router)#version 2

?Lab(config-router)#passive-interface serial 0/1

Lab(config-router)#^Z

Lab#

Lab#sh ip route

[...]

R 192.168.30.0[120/1]via 192.168.40.1, 00:00:04, Serial0/0

Что не так с этим маршрутом ?

show ip route rip

show ip protocol

debug ip rip

Interior Gateway Routing Protocol (IGRP)

IGRP

Can be used in large internetworks

Uses an autonomous system number for activation

Gives a full route table update every 90 seconds

Has an administrative distance of 100

Uses bandwidth and delay of the line as metric (lowest composite metric), with a maximum hop count of 255

RIP

Works best in smaller networks

Does not use autonomous system numbers

Gives full route table update every 30 seconds

Has an administrative distance of 120

Uses only hop count to determine the best path to a remote network, with 15 hops being the maximum

Устарел, замена - гибридный Enhanced IGRP (EIGRP)

Таймеры IGRP

- **Update timers**
 - 90 seconds.
- **Invalid timers**
 - 3 * update
- **Holddown timers**
 - update timer + 10.
- **Flush timers**
 - 7 x update = 630

Настройка IGRP

```
Lab#config t
Lab(config)#router igrp 10
Lab(config-router)#netw 192.168.10.0
Lab(config-router)#netw 192.168.20.0
Lab(config-router)#^Z
Lab#
```

Lab#sh ip route

```
[...]
C 192.168.50.0 is directly connected, FastEthernet 0/0
C 192.168.40.0 is directly connected, Serial0/0
I 192.168.30.0 [100/143723] via 192.168.40.1, 00:00:42, Serial0/0
I 192.168.20.0 [100/152365] via 192.168.40.1, 00:00:52, Serial0/0
I 192.168.10.0 [100/158350] via 192.168.20.1, 00:00:36, Serial0/0
Lab_C#
```

158350 – composite metric

```
debug ip igrp events
debug ip igrp transactions
undebug all
```

Enhanced IGRP (EIGRP)

- Поддерживает IP, IPX, AppleTalk с помощью protocol-dependent modules
- Бесклассовый (как и RIPv2, OSPF)
- VLSM/CIDR (для поддержки разрывов, no auto-summary)
- Summaries, discontinuous (с разрывами) сети
- Обнаруживает соседей (MD5-auth.) и их состояние
- Работает через RTP: proprietary протокол, multicast с unicast откатом.
- Выбор пути с помощью Diffusing Update Algorithm (DUAL) алгоритма
- Метрика – композитная (составная): полоса, задержка (можно добавить дополнительно загрузку линии и надежность). Фигурируют в виде K-values.

Настройка EIGRP

```
Lab#config t
Lab(config)#router eigrp 100
Lab(config-router)#network 172.16.0.0
Lab(config-router)#network 10.0.0.0
Lab(config-router)#no auto-summary
```

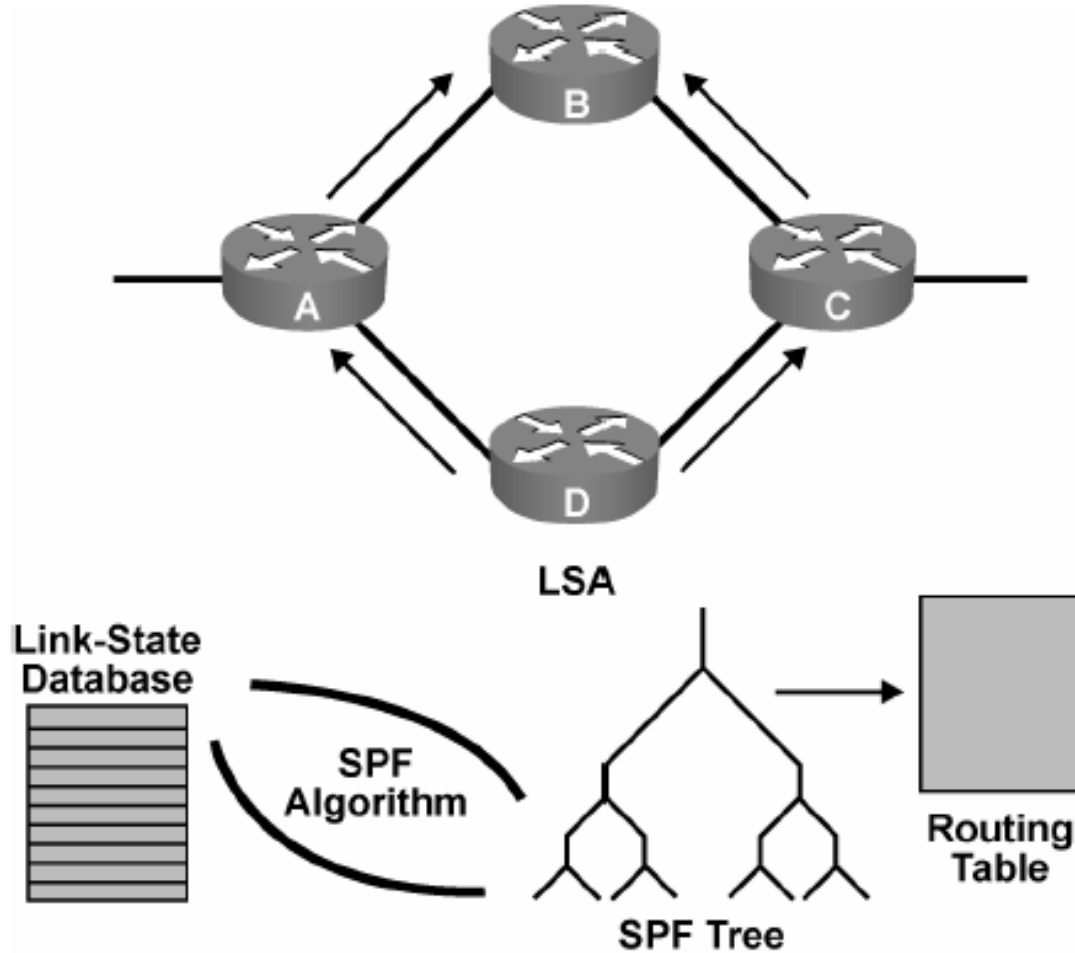
```
show ip route eigrp
show ip eigrp neighbors
show ip eigrp topology
```

```
Lab#sh ip route
[...]
D 192.168.50.0/24 [90/2707456] via 192.168.20.2,00:04:35, Serial0/0
```

