# CCIE за год - материалы для изучения

## 

## 

[CCIE за год - материалы для изучения](#_j3ts5fk9um99)

[Цикл 1.](#_9yi4brm2uev3)

[Лабораторная работа по Теме 1. VLAN, trunking 1.1](#_3btksjvj09rn)

[Лабораторная работа по Теме 2. HDLC, PPP](#_7k6w64s0nksh)

[Лабораторная работа по Теме 3. Routing general](#_n1ktser40qlb)

[Лабораторная работа по Теме 4. Hold-Q, TX Ring, WFQ, Packet discard](#_8rzwm985psn0)

[Лабораторная работа по Теме 5. Console, Telnet, SSH](#_sb9nbby90rv8)

[Лабораторная работа по Теме 6. Private VLAN](#_uxtkg0rl0zya)

[Цикл 2.](#_egaia1fv5zo9)

[Лабораторная работа по Теме 7: VTP](#_ibd79rkypes)

[Задание #1 для лабораторной:](#_c0iudlkoxyz)

[Задание #2 для лабораторной:](#_co2q56ny9bgx)

[Задание #3 для лабораторной:](#_latpkgi330c7)

[Лабораторная работа по Теме 8: PPP Multilink, PPPoE](#_4wmihnuvt974)

[Задание #1 для лабораторной:](#_ijpeobpw6eww)

[Задание #2 для лабораторной:](#_atdpqyy0zqqn)

[Лабораторная работа по Теме 9: Static routing](#_s0kd6ptes3pw)

[Лабораторная работа по Теме 10: Compression, Fragmentation](#_90na64k2po91)

[Лабораторная работа по Теме 11: HTTP, TFTP, FTP](#_5gvu1taxee9o)

[Задание #1 для лабораторной:](#_dd0pxelcnpxa)

[Задание #2 для лабораторной:](#_1ewbv8d4nzdf)

[Задание #3 для лабораторной:](#_z0qo1asw3ovo)

[Лабораторная работа по Теме 12: ACL (VACL, Port ACL)](#_dz5ee41off1e)

[Первая большая лабораторная работа](#_bx572ntowcy5)

[Задание лабораторной](#_ew2pvc4ujktv)

[1. (2 баллов)](#_et9izxcu4ovu)

[2. (4 баллов)](#_pt9ozi17e0rj)

[3. (8 баллов)](#_n01t5jy8ic35)

[4. (6 баллов)](#_cud0syg4pz2i)

[5. (8 баллов)](#_samu8vve9pai)

[6. (8 баллов)](#_9yyf7d57q0ha)

[7. (6 баллов)](#_busc6ftnzap4)

[8. (6 баллов)](#_aeqwcbyq8m2y)

[9. (12 баллов)](#_skvnf6pdnz5l)

[Проверка лабораторной](#_4hy8z4vjaygg)

[Цикл 3.](#_73xjtc8bk7jb)

[Лабораторная работа по Теме 13: EtherChannel](#_drh92w7ij4g2)

[Задание #1 для лабораторной:](#_ukma2eh56rat)

[Задание #2 для лабораторной:](#_didqlctu9smr)

[Лабораторная работа по Теме 14: CAM, CDP, LLDP, UDLD](#_khmu72p8ywh8)

[Лабораторная работа по Теме 15: Routing Protocol features](#_4krq4s5a1lsn)

[Лабораторная работа по Теме 16: QoS 6.7-6.10](#_b0v60beo6r5y)

[Задание #1 для лабораторной:](#_io7x4kypbiks)

[Задание #2 для лабораторной:](#_xzdvj1pz40xr)

[Задание #3 для лабораторной:](#_gr1znvjuarte)

[Лабораторная работа по теме 17: Device Management 8.1.8 (SNMP)](#_7g1vlqubqvv2)

[Задание #1 для лабораторной:](#_jznwzs433ex3)

[Задание #2 для лабораторной:](#_jam2gobc4y8o)

[Лабораторная работа по теме 18: Layer 2 Security 7.1](#_gpf6ymfn94nj)

[Цикл 4.](#_t86hjldw5odt)

[Лабораторная работа по теме 19: PVST+ 1.4](#_4pbplmd0mc92)

[Задание #1 для лабораторной:](#_jwms9tm6eql1)

[Задание #2 для лабораторной:](#_os7yir1bx8ll)

[Лабораторная работа по теме 20: SPAN, RSPAN](#_1c19goajk2kp)

[Лабораторная работа по теме 21: RIPv2 3.4](#_krtlfvcbqp81)

[Лабораторная работа по теме 22: MQC WRED, GTC](#_40kybl6ocxv2)

[Задание #1 для лабораторной:](#_ia3f82jit92c)

[Задание #2 для лабораторной:](#_dwx1tnaakdzi)

[Лабораторная работа по теме 23: Logging 8.2](#_82xdcxmsmtnc)

[Лабораторная работа по теме 24: Layer 2 Security 7.1](#_xy46nne8ghx)

[Вторая большая лабораторная работа](#_9mp6tqb752ha)

[Задание лабораторной](#_i9m54mu1shk3)

[1. (6 баллов)](#_5w1rgzu61d01)

[2. (4 балла)](#_q34hwdc96fhp)

[3. (6 баллов)](#_8051p2laie62)

[4. (10 баллов)](#_r1nqe4g9nhzn)

[5. (3 балла)](#_cr29ah78q8ex)

[6. (4 балла)](#_j7cj695261gs)

[7. (3 балла)](#_u61xze2ar0v2)

[8. (6 баллов)](#_sqx34dwjunox)

[9. (7 баллов)](#_ukd2nrba3ok5)

[10. (11 баллов)](#_6s2l9q1rxs6r)

[Проверка лабораторной](#_zd7zpu4c8d2w)

[Цикл 5.](#_jot70czga1pq)

[Лабораторная работа по теме 25: STP 1.4](#_pznoh738ifzx)

[Лабораторная работа по теме 26: Miscellaneous 1.6](#_797r5g8kf4t4)

[Лабораторная работа по теме 27: RIPv2 3.4](#_7180z3dgykag)

[Лабораторная работа по теме 28: QoS 6.16-6.18, 6.22](#_dnv494csdvaz)

[Лабораторная работа по теме 29: NTP 8.3](#_bgtdnw226jh4)

[Лабораторная работа по теме 30: Management Plane Security 7.2](#_5v0pm448xjsk)

[Цикл 6.](#_r90v7htvfpx9)

[Лабораторная работа по теме 31: STP 1.4](#_vvusmfiqgghn)

[Лабораторная работа по теме 32: Layer 2 Security 7.1](#_ux74va57j331)

[Лабораторная работа по теме 33: EIGRP 3.5](#_vaxcinrsl9yj)

[Лабораторная работа по теме 34: QoS 6.19-6.20](#_dohoal4trzw4)

[Задание #1 для лабораторной:](#_3efknlrfl64j)

[Задание #2 для лабораторной:](#_s724f7ic4sgj)

[Лабораторная работа по теме 35: EEM 8.4](#_l3p300arbgu)

[Задание #1 для лабораторной:](#_kl40y688itz1)

[Задание #2 для лабораторной:](#_59lscgtwyxog)

[Лабораторная работа по теме 36: Management Plane Security 7.2](#_16h2xd4y0kva)

[Цикл 7.](#_l0gpm7ts3c4h)

[Лабораторная работа по теме 37: MST](#_qb6ixw5pakph)

[Лабораторная работа по теме 38: Object Tracking 9.1](#_xdxxgftqs789)

[Лабораторная работа по теме 39: EIGRP 3.5](#_ty8tzrxxqyig)

[Лабораторная работа по теме 40: QoS 6.21,6.23](#_yzx1v2xyo2dh)

[Лабораторная работа по теме 41: EEM 8.4](#_cfqd8m64umjf)

[Лабораторная работа по теме 42: Control Plane Security 7.3](#_slkxvvdl3dix)

[Цикл 8.](#_u2hwzeq5tog9)

[Лабораторная работа по теме 43: OSPF 3.6](#_hqqpovvsig0v)

[Лабораторная работа по теме 44: FHRP 9.2](#_iydyk24gufib)

[Лабораторная работа по теме 45: EIGRP 3.5](#_md1zn0vuai71)

[Лабораторная работа по теме 46: QoS. 6.24-6.25 Classification NBAR, L2 QoS](#_8jur6n1oi398)

[Лабораторная работа по теме 47: Auto-install, Menu, banner, alias](#_xiastfc4oi6e)

[Лабораторная работа по теме 48: ACL](#_dai0oruj5n3r)

[Задание #1](#_39qsaqg7wy7r)

[Задание#2](#_yp6plygmn0u1)

[Цикл 9](#_vht9ys6r8qjq)

[Лабораторная работа по теме 49: OSPF Network Types](#_ck924srp80ai)

[Задание 1:](#_dvtzcdg5djwr)

[Задание 2:](#_hlilwi4s30r4)

[Лабораторная работа по теме 50: DHCP 9.3](#_nxa4lo2zewww)

[Лабораторная работа по теме 51: EIGRP 3.5](#_qhn5ndlvuxda)

[Лабораторная работа по теме 52: Protocol Independent IPv4 Routing 3.1](#_em3bhaw6eipt)

[Лабораторная работа по теме 53: Miscellaneous System Management](#_yfim6gkz5bqb)

[Лабораторная работа по теме 54: Data Plane Security](#_34mko9efswes)

[Цикл 10](#_okfa02angpf7)

[Лабораторная работа по теме 55: OSPF 3.6](#_e9om97e8r06d)

[Лабораторная работа по теме 56: DHCP 9.3](#_feraepe4m3u8)

[Лабораторная работа по теме 57: EIGRP 3.5](#_89n0bkwmd8ij)

[Лабораторная работа по теме 58: IPsec LAN-to-LAN 4,2](#_rbralpi7oiju)

[Лабораторная работа по теме 59: Miscellaneous System Management 8.5](#_w613aac7gc1u)

[Лабораторная работа по теме 60: Data Plane Security 7.4](#_jv69wdz64d9x)

[Цикл 11](#_4bydxjbhc8hd)

[Лабораторная работа по теме 61: OSPF 3.6](#_vwh8fa7ix1xa)

[Лабораторная работа по теме 62: DNS 9.4](#_m3ubnetgwzgk)

[Лабораторная работа по теме 63: EIGRP 3.5](#_4y0xfkzu72y)

[Лабораторная работа по теме 64: IPsec LAN-to-LAN 4.2](#_27y8mm6kxmew)

[Задание №1](#_236y5s3e5oqv)

[Задание №2](#_iid7k5h5s3ym)

[Лабораторная работа по теме 65: Protocol Independent IPv4 Routing 3.1](#_kcq3axg63tw4)

[Лабораторная работа по теме 66: Data Plane Security 7.4](#_u4g6zvktsnbk)

[Цикл 12](#_ljdhr1kgnf56)

[Лабораторная работа по теме 67: OSPF 3.6](#_a4mr53f7w1p6)

[Лабораторная работа по теме 68: NAT 9.5](#_nb44vo2lfwoz)

[Лабораторная работа по теме 69: Miscellaneous EIGRP](#_9l6l9tvian04)

[Лабораторная работа по теме 70: IPsec LAN-to-LAN 4.2](#_11rpy9js6wc1)

[Лабораторная работа по темам 71-72: Policy routing (PBR), Traffic Filtering with Policy-Based Routing](#_w82ii5ky66ir)

[Цикл 13](#_319soyn9tvol)

[Лабораторная работа по теме 73: OSPF 3.6](#_od0jb4snf6cl)

[Лабораторная работа по теме 74: NAT 9.5](#_htuks0dyhfwd)

[Лабораторная работа по теме 75: Route redistribution](#_hmq7xssm7xsy)

[Лабораторная работа по теме 76: DMVPN 4.3](#_rv1wtshily14)

[Лабораторная работа по теме 77: Protocol Independent IPv4 Routing 3.1](#_h36olr4q9s2)

[Лабораторная работа по теме 78: Layer 2 Multicast 5.1](#_vgbi1s6mos4d)

[Цикл 14](#_tv09iifnqh8)

[Лабораторная работа по теме 79: OSPF Stub Areas](#_9u1dc8z6zwlr)

[Лабораторная работа по теме 80: Statefull NAT](#_pe45gu4e4ngo)

[Лабораторная работа по теме 81: IGMP snooping, proxy, filtering](#_18sbh2ek40d7)

[Лабораторная работа по теме 82: DMVPN Phase 1, Phase 2, Phase 3](#_n975eoevaalq)

[Задание 1](#_ga5e7bak4lqt)

[Задание 2](#_s5yf7vjj20mv)

[Задание 3](#_hodmif95u00a)

[Задание 4](#_islwwzczpusx)

[Цикл 14, Лабораторная работа по теме 84: BGP 3.7](#_s4icpexjotjt)

[Цикл 15](#_6111lyqtj080)

[Цикл 15, Лабораторная работа по теме 85: OSPF 3.6](#_m4q9yki4gmu7)

[Цикл 15, Лабораторная работа по теме 86: NAT 9.5](#_n55tmdbhgkau)

[Цикл 15, Лабораторная работа по теме 87: IGMP profiles, Multicast VLAN registration](#_k21xf441hzmr)

[Цикл 15, Лабораторная работа по теме 88: DMVPN 4.3](#_9m1why5pkrua)

[Цикл 15, Лабораторная работа по теме 90: BGP 3.7](#_r293rio6utu1)

[Цикл 16](#_aau2gyob4pff)

[Цикл 16, Лабораторная работа по теме 91: Default Routing](#_t04mu0fvtc3b)

[Цикл 16, Лабораторная работа по теме 92: Static Extendable NAT, NAT ALG](#_47qm1mfhhlgi)

[Цикл 16, Лабораторная работа по теме 93: Multicast routing intro. PIM Dense Mode](#_aq2go7tnc85u)

[Цикл 16, Лабораторная работа по теме 94: QoS Pre-classification](#_pzm6kel8qt2d)

[Цикл 16, Лабораторная работа по теме 95: Protocol Independent IPv6 Routing 3.2](#_mcybc7caxudk)

[Цикл 16, Лабораторная работа по теме 96: BGP 3.7](#_m9bnbaqwmkp2)

[Цикл 17](#_d77en2naxc3h)

[Цикл 17, Лабораторная работа по теме 97: OSPF 3.6](#_8nyijn5q04qo)

[Цикл 17, Лабораторная работа по теме 98: Traffic Accounting 9.6](#_85yo3q49qd1g)

[Цикл 17, Лабораторная работа по теме 99: IPv4 Multicast Routing 5.2](#_8ami3s3mmx3t)

[Цикл 17, Лабораторная работа по теме 100: BGP 3.7](#_icjmnn499js7)

[Цикл 17, Лабораторная работа по теме 101: EUI-64, SLAAC](#_f2es9pndn4gf)

[Цикл 17, Лабораторная работа по теме 102: BGP 3.7](#_bcr9q0axhadi)

[Цикл 18](#_8ovx54ligt0e)

[Цикл 18, Лабораторная работа по теме 103: OSPF 3.6](#_24c6euqqun2d)

[Цикл 18, Лабораторная работа по теме 104: NetFlow 9.7](#_s37ytilkdkcu)

[Цикл 18, Лабораторная работа по теме 105: IPv4 Multicast Routing](#_qq22vmq28efp)

[Цикл 18, Лабораторная работа по теме 106: BGP 3.7](#_bdo083kokb7d)

[Цикл 18, Лабораторная работа по теме 107: DHCPv6](#_z4h1hjkf31sk)

[Цикл 18, Лабораторная работа по теме 108: BGP 3.7](#_glm3q2rkio36)

[Цикл 19](#_x2q96w7qixuf)

[Цикл 19, Лабораторная работа по теме 109: OSPF 3.6](#_cdk53qrncmhm)

[Цикл 19, Лабораторная работа по теме 110: Miscellaneous Network Services 9.8](#_f0s1p5oaj45p)

[Цикл 19, Лабораторная работа по теме 111: IPv4 Multicast Routing](#_fbq5l9aj8k19)

[Цикл 19, Лабораторная работа по темам 112 и 114: BGP](#_w8hsfdfu3cun)

[Цикл 20](#_3alt44bzyw)

[Цикл 20, Лабораторная работа по теме 115-116: MPLS, Miscellaneous Network Services](#_pz40ubcek321)

[Цикл 20, Лабораторная работа по теме 117: IPv4 Multicast Routing](#_nutahzboxp4z)

[Цикл 20, Лабораторная работа по теме 118: BGP](#_d03wxu9alr8c)

[Цикл 20, Лабораторная работа по теме 119: First Hop Redundancy Protocols 9.2 (IPv6)](#_w7sspio9tmdb)

[Цикл 20, Лабораторная работа по теме 120: BGP](#_wz9lpj9i3n0b)

[Цикл 21](#_qne54anpolql)

[Цикл 21, Лабораторная работа по теме 121: MPLS](#_jeqtnusiket6)

[Цикл 21, Лабораторная работа по теме 122: BGP](#_6j5c51afhxby)

[Цикл 21, Лабораторная работа по теме 123: BGP](#_95ms3dgfm634)

[Цикл 21, Лабораторная работа по теме 124: MPLS](#_y8dbbp2fly0y)

[Цикл 21, Лабораторная работа по теме 125: Data Plane Security (IPv6)](#_df7e3nw5uv7k)

[Цикл 21, Лабораторная работа по теме 126:](#_26jp3e9dhur)

[Цикл 22](#_czjn8t54m1cl)

[Цикл 22, Лабораторная работа по теме 127:MPLS](#_758r0ui6vjcz)

[Цикл 22, Лабораторная работа по теме 128:BGP](#_xk0tgvi9kd0k)

[Цикл 22, Лабораторная работа по теме 130:MPLS](#_3j7drxjjhqrw)

[Цикл 23](#_y7kcixgd71bo)

[Цикл 24](#_u6k1akg34prh)

[Цикл 25](#_tw1t2gbj1t1i)

[Цикл 26](#_bklco3ealeyn)

## 

# [**Цикл 1.**](http://ccie.linkmeup.ru/2016/04/02/tsikl-1-razdel-1-vlan-trunking-1-1/)

## [**Лабораторная работа по Теме 1.**](http://ccie.linkmeup.ru/2016/04/04/laboratornaya-rabota-po-teme1/) **VLAN, trunking 1.1**

1. Загрузить начальную конфигурацию на SW1, SW2, SW3, SW4. [Ссылка](https://drive.google.com/file/d/0ByVf6yfX4EBfQ0x4WkUwaHkwaGs/view?usp=drive_web) на начальную конфигурацию.
2. На SW1 интерфейсы eth0/1, eth0/2, eth0/3, eth1/0 должны быть в режиме access в таких VLAN, соответственно: 10, 20, 30, 40.
3. На SW2: интерфейс eth0/2 должен быть в режиме access в VLAN 20. Задать ему имя VLAN: TWENTY.
4. На SW3: интерфейс eth0/2 добавить в режиме access в VLAN 30. VLAN 30 задать имя THiRTY.
5. На SW4: интерфейсы eth0/2-3 добавить в режиме access в VLAN 40.
6. На SW2, порты, подключенные к SW1 перевести в режим режим «desirable» создания транка.
7. На SW1 порты, подключенные к SW2 перевести в режим ручного создания транка.
8. На SW3 на портах, подключенных к SW1 создать транк вручную.
9. Порты между SW4 и SW1 перевести в ручной режим транка и убрать dtp.
10. На всех транках VLAN 108 должен передаваться нетегированным.
11. На SW1 создать int vlan 20 c ip 10.10.20.10/24, int vlan 30 c ip 10.10.30.10/24, int vlan 40 c ip 10.10.40.10/24
12. На SW2 создать int vlan 20 с ip 10.10.20.20/24. На SW3 создать int vlan 30 с ip 10.10.30.30/24. На SW4 создать int vlan 40 с ip 10.10.40.40/24
13. На SW1 разрешить передавать в транках только те VLANы, которые настроены на других коммутаторах.
14. Отправить пинг с SW1 на 255.255.255.255. Все ip адреса, настроенные на свичах должны пинговаться.

В лабораторной работе может быть несколько заданий соответственно в папках (task1, task2 и т.д.). Участникам нужно будет загрузить конечные конфигурации в папки task1, task2 и т.д. в соответствующую папку(в данной лабораторной работе папка lab001).

## 

## [**Лабораторная работа по Теме 2**](http://ccie.linkmeup.ru/2016/04/06/laboratornaya-rabota-po-teme-2/)[**.**](http://ccie.linkmeup.ru/2016/04/06/materialy-po-tsiklu-1-teme-2/) **HDLC, PPP**

Задание #1 для лабораторной:

1) Загрузить начальную конфигурацию R1, R2, R9, R10. [Ссылка](https://drive.google.com/open?id=0ByVf6yfX4EBfSW4zb2ZzblFreXM) на начальную конфигурацию.

2) Настроить инкапсуляцию PPP между маршрутизаторами R1 и R2.Настроить инкапсуляцию PPP между маршрутизаторами R9 и R10.

3) Поменять ip адрес 188.1.91.1/24 на интерфейсе S1/0 маршрутизатора R9 и задать ip адрес 10.9.8.7/24 и отправить пинг на R10

4) Настроить двустороннюю аутентификацию PAP на R1 к R2. Задать пароль CCIEinaYEAR? глобально на обоих маршрутизаторах.

5) Настроить одностороннюю аутентификацию CHAP от R9к R10 используя hostname Server. Задать пароль по умолчанию CCIEinaYEAR? на интерфейсе S1/0 маршрутизатора R10 для ответа на любой запрос .

## [**Лабораторная работа по Теме 3**](http://ccie.linkmeup.ru/2016/04/08/laboratornaya-rabota-po-teme-3/)**. Routing general**

Ребята, сегодня пятница и кина лабораторной не будет.

По данной теме одна теория, поэтому мы решили не заморачиваться с лабораторной работой и дать вам немного отдохнуть от первой напряженной недели обучения.

У вас есть возможность остановиться и проанализировать проделанную работу. Тем более, что отдых, как показывают новые [исследования](http://psypress.ru/articles/27528.shtml), позволяет лучше запомнить пройденный материал.

У вас появляется немного больше времени на то, чтобы «закрыть хвосты»- ответить на все оставшиеся теоретические вопросы, доделать 2 начальные лабораторные работы и написать эссе.

Честно говоря, мы не ожидали такого ажиотажа по поводу материалов и лабораторных работ.

Было много вопросов по поводу их формулировок. Хотелось бы внести ясность. Мы стараемся, чтобы формулировки были предельно понятны. И спасибо всем, кто дает свои комментарии по этому поводу.

Также хочется заострить внимание на том, что все задания построены таким образом, чтобы дать вам больше возможностей найти информацию самостоятельно.

Таким образом, мы даем в задании или лабораторной работе небольшие подсказки и, как видите, это приносит свои плоды. Вы стали приводить множество примеров настройки той или иной технологии. Вы узнаёте различные способы настроек одной и той же технологии. А постоянный поиск дает возможность закрепить знания в долговременную память.

Это очень показательно и мы будем стараться, чтобы дальше вам было еще интересней.

Нам интересно узнать сколько времени вы потратили на поиск ответов и выполнение лабораторных заданий. Пожалуйста, отпишитесь в комментариях.

## [**Лабораторная работа по Теме 4.**](http://ccie.linkmeup.ru/2016/04/11/laboratornaya-rabota-po-teme-4/) [**Hold-Q, TX Ring, WFQ, Packet discard**](http://ccie.linkmeup.ru/2016/04/09/tsikl-2-tema-4-hold-q-tx-ring-wfq-packet-discard/)

Задание для лабораторной:

1. Загрузить начальную конфигурацию R1, R2. [Ссылка](https://drive.google.com/open?id=0ByVf6yfX4EBfZFFjU0hNWnlzLUE) на начальную конфигурацию.
2. На маршрутизаторе R1 настроить политику с названием WFQ. Политика передачи трафика от r1 к r2, должна использовать по умолчанию технологию WFQ.
3. Поменять ограничение по пакетам на 100 в политике. Применить политику на интерфейсе.
4. Проверить конфигурацию, используя соответствующие команды show

## [**Лабораторная работа по Теме 5.**](http://ccie.linkmeup.ru/2016/04/13/494/) [**Console, Telnet, SSH**](http://ccie.linkmeup.ru/2016/04/11/tsikl-1-tema-5-console-telnet-ssh/)

Задание для лабораторной:

1. Загрузить начальную конфигурацию SW1, SW2, SW3, SW4. [Ссылка](https://drive.google.com/open?id=0ByVf6yfX4EBfUjRtYmFhTDNrVG8) на начальную конфигурацию.
2. На SW1, SW2, SW3, SW4 настроить доступ на консоль с шифрованным паролем CCIEinaYEAR?
3. На SW1 и SW4 настроить ssh версию 2.
4. На SW2 настроить доступ на vty 0 4 с паролем CCIEinaYEAR?
5. На SW1 настроить интерфейс vlan 40 c ip 188.1.40.2/24
6. На SW1, SW3 настроить доступ по SSH c длиной ключа rsa 1024. Использовать имя домена ccie.linkmeup.ru. Создать пользователя CCIEadmin. Прописать для него шифрованный пароль CCIEinaYEAR?  
   Включить для SSH аутентификацию по локальной базе пользователей.
7. На SW4 настроить интерфейс vlan 40 c ip 188.1.40.1/24
8. На SW4 настроить доступ по SSH c длиной ключа rsa 1024 на порт 4040 на линии 4. Прописать имя домена ccie.linkmeup.ru. Создать пользователя CCIEadmin. Прописать для него шифрованный пароль CCIEinaYEAR?  
   Включить для SSH аутентификацию по локальной базе пользователей.  
   Настроить таймаут в 30 сек для SSH. Включить журналирование событий SSH. Настроить 3 попытки подключения для SSH. Все сессии SSH должны использовать IP-адрес интерфейса vlan 40 как адрес отправителя.
9. Проверить соединение от SW1 к SW4 и обратно.

## [**Лабораторная работа по Теме 6.**](http://ccie.linkmeup.ru/2016/04/15/laboratornaya-rabota-po-teme-6/) [**Private VLAN**](http://ccie.linkmeup.ru/2016/04/13/tsikl-1-tema-6-private-vlan/)

Для выполнения заданий используются материалы, соответствующие главам рассмотренным в данной теме. Для этого необходимо использовать функционал, соответствующий данному подразделу, в противном случае, задание не будет засчитано.

Задание для лабораторной:

1. Загрузить начальную конфигурацию R1, SW1, SW2, SW3, SW4. [Ссылка](https://drive.google.com/open?id=0ByVf6yfX4EBfVm5ZRklBNjNDZEk) на начальную конфигурацию.

2. На SW4 настроить интерфейс Ethernet 3/2 так, чтобы он блокировал любой unicast, multicast, или broadcast трафик на порт, настроенный в таком же режиме и наоборот. При этом, со всеми остальными портами коммутатора sw4, порт должен работать в обычном режиме.

3. На R1 интерфейcу Ethernet0/1 задать IP-адрес 192.168.10.11/24.

4. Перевести SW1 в VTP режим, при котором коммутатор принимает и передает VTP сообщения, но не изменяет локальную базу VLAN’ов, и настроить следующие VLAN’ы:

a) VLAN 11 — настроить как PVLAN позволяющий передавать трафик на любой порт;

b) VLAN 3030 — настроить как PVLAN, ограниченный передачей трафика только на Promiscuous порт;

c) VLAN 3031 — настроить как PVLAN, ограниченный передачей трафика только на Promiscuous порт и порты, настроенные в том же типе (и том же VLAN’е).

d) Соотнести типы PVLAN друг с другом.

e) Проверить настройки PVLAN командой sh run | s vlan.

f) Настроить интерфейс Ethernet0/0 коммутатора SW1, подключенный к R1, в режиме Promiscuous

g) Задать соответствие между PVLAN 11, 3030, 3031 согласно их типам в пунктах a) b) и c)

h) Проверить правильность настройки командами show vlan private-vlan, show interface status или show interface eth0/0 switchport.

5. На интерфейсах SW2, SW3, SW4, подключенных к SW1, задать IP-адреса:

192.168.10.21/24 – на Ethernet2/2 SW2,

192.168.10.31/24 – на Ethernet3/1 SW3,

192.168.10.41/24 – на Ethernet3/3 SW4

6. Интерфейс SW1, подключенный к SW4, должен быть в VLAN 3030, настроенный согласно пункта 4 b).

7. Интерфейсы SW1, подключенные к коммутаторам SW2 и SW3, должны быть в VLAN 3031, настроенные согласно пункта 4 c).

8. Отправить с маршрутизатора и коммутаторов ICMP-запрос таким образом, чтобы это позволило опросить все устройства в одном broadcast домене. Убедиться, что со стороны R1 доступны все IP-адреса, SW2 и SW3 доступны только друг для друга и для них доступен R1, а с SW4 доступен только IP адрес 192.168.10.11.

# [**Цикл 2.**](http://ccie.linkmeup.ru/2016/04/16/544/)

## **[Лабораторная работа по Теме 7: VTP](http://ccie.linkmeup.ru/2016/04/18/laboratornaya-rabota-po-teme-7-vtp/)**

### Задание #1 для лабораторной:

Подготовка лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfQmhxYm5NUDJMdEU) на SW1, SW2, SW3, SW4 .
2. Перевести все неиспользуемые интерфейсы, не подключенные ни к одному устройству в состояние shutdown и в access VLAN 999.

|  |  |
| --- | --- |
| **SWITCH** | **PORT** |
| **SW1** | E1/1 |
| E1/2 |
| E1/3 |
| E2/0 |
| E2/1 |
| **SW2** | E0/2 |
| E0/3 |
| E1/0 |
| E1/1 |
| E1/2 |
| E1/3 |
| E2/1 |
| — |
| **SW3** | E0/1 |
| E0/2 |
| E0/3 |
| E1/0 |
| E1/1 |
| E1/2 |
| E1/3 |
| E2/1 |
| — |
| **SW4** | E0/2 |
| E0/3 |
| E1/0 |
| E1/1 |
| E1/2 |
| E1/3 |
| E2/1 |
| — |

1. Убедиться что все неиспользуемые интерфейсы переведены в состояние shutdown.
2. Убедиться что Inter-switch линки соответствуют следующей таблице.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Switch** | **Port** | **Switch** | **Port** | **Mode** | **State** |
| SW1 | 2/2 | SW2 | 2/2 | Trunk | Up |
| 2/3 | 2/3 | Trunk | Up |
| 3/0 | SW3 | 3/0 | Trunk | Up |
| 3/1 | 3/1 | Trunk | Up |
| 3/2 | SW4 | 3/2 | Trunk | Up |
| 3/3 | 3/3 | Trunk | Up |
| SW2 | 3/0 | SW4 | 3/0 | — | Shutdown |
| 3/1 | 3/1 | — | Shutdown |
| 3/2 | SW3 | 3/2 | — | Shutdown |
| 3/3 | 3/3 | — | Shutdown |
| SW3 | 2/2 | SW4 | 2/2 | — | Shutdown |
| 2/3 | 2/3 | — | Shutdown |

Конфигурация

1. Коммутаторы SW1, SW2, SW3, SW4 перевести в режим VTP Server. На коммутаторе SW1 настроить 2-ую версию VTP, домен CCIEinaYEAR. Проверить командой sh vtp status на коммутаторах SW1, SW2, SW3, SW4, что они синхронизированы и имеют одинаковый номер ревизии.
2. Перевести SW1 в VTP режим, при котором коммутатор не распространяет информацию своего VLAN Database. Коммутаторы SW2, SW3 перевести в режим VTP в котором устройство может изменять VLAN Database только на основании обновлений VTP. Перевести SW4 в режим, при котором коммутатор может создавать, удалять и изменять VLANы в домене.
3. На SW4 создать следующие VLAN’ы: VLAN 100; VLAN 200; VLAN 300.
4. На SW4 создать SVI для VLAN 100 и задать ему IP-адрес 192.168.1.4/24. На SW2 создать SVI для VLAN 100 и задать ему IP-адрес 192.168.1.2/24. На SW3 создать SVI для VLAN 100 и задать ему IP-адрес 192.168.1.3/24. Проверить командой sh vtp status на SW2, SW3, SW4, что они синхронизированы и имеют одинаковый номер ревизии, а SW1 не синхронизирован.
5. На коммутаторе SW1 создать VLAN 100
6. C коммутатора SW4 отправить пинг на адреса 192.168.1.2, адрес 192.168.1.3/24
7. На SW1 проверить командой show spanning-tree vlan 100, что у нас отправляется трафик по VLAN 100.

### Задание #2 для лабораторной:

Подготовка лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B3uwAH0p4u2NZm1aLTFUWTFhY1k) на SW1, SW2, SW3, SW4 .

Конфигурация

1. На SW4 создать следующие VLAN: 10, 20, 30, 40, 50, 60, 333. На коммутаторе SW4 настроить VTP, в режиме ограничения нежелательного трафика к коммутаторам, не использующих какие либо VLANы из списка для коммутации трафика.
2. Перевести SW1 в режим, при котором коммутатор может изменять VLAN Database только на основании обновлений VTP.
3. Проверить синхронизацию VLAN database на коммутаторе SW1.
4. На коммутаторе SW4 добавить интерфейс Ethernet 0/3 в VLAN 60, и включить его командой no shutdown.
5. На коммутаторе SW3 добавить интерфейс Ethernet 0/3 в VLAN 333, и включить его командой no shutdown.
6. Проверить работу VTP Pruning на всех коммутаторах командой sh int pruning, sh int trunk.
7. Настроить интерфейс eth0/0 на SW1 в режиме транк.
8. Проверить работу VTP Pruning командой sh int pruning, sh int trunk.
9. Разрешить на интерфейсе eth0/0 работу только следующих VLAN’ов: 10, 20, 30, 40 командой switchport trunk allowed vlan 10, 20, 30, 40.
10. Проверить работу VTP Pruning командой sh int pruning.
11. В VTP домене назначить пароль CCIEinaYEAR. Командой sh vtp status проверить идентичность номера ревизии и md5 hash на всех коммутаторах.

### Задание #3 для лабораторной:

Подготовка лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfSHFiU3lHNDhBRlk) на SW1, SW2, SW3, SW4.

Конфигурация:

1. На SW1, SW2, SW3, SW4 настроить домен CCIEinaYEAR и настроить VTP так, чтобы он имел возможность обрабатывать PVLAN.
2. Проверить командой sh vtp status на SW1, SW2, SW3, SW4, что они синхронизированы и имеют одинаковый номер ревизии.
3. Перевести SW1 в режим в котором он может создавать, удалять и изменять VLAN DB, и при этом является основным источником информации о VLAN в сегменте сети.
4. Проверить статусы и роли коммутаторов SW1,SW2,SW3,SW4 в VTP процессе, по выводам команды sh vtp status.

Внимание для ОГ: по всем заданиям в конце файла конфигурации каждого коммутатора добавьте вывод команды sh vtp status.

Мы перезалили конфигурационные файлы для 2-го задания. Спасибо Larchen за комментарий.

## **[Лабораторная работа по Теме 8: PPP Multilink, PPPoE](http://ccie.linkmeup.ru/2016/04/20/laboratornaya-rabota-po-teme-8-ppp-multilink-pppoe/)**

### Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfTXBaUnNIcDYyNk0) для SW1, SW4, R6, R7

2. Включить физический интерфейс E0/1 на маршрутизаторах R6 и R7.

3. На маршрутизаторе R7 задать команду int virtual-template1 и командой sh int virtual-template1 проверить свойства созданного интерфейса и задать ip адрес 188.1.67.2/24

4. Командой bba-group pppoe R6 определить BBA группу на сервере и привязать int virtual-template1 к группе.

5. Зайти на интерфейс E0/1.67 маршрутизатора R7 и настроить команду pppoe enable group R6.

6. На маршрутизаторе R6 командой int dial 1 создаем заданный интерфейс, настраиваем инкапсуляцию ppp, задаем ip 188.1.67.1/24, и задаем пул командой dialer pool 6

7. Зайти на интерфейс E0/1.67 маршрутизатора R6 и привязать созданный пул к интерфейсу командой pppoe-client dial-pool-number 6

8. С маршрутизатора R6 отправить пинг на ip 188.1.67.2

### Задание #2 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfbHFIaVYtQkFZTlk) R9, R10

2. Создать мультилинк интерфейс на R9 под номером 91 и ip 188.1.91.1/30 и соотнести его с группой 91. Применить мультилинк на физических интерфейсах согласно топологии.

3. Создать мультилинк интерфейс на R10 под номером 91 и ip 188.1.91.2/30 и соотнести его с группой 91. Применить мультилинк на физических интерфейсах согласно топологии.

4. Поменять ip на R10 на ip 1.2.3.4/24 и отправить пинг на R9.

5. Настроить одностороннюю аутентификацию CHAP от R9 к R10(команда ppp authentication сhap на маршрутизаторе R9) используя hostname Server. Задать пароль по умолчанию CCIEinaYEAR? на интерфейсе мультилинка для ответа на любой запрос на маршрутизаторе R10.

## **[Лабораторная работа по Теме 9: Static routing](http://ccie.linkmeup.ru/2016/04/22/laboratornaya-rabota-po-teme-9-static-routing/)**

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfVmhGSFBxLU1LWm8) для SW1,SW2, SW3, SW4, R2, R3, R4, R5.

2. На интерфейсе E0/1.235 R2 задать ip 188.1.235.2/24, на интерфейсе E0/1.235 R3 задать ip 188.1.235.3/24, на интерфейсе E0/1.235 R5 задать ip 188.1.235.5/24, на интерфейсе E0/1.34 R3 задать ip 188.1.34.3/24, на интерфейсе E0/1.34 R4 задать ip 188.1.34.4/24.

3. Включить физические интерфейсы E0/1 на этих маршрутизаторах.

4. Проверить соединение между маршрутизаторами, отправив пинг на ip адреса настроенных интерфейсов.

5. Настроить на R3 статический маршрут к loopback интерфейсу R5, используя nexthop адрес R5 188.1.235.5/24

6. Настроить на R3 статический маршрут к loopback интерфейсу R2, используя исходящий интерфейс E0/1.235

7. Проверить командой sh ip route настройки маршрутов на R3

8. Отправить пинг с R3 на ip адреса loopback интерфейсов R2 и R5

9. Настроить маршрут по умолчанию на R2, используя исходящий интерфейс E0/1.235

10. Настроить маршрут по умолчанию на R5, используя исходящий интерфейс E0/1.235 и nexthop адрес R3 188.1.235.3/24

11. Отправить пинг с R2 на ip адрес loopback интерфейса R5

## **[Лабораторная работа по Теме 10: Compression, Fragmentation](http://ccie.linkmeup.ru/2016/04/25/laboratornaya-rabota-po-teme-10-compression-fragmentation/)**

Друзья, в честь долгожданной премьеры сериала «Игра престолов», мы решили не загружать вас лабораторной работой.

Это конечно же шутка, но в ней есть доля правды. Сегодняшняя наша тема сугубо теоретическая и мы не придумали ничего лучше как дать вам ответить на пару вопросов о проекте. Это небольшой соцопрос. Пожалуйста, уделите немного своего времени для [ответов на вопросы](http://goo.gl/forms/tgkDQlzRd8). Спасибо

## **[Лабораторная работа по Теме 11: HTTP, TFTP, FTP](http://ccie.linkmeup.ru/2016/04/27/laboratornaya-rabota-po-teme-11-http-tftp-ftp/)**

### Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfT1FnQjl4UmRnTVU) для R1, R2.

2. Настроить R2 таким образом, чтобы можно было скачать файл конфигурации с NVRAM R1 с помощью HTTP.

3. R2 должен пройти проверку подлинности с помощью пары имени пользователя / пароля CCIEadmin / CCIEinaYEAR?, сконфигурированных на R1.

4. R1 должен разрешить входящие HTTP-соединения только на порт 8080 из подсети 180.1.0.0/16. Настроить access-list 80, для ограничения доступа.

5. На R1 ограничить максимальное количество одновременных подключений к HTTP-серверу до двух.

6. При необходимости настроить нужные интерфейсы.

7. R2 должен разрешить входящие защищенные соединения HTTP на порт 4043, но ограничить функции безопасности, использовать только DES шифрование.

### Задание #2 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfLWdka3ZuN0Z5ZVU) для R1, R2.

2. Настроить R2 в роли FTP клиента, чтобы он инициировал сессию с помощью пары имени пользователя / пароля CCIEadmin / CCIEinaYEAR?, сконфигурированных на R1. А также, чтобы он использовал только пассивный режим соединений FTP.

3. Использовать в роли source interface loopback адрес R2 (настроить Loopback0 согласно топологии).

### Задание #3 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfYzE3WHRhWGY0aEU) для R1, R2.

2. Настроить R2 в роли TFTP клиента. Использовать в роли source interface loopback адрес R2 (настроить Loopback0 согласно топологии).

3. Настроить R1 в роли TFTP сервера таким образом, чтобы файл с названием ccieinayear.log мог быть выгружен из nvram, используя название aliasccie.

4. R1 должен разрешить входящее соединение по TFTP только с IP-адреса интерфейса loopback R2 (настроить Loopback0 согласно топологии). Настроить access-list 20, для ограничения доступа.

## [Лабораторная работа по Теме 12: ACL (VACL, Port ACL)](http://ccie.linkmeup.ru/2016/04/29/laboratornaya-rabota-po-teme-12-acl-vacl-port-acl/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfNGIzVmQtVXUyR28) на R1, R2, SW1

2. На интерфейсе E0/1 R1 задать ip адрес 188.1.12.1/24, на интерфейсе E0/1 R2 задать ip адрес 188.1.12.3/24 (IP указан не по топологии, так как он нужен для проверки задания)

3. Командой spanning-tree portfast задать все интерфейсы SW1 в режим portfast.

4. На R2 настроить подключение по Telnet, с аутентификацией по паролю CCIEinaYEAR?. С R1 попробовать подключиться к R2 по Telnet.

5. На SW1 создать расширенный ACL под именем BLK и

Запретить:

a) Использование Telnet сессий в направлении от R1 к R2, для таких нечетных IP адресов (отправителей) из сети 188.1.12.0/24: 1..3..5..7..9..11..13..15.

b) Обмен маршрутами по протоколу EIGRP между R1 и R2.

c) Разрешить весь остальной трафик (проверить настройки командой sh access-lists BLK).

6. Применить этот ACL на интерфейсе E0/0.

7. Подключиться с R1 на R2 по Telnet. Отправить пинг от R1 к R2 и обратно.

# [**Первая большая лабораторная работа**](http://ccie.linkmeup.ru/2016/05/02/pervaya-bolshaya-laboratornaya-rabota/)

Изменения топологии:

* Диагональные линки e3/2, e3/3 между коммутаторами выключены.
* DMVPN underlay линки (e0/1.144) выключены.
* Линки между R8, R9 и R10 (VLAN89, VLAN108, сериал линки s1/0-s1/1) выключены.
* На R6, R9 и R10 добавлен интерфейс в VLAN200.

[ССЫЛКА НА ТОПОЛОГИЮ](https://drive.google.com/file/d/0ByVf6yfX4EBfNDRkNFdBMHMxeFU/view)

Скачать [файлы для импорта лабораторной работы в UNL](https://drive.google.com/open?id=0ByVf6yfX4EBfeHNZTDBVSjBZOVk). Вам нужно будет импортировать zip файл в свою виртуальную машину.

Или [загрузить начальную конфигурацию](https://drive.google.com/file/d/0B3uwAH0p4u2NUUIyc3dCQ3l1ekk/view?usp=sharing).

Всё, что относится к лабораторной на [Google Disk](https://drive.google.com/folderview?id=0B3uwAH0p4u2NR2ppOEh4MWFwbFU&usp=sharing).

Советы:

* При выполнении заданий если вы заметили необычный конфиг, запишите его себе — вполне возможно, что это поможет вам решить последующие задания.
* Не забывайте включать обратно интерфейсы, если вы их выключали для теста.
* Проверки, указанные после задания, не гарантируют, что вы выполнили задание на 100% правильно.
* Будьте внимательны! Из-за неправильно выполненного подзадания вы можете получить 0 баллов за всё задание.

Правила (UPD: 05.04.2016):

* Нельзя добавлять дополнительные интерфейсы/IP адреса, если в задании это явно не упомянуто.
* Нельзя использовать PBR.
* Нельзя использовать динамическую маршрутизацию.
* Нельзя использовать Multilink и сериал интерфейсы на R9, R10.
* Нельзя использовать менеджмент Vlan 1 (10.0.0.0/24).
* Лабораторная работа включает в себя смешанные задания по configuration и troubleshooting.
* Большинство устройств преднастроено (но не всегда верно).
* При решении заданий проверяйте есть ли уже конфигурация, которую можно использовать.
* Не рекомендуется удалять любой существующий конфиг — удаляйте только в случае, если других решений нет.
* В своих решения вы должны быть как можно более специфичны:

Пример с access-list:

ip access-list extended TEST

5 deny ip 10.0.0.0 0.255.255.255 any

10 permit ip any any

interface e0/0

ip access-group TEST in

Проблема: Специфичный HTTP траффик (src IP: 10.10.10.10, dst IP: 2.2.2.2, port 80) дропается, когда приходит на e0/0.

Неправильные решения:

1.

**inteface e0/0**

**no ip access-group TEST in**

2.

**ip access-list extended TEST**

**no 5**

Нейтральное решение (правильность оценивается на усмотрение эксперта):

**ip access-list extended TEST**

**4 permit ip 10.0.0.0 0.255.255.255 any**

Правильное решение:

**ip access-list extended TEST**

**4 permit tcp host 10.10.10.10 host 2.2.2.2 eq 80**

Удачи! Она вам пригодится!

### **Задание лабораторной**

##### **1. (2 баллов)**

На всех коммутаторах VTP должен быть полностью выключен.

##### **2. (4 баллов)**

R2 должен пинговать IP адрес R1 Loopback0 (180.1.1.1) и путь до него должен проходить через s1/0.

Если интерфейс s1/0 в состоянии down, то пинг должен идти через e0/1.12

Нельзя изменять существующие и добавлять новые статические маршруты, использование PBR также запрещено.

Проверка:

**R2#ping 180.1.1.1**

**Type escape sequence to abort.**

**Sending 5, 100-byte ICMP Echos to 180.1.1.1, timeout is 2 seconds:**

**!!!!!**

**Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/9 ms**

**R2#show ip cef | i 180.1.1.1**

**180.1.1.1/32 attached Serial1/0**

**R2#conf t**

**R2(config)#int s1/0**

**R2(config-if)#shut**

**R2(config-if)#end**

**R2#ping 180.1.1.1**

**Type escape sequence to abort.**

**Sending 5, 100-byte ICMP Echos to 180.1.1.1, timeout is 2 seconds:**

**!!!!!**

**Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms**

**R2#show ip cef | i 180.1.1.1**

**180.1.1.1/32 188.1.12.1 Ethernet0/1.12**

##### **3. (8 баллов)**

Настройте SSH доступ на R4 согласно следующим требованиям:

1) Доменное имя: linkmeup.ru

2) Размер RSA ключа должен быть 2048 бит

3) Из протоколов удаленного доступа только SSH должен быть разрешён

4) Использовать локальную базу пользователей для аутентификации (пользователь cisco/cisco преднастроен)

5) SSH тайм-аут до успешной аутентификации должен быть в два раза меньше значения по умолчанию.

6) Версия SSH: 2

7) После двух неудачных попыток логина в течение 60 секунд, маршрутизатор должен запрещать последующие

попытки входа на vty на 30 секунд.

В результате R6 должен успешно подключиться к R4 Loopback0 по SSH.

Проверка:

**R6#ssh -l cisco 180.1.4.4**

**Password: cisco**

**R4>**

##### **4. (6 баллов)**

Настройте Telnet доступ на R8 согласно следующим требованиям:

1) При подключении устройство не должно запрашивать пароль

2) Пользователь должен сразу попадать в privileged-level EXEC

3) Из протоколов удаленного доступа только Telnet должен быть разрешён

4) Устройство также должно слушать на 3008 порту для входящих telnet сессий.

5) При вводе неправильной команды устройство не должно пробовать подключаться через telnet,

пытаясь разрешить DNS имя неправильной команды. При этом устройство всё равно может разрешать DNS имена (например, если используется ping). Этот подпункт должен быть выполнен для консоли и виртуальных линий (vty).

После настройки убедитесь, что можно подключиться по Telnet с R7 на R8 Loopback0

Проверка:

**R7#telnet 180.1.8.8 3008**

**Trying 180.1.8.8, 3008 ... Open**

**R8# q**

**[Connection to 180.1.8.8 closed by foreign host]**

**R7#telnet 180.1.8.8**

**Trying 180.1.8.8 ... Open**

**R8#**

**R8#wrong**

**^**

**% Invalid input detected at '^' marker**

**R8#ping linkmeup.ru repeat 1**

**Translating "linkmeup.ru"...domain server (255.255.255.255)**

**Translating "linkmeup.ru"...domain server (255.255.255.255)**

**^**

**% Invalid input detected at '^' marker.**

##### **5. (8 баллов)**

R5 должен подключаться к R1 Loopback0 по Telnet.

Для этого задания изменения на R1 запрещены.

Заметка: пароль cisco.

Проверка:

**R5#telnet 180.1.1.1**

**Trying 180.1.1.1 ... Open**

**User Access Verification**

**Password: cisco**

**R1>**

##### **6. (8 баллов)**

Между R6 и R7 должна быть поднята PPPoE сессия. R6 — сервер, R7 — клиент.

Настройте клиент согласно следующим требованиям:

1) Номер интерфейса должен быть 1.

2) Номер dialer pool должен равняться количеству возможных режимов в VTPv2

3) R7 должен получить IP адрес от R6 из подсети 188.1.76.0/24

\* Заметка: это не означает, что маска должна быть /24.

4) Сервер должен аутентифицировать клиента (но не наоборот) с помощью CHAP, пароль — «CCIE» (без кавычек)

5) R7 должен установить дефолтный маршрут, указывающий на PPPoE сервер.

\* Заметка: для этого подзадания нельзя использовать команду «ip route»

Подсказка: key chain может помочь.

Проверка подзадания 5:

**R7#show ip cef 0.0.0.0/0**

**0.0.0.0/0**

**nexthop 188.1.76.6 Dialer1**

##### **7. (6 баллов)**

R9 должен пинговать R10 IP адрес интерфейса e0/1.200.

Изменения на всех свитчах запрещены.

Использование статических маршрутов/PBR запрещено.

Проверка:

**R9#ping 188.1.200.10**

**Type escape sequence to abort.**

**Sending 5, 100-byte ICMP Echos to 188.1.200.10, timeout is 2 seconds:**

**!!!!!**

**Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms**

##### **8. (6 баллов)**

На R3 настройте плавающий статический дефолтный маршрут:

— Основной маршрут должен идти через R4 (188.1.34.4).

— Запасной маршрут должен идти через R5 (188.1.235.5) и вступать в силу только, если line protocol интерфейса e0/1.34 на R3 в down.

\* Заметка: для этого задания нельзя использовать track

Для теста используйте R6 Loopback0 (180.1.6.6)

Проверка:

**R3#trace 180.1.6.6 so lo0 nu**

**Type escape sequence to abort.**

**Tracing the route to 180.1.6.6**

**VRF info: (vrf in name/id, vrf out name/id)**

**1 188.1.34.4 2 msec 1 msec 2 msec**

**2 188.1.45.6 2 msec 2 msec 2 msec**

**R3#conf t**

**R3(config)#int e0/1.34**

**R3(config-subif)#shut**

**R3(config-subif)#end**

**R3#trace 180.1.6.6 so lo0 nu**

**Type escape sequence to abort.**

**Tracing the route to 180.1.6.6**

**VRF info: (vrf in name/id, vrf out name/id)**

**1 188.1.235.5 2 msec 0 msec 0 msec**

**2 188.1.45.6 2 msec 1 msec 1 msec**

##### **9. (12 баллов)**

Все роутеры должны пинговать Loopback0 друг друга, если source IP — Loopback0.

### **Проверка лабораторной**

В большой лабораторной проверяется не только разница с ответом в конфигурации.

Кроме того, ваши конфиги будут загружены экспертом на оборудование и проверка будет выполняться командами show/ping и тд.

Поэтому то, что показано в проверке к заданиям лабы (вывод команд show/ping/…), должно у Вас выглядеть точно так же.

Обязательно, после каждого задания, выполняйте проверочные команды, которые указаны в лабораторной.

Вам не нужно выкладывать вывод команд show в ответе. Для больших лаб, мы это проверяем сами. Нужно выложить только конфигурацию.

# [**Цикл 3.**](http://ccie.linkmeup.ru/2016/05/07/tsikl-3-tema-13-etherchannel/)

## [Лабораторная работа по Теме 13: EtherChannel](http://ccie.linkmeup.ru/2016/05/09/laboratornaya-rabota-po-teme-13-etherchannel/)

### Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfai16bWxrcng5Z1U) на SW1, SW2, SW3, SW4

2. Настроить интерфейсы между SW1 и SW2 L2 Etherchannel при этом:

· Перевести интерфейсы между SW1 и SW2 в режим работы access к vlan 21;

· Не использовать какие либо протоколы автосогласования;

· Использовать для номера агрегированного канала, номер vlan на интерфейсах между устройствами.

3. Проверить настройки EtherChannel на SW1 и SW2

4. Настроить интерфейсы между SW1 и SW3 L2 Etherchannel при этом:

· Перевести интерфейсы между SW1 и SW3 в режим работы access к vlan 31;

· Использовать проприетарный протокол Cisco;

· Только SW1 должен активно инициировать автосогласование параметров канала;

· Использовать для номера агрегированного канала, номер vlan на интерфейсах между устройствами.

5. Проверить настройки EtherChannel на SW1 и SW3

6. Настроить интерфейсы между SW1 и SW4 L2 Etherchannel при этом:

· Перевести интерфейсы между SW1 и SW4 в режим работы access к vlan 41

· В итоге вывод show etherchannel summary должен выглядеть для линка SW1 к SW4 следующим образом:

SW1#sh etherchannel summary

<——output ommited——>

Number of channel-groups in use: 3

Number of aggregators: 3

Group Port-channel Protocol Ports

——+————-+————+————————————————

21 <—-output ommited—->

31 <—-output ommited—->

41 Po41(SU) LACP Et3/2(P) Et3/3(P)

· Только SW1 должен активно инициировать автосогласование параметров канала;

· Использовать для номера агрегированного канала, номер vlan на интерфейсах между устройствами.

7. Проверить настройки EtherChannel на SW1 и SW4

8. Переведите все неиспользуемые порты на всех четырех коммутаторах в состояние shutdown и настройте в режиме работы access в vlan 998

Проверка: sh run

### Задание #2 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfSXVoWUVfZi16VWs) на SW1, SW2, SW3, SW4

2. На SW1 создать vlan 200 c ip 10.10.20.10/24, vlan 300 c ip 10.10.30.10/24, vlan 400 c ip 10.10.40.10/24

3. На SW2 создать vlan 200 c ip 10.10.20.20/24.

4. На SW3 создать vlan 300 c ip 10.10.30.30/24,

5. На SW4 создать vlan 400 c ip 10.10.40.40/24

6. Настроить агрегированный транковый интерфейс от коммутатора SW1 до коммутаторов SW2, SW3, SW4 с общим bandwidth до 20 Mb/s.

При этом:

· Между коммутаторами SW1 и SW2 не использовать протоколы автосогласования;

· Между коммутаторами SW1 и SW3 использовать протокол автосогласования проприетарный протокол Cisco;

· Между коммутаторами SW1 и SW4 использовать протокол автосогласования IEEE 802.3ad;

· Только SW1 выступает в качестве активного инициатора процесса автосогласования;

· Не использовать в качестве транкового протокола проприетарный протокол Cisco и режим автосогласования транка;

· Разрешить на агрегированных транковых интерфейсах от SW1 до SW2,SW3,SW4 только те VLAN, для которых были созданы SVI интерфейсы на каждом из коммутаторов;

· В качестве номера агрегированного канала использовать номера: 21, 31, 41

по аналогии с предыдущим заданием.

7. Проверить настройки EtherChannel на всех коммутаторах.

8. Отправить пинг на 255.255.255.255 с SW1 для проверки доступности всех SVI на коммутаторах.

9. Настроить коммутаторы таким образом, чтобы приходящий на коммутатор IP пакет, с одним и тем же Source IP, но различными Destination IP распределялся по портам входящим в Etherchannel группу, однако при этом IP пакеты, с различными Source IP и одинаковым Destination IP отправлялись по одному и тому же интерфейсу.

10. Переведите все неиспользуемые порты на всех четырех коммутаторах в состояние shutdown и настройте в режиме работы access в vlan 998

## [Лабораторная работа по Теме 14: CAM, CDP, LLDP, UDLD](http://ccie.linkmeup.ru/2016/05/11/laboratornaya-rabota-po-teme-14-cam-cdp-lldp-udld/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfX2I5SGJvN2NxV1E) на SW1, R1, R2, R9, R10

2. Проверить cdp neighbors на SW1, SW2, R1, R2, R9, R10

3. Проставить cdp timer 10 сек и holdtime 30 на всех устройствах.

4. R9 и R10 должны указывать IP-адрес Loopback0 как Entry address в сообщениях CDP.

5. Проверка: sh run

## [Лабораторная работа по Теме 15: Routing Protocol features](http://ccie.linkmeup.ru/2016/05/13/laboratornaya-rabota-po-teme-15-routing-protocol-features/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfRUw5MGdBalFkSXM) на SW1, SW2, SW3, SW4, R1, R2, R3, R4, R5, R6, R7, R8, R9, R10

\* DMVPN туннели и подинтерфейсы Underlay сети, не участвуют в лабораторной работе.

2. На всех маршрутизаторах настроить протокол динамической маршрутизации RIPv2 с анонсированием сетей 188.1.0.0 и 180.1.0.0

3. Отключить автоматическое суммирование маршрутов на всех маршрутизаторах.

4. Настроить на сегменте сети между маршрутизаторами R6-R4-R5 RIPv2 аутентификацию.

Используйте режим MD5 и ключ 1 с паролем CCIEinaYEAR

5. Сконфигурировать на сегменте сети между R9 и R10 для VLAN 109 параметры отправки и приема апдейтов только для протокола RIP версии 2.

6. На сегменте сети между маршрутизаторами R4 и R3 настроить RIPv2 аутентификацию.

Используйте режим clear text и ключ 1 с паролем CCIEtoBE

7. Для сегмента сети между R6 и R7 VLAN 67, не использовать мультикаст и броадкаст для RIP сообщений.

8. Отключить автоматическую отправку RIP сообщений на всех маршрутизаторах для интерфейсов не подключенных к другим устройствам или являющихся тупиковыми сетями (подинтерфейсы и лупбек интерфейсы).

Не использовать правило default.

9. Проверить с R1 доступность всех лупбек адресов всех маршрутизаторов с использованием протокола icmp.

10. Если есть проблема с соединением решить ее

## [Лабораторная работа по Теме 16: QoS 6.7-6.10](http://ccie.linkmeup.ru/2016/05/16/laboratornaya-rabota-po-teme-16-qos-6-7-6-10/)

### Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxZHpJcWVYaDVuYnM) на SW1, SW2, SW3, R3, R2, R5

2. На R2 создать пользователя CCIEadmin с паролем CCIEinaYEAR. Разрешить подключение по телнет.

3. На всех маршрутизаторах настроить протокол маршрутизации RIP версии 2 с анонсированием сети 188.1.0.0. Убрать автосуммирование маршрутов.

4. На маршрутизаторе R3 создать class-map TELNET, Policy map R2 и классифицировать трафик по протоколу телнет, идущий через исходящий интерфейс к R2.

5. Проверить настройки

### Задание #2 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxWTRhSG4tbGU4QTA) R1, R2.

2. На маршрутизаторе R1 настроить политику передачи трафика, используя для настройки подход HQF. Политику назвать HQF. Создать отдельные class-map для протоколов Telnet, HTTP, SMTP.

3. Для Telnet установить полосу пропускания в 10%, для SMTP 20%, для HTTP 30%

4. Определить для HTTP трафика правило выстраивание очереди по каждому потоку (flow) отдельно.

5. Проверить настройки

### Задание #3 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxdk1oeWlqSmZjZFU) R1, R2.

2. На маршрутизаторе R1 настроить политику передачи трафика по технологии LLQ по умолчанию и названием LLQ. Создать отдельные class-map для протоколов Telnet, HTTP, SMTP и RTP с соответствующими названиями TELNET, HTTP, SMTP, VOIP.

3. RTP должен быть самым приоритетным трафиком. Для Telnet установить полосу пропускания в 10%, для SMTP 20%, для HTTP 30% оставшейся полосы пропускания.

4. На стороне R2 полоса пропускания принимает трафик только на скорости 25мб/с. На R1 настроить полосу пропускания в соответствии со скоростью приема трафика на R2, чтобы распределение полосы в политике LLQ, делалось на основе этого значения.

Проверить настройки

## [Лабораторная работа по теме 17: Device Management 8.1.8 (SNMP)](http://ccie.linkmeup.ru/2016/05/18/laboratornaya-rabota-po-teme-17-device-management-8-1-8-snmp/)

### Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B3uwAH0p4u2NQ1VOZG81VlZhVjg)
2. На R1,R2,R3,R4,R5,R6 создать view SNMP сервера версии 3 под названием ALLINT и разрешить доступ для всех объектов интерфейса (к соответствующему поддереву MIB).
3. На R1,R2,R3,R4,R5,R6 создать группу под названием CCIEinaYEAR с использованием SNMP версии 3 и дать разрешение на чтение и запись для view ALLINT.
4. На R1,R2,R3,R4,R5,R6 создать пользователя под названием CCIEadmin, привязать его к группе CCIEinaYEAR c доступом на чтение и запись по протоколу SNMP, только в случае если пользователь пройдет SNMP аутентификацию:
   * Использовать аутентифкацию sha с паролем CCIEinaYEAR? , параметрами шифрования 3des и паролем шифрования CCIEinaYEAR?
   * Разрешить доступ для пользователя CCIEadmin только с адреса 180.1.3.3 используя ACL с номером 90
5. В конце конфигурации каждого устройства, добавить вывод команды sh snmp user

### Задание #2 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B3uwAH0p4u2NZWd3Tk5oS1REbEU)
2. На R1 настроить SNMPv2c с такими ограничениями:
   * Для community OPEN разрешить доступ на чтение к поддереву iso, но, при этом, запретить доступ к поддеревьям: к поддереву, которое начинается на ospf и поддереву, которое начинается на ip.
   * Объект, в котором описываются поддеревья MIB, должен называться RO\_OPEN.
   * Для community ADMIN разрешить доступ на чтение и запись, но только для IP 180.100.3.3. Использовать для этого ACL 20
3. На R2 настроить SNMPv2c с такими ограничениями:
   * Для community OPEN разрешить доступ на чтение только к поддереву ifEntry. Объект, в котором описывается поддерево MIB, должен называться R2\_INT.
   * Индексы интерфейсов не должны меняться после перезагрузки
4. На R3 настроить SNMPv2c с такими ограничениями:
   * Для community ADMIN разрешить доступ на чтение и запись
   * Включить отправку сообщений trap на IP 180.1.4.4 (Loopback R4) используя версию 2c и community ADMIN
   * Trap должны отправляться, если интерфейс упал или поднялся; если сосед OSPF упал или поднялся.
   * Для проверки, включить на R3 debug snmp packets и сделать clear ip ospf process. Аналогично можно проверить генерацию trap, если меняется статус интерфейсов. В выводе debug вы должны увидеть сформированные сообщения trap, которые идут на R4

## [Лабораторная работа по теме 18: Layer 2 Security 7.1](http://ccie.linkmeup.ru/2016/05/20/laboratornaya-rabota-po-teme-18-layer-2-security-7-1/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxUl8xWlo2a3VJdHM) SW1, SW2, SW3, SW4, R3, R4, R5.

2. Отправить пинг c R3, R4, R5, соответственно, на IP-адреса VLAN’ов 30, 40, 20 на SW1 и убедиться, что они проходят.

3. На SW1 на портах, подключенных к SW2:

* разрешить 5 мак-адресов для vlan 20.
* При обнаружении нарушения на этих портах, коммутатор должен сгенерировать сообщение о нарушении, увеличить счетчик нарушений и перевести порт в состояние err-disable.
* Все MAC-адреса, которые разрешены по настройкам порта, должны автоматически записываться в текущую конфигурацию.

4. На портах, подключенных к SW3:

* разрешить 10 мак-адресов для vlan 30.
* При обнаружении нарушения на этих портах, коммутатор должен сгенерировать сообщение о нарушении и увеличить счетчик нарушений.
* Порт не должен переходить в err-disable.
* Все MAC-адреса, которые разрешены по настройкам порта, должны автоматически записываться в текущую конфигурацию.

5. На портах, подключенных к SW4:

* разрешить 15 мак-адресов для vlan 40.
* При обнаружении нарушения на этих портах, коммутатор должен тихо блокировать трафик от MAC-адресов, которые нарушают настройки.
* Не должно генерироваться сообщение о нарушении и не должен увеличиваться счетчик нарушений.
* Все MAC-адреса, которые разрешены по настройкам порта, должны автоматически записываться в текущую конфигурацию.

6. На SW1 настроить механизм автоматического восстановления портов из состояния err-disable, если порты попали в это состояние из-за port-security. Порты должны возвращаться в нормальное состояние через 2 минуты.

7. Отправить пинг c R3, R4, R5 на соответствующие вланы на SW1.

8. На SW3 порт Eth 0/1 планируется использовать для гостевого доступа. Настройте порт:

* в режиме access в 30 VLAN,
* и разрешите доступ для одной рабочей станций,
* с учетом, что в случае, если первая подключившаяся рабочая станция неактивна в течение 3х минут, доступ в сеть через этот порт может быть предоставлен другой рабочей станции.
* При обнаружении нарушения на этом порту, коммутатор должен сгенерировать сообщение о нарушении и увеличить счетчик нарушений.
* Порт не должен переходить в err-disable. Оставить порт в состоянии shutdown.

9. На SW4 порт Eth1/2 настроить в режиме access в 40 VLAN, и разрешить доступ для 5 MAC-адресов. При этом:

* коммутатор должен автоматически удалять все изученные для этого порта MAC-адреса через 3 часа.
* При обнаружении нарушения на этих портах, коммутатор должен тихо блокировать трафик от MAC-адресов, которые нарушают настройки.
* Не должно генерироваться сообщение о нарушении и не должен увеличиваться счетчик нарушений.
* Оставить порт в состоянии shutdown.

10. Проверить настройки

# [**Цикл 4.**](http://ccie.linkmeup.ru/2016/05/21/tsikl-4-tema-19-pvst-1-4/)

## [Лабораторная работа по теме 19: PVST+ 1.4](http://ccie.linkmeup.ru/2016/05/23/laboratornaya-rabota-po-teme-19-pvst-1-4/)

Прописать все необходимые вланы. Cost прописать на любом коммутаторе с условием, чтобы все соответствовало заданию.

Вся приоритетность на коммутаторах меняется с учетом 4 битов приоритетности коммутатора по умолчанию.

### Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxaTZDN3FIRk9kWnc) SW1, SW2, SW3, SW4.

2. Настроить etherchannel между всеми свичами по протоколу LACP. Между SW1 и SW2 создать под номером 12, между SW1 и SW3 создать под номером 13, между SW1 и SW4 создать под номером 14. Между SW2 и SW3 создать под номером 23, между SW2 и SW4 создать под номером 24. между SW3 и SW4 создать под номером 34.

3. Настроить SW4 таким образом, чтобы он стал Root Bridge для vlan 40, не меняя приоритетности.

4. Настроить SW2 таким образом, чтобы он стал Root Bridge для vlan 20, не применяя команды root primary и изменив приоритетность на 2 шага инкрементирования по сравнению с значением приоритета по умолчанию.

5. Настроить SW3 таким образом, чтобы он стал Root Bridge для vlan 30, не применяя команды root primary и изменив приоритетность на 3 шага инкрементирования по сравнению с значением приоритета по умолчанию.

6. Настроить SW1 таким образом, чтобы он стал Root Bridge для vlan 10, не применяя команды root primary и изменив приоритетность на 4 шага инкрементирования по сравнению с значением приоритета по умолчанию.

7. Проверить настройки

### Задание #2 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxNkJkNTBVQVNhX2s) SW1, SW2, SW3, SW4.

2. Настроить etherchannel между всеми свичами по протоколу LACP. Между SW1 и SW2 создать под номером 12, между SW1 и SW3 создать под номером 13, между SW1 и SW4 создать под номером 14. Между SW2 и SW3 создать под номером 23, между SW2 и SW4 создать под номером 24. между SW3 и SW4 создать под номером 34.

2. Назначить SW4 root bridge для VLAN40 не меняя приоритетности. Переделать путь, таким образом, чтобы трафик с vlan40 на SW1 до vlan40 на SW4 гарантированно проходил через SW2 следующим образом SW1-SW2-SW4, используя cost.

3. Назначить SW3 root bridge для VLAN30, не применяя команды root primary и изменив приоритетность на 3 шага инкрементирования по сравнению с значением приоритета по умолчанию. Переделать путь, таким образом, чтобы трафик с vlan30 на SW2 до vlan30 на SW3 гарантированно проходил через SW4 следующим образом SW2-SW4-SW3, используя cost.

4. Назначить SW2 root bridge для VLAN20, не применяя команды root primary и изменив приоритетность на 2 шага инкрементирования по сравнению с значением приоритета по умолчанию. Переделать путь, таким образом, чтобы трафик с vlan20 на SW3 до vlan20 на SW2 гарантированно проходил через SW1 следующим образом SW3-SW1-SW2, используя cost.

5. Назначить SW1 root bridge для VLAN10, не меняя приоритетности. Переделать путь, таким образом, чтобы трафик с vlan10 на SW4 до vlan10 на SW1 гарантированно проходил через SW3 следующим образом SW4-SW3-SW1, используя cost.

6. Проверить настройки

## [Лабораторная работа по теме 20: SPAN, RSPAN](http://ccie.linkmeup.ru/2016/05/25/laboratornaya-rabota-po-teme-20-span-rspan/)

Ребята, карты легли таким образом, что лабораторной работы по данной теме сегодня не будет. А пока вы можете послушать подкаст: «[Как положить сеть так, чтобы потом не было больно»](http://linkmeup.ru/blog/240.html).

## [Лабораторная работа по теме 21: RIPv2 3.4](http://ccie.linkmeup.ru/2016/05/27/laboratornaya-rabota-po-teme-21-ripv2-3-4/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B3uwAH0p4u2Nek16RFZpRncwQWM) SW1, SW2, SW3, SW4, R1, R2, R3, R4, R5, R6, R7, R8, R9, R10

2. Настроить на всех маршрутизаторах протокол ripv2 для сетей 180.1.0.0 и 188.1.0.0 и отключить автоматическую суммаризацию сетей.

3. Проверить, что все сети на маршрутизаторах анонсированы и решить проблему в случае, если нет каких-то маршрутов

4. Маршрутизаторы R3 и R5 настроить таким образом, чтобы они не отправляли RIP сообщения для сегмента сети на интерфейсе E0/1.235, но при этом сохранили возможность получать RIP сообщения от маршрутизатора R2 по этому интерфейсу.

5. Сформируйте отправляемые от R8 к R7 маршруты так, чтобы они содержали минимальное количество информации для доступа к следующим подсетям: 188.1.89.0\24 188.1.109.0\24 188.1.9.0\24 188.1.10.0\24 180.1.10.10\32 180.1.9.9\32 180.1.8.8\32. При этом не должны быть затронуты IP адреса остальных loop-бэков.

6. Настроить сегменте сети между маршрутизаторами R6-R7 RIP аутентификацию MD5 c паролем ##CC1E2B3## . Для названия ключниц использовать имя локального маршрутизатора, для идентификатора ключа использовать единицу (1).

7. На маршрутизаторе R4 рассылать RIP сообщения только по тем сегментам сети, на которых находятся источники RIP сообщений.

8. Для маршрутизаторов, участвующих в организации сегмента сети VLAN 235, принудительно определить используемую версию RIP сообщений как версию 2, на прием и передачу.

9. Настроить на маршрутизаторе R9 отправку маршрутов таким образом, чтобы в случае падения линка Eth 0/1.235 на R5, маршрутизатору R10 не был доступен маршрут до Loopback на R1. Не использовать трекинг SLA, статические маршруты, route-map.

В качестве названий использовать номер локального маршрутизатора.

## [Лабораторная работа по теме 22: MQC WRED, GTC](http://ccie.linkmeup.ru/2016/05/31/laboratornaya-rabota-po-teme-22-mqc-wred-gtc/)

### Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfMGE3RlU2V0VGLUU) R1, R2, R3, SW1, SW2, SW3, SW4.

2. На маршрутизаторе R2 cоздать 2 class-map, для маркировки SMTP и HTTP трафика.

3. Для HTTP трафика:

* ACL с именем HTTP и идентификацией HTTP трафика по 80 порту на источнике.
* Имя class-map HTTP

4. Для SMTP трафика

* ACL с именем SMTP и идентификацией трафика по порту на источнике.
* Имя class-map SMTP

5. Создать отдельную Policy-map с названием MARK и присвоить для SMTP трафика Precedence 3 , для HTTP трафика Precedence 2.

6. Policy-map MARK применить на все Ethernet сабинтерфейсы маршрутизатора R2 на вход.

7. На маршрутизаторе R2 с использованием MQC настроить механизм предотвращений перегрузок WRED и названием WRED. Применить настройки для class-default.

8. Сконфигурировать следующие настройки:

* Использовать для данного класса 75% оставшейся пропускной способности канала.
* Изменить значения минимального и максимального порога срабатывания RED, на основании Precedence, для SMTP трафика, в следующем соотношении : минимальный 30 пакетов, максимальный 60 пакетов, отбрасывание происходит для 1 из 10 пакетов
* Изменить значения минимального и максимального порога срабатывания RED, на основании Precedence, для HTTP трафика, в следующем соотношении : минимальный 33 пакетов, максимальный 55 пакетов, отбрасывание происходит для 1 из 5 пакетов
* Изменить весовой коэффициент (exponential-weighting-constant ) на 1

9. Применить Policy-map с именем WRED на интерфейс маршрутизатора R2 Serial 1/0 на исходящий поток.

### Задание #2 для лабораторной:

Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfMGE3RlU2V0VGLUU).