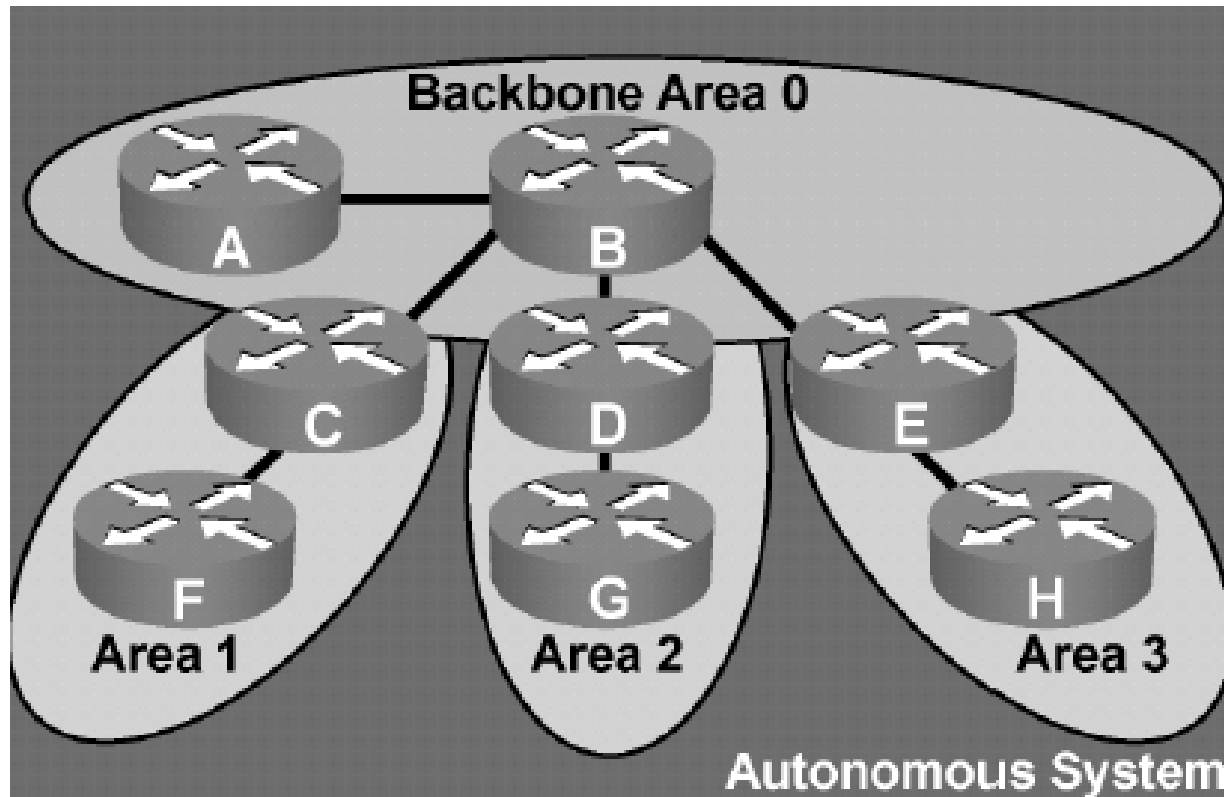
OSPF (Open Shortest Path First)