В задании необходимо настроить:

* политики QoS для трафика в направлении от r1 к r5.
* политики настраиваются на r2, r3, r4 и проверяются с r1, отправляя трафик на r5.
* в обратном направлении, политики настраивать не нужно.
* все политики применяются к физическому интерфейсу Ethernet0/1 (на r2, r3, r4).

Легенда задания:

* Маршрутизатор r2 понимает только стандарт IP Precedence. И находится ближе всего к клиенту (r1), поэтому на нем выполняем классификацию пакетов и маркировку их IP Precedence
* Маршрутизатор r3 понимает оба стандарта, и IP Precedence и DiffServ. Он выполняет перемаркировку из IP Precedence в DiffServ по заданию
* Маршрутизатор r4 понимает только DiffServ. Ожидает от r3 пакеты с маркерами DSCP
* На всех маршрутизаторах, для одного и того же типа трафика, настроена одна и та же политика обслуживания на выход

В качестве проверок, на r1 можно, к примеру, использовать:

1. Для проверки ICMP: ping 180.1.5.5 size 1450
2. Для проверки HTTP: telnet 180.1.5.5 80
3. Для проверки UDP включить заготовленный IP SLA тест с номером 100 (если начинаются какие-то нюансы со связью между устройствами, то лучше тест, после проверки, опять отключить).

Для проверки работы политик используйте команду show policy-map interface e0/1. А так будет легче увидеть где растут счетчики:

**sh policy-map interface e0/1 | i Class-map|packets,**

Ниже описаны политики, которые нужно настроить на маршрутизаторах r2, r3, r4.

На маршрутизаторе R2 создать такую входящую политику, с названием VLAN12 (порядок правил должен соблюдаться):

1. UDP пакеты из VLAN 12, с портами получателя в диапазоне 16384-18000 и размером от 40 до 60 byte:

* для описания пакетов использовать ACL. Назвать ACL: VOIP
* явно указать, что пакеты идут из VLAN 12
* для class-map использовать название VOIP
* пакеты должны быть промаркированы значением IP Precedence 5

2. HTTP трафик из VLAN 12:

* для описания HTTP пакетов использовать существующий расширенный ACL: HTTP (его нельзя менять)
* явно указать, что пакеты идут из VLAN 12
* для class-map использовать название HTTP
* пакеты должны быть промаркированы значением IP Precedence 3

3. ICMP пакеты из VLAN 12, размер которых больше чем 1400 byte:

* для описания ICMP пакетов использовать существующий расширенный ACL: ICMP (его нельзя менять)
* явно указать, что пакеты идут из VLAN 12
* для class-map использовать название ICMP
* пакеты должны быть промаркированы значением IP Precedence 2

4. Остальные пакеты с ненулевым значением IP Precedence, должны быть перемаркированы значением IP Precedence 1

* явно указать, что пакеты идут из VLAN 12 (уточнение в 21:50 МСК 31.05)
* для class-map использовать название NONDEFAULT (уточнение в 21:50 МСК 31.05)
* попробуйте в class-map описать эти «остальные пакеты с ненулевым значением IP Precedence» одной строкой

На маршрутизаторе R2 создать такую исходящую политику, с названием OUT (порядок правил должен соблюдаться):

1. Пакеты со значением IP Precedence 5:

* явно указать, что пакеты идут в VLAN 23
* для class-map использовать название IPPREC5
* пакеты должны передаваться с наивысшим приоритетом. Выделить для них 20% от пропускной способности интерфейса

2. Пакеты со значением IP Precedence 3:

* явно указать, что пакеты идут в VLAN 23
* для class-map использовать название IPPREC3
* выделить для них 15% от пропускной способности интерфейса

3. Пакеты со значением IP Precedence 2:

* явно указать, что пакеты идут в VLAN 23
* для class-map использовать название IPPREC2
* выделить для них 5% от пропускной способности интерфейса

4. Пакеты со значением IP Precedence 1:

* явно указать, что пакеты идут в VLAN 23
* для class-map использовать название IPPREC1
* выделить для них 30% от пропускной способности интерфейса

5. Включить в class-default WRED с такими параметрами:

* использовать значения IP Precedence для распределения веса в WRED
* для пакетов со значение IP Precedence равным 5 и 6 изменить настройки по умолчанию:
  + WRED должен начать отбрасывать пакеты, при условии, что средний размер очереди находится между 101 и 102. Отбрасываться должен каждый 10 пакет
  + При необходимости, увеличить размер очереди (исправлено в 19:15 МСК 1.06)

На маршрутизаторе R3 создать такую исходящую политику, с названием OUT (порядок правил должен соблюдаться):

1. Пакеты со значением IP Precedence 5:

* явно указать, что пакеты идут в VLAN 34
* для class-map использовать название IPPREC5
* пакеты должны передаваться с наивысшим приоритетом. Выделить для них 20% от пропускной способности интерфейса
* пакеты должны быть промаркированы значением DSCP EF

2. Пакеты со значением IP Precedence 3:

* явно указать, что пакеты идут в VLAN 34
* для class-map использовать название IPPREC3
* выделить для них 15% от пропускной способности интерфейса
* пакеты должны быть промаркированы значением DSCP AF41

3. Пакеты со значением IP Precedence 2:

* явно указать, что пакеты идут в VLAN 34
* для class-map использовать название IPPREC2
* выделить для них 5% от пропускной способности интерфейса
* пакеты должны быть промаркированы значением DSCP AF31

4. Пакеты со значением IP Precedence 1:

* явно указать, что пакеты идут в VLAN 34
* для class-map использовать название IPPREC1
* выделить для них 30% от пропускной способности интерфейса
* пакеты должны быть промаркированы значением DSCP AF21

5. Включить в class-default WRED с такими параметрами:

* использовать значения DSCP для распределения веса в WRED
* для пакетов со значение DSCP равным AF41 и EF изменить настройки по умолчанию:
  + WRED должен начать отбрасывать пакеты, при условии, что средний размер очереди находится между 101 и 102. Отбрасываться должен каждый 10 пакет
  + При необходимости, увеличить размер очереди (исправлено в 19:15 МСК 1.06)

На маршрутизаторе R4 создать такую исходящую политику, с названием OUT (порядок правил должен соблюдаться):

1. Пакеты со значением DSCP EF:

* явно указать, что пакеты идут в VLAN 456
* для class-map использовать название EF
* пакеты должны передаваться с наивысшим приоритетом. Выделить для них 20% от пропускной способности интерфейса

2. Пакеты со значением DSCP AF41:

* явно указать, что пакеты идут в VLAN 456
* для class-map использовать название AF41
* выделить для них 15% от пропускной способности интерфейса

3. Пакеты со значением DSCP AF31:

* явно указать, что пакеты идут в VLAN 456
* для class-map использовать название AF31
* выделить для них 5% от пропускной способности интерфейса

4. Пакеты со значением DSCP AF21:

* явно указать, что пакеты идут в VLAN 456
* для class-map использовать название AF21
* выделить для них 30% от пропускной способности интерфейса

5. Включить в class-default WRED с такими параметрами:

* использовать значения DSCP для распределения веса в WRED
* для пакетов со значение DSCP равным AF41 и EF изменить настройки по умолчанию:
  + WRED должен начать отбрасывать пакеты, при условии, что средний размер очереди находится между 101 и 102. Отбрасываться должен каждый 10 пакет
  + При необходимости, увеличить размер очереди (исправлено в 19:15 МСК 1.06)

## [Лабораторная работа по теме 23: Logging 8.2](http://ccie.linkmeup.ru/2016/06/01/1024/)

Задание для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxZ2lCWnhOak5JS1U) R1, R2.

2. На маршрутизаторах R1 и R2 включить порядковый номер логирования.

3. На маршрутизаторах R1 и R2 включить отображение года и микросекунд в логах.

4. Маршрутизаторы R1 и R2 настроить таким образом, чтобы они отправляли уведомления об изменениях конфигурации в локальный syslog процесс. При этом указать число логируемых команд в 2 раза меньше, чем оно задано по умолчанию

5. Проверить командой show archive log config all.

6. Настроить syslog сервер следующим образом:

a. R1 должен стать сервером для R2 и наоборот;

b. Ограничить прием до 10 syslog сообщений в секунду на R1

c. Ограничить прием до 10 syslog сообщений в секунду на R2 кроме сообщений уровнем error и выше.

## [Лабораторная работа по теме 24: Layer 2 Security 7.1](http://ccie.linkmeup.ru/2016/06/03/laboratornaya-rabota-po-teme-24-layer-2-security-7-1/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxWlNPektzenIwMVU) на R2, R3, R5,R7, SW1, SW2, SW3, SW4.

2. На всех коммутаторах для VLAN 235 включить режим защиты DHCP-клиентов в сети от получения адреса от неавторизованного DHCP-сервера.

3. Назначить R2 авторизованным DHCP-сервером, произвести необходимую настройку портов коммутаторов SW1, SW2, SW4 как в сторону сервера, так и между коммутаторами

4. На недоверенных портах SW1 настроить ограничение в скорости получения DHCP-сообщений на рекомендуемое производителем значение.

5. Проверить настройки

# [**Вторая большая лабораторная работа**](http://ccie.linkmeup.ru/2016/06/06/vtoraya-bolshaya-laboratornaya-rabota/)

Изменения топологии:

* Диагональные линки e3/2, e3/3 между коммутаторами выключены.
* Интерфейсы e3/1, e2/3 между коммутаторами выключены.
* Вместо DMVPN между r7 и r2, r3, r4 настроены GRE-туннели.
* На r6 выключен интерфейс e0/1.144
* На r3 и r2 выключен интерфейс e0/1.23
* На r5 выключен интерфейс e0/1.456

[ССЫЛКА НА ТОПОЛОГИЮ](https://drive.google.com/open?id=0B3uwAH0p4u2NX3pBUEpCNkRva2s)

Скачать [файлы для импорта лабораторной работы в UNL](https://drive.google.com/open?id=0B1ftcXtQO2yOWEk4UnNRck9PUmM). Вам нужно будет импортировать zip файл в свою виртуальную машину.

Или [загрузить начальную конфигурацию](https://drive.google.com/open?id=0B3uwAH0p4u2NZnloUU5aYVY2aUk).

Всё, что относится к лабораторной на [Google Disk](https://drive.google.com/open?id=0B1ftcXtQO2yOSVpHWGhSUkx5cjA).

Советы:

* При выполнении заданий если вы заметили необычный конфиг, запишите его себе — вполне возможно, что это поможет вам решить последующие задания.
* Не забывайте включать обратно интерфейсы, если вы их выключали для теста.
* Проверки, указанные после задания, не гарантируют, что вы выполнили задание на 100% правильно.
* Будьте внимательны! Из-за неправильно выполненного подзадания вы можете получить 0 баллов за всё задание.

Правила:

* Нельзя изменять топологию
* Нельзя добавлять дополнительные интерфейсы/IP адреса, если в задании это явно не упомянуто.
* Нельзя использовать PBR.
* Нельзя включать динамическую маршрутизацию на маршрутизаторах r1, r5, r6.
* Нельзя использовать перераспределение (redistribute) маршрутов
* Нельзя использовать сериал интерфейсы на R9, R10 и R1, R2.
* Нельзя использовать менеджмент Vlan 1 (10.0.0.0/24).
* Лабораторная работа включает в себя смешанные задания по configuration и troubleshooting.
* Большинство устройств преднастроено (но не всегда верно).
* При решении заданий проверяйте есть ли уже конфигурация, которую можно использовать.
* Не рекомендуется удалять любой существующий конфиг — удаляйте только в случае, если других решений нет.
* В своих решения вы должны быть как можно более специфичны:

Пример с access-list:

**ip access-list extended TEST**

**5 deny ip 10.0.0.0 0.255.255.255 any**

**10 permit ip any any**

**interface e0/0**

**ip access-group TEST in**

Проблема: Специфичный HTTP траффик (src IP: 10.10.10.10, dst IP: 2.2.2.2, port 80) дропается, когда приходит на e0/0.

Неправильные решения:

1.

**inteface e0/0**

**no ip access-group TEST in**

2.

**ip access-list extended TEST**

**no 5**

Нейтральное решение (правильность оценивается на усмотрение эксперта):

**ip access-list extended TEST**

**4 permit ip 10.0.0.0 0.255.255.255 any**

Правильное решение:

**ip access-list extended TEST**

**4 permit tcp host 10.10.10.10 host 2.2.2.2 eq 80**

Удачи! Она вам пригодится!

### **Задание лабораторной**

##### **1. (6 баллов)**

* Настроить на всех коммутаторах режим Rapid PVST+.
  + Когда на коммутаторах работает Rapid PVST+, могут возникнуть проблемы со связностью, с прохождением трафика через коммутаторы и так далее.
  + Для того, чтобы избавиться от этого, переключитесь на режим PVST+.
  + Лабораторная будет засчитана и с тем и с тем режимом, как правильная.
* Настроить STP таким образом, чтобы:
  + для нечетных номеров VLAN, созданных на коммутаторах, заблокированным был порт e3/0 на коммутаторе SW2.
    - Не использовать для этого настройки STP на интерфейсах.
    - У корневого коммутатора приоритет должен быть настроен на основании вывода ниже.

**SW2#sh spanning-tree vlan 1**

**VLAN0001**

**Root ID Priority 1**

**...**

**Interface Role Sts Cost Prio.Nbr Type**

**------------------- ---- --- --------- -------- --------------------------------**

**...**

**Et3/0 Altn BLK 100 128.13 Shr**

* для четных номеров VLAN, созданных на коммутаторах, заблокированным был порт e3/0 на коммутаторе SW4.
  + Не использовать для этого настройки STP на интерфейсах.
  + У корневого коммутатора приоритет должен быть настроен на основании вывода ниже.

**SW4#sh spanning-tree vlan 2**

**VLAN0002**

**Root ID Priority 2**

**...**

**Interface Role Sts Cost Prio.Nbr Type**

**------------------- ---- --- --------- -------- --------------------------------**

**...**

**Et3/0 Altn BLK 100 128.13 Shr**

* Настроить порты, к которым подключены маршрутизаторы таким образом, чтобы изменение их состояния не приводило к генерации TCN в STP.

##### **2. (4 балла)**

На всех коммутаторах VTP должен быть полностью выключен. В выбранном режиме, сообщения VTP не должны передаваться через коммутаторы.

На каждом коммутаторе настроить имя VTP домена равным имени коммутатора.

При переключении в режим Server или Client, коммутаторы должны хранить информацию в nvram, в файле с именем ccie.dat (коммутаторы не нужно переключать в режим Server или Client).

##### **3. (6 баллов)**

Настройте r1 и r7 согласно выводу команд ниже.

Параметры SSH:

* Доменное имя: linkmeup.ru
* Размер RSA ключа должен быть 1024 бит
* Из протоколов удаленного доступа только SSH должен быть разрешён
* Использовать локальную базу пользователей для аутентификации (на r1 пользователь cisco/cisco преднастроен)
* Версия SSH: 2

Ограничения:

* Нельзя использовать NAT для решения задачи.
* Нельзя менять IP-адреса
* Номер vty имеет значение
* Совет: не используйте аутентификацию по ключам, в этом задании

Остальные настройки нужно определить из вывода ниже (порт со стороны клиента может быть любым):

**R2#ssh -l cisco -p 3009 180.1.1.1**

**Password:**

**R7> sh users**

**Line User Host(s) Idle Location**

**0 con 0 idle 00:01:27**

**\* 5 vty 3 ccie idle 00:00:00 188.1.12.1**

**R7> sh control-plane host open-ports**

**Active internet connections (servers and established)**

**Prot Local Address Foreign Address Service State**

**...**

**tcp \*:9009 \*:0 SSH-Server LISTEN**

**tcp \*:9009 188.1.12.1:45963 SSH-Server ESTABLIS**

Вывод с r1:

**R1#sh users**

**Line User Host(s) Idle Location**

**\* 0 con 0 idle 00:00:00**

**5 vty 3 cisco 180.1.7.7 00:00:06 188.1.12.2**

##### **4. (10 баллов)**

RIPv2 настроен на маршрутизаторах: r2, r3, r4, r7, r8, r9, r10.

Нельзя удалять настройки RIP.

* Настроить между r9 и r10 в сети интерфейса e0/1.109 RIPv2 таким образом, чтобы обновления между ними отправлялись только на directed broadcast адрес сети.
  + Обновление (7.06 20:45): нельзя использовать команду neighbor
  + Интерфейсы e0/1.201-203 и e0/1.211-213 нужны для проверки правил QoS в 10 задании. Для выполнения этого задания, их лучше выключить
* Восстановить обмен маршрутами RIPv2 между r8 и r9.  
  Кроме того, с Loopback0 r8 должен пинговаться с loopback0 r9.
  + Для выполнения этого задания:
    - нельзя менять IP-адреса на r8 и r9
      * Уточнение: на r9 IP-адрес e0/1.89 настроен не по топологии. Это умышлено! Нельзя менять ни его, ни адрес на r8 (из-за этого запрет про изменения адреса и написан)
    - нельзя настраивать neighbor в RIP
* Проверить, что между всеми маршрутизаторами, на которых включен RIPv2, происходит обмен сообщениями RIP и получены маршруты.

##### **5. (3 балла)**

* На r6:
  + Отключить DHCP сервер и relay agent минимальным количеством команд
  + Отключить всё логирование минимальным количеством команд
  + Изменить в консоли комбинацию, с помощью которой прерывается ping и traceroute в IOS, на Ctrl-C.

##### **6. (4 балла)**

* На r9 настроить отправку логов:
  + Используя как транспорт TCP
  + Логи должны отправляться на порт 10001
  + Отправлять логи на Loopback0 r7
  + Остальные параметры надо определить по выводу ниже
  + Настроить r7 таким образом, чтобы TCP сессия между r9 и r7 установилась (подсказка в выводе ниже).

Вывод должен быть таким (порты со стороны клиента могут быть любыми):

**R9#sh control-plane host open-ports**

**Active internet connections (servers and established)**

**Prot Local Address Foreign Address Service State**

**...**

**tcp \*:50254 180.1.7.7:10001 Syslog ESTABLIS**

**R7#sh control-plane host open-ports**

**Active internet connections (servers and established)**

**Prot Local Address Foreign Address Service State**

**...**

**tcp \*:10001 \*:0 HTTP CORE LISTEN**

**tcp \*:10001 180.1.9.9:50254 HTTP CORE ESTABLIS**

##### **7. (3 балла)**

Настроить DHCP для VLAN 235:

* r7 DHCP сервер:
  + создать пул с именем VLAN235
  + шлюз для пула должен быть r2
  + из сети VLAN’а 235 должен выдаваться только один адрес 188.1.235.5
* r2 и r3 должны быть настроены DHCP relay
* Интерфейс e0/1.235 R5 должен быть настроен как DHCP клиент
* Проверить, что r5 может получать адрес от r7 и через r2 и через r3.

##### **8. (6 баллов)**

На коммутаторах sw1, sw2, sw3 настроить DHCP snooping для VLAN 235.

Убедиться, что, после настройки DHCP snooping, r5 по-прежнему может получит адрес от r7.

В этом задании такие ограничения:

* на sw2 только один порт может быть trust
* на sw1 только два порта могут быть trust
* на sw3 только один порт может быть trust

##### **9. (7 баллов)**

Все роутеры должны пинговать Loopback0 друг друга, если source IP — Loopback0.

##### **10. (11 баллов)**

В задании необходимо настроить:

* политики QoS для трафика в направлении от r10 к r5.
* политики настраиваются на r9, r8, r7, r2, r3, r4 и проверяются с r10, отправляя трафик на r5.
* в обратном направлении, политики настраивать не нужно.

Легенда задания:

* Маршрутизатор r9 находится ближе всего к клиенту (r10), поэтому на нем выполняем классификацию пакетов и маркировку их DSCP
* На всех маршрутизаторах, для одного и того же типа трафика, настроена одна и та же политика обслуживания на выход
* В сети есть два типа трафика:
  + бизнес-трафик (сокращение в объектах BS)
    - VLAN’ы 201-203
  + enterprise-трафик (сокращение в объектах ENT)
    - VLAN’ы 211-213
* Между r9 и r10, для проверки QoS, созданы дополнительные интерфейсы:
  + e0/1.201-203 для проверки политик для BS трафика
  + e0/1.211-213 для проверки политик для ENT трафика

Ниже описаны политики, которые нужно настроить на маршрутизаторах r9, r8, r7, r2, r3, r4.

На маршрутизаторе R9 создать такую входящую политику, с названием IN\_QOS (порядок правил должен соблюдаться):

1. UDP пакеты из VLAN’ов 201, 202 или 203, с портами получателя в диапазоне 16384-18000:

* для описания пакетов использовать существующий ACL: VOIP
* явно указать, что пакеты идут из VLAN’ов 201, 202 или 203
  + объединить VLAN’ы в class-map. Назвать class-map BS\_VLAN
* для class-map использовать название BS\_VOIP
* пакеты должны быть промаркированы значением DSCP EF (используйте вариант set ip dscp)

2. HTTP трафик из VLAN’ов 201, 202 или 203:

* для описания HTTP пакетов использовать существующий ACL: HTTP
* явно указать, что пакеты идут из VLAN’ов 201, 202 или 203
  + использовать для этого созданную class-map BS\_VLAN
* для class-map использовать название BS\_HTTP
* пакеты должны быть промаркированы значением DSCP AF31 (используйте вариант set ip dscp)

3. ICMP пакеты из VLAN’ов 201, 202 или 203:

* для описания пакетов использовать существующий ACL: ICMP
* явно указать, что пакеты идут из VLAN’ов 201, 202 или 203
  + использовать для этого созданную class-map BS\_VLAN
* для class-map использовать название BS\_ICMP
* пакеты должны быть промаркированы значением DSCP AF21 (используйте вариант set ip dscp)

4. UDP пакеты из VLAN’ов 211, 212 или 213, с портами получателя в диапазоне 16384-18000:

* для описания пакетов использовать существующий ACL VOIP
* явно указать, что пакеты идут из VLAN’ов 211, 212 или 213
  + объединить VLAN’ы в class-map. Назвать class-map ENT\_VLAN
* для class-map использовать название ENT\_VOIP
* пакеты должны быть промаркированы значением DSCP AF41 (используйте вариант set ip dscp)

5. HTTP трафик из VLAN’ов 211, 212 или 213:

* для описания пакетов использовать существующий ACL HTTP
* явно указать, что пакеты идут из VLAN’ов 211, 212 или 213
  + использовать для этого созданную class-map ENT\_VLAN
* для class-map использовать название ENT\_HTTP
* пакеты должны быть промаркированы значением DSCP AF32 (используйте вариант set ip dscp)

6. ICMP пакеты из VLAN’ов 211, 212 или 213:

* для описания пакетов использовать существующий ACL ICMP
* явно указать, что пакеты идут из VLAN’ов 211, 212 или 213
  + использовать для этого созданную class-map ENT\_VLAN
* для class-map использовать название ENT\_ICMP
* пакеты должны быть промаркированы значением DSCP AF11 (используйте вариант set ip dscp)

7. Остальные пакеты из VLAN’ов 211, 212 или 213, с ненулевым значением DSCP:

* явно указать, что пакеты идут из VLAN’ов 211, 212 или 213
  + использовать для этого созданную class-map ENT\_VLAN
* для class-map использовать название ENT\_NON\_DEFAULT
* перемаркировать пакеты значением DSCP 0 (используйте вариант set ip dscp)

8. Применить политику на интерфейс e0/1

На маршрутизаторе R8 и r9 создать такую исходящую политику, с названием OUT (порядок правил должен соблюдаться):

1. Для трафика BS и ENT на выход должно быть разделение пропускной способности 70%/30% (BS 70% / ENT 30%)

Подсказка: для этого нужно будет создать иерархическую политику

2. Для BS трафика создаем политику с названием BS\_QOS. В этой политике:

* Пакеты со значением DSCP EF:
  + для class-map использовать название EF
  + должны передаваться с наивысшим приоритетом. Выделить для них 10% пропускной способности (так как политика иерархическая, то это будет 10% от 70%)
* Пакеты со значением DSCP AF31:
  + для class-map использовать название AF31
  + должны передаваться с наивысшим приоритетом. Выделить для них 5% пропускной способности
* Пакеты со значением DSCP AF21:
  + для class-map использовать название AF21
  + выделить для них 35% пропускной способности
* Пакеты с ненулевым значением DSCP:
  + для class-map использовать название NON\_DEFAULT
  + выделить для них 25% пропускной способности
* Для всех остальных пакетов, включить WRED на основании DSCP с настройками по умолчанию

3. Для ENT трафика создаем политику с названием ENT\_QOS. В этой политике:

* Пакеты со значением DSCP AF41:
  + для class-map использовать название AF41
  + должны передаваться с наивысшим приоритетом. Выделить для них 10% пропускной способности (так как политика иерархическая, то это будет 10% от 30%)
* Пакеты со значением DSCP AF32:
  + для class-map использовать название AF32
  + должны передаваться с наивысшим приоритетом. Выделить для них 5% пропускной способности
* Пакеты со значением DSCP AF11:
  + для class-map использовать название AF11
  + выделить для них 35% от пропускной способности интерфейса
* Для всех остальных пакетов, включить WRED на основании DSCP с настройками по умолчанию

4. Применить политику:

* на маршрутизаторе r9 на интерфейс e0/1.89
* на маршрутизаторе r8 на интерфейс e0/1.78

На маршрутизаторе R7 создать разные исходящие политики, для разных туннелей:

1. Для туннеля между r7 и r2:

* Для трафика BS и ENT на выход должно быть разделение пропускной способности 50%/50% (BS 50% / ENT 50%). Назвать политику OUT72

2. Для туннеля между r7 и r3:

* Для трафика BS и ENT на выход должно быть разделение пропускной способности 60%/40% (BS 60% / ENT 40%). Назвать политику OUT73

3. Для туннеля между r7 и r4:

* Для трафика BS и ENT на выход должно быть разделение пропускной способности 70%/30% (BS 70% / ENT 30%). Назвать политику OUT74

4. Политики применить к соответствующим туннелям

Подсказка: бывают еще более иерархические политики. Если вам понадобился еще один уровнять иерархии, добавьте к названию самой верхней политики приставку TUN\_

5. Вложенные политики для BS и ENT трафика, аналогичны политике на r8 и r9

На маршрутизаторах r2, r3, r4 создать исходящие политики:

1. Вложенные политики для BS и ENT трафика, аналогичны политикам на r8 и r9

2. Процентное соотношение между BS и ENT должно соответствовать аналогичному соотношению в туннеле

3. Применить политики на исходящие логические интерфейсы (subinterface) по пути к r5 (на r4 применить к интерфейсу e0/1.34).

Проверить политики с r10 самостоятельно (для UDP пакетов на r10 создан IP SLA тест).

Убедиться, что трафик одного типа попадает во все соответствующие классы.

### **Проверка лабораторной**

В большой лабораторной проверяется не только разница с ответом в конфигурации.

Кроме того, ваши конфиги будут загружены экспертом на оборудование и проверка будет выполняться командами show/ping и тд.

Поэтому то, что показано в проверке к заданиям лабы (вывод команд show/ping/…), должно у Вас выглядеть точно так же.

Обязательно, после каждого задания, выполняйте проверочные команды, которые указаны в лабораторной.

Вам не нужно выкладывать вывод команд show в ответе. Для больших лаб, мы это проверяем сами. Нужно выложить только конфигурацию.

# [**Цикл 5.**](http://ccie.linkmeup.ru/2016/06/18/tsikl-5-tema-25-stp-1-4/)

## [Лабораторная работа по теме 25: STP 1.4](http://ccie.linkmeup.ru/2016/06/20/laboratornaya-rabota-po-teme-25-stp-1-4/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxZ0ptZjAzd29uTW8) R1, R2,R4, SW1, SW2, SW3, SW4.

2. Назначить SW1 Root Bridge используя команду root primary для vlan 10.

3. Выполнить следующие настройки на всех коммутаторах для vlan 10:

• Уменьшить время отправки Сonfiguration BPDU на половину от значения по умолчанию.

• Уменьшить максимальное время ожидания BPDU пакетов на половину от значения по умолчанию.

• Уменьшить время обновления MAC-таблиц в случае получения сообщения об изменении топологии на треть от значения по умолчанию.

4. Порты E0/0 на SW1 и SW4 коммутаторах перевести в режим, в котором при изменении состояния порта не будет отправляться TCN.

5. На SW4 настроить режим, который позволяет коммутаторам обновить записи в таблицах коммутации без использования TCN при падении Root Port на SW4.

6. На всех коммутаторах настроить режим, который позволяет быстрее найти альтернативный путь, после изменения топологии, устанавливая MaxAge как “Истекший”.

7. Порты E0/0 на SW1 и SW4 коммутаторах настроить таким образом, чтобы BPDU сообщение не отправлялись и не принимались.

8. Настроить SW1 таким образом, чтобы на порту e0/1 BPDU не принимались и не отправлялись, но в случае получения BPDU на данном порте данный порт мог учитываться в STP-домене.

9. Порты E0/0 на SW1 и SW4 коммутаторах настроить таким образом, чтобы при получении BPDU они переходили в режим Error disable.

10. На SW1 и SW4 настроить время восстановления портов, попавших под режим Error disable вследствие получения BPDU за 30 секунд.

11. Порты E0/0 на SW1 и SW4 коммутаторах настроить таким образом, чтобы при получении Superior BPDU они переставали передавать трафик.

## [Лабораторная работа по теме 26: Miscellaneous 1.6](http://ccie.linkmeup.ru/2016/06/22/laboratornaya-rabota-po-teme-26-miscellaneous-1-6/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxTEtDYUF3R0tDTEE) R1, R5, SW1, SW2.

2. Назначить SW1 Root Bridge используя команду root primary для вланов 10 и 20.

3. Выполнить следующие настройки на SW1 и SW2 для vlan 10 и 20:

♦ Уменьшить время отправки BPDU на половину от значения по умолчанию.

♦ Уменьшить время ожидания BPDU пакетов на половину от значения по умолчанию, пока линк не уйдет в down.

♦ Уменьшить время обновления МАК-таблиц в случае получения сообщения об изменении топологии на треть от значения по умолчанию.

4. Настроить порт E0/0 на SW1 режиме access для передачи пакетов данных в VLAN10 и передачи голосовых пакетов в VLAN20.

5. Транковые порты SW1 и SW2 должны быть настроены таким образом, чтобы выполнялись следующие условия:

♦ Порты должны передавать трафик VLAN10 нетегированным.

♦ Сконфигурировать Vlan 20 таким образом, чтобы он анонсировался как Voice VLAN через CDP.

♦ Порты должны передавать только эти два влана.

6. Настроить порт E0/0 на и SW2 таким образом, чтобы и пакеты данных и глосовые пакеты передавались в влан 10 c 802.1q заголовком.

## [Лабораторная работа по теме 27: RIPv2 3.4](http://ccie.linkmeup.ru/2016/06/24/laboratornaya-rabota-po-teme-27-ripv2-3-4/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxMWdua0J3ZzFGbGs) SW1, SW2, SW3, SW4, R1, R2, R3, R4, R5, R6, R7, R8, R9, R10.

2. Настроить на всех маршрутизаторах протокол ripv2 для сетей 180.1.0.0 и 188.1.0.0 и отключить автоматическую суммаризацию сетей.

3. Проверить что все сети на маршрутизаторах анонсированы и решить проблему в случае, если нет каких-то маршрутов

4. Маршрутизаторы R3 и R5 настроить таким образом, чтобы они не отправляли RIP сообщения для сегмента сети на интерфейсе E0/1.235, но при этом сохранили возможность получать RIP сообщения от маршрутизатора R2 по этому интерфейсу.

5. Сформируйте отправляемые от R8 к R7 маршруты так, чтобы они содержали минимальное количество информации для доступа к подсетям, но так чтобы минимально повлиять на маршруты до Loopback интерфейсов других маршрутизаторов: 188.1.89.0\24, 188.1.109.0\24, 188.1.9.0\24, 188.1.10.0\24, 180.1.10.10\32, 180.1.9.9\32, 180.1.8.8\32

6. Маршрутизатор R1 должен иметь только один общий маршрут, полученный по RIP для получения доступа до всей остальной части сети. Не использовать фильтрацию маршрутов.

7. Настройте статический маршрут 10.10.10.0/24 на R6 в сторону R7 c отправив его в Null0. Редистрибьютьте его в RIP.

8. На R2 настроить offset-list таким образом, чтобы трафик до R3 отправлялся через интерфейс E0/1.23

9. На R6 настроить offset-list таким образом, чтобы маршрут 10.10.10.0 шел не дальше R3

10. Настроить prefix-list на R6 таким образом, чтобы маршрут 180.1.2.2 не передавался в update rip на всех интерфейсах.

## [Лабораторная работа по теме 28: QoS 6.16-6.18, 6.22](http://ccie.linkmeup.ru/2016/06/27/laboratornaya-rabota-po-teme-28-qos-6-16-6-18-6-22/)

Задание #1 для лабораторной ([начальный конфиг](https://drive.google.com/open?id=0B8TdfSzCKkaxbWxpZzZHN1lMUjQ)):

Ограничения:

• На R3 отключены некоторые интерфейсы. По условию они должны оставаться в выключенном состоянии.

• Не включены DMVPN интефрейсы

Проверка:

• Для проверки можно воспользоваться заготовленными IP SLA на R10.

1) Настроить на R9 для подинтерфейса Eth0/1.109 следующие настройки Class Based Policing для policy-map CustomerR10:

\* Определить классы для следующих удаленных приложений HTTP, SSH, FTP

\* Для классификации трафика использовать ACL по направлению к удаленным сервисам. Названия ACL использовать в соотвествии с классом определяемого трафика.

\* Для HTTP трафика выделить 192 kbps

\* Для SSH трафика выделить 64 kbps

\* Для FTP трафика выделить 128 kbps

\* Для всего остального трафика выделить 128 kbps.

\* Для всех классов при уровне трафика ниже определенного «контрактом» применять действие transmit

\* Для всех классов превыщающих заданный «контрактом» уровень трафика применить значение DSCP 10

\* Для всех классов нарушающих уровень заданный «контрактом» уровень трафика применить действие drop

\* Для всех классов задать значения Bc и Be , не менее 1 секунды и 0,5 секунды соответственно

2) Настроить на R6 для подыинтерфейса Eth0/1.67 CB Policing для policy-map Branch1:

\* Определить для трафика с источником от подсетей маршрутизатора R10 полосу в 384 kbps

\* confirm, exceed, violation задать в следующим образом : передать, задать DSCP 0, отбросить

\* Для всего остального трафика задать полосу в 512 kbps

\* confirm, exceed, violation задать в следующим образом : передать , задать DSCP 0, отбросить

\* Для всех типов трафика допускается значение Bc 1000 милисекунд и Be 500 милисекунд соответственно

\* Использовать название R10 соответсвенно.

3) Настроить на R2 для подинтерфейса Eth 0/1.235 следующие настройки CB Policing для policy-map IncomingPolicy

\* определить HTTP трафик в классе HTTP\_R1

\* трафик классифицировать только по направлению к Loopback адресу R1 как к вебсерверу

\* выделить полосу в 384 kbps

\* Допустимо значение Bc 800 милисекунд и Be в 400 милисекунд

\* определить весь остальной HTTP трафик в класс HTTP\_ANY по направлению к вебсерверу

\* выделить полосу в 96 kbps

\* Определить трафик FTP в класс FTP по направлению к ftp серверу

\* выделить полосу 256 kbps

\* Определить трафик SSH в класс SSH по направлению к ssh серверу

\* Выделить полосу 128 kbps

\* Весь остальной трафик не лимитировать

\* Для классов для которых явно не указано значение Bc\Be задать значение 200 и 300 милисекунд соответственно

\* Ко всем классам применить следующие правила confirm, exceed, violation:

передать, передать , отбросить

\* Использовать при необходимости названия соотвествующие названиям классов

## [Лабораторная работа по теме 29: NTP 8.3](http://ccie.linkmeup.ru/2016/06/29/laboratornaya-rabota-po-teme-29-ntp-8-3/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxekwybk16SFRYTHM) SW1, SW2, SW3, SW4, R1, R2, R3, R4, R5, R6, R7, R8, R9, R10.

2. На всех маршрутизаторах настроить протокол маршрутизации RIP версии 2, отключить автосуммаризацию. Если есть проблемы с маршрутизацией, решить ее.

3. Назначить R10 NTP сервером и настроить часовой пояс по МСК +00.

4. Настроить R1, R4, R5, R6, R7, R8, R9 для синхронизации времени от R10, используя соответствующий Source интерфейс.

5. Настроить R3 для синхронизации времени от R10, используя Source интерфейс E0/1.34 как основной, а интерфейс E0/1.235 как дополнительный

6. Настроить R2 для синхронизации времени от R10, используя Source интерфейс E0/1.23 как основной, а интерфейс E0/1.235 как дополнительный.

7. На всех маршрутизаторах настроить аутентификацию NTP с номером ключа 1 и паролем CCIEinaYEAR

8. На всех клиентских маршрутизаторах настроить access-list с названием NTP\_SERVER для доверенного сервера NTP R10.

9. На R10 настроить access-list с названием NTP\_CLIENTS с указанием диапазона адресов клиентов для синхронизации времени.

## [Лабораторная работа по теме 30: Management Plane Security 7.2](http://ccie.linkmeup.ru/2016/07/01/laboratornaya-rabota-po-teme-30-management-plane-security-7-2/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxNEhfeG1GQ0NzOFE) R1, R2.

2. На R2 создать локального пользователя под именем CCIEConsole c привилегией 15 и с шифрованным паролем CCIEinaConsole. Включить ААА.

3. На R2 задать шифрованный пароль CCIEinaYEAR для Enable.

4. На R2 создать authentication list под названием CONSOLE с использованием локальной базы пользователей и паролем. Применить его на консоли.

5. На R2 создать authentication list под названием TELNET c использованием локальной базы пользователей, но паролем для Enable. Применить на терминальной линии.

6. Настроить 3 максимальные попытки подключения.

7. Настроить баннер, который будет требовать ввести пароль “Password Required” при подключении.

8. Настроить баннер, который будет требовать ввести имя пользователя “Username Required” при подключении.

9. Настроить баннер, который будет выводить сообщение “Authentication Failed , try again, при неудачной попытке аутентификации.

10. На R2 настроить авторизацию exec по умолчанию с использованием локальной базы.

# [**Цикл 6.**](http://ccie.linkmeup.ru/2016/07/02/materialy-po-tsiklu-6-tema-31-stp-1-4/)

## [Лабораторная работа по теме 31: STP 1.4](http://ccie.linkmeup.ru/2016/07/04/laboratornaya-rabota-po-teme-31-stp-1-4/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxMmUyRzdTNnBJZEk) R1, R4, SW1, SW2, SW3, SW4.

2. Перевести все коммутаторы в режим работы RSTP.

3. Назначить SW1 Root Bridge используя команду root primary для vlan 10, определив максимальное количество коммутаторов между R1 и R4 равное 4.

4. Назначить SW4 Secondary Root Bridge используя команду root secondary для vlan 10, определив максимальное количество коммутаторов между R1 и R4 равное 4.

5. Выполнить следующие настройки на всех коммутаторах для vlan 10:

• Уменьшить время отправки на половину от значения по умолчанию.

6. Порты E0/0 на SW1 и SW4 коммутаторах перевести в режим, в котором при изменении состояния порта не будет отправляться TCN.

7. Порты E0/0 на SW1 и SW4 коммутаторах настроить таким образом, чтобы при получении BPDU они переходили в режим Error disable.

8. На SW1 и SW4 настроить время восстановления портов, попавших под режим Error disable вследствии получения BPDU за 30 секунд.

9. Порты E0/0 на SW1 и SW4 коммутаторах настроить таким образом, чтобы при получении Superior BPDU они переставали передавать трафик.

10. Перевести все активные порты на коммутаторах в режим работы point-to-point.

## [Лабораторная работа по теме 32: Layer 2 Security 7.1](http://ccie.linkmeup.ru/2016/07/07/laboratornaya-rabota-po-teme-32-layer-2-security-7-1/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxaUZOS1Q2QTRYZDQ) R1, R5, SW1, SW2.

2. Назначить SW1 Root Bridge используя команду root primary для vlan 10, определив максимальное количество коммутаторов между R1 и R5 равное 2, уменьшив при этом время отправки BPDU на половину от значения по умолчанию.

3. Назначить SW2 Secondary Root Bridge используя команду root secondary для vlan 10, определив максимальное количество коммутаторов между R1 и R5 равное 2, уменьшив при этом время отправки BPDU на половину от значения по умолчанию.

4. Порты E0/0 на SW1 и S2 коммутаторах перевести в режим, в котором при изменении состояния порта не будет отправляться TCN, а также в режим работы point-to-point.

5. Перевести все транковые порты на коммутаторах в режим работы point-to-point.

6. Назначить SW1 в роли аутентификатора, выполнив следующие настройки:

• Включить aaa new model.

• Создать список метода аутентификации, который будет применяться по умолчанию ко всем портам. Также указать список всех серверов аутентификации Radius.

• Настроить коммутатор для авторизации на Radius серверах, для запросов всех сетевых сервисов.

• Включить 802.1x аутентификацию на коммутаторе глобально

• Указать в качестве Radius сервера R5 c ключом CCIEinaYEAR

• Настроить порт E0/0 в режиме работы single-host, указать очередность аутентификации сначала 802.1 x, затем MAB. Включить МАВ и аутентификацию на порту. Настроить период таймаута в 5 секунд для повторного запроса от Supplicant. Настроить порт в качестве Authenticator.

## [Лабораторная работа по теме 33: EIGRP 3.5](http://ccie.linkmeup.ru/2016/07/08/laboratornaya-rabota-po-teme-33-eigrp-3-5/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxUjI5STVOdC00THc) R1,R2,R3,R4, R5, R6, R7, R8, R9, R10, SW1, SW2, SW3, SW4.

2. Настроить R1, R2, R3, R4, R5 в режиме работы классического EIGRP с номером автономной системы 100 таким образом, чтобы были анонсированны сети 188.1.0.0/16 и 180.1.0.0/16

3. Настроить R6, R7, R8, R9, R10 в режиме работы Named EIGRP с названием CCIEinaYEAR и номером автономной системы 100 таким образом, чтобы были анонсированны сети 188.1.0.0/16 и 180.1.0.0/16.

4. На маршрутизаторах, где необходимо, запретить анонсирование EIGRP пакетов.

5. Убедиться, что все маршруты доступны на всех маршрутизаторах.

## [Лабораторная работа по теме 34: QoS 6.19-6.20](http://ccie.linkmeup.ru/2016/07/11/laboratornaya-rabota-po-teme-34-qos-6-19-6-20/)

### Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxU0dxVGFLdkdUVzQ) R1, R2.

2. Настроить R1 следующим образом:

• Весь трафик HTTP в сторону R2 должен шейпится через S 1/0 с peak rate в 512 kb/s. Для классификации трафика использовать access-list HTTP\_PEAK.

• Tc не должен превышать интервал в 40 msec.

### Задание #2 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxR2lqZHZkYm43RU0) R9, R10.

2. Настроить R10 следующим образом:

• Пиковая скорость должна составлять 40 % от общей пропускной способности

• Гарантированная скорость должна составлять 20 % от общей пропускной способности.

• Bc должен быть равен 250 ms

• Be должен быть равен 300 ms

3. Применить политику на R10 на входящем интерфейсе от R9

## [Лабораторная работа по теме 35: EEM 8.4](http://ccie.linkmeup.ru/2016/07/13/laboratornaya-rabota-po-teme-35-eem-8-4/)

### Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxa2F5V1RVXzc4OUE) R1,R2.

2. R1 играет роль TFTP-сервера:

• На R1 в директории unix создать папку DayliBackups, куда будут сохраняться все конфиги.

3. Настроить автоматизирование бэкапа на R2 следующим образом:

1. Создать архивный путь с указанием R1 в качестве tftp-сервера, таким образом, чтобы при каждом архивировании в имени файла указывался hostname R1 и время архивирования.

2. Создать событие KRON с наименованием Run\_Config\_Backup , при котором выполняется бэкап running-config.

3. Running-config должен архивироваться на TFTP сервере каждый день в 18.00

### Задание #2 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxM2pwYTJvQkRRajg) R1,R2.

2. На R1 и R2 создайте апплет под названием “IP\_Add\_lo0” для автоматического создания loopback 0 c ip адресами согласно топологии. При этом команды cli должны идти одна за другой и апплет должен запускаться вручную.

3. На R1 и R2 создайте апплет под названием “No\_Ping” для запрета пинга ip адресов непосредственно подключенных интерфейсов устройств. При пинге должно генерироваться сообщение “No ping for you, buddy!”

## [Лабораторная работа по теме 36: Management Plane Security 7.2](http://ccie.linkmeup.ru/2016/07/15/laboratornaya-rabota-po-teme-36-management-plane-security-7-2/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxaG5xaExNQU9Ld0k) R1,R2.

2. На R1 и R2 создайте апплет под названием “Rolebased” для автоматического создания шифрованного пароля enable «Rolebased». При этом команды cli должны идти одна за другой и аплет должен запускаться вручную.

3. На R1 и R2 создать view L1 и паролем Layer1 и привязать к нему пару пользователь/шифрованный пароль cableguy/onlylayer1 со следующим доступом:

• Он должен иметь доступ только к командам shut и no shut на интерфесах S1/0 и E0/1

• Мог выполнять команду sh ip int br и не мог использовать команду sh run

4. На R1 и R2 создать view Sup1 и паролем Support и привязать к нему пару пользователь/шифрованный пароль miniadmin/onlymin со следующим доступом:

• Он должен иметь доступ к командам configure terminal.

• Он должен иметь доступ только к команде show run.

• Он не должен иметь доступ командам конфигурирования к протоколов маршрутизации.

5. На R1 и R2 создать view Superadmin superview и паролем IAlmighty и привязать к нему пару пользователь/шифрованный пароль superadmin/Iadmin со следующими настройками:

• Добавить все ранее созданные view в Superadmin.

6. На R1 и R2 настроить Radius- сервер c ip адресом 188.1.23.3, с портом для аутентификации 1414, и accounting портом 1415 и ключом LinkmeUp

7. На R1 и R2 настроить Tacacs- сервер ip адресом 188.1.23.3 и ключом LinkmeUp\_Tacacs.

8. Аутентификацию и авторизацию пользователи должны проходить следующим путем:

• Сначала на сервере Tacacs, если не получилось, то на сервере Radius, если нет, то локально

# [**Цикл 7.**](http://ccie.linkmeup.ru/2016/07/23/tsikl-7-tema-37-stp-1-4/)

## [Лабораторная работа по теме 37: MST](http://ccie.linkmeup.ru/2016/07/25/laboratornaya-rabota-po-teme-37-mst/)

1) Загрузить начальную [конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfMXlKVjd4aVRJdGs) R2,R3,R4, R5, SW1, SW2, SW3, SW4.

2) Для задания используется логическая и физическая топологии проекта.

3) Все настройки делаются в одном регионе. Название региона: REGION1.

4) Настроить MST на коммутаторах следующим образом:

* Трафик вланов, относящихся к R2 и R3:
  + Должен идти сначала SW1-SW2-SW3, если падает SW2, то SW1-SW4-SW3, если падает SW4, то SW1-SW3.
  + В конфигурации не менять настройки портов.
  + Отнести все вланы в MST 23.
  + Назначить SW2 root в MST 23, используя команду с указанием приоритета.
* Трафик вланов, относящихся к R3 и R4:
  + Должен идти сначала SW3-SW1-SW4, если падает SW1, SW3-SW2-SW4, если падает SW2, то SW3-SW4.
  + В конфигурации не менять настройки портов.
  + Отнести все вланы в MST 34.
  + Назначить SW1 root в MST 34, используя команду macro.
* Трафик вланов, относящихся к R3 и R5:
  + Должен идти сначала SW3-SW4-SW2, если падает SW4, SW3-SW1-SW2, если падает SW1, то SW3-SW2.
  + В конфигурации не менять настройки портов.
  + Отнести все вланы в MST 235.
  + Назначить SW4 root в MST 235, используя команду с указанием приоритета.

5) Назначить SW1 CIST Root для REGION1.

## [Лабораторная работа по теме 38: Object Tracking 9.1](http://ccie.linkmeup.ru/2016/07/27/laboratornaya-rabota-po-teme-38-object-tracking-9-1/)

Задание #1 для лабораторной:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxVTZQc3dLWkpzbEE) всех устройств.

2. В задании используется логическая топология проекта без DMVPN.

3. На всех мартшрутизаторах настроить протокол маршрутизации Named EIGRP с названием IPSLA с номером автономной системы 10. При этом должны анонсироваться сети 188.1.0.0 и 180.1.0.0

4. На R10 настроить http server следующим образом:

а) К нему должен получать доступ только R1 c ip адресом 188.1.12.1 на порту 80.

в) Сервер должен отвечать на этот запрос.

5. На R1 создать IP SLA со следующей настройкой:

IP SLA под номером 1 для отправки HTTP get запроса на R10.

6. На R10 настроить симуляцию ответа на запрос голосового трафика следующим образом:

Настроить IP SLA Responder для ответы на на все udp запросы R1 c ip адреса 188.1.12.1 .

7. На R1 создать IP SLA со следующей настройкой:

а) IP SLA под номером 2 для симуляции проверки производительности сети на голосовой трафик. Запрос отправляется на R10. Настроить проверку jitter для проверки по кодеку g729a.

8. На R1 создать IP SLA со следующей настройкой:

а) IP SLA под номером 3 для проверки задержек на каждом маршрутизаторе от R1 до R10.

В конце конфига R1 выложить вывод команды sh ip sla statistics

## [Лабораторная работа по теме 39: EIGRP 3.5](http://ccie.linkmeup.ru/2016/07/29/laboratornaya-rabota-po-teme-39-eigrp-3-5/)

Задание для лабы:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxbUlHU0x3VzAxWW8) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3 настроить classic mode EIGRP следующим образом:
   1. Номер автономной системы 100
   2. Аннонсировать сети 188.1.0.0 и 180.1.0.0
   3. Отключить автосуммаризацию
4. На маршрутизаторах R4, R5, R6, R7, R8, R9, R10 настроить Named mode EIGRP следующим образом:
   1. Имя NAMEDEIGRP
   2. Номер автономной системы 100
   3. Аннонсировать сети 188.1.0.0 и 180.1.0.0
   4. Отключить автосуммаризацию
5. Отключить на маршрутизаторах аннонсирование EIGRP пакетов, туда где в них нет необходимости.
6. На всех маршрутизаторах изменить ограничение по хопам с 100 на 200
7. Изменить метрику на маршрутизаторе R3 таким образом, чтобы маршруты от R1 приходили через интерфейс E0/1.23. При этом не изменять значение Bandwidth
8. Уменьшить метрику rib-scale на маршрутизаторах c Named Mode в 2 раза от значения по-умолчанию.
9. Настроить BFD на маршрутизаторах R2, R3, R5 со следующими настройками:
   1. Настроить на всех интерфейсе E0/1.235 с интервалом между bfd пакетами в 250 миллисекунд, минимальный интервал приема 250 миллисекунд, multiplayer 3
   2. Применить в автономной системе 100

## [Лабораторная работа по теме 40: QoS 6.21,6.23](http://ccie.linkmeup.ru/2016/08/01/laboratornaya-rabota-po-teme-40-qos-6-21-6-23/)

Задание для лабы:

1. Загрузить [начальную конфигурацию](https://drive.google.com/file/d/0B8TdfSzCKkaxc0JhRG5lZ1ZVMHM/view) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3 настроить classic mode EIGRP следующим образом:
   1. Номер автономной системы 100
   2. Аннонсировать сети 188.1.0.0 и 180.1.0.0
   3. Отключить автосуммаризацию
4. На маршрутизаторах R4, R5, R6, R7, R8, R9, R10 настроить Named mode EIGRP следующим образом:
   1. Имя NAMEDEIGRP
   2. Номер автономной системы 100
   3. Аннонсировать сети 188.1.0.0 и 180.1.0.0
   4. Отключить автосуммаризацию
5. На всех маршрутизаторах изменить ограничение по хопам от 100 до 200
6. Уменьшить метрику rib-scale на маршрутизаторах c Named Mode в 2 раза от значения по-умолчанию.
7. Настроить RTP compression на маршрутизаторе R9 следующим образом:
   1. Создать class map RTP для классификации трафика rtp, используя access-list RTP где разрешить трафик по диапазону udp портов от 16384 до 32767
   2. Создать policy map с названием COMPRESS для сжатия заголовка rtp
   3. Применить его на интерфейсе Multilink
8. Создать ip sla на маршрутизаторе R1 для генерирования rtp трафика со следующими настройками:
   1. IP SLA под номером 1
   2. тип задержки udp на R10 c ip адресом 188.1.109.10 на любой порт из диапазона 16384 до 32767 с использованием кодека g729a
   3. Запустить сразу
9. На маршрутизаторе R10 настроить ip sla responder
10. Дать выводы команды sh policy-map int Multilink1 на маршрутизаторе R9

## [Лабораторная работа по теме 41: EEM 8.4](http://ccie.linkmeup.ru/2016/08/03/laboratornaya-rabota-po-teme-41-eem-8-4/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxTHczeUxRVDdnVDQ) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3 настроить classic mode EIGRP следующим образом:
   * Номер автономной системы 100
   * Аннонсировать сети 188.1.0.0 и 180.1.0.0
   * Отключить автосуммаризацию
4. На маршрутизаторах R4, R5, R6, R7, R8, R9, R10 настроить Named mode EIGRP следующим образом:
   * Имя NAMEDEIGRP
   * Номер автономной системы 100
   * Аннонсировать сети 188.1.0.0 и 180.1.0.0
   * Отключить автосуммаризацию
5. На всех маршрутизаторах изменить ограничение по хопам от 100 до 200
6. Создать аплет NamedEigrp который переведет маршрутизаторы из режима classic mode в named mode через 30 сек и при этом сгенерируется сообщение «Now we are in NamedEigrp»
7. Создать аплет под названием Broadcasts для мониторига броадкаст пакетов, приходящих на интерфейс E0/1 маршрутизатора R3 следующим образом:
   * при получении более 5 броадкаст сообщений на инт в течении 10 сек, будет генерироваться сообщение «Broadcast storm detected on E0/1»
8. Создать 2 аплета на R10 для создания бэкапного пути через мультилинк при падении основного инт E0/1.109 следующим образом:
   * создать ip sla под номером 1, который будет отправлять icmp-echo на ip адрес 188.1.109.9
   * создать ip sla track с задержкой в 60 секунд
   * запустить выполнение ip sla сразу
   * создать аплет BackupPath, который будет отправлять сообщение «Main path is no longer reachable» и включать интерфейс Multilink1 если пропадет линк на интерфейсе E0/1.109. После включения интерфейса Multilink1 должно отправляться сообщение «Failed over E0/1.109»
   * создать аплет MainPath, который при будет отправлять сообщение «Main path has been restored», если поднимется линк на интерфейсе E0/1.109 , при этом интерфейс Multilink1 отключится и отправится сообщение «Returned traffic over int E0/1.109»

Для проверки настроенных апплетов и правильной их работы используйте следующие алгоритмы:

* для проверки перехода на вспомогательный канал — выключили саб-интерфейс на R9 и там же включили мультилинк, на R10 автоматически должен произойти переход на вспомогательный канал;
* для проверки перехода на основной канал — на R9 выключили мультилинк, включили сабинтерфейс, на R10 через shut/no shut подняли физический интерфейс, апплет должен отработать и перевести всё на основной канал

## [Лабораторная работа по теме 42: Control Plane Security 7.3](http://ccie.linkmeup.ru/2016/08/05/1372/)

Необходимо перенастроить хождение трафика через sw1, с использованием eth0/1.12. Адресацию с serial интерфейса также можно перенести на этот саб-интерфейс.

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B3uwAH0p4u2NN1JTUC1yZHhjVVE) на R1,R2,SW1
2. Настроить доступ на R2 ssh 2 версии со следующими ограничениями:
   * длина ключа 1024
   * доменное имя CCIEinaYEAR
   * пара пользователь/пароль CCIEadmin/CCIEinaYEAR
   * аутентификация локальная
   * доступ к R2 должен быть разрешен только по протоколу ssh, по всем остальным портам доступ должен быть запрещен для всего трафика предоставленного интерфейсам устройства
3. Настроить политику так, чтобы только с loopback R2 на R1 пинги не ограничивались. Для всех остальных адресов каждую минуту разрешено пропустить 240 пакетов. Использовать динамическую маршрутизацию запрещено.
4. Зафильтровать получение всего cdp-трафика на R1. Необходимо использовать возможности только CPPr. (подсказка — при применении этой фильтрации может быть заблокирован не только cdp, применённый фильтр не должен мешать работе протокола ARP -проверка путём очистки арп-таблицы и успешный пинг между лупбэками R1 и R2) При именовании классов, политик, списков доступа использовать наименования соответствующих протоколов.

# 

# [**Цикл 8.**](http://ccie.linkmeup.ru/2016/08/05/tsikl-8-tema-43-ospf-3-6-2/)

## [Лабораторная работа по теме 43: OSPF 3.6](http://ccie.linkmeup.ru/2016/08/08/laboratornaya-rabota-po-teme-43-ospf-3-6/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxSXNqdkVyRG0wNlk) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На всех маршрутизаторах настроить протокол OSPF следующим образом:
   * Номер процесса 100
   * Подключить все интерфейсы к area 0 одной командой
   * Убедиться что все маршруты анонсированы на всех маршрутизаторах. Если возникли проблемы, устранить
   * На всех маршрутизаторах настроить RID по такой логике:
     + RID маршрутизатора R1 — 1.1.1.1
     + RID маршрутизатора R2 — 2.2.2.2 и т.д.
     + Для назначения RID нельзя создавать новые интерфейсы и нельзя менять IP-адреса.
   * Интерфейсы E0/1.5 и E0/1.6 маршрутизаторов R5 и R6 подключить к процессу 50 area 1 не используя команду network
   * Тупиковые интерфейсы на маршрутизаторах R7, R9, R10 настроить таким образом, чтобы они анонсировались в домен OSPF, но отношения соседства на них не могли установиться

## [Лабораторная работа по теме 44: FHRP 9.2](http://ccie.linkmeup.ru/2016/08/10/laboratornaya-rabota-po-teme-44-fhrp-9-2/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B3uwAH0p4u2NVkp6Mm43RmVqVUE) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На всех маршрутизаторах настроить протокол OSPF следующим образом:
   * Номер процесса 100
   * Подключить все интерфейсы к area 0 одной командой
4. Убедиться что все маршруты анонсированы на всех маршрутизаторах. Если возникли проблемы, устранить
5. На всех маршрутизаторах настроить RID по такой логике:
   * RID маршрутизатора R1 — 1.1.1.1
   * RID маршрутизатора R2 — 2.2.2.2 и т.д.
   * Для назначения RID нельзя создавать новые интерфейсы и нельзя менять IP-адреса.
6. На R5 и R6 настроить HSRP следующим образом:
   * Задать номер группы 456
   * Задать адрес шлюза по умолчанию последний адрес подсети vlan’а 456
   * R5 должен получить роль Active
     + приоритет можно менять только на R5
   * Уменьшить hello и hold тамеры соответственно на 2 и 5 сек.
   * Настроить маршрутизаторы таким образом, чтобы они автоматически забирали роль Aсtive на себя если их приоритет выше чем у действующего Active в данный момент.
7. На R5 и R2 настроить VRRP следующим образом:
   * Задать номер группы 235
   * Задать адрес шлюза по умолчанию последний адрес подсети vlan’а 235
   * Указать R2 как Master
8. На R5 и R6 настроить GLBP следующим образом:
   * Задать номер группы 456
   * Задать адрес шлюза по умолчанию предпоследний адрес подсети vlan’а 456
9. На R5 настроить ip sla следующим образом:
   * номер ip sla 1
   * отправляется icmp-echo на адрес 188.1.235.3 с частотой раз в 3 секунды, ждем 1 сек.
   * запустить сразу
10. Настроить трекинг для ip sla 1:
    * Задать номер 1
    * Настроить reachibility c задержкой на состояние up в 1 минуту
    * Применить к HSRP на R5 с Decrement’ом в 255

## [Лабораторная работа по теме 45: EIGRP 3.5](http://ccie.linkmeup.ru/2016/08/12/laboratornaya-rabota-po-teme-45-eigrp-3-5/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxUmhmZnRBOTJIMGs) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R6, R7, R8, R9, R10 настроить classic mode EIGRP следующим образом:
   * Номер автономной системы 100
   * Аннонсировать сети 188.1.0.0 и 180.1.0.0
   * Отключить автосуммаризацию
   * Отключить на маршрутизаторах аннонсирование EIGRP пакетов, туда где в них нет необходимости.
   * Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам Classic Mode следующим образом:
     + Название ключа CLASSIC\_MODE
     + Номер ключа 1
     + Пароль CLASSIC
   * Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторамс Named Mode следующим образом:
     + Название ключа CLASSIC\_NAMED
     + Номер ключа 2
     + Пароль CLASSIC NAMED
4. На маршрутизаторах R1, R2, R3, R4, R5 настроить Named mode EIGRP следующим образом:
   * Имя NAMEDEIGRP
   * Номер автономной системы 100
   * Аннонсировать сети 188.1.0.0 и 180.1.0.0
   * Отключить автосуммаризацию
   * Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам с Named Mode следующим образом:
     + Пароль NAMED, зашифрованный уровнем 7
   * Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам с Classic Mode следующим образом:
     + Название ключа CLASSIC\_NAMED
     + Номер ключа 2
     + Пароль CLASSIC NAMED
5. На всех маршрутизаторах изменить ограничение по хопам от 100 до 200
6. На маршрутизаторе R9 суммаризировать все loopback маршруты в сторону R10
7. На маршрутизаторе R2 настроить маршрут суммарный маршрут по умолчанию в сторону R1.
8. На маршрутизаторе R2 настроить summary-metric со значениями метрик в 1 , применить ее на маршрут по-умолчанию. После всех произведенных действий добиться, чтобы R1 мог использовать маршрут по-умолчанию.

## [Лабораторная работа по теме 46: QoS. 6.24-6.25 Classification NBAR, L2 QoS](http://ccie.linkmeup.ru/2016/08/15/laboratornaya-rabota-po-teme-46-qos-6-24-6-25-classification-nbar-l2-qos/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B3uwAH0p4u2NWmN1VHFRX3lxZW8) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На R1 настроить полисер следующим образом:
   1. Настроить class map c наименованием Youtube с соответствием NBAR для протокола Youtube
   2. Настроить class map c наименованием Skype с соответствием NBAR для протокола Skype
   3. Настроить policy map c наименованием Youtube\_Skype и следующими настройками:
   4. Ограничить пропускную способностью трафика youtube 1.5 Mbit/sec, TC должен быть 40 мс. Кроме того, можно дополнительно пропускать 1000 байт за интервал, но траффик должен быть перекрашен в dscp 0. Всё, что свыше этого лимита — дропать.
   5. Запретить использование Skype
   6. UPD: Применить на e0/1.12 во входящем направлении
4. На R10 настроить MQC следующим образом:
   1. class map HTTP:
      1. Примерно раз в минуту на роутер приходит 2 разных GET запроса.
      2. Используя NBAR составить одно (!) регулярное выражение, которое будет распознавать запрашиваемые имена файлов (веб-страниц) в GET запросах.
      3. Длина регулярного выражения должна быть меньше 20 символов, не считая кавычек.
      4. Имя файла может находиться, где угодно в URL.
      5. Замечание:
         1. В решении экспертов, счетчик для этого класса растет со скоростью примерно ~8-12 пакетов в минуту.
         2. Embedded Packet Capture может пригодиться
   2. class map ICMP:
      1. Должен распознавать любой ICMP траффик, не используя NBAR.
      2. При этом длина IP пакета должна быть не менее 500 байт и не более 1000 байт.
   3. Настроить policy-map QoS, где траффик класса HTTP будет дропаться, а для класса ICMP будет использован policer с CIR 8 kbps.
   4. Применить на multilink1
5. На R10 дропать все IP пакеты с опциями. Нельзя использовать MQC/ACL.

При необходимости использовать extended ACL, нужно использовать нумерованный ACL, где номер ACL равен RIP holddown timer.

## [Лабораторная работа по теме 47: Auto-install, Menu, banner, alias](http://ccie.linkmeup.ru/2016/08/17/laboratornaya-rabota-po-teme-47-auto-install-menu-banner-alias/)

* 1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfVGVpTlpNNngyOU0) всех устройств.
  2. Для задания используется логическая и физическая топологии проекта.
  3. На маршрутизаторе R1 настроить баннер «No banner to login», который будет появляться до всех остальных сообщений (включая запрос username) на консоли и на vty, при этом:
     + нельзя менять способ аутентификации на консоли и vty
     + несмотря на метод подключения, должен выводиться только один баннер
  4. На маршрутизаторе R1 настроить alias «rib», при вызове которого будет запускаться EEM со следующими свойствами:
     + вывод команды «show clock» будет сохраняться в файле ip\_route.txt, находящийся в корне раздела unix;
     + вывод команды «show ip route» будет сохраняться в том же файле;
     + вывод команды «show ip cef» будет сохраняться в том же файле;
     + ни в одной команде апплета не должно быть строки «ip\_route.txt»
     + файл должен содержать выводы всех комманд. Кроме того, при повторном запуске скрипта все выводы должны записываться в тот же файл, не затирая предыдущие выводы.
     + скрипт должен вывести содержимое файла на экран;
     + после выполнения всех вышеперечисленных действий содержимое файла должно отправляться на основной адрес support@linkmeup.ru smtp сервера 180.1.2.2 от r1@linkmeup.ru, копия должна отправляться на ccie@linkmeup.ru, тема письма должна быть «Data was collected».

## [Лабораторная работа по теме 48: ACL](http://ccie.linkmeup.ru/2016/08/19/laboratornaya-rabota-po-teme-48-acl/)

### Задание #1

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfQTZGclZVaG9WMlU) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3 настроить RIPv2 следующим образом:
   * настроить аннонсирование сетей 180.1.0.0 и 188.1.0.0
   * отключить автоматическую суммаризацию сетей.
   * настроить named ACL с названием «RIP» со следующими настройками:
     + разрешить трафик control-plane, используемый протоколом RIP по-умолчанию.
     + разрешить трафик ICMP для проверки соединения между маршрутизаторами
     + запретить трафик control-plane, используемый другими протоколами IGP .
     + применить на всех интерфейсах, кроме тупиковых
4. На маршрутизаторах R4, R5, R6 настроить протокол EIGRP следующим образом:
   * настроить аннонсирование сетей 180.1.0.0 и 188.1.0.0
   * отключить автоматическую суммаризацию сетей.
   * настроить named ACL с названием «EIGRP», где разрешить трафик control-plane, используемый протоколом EIGRP по-умолчанию:
     + разрешить трафик control-plane, используемый протоколом EIGRP по-умолчанию.
     + разрешить трафик ICMP для проверки соединения между маршрутизаторами
     + запретить трафик control-plane, используемый другими протоколами IGP .
     + применить на всех интерфейсах, кроме тупиковых
5. На маршрутизаторах R7, R8, R9,R10 настроить протокол OSPF следующим образом:
   * Номер процесса 100
   * Подключить все интерфейсы к area 0 одной командой
   * настроить named ACL с названием «OSPF», где разрешить трафик control-plane, используемый протоколом OSPF по-умолчанию:
     + разрешить трафик control-plane, используемый протоколом OSPF по-умолчанию.
     + разрешить трафик ICMP для проверки соединения между маршрутизаторами
     + запретить трафик control-plane, используемый другими протоколами IGP .
     + применить на всех интерфейсах, кроме тупиковых.

### Задание#2

12:53 msk time: На R4 на саб-интерфейс e0/1.456 пропишите адрес 188.1.45.4/24 вместо dhcp.

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfSW5Ba042Z3N4V2M) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На всех маршрутизаторах настроить протокол OSPF следующим образом:
   * Номер процесса 100
   * Подключить все интерфейсы к area 0 одной командой
4. На R5 и R6 настроить HSRP следующим образом:
   * Задать номер группы 456
   * Задать адрес шлюза по умолчанию последний адрес подсети vlan’а 456
   * R5 должен получить роль Active
5. На R5 и R2 настроить VRRP следующим образом:
   * Задать номер группы 235
   * Задать адрес шлюза по умолчанию последний адрес подсети vlan’а 235
   * Указать R2 как Master
6. На R5 и R6 настроить GLBP следующим образом:
   * Задать номер группы 456
   * Задать адрес шлюза по умолчанию предпоследний адрес подсети vlan’а 456
   * настроить named ACL с названием «HSRP\_GLBP»
     + разрешить трафик control-plane, используемый протоколом GLBP по-умолчанию
     + разрешить трафик control-plane, используемый протоколом HSRP по-умолчанию
     + разрешить трафик ICMP для проверки соединения между маршрутизаторами
     + разрешить трафик control-plane, используемый протоколом OSPF по-умолчанию
     + запретить весь остальной трафик
     + применить на интерфейсе, подключенном к R4.
   * На R4 настроить named ACL с названием «HSRP\_GLBP»
     + разрешить трафик control-plane, используемый протоколом GLBP по-умолчанию
     + разрешить трафик control-plane, используемый протоколом HSRP по-умолчанию
     + разрешить трафик control-plane, используемый протоколом OSPF по-умолчанию
     + разрешить трафик ICMP для проверки соединения между маршрутизаторами
     + запретить весь остальной трафик
     + применить на интерфейсе, подключенном к R5 и R6.
7. На R5 настроить ip sla следующим образом:
   * номер ip sla 1 отправляется icmp-echo на адрес 188.1.235.3 с частотой раз в 3 секунды, ждем 1 сек.
   * запустить сразу
   * настроить named ACL с названием «VRRP\_IPSLA» со следующими настройками:
     + разрешить трафик control-plane, используемый IPSLA по-умолчанию
     + разрешить трафик control-plane, используемый протоколом VRRP по-умолчанию
     + разрешить трафик ICMP для проверки соединения между маршрутизаторами
     + разрешить трафик control-plane, используемый протоколом OSPF по-умолчанию
     + запретить весь остальной трафик
     + применить его на интерфейсе, подключенном к R3.
   * На R3 настроить named ACL с названием «VRRP\_IPSLA» со следующими настройками:
     + разрешить трафик control-plane, используемый IPSLA по-умолчанию
     + разрешить трафик control-plane, используемый протоколом VRRP по-умолчанию
     + разрешить трафик ICMP для проверки соединения между маршрутизаторами
     + разрешить трафик control-plane, используемый протоколом OSPF по-умолчанию
     + запретить весь остальной трафик
     + и применить его на интерфейсе, подключенном к R5
8. На R5 Настроить трекинг для ip sla 1:
   * Задать номер 1
   * Настроить reachibility c задержкой на состояние up в 1 минуту
   * Применить к HSRP на R5 с Decrement’ом в 255

# [**Цикл 9**](http://ccie.linkmeup.ru/2016/08/27/tsikl-9-tema-49-ospf-network-types/)

## [Лабораторная работа по теме 49: OSPF Network Types](http://ccie.linkmeup.ru/2016/08/29/laboratornaya-rabota-po-teme-49-ospf-network-types/)

### Задание 1:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfZVd5VVJmZmdwZWc) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. R7 настроить в качестве pppoe сервера следующим образом:
   1. настроить BBA группу следующим образом:
      1. использовать наименование группы «ospf»
      2. закрепить интерфейс Virtual Template 1 к группе
   2. настроить интерфейс Virtual Template следующим образом:
      1. задать номер интерфейса как 1
      2. настроить его таким образом, чтобы он получал ip адрес от loopback 0 интерфейса
      3. интерфейс должен раздавать ip адреса из пула ip адресов диапазоном 10.10.1.1-10.10.1.250, используя IPCP
      4. прикрепить интерфейс к интерфейсу e0/1.144
4. Настроить R2, R3, R4, R6 в качестве клиента pppoe сервера R7 следующим образом:
   1. настроить интерфейс Dialer следующим образом:
      1. задать номер 1
      2. ip адреса интерфейс должен получать от R7
      3. настроить mtu равным 1492
   2. прикрепить интерфейс Dialer 1 к E0/1.144
5. На всех маршрутизаторах настроить протокол OSPF следующим образом:
   1. Номер процесса 100
   2. Подключить все интерфейсы к area 0 одной командой

### Задание 2:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfa1hEc0FnM0lYbDA) всех устройств.
2. Для задания используется логическая и физическая топологии проекта и конфигурация предыдущего задания.
3. На R7 настроить тип сети ospf как Point-to Multipoint.
4. R2, R3, R4, R6 должны образовать соседство с R7. При этом должны выполняться следующие условия:
   1. на маршрутизаторах нельзя менять тип сети ospf
   2. на маршрутизаторах нельзя менять ip адреса
   3. маршрутизаторы должны получать большинство маршрутов от R7.

## [Лабораторная работа по теме 50: DHCP 9.3](http://ccie.linkmeup.ru/2016/08/31/laboratornaya-rabota-po-teme-50-dhcp-9-3/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxV25LTnRBUmhsTGc) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На R5 и R6 настроить VRRP cледующим образом:
   1. R6 будет играть роль основного:
      1. номер группы для VRRP задать как сумму номеров портов, используемых клиентом при отправке сообщения DHCPDISCOVER;
      2. задать приоритет, который равен номеру протокола, используемый VRRP;
      3. настроить аутентификацию с использованием key-chain ключа под названием VRRP и паролем VRRP\_P@ss;
      4. в качестве ip адреса использовать последний адрес подсети влана 456
   2. R5 настроить как бэкапный:
      1. номер группы для VRRP задать как сумму номеров портов, используемых клиентом при отправке сообщения DHCPDISCOVER;
      2. приоритет оставить по-умолчанию;
      3. настроить аутентификацию с использованием key-chain ключа под названием VRRP и паролем VRRP\_P@ss;
      4. в качестве ip адреса использовать последний адрес подсети влана 456
4. Настроить R7 в качестве dhcp сервера следующим образом:
   1. Использовать пул адресов сети 188.1.34.0/24 под названием R3
   2. в качестве шлюза по-умолчанию использовать ip адрес, используемый в VRRP R5 и R6
   3. настроить время аренды неограниченным
5. Настроить R3 таким образом, чтобы он получал ip адрес по DHCP от сервера через R4.