- открытый стандарт
- Использует метод «состояний связи/канала»
 - Распространяет пакеты LS (link state)
 - Таблица полной топологии сети на каждом узле
 - Выбор маршрута – алгоритм Dijkstra
- Анонсы распространяются внутри зоны
 - Использует IP, а не транспорты TCP или UDP

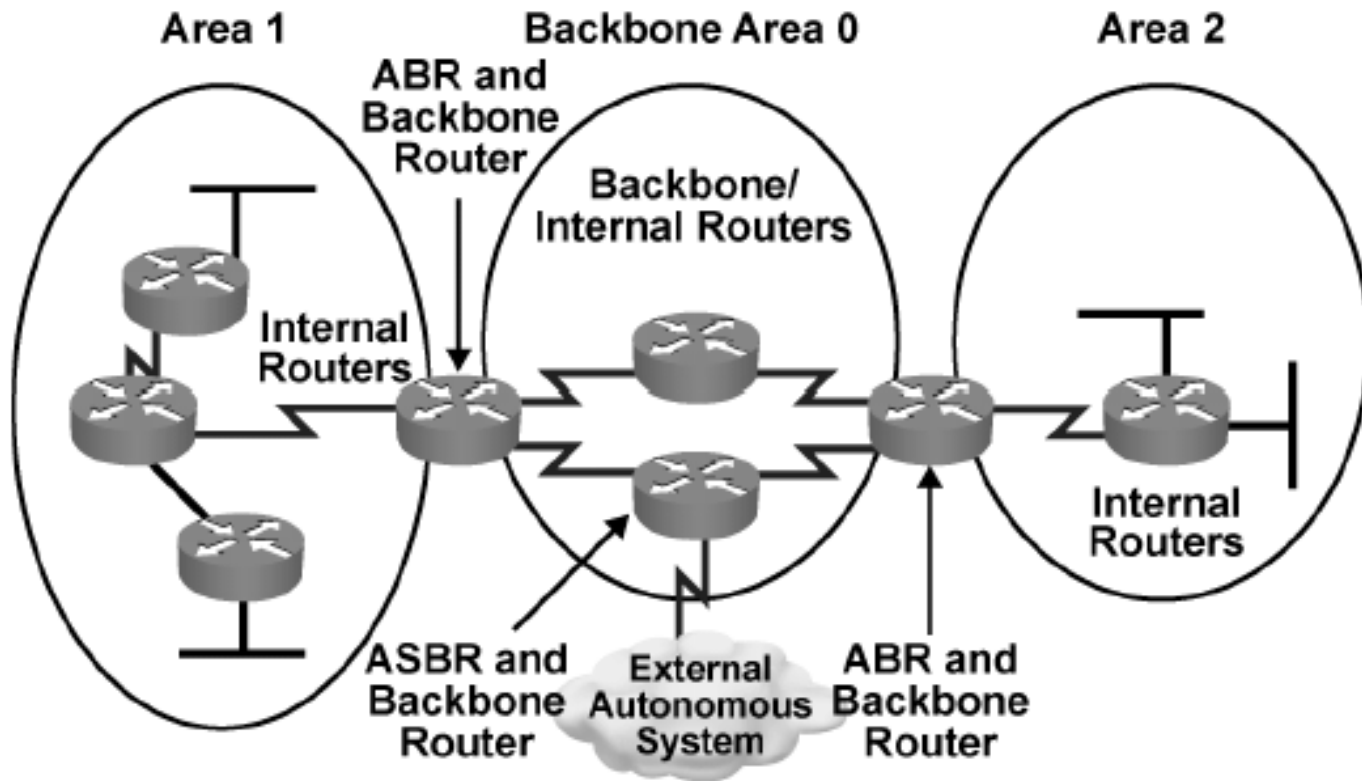
OSPF (Open Shortest Path First)



Дизайн сети для OSPF



Маршрутизаторы специального назначения в OSPF



OSPF особенности (нет в RIP)

- Иерархический подход (зоны, area) позволяет применять в крупных сетях
- Сообщения аутентифицированы
- Поддержка нескольких путей с одинаковой стоимостью
- Поддерживает ToS
- Имеет расширение для многоадресного режима Multicast OSPF (MOSPF)

Настройка OSPF

```
Lab#config t
```

```
Lab(config)#router ospf 64999
```

```
Lab(config-router)#network 192.168.40.0 0.0.0.255 area 0
```

```
Lab(config-router)#network 192.168.50.0 0.0.0.255 area 0
```

```
Lab(config-router)#^Z
```

```
Lab#
```

```
show ip ospf
```

```
show ip ospf database
```

```
show ip ospf interface
```

shows: IP, Area assignment, Process ID, RID, Network type, Cost, Priority, DR/BDR election information (if applicable), Hello and Dead timer intervals, Adjacent neighbor information

```
show ip ospf neighbor
```

```
show ip protocols
```

```
Lab#sh ip route
```