## [Лабораторная работа по теме 51: EIGRP 3.5](http://ccie.linkmeup.ru/2016/09/02/laboratornaya-rabota-po-teme-51-eigrp-3-5/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxVXRkbWZHclMxQWs) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R6, R7, R8, R9,R10 настроить classic mode EIGRP следующим образом:
   1. Номер автономной системы 100
   2. Аннонсировать сети 188.1.0.0 и 180.1.0.0
   3. Увеличить значение таймеров hello и hold на 2 по сравнению со значением по-умолчанию на интерфейсах, подключенных к соседям в Classic Mode.
   4. Значение таймеров на маршрутизаторах между Classic Mode и Named mode оставить без изменений.
4. На маршрутизаторах R1, R2, R3, R4, R5 настроить Named mode EIGRP следующим образом:
   1. Имя NAMEDEIGRP
   2. Номер автономной системы 100
   3. Аннонсировать сети 188.1.0.0 и 180.1.0.0
   4. Увеличить значение таймеров hello и hold в 2 раз по сравнению со значением по-умолчанию на интерфейсах, подключенных к соседям, подключенных к соседям в Named Mode
   5. Значение таймеров на маршрутизаторах между Classic Mode и Named mode оставить без изменений.
5. На всех маршрутизаторах изменить ограничение по хопам от 100 до 200
6. Между R9 и R10 настроить bfd со следующими свойствами:
   1. интервалом между bfd пакетами в 250 миллисекунд, минимальный интервал приема 250 миллисекунд, multiplayer 3
   2. Применить в автономной системе 100
7. На интерфейсе E0/1.235 R3 настроить полосу пропускания для eigrp значением в 10%
8. На R3 настроить NSF таймер, уменьшив значение по умолчанию в 3 раза
9. Настроить R1 и R10 в качестве тупиковых маршрутизаторов, при этом они должны адвертайзить Connected, Static и Summary маршруты.

## [Лабораторная работа по теме 52: Protocol Independent IPv4 Routing 3.1](http://ccie.linkmeup.ru/2016/09/05/laboratornaya-rabota-po-teme-52-protocol-independent-ipv4-routing-3-1/)

* Ребята, чтобы не было проблем с адресацией, добавьте, пожалуйста, no ip address в секцию интерфейса ethernet0/1

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxM0JmVC1Hc1BjLVE) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R6, R7, R8, R9,R10 настроить classic mode EIGRP следующим образом:
   1. Номер автономной системы 200
   2. Аннонсировать сети 188.1.0.0 и 180.1.0.0
4. На маршрутизаторах R1, R2, R3, R4, R5 настроить Named mode EIGRP следующим образом:
   1. Имя NAMEDEIGRP
   2. Номер автономной системы 200
   3. Аннонсировать сети 188.1.0.0 и 180.1.0.0
5. На всех маршрутизаторах изменить ограничение по хопам от 100 до 200
6. На R2 и R9 настроить GRE туннель под номером 29 следующим образом:
   1. В качестве источника использовать Loopback0 интерфейсы устройств
   2. ip адрес на R2 указать 10.10.10.2/24, на R9- 10.10.10.9/24
7. На R3 и R7 настроить IP in IP туннель под номером 73 следующим образом:
   1. В качестве источника на R3 использовать ip адрес интерфейса E0/1.34, в качестве назначения использовать ip адрес интерфейса E0/1.67 на R7
   2. В качестве источника на R7 использовать ip адрес интерфейса E0/1.67, в качестве назначения использовать ip адрес интерфейса E0/1.34 R3
   3. ip адрес на R3 указать 73.0.0.3/24, на R7- 73.0.0.7/24

## [Лабораторная работа по теме 53: Miscellaneous System Management](http://ccie.linkmeup.ru/2016/09/07/laboratornaya-rabota-po-teme-53-miscellaneous-system-management/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfaTVlZFkwM0EycmM) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На R2 настроить телнет следующим образом:
   1. создать локального пользователя под именем TelAdmin c привилегией 15 и с шифрованным паролем TeLneT. Включить ААА.
   2. создать authentication list под названием TELNET c использованием локальной базы пользователей. Применить на терминальной линии.
   3. Настроить R2 таким образом, что если он обнаружит неактивную сессию телнет, он сбросит ее.
4. На R9 настроить debug сообщения таким образом, чтобы они показывали сообщения только с интерфеса Multilink1. Приложите вывод команды show debug в решение.

# 

## [Лабораторная работа по теме 54: Data Plane Security](http://ccie.linkmeup.ru/2016/09/10/laboratornaya-rabota-po-teme-54-data-plane-security/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxWTRpUk1MaWNTU0k) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На R2 настроить телнет следующим образом:
   1. создать подключения для пары username/password TempAccess/TemP:
      1. Разрешить временный доступ пользователю TempAccess на 60 минут с диапазона адресов 188.1.34.4/24 на интерфейс E0/1.235 маршрутизатора R2;
      2. Если со стороны TempAccess не будет активности в течении 1 минуты, сессия должна закрываться.
   2. создать подключения для пары username/password Teleworker/TeleworK:
      1. Разрешить временный доступ пользователю Teleworker в период с 22.00 по 06.00 на ежедневной основе с адреса Loopback 0 маршрутизатора R5 на интерфейс E0/1.235 маршрутизатора R2;
4. На R2 настройте ACL с фразой «fragment» для протокола eigrp следующим образом:
   1. разрешить прохожение фрагменитрованных и нефрагменитрованных пакетов

# 

# [**Цикл 10**](http://ccie.linkmeup.ru/2016/09/09/tsikl-9-tema-55-lsa-types-ospf-next-hop-processing-unicast-vs-multicast-hellos/)

## [Лабораторная работа по теме 55: OSPF 3.6](http://ccie.linkmeup.ru/2016/09/12/laboratornaya-rabota-po-teme-55-ospf-3-6/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfbkFtUFFHRkdaTms) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Настроить маршрутизаторы R4, R5, R6 таким образом, чтобы следующие интерфейсы находились в Area 0 :
   1. Номер ospf процесса 100
   2. R4 — интерфейсы Loopback 0 и E0/1.456
   3. R5 — интерфейсы Loopback 0, E0/1.456, E0/1.5
   4. R6 — интерфейсы Loopback 0, E0/1.456, E0/1.6
4. Настроить маршрутизаторы R1, R2, R3, R4, R5 таким образом, чтобы следующие интерфейсы находились в Area 15 :
   1. Номер ospf процесса 100
   2. все интерфейсы R2, R3
   3. R1 — интерфейс E0/1.12
   4. R4 — интерфейс E0/1.34
   5. R5 — интерфейс E0/1.235
5. Настроить маршрутизаторы R6, R7, R8, R9, R10 таким образом, чтобы следующие интерфейсы находились в Area 107 :
   1. Номер ospf процесса 100
   2. все интерфейсы R7, R8, R9, R10
   3. R6 — интерфейс E0/1.67
6. Настроить маршрутизатор R1 таким образом, чтобы интерфейс Loopback 0 автономной системе EIGRP 100. Редистрибьютить его в ospf.

## [Лабораторная работа по теме 56: DHCP 9.3](http://ccie.linkmeup.ru/2016/09/14/laboratornaya-rabota-po-teme-56-dhcp-9-3/)

Задание 1:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfSktjRmpFTVlINFk) R1 и R2.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1 и R2 настроить инкапсуляцию PPP
4. R2 настроить следующим образом:
   1. R1 должен получать ip адрес 188.1.12.1 через IPCP
   2. R1 должен получать маску подсети /24 через IPCP
5. Настроить R1 следующим образом:
   1. Настроить DHCP pool под названием ONDEMAND
   2. Пул ONDEMAND должен импортировать маску подсети, которую он получает от R2

Задание 2:

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfR3Y4WlJONmV2MDQ) R4, R5, R6, SW1, SW2, SW3, SW4
2. Для задания используется логическая и физическая топологии проекта.
3. R4 настроить в качестве DHCP сервера следующим образом:
   1. Настроить DHCP pool под названием ARP
   2. Пул должен сосоять из диапазона адресов 188.1.45.0/24
   3. Всякий раз при получении DHCP Discover, R4 должен устанавливать безопасную ARP запись.
   4. Должен отправлять ARP сообщения каждые 30 секунд
4. R5 настроить в качестве DHCP клиента.
5. Попробовать отправить пинг с R6 на R4.
6. Настроить статическую запись ARP для R6

## [Лабораторная работа по теме 57: EIGRP 3.5](http://ccie.linkmeup.ru/2016/09/16/laboratornaya-rabota-po-teme-57-eigrp-3-5/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxU0ZKMU55YWxfUGM) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R6, R7, R8, R9,R10 настроить classic mode EIGRP следующим образом:
   1. Номер автономной системы 100
   2. В автономной системе 100 eigrp на маршрутизаторах должны анонсироваться только те префиксы, которые настроены на интерфейсах согласно топологии
4. На маршрутизаторах R1, R2, R3, R4, R5 настроить Named mode EIGRP следующим образом:
   1. Имя NAMEDEIGRP
   2. В автономной системе 100 eigrp на маршрутизаторах должны анонсироваться только те префиксы, которые настроены на интерфейсах согласно топологии
5. На всех маршрутизаторах изменить ограничение по хопам от 100 до 200
6. Настроить R2 следующим образом:
   1. Он должен принимать префиксы на интерфейсы E0/1.23 и E0/1.12
   2. Он не должен приниматься префиксы на интерфейс E0/1.235, при это он должен аннонсировать 188.1.235.0
   3. Нельзя использовать access-list, distribute-list, route-map, distance
7. На R3 настроить prefix-list следующим образом:
   1. Он не должен принимать префиксы от Loopback интерфейсов других маршрутизаторов
   2. Он должен разрешить транзитные сети других маршрутизаторов
   3. Применить к eigrp процессу
8. Настроить R10 следующим образом
   1. метрика от маршрута 188.1.9.0 при заходе на интерфейс Multilink 1 увеличивалась на 100
   2. нельзя использовать команду metric

## [Лабораторная работа по теме 58: IPsec LAN-to-LAN 4,2](http://ccie.linkmeup.ru/2016/09/19/laboratornaya-rabota-po-teme-58-ipsec-lan-to-lan-4-2/)

1. Для задания используется логическая и физическая топологии проекта.
2. На маршрутизаторах R9 и R2 настроить политику ISAKMP следующим образом:
   1. Номер политики 10
   2. Настроить аутентификацию PSK c паролем IPsec, в качестве адресов указать IP адреса Loopback интерфейсов.
   3. Настроить шифрование AES с длиной ключа, равной первым 8 битам IP адресов класса «С» в десятичной системе измерения.
   4. Настроить DH под номером 5
   5. Настроить hash — SHA 384
3. На маршрутизаторах R9 и R2 настроить Crypto Map следующим образом:
   1. Название Cryp\_Map с порядковым номером 10 и политикой ISAKMP
   2. В качестве пира указать ip адреса Loopback интерфейсов.
   3. в качестве источника указать ip адреса Loopback интерфейсов.
4. Настроить расширенный ACL следующим образом:
   1. Название R1\_R10
   2. Разрешить трафик идущий от R1 к R10 и обратно
5. Применить ACL к Crypto Map
6. Настроить Transform Set следующим образом:
   1. Название — ESP\_AES\_192\_SHA1
   2. Настроить политику согласно названию
   3. режим — оставить по-умолчанию
7. Применить Transform Set к Crypto Map
8. Применить Crypto Map к исходящим интерфейсам от R2 к R9 и в обратную сторону.
9. Проверить работу туннеля

## [Лабораторная работа по теме 59: Miscellaneous System Management 8.5](http://ccie.linkmeup.ru/2016/09/21/laboratornaya-rabota-po-teme-59-miscellaneous-system-management-8-5/)

Задание

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxNWdmRUp2UFFVUHM) устройств.
2. Для задания используется физическая топологии проекта.
3. На маршрутизаторах R1 и R5 настроить buffer tuning следующим образом:
   1. Public Buffer Pool:
      1. Small buffers initial = 250, min-free, max-free и permanent до соответствующих показателей в Middle buffers
4. Решить проблему cdp на SW1 и SW5
5. Настроить на R5 доступ по Remote Shell следующим образом:
   1. Настроить ACL, где разрешить доступ ip 10.0.0.1
   2. Привязать ACL к RSH
   3. Создать пару пользователь/пароль R1/RSH с привелегией 15
6. Попробовать подключиться через RSH

## [Лабораторная работа по теме 60: Data Plane Security 7.4](http://ccie.linkmeup.ru/2016/09/23/laboratornaya-rabota-po-teme-60-data-plane-security-7-4/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxZnF1ZkJ4bkFteWs) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На граничных маршрутизаторах между EIGRP NAMED и CLASSIC Mode настроить NBAR для ограничения Smurf трафика следующим образом:
   1. Настроить ACL под названием AntiSmurf и применить следующие настройки:
      1. разрешить ICMP ECHO в обе стороны
      2. разрешить ICMP ECHO Reply в обе стороны
   2. Настроить Class-map под названием AnySmurf и применить следующие настройки:
      1. привязать его к ACL AntiSmurf
   3. Настроить Policy-map под названием MarkSmurf и применить следующие настройки::
      1. привязать его к Class-map AnySmurf
      2. установить DSCP раной 1
   4. Настроить Class-map под названием SmurfMarked и применить следующие настройки:
      1. привязать его к DSCP 1
   5. Настроить Policy-map под названием LimitSmurf и применить следующие настройки::
      1. привязать его к Class-map SmurfMarked
      2. настроить политику где ICMP-трафик ограничен средней пропускной способностью 64 кбит, с всплеском 4 кбайта. Если какой-либо из этих пределов превышен, то политика должна отбросить эти избыточные сообщения ICMP.
   6. Применить Policy-map MarkSmurf на интерфейсах между EIGRP NAMED и CLASSIC Mode.
   7. Применить Policy-map LimitSmurf на интерфейсах, смотрящих в сторону маршрутизаторов локального режима
4. На маршрутизаторе R9 настроить TCP Intercept в Watch Mode следующим образом:
   1. Настроить ACL под названием TCPINT и применить следующие настройки:
      1. разрешить трафик по портам 25 и 80
   2. Настроить изменение таймеров:
      1. Максимальное время ожидания окончания three-way handshake в Watch Mode 400 секунд
      2. Максимальное время ожидания пакетов с флагами RST или FIN 50 секунд
      3. Максимальное время управления сессией 30 часов
      4. Указать значение максимального порога для начала сбрасывания неполных соединений в 400 и минимального значения в 300
      5. Указать максимальное значение для ожидания неполных соединений в период 1-ой минуты в 80, а минимальной в 50
      6. Настроить Drop Mode случайным образом
5. На маршрутизаторе R3 настроить uRPF следующим образом:
   1. Настроить ACL под номером 100 и применить следующие настройки:
      1. запретить ip адрес интерфейса E0/1.235 R5, все данные должны писаться в лог
      2. разрешить ip адрес интерфейса E0/1.235 R2, все данные должны писаться в лог
   2. Применить ACL 100 совместно с uRPF на интерфесе E0/1.235

# [**Цикл 11**](http://ccie.linkmeup.ru/2016/09/30/tsikl-11-tema-61-ospf-3-6/)

## [Лабораторная работа по теме 61: OSPF 3.6](http://ccie.linkmeup.ru/2016/10/03/laboratornaya-rabota-po-teme-61-ospf-3-6/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxbXQ2a1lJMm9WR2s) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Настроить маршрутизаторы R4, R5, R6 таким образом, чтобы следующие интерфейсы находились в Area 0 :
   1. Номер ospf процесса 100
   2. R4 — интерфейсы Loopback 0 и E0/1.456
   3. R5 — интерфейсы Loopback 0, E0/1.456, E0/1.5
   4. R6 — интерфейсы Loopback 0, E0/1.456, E0/1.6
4. Настроить маршрутизаторы R2, R3, R4, R5 таким образом, чтобы следующие интерфейсы находились в Area 15 :
   1. Номер ospf процесса 100
   2. R2- интерфейсы E0/1.23, E0/1.235
   3. все интерфейсы R3
   4. R4 — интерфейс E0/1.34
   5. R5 — интерфейс E0/1.235
5. Настроить маршрутизаторы R6, R7, R8, R9, R10 таким образом, чтобы следующие интерфейсы находились в Area 107 :
   1. Номер ospf процесса 100
   2. все интерфейсы R7, R8, R9, R10
   3. R6 — интерфейс E0/1.67
6. Настроить маршрутизаторы R1, R2 таким образом, чтобы следующие интерфейсы находились в Area 10 :
   1. Номер ospf процесса 100
   2. R1- интерфейс E0/1.12
   3. R2- интерфейс E0/1.12
7. Настроить маршрутизатор R1 таким образом, чтобы интерфейс Loopback 0 находился в процессе EIGRP 100. Редистрибьютить его в ospf.
8. Поменять полосу пропускания на интерфейсе Multilink1 R9 таким образом, чтобы метрика в таблице маршрутизации на R8 до 180.1.10.10 стала равной 12.
9. На R8 применить auto-cost таким образом, чтобы метрика в таблице маршрутизации на R2 до 180.1.10.10 стала равной последнему октету ip адреса протокола GLBP.
10. Решить проблему получения маршрутов маршрутизатором R1 стандартным для OSPF способом.

## [Лабораторная работа по теме 62: DNS 9.4](http://ccie.linkmeup.ru/2016/10/06/laboratornaya-rabota-po-teme-62-dns-9-4/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxR0VlRDZVSDVaYjQ) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Настроить марштрутизатор R7 в качестве DHCP сервера следующим образом:
   1. Он должен отдавать диапазон сети 188.1.34.0/24
   2. В качестве ip адреса маршрута по-умолчанию должен быть взят ip адрес Loopback интерфейса R5
   3. В качестве DNS указать [ccie.linkmeup.ru](http://ccie.linkmeup.ru/)
4. Настроить R8 качестве клиента DNS сервера R9 следующим образом:
   1. В качестве IP адреса сервера задать IP адрес адрес Loopback интерфейса R9
   2. При пинге потере связи с R9, R8 должен отвечать на все запросы DNS от других ip адресом своего Loopback интерфейса
5. Настроить R9 в качестве DNS сервера следующим образом:
   1. Имя домена [ccie.linkmeup.ru](http://ccie.linkmeup.ru/)
6. Настроить R3 в качестве DHPC клиента R7 и DNS клиента R8
7. Настроить все остальные маршрутизаторы в качестве DNS клиентов R8

## [Лабораторная работа по теме 63: EIGRP 3.5](http://ccie.linkmeup.ru/2016/10/07/laboratornaya-rabota-po-teme-63-eigrp-3-5/)

Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxcVpvNzNVUkdxNkU) всех устройств.

1. Для задания используется логическая и физическая топологии проекта.
2. Создать Route Map TAG следующим образом:
   1. применить метрику 1 1 1 1 1
   2. применить тег со значением 1
3. На маршрутизаторе R1 редистрибьютить ip адрес интерфейса Loopback 0 следующим образом:
   1. использовать процесс EIGRP 100
   2. использовать route-map с наименованием TAG
4. Префикс Ip адреса интерфейса Loopback 0 R1 не должен распространяться дальше R7. Нельзя использовать при этом ACL, prefix листы. Разрешить все остальные маршруты.
5. На R3 измените настройки так, чтобы AD для всех маршрутов стало равной 50
6. На R6 измените настройки так, чтобы AD для всех маршрутов, приходящих от R4 и R5 стало равной 30

## [Лабораторная работа по теме 64: IPsec LAN-to-LAN 4.2](http://ccie.linkmeup.ru/2016/10/10/laboratornaya-rabota-po-teme-64-ipsec-lan-to-lan-4-2/)

[Начальные конфиги](https://drive.google.com/open?id=0B8TdfSzCKkaxa2hJczZNQ19ubFE) для обоих заданий

### Задание №1

1. Для задания используется логическая и физическая топологии проекта.
2. На R2 настроить GRE туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R2
   2. В качестве назначения использовать Loopback интерфейс R9
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.2/24
   4. Настроить OSPF процесс 100 в Ареа 0 на интерфейсе туннеля и E0/1.12
3. На R9 настроить туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R9
   2. В качестве назначения использовать Loopback интерфейс R2
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.9/24
   4. Настроить OSPF процесс 100 в Ареа 0 на интерфейсах туннеля и Multilink1
4. Настроить OSPF процесс 100 в Ареа 0 на всех интерфейсах маршрутизаторов R1 и R10 одной командой
5. Настроить фазу 1 IPsec на R2 и R9 следующим образом:
   1. Номер политики 10
   2. Шифрование 3 DES
   3. Хэш MD5
   4. Аутентификация PSK
   5. Diffie-Hellman 5
   6. Для аутентификации пароль брать из названия используемого протокола инкапсуляции VTI, необходимо привязать его к 32-битному адресу пира
6. Настроить фазу 2 IPsec на R2 и R9 следующим образом:
   1. В ACL под названием GRE разрешить все GRE пакеты
   2. Создать Transform Set под названием ESP\_AES\_SHA:
      1. в качестве протокола использовать ESP
      2. в качестве аутентификации использовать HMAC SHA1
   3. Создать Crypto Map под названием GRE\_IPSEC:
      1. будет матчить ACL под названием GRE
      2. будет использовать Transform Set под названием ESP\_AES\_SHA
      3. в качестве пира будет использовать Loopback адреса R2, R9
      4. в качестве локального адреса указать Loopback адреса R2, R9
7. На R2 и R9 применить Crypto Map на следующих интерфесах
   1. R2 — E0/1.23 и E0/1.235
   2. R9 — E0/1.89
8. На интерфейсе Tunnel 0 R2 и R9 изменить значение MTU до 1400 байт и настроить TCP Adjust MSS до 1360

### Задание №2

1. Для задания используется логическая и физическая топологии проекта.
2. На R2 настроить туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R2
   2. В качестве назначения использовать Loopback интерфейс R9
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.2/24
   4. Настроить OSPF процесс 100 в Ареа 0 на интерфейсе туннеля и E0/1.12
3. На R9 настроить туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R9
   2. В качестве назначения использовать Loopback интерфейс R2
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.9/24
   4. Настроить OSPF процесс 100 в Ареа 0 на интерфейсах туннеля и Multilink1
4. Настроить OSPF процесс 100 в Ареа 0 на всех интерфейсах маршрутизаторов R1 и R10 одной командой
5. Настроить фазу 1 IPsec на R2 и R9 следующим образом:
   1. Номер политики 10
   2. Шифрование 3 DES
   3. Хэш MD5
   4. Аутентификация PSK
   5. Diffie-Hellman 5
   6. Для аутентификации пароль брать из названия используемого протокола инкапсуляции VTI, необходимо привязать его к 32-битному адресу пира
6. Настроить фазу 2 IPsec на R2 и R9 следующим образом:
   1. Создать Transform Set под названием ESP\_AES\_SHA:
      1. в качестве протокола использовать ESP
      2. в качестве аутентификации использовать HMAC SHA1
   2. Создать IPSec Profile под названием VTI\_IPSEC:
      1. будет использовать Transform Set под названием ESP\_AES\_SHA
      2. в качестве пира будет использовать Loopback адреса R2, R9
      3. в качестве локального адреса указать Loopback адреса R2, R9
7. На R2 и R9 изменить режим интерфеса Tunnel 0 c GRE на IPSEC IPv4 и применить IPSec Profile VTI\_IPSEC

## [Лабораторная работа по теме 65: Protocol Independent IPv4 Routing 3.1](http://ccie.linkmeup.ru/2016/10/13/laboratornaya-rabota-po-teme-65-protocol-independent-ipv4-routing-3-1/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxbGdYX2xWNzd0SFE) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На R3 настроить GRE туннель следующим образом:
   1. В качестве источника туннеля использовать Looback интерфейс R3
   2. В качестве назначения использовать Looback интерфейс R7
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.3/24
   4. Настроить OSPF процесс 144 в Ареа 0 на интерфейсе туннеля и E0/1.23
4. На R7 настроить туннель следующим образом:
   1. В качестве источника туннеля использовать Looback интерфейс R7
   2. В качестве назначения использовать Looback интерфейс R3
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.7/24
   4. Настроить OSPF процесс 144 в Ареа 0 на интерфейсах туннеля и E0/1.78
5. Настроить R8 в качестве DNS сервера для R7 следующим образом:
   1. настроить dns resolving для хоста [R8.ccie.linkmeup.ru](http://r8.ccie.linkmeup.ru/), используя адреса 180.1.8.8 188.1.78.8
6. Настроить R7 в качестве DNS сервера для R3, перенаправляя DNS запросы к R8
7. Настроить IP SLA под номером 1 следующим образом:
   1. IP SLA должен отправлять DNS запросы на [R8.ccie.linkmeup.ru](http://r8.ccie.linkmeup.ru/), используя в качестве источника пару IP Address/ Port Number — 188.1.34.3/4500
8. Настроить трэкинг IP SLA 1 следующим образом:
   1. Reachability
   2. Если в Down’e ждать 10 секунд
   3. Если в Up’e ждать 5 секунд
9. На R7 редистрибьютить OSPF маршруты в EIGRP c метрикой 1 1 1 1 1
10. Настроить R4, R5 одной командой таким образом, чтобы внешние маршруты, пришедшие из OSPF отображались в таблице маршрутизации
11. Настроить работу R3 следующим образом:
    1. Интерфейс E0/1.34 должен быть включен
    2. Интерфейс E0/1.235 должен быть выключен и использован в качестве бэкапного.
    3. создать аплет BackupPath, который будет отправлять сообщение «Main path is no longer reachable» и включать интерфейс E0/1.235 если пропадет линк на интерфейсе E0/1.34. После включения интерфейса E0/1.235 должно отправляться сообщение «Failed over E0/1.34» . Апплет должен реагировать на изменение сообщений трекинга IP SLA 1
    4. создать аплет MainPath, который при будет отправлять сообщение «Main path has been restored», если поднимется линк на интерфейсе E0/1.34 , при этом интерфейс E0/1.235 отключится и отправится сообщение «Returned traffic over E0/1.34»

## [Лабораторная работа по теме 66: Data Plane Security 7.4](http://ccie.linkmeup.ru/2016/10/15/laboratornaya-rabota-po-teme-66-data-plane-security-7-4/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfTE5zLXlfSzlsejQ) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На R2 настроить GRE туннель следующим образом:
   1. В качестве источника туннеля использовать Looback интерфейс R2
   2. В качестве назначения использовать Looback интерфейс R9
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.2/24
   4. Настроить OSPF процесс 100 в Ареа 0 на интерфейсе туннеля и E0/1.12
4. На R9 настроить туннель следующим образом:
   1. В качестве источника туннеля использовать Looback интерфейс R9
   2. В качестве назначения использовать Looback интерфейс R2
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.9/24
   4. Настроить OSPF процесс 100 в Ареа 0 на интерфейсах туннеля и Multilink1
5. Настроить OSPF процесс 100 в Ареа 0 на всех интерфейсах маршрутизаторов R1 и R10 одной командой
6. Настроить фазу 1 IPsec на R2 и R9 следующим образом:
   1. Номер политики 10
   2. Шифрование 3 DES
   3. Хэш MD5
   4. Аутентификация PSK
   5. Diffie-Hellman 5
   6. Источником для пароля GRE должен служить Loopback адрес
7. Настроить фазу 2 IPsec на R2 и R9 следующим образом:
   1. Настроить ACL следующим образом :
      1. название — GRE
      2. разрешить все GRE пакеты
      3. Настроить логирование для отображением интерфейса в сообщении
      4. Настроить частоту генерирования syslog сообщения через каждые 100 в пакетов
      5. Настроить ограничение пакетов в process switching в 100 пакетов в секунду
   2. Создать Transform Set под названием ESP\_AES\_SHA:
      1. в качестве протокола использовать ESP
      2. в качестве аутентификации использовать HMAC SHA1
      3. в качестве алгоритма шифрования использовать AES
   3. Создать Crypto Map под названием GRE\_IPSEC:
      1. будет матчить ACL под названием GRE
      2. будет использовать Transform Set под названием ESP\_AES\_SHA
      3. в качестве пира будет использовать Loopback адреса R2, R9
      4. в качестве локального адреса указать Loopback адреса R2, R9
8. На R2 и R9 применить Crypto Map на следующих интерфесах
   1. R2 — E0/1.23 и E0/1.235
   2. R9 — E0/1.89
9. Настроить RITE на R2 следующим образом:
   1. Настроить ACL для матчинга трафика, идущего с ip адреса пира GRE тунеля
   2. Настроить профиль следующим образом:
      1. Название GRE
      2. исходящий интерфейс для экспорта трафика Ethernet0/1.12
      3. в качестве мак-адреса использовать мак-адрес R1
      4. Включить выборку экспортируемого трафика на каждые 5 пакетов
      5. Применить профиль на интерфейсе Tunnel 0
10. Настроить ACL на R9 следующим образом:
    1. Название DROP\_OPTION
    2. Запретить опции Traceroute и Timestamp
    3. Разрешить весь остальной трафик
    4. Применить на интерфейсе Tunnel 0

# [**Цикл 12**](http://ccie.linkmeup.ru/2016/10/16/tsikl-12-tema-67-ospf-authentication/)

## [Лабораторная работа по теме 67: OSPF 3.6](http://ccie.linkmeup.ru/2016/10/17/laboratornaya-rabota-po-teme-67-ospf-3-6/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxbWl6WGw5STY2YU0) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R6, R7 настроить classic mode EIGRP следующим образом:
   1. Номер автономной системы 100
   2. На R6 интерфейсы должны анонсировать все префиксы :
   3. На R7 только E0/1.67 и Loopback 0 интерфейсы должны участвовать в процессе EIGRP
   4. Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам Classic Mode следующим образом:
      1. Название ключа CLASSIC
      2. Номер ключа 1
      3. Пароль CLASSIC
   5. Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам Named Mode следующим образом:
      1. Название ключа CLASSIC\_NAMED
      2. Номер ключа 1
      3. Пароль CLASSIC\_NAMED
4. На маршрутизаторах R2, R3, R4, R5 настроить Named mode EIGRP следующим образом:
   1. Имя NAMEDEIGRP
   2. На R5 и R4 интерфейсы должны анонсировать все префиксы :
   3. На R2 и R3 E0/1.235 и Loopback 0 интерфейсы должны участвовать в процессе EIGRP
   4. Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам с Named Mode следующим образом:
      1. Пароль NAMED
   5. Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам с Classic Mode следующим образом:
      1. Название ключа CLASSIC\_NAMED
      2. Номер ключа 1
      3. Пароль CLASSIC\_NAMED
5. На R3 настроить GRE туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R3
   2. В качестве назначения использовать Loopback интерфейс R7
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.3/24
   4. Настроить OSPF процесс 100 в Ареа 0 на интерфейсе туннеля
6. На R7 настроить туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R7
   2. В качестве назначения использовать Loopback интерфейс R3
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.7/24
   4. Настроить OSPF процесс 100 в Ареа 0 на интерфейсе туннеля
7. Настроить фазу 1 IPsec на R3 и R7 следующим образом:
   1. Номер политики 10
   2. Шифрование 3 DES
   3. Хэш MD5
   4. Аутентификация PSK
   5. Diffie-Hellman 5
   6. Источником для пароля «GRE» должен служить Loopback адрес
8. Настроить фазу 2 IPsec на R3 и R7 следующим образом:
   1. В ACL под названием GRE разрешить все GRE пакеты
   2. Создать Transform Set под названием ESP\_AES\_SHA:
      1. в качестве протокола использовать ESP
      2. в качестве аутентификации использовать HMAC SHA1
   3. Создать Crypto Map под названием GRE\_IPSEC:
      1. будет матчить ACL под названием GRE
      2. будет использовать Transform Set под названием ESP\_AES\_SHA
      3. в качестве пира будет использовать Loopback адреса R3, R7
      4. в качестве локального адреса указать Loopback адреса R3, R7
9. На R3 и R7 применить Crypto Map на следующих интерфейсах
   1. R3 — E0/1.34 и E0/1.235
   2. R7 — E0/1.67
10. На R7, R8, R9, R10 Настроить OSPF процесс 100 в Ареа 107 на следующих интерфейсах:
    1. R7- E0/1.78
    2. R8- E0/1.78, E0/1.89, Loopback 0
    3. R9 — E0/1.9, E0/1.89, Loopback 0, Mul1
    4. R10 — Mul1
    5. Между маршрутизаторами настроить тип аутентификации Type 0
11. На R1, R2, R3 Настроить OSPF процесс 100 в Ареа 103 на следующих интерфейсах:
    1. R1- E0/1.12
    2. R2- E0/1.12, E0/1.23, Loopback 0,
    3. R3 — E0/1.23
    4. Между маршрутизаторами настроить тип аутентификации Type 1
12. На R10 настроить OSPF процесс 100 в Ареа 10 на следующих интерфейсах:
    1. R10- Loopback 0
13. Настроить Virtual Link к Area 0 следующим образом:
    1. На R7 в сторону R10
    2. На R10 в сторону R7
    3. На Virtual Link настроить аутентификацию следующим образом:
       1. На R7 — глобально
       2. На R10 — на Virtual Link
       3. Применить пароль VIRTUAL
       4. Настроить тип аутентификации на Virtual Link Type 2
14. На интерфейсе Tunnel 0 настроить тип аутентификации следующим образом:
    1. Название ключа OSPF\_TUNNEL
    2. Номер ключа 1
    3. Пароль SHA256
    4. алгоритм SHA256

## [Лабораторная работа по теме 68: NAT 9.5](http://ccie.linkmeup.ru/2016/10/20/laboratornaya-rabota-po-teme-68-nat-9-5/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfcFhwUTd5Y0IwWmM) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Для связности в начальной конфигурации настроен протокол OSPF.
4. На R3 настроить GRE туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R3
   2. В качестве назначения использовать Loopback интерфейс R7
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.3/24
   4. Настроить OSPF процесс 100 в Ареа 144 на интерфейсе туннеля
5. На R7 настроить туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R7
   2. В качестве назначения использовать Loopback интерфейс R3
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.7/24
   4. Настроить OSPF процесс 100 в Ареа 144 на интерфейсе туннеля
6. Настроить Virtual Link на R7 в сторону R6 и обратно
7. Настроить R10 в качестве DNS сервера для всех маршрутизаторов следующим образом:
   1. настроить dns resolving для хоста R10 , используя адреса 180.1.10.10
8. Настроить R7 в качестве DNS сервера для маршрутизаторов, который будет перенаправлять DNS запросы к R10 при обращении к 10.10.10.10
9. Настроить R6 в качестве DNS сервера для маршрутизаторов следующим образом, который будет отвечать на DNS запросы к 180.1.6.6:
   1. настроить dns resolving для хоста R6 , используя адреса 180.1.6.6
10. Настроить на R2 IP SLA под номером 1 следующим образом:
    1. IP SLA должен отправлять DNS запросы на R10
11. Настроить на R7 Static NAT следующим образом:
    1. inside адрес 180.1.10.10 должен транслироваться в outside 10.10.10.10
    2. применить на интерфейсах:
       1. Out- E0/1.67, Tunnel 0
       2. In — E0/1.78
    3. Решить проблему с маршрутизацией транслируемых адресов при помощи статического маршрута.
12. Настроить на R3 NAT c Route Map следующим образом:
    1. Настроить ACL под названием DNS\_R10:
       1. разрешить диапазон адресов 180.1.0.0/16 к хосту 10.10.10.10
       2. разрешить диапазон адресов 188.1.0.0/16 к хосту 10.10.10.10
    2. Настроить ACL под названием DNS\_R6:
       1. разрешить диапазон адресов 180.1.0.0/16 к хосту 180.1.6.6
       2. разрешить диапазон адресов 188.1.0.0/16 к хосту 180.1.6.6
    3. Настроить Route Map под названием DNS\_R10:
       1. при совпадении адреса из ACL DNS\_R10 устанавливать интерфейс Tunnel0
    4. Настроить Route Map под названием DNS\_R6:
       1. при совпадении адреса из ACL DNS\_R6 устанавливать интерфейс E0/1.34
    5. Настроить NAT Inside:
       1. при совпадении Route Map DNS\_R10 использовать интерфейс Tunnel 0
       2. при совпадении Route Map DNS\_R6 использовать интерфейс E0/1.34
    6. применить на интерфейсах:
       1. Out- E0/1.34, E0/1.235, Tunnel 0
       2. In — E0/1.23
13. Настроить IPSec для шифрования всего трафика на R3 и R7 следующим образом:
    1. фазу 1 IPsec
       1. Номер политики 10
       2. Шифрование 3 DES
       3. Хэш MD5
       4. Аутентификация PSK
       5. Diffie-Hellman 5
       6. Источником для пароля «GRE» должен служить Loopback адрес
    2. Настроить фазу 2 IPsec на R3 и R7 следующим образом:
       1. В ACL под названием GRE\_IPSEC разрешить все GRE пакеты
       2. Создать Transform Set под названием ESP\_AES\_SHA:
          1. в качестве протокола использовать ESP
          2. в качестве аутентификации использовать HMAC SHA1
       3. Создать Crypto Map под названием GRE\_IPSEC:
          1. будет матчить ACL под названием GRE\_IPSEC
          2. будет использовать Transform Set под названием ESP\_AES\_SHA
          3. в качестве пира будет использовать Loopback адреса R3, R7
          4. в качестве локального адреса указать Loopback адреса R3, R7
    3. На R3 и R7 применить Crypto Map на следующих интерфейсах:
       1. R3 — E0/1.34, E0/1.235, Tunnel 0
       2. R7 — E0/1.67 и Tunnel 0
14. Проверить работу NAT

## [Лабораторная работа по теме 69: Miscellaneous EIGRP](http://ccie.linkmeup.ru/2016/10/24/laboratornaya-rabota-po-teme-69-miscellaneous-eigrp/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfSVlzUU4xcm5TTkE) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На R1 и R2 настроить RIP следующим образом:
   1. R1 и R2 — Версия 2
   2. R1 — аннонсировать сети 180.1.0.0 и 188.1.0.0
   3. R2 — аннонсировать сети 188.1.0.0 и настроить редистрибьюцию из EIGRP c метрикой 1
4. На R2 настроить маршрут по-умолчанию следующим образом:
   1. Нельзя использовать статический маршрут, редистрибьюцию или суммаризацию
   2. использовать сеть 180.1.0.0
5. На R2 настроить Route Map под названием TAG\_RIP следующим образом:
   1. матчить протокол RIP
   2. проставить метрику 100 100 255 1 1500
   3. проставить тег 100.100.100.1
6. На R2 в EIGRP редистрибьютить Route Map под названием TAG\_RIP
7. На R3 настроить команду route-tag notation dotted-decimal
8. На R3 настроить TAG LIST ROUTE\_TAG следующим образом:
   1. Порядковый номер 5
   2. разрешить сеть 100.100.0.0/16
9. На R3 настроить Route Map под названием EIGRP\_ROUTE\_TAG следующим образом:
   1. матчить TAG LIST ROUTE\_TAG
   2. проставить метрику 50 50 255 1 1500
10. На R3 настроить Distribute List следующим образом:
    1. применить Route Map под названием EIGRP\_ROUTE\_TAG на входе интерфейса Ethernet0/1.23
11. На R9 и R10 настроить OSPF 100 в зоне 0 следующим образом:
    1. R9 — аннонсировать сеть 188.1.109.0/24 и настроить редистрибьюцию из EIGRP
    2. R10 — аннонсировать все сети
12. На R9 настроить маршрут по-умолчанию в сторону R10. Настроить аннонсирование сети 0.0.0.0/0 в EIGRP не используя redistribute/summary route.
13. На R9 настроить редистрибьюцию из OSPF в EIGRP c метрикой 1 1 1 1 1
14. В процессе EIGRP применить соответствующую команду таким образом, чтобы маршрут по-умолчанию не распространялся дальше R4.