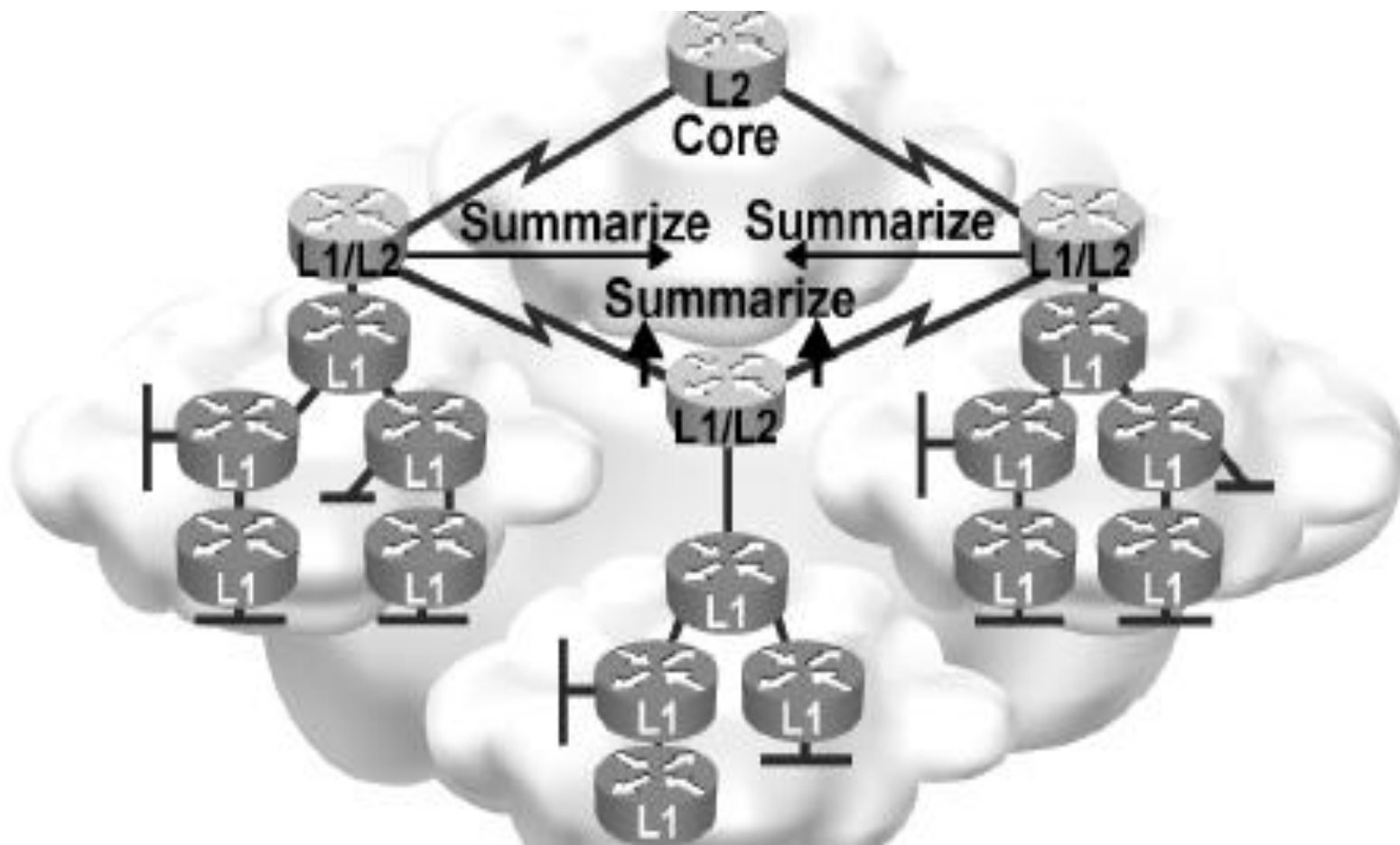
```
[...]
```

```
O 192.168.30.0/24 [110/65] via 192.168.20.2, 00:01:07, Serial0/0
```

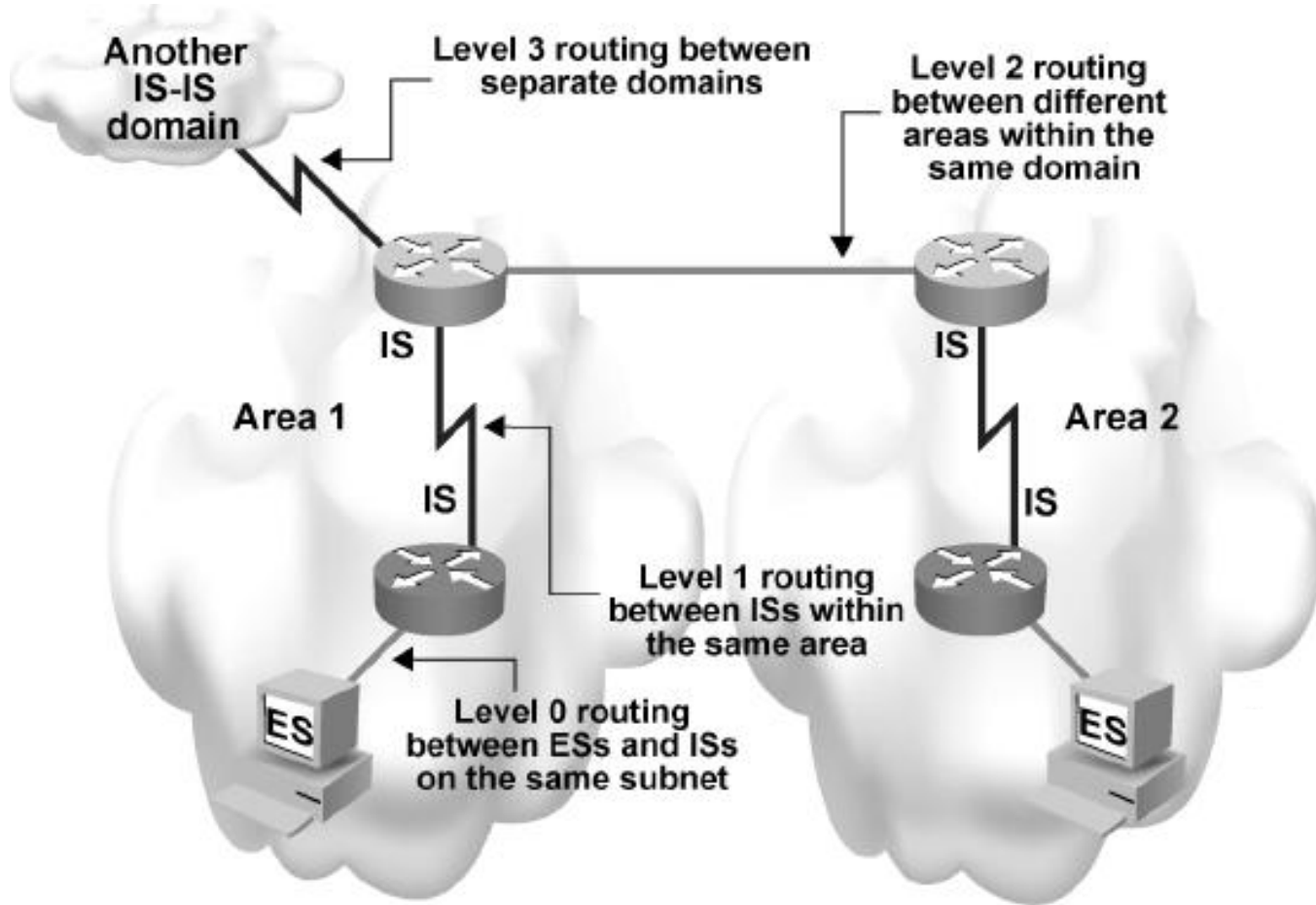
Intermediate System-to-Intermediate System (IS-IS)

- Разработан DEC для DECNet, затем стандартизирован ISO и позже дополнен для маршрутизации IP (Integrated IS-IS)
- Ориентирован на CLNS (3 уровень OSI)
- Протокол 3 уровня, реализующий CLNS, называется CLNP (Connectionless Network Protocol)
- IS-IS использует в т.ч. адресацию CLNS для идентификации маршрутизаторов (IS) и построения базы LSDB, даже работая в IP-сетях
- Является Link-State протоколом
- Использует подход OSPF, алгоритм Дейкстры