## [Лабораторная работа по теме 70: IPsec LAN-to-LAN 4.2](http://ccie.linkmeup.ru/2016/10/26/laboratornaya-rabota-po-teme-70-ipsec-lan-to-lan-4-2/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxLWpaWDd2Y0lWRFE) всех устройств.
2. Для задания используется логическая и физическая топологии проекта
3. Настроить на R2, R5, R8 IPSEC Phase 1 следующим образом:
   1. Номер политики 10
   2. Шифрование 3 DES
   3. Хэш SHA 256
   4. Аутентификация PSK
   5. Деффи-Хелман 5
   6. Время жизни 2 часа
   7. Пароль для ключа:
      1. «GETVPN»
      2. в качестве адресов соседей использовать ip адреса Loopback интерфейсов
4. Настроить R5 в качестве Key Server’a следующим образом:
   1. Настроить ACL под названием GETVPN для трафика, который будет шифроваться:
      1. использовать диапазон адресов устройств, находящихся за R2 и R8, не использовать адреса Loopback интерфейсов
   2. Настроить ключ RSA под названием GETVPN\_RSA длиной 1024
   3. Настроить Trasnform SET под названием ESP\_3DES\_SHA:
      1. Алгоритм шифрования 3 DES
      2. Хеш SHA 1
   4. Настроить IPSec Profile под названием GETVPN\_PROFILE и применить к нему Trasnform SET «ESP\_3DES\_SHA»
   5. Настроить GDOI группу под названием GETVPN:
      1. В качестве IP адреса сервера использовать IP адрес интерфейса Loopback 0
      2. Идентификационный номер группы 100
      3. Применить ACL «GETVPN»
      4. Применить IPSec Profile GETVPN\_PROFILE
      5. Применить ключ GETVPN\_RSA
5. Настроить R2 и R8 в качестве клиентов Key Server’a R5:
   1. Настроить GDOI группу под названием GETVPN:
      1. В качестве Key Server’a указать IP адрес интерфейса Loopback 0 R5
      2. Применить иджентификационный номер группы 100
   2. Настроить Crypto Map под названием GETVPN:
      1. Применить GDOI группу GETVPN
   3. Применить Crypto Map на интерфейсах R2 и R8:
      1. R2- E0/1.23, E0/1.235
      2. R8 — E0/1.78
6. Проверить работу GETVPN

## [Лабораторная работа по темам 71-72: Policy routing (PBR), Traffic Filtering with Policy-Based Routing](http://ccie.linkmeup.ru/2016/11/12/laboratornaya-rabota-po-temam-71-72-policy-routing-pbr-traffic-filtering-with-policy-based-routing/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfdG9IYkVYRHBEMjQ) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На R3 настроить GRE туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R3
   2. В качестве назначения использовать Loopback интерфейс R7
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.3/24
   4. Включить EIGRP процесс 100 на интерфейсе туннеля
4. На R7 настроить туннель следующим образом:
   1. В качестве источника туннеля использовать Loopback интерфейс R7
   2. В качестве назначения использовать Loopback интерфейс R3
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.7/24
   4. Включить EIGRP процесс 100 на интерфейсе туннеля
5. На R3 настроить PBR следующим образом:
   1. Настроить ACL под названием PBR и разрешить трафик от интерфейса Loopback R2 к интерфейсу Loopback R8
   2. Настроить Route Map под названием PBR, который будет использоваться с условиями:
      1. Будет совпадение с ACL PBR
      2. Применить на интерфейсах E0/1.23 и E0/1.235
6. На R7 настроить PBR следующим образом:
   1. Настроить ACL под названием PBR и разрешить трафик от интерфейса Loopback R8 к интерфейсу Loopback R2
   2. Настроить Route Map под названием PBR,со следующими настройками:
      1. Применить ACL PBR
      2. Будет использовать интерфейс Tunnel0
      3. Применить на интерфейсе E0/1.78
7. На R3 настроить IP SLA для отслеживания досягаемости R7 по туннелю:
   1. Номер 1
   2. Настроить отправку пинга, используя в качестве назначения и источника ip адреса интерфейсов Tunnel0
   3. Частота отправки пинга — каждые 5 секунд
   4. Время ожидания ответа 2 секунды
   5. Включить сразу
8. На R3 настроить Track Object следующим образом:
   1. Номер 1
   2. Отслеживать IP SLA 1
9. На R3 применить в Route Map под названием PBR отслеживание Track Object 1
10. На R3 запретить исходящую телнет сессию к Loopback интерфейсу R7, используя PBR следующим образом:
    1. Настроить ACL под названием BLK\_TELNET:
       1. разрешить TCP к Loopback интерфейсу R7 при обращении к телнет сессии
    2. Настроить Route Map под названием FILTER:
       1. Применить ACL BLK\_TELNET
       2. Использовать интерфейс Null0
    3. Настроить глобально Local Policy Routing применив Route Map FILTER
11. Настроить IPSec для шифрования всего трафика на R3 и R7 следующим образом:
    1. фазу 1 IPsec
       1. Номер политики 10
       2. Шифрование 3 DES
       3. Хэш SHA256
       4. Аутентификация PSK
       5. Diffie-Hellman 5
       6. Источником для пароля «PBR» должен служить Loopback адрес
    2. Настроить фазу 2 IPsec на R3 и R7 следующим образом:
       1. Использовать ACL под названием «PBR» соответственно
       2. Создать Transform Set под названием ESP\_3DES\_SHA:
          1. в качестве протокола использовать ESP
          2. в качестве протокола шифрования использовать 3 DES
          3. в качестве аутентификации использовать HMAC SHA1
       3. Создать Crypto Map под названием GRE\_IPSEC:
          1. будет матчить ACL под названием PBR
          2. будет использовать Transform Set под названием ESP\_3DES\_SHA
          3. в качестве пира будет использовать Loopback адреса R3, R7
          4. в качестве локального адреса указать Loopback адреса R3, R7
    3. На R3 и R7 применить Crypto Map на интерфейсах Tunnel0

# [**Цикл 13**](http://ccie.linkmeup.ru/2016/11/18/tsikl-13-tema-73-ospf-summarization/)

## [Лабораторная работа по теме 73: OSPF 3.6](http://ccie.linkmeup.ru/2016/11/21/laboratornaya-rabota-po-teme-73-ospf-3-6/)

Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxN2JYWU5mNWtBWEU) всех устройств.

* 1. Для задания используется логическая и физическая топологии проекта.
  2. На маршрутизаторах R1 и R2 настроить Named mode EIGRP следующим образом:
     1. Имя Named
     2. На R1 интерфейсы должны анонсировать все префиксы :
     3. На R2 E0/1.12 интерфейс должен участвовать в процессе EIGRP
     4. Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам с Named Mode следующим образом:
        1. Режим HMAC
        2. Пароль NAMED MODE
  3. На R2, R3, R4, R5 настроить OSPF процесс 100 в Аrea 25, на следующих интерфейсах:
     1. R2- E0/1.23, E0/1.235, Loopback 0
     2. R3- настроить процесс глобально одной командой
     3. R4 — E0/1.34
     4. R5 -E0/1.235
     5. Между маршрутизаторами настроить тип аутентификации Type 2
        1. Пароль SUMMARY
  4. На R4, R5, R6 Настроить OSPF процесс 100 в Ареа 0 на следующих интерфейсах:
     1. R4- E0/1.456, Loopback 0
     2. R5- E0/1.456, Loopback 0
     3. R6 — E0/1.456, Loopback 0
     4. Между маршрутизаторами настроить тип аутентификации Type 2
        1. Название ключа OSPF\_SUMMARY
        2. Номер ключа 1
        3. Пароль SUMMARY
        4. алгоритм SHA256
  5. На На R6, R7, R8,R9, R10 Настроить OSPF процесс 100 в Ареа 106 на следующих интерфейсах:
     1. R6- E0/1.67
     2. R7- настроить процесс глобально одной командой
     3. R8 — настроить процесс глобально одной командой
     4. R9 — настроить процесс глобально одной командой
     5. R10 — настроить процесс глобально одной командой
     6. Между маршрутизаторами настроить тип аутентификации Type 1
     7. Название ключа SUMMARY
  6. На R2 настроить редистрибуцию из EIGRP в OSPF через subnets
  7. На R2 настроить редистрибуцию из OSPF в EIGRP с метрикой 10000 10 255 1 1500
  8. На R6 настроить Internal Summarization из Area 0, просуммировав диапазон IP адресов Loopback интерфейсов R4, R5, R6
  9. На R2 настроить GRE туннель следующим образом:
     1. В качестве источника туннеля использовать Loopback интерфейс R2
     2. В качестве назначения использовать Loopback интерфейс R7
     3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.2/24
     4. Включить OSPF процесс 100 в Area 1 NSSA на интерфейсе туннеля
  10. На R7 настроить туннель следующим образом:
      1. В качестве источника туннеля использовать Loopback интерфейс R7
      2. В качестве назначения использовать Loopback интерфейс R2
      3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.7/24
      4. Включить OSPF процесс 100 в Area 1 NSSA на интерфейсе туннеля
  11. На R2 настроить External Summarization, просуммировав IP адрес 188.1.12.0/24 до 188.1.8.0/21
  12. Проверить каким образом ходит трафик до 188.1.12.1
  13. На R6 настроить анонсирование маршрута по-умолчанию
  14. На R2 изменить настройки Discard Route так, чтобы он не отражался в таблице маршрутизации.
  15. Настроить фазу 1 IPsec на R2 и R7 следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш MD5
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля GRE должен служить Loopback адрес
  16. Настроить фазу 2 IPsec на R2 и R7 следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием SUM:
         1. будет использовать Transform Set под названием ESP\_3DES\_SHA
  17. На R2 и R7 изменить режим интерфейса Tunnel 0 c GRE на IPSEC IPv4 и применить IPSec Profile SUM

## [Лабораторная работа по теме 74: NAT 9.5](http://ccie.linkmeup.ru/2016/11/23/laboratornaya-rabota-po-teme-74-nat-9-5/)

1. Для лабораторной работы в качестве начальной конфигурации используется конечная конфигурация лабораторной работы 73.
2. Для задания используется логическая и физическая топологии проекта.
3. На R2 настроить Static Policy NAT следующим образом:
   1. Настроить в качестве Inside интерфейса — E0/1.12
   2. Настроить в качестве Outside интерфейсов:
      1. E-0/1.23
      2. E-0/1.235
      3. Tunnel0
   3. Настроить Loopbaсk интерфейсы 1 и 2, где:
      1. IP адрес для Loopbaсk 1- 7.7.7.7/32
      2. Primary IP адрес для Loopbaсk 2- 4.4.4.4/32
      3. Secondary IP адрес для Loopbaсk 2- 188.1.55.55/24
   4. Настроить первое NAT правило для трафика следующим образом:
      1. Настроить ACL под названием R1L0\_R4L0 :
         1. разрешить трафик от Loopback интерфейса R1 к Loopback интерфейсу R4
      2. Настроить Route Map под названием R1L0\_R4L0:
         1. Использовать ACL R1L0\_R4L0
      3. Настроить Static Policy NAT следующим образом:
         1. При вхождении пакета с источником IP адреса Loopback 0 маршрутизатора R1 должно происходить транслирование на Primary IP адрес Loopback2 маршрутизатора R2. Как исто чник и назначение использовать Route Map под названием R1L0\_R4L0
   5. Настроить второе NAT правило для трафика следующим образом:
      1. Настроить ACL под названием R1L0\_R5L0 :
         1. разрешить трафик от Loopback интерфейса R1 к Loopback интерфейсу R5
      2. Настроить Route Map под названием R1L0\_R5L0:
         1. Использовать ACL R1L0\_R5L0
      3. Настроить Static Policy PAT следующим образом:
         1. При вхождении пакета с источником IP адреса Loopback0 и портом 4000 маршрутизатора R1 должно происходить транслирование на Secondary IP адрес Loopback2 маршрутизатора R2. Как источник и назначение использовать Route Map под названием R1L0\_R5L0
   6. Настроить третье NAT правило для трафика следующим образом:
      1. Настроить ACL под названием R1E12\_R8L0 :
         1. разрешить трафик от Ethernet0/1.12 интерфейса R1 к Loopback интерфейсу R8
      2. Настроить Route Map под названием R1E12\_R8L0:
         1. Использовать ACL R1E12\_R8L
      3. Настроить Static Policy NAT следующим образом:
         1. При вхождении пакета с источником IP адреса Ethernet 0/1.12 маршрутизатора R1 должно происходить транслирование на IP адрес Loopback1 маршрутизатора R2. Как источник и назначение использовать Route Map под названием R1E12\_R8L0

## [Лабораторная работа по теме 75: Route redistribution](http://ccie.linkmeup.ru/2016/11/25/laboratornaya-rabota-po-teme-75-route-redistribution/)

* 1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfandyeHpCUzVUbWM) всех устройств.
  2. Для задания используется логическая и физическая топологии проекта.
  3. На маршрутизаторах R1, R2, R9, R10 настроить RIP следующим образом:
     1. Версия 2
     2. Исключить автосуммирование маршрутов
     3. Включить аннонсирование сетей 188.1.0.0 и 180.1.0.0
  4. На маршрутизаторах R2 и R3 настроить OSPF процесс 100 в Аrea 23, на следующих интерфейсах:
     1. R2- E0/1.23, Loopback 0
     2. R3- E0/1.23, Loopback 0
     3. Между маршрутизаторами настроить тип аутентификации Type 2
        1. Алгоритм MD5
        2. Пароль OSPF23
  5. На маршрутизаторах R3 и R4 настроить OSPF процесс 100 в Аrea 34, на следующих интерфейсах:
     1. R4- E0/1.34
     2. R3- E0/1.34
     3. Между маршрутизаторами настроить тип аутентификации Type 1
        1. Пароль AREA34
  6. На маршрутизаторах R2, R3, R5 настроить OSPF процесс 100 в Аrea 52, на следующих интерфейсах:
     1. R2- E0/1.235
     2. R3- E0/1.235
     3. R5- E0/1.235
     4. Между маршрутизаторами настроить тип аутентификации Type 2
        1. Название ключа OSPF52
        2. Номер ключа 1
        3. Пароль SHA\_256
        4. алгоритм SHA256
  7. На маршрутизаторах R4, R5, R6 настроить OSPF процесс 100 в Аrea 0, на следующих интерфейсах:
     1. R4- E0/1.456, Loopback 0
     2. R5- E0/1.456, Loopback 0
     3. R6- E0/1.456, Loopback 0
     4. Между маршрутизаторами настроить тип аутентификации Type 2
        1. Название ключа OSPF0
        2. Номер ключа 1
        3. Пароль SHA\_256
        4. алгоритм SHA256
  8. На маршрутизаторах R6, R7, R8, R9 настроить Named mode EIGRP следующим образом:
     1. Имя Named
     2. Номер процесса 69
     3. Следующие интерфейсы устройств должны участвовать в процессе:
        1. R8 -все интерфейсы
        2. R6 — E0/1.67
        3. R7 — E0/1.67, E0/1.78, Loopback 0
        4. R9 — E0/1.89, Loopback 0
     4. Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам с Named Mode следующим образом:
        1. Название ключа EIGRP
        2. Режим HMAC
        3. Пароль EIGRP69
  9. На R3 настроить GRE туннель следующим образом:
     1. В качестве источника туннеля использовать Looback 0 интерфейс R3
     2. В качестве назначения использовать IP адрес Looback0 интерфейс R7
     3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.3/24
     4. Включить EIGRP процесс 73 на интерфейсе туннеля
  10. На R7 настроить туннель следующим образом:
      1. В качестве источника туннеля использовать Looback 0 интерфейс R7
      2. В качестве назначения использовать Looback0 интерфейс R3
      3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.7/24
      4. Включить EIGRP процесс 73 на интерфейсе туннеля
  11. Настроить Virtual Link к Area 0 следующим образом:
      1. На R3 в сторону R4
      2. На R4 в сторону R3
      3. На Virtual Link настроить аутентификацию следующим образом:
         1. На R3 и R4 — на Virtual Link
         2. Применить пароль VIRT
         3. Настроить тип аутентификации на Virtual Link Type 2
  12. На R6 настроить редистрибьюцию из OSPF в EIGRP с метрикой 10000000 1 255 1 1500
  13. На R6 настроить редистрибьюцию по-умолчанию из EIGRP в OSPF.
  14. На R9 настроить редистрибьюцию из RIP в EIGRP с метрикой 10000000 1 255 1 1500.
  15. На R7 настроить редистрибьюцию из EIGRP 69 в EIGRP 73 и обратно следующим образом:
      1. Настроить Route Map TO\_EIGRP\_73:
         1. Строка 10 запретить:
            1. Матчить по тегу 73
         2. Строка 20 разрешить:
            1. Проставить сет по тегу 69
      2. Настроить Route Map TO\_EIGRP\_69:
         1. Строка 10 запретить:
            1. Матчить по тегу 69
         2. Строка 20 разрешить:
            1. Поставить set по тегу 73
      3. Применить в EIGRP 73 процессе редистрибьюции Route Map TO\_EIGRP\_73
      4. Применить в EIGRP 69 процессе редистрибьюции Route Map TO\_EIGRP\_69
  16. На R3 настроить редистрибьюцию из EIGRP в OSPF следующим образом:
      1. Применить метрику 10
  17. На R2 настроить редистрибьюцию из RIP в OSPF следующим образом:
      1. Применить метрику 0
  18. Настроить Virtual Link к Area 0 следующим образом:
      1. На R2 в сторону R5
      2. На R5 в сторону R2
  19. На R2 настроить редистрибьюцию из OSPF в RIP следующим образом:
      1. Редистрибьютить в RIP маршруты с метрикой 0

## [Лабораторная работа по теме 76: DMVPN 4.3](http://ccie.linkmeup.ru/2016/11/28/laboratornaya-rabota-po-teme-76-dmvpn-4-3/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxT09lWXdhNW1qelE) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Настроить маршрутизатор R7 в качестве хаба следующим образом:
   1. Настроить интерфейс Tunnel0:
      1. IP адрес — использовать Overlay адрес топологии
      2. Аутентификация NHRP — SING\_HUB
      3. Настроить динамическую поддержку мультикаста
      4. NHRP ID — 100
      5. Источник — интерфейс Ethernet 0/1.144
      6. Режим — GRE Multipoint
      7. Ключ туннеля 100000
4. Настроить маршрутизаторы R2, R3, R4, R6 в кечечтве Spok’ов следующим образом:
   1. IP адрес — использовать Overlay адрес топологии
   2. Аутентификация NHRP — SING\_HUB
   3. NHRP ID — 100
   4. Сделать мапинг между Underlay и Overlay адресами хаба
   5. Настроить поддержку мультикаста
   6. В качестве сервера NHRP указать R7
   7. Источник — интерфейс Ethernet 0/1.144
   8. Назначение — адрес R7
   9. Ключ туннеля 100000
5. На хабе и спока настроить RIP следующим образом:
   1. Версия 2
   2. Исключить автосуммирование маршрутов
   3. Включить аннонсирование сетей 188.1.0.0 и 180.1.0.0
   4. На хабе убрать split-horizone
6. На остальных маршрутизаторах настроить RIP следующим образом:
   1. Версия 2
   2. Исключить автосуммирование маршрутов
   3. Включить анонсирование сетей 188.1.0.0 и 180.1.0.0

## [Лабораторная работа по теме 77: Protocol Independent IPv4 Routing 3.1](http://ccie.linkmeup.ru/2016/11/30/laboratornaya-rabota-po-teme-77-protocol-independent-ipv4-routing-3-1/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxZmZEUlJLOGdoTzg) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Настроить маршрутизатор R7 в качестве хаба DMVPN следующим образом:
   1. Настроить фазу 1 IPsec на R7 следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «DMVPN\_VRF» должен служить адрес 0.0.0.0/0
   2. Настроить фазу 2 IPsec на R7 следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием DMVPN\_VRF:
         1. применить Transform Set под названием ESP\_3DES\_SHA
4. На R7 на интерфесе Tunnel 0 применить IPSec Profile DMVPN\_VRF
   1. Настроить интерфейс Tunnel0:
      1. Настроить VFR Forwarding — GREEN
      2. IP адрес — 188.1.100.71/24
      3. Аутентификация NHRP — VRFGREEN
      4. Настроить динамическую поддержку мультикаста
      5. NHRP ID — 100
      6. Источник — интерфейс Ethernet 0/1.144
      7. Режим — GRE Multipoint
      8. Ключ туннеля 10000
      9. Применить профиль DMVPN\_VRF с ключом shared
5. На R7 на интерфесе Tunnel 1 применить IPSec DMVPN\_VRF
   1. Настроить интерфейс Tunnel1:
      1. Настроить VFR Forwarding — RED
      2. IP адрес — 188.1.100.72/24
      3. Аутентификация NHRP — VRF\_RED
      4. Настроить динамическую поддержку мультикаста
      5. NHRP ID — 200
      6. Источник — интерфейс Ethernet 0/1.144
      7. Режим — GRE Multipoint
      8. Ключ туннеля 20000
      9. Применить профиль DMVPN\_VRF с ключом shared
6. Настроить маршрутизаторы R2, R3 качеcтве Spok’ов VRF GREEN следующим образом:
   1. Настроить фазу 1 IPsec на R2 и R3 следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «DMVPN\_VRF» должен служить адрес 0.0.0.0/0
   2. Настроить фазу 2 IPsec на R2 и R3 следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием DMVPN\_VRF:
         1. применить Transform Set под названием ESP\_3DES\_SHA
   3. Настроить интерфейс Tunnel0:
      1. Настроить VFR Forwarding — GREEN
      2. IP адрес — использовать Overlay адрес топологии
      3. Аутентификация NHRP — VRFGREEN
      4. Настроить динамическую поддержку мультикаста
      5. NHRP ID — 100
      6. Сделать мапинг между Underlay и Overlay адресами хаба
      7. В качестве сервера NHRP указать R7
      8. Источник — интерфейс Ethernet 0/1.144
      9. Назначение — адрес R7
      10. Ключ туннеля 10000
      11. Применить профиль DMVPN\_VRF с ключом shared
7. Настроить маршрутизаторы R4, R6 качеcтве Spok’ов VRF RED следующим образом:
   1. Настроить фазу 1 IPsec на R4 и R6 следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «DMVPN\_VRF» должен служить адрес 0.0.0.0/0
   2. Настроить фазу 2 IPsec на R4 и R6 следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием DMVPN\_VRF:
         1. применить Transform Set под названием ESP\_3DES\_SHA
   3. Настроить интерфейс Tunnel0:
      1. Настроить VFR Forwarding — RED
      2. IP адрес — использовать Overlay адрес топологии
      3. Аутентификация NHRP — VRF\_RED
      4. Настроить динамическую поддержку мультикаста
      5. NHRP ID — 200
      6. Ключ туннеля 20000
      7. Сделать мапинг между Underlay и Overlay адресами хаба
      8. В качестве сервера NHRP указать R7
      9. Источник — интерфейс Ethernet 0/1.144
      10. Назначение — адрес R7
      11. Применить профиль DMVPN\_VRF с ключом shared
8. На маршрутизаторах R2, R3, R4, R6, R7 настроить Named mode EIGRP следующим образом:
   1. Имя VRF
   2. Интерфейс Ethernet 0/1.144 должtн участвовать в процессе EIGRP
   3. IP адрес 188.1.100.0/24 должен аннонсироваться в процессе EIGRP
   4. Настроить аутентификацию на интерфейсах R7, подключенных к VRF GREEN с следующим образом:
      1. Пароль DMVPN\_VRF\_GREEN
      2. Режим HMAC
   5. Настроить аутентификацию на интерфейсах R7, подключенных к VRF RED с следующим образом:
      1. Пароль DMVPN\_VRF\_RED
      2. Режим HMAC
   6. Настроить аутентификацию на интерфейсах R2 и R3, подключенных к VRF GREEN с следующим образом:
      1. Пароль DMVPN\_VRF\_GREEN
      2. Режим HMAC
   7. Настроить аутентификацию на интерфейсах R4 и R6, подключенных к VRF RED с следующим образом:
      1. Пароль DMVPN\_VRF\_RED
      2. Режим HMAC

## [Лабораторная работа по теме 78: Layer 2 Multicast 5.1](http://ccie.linkmeup.ru/2016/12/04/laboratornaya-rabota-po-teme-78-layer-2-multicast-5-1/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfYnk3OUwtbEVwdk0) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R9, R10 настроить RIP следующим образом:
   1. Версия 2
   2. Исключить автосуммирование маршрутов
   3. Включить аннонсирование сетей 188.1.0.0 и 180.1.0.0
4. На маршрутизаторах R2 и R3 настроить OSPF процесс 100 в Аrea 23, на следующих интерфейсах:
   1. R2- E0/1.23, Loopback 0
   2. R3- E0/1.23, Loopback 0
   3. Между маршрутизаторами настроить тип аутентификации Type 2
      1. Алгоритм MD5
      2. Пароль OSPF23
5. На маршрутизаторах R3 и R4 настроить OSPF процесс 100 в Аrea 34, на следующих интерфейсах:
   1. R4- E0/1.34
   2. R3- E0/1.34
   3. Между маршрутизаторами настроить тип аутентификации Type 1
      1. Пароль AREA34
6. На маршрутизаторах R2, R3, R5 настроить OSPF процесс 100 в Аrea 52, на следующих интерфейсах:
   1. R2- E0/1.235
   2. R3- E0/1.235
   3. R- E0/1.235
   4. Между маршрутизаторами настроить тип аутентификации Type 2
      1. Название ключа OSPF52
      2. Номер ключа 1
      3. Пароль SHA\_256
      4. алгоритм SHA256
7. На маршрутизаторах R4, R5, R6 настроить OSPF процесс 100 в Аrea 0, на следующих интерфейсах:
   1. R4- E0/1.456, Loopback 0
   2. R5- E0/1.456, Loopback 0
   3. R6- E0/1.456, Loopback 0
   4. Между маршрутизаторами настроить тип аутентификации Type 2
      1. Название ключа OSPF0
      2. Номер ключа 1
      3. Пароль SHA\_256
      4. алгоритм SHA256
8. На маршрутизаторах R6, R7, R8, R9 настроить Named mode EIGRP следующим образом:
   1. Имя Named
   2. Номер процесса 69
   3. Следующие интерфейсы устройств должны участвовать в процессе:
      1. R8 -все интерфейсы
      2. R6 — E0/1.67
      3. R7 — E0/1.67, E0/1.78, Loopback 0
      4. R9 — E0/1.89, Loopback 0
   4. Настроить аутентификацию на интерфейсах, подключенных к маршрутизаторам с Named Mode следующим образом:
      1. Пароль EIGRP
      2. Режим HMAC
9. На R3 настроить GRE туннель следующим образом:
   1. В качестве источника туннеля использовать Looback 0 интерфейс R3
   2. В качестве назначения использовать IP адрес Looback0 интерфейс R7
   3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.3/24
   4. Включить EIGRP процесс 73 на интерфейсе туннеля
10. На R7 настроить туннель следующим образом:
    1. В качестве источника туннеля использовать Looback 0 интерфейс R7
    2. В качестве назначения использовать Looback0 интерфейс R3
    3. В качестве IP адреса туннеля использовать Underlay адрес 144.1.0.7/24
    4. Включить EIGRP процесс 73 на интерфейсе туннеля
11. Настроить Virtual Link к Area 0 следующим образом:
    1. На R3 в сторону R4
    2. На R4 в сторону R3
    3. На Virtual Link настроить аутентификацию следующим образом:
       1. На R3 и R4 — на Virtual Link
       2. Применить пароль VIRT
       3. Настроить тип аутентификации на Virtual Link Type 2
12. На R6 настроить редистрибьюцию из OSPF в EIGRP с метрикой 10000000 1 255 1 1500
13. На R6 настроить редистрибьюцию по-умолчанию из EIGRP в OSPF.
14. На R9 настроить редистрибьюцию из RIP в EIGRP с метрикой 10000000 1 255 1 1500.
15. На R7 настроить редистрибьюцию из EIGRP 69 в EIGRP 73 и обратно следующим образом:
    1. Настроить Route Map TO\_EIGRP\_73:
       1. Строка 10 запретить:
          1. Проставить match 73
       2. Строка 20 разрешить:
          1. Проставить match 69
    2. Настроить Route Map TO\_EIGRP\_69:
       1. Строка 10 запретить:
          1. Проставить set 69
       2. Строка 20 разрешить:
          1. Проставить set 73
    3. Применить в EIGRP 73 процессе редистрибьюции Route Map TO\_EIGRP\_73
    4. Применить в EIGRP 69 процессе редистрибьюции Route Map TO\_EIGRP\_69
16. На R3 настроить редистрибьюцию из EIGRP в OSPF следующим образом:
    1. Применить метрику 10
17. На R2 настроить редистрибьюцию из RIP в OSPF следующим образом:
    1. Применить метрику 0
18. Настроить Virtual Link к Area 0 следующим образом:
    1. На R2 в сторону R5
    2. На R5 в сторону R2
19. На R2 настроить редистрибьюцию из OSPF в RIP следующим образом:
    1. Редистрибьюить в RIP с метрикой 1
20. На R9 настроить редистрибьюцию из EIGRP в RIP следующим образом:
    1. Редистрибьюить в RIP с метрикой 1
21. Настроить на всех маршрутизаторах PIM Dense Mode следующим образом:
    1. Настроить Multicast Routing
    2. Настроить на интерфейсе E0/1.10 R10 мультикастовую группу 232.10.10.10
    3. Настроить PIM Dense Mode на соответствующих интерфесах маршрутизаторов, таким образом, чтобы они могли пинговать адрес мультикастовой группы 232.10.10.10

# [**Цикл 14**](http://ccie.linkmeup.ru/2016/12/02/tsikl-14-tema-79-ospf-3-6/)

## [Лабораторная работа по теме 79: OSPF Stub Areas](http://ccie.linkmeup.ru/2016/12/06/laboratornaya-rabota-po-teme-79-ospf-stub-areas/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfNHB5eng1LUR4TFU) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Настроить маршрутизатор R8 в качестве хаба DMVPN следующим образом:
   1. Настроить фазу 1 IPsec на R8 следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «STUB» должен служить адрес 0.0.0.0/0
   2. Настроить фазу 2 IPsec на R8 следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием OSPF\_STUB:
         1. применить Transform Set под названием ESP\_3DES\_SHA
4. На R8 на интерфесе Tunnel 0 применить IPSec Profile OSPF\_STUB
   1. Настроить интерфейс Tunnel0:
      1. IP адрес — 188.1.100.8/24
      2. Аутентификация NHRP — OSPFSTUB
      3. Настроить динамическую поддержку мультикаста
      4. NHRP ID — 100
      5. Источник — интерфейс Ethernet 0/1.144
      6. Режим — GRE Multipoint
      7. Ключ туннеля 10000
      8. Применить профиль OSPF\_STUB с ключом shared
5. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов следующим образом:
   1. Настроить фазу 1 IPsec следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «STUB» должен служить адрес 0.0.0.0/0
   2. Настроить фазу 2 IPsec следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием OSPF\_STUB:
         1. применить Transform Set под названием ESP\_3DES\_SHA
   3. Настроить интерфейс Tunnel0:
      1. IP адрес — использовать Overlay адрес топологии
      2. Аутентификация NHRP — OSPFSTUB
      3. Настроить динамическую поддержку мультикаста
      4. NHRP ID — 100
      5. Сделать мапинг между Underlay и Overlay адресами хаба
      6. В качестве сервера NHRP указать R8
      7. Источник — интерфейс Ethernet 0/1.144
      8. Назначение — адрес R8
      9. Ключ туннеля 10000
      10. Применить профиль OSPF\_STUB
6. На маршрутизаторах R2, R3, R4, R6, R8 настроить OSPF процесс 100 в Аrea 0 на интерфейсах Tunnel0 и Loopback0:
7. На маршрутизаторах R2, R3, R5 настроить OSPF процесс 100 в Аrea 52 на интерфейсах E0/1.235
8. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 21, на следующих интерфейсах:
   1. R1- E0/1.12, Интерфейс Loopback0
   2. R2- E0/1.12
9. На маршрутизаторах R4, R5, R6 настроить OSPF процесс 100 в Аrea 64 на интерфейсах E0/1.456
10. На маршрутизаторах R7, R8 настроить OSPF процесс 100 в Аrea 78, на следующих интерфейсах:
    1. R7- E0/1.78, Интерфейс Loopback0
    2. R8- E0/1.78
11. На маршрутизаторах R8, R9 настроить OSPF процесс 100 в Аrea 89, на следующих интерфейсах:
    1. R8- E0/1.89,
    2. R9- E0/1.89, Интерфейс Loopback0
12. На маршрутизатор R5, R9, R10 настроить Named mode EIGRP следующим образом:
    1. Имя STUB
    2. Номер автономной системы 100
    3. R5 — Интерфейс Loopback0
    4. R9 — Интерфейс Multilink1
    5. R10 — Интерфейс Multilink1, Loobpack0
13. На маршрутизаторе R5 настроить RIP следующим образом:
    1. Версия 2
    2. Исключить автосуммирование маршрутов
    3. Включить аннонсирование сети 188.1.0.0
14. На R5 настроить редистрибьюцию из EIGRP в OSPF с метрикой 10
15. На R9 настроить редистрибьюцию из EIGRP в OSPF c метрикой 30
16. Area 78 настроить таким образом, чтобы в ней блокировались LSA 4 и 5, но аннонсировались LSA 1, 2, 3 и маршрут по-умолчанию.
17. Area 21 настроить таким образом, чтобы в ней блокировались LSA 3, 4, 5, но аннонсировались LSA 1,2 и маршрут по-умолчанию.
18. Area 52 настроить таким образом, чтобы в ней блокировались LSA 4, 5, но аннонсировались LSA 1,2,3,7. И маршруты, пришедшие из Area 0 не редистрибьютились.
19. Area 89 настроить таким образом, чтобы в ней блокировались LSA 4, 5, но аннонсировались LSA 1,2,3,7 и маршрут по-умолчанию.
20. Area 64 настроить таким образом, чтобы в ней блокировались LSA 3, 4, 5, но аннонсировались LSA 1,2,7 и маршрут по-умолчанию.