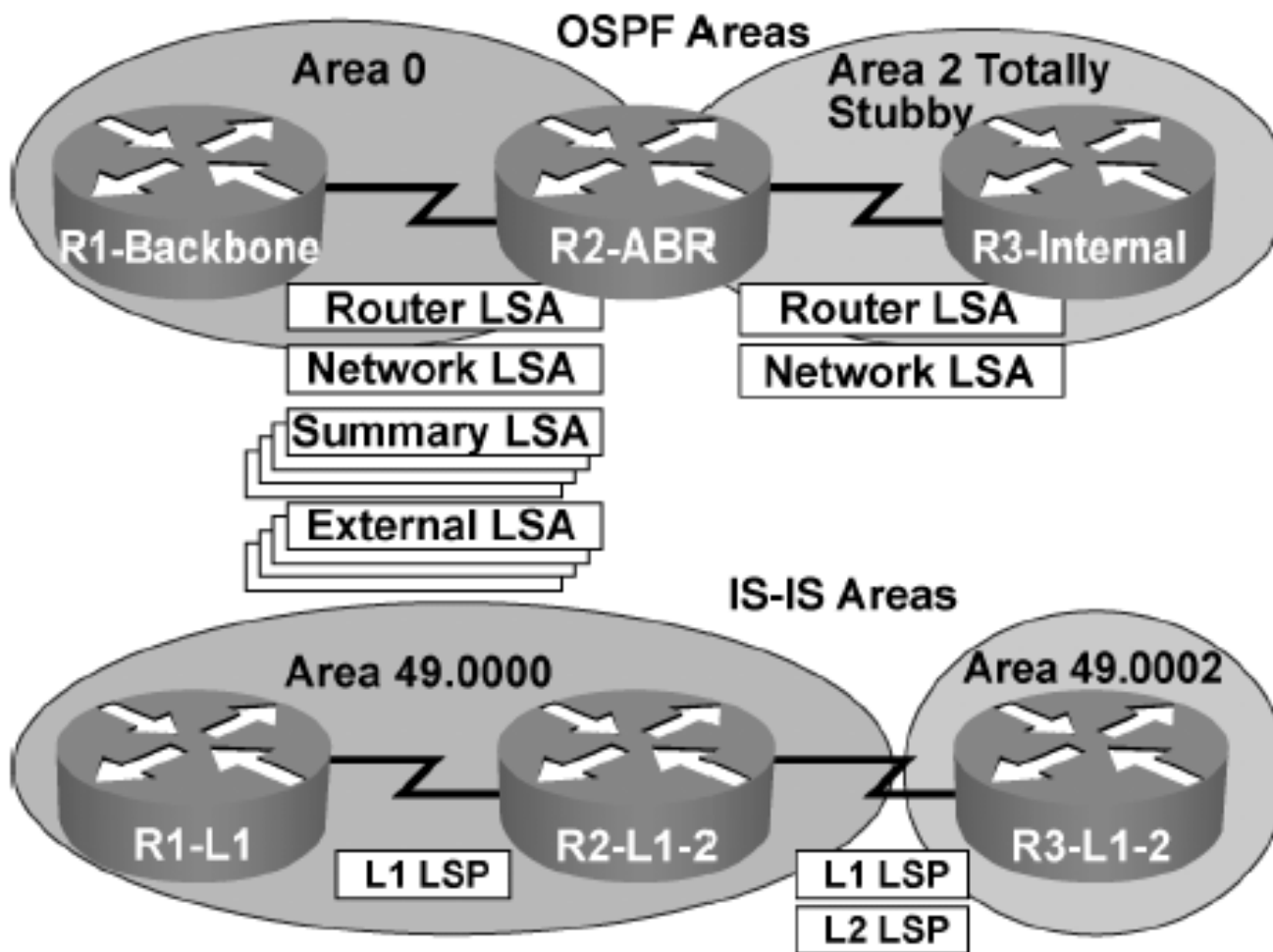
Integrated IS-IS. Используются CLNS PDU инкапсулированные непосредственно в кадры



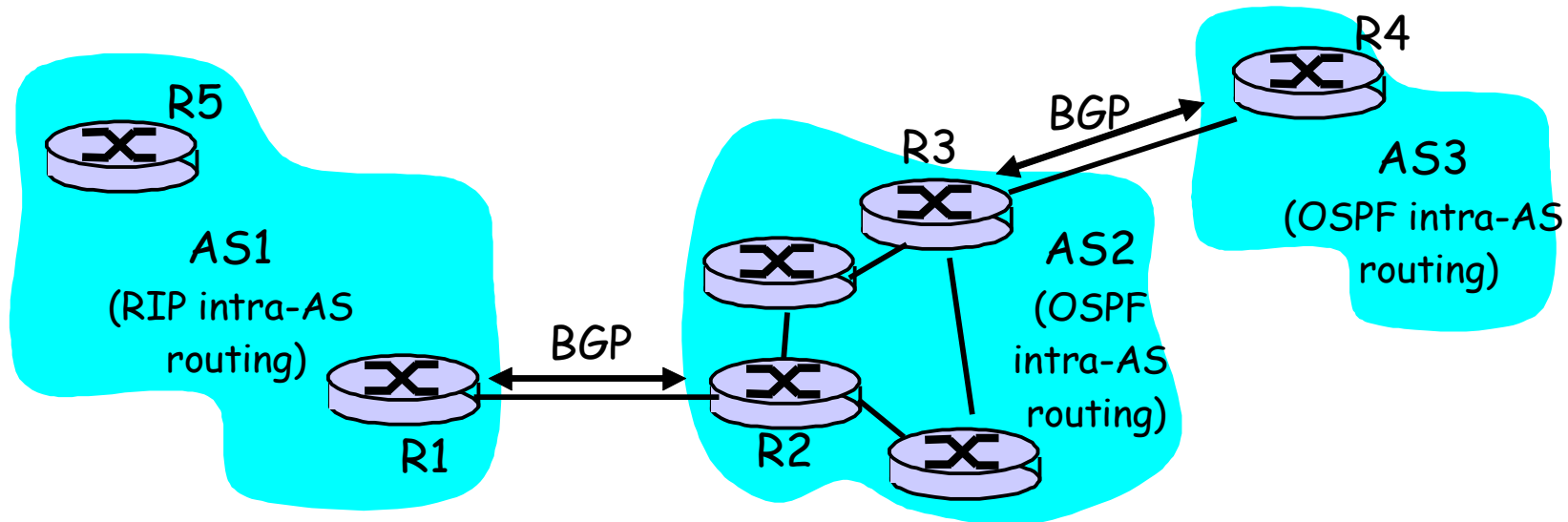
Уровни маршрутизации IS-IS



OSPF и IS-IS



Маршрутизация Inter-AS, BGP



Internet inter-AS routing: BGP

- BGP (Border Gateway Protocol): *стандарт de facto*
- **Протокол вектора пути (Path Vector):**
 - аналогичен Distance Vector
 - каждый Border Gateway передает пирам (peers) *полный путь, последовательность AS* до назначения
 - BGP маршрутизирует к AS, а не к отдельным узлам.
- Иногда используется внутри AS

Настройка BGP

- `router BGP 7777`
 - где 7777 - AS под Вашим контролем
- `neighbor 1.2.3.4 remote-as 8888`
- `network 9.10.11.0 mask 255.255.255.0`

- `show ip bgp summary`
- `show ip bgp`

Списки доступа IOS (Access Lists)

Управление трафиком с помощью списков доступа

- ***access list*** (список доступа) – это фильтр с набором правил обработки IP пакетов
- Правила:
 1. Порядок обработки IP пакета: сначала проверяется соответствие пакета условиям первой строки-правила списка доступа, затем второй и т.д.
 2. Пакет сверяется со строками-правилами списка пока не произойдет первое совпадение.
 3. Если нет строки-правила, которому соответствует пакет, то пакет сбрасывается. Т.о. действует подразумеваемое отвержение пакета (implicit "deny").

IOS команды для работы со списками доступа

- **access-list** Создает список строк-правил
-
- **ip access-list** Современный вариант создания СД (редактирование, etc.)
-
- **host** Определяет, что далее следует адрес узла.
-
- **0.0.0.0 255.255.255.255** Соответствует любой сети или узлу
-
- **any** тоже, что и **0.0.0.0 255.255.255.255**.
-
- **ip access-group** Применить список доступа к интерфейсу.
-
- **access-class** Применить список доступа к VTY линии.
-
- **show access-list** Показать списки доступа маршрутизатора.
-
- **show access-list 110** Показать только список доступа номер 110.
-
- **show ip access-list** Показать только списки доступа протокола IP.
-
- **show ip interface** Показать к каким интерфейсам применены списки.

Два ОСНОВНЫХ ТИПА СПИСКОВ

● Standard access lists

- Router(config)# access-list 10 deny 172.16.10.0 0.0.0.255
- Router(config)# access-list 10 deny host 172.16.30.2
- Router(config)# access-list 10 permit any
- or Router(config)# access-list 10 permit 0.0.0.0 255.255.255.255
- or Router(config)# access-list 10 permit 0.0.0.0 255.255.255.255 log
- Router(config)# int s0/0
- Router(config-if)# ip access-group 10 out

● Extended access lists

- Router(config)#access-list 110 deny tcp any 172.16.50.0 0.0.0.255 eq 23
- Router(config)#access-list 110 permit ip any any
- Router(config)#interface s0/0
- Router(config-if)#ip access-group 110 out

● Named access lists создаются и обозначаются не номерами, а именами

Управление доступом к VTY

- Router(config)#access-list 50 permit host 172.16.10.3
- Router(config)#line vty 0 4
- Router(config-line)#access-class 50 in

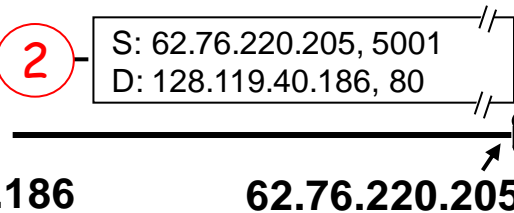
Верификация списков доступа

- Router#show running-config
- Router#show access-list
- Router#show access-list 110
- Router#show ip access-list
- Router#show ip interface

NAT: Network Address Translation, PAT

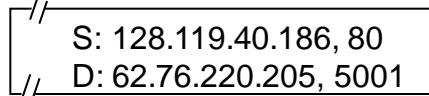
2. NAT

маршрутизатор
изменяет адрес
источника в
дейтаграмме
с 10.0.0.1, 3345 на
62.76.220.205, 5001,
актуализирует
таблицу