## 

## [Лабораторная работа по теме 80: Statefull NAT](http://ccie.linkmeup.ru/2016/12/11/laboratornaya-rabota-po-teme-80-statefull-nat/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfa1FmU3F3MFhNcE0) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Маршрутизаторы R2 и R4 настроить в качестве HTTP серверов.
4. На маршрутизаторе R3 настроить NAT Load Balancing следующим образом:
   1. Настроить inside интерфейсы Ethernet0/1.23 и Ethernet0/1.34
   2. Настроить outside интерфейс Tunnel0
   3. Настроить правила Nat следующим образом:
      1. Настроить ACL под названием NAT:
         1. разрешить TCP c любого источника к порту 80 IP адреса 188.1.100.3
      2. Настроить NAT Pool под названием NAT:
         1. указать диапазон адресов 180.1.2.2 — 180.1.4.4/16
      3. настроить Destination List с привязкой ACL и NAT Pool
5. Проверить подключение по телнет через туннель к IP адресу 188.1.100.3
6. На маршрутизаторах R4 и R5 настроить NAT Box-to-Box следующим образом:
   1. Настроить Object Trаcking под номером 200 маршрута 188.1.45.254/32 с опцией reachability
   2. Задать интерфейсам Ethernet0/1 IP адреса из диапазона 5.5.5.0/24
   3. Настроить Redundancy Application Group:
      1. номер 1
      2. Настроить preempt
      3. Настроить отслеживание Tracking’а 200 со значением декремента 200
      4. На R4 проставить приоритет 105
      5. Интерфейс Ethernet0/1 настроить в качестве Control/Data Plane и Asymmetric Routing.
   4. Настроить в качестве Inside интерфейса — E0/1.456
      1. Номер rii 100
      2. Номер группы 1 с IP 188.1.45.254 с номером значения декремента 100
   5. На R4 настроить в качестве Outside интерфейса:
      1. E-0/1.34
      2. Номер rii 100
      3. Настроить Asymmetric Routing.
   6. На R5 настроить в качестве Outside интерфейса:
      1. E-0/1.235
      2. Номер rii 200
      3. Настроить Asymmetric Routing.
   7. Настроить NAT правило на R4 и R5 для трафика следующим образом:
      1. Настроить ACL под названием REDUNDENCY :
         1. разрешить трафик от Loopback интерфейса R7 к Loopback интерфейсу R3
      2. Настроить Route Map под названием BALANCE:
         1. Использовать ACL REDUNDENCY
      3. Настроить Static Policy NAT следующим образом:
         1. При вхождении пакета с источником IP адреса Loopback1 маршрутизатора R7 должно происходить транслирование на IP адрес 10.10.10.10.
         2. Как исто чник и назначение использовать Route Map под названием BALANCE.
         3. Указать Mapping-ID 120

## [Лабораторная работа по теме 81: IGMP snooping, proxy, filtering](http://ccie.linkmeup.ru/2016/12/13/laboratornaya-rabota-po-teme-81-igmp-snooping-proxy-filtering/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfbTlFcXRyR1Q0dzA) всех устройств.
2. Для задания используется логическая и физическая топологии проекта
3. Настроить R1 в качестве мультикастового сервера следующим образом:
   1. На интерфейсе Ethernet0/1.12 прописать:
      1. Режим PIM Dense
      2. Диапазон групп от 234. 2.2.2 до 234.6.6.6
4. Настроить R2 в качестве клиента только группы 234. 2.2.2 следующим образом:
   1. Настроить стандартный ACL под названием FILTER:
      1. запретить группы от 234.3.3.3 до 234.6.6.6
      2. разрешить весь остальной мультикастовый диапазон.
      3. Применить ACL на интерфейсе Ethernet0/1.12
5. Проверить работу фильтра.

## [Лабораторная работа по теме 82: DMVPN Phase 1, Phase 2, Phase 3](http://ccie.linkmeup.ru/2016/12/19/laboratornaya-rabota-po-teme-82-dmvpn-phase-1-phase-2-phase-3/)

Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfMjBpRnNSRGV2OXM) устройств всех заданий.

### Задание 1

1. Для задания используется логическая и физическая топологии проекта.
2. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 12, на следующих интерфейсах:
   1. R1- E0/1.12, Интерфейс Loopback0
   2. R2- E0/1.12
3. На маршрутизаторах R3, R5 настроить OSPF процесс 100 в Аrea 53, на следующих интерфейсах:
   1. R3- E0/1.235,
   2. R5- E0/1.235, Интерфейс Loopback0
4. На маршрутизаторах R4, R6 настроить OSPF процесс 100 в Аrea 46 на интерфейсах E0/1.456
5. На маршрутизаторах R7, R8,R9,R10 настроить OSPF процесс 100 в Аrea 107, на следующих интерфейсах:
   1. R7- E0/1.78,
   2. R8- E0/1.78, E0/1.89,Интерфейс Loopback0
   3. R9- E0/1.89, Интерфейс Loopback0, Интерфейс Multilink1
   4. R10- Интерфейс Loopback0, Интерфейс Multilink1
6. Настроить DMVPN Phase 2 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — DMVPN
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
         8. Настроить OSPF процесс 100 в Аrea 0 с типом сети, при которой Hello пакеты отправляются Broadcast’ом.
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — DMVPN
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
7. Настроить IPSec DMVPN следующим образом:
   1. Настроить фазу 1 IPsec следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «DMVPN1» должен служить адрес 0.0.0.0/0
   2. Настроить фазу 2 IPsec следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием DMVPN1:
         1. применить Transform Set под названием ESP\_3DES\_SHA
   3. Применить IPSec Profile на интерфейсе Tunnel0 устройств, находящихся в DMVPN.

### Задание 2

1. Для задания используется логическая и физическая топологии проекта.
2. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 12, на следующих интерфейсах:
   1. R1- E0/1.12, Интерфейс Loopback0
   2. R2- E0/1.12
3. На маршрутизаторах R3, R5 настроить OSPF процесс 100 в Аrea 53, на следующих интерфейсах:
   1. R3- E0/1.235,
   2. R5- E0/1.235, Интерфейс Loopback0
4. На маршрутизаторах R4, R6 настроить OSPF процесс 100 в Аrea 46 на интерфейсах E0/1.456
5. На маршрутизаторах R7, R8,R9,R10 настроить OSPF процесс 100 в Аrea 107, на следующих интерфейсах:
   1. R7- E0/1.78,
   2. R8- E0/1.78, E0/1.89,Интерфейс Loopback0
   3. R9- E0/1.89, Интерфейс Loopback0, Интерфейс Multilink1
   4. R10- Интерфейс Loopback0, Интерфейс Multilink1
6. Настроить DMVPN Phase 2 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — DMVPN2
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
         8. Настроить OSPF процесс 100 в Аrea 0 с типом сети, при которой Hello пакеты отправляются Unicast’ом.
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — DMVPN2
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
7. Настроить IPSec DMVPN следующим образом:
   1. Настроить фазу 1 IPsec следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «DMVPN2» должен служить адрес 0.0.0.0/0
   2. Настроить фазу 2 IPsec следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием DMVPN2:
         1. применить Transform Set под названием ESP\_3DES\_SHA
   3. Применить IPSec Profile на интерфейсе Tunnel0 устройств, находящихся в DMVPN.

### Задание 3

1. Для задания используется логическая и физическая топологии проекта.
2. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 12, на следующих интерфейсах:
   1. R1- E0/1.12, Интерфейс Loopback0
   2. R2- E0/1.12
3. На маршрутизаторах R3, R5 настроить OSPF процесс 100 в Аrea 53, на следующих интерфейсах:
   1. R3- E0/1.235,
   2. R5- E0/1.235, Интерфейс Loopback0
4. На маршрутизаторах R4, R6 настроить OSPF процесс 100 в Аrea 46 на интерфейсах E0/1.456
5. На маршрутизаторах R7, R8,R9,R10 настроить OSPF процесс 100 в Аrea 107, на следующих интерфейсах:
   1. R7- E0/1.78,
   2. R8- E0/1.78, E0/1.89,Интерфейс Loopback0
   3. R9- E0/1.89, Интерфейс Loopback0, Интерфейс Multilink1
   4. R10- Интерфейс Loopback0, Интерфейс Multilink1
6. Настроить DMVPN Phase 2 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — DMVPN3
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — DMVPN3
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
7. Настроить на R2, R3, R4, R6, R7 Named EIGRP процесс 73 под названием «DMVPN\_Phase2» на интерфейсах Tunnel 0 и Loopback 0.
8. Настроить редистрибьюцию из OSPF процессов в EIGRP следующим образом:
   1. На R2, R3, R4, R6, R7 — с показателями метрик 100000 1 255 1 1500
9. Настроить редистрибьюцию из EIGRP в OSPF процессы вследующим образом:
   1. На R2, R3, R4, R6, R7 — с показателем метрики 1
10. На R7 настроить суммарный маршрут 0.0.0.0/24
11. Настроить IPSec DMVPN следующим образом:
    1. Настроить фазу 1 IPsec следующим образом:
       1. Номер политики 10
       2. Шифрование 3 DES
       3. Хэш SHA 256
       4. Аутентификация PSK
       5. Diffie-Hellman 5
       6. Источником для пароля «DMVPN3» должен служить адрес 0.0.0.0/0
    2. Настроить фазу 2 IPsec следующим образом:
       1. Создать Transform Set под названием ESP\_3DES\_SHA:
          1. в качестве протокола использовать ESP
          2. в качестве шифрования 3DES
          3. в качестве аутентификации использовать HMAC SHA1
       2. Создать IPSec Profile под названием DMVPN3:
          1. применить Transform Set под названием ESP\_3DES\_SHA
    3. Применить IPSec Profile на интерфейсе Tunnel0 устройств, находящихся в DMVPN.

### Задание 4

1. Для задания используется логическая и физическая топологии проекта.
2. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 12, на следующих интерфейсах:
   1. R1- E0/1.12, Интерфейс Loopback0
   2. R2- E0/1.12
3. На маршрутизаторах R3, R5 настроить OSPF процесс 100 в Аrea 53, на следующих интерфейсах:
   1. R3- E0/1.235,
   2. R5- E0/1.235, Интерфейс Loopback0
4. На маршрутизаторах R4, R6 настроить OSPF процесс 100 в Аrea 46 на интерфейсах E0/1.456
5. На маршрутизаторах R7, R8,R9,R10 настроить OSPF процесс 100 в Аrea 107, на следующих интерфейсах:
   1. R7- E0/1.78,
   2. R8- E0/1.78, E0/1.89,Интерфейс Loopback0
   3. R9- E0/1.89, Интерфейс Loopback0, Интерфейс Multilink1
   4. R10- Интерфейс Loopback0, Интерфейс Multilink1
6. Настроить DMVPN Phase 3 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — DMVPN3
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — DMVPN3
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
7. Настроить на R2, R3, R4, R6, R7 Named EIGRP процесс 73 под названием «DMVPN\_Phase3» на интерфейсах Tunnel 0 и Loopback 0.
8. Настроить редистрибьюцию из OSPF процессов в EIGRP следующим образом:
   1. На R2, R3, R4, R6, R7 — с показателями метрик 100000 1 255 1 1500
9. Настроить редистрибьюцию из EIGRP в OSPF процессы вследующим образом:
   1. На R2, R3, R4, R6, R7 — с показателем метрики 1
10. Настроить IPSec DMVPN следующим образом:
    1. Настроить фазу 1 IPsec следующим образом:
       1. Номер политики 10
       2. Шифрование 3 DES
       3. Хэш SHA 256
       4. Аутентификация PSK
       5. Diffie-Hellman 5
       6. Источником для пароля «DMVPN3» должен служить адрес 0.0.0.0/0
    2. Настроить фазу 2 IPsec следующим образом:
       1. Создать Transform Set под названием ESP\_3DES\_SHA:
          1. в качестве протокола использовать ESP
          2. в качестве шифрования 3DES
          3. в качестве аутентификации использовать HMAC SHA1
       2. Создать IPSec Profile под названием DMVPN3:
          1. применить Transform Set под названием ESP\_3DES\_SHA
    3. Применить IPSec Profile на интерфейсе Tunnel0 устройств, находящихся в DMVPN.

## [Цикл 14, Лабораторная работа по теме 84: BGP 3.7](http://ccie.linkmeup.ru/2016/12/28/tsikl-14-laboratornaya-rabota-po-teme-82-dmvpn/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxZ1VOY0pNc0M4c1k) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R3, R4, R5, R6, R7 настроить внутренний BGP процесс следующим образом:
   1. Номером AS 73
   2. Создать полное соседство друг с другом, используя Loopback интерфейсы друг друга.
   3. Для транспорта использовать EIGRP процесс:
      1. Название BGP
      2. Номер 73
4. На маршрутизаторах R1, R2 настроить внутренний BGP процесс следующим образом:
   1. Номером AS 12
   2. Создать полное соседство друг с другом, используя Loopback интерфейсы друг друга.
   3. Для транспорта использовать EIGRP процесс:
      1. Название BGP
      2. Номер 12
5. На маршрутизаторах R8, R9, R10 настроить внутренний BGP процесс следующим образом:
   1. Номером AS 108
   2. Создать полное соседство друг с другом, используя Loopback интерфейсы друг друга.
   3. Для транспорта использовать EIGRP процесс:
      1. Название BGP
      2. Номер 108
6. Между марщрутизаторами R7 и R8 настроить внешний BGP процесс следующим образом:
   1. Создать соседство друг с другом, используя IP адрсеа интерфейса E0/1.78 друг друга.
7. Между марщрутизаторами R2 и R3 настроить внешний BGP процесс следующим образом:
   1. Создать соседство друг с другом, используя IP адрсеа интерфейса E0/1.23 друг друга.

# [**Цикл 15**](http://ccie.linkmeup.ru/2017/01/08/tsikl-15-tema-85-ospf-filtering/)

## [Цикл 15, Лабораторная работа по теме 85: OSPF 3.6](http://ccie.linkmeup.ru/2017/01/09/tsikl-15-laboratornaya-rabota-po-teme-85-ospf-3-6/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxVkRpbUdQN1hfYTQ) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1и R2 настроить OSPF процесс 100 в Аrea 12, на следующих интерфейсах:
   1. R1- E0/1.12
   2. R2- E0/1.12, E0/1.23
4. На маршрутизаторах R7, R8,R9, R10 настроить OSPF процесс 100 в Аrea 107, на следующих интерфейсах:
   1. R7- E0/1.78
   2. На остальных маршрутизаторах все интерфейсы должны находиться в процессе OSPF
5. На маршрутизаторах R3, R5 настроить Named mode EIGRP следующим образом:
   1. Имя FILTER
   2. Номер процесса 100
   3. Следующие интерфейсы устройств должны участвовать в процессе:
      1. R3 — E0/1.235, Loopback 0
      2. R5 — E0/1.235, Loopback 0
6. На маршрутизаторах R1 настроить Named mode EIGRP следующим образом:
   1. Имя FILTER
   2. Номер процесса 100
   3. Следующие интерфейсы устройств должны участвовать в процессе:
      1. Loopback 0
7. Настроить DMVPN Phase 2 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — FILTER
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
         8. Настроить OSPF процесс 100 в Аrea 0 с типом сети, при которой Hello пакеты отправляются Broadcast’ом.
   2. Настроить маршрутизаторы R2, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — FILTER
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
         8. Настроить OSPF процесс 100 в Аrea 0 с типом сети, при которой Hello пакеты отправляются Broadcast’ом.
8. На маршрутизаторах R4 и R6 настроить OSPF процесс 100 в Аrea 0, на следующих интерфейсах:
   1. R4- E0/1.456, Loopback 0
   2. R6- E0/1.67, Loopback 0
9. На R4 настроить настроить статические маршруты следующим образом:
   1. настроить статические маршруты 180.1.3.3/32, 180.1.5.5/32, 188.1.235.0/24
   2. использовав IP адрес интерфейса E0/1.456 маршрутизатора R5 в качестве Next HOP
10. На R4 настроить редистрибьюцию статического маршрута в OSPF
11. На R2 настроить настроить статические маршруты следующим образом:
    1. настроить статические маршруты 180.1.3.3/32, 180.1.5.5/32, 188.1.235.0/24
    2. использовав IP адрес интерфейса E0/1.23 маршрутизатора R3 в качестве Next HOP
12. На R2 настроить редистрибьюцию статического маршрута в OSPF
13. На R5 настроить статический маршрут по-умолчанию использовав IP адрес интерфейса E0/1.456 маршрутизатора R4 в качестве Next HOP
14. На R5 настроить редистрибьюцию статический маршрута в EIGRP с метрикой 10000000 1 255 1 1512
15. На R1 настроить редистрибьюцию из EIGRP в OSPF c метрикой 50
16. Настроить R4 таким образом, чтобы трафик с R7 до IP адресов Loopback интерфейсов маршрутизаторов R3 и R5 ходил только через R4.
17. Настроить R6 таким образом, чтобы маршрут 180.1.1.1 не устанавливался в таблицу маршрутизации. При этом нельзя использовать Distribute List’ы.
18. Настроить R4 таким образом, чтобы маршрут 180.1.10.10 не устанавливался в таблицу маршрутизации. Для матчинга использовать ACL.
19. Настроить R2 таким образом, чтобы маршрут 180.1.9.9 не устанавливался в таблицу маршрутизации. Для матчинга использовать Prefix List.
20. Настроить R2 таким образом, чтобы маршруты 180.1.4.4 и 180.1.6.6 не устанавливались в таблицу маршрутизации R1. При этом не использовать Prefix List’ы, ACL и Destribute List’ы
21. Настроить R7 таким образом, чтобы маршрут 180.1.8.8 не устанавливались в базу данных OSPF и не распространялcя далее в Area 0.
22. Настроить R2 таким образом, чтобы маршрут 188.1.23.0/24 относился к процессу OSPF 100 Area 0, но не распространялcя далее в Area 12, но при этом устанавливался в базу данных OSPF.
23. Настроить area 12 качестве NSSA.
24. Настроить R2 таким образом, чтобы трафик с R7 до IP адресов Loopback интерфейсов маршрутизаторов R3 и R5 начал ходить и через R2 и через R4. При этом конфигурация на R4 должна оставаться неизменной.
25. Настроить R1 таким образом, чтобы маршрут приходящий из EIGRP рапространялся не далее R2.

## [Цикл 15, Лабораторная работа по теме 86: NAT 9.5](http://ccie.linkmeup.ru/2017/01/11/tsikl-15-laboratornaya-rabota-po-teme-86-nat-9-5/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxeXd6bzRMNjlqTzQ) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Между марщрутизаторами R2, R4, R5, R6 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 2, 4, 5 и 6 соответсвенно для маршрутизаторов R2, R4, R5, R6
   2. Создать соседство следующим образом:
      1. R2-R5, используя IP адреса интерфейса E0/1.235
      2. R4-R5, используя IP адреса интерфейса E0/1.456
      3. R5-R6, используя IP адреса интерфейса E0/1.456
4. На маршрутизаторах R3 и R4 настроить внутренний BGP процесс следующим образом:
   1. Номером AS 4
   2. Создать полное соседство друг с другом, используя Loopback интерфейсы друг друга.
   3. Для транспорта настроить OSPF процесс 100 в Аrea 0, на следующих интерфейсах:
      1. R3- E0/1.34, Loopback 0
      2. R4- E0/1.34, Loobpack0
5. На маршрутизаторах R2и R3 настроить OSPF процесс 100 в Аrea 23 NSSA, на следующих интерфейсах:
   1. R2- E0/1.23, Loopback 0
   2. R3- E0/1.23
6. На маршрутизаторах R6, R7, R8,R9, R10 настроить OSPF процесс 100 в Аrea 106, на следующих интерфейсах:
   1. R6- E0/1.67, Loopback 0
   2. На остальных маршрутизаторах все интерфейсы должны находиться в процессе OSPF
7. На маршрутизаторах R1, R2 настроить Named mode EIGRP следующим образом:
   1. Имя NAT
   2. Номер процесса 100
   3. Следующие интерфейсы устройств должны участвовать в процессе:
      1. R2 — E0/1.12
      2. R1 — E0/1.12, Loopback 0
8. На маршрутизаторе R5 настроить настроить Named mode EIGRP следующим образом:
   1. Имя NAT
   2. Номер процесса 100
   3. Следующие интерфейсы устройств должны участвовать в процессе:
      1. Loopback 0
9. На маршрутизаторе R6 настроить NAT Virtual Interface следующим образом:
   1. Настроить ACL под названием NVI, где разрешить диапазон 180.1.0.0/20
   2. Настроить NAT POOL:
      1. Название — NVI
      2. Диапазон адресов — 188.1.100.0/24
      3. В таблицу маршрутизации должен добавляться статический маршрут — 188.1.100.0/24
   3. В качестве источника использовать ACL NVI с привязкой к пулу NVI
10. На маршрутизаторе R6 настроить редистрибьюцию маршрутов в BGP следующим образом:
    1. Настроить ACL под названием REDISTRIBUTION\_BGP, где:
       1. запретить диапазон 180.1.0.0/20
       2. разрешить весь остальной диапазон адресов
    2. Настроить Route Map:
       1. Название — REDISTRIBUTION\_BGP:
       2. Заматчить к ACL REDISTRIBUTION\_BGP
    3. Настроить редистрибьюцию статических маршрутов
    4. Настроить редистрибьюцию OSPF маршрутов с привязкой к Route Map REDISTRIBUTION\_BGP
11. На маршрутизаторах R2 и R4 настроить NAT Default Interface следующим образом:
    1. Настроить ACL под названием DEFAULT\_SERVER, где разрешить любой трафик
    2. Настроить NAT таким образом, чтобы при обращении к IP адресам интерфейсов E0/1.235 и E0/1.456 соответственно R2 и R4 , трафик перенаправлялся а IP адресу Loopback интерфейса R3.
    3. Настроить NAT таким образом, чтобы весь внутренний трафик, не соответсвующий ни одному существующему потоку трафика мог достичь назначения через интерфейсы E0/1.235 и E0/1.456 соответственно R2 и R4.
12. На маршрутизаторе R2 и R4 настроить редистрибьюцию маршрутов в BGP следующим образом:
    1. Настроить ACL под названием RESTRICT\_R3\_LO, где:
       1. запретить 180.1.3.3/32
       2. разрешить весь остальной диапазон адресов
    2. Настроить Route Map:
       1. Название — RESTRICT\_R3\_LO:
       2. Заматчить к ACL RESTRICT\_R3\_LO
    3. Настроить редистрибьюцию маршрутов EIGRP.
    4. Настроить редистрибьюцию OSPF маршрутов с привязкой к Route Map RESTRICT\_R3\_LO

## [Цикл 15, Лабораторная работа по теме 87: IGMP profiles, Multicast VLAN registration](http://ccie.linkmeup.ru/2017/01/14/tsikl-15-laboratornaya-rabota-po-teme-87-igmp-profiles-multicast-vlan-registration/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfS01lcXVjQlBBSzQ) всех устройств.
2. Для задания используется логическая и физическая топологии проекта
3. Настроить R4 в качестве мультикастового клиента следующим образом:
   1. интерфейсе Ethernet0/1.456 подключить к диапазону групп от 234.2.4.4 до 234.2.6.6
4. Настроить R5 в качестве сервера, настроив PIM Spars Mode на интерфейсе Ethernet0/1.456
5. Настроить свичи SW2 и SW4 следующим образом:
   1. Режим прослушки IGMP и PIM трафика только для влана 456.
   2. Установить 90 секундный интервал перед тем, как свич перестанет обрабатывать мультикаст, как броадкаст
   3. Настроить ограничение на подключение к группам в количестве 3 на порту SW4, подключенного к R4. При превышении указанного количества подключение будет запрещаться.
6. Настроить остальные свичи в режиме прослушки общего IGMP и PIM трафика.
7. На R5 настроить следующие интервалы
   1. равный 90 секундам, в течении которого маршрутизатор будет ждать запрос от группы, прежде чем удалит ее.
   2. настроить максимальное время отклика от хоста равное 2 секундам
   3. настроить максимальный отклик от хоста, который отправил IGMPv2 Leave Report в 1000 ms
   4. настроить отправку запроса хостам, после получения IGMPv2 Leave Report маршрутизатором от хоста, равную 2 запросам.

## [Цикл 15, Лабораторная работа по теме 88: DMVPN 4.3](http://ccie.linkmeup.ru/2017/01/16/tsikl-15-laboratornaya-rabota-po-teme-88-dmvpn-4-3/)

[Начальная конфигурация](https://drive.google.com/open?id=0B8TdfSzCKkaxVnF3aFFWX1Z3TEE)

1. Настроить DMVPN Phase 3 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — QoS
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Настроить NHRP Redirect
         6. Источник — интерфейс Ethernet 0/1.144
         7. Режим — GRE Multipoint
         8. Ключ туннеля 10000
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — QoS
         3. Настроить маппинг мультикаста к R7
         4. NHRP ID — 100
         5. В качестве сервера NHRP NHS указать R7
         6. Настроить NHRP Shortcut
         7. Источник — интерфейс Ethernet 0/1.144
         8. Режим — GRE Multipoint
         9. Ключ туннеля 10000
2. На маршрутизаторах R2, R3, R4, R6, R7 настроить Named mode EIGRP следующим образом:
   1. Имя QoS\_Tunnel
   2. Номер процесса 72
   3. Следующие интерфейсы устройств должны участвовать в процессе:
      1. R2 — Интерфейс Tunnel 0
      2. R3 — Интерфейс Tunnel 0
      3. R4- Интерфейс Tunnel 0, Interface Loopback0
      4. R6- Интерфейс Tunnel 0, Interface Loopback0
      5. R7 — Интерфейс Tunnel 0, Interface Loopback0
   4. Настроить редистрибьюцию на Spok’ах из EIGRP 100 со следующими показателями метрики:
      1. BW- 1000000000
      2. DLY-1
      3. Reliability — 255
      4. Loading — 1
      5. MTU — 1400
   5. На R7 настроить суммарный маршрут для диапазона адресов 180.1.0.0/20
3. На R7 настроить политику QoS следующим образом:
   1. Настроить ACL под названием QOS, где разрешить диапазон адресов 180.1.0.0/20
   2. Настроить Class Map под наименованием R2\_R4\_VOICE с логическим AND для всех совпадающих утверждений в рамках данного Class Map’a:
      1. Заматчить ACL под названием QOS
   3. Настроить Class Map под наименованием R3\_R6\_VOICE с логическим AND для всех совпадающих утверждений в рамках данного Class Map’a:
      1. Заматчить ACL под названием QOS
   4. Настроить Class Map под наименованием R2\_R4\_ROUTING:
      1. Заматчить IP Precedence 6
   5. Настроить Class Map под наименованием R3\_R6\_ROUTING:
      1. Заматчить IP Precedence 6
   6. Настроить Policy Map под наименованием R2\_R4:
      1. применить Class Map под наименованием R2\_R4\_VOICE c приоритетом 1000
      2. применить Class Map под наименованием R2\_R4\_ROUTING c с BW в 20 процентов
   7. Настроить Policy Map под наименованием R3\_R6:
      1. применить Class Map под наименованием R3\_R6\_VOICE c приоритетом в 20 процентов
      2. применить Class Map под наименованием R3\_R6\_ROUTING с BW в 10 процентов
   8. Настроить Policy Map под наименованием R2\_R4\_MAIN:
      1. Для Class’a Default применить шейпер в 3 мб с Service Policy R2\_R4
   9. Настроить Policy Map под наименованием R3\_R6\_MAIN:
      1. Для Class’a Default применить шейпер в 2 мб с Service Policy R3\_R6
4. На интерфейсе Tunnel0 R7 применить политику QoS следующим образом:
   1. Настроить группу под названием R2\_R4 с применением Service Policy R2\_R4\_MAIN
   2. Настроить группу под названием R3\_R6 с применением Service Policy R3\_R6\_MAIN
5. На интерфейсе Tunnel0 R2 и R4 применить группу R2\_R4
6. На интерфейсе Tunnel0 R3 и R6 применить группу R3\_R6

## [Цикл 15, Лабораторная работа по теме 90: BGP 3.7](http://ccie.linkmeup.ru/2017/01/20/tsikl-15-laboratornaya-rabota-po-teme-90-bgp-3-7/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxM3JBSlBYRHJwTXM) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3, R4, R5 настроить OSPF процесс 100 в Аrea 51 на следующих интерфейсах:
   1. R4- E0/1.34, Loopback 0
   2. R5- E0/1.235, Loopback 0
   3. На остальных настроить OSPF процесс одной командой
4. На маршрутизаторах R6, R7, R8, R9, R10 настроить OSPF процесс 100 в Аrea 51 на следующих интерфейсах:
   1. R6- E0/1.67, Loopback 0
   2. На остальных настроить OSPF процесс одной командой
5. Между марщрутизаторами R4, R5, R6 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 456, 546, 654 соответсвенно для маршрутизаторов R4, R5, R6
   2. Создать ebgp сессию следующим образом:
      1. использовать IP адреса интерфейсов Loopback0
      2. на R4 создать соседство c R5 и R6, используя пароль R4\_R6 и R4\_R5 соответственно. Настроить возможность бесшумного сбрасывания пакета при достижении TTL = 223.
      3. на R5 создать соседство c R4, используя пароль R4\_R5. Настроить возможность бесшумного сбрасывания пакета при достижении TTL = 223.
      4. на R5 создать соседство c R6, используя пароль R5\_R6. Настроить возможность изменения TTL = 2 и более.
      5. на R6 создать соседство c R4, используя пароль R4\_R6. Настроить возможность бесшумного сбрасывания пакета при достижении TTL = 223.
      6. на R6 создать соседство c R5, используя пароль R5\_R6. Настроить возможность изменения TTL = 2 и более.
6. На маршрутизаторе R4 настроить маршрут по-умолчанию следующим образом:
   1. в качестве Next Hop’a использовать IP адрес интерфейса E0/1.456 маршрутизатора R6
   2. маршрут должен адвертайзится в OSPF процесс 100 с метрикой 10
7. На маршрутизаторе R5 настроить маршрут по-умолчанию следующим образом:
   1. в качестве Next Hop’a использовать IP адрес интерфейса E0/1.456 маршрутизатора R6
   2. маршрут должен адвертайзится в OSPF процесс 100 с метрикой 100
8. На маршрутизаторе R6 настроить маршрут по-умолчанию следующим образом:
   1. в качестве Next Hop’a использовать интерфейс E0/1.456
   2. маршрут должен адвертайзится в OSPF процесс 100

# 

# [**Цикл 16**](http://ccie.linkmeup.ru/2017/01/20/tsikl-16-tema-91-default-routing/)

## [Цикл 16, Лабораторная работа по теме 91: Default Routing](http://ccie.linkmeup.ru/2017/01/23/tsikl-16-laboratornaya-rabota-po-teme-91-default-routing/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfcFU4YlhCWll1OGc) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Между марщрутизаторами R2, R3, R4, R5, R6 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 2, 3, 5 и 6 соответственно для маршрутизаторов R2, R3, R5, R6
   2. Создать соседство следующим образом:
      1. Использовать IP адреса Loopback0 интерфейсов маршрутизаторов.
      2. на R2 и R5 создать соседство друг с другом:
         1. Настроить возможность изменения TTL = 2 и более
         2. Настроить статический маршрут, используя IP адреса Loopback интерфейсов друг друга и в указать в качестве Next Hop IP адрес интерфейса E0/1.235
      3. на R3 и R5 создать соседство друг с другом:
         1. Настроить возможность изменения TTL = 2 и более
         2. Настроить статический маршрут, используя IP адреса Loopback интерфейсов друг друга и в указать в качестве Next Hop IP адрес интерфейса E0/1.235
4. На маршрутизаторах R1и R2 настроить OSPF процесс 100 в Аrea 0 на следующих интерфейсах:
   1. R1, R2- E0/1.12, Loopback 0
5. На маршрутизаторах R3и R4 настроить OSPF процесс 100 в Аrea 34 NSSA, на следующих интерфейсах:
   1. R3, R4- E0/1.34, Loopback 0
6. На маршрутизаторах R6, R7, R8,R9, R10 настроить OSPF процесс 100 в Аrea 106, на следующих интерфейсах:
   1. R6- E0/1.67, Loopback 0
   2. На остальных маршрутизаторах настроить внести все интерфейсы в OSPF процесс одной командой.
7. На маршрутизаторе R5 настроить маршрут по-умолчанию следующим образом:
   1. использовать в качестве Next Hop IP интерфейс Null0.
   2. Адвертайзить данный маршрут в BGP использовав команду Network.
8. На маршрутизаторе R2 настроить маршрут по-умолчанию, использовав в качестве Next Hop IP адрес интерфейса E0/1.23 маршрутизатора R3.
9. На маршрутизаторе R2 настроить Conditional default route следующим образом:
   1. Настроить Prefix List под названием DEFAULT\_ROUTE в котором разрешить префиксы 188.1.23.0/24 и 188.1.235.0/24
   2. Настроить Route Map под названием DEFAULT\_ROUTE в котором заматчить Prefix List под названием DEFAULT\_ROUTE
   3. Включить в процесс OSPF распространение маршрута по-умолчанию с опцией Always и применением Route Map под названием DEFAULT\_ROUTE
10. На маршрутизаторе R3 настроить распространение маршрута по-умолчанию с метрикой 10 только в NSSA Area.
11. На маршрутизаторе R6 настроить маршрут по-умолчанию использовав в качестве Next Hop IP адрес интерфейса E0/1.45 маршрутизатора R4.
12. На маршрутизаторе R6 настроить Reliable Conditional Default Routing следующим образом:
    1. Создать IP SLA под номером 1:
       1. должно отправлять ICMP к IP адресу интерфейса E0/1.456 маршрутизатора R4 от IP адресу интерфейса E0/1.456 маршрутизатора R6 с частотой в 5 с.
       2. запустить сразу
    2. Привязать IP SLA под номером 1 к треку под номером 1 с ключом Reachability
    3. Создать IP SLA под номером 2:
       1. должно отправлять ICMP к IP адресу интерфейса E0/1.456 маршрутизатора R5 от IP адресу интерфейса E0/1.456 маршрутизатора R6 с частотой в 5 с.
       2. запустить сразу
    4. Привязать IP SLA под номером 2 к треку под номером 2 с ключом Reachability
    5. Создать статические маршруты с IP адресами 169.254.1.1/32 и 169.254.1.2/32 с Next Hop интерфейсом NULL0 и привязкой к трекам 1 и 2 соответсвенно
    6. Настроить Prefix List под названием DEFAULT\_ROUTE в котором разрешить префиксы 169.254.1.1/32 и 169.254.1.2/32
    7. Настроить Route Map под названием DEFAULT\_ROUTE в котором заматчить Prefix List под названием DEFAULT\_ROUTE
    8. Включить в процесс OSPF распространение маршрута по-умолчанию с опцией Always и применением Route Map под названием DEFAULT\_ROUTE.

## [Цикл 16, Лабораторная работа по теме 92: Static Extendable NAT, NAT ALG](http://ccie.linkmeup.ru/2017/01/31/tsikl-16-laboratornaya-rabota-po-teme-92-static-extendable-nat-nat-alg/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfUjc0TDRwS3RWSjQ) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Между маршрутизаторами R1, R2, R5 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 1, 2, 5 соответственно для маршрутизаторов R1, R2, R5
   2. Создать ebgp сессию следующим образом:
      1. Использовать IP адреса Loopback0 интерфейсов маршрутизаторов.
      2. на R1 и R2 создать соседство друг с другом:
         1. Настроить возможность изменения TTL = 2 и более
         2. Настроить статический маршрут, используя IP адреса Loopback интерфейсов друг друга и в указать в качестве Next Hop IP адрес интерфейса E0/1.12
      3. на R2 и R5 создать соседство друг с другом:
         1. Настроить возможность изменения TTL = 2 и более
         2. Настроить статический маршрут, используя IP адреса Loopback интерфейсов друг друга и в указать в качестве Next Hop IP адрес интерфейса E0/1.235
4. На маршрутизаторах R2, R3, R4, R6, R7, R8, R9, R10 настроить OSPF процесс 100 в Аrea 0 на следующих интерфейсах:
   1. R2-E0/1.23, Loopback
   2. R6-E0/1.456, Loopback 0
   3. R7-E0/1.67, Loopback 0
   4. R3, R4, R8, R9, R10 — настроить все интерфесы одной командой
5. Настроить DMVPN Phase 3 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — NAT\_EXT
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — NAT\_EXT
         3. Настроить поддержку мультикаста, указав NMBA адрес R7
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
6. Настроить на R2, R3, R4, R6, R7 Named EIGRP процесс 100 под названием «DMVPN» на интерфейсах Tunnel 0 и Loopback 0.
7. Настроить на R7, R8, R9, R10 Named EIGRP процесс 107 под названием «NAT\_EXT» на следующих интерфейсах :
   1. R7- интерфейс E0/1.78
   2. R8, R9, R10 — все интерфейсы должны быть в процессе EIGRP
8. Настроить редистрибьюцию из EIGRP процесса 107 в EIGRP процесса 100 и обратно следующим образом:
   1. На R7 — с показателями метрик 10000000 1 255 1 1500
9. На маршрутизаторе R5 настроить маршрут по-умолчанию следующим образом:
   1. использовать в качестве Next Hop IP интерфейс Null0.
   2. Адвертайзить данный маршрут в BGP использовав команду Network.
10. На маршрутизаторе R2 настроить маршрут по-умолчанию, использовав в качестве Next Hop IP адрес интерфейса E0/1.12 маршрутизатора R1.
11. На маршрутизаторе R2 настроить Static Extendable NAT следующим образом:
    1. Настроить IP адреса 1.1.1.1/32 и 5.5.5.5/32 Loopback интерфейсов под номерами 1 и 5 соответственно.
    2. Указать в качестве NAT outside интерфейсы E0/1.12 и E0/1.235
    3. Указать в качестве NAT inside интерфейс Tunnel 0
    4. Настроить ACL под названием DNS, где разрешить даипазон 188.1.0.0/16 к любому префиксу
    5. Настроить ACL под названием ISP\_2, где разрешить ip адрес 188.1.235.5 к любому префиксу
    6. Настроить Route Map под названием ISP\_1 в котором заматчить ACL под названием DNS и интерфейс E0/1.12
    7. Настроить Route Map под названием ISP\_12 в котором заматчить ACL под названием DNS и Next Hop ACL под названием ISP\_2
    8. Настроить NAT Pool под названием ISP\_1 с диапазоном адресов с 1.1.1.2/24 по 1.1.1.254/24
    9. Настроить NAT Pool под названием ISP\_2 с диапазоном адресов с 5.5.5.6/24 по 5.5.5.254/24
    10. Настроить статический NAT с опцией Extandable , где в качестве Inside Local адреса указать IP адрес Loopback интерфейса R10, а в качестве Inside Global адресов IP адреса Loopback интерфейсов под номерами 1 и 5
12. Проверить трансляцию.