128.119.40.186

62.76.220.205



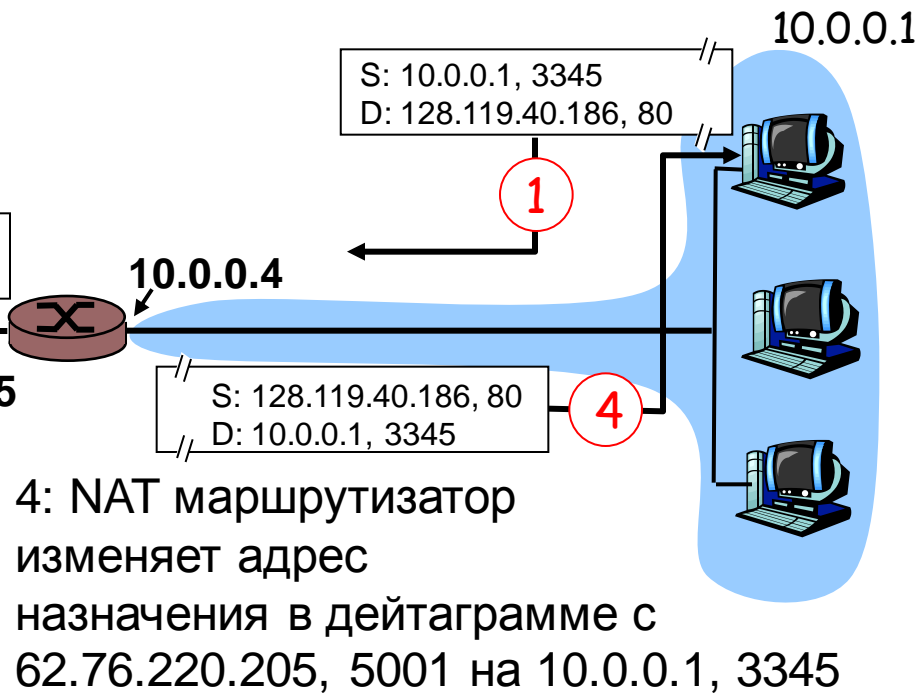
3: ответ поступает на
62.76.220.205, 5001

Типы: динам., стат., PAT

NAT таблица

WAN адрес	LAN адрес
62.76.220.205,5001	10.0.0.1, 3345
.....

1: Узел 10.0.0.1
посылает данные на
веб-сервер
128.119.40.186, 80



Конфигурирование статической NAT в IOS

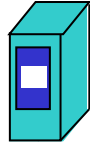
- # show running-config
- [...]
- interface Ethernet0/0
- ip address 10.1.1.3 255.255.255.0
- ip nat inside
- !
- interface Serial0/0
- ip address 200.1.1.251 255.255.255.0
- ip nat outside
- !
- ip nat inside source static 10.1.1.2 200.1.1.2
- ip nat inside source static 10.1.1.1 200.1.1.1
- # show ip nat translations

Конфигурирование динамической NAT и NAT/PAT (overload) в IOS

- # show running-config
- [...]
- interface Ethernet0/0
- ip address 10.1.1.3 255.255.255.0
- ip nat inside
- !
- interface Serial0/0
- ip address 200.1.1.251 255.255.255.0
- ip nat outside
- !
- ip nat pool fred 200.1.1.1 200.1.1.2 netmask 255.255.255.252
- ip nat inside source list 1 pool fred (доп. аргумент overload включает PAT)
- !
- access-list 1 permit 10.1.1.2
- access-list 1 permit 10.1.1.1
- # show ip nat translations

DHCP – Dynamic Host Configuration Protocol

DHCP server: 62.76.175.204



DHCP discover

```
src : 0.0.0.0
dest.: 255.255.255.255
yiaddr: 0.0.0.0
transaction ID: 654
```

НОВЫЙ КЛИЕНТ



DHCP offer

```
src: 62.76.175.204
dest: 255.255.255.255
yiaddr: 62.76.175.111
transaction ID: 654
Lifetime: 3600 secs
```

DHCP request

```
src: 0.0.0.0
dest.: 255.255.255.255
yiaddr: 62.76.175.111
transaction ID: 655
Lifetime: 3600 secs
```

DHCP ACK

```
src: 62.76.175.204
dest: 255.255.255.255
yiaddr: 62.76.175.111
transaction ID: 655
Lifetime: 3600 secs
```

время



- ip dhcp pool CS
- network 10.16.1.0/24
- domain-name cs.vsu.ru
- dns-server 10.16.1.205
- default-router 10.16.1.2

- RouterA(config-if)#ip address ?
- A.B.C.D IP address
- dhcp IP Address negotiated via DHCP
- pool IP Address autoconfigured from a local DHCP pool

ССЫЛКИ

- Building Scalable Cisco Internetworks, © 2006 Cisco Systems