## [Цикл 16, Лабораторная работа по теме 93: Multicast routing intro. PIM Dense Mode](http://ccie.linkmeup.ru/2017/02/03/tsikl-16-laboratornaya-rabota-po-teme-93-multicast-routing-intro-pim-dense-mode/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfbmdOdWRIR1BJbkU) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3, R4, R5, R6, R7 настроить OSPF процесс 100 в Аrea 0 на следующих интерфейсах:
   1. R1- E0/1.12, Loopback 0
   2. R2-E0/1.12, E0/1.23, Loopback 0
   3. R3-E0/1.34, E0/1.23, E0/1.235, Loopback 0
   4. R4-E0/1.34, E0/1.456, E0/1.235, Loopback 0
   5. R5- на всех интерфейсах
   6. R6-E0/1.67, E0/1.456, Loopback 0
   7. R7-E0/1.67, Loopback 0
4. Настроить DMVPN Phase 3 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — PIM\_DN
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — PIM\_DN
         3. Настроить поддержку мультикаста, указав NMBA адрес R7
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
5. Настроить на R2, R3, R4, R6, R7 Named EIGRP процесс 100 под названием «DMVPN» на интерфейсах Tunnel 0.
6. Настроить на R7, R8, R9, R10 Named EIGRP процесс 107 под названием «PIM\_DENSE» на следующих интерфейсах :
   1. R7- интерфейс E0/1.78
   2. R8, R9, R10 — все интерфейсы должны быть в процессе EIGRP
7. Настроить суммирование маршрута по-умолчанию из EIGRP процесса 107 в EIGRP процесса 100 и обратно.
8. Настроить на всех маршрутизаторах Multicast Routing, настроив PIM Dense Mode на следующих интерфейсах:
   1. R7 — интерфейс Ethernet 0/1.78, интерфейс Tunnel0
   2. R10 — интерфейс Multilink1
   3. На остальных все интерфейсы
9. Настроить на R2 подключить интерфейс E0/1.12 к IGMP группе 234.12.12.12
10. Проверить работу Multicast Routing с разных устройств, отправив пинг до группы 234.12.12.12

## [Цикл 16, Лабораторная работа по теме 94: QoS Pre-classification](http://ccie.linkmeup.ru/2017/02/07/tsikl-16-laboratornaya-rabota-po-teme-94-qos-pre-classification/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfNVhTeW1WX1Yyclk) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3, R4, R5, R6, R7 настроить OSPF процесс 100 в Аrea 0 на следующих интерфейсах:
   1. R1- E0/1.12, Loopback 0
   2. R2-E0/1.12, E0/1.23, Loopback 0
   3. R3-E0/1.34, E0/1.23, E0/1.235, Loopback 0
   4. R4-E0/1.34, E0/1.456, E0/1.235, Loopback 0
   5. R6-E0/1.67, E0/1.456, Loopback 0
   6. R7-E0/1.67, Loopback 0
4. Настроить DMVPN Phase 3 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — QoS
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — QoS
         3. Настроить поддержку мультикаста, указав NMBA адрес R7
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
5. Настроить на R2, R3, R4, R6, R7 Named EIGRP процесс 100 под названием «DMVPN» на интерфейсах Tunnel 0.
6. Настроить на R7, R8, R9, R10 Named EIGRP процесс 107 под названием «QOS\_PRECLASS» на следующих интерфейсах :
   1. R7- интерфейс E0/1.78
   2. R8, R9, R10 — все интерфейсы должны быть в процессе EIGRP
7. Настроить суммирование маршрута по-умолчанию из EIGRP процесса 107 в EIGRP процесса 100 и обратно .
8. Настроить фазу 1 IPsec на R2, R3, R4, R6, R7 следующим образом:
   1. Номер политики 10
   2. Шифрование 3 DES
   3. Хэш MD5
   4. Аутентификация PSK
   5. Diffie-Hellman 5
   6. Источником для пароля «QOS\_PRECLASS» для R7 должен служить адрес 0.0.0.0
9. Настроить фазу 2 IPsec на R2, R3, R4, R6, R7 следующим образом:
   1. Создать Transform Set под названием ESP\_AES\_SHA:
      1. в качестве протокола использовать ESP
      2. в качестве аутентификации использовать HMAC SHA1
   2. Создать IPSec Profile под названием QOS\_PRECLASS:
      1. будет использовать Transform Set под названием ESP\_AES\_SHA
10. На R2, R3, R4, R6, R7 на интерфесе Tunnel 0 применить IPSec QOS\_PRECLASS
11. На R2 настроить маршрут по-умолчанию для процесса OSPF 100 с метрикой 10
12. Настроить правила QoS на R2 следующим образом:
    1. настроить ACL под названием GRE, где разрешить трафик протокола GRE в любом направлении
    2. настроить ACL под названием ICMP, где разрешить трафик протокола ICMP в любом направлении
    3. создать Class Map под названием ICMP и заматчить ACL под названием ICMP
    4. создать Class Map под названием GRE и заматчить ACL под названием GRE
    5. создать Policy Map под названием MATCH\_ICMP\_GRE и заматчить Class Map’ы под названием GRE и ICMP
    6. применить Pilicy Map под названием MATCH\_ICMP\_GRE на интерфейсе E0/1.144
    7. настроить QoS Pre-Classification на интферфейсе Tunnel0 R2
13. Проверить работу QoS Pre-Classification

## [Цикл 16, Лабораторная работа по теме 95: Protocol Independent IPv6 Routing 3.2](http://ccie.linkmeup.ru/2017/02/08/tsikl-16-laboratornaya-rabota-po-teme-95-protocol-independent-ipv6-routing-3-2/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxN2d5bkhvWTlDYjg) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На всех маршрутизаторах настроить OSPF процесс 100 в Аrea 0 на следующих интерфейсах:
   1. R1- E0/1.12, Loopback 0
   2. R2-E0/1.12, E0/1.23, Loopback 0
   3. R3-E0/1.34, E0/1.23, E0/1.235, Loopback 0
   4. R4-E0/1.34, E0/1.456, Loopback 0
   5. R6-E0/1.67, E0/1.456, Loopback 0
   6. R7-E0/1.67, Loopback 0
   7. R5, R8, R9, R10 настроить одной командой
4. Настроить DMVPN IPv6 через IPv4 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IPv6 адрес — 2001:CC1E:1:100:7/64
         2. Аутентификация NHRP — IPv6
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — IPv6
         3. Настроить поддержку мультикаста, указав NMBA адрес R7
         4. Настроить маппинг IPv6 адреса к IPv4 адресу R7
         5. NHRP ID — 100
         6. В качестве сервера NHRP указать IPv6 адрес R7
         7. Источник — интерфейс Ethernet 0/1.144
         8. Режим — GRE Multipoint
         9. Ключ туннеля 10000
5. Проверить подключение DMVPN IPv6

## [Цикл 16, Лабораторная работа по теме 96: BGP 3.7](http://ccie.linkmeup.ru/2017/02/10/tsikl-16-laboratornaya-rabota-po-teme-96-bgp-3-7/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfandkbm43WkZXdVE) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R2, R3, R4, R5, R6, R7 настроить OSPF процесс 100 в Аrea 0 на следующих интерфейсах:
   1. R2- E0/1.23, Loopback 0
   2. R3- E0/1.34, E0/1.23, Loopback 0
   3. R4-E0/1.34, E0/1.456, Loopback 0
   4. R6-E0/1.67, E0/1.456, Loopback 0
   5. R7-E0/1.67, Loopback 0
   6. R5 — настроить одной командой
4. На маршрутизаторах R2, R3, R5 настроить OSPF процесс 100 в Аrea 52 на интерфейсе E0/1.235
5. Настроить на R1 и R2 Named EIGRP процесс 100 под названием «BGP\_PEER\_GROUP» на на следующих интерфейсах:
   1. R2- E0/1.12
   2. R1 -E0/1.12, Loopback 0
6. Настроить на R7, R8, R9, R10 Named EIGRP процесс 100 под названием «BGP\_PEER\_GROUP» на на следующих интерфейсах:
   1. R7- E0/1.78
   2. R8 -E0/1.78, E0/1.89, Loopback 0
   3. R9- E0/1.89, Loopback 0, Multilink 1
   4. R10 — Loopback 0, Multilink 1
7. Настроить DMVPN IPv6 через IPv4 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IPv6 адрес — 2001:CC1E:1:100::7/64
         2. Аутентификация NHRP — BGP\_PEER
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — BGP\_PEER
         3. Настроить поддержку мультикаста, указав NMBA адрес R7
         4. Настроить маппинг IPv6 адреса к IPv4 адресу R7
         5. NHRP ID — 100
         6. В качестве сервера NHRP указать IPv6 адрес R7
         7. Источник — интерфейс Ethernet 0/1.144
         8. Режим — GRE Multipoint
         9. Ключ туннеля 10000
8. Проверить подключение DMVPN IPv6
9. На маршрутизаторе R7 настроить внешний BGP процесс для IPv6 следующим образом:
   1. Номер AS — 1.7
   2. Создать ebgp сессию следующим образом:
      1. Настроить Peer Group под названием BGP\_PEER:
         1. Использовать Tunnel 0 интерфейс в качестве Update Source
         2. Внести в Peer Group соседей их IPv6 адресам
10. На маршрутизаторах R2, R3, R4, R6 настроить внешний BGP процесс для IPv6 следующим образом:
    1. Номер AS — 1.2, 1.3, 4, 6 — соответственно
    2. Создать ebgp сессию с R7 следующим образом:
       1. Использовать Tunnel 0 интерфейс в качестве Update Source
       2. Указать в качестве соседа IPv6 адрес R7
       3. Указать в качестве Remote As ANS R7
11. Решить проблему создания соседства между R7 и R2, R3, R4, R6

# [**Цикл 17**](http://ccie.linkmeup.ru/2017/02/17/tsikl-17-tema-97-ospf/)

## [Цикл 17, Лабораторная работа по теме 97: OSPF 3.6](http://ccie.linkmeup.ru/2017/02/20/tsikl-17-laboratornaya-rabota-po-teme-97-ospf-3-6/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxMlhvelk3QTNUMTA) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3, R4, R5 настроить OSPF процесс 100 в Аrea 51 на следующих интерфейсах:
   1. R2- E0/1.12,E0/1.23, E0/1.235,Loopback 0
   2. R3- E0/1.34, E0/1.23, E0/1.235,Loopback 0
   3. R4-E0/1.34, Loopback 0
   4. R5- E0/1.235, Loopback 0
   5. R1 — настроить одной командой
4. На маршрутизаторах R7, R8, R9, R10 настроить OSPF процесс 100 в Аrea 107 на на следующих интерфейсах:
   1. R7- E0/1.78, Loopback 0
   2. R8, R9, R10 -настроить одной командой
5. Настроить DMVPN Phase 2 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — 188.1.100.7/24
         2. Аутентификация NHRP — LSAOPTIM
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. Источник — интерфейс Ethernet 0/1.144
         6. Режим — GRE Multipoint
         7. Ключ туннеля 10000
         8. Настроить OSPF процесс 100 в Аrea 72 с типом сети, при которой Hello пакеты отправляются Broadcast’ом.
   2. Настроить маршрутизаторы R2, R3, R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — LSAOPTIM
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
         8. Настроить OSPF процесс 100 в Аrea 72 с типом сети, при которой Hello пакеты отправляются Broadcast’ом при этом Spok’и не должны участвовать в выборах DR.
6. На R6 настроить статические маршруты следующим образом:
   1. маршрут по-умолчанию, в качестве Next Hop интерфейс Null0
   2. статический маршрут к IP адресу Loopback интерфейса R4. В качестве Next Hop указать интерфейс E0/1.456 R6
   3. статический маршрут к IP адресу Loopback интерфейса R5. В качестве Next Hop указать интерфейс E0/1.456 R6
   4. статический маршрут к IP адресу Loopback интерфейса R7. В качестве Next Hop указать IP адрес интерфейса E0/1.67 R7
7. На маршрутизаторе R6 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 1.6
   2. Создать ebgp сессию следующим образом:
      1. Настроить Peer Group под названием LSA:
         1. Использовать Loopback интерфейс в качестве Update Source
         2. Внести в Peer Group соседей их IP адреса интерфейсов Loopback0
         3. Позволить увеличение значения TTL только до 2 хопов
         4. Настроить распространение маршрута по-умолчанию не используя команду redistribute.
8. На маршрутизаторах R4, R5, R7 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 4, 5, 1.7 — соответственно
   2. Создать ebgp сессию с R6 следующим образом:
      1. Использовать Loopback0 интерфейс в качестве Update Source
      2. Указать в качестве Remote As номер AS 1.6
      3. Позволить увеличение значения TTL только до 2 хопов
9. На R7 в OSPF процесс 100 адвертайзить маршрут по-умолчанию
10. На R7 настроить статический маршрут к IP адресу Loopback интерфейса R6. В качестве Next Hop указать IP адрес интерфейса E0/1.67 R6
11. На R4 в OSPF процесс 100 адвертайзить маршрут по-умолчанию всегда с метрикой 10.
12. На R4 настроить статический маршрут к IP адресу Loopback интерфейса R6. В качестве Next Hop указать IP адрес интерфейса E0/1.456 R6
13. На всех маршрутизаторах настроить оптимизацию OSPF процесса следующим образом:
    1. Throttle таймер для SPF алгоритма со следующими значениями:
       1. Таймер начальной задержки калькуляции SPF в 5 секунд
       2. Hold таймер между двумя SPF калькуляциями 10 секунд
       3. Таймер максимального ожидания 90 секунд
    2. Pacing таймер со следующими значениями:
       1. Groupe таймер 75 сек
       2. Таймер ретрансмиссии 100 мсек
       3. Таймер флдудинга 50 мсек
14. На интрефейсах Tunnel0 маршрутизаторов R2, R3, R4, R6, R7 настроить Fast Hello c отправкой Hello 5 пакетов в секунду

## [Цикл 17, Лабораторная работа по теме 98: Traffic Accounting 9.6](http://ccie.linkmeup.ru/2017/02/22/tsikl-17-laboratornaya-rabota-po-teme-98-traffic-accounting-9-6/)

1. Для задания используется конечные конфиги лабораторной работы 97.
2. На маршрутизаторе R6 настроить передачу только маршрута по-умолчанию следующим образом:
   1. настроить ACL под названием DEFAULT и разрешить только трафик маршрута по-умолчанию.
   2. в протоколе BGP настроить Distribute List c ACL под названием DEFAULT на выход.
3. На маршрутизаторах R2, R3, R7 настроить IP Precedence Accounting следующим образом:
   1. На маршрутизаторе R2:
      1. настроить ACL под названием ICMP разрешить весь трафик ICMP
      2. настроить Class Map под названием ICMP и заматчить ACL под названием ICMP
      3. настроить Policy Map под названием ICMP, классифицировать Class Map под названием ICMP и проставить Precedence 5
      4. применить Policy Map под названием ICMP на интерфейсе Ethernet 0/1.144
      5. настроить на интерфейсе Tunnel0 Qos Pre-classification
   2. На маршрутизаторе R3:
      1. На маршрутизаторе R3 настроить IP Precedence Accounting следующим образом:
      2. настроить ACL под названием TELNET разрешить весь трафик TELNET
      3. настроить Class Map под названием TELNET и заматчить ACL под названиемTELNET
      4. настроить Policy Map под названием TELNET, классифицировать Class Map под названием TELNET и проставить Precedence 3
      5. применить Policy Map под названием TELNET на интерфейсе Ethernet 0/1.144
      6. настроить на интерфейсе Tunnel0 Qos Pre-classification
   3. Настроить на интерфейсе Ethernet 0/1.144 маршрутизатора R7 в IP Precedence Accounting
4. На маршрутизаторе R7 настроить IP Access Violation Accounting следующим образом:
   1. настроить ACL под названием BLOCK\_R2L0\_TO\_R8L0 и запретить весь трафик от IP адреса интерфейса Loopback0 маршрутизатора R2 к IP адресу интерфейса Loopback0 маршрутизатора R8. Разрешить весь остальной трафик
   2. применить ACL под названием BLOCK\_R2L0\_TO\_R8L0 на выходе интерфейса Ethernet 0/1.78
   3. настроить на интерфейсе Ethernet 0/1.78 IP Access Violation Accounting
5. На маршрутизаторе R7 настроить IP Output Packet Accounting следующим образом:
   1. настроить IP Accounting List для IP адреса интерфейса Loopback0 маршрутизатора R10.
   2. настроить на интерфейсе Ethernet 0/1.78 IP Output Packet Accounting
6. Проверить работу всех настроек.

## [Цикл 17, Лабораторная работа по теме 99: IPv4 Multicast Routing 5.2](http://ccie.linkmeup.ru/2017/02/24/tsikl-17-laboratornaya-rabota-po-teme-99-ipv4-multicast-routing-5-2/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxVzFnV01wSy10LUU) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3, R4, R5 настроить OSPF процесс 100 в Аrea 51 на следующих интерфейсах:
   1. R2- E0/1.12,E0/1.23, E0/1.235,Loopback 0
   2. R3- E0/1.34, E0/1.23, E0/1.235,Loopback 0
   3. R4-E0/1.34, Loopback 0
   4. R5- E0/1.235, Loopback 0
   5. R1 — настроить одной командой
4. На маршрутизаторах R4, R5, R6 настроить OSPF процесс 100 в Аrea 0 на на интерфейсе E0/1.456
5. На маршрутизаторах R6, R7, R8, R9, R10 настроить OSPF процесс 100 в Аrea 106 на следующих интерфейсах:
   1. R6- E0/1.67, Loopback 0
   2. R7, R8, R9, R10 — настроить одной командой
6. На всех маршрутизаторах настроить IP Multicast Routing
7. На всех маршрутизаторах настроить Sparse Mode на следующих интерфейсах:
   1. R1 — E0/1.12, Loopback0
   2. R2 — E0/1.12, E0/1.23, E0/1.235
   3. R3- E0/1.34, E0/1.23, E0/1.235
   4. R4 — E0/1.456
   5. R5 — E0/1.456, E0/1.235
   6. R6 -E0/1.67, E0/1.456, Loopback0
   7. R7 — E0/1.78, E0/1.67
   8. R8 — E0/1.78, E0/1.89
   9. R9 — E0/1.89, Multilink 1
   10. R10 — Multilink 1
8. На всех маршрутизаторах настроить IP адрес интрефейса Loopback 0 маршрутизатора R6 в качестве RP
9. Настроить маршрутизатор R7 в качестве DR для маршрутизатора R8 с приоритетом равным 10
10. Настроить интерфейс Loopback0 маршрутизатора R10 в качестве клиента группы 224.1.10.10

## [Цикл 17, Лабораторная работа по теме 100: BGP 3.7](http://ccie.linkmeup.ru/2017/02/27/tsikl-17-laboratornaya-rabota-po-teme-100-bgp-3-7/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxVzJORXRtZTdjSTg) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3, R4, R5 настроить OSPF процесс 100 в Аrea 51 на следующих интерфейсах:
   1. R2- E0/1.12,E0/1.23, E0/1.235,Loopback 0
   2. R3- E0/1.34, E0/1.23, E0/1.235,Loopback 0
   3. R4-E0/1.34
   4. R5- E0/1.235
   5. R1 — настроить одной командой
4. На маршрутизаторах R6, R7, R8, R9, R10 настроить OSPF процесс 100 в Аrea 106 на на следующих интерфейсах:
   1. R6 — E0/1.67, Loopback 0
   2. R7- E0/1.78, Loopback 0
   3. R8, R9, R10 -настроить одной командой
5. На маршрутизаторах R4, R5, R6 настроить OSPF процесс 100 в Аrea 0 на интерфейсах E0/1.456, Loopback 0.
6. На маршрутизаторe R7 настроить VRF под названием VOICE и VIDEO с номерами RD 1:1 и 1:2 соответственно.
7. Настроить DMVPN Phase 3 следующим образом:
   1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
      1. Настроить интерфейс Tunnel0:
         1. Присвоить VRF под названием VOICE
         2. IP адрес — 188.1.100.7/24
         3. Аутентификация NHRP — MULTISES
         4. Настроить динамическую поддержку мультикаста
         5. NHRP ID — 100
         6. Источник — интерфейс Ethernet 0/1.144
         7. Режим — GRE Multipoint
         8. Ключ туннеля 10000
         9. Настроить значение MTU 1400
         10. Настроить значение Adjust MSS 1360
      2. Настроить интерфейс Tunnel1:
         1. Присвоить VRF под названием VIDEO
         2. IP адрес — 188.1.100.7/24
         3. Аутентификация NHRP — MULTISES
         4. Настроить динамическую поддержку мультикаста
         5. NHRP ID — 101
         6. Источник — интерфейс Ethernet 0/1.144
         7. Режим — GRE Multipoint
         8. Ключ туннеля 10001
         9. Настроить значение MTU 1400
         10. Настроить значение Adjust MSS 1360
   2. Настроить маршрутизаторы R2, R3 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — MULTISES
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 100
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10000
         8. Настроить значение MTU 1400
         9. Настроить значение Adjust MSS 1360
   3. Настроить маршрутизаторы R4, R6 качеcтве Spok’ов:
      1. Настроить интерфейс Tunnel0:
         1. IP адрес — использовать Overlay адрес топологии
         2. Аутентификация NHRP — MULTISES
         3. Настроить динамическую поддержку мультикаста
         4. NHRP ID — 101
         5. В качестве сервера NHRP указать R7
         6. Источник — интерфейс Ethernet 0/1.144
         7. Ключ туннеля 10001
         8. Настроить значение MTU 1400
         9. Настроить значение Adjust MSS 1360
8. На маршрутизаторе R7 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 1.7
   2. Создать ebgp сессию для VRF VOICE следующим образом:
      1. Настроить Peer Group под названием VOICE:
         1. Указать в качестве Remote AS номер 2.3
         2. Позволить увеличение значения TTL только до 2 хопов
         3. Внести в Peer Group IP адреса интерфейсов Tunnel0 маршрутизаторов R2 и R3
         4. Адвертайзить маршрут 188.1.100.0/24
   3. Создать ebgp сессию для VRF VIDEO следующим образом:
      1. Настроить Peer Group под названием VIDEO:
         1. Указать в качестве Remote AS номер 4.6
         2. Позволить увеличение значения TTL только до 2 хопов
         3. Внести в Peer Group IP адреса интерфейсов Tunnel0 маршрутизаторов R4 и R6
         4. Адвертайзить маршрут 188.1.100.0/24
9. На маршрутизаторах R2, R3 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 2.3
   2. Создать ebgp сессию с R7 следующим образом:
      1. Указать в качестве Remote As номер 1.7
      2. Адвертайзить маршрут 188.1.100.0/24
10. На маршрутизаторах R4, R6 настроить внешний BGP процесс следующим образом:
    1. Номер AS — 4.6
    2. Создать ebgp сессию с R7 следующим образом:
       1. Указать в качестве Remote As номер 1.7
       2. Адвертайзить маршрут 188.1.100.0/24

## [Цикл 17, Лабораторная работа по теме 101: EUI-64, SLAAC](http://ccie.linkmeup.ru/2017/03/01/tsikl-17-laboratornaya-rabota-po-teme-101-eui-64-slaac/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfR2Z0N05DelJSNk0) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На всех маршрутизаторах изменить IPv6 адреса для интерфейсов Loopback0 следующим образом:
   1. Использовать первые 64 бита адреса по топологии
   2. Остальная часть адреса должна быть настроена автоматически
4. На всех маршрутизаторах изменить IPv6 Link Local адреса следующим образом:
   1. R1 — интерфейс E0/1.12 — FE80::A8BB:CCFF:FE00:110
   2. R2 — интерфейсы E0/1.12, E0/1.23, E0/1.235 — FE80::A8BB:CCFF:FE00:210
   3. R3 — интерфейсы E0/1.23, E0/1.34, E0/1.235 — FE80::A8BB:CCFF:FE00:310
   4. R4 — интерфейсы E0/1.456, E0/1.34 — FE80::A8BB:CCFF:FE00:410
   5. R5 — интерфейсы E0/1.456, E0/1.235 — FE80::A8BB:CCFF:FE00:510
   6. R6 — интерфейсы E0/1.67, E0/1.456 — FE80::A8BB:CCFF:FE00:610
   7. R7 — интерфейсы E0/1.67, E0/1.78 — FE80::A8BB:CCFF:FE00:710
   8. R8 — интерфейсы E0/1.78, E0/1.89 — FE80::A8BB:CCFF:FE00:810
   9. R9 — интерфейсы E0/1.89, Multilink1 — FE80::A8BB:CCFF:FE00:910
   10. R10 — интерфейс Multilink1 — FE80::A8BB:CCFF:FE00:A00
5. На всех маршрутизаторах добавить IPv6 Global Unicast адреса, на интерфейсах, подключенные к соседним маршрутизаторам таким образом, чтобы конечная 64-битная часть представляла собой точную копию IPv4 адреса данного интерфейса с префиксом /128.

## [Цикл 17, Лабораторная работа по теме 102: BGP 3.7](http://ccie.linkmeup.ru/2017/03/03/tsikl-17-laboratornaya-rabota-po-teme-102-bgp-3-7/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxOVVfXzNMM3VEQ0E) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1 и R2 настроить OSPF процесс 21 в Аrea 21 на всех интерфейсах:
4. На маршрутизаторах R3, R4, R5, R6 настроить OSPF процесс 6543 в Аrea 6543 на всех интерфейсах:
5. На маршрутизаторах R7, R8, R9, R10 настроить OSPF процесс 10987 в Аrea 10987 на всех интерфейсах.
6. На маршрутизаторах R1, R2 настроить внутренний BGP процесс следующим образом:
   1. Номер AS — 21
   2. Создать bgp сессию следующим образом:
      1. Указать в качестве Remote AS номер 21
      2. Указать в качестве соседей IP адреса интерфейсов Loopback 0
      3. Настроить команду, при которой все Next Hop адреса узнаются через OSPF
      4. На R2 указать R1 в качестве клиента Route Reflector’a
7. На маршрутизаторе R2 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 21
   2. Создать bgp сессию следующим образом:
      1. Указать в качестве Remote AS номер 6543
      2. Указать в качестве соседей IP адреса интерфейсов Loopback 0
      3. Позволить увеличение значения TTL только до 2 хопов
      4. Адвертайзить маршрут 180.1.0.0/22 с помощью команды network
8. На маршрутизаторах R3, R4, R5, R6 настроить Confederation BGP процесс следующим образом:
   1. R3 — номер AS — 3
   2. R4, R5 — номер AS — 54
   3. R6 — номер AS — 6
   4. Создать внешнюю bgp сессию на R3 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 6543
      2. Указать в качестве пиров конфедерации 54
      3. Указать в качестве Remote AS номера AS 21 и 54
      4. Указать в качестве соседей IP адреса интерфейсов Loopback 0
      5. Позволить увеличение значения TTL только до 2 хопов
      6. Для соседа в AS 54 настроить команду, при которой все Next Hop адреса узнаются через OSPF
      7. Адвертайзить маршрут по-умолчанию с помощью команды network
   5. Создать внешнюю и внутреннюю bgp сессии на R4 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 6543
      2. Указать в качестве пиров конфедерации AS номера 3 и 6
      3. Для внешней bgp сессии:
         1. Создать пир группу под названием CONFEDERATION:
            1. Позволить увеличение значения TTL только до 2 хопов
            2. Для соседей настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номера AS R3 и R6
         3. Указать в качестве членов группы IP адреса интерфейсов Loopback 0 R3 и R6
      4. Для внутренней bgp сессии:
         1. Создать пир группу под названием REFLECT:
            1. На R4 указать R5 в качестве клиента Route Reflector’a
            2. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номер AS 54
         3. Указать в качестве члена группы IP адрес интерфейса Loopback 0 R5
   6. Создать внутреннюю bgp сессию на R5 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 6543
      2. Указать в качестве Remote AS номер AS 54
      3. Для соседа R4 настроить команду, при которой все Next Hop адреса узнаются через OSPF
   7. Создать внешнюю и внутреннюю bgp сессии на R6 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 6543
      2. Указать в качестве пиров конфедерации AS номер 54
      3. Для внешней bgp сессии конфедерации:
         1. Создать пир группу под названием CONFEDERATION:
            1. Позволить увеличение значения TTL только до 2 хопов
            2. Для соседей настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номер AS R4
         3. Указать в качестве членов группы IP адрес интерфейса Loopback 0 R4
      4. Для внешней bgp сессии:
         1. Указать в качестве Remote AS номер AS 10987
         2. Указать в качестве члена группы IP адрес интерфейса Loopback 0 R7
         3. Позволить увеличение значения TTL только до 2 хопов
         4. Адвертайзить маршрут по-умолчанию с помощью команды network
9. На маршрутизаторах R7, R8, R9, R10 настроить Confederation BGP процесс следующим образом:
   1. R7 — номер AS — 7
   2. R8, R9, R10 — номер AS — 1098
   3. Создать внешнюю bgp сессию на R7 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 10987
      2. Указать в качестве пиров конфедерации 1098
      3. Указать в качестве Remote AS номера AS 6543 и 1098
      4. Указать в качестве соседей IP адреса интерфейсов Loopback 0
      5. Позволить увеличение значения TTL только до 2 хопов
      6. Для соседа в AS 1098 настроить команду, при которой все Next Hop адреса узнаются через OSPF
      7. Адвертайзить маршрут 180.1.0.0/20 с помощью команды network
   4. Создать внешнюю и внутреннюю bgp сессии на R8 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 10987
      2. Указать в качестве пиров конфедерации AS номер 7
      3. Для внешней bgp сессии:
         1. Создать пир группу под названием CONFEDERATION:
            1. Позволить увеличение значения TTL только до 2 хопов
            2. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номер AS R7
         3. Указать в качестве членов группы IP адреса интерфейсов Loopback 0 R7
      4. Для внутренней bgp сессии:
         1. Создать пир группу под названием REFLECT:
            1. Указать R9 в качестве клиента Route Reflector’a
            2. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номер AS 1098
         3. Указать в качестве члена группы IP адрес интерфейса Loopback 0 R9
   5. Создать внутреннюю bgp сессию на R9 следующим образом:
      1. Создать пир группу под названием REFLECT:
         1. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
      2. Указать в качестве Remote AS номер AS 1098
      3. Указать в качестве членов группы IP адреса интерфейсов Loopback 0 R8 и R9
   6. Создать внутреннюю bgp сессию на R10 следующим образом:
      1. Создать пир группу под названием REFLECT:
         1. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
      2. Указать в качестве Remote AS номер AS 1098
      3. Указать в качестве члена группы IP адрес интерфейса Loopback 0 R9
10. На маршрутизаторах R2 и R3 настроить статические маршруты к друг другу следующим образом:
    1. В качестве маршрута указать IP адрес Loopback0 интерфейса друг друга
    2. В качестве Next Hop указать IP адрес интерфейса E0/1.23 друг друга.
11. На маршрутизаторах R6 и R7 настроить статические маршруты к друг другу следующим образом:
    1. В качестве маршрута указать IP адрес Loopback0 интерфейса друг друга
    2. В качестве Next Hop указать IP адрес интерфейса E0/1.67 друг друга.
12. На маршрутизаторе R3 настроить маршрут по-умолчанию указав в качестве Next Hop интерфейс Null0.
13. На маршрутизаторе R6 настроить маршрут по-умолчанию указав в качестве Next Hop интерфейс Null0.
14. На маршрутизаторе R2 настроить статический маршрут 180.1.0.0/22 указав в качестве Next Hop интерфейс Null0.
15. На маршрутизаторе R7 настроить статический маршрут 180.1.0.0/20 указав в качестве Next Hop интерфейс Null0.

# [**Цикл 18**](http://ccie.linkmeup.ru/2017/03/03/voprosy-po-tsiklu-17-tema-103-ospf-convergence-optimization-scalability/)

## [Цикл 18, Лабораторная работа по теме 103: OSPF 3.6](http://ccie.linkmeup.ru/2017/03/07/tsikl-18-laboratornaya-rabota-po-teme-103-ospf-3-6/)

Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxZWw0U3U0cWxJSkE) всех устройств.

* 1. Для задания используется логическая и физическая топологии проекта.
  2. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 21 на следующих интерфейсах c типом сети Point-to-Point:
     + 1. R2- E0/1.12
       2. R1 — E0/1.12, Loopback0
  3. На маршрутизаторах R2, R5 настроить OSPF процесс 100 в Аrea 52 на следующих интерфейсах c типом сети Point-to-Point:
     1. R2- E0/1.235
     2. R5 — E0/1.235, Loopback0
  4. На маршрутизаторах R2, R3, R4 настроить OSPF процесс 100 в Аrea 42 на следующих интерфейсах c типом сети Point-to-Point:
     1. R2- E0/1.23, Loopback0
     2. R3 — E0/1.23, E0/1.34, Loopback0
     3. R4 — E0/1.34, Loopback0
  5. На маршрутизаторах R4, R5, R6 настроить OSPF процесс 100 в Аrea 0 на следующих интерфейсах:
     1. R4, R5 -E0/1.456,
     2. R6- E0/1.456, Loopback 0.
  6. На маршрутизаторах R6 и R7 настроить OSPF процесс 76 в Аrea 76 на следующих интерфейсе E0/1.67
  7. На маршрутизаторах R2, R4, R5 настроить OSPF Virtual линки следующим образом:
     1. R2- в строну R4, R5, используя IP адреса их Loopback интерфейсов
     2. R4, R5 — в сторону R2, используя IP адрес Loopback интерфейса R2
  8. На маршрутизаторе R6 настроить следующие статические маршруты:
     1. Маршрут 180.1.0.0/16, в качестве Next Hop указать интерфейс Null0
     2. Маршрут 180.1.7.7/32, в качестве Next Hop указать IP адрес интерфейса E0/1.67 маршрутизатора R7
  9. На маршрутизаторе R7 настроить следующие статические маршруты:
     1. Маршрут по-умолчанию, в качестве Next Hop указать интерфейс Null0
     2. Маршрут 180.1.6.6/32, в качестве Next Hop указать IP адрес интерфейса E0/1.67 маршрутизатора R6
  10. На маршрутизаторе R6 настроить внешний BGP процесс следующим образом:
      1. Номер AS — 6
      2. Создать ebgp сессию c маршрутизатором R7 следующим образом:
         1. Указать в качестве Remote AS номер 7
         2. Позволить увеличение значения TTL только до 2 хопов
         3. Указать в качестве Update Source интерфейс Loopback0
         4. Адвертайзить маршрут 180.1.0.0/16
  11. На маршрутизаторе R7 настроить внешний BGP процесс следующим образом:
      1. Номер AS — 7
      2. Создать ebgp сессию c маршрутизатором R6 следующим образом:
         1. Указать в качестве Remote AS номер 6
         2. Позволить увеличение значения TTL только до 2 хопов
         3. Указать в качестве Update Source интерфейс Loopback0
         4. Адвертайзить маршрут по-умочанию
  12. На маршрутизаторе R6 адвертайзить маршрут по-умолчанию в OSPF процесс 100
  13. На маршрутизаторе R7 настроить редистрибьюцию BGP в OSPF процесс 100 с мерикой равной 5.
  14. На маршрутизаторе R2 настроить в OSPF процессе 100 адвертайзинг максимальной метрики при перезагрузке или выключении маршрутизатора. Указать постоянное время.
  15. На маршрутизатора R6 и R7 настроить в OSPF процессе 76 адвертайзинг максимальной метрики при загрузке BGP таблиц или выключении маршрутизатора.
  16. На маршрутизаторах R4, R5 в OSPF процессе 100 настроить адвертайзинг максимальной метрики в течении 100 секунд после перезагрузки

## [Цикл 18, Лабораторная работа по теме 104: NetFlow 9.7](http://ccie.linkmeup.ru/2017/03/08/tsikl-18-laboratornaya-rabota-po-teme-104-netflow-9-7/)

1. Загрузить начальную конфигурацию всех устройств (использовать финальную конфигурацию из 103-й лабораторной работы).
2. Для задания используется логическая и физическая топологии проекта.
3. Для задания используется конечная конфигурация лабораторной работы 103
4. На маршрутизаторе R6 настроить NetFlow следующим образом:
   1. Настроить учитывание входящего трафика на порту E0/1.456
   2. Настроить локальный коллектор трафика:
      1. Максимальное количество записей 10
      2. Сортировать по пакетам
   3. Настроить удаленный коллектор трафика:
      1. Указать IP адрес интерфейса Loopback0 маршрутизатора R1 порт 991
   4. Настроить версию 9
   5. Указать обновление кэш NetFlow данными о трафике еще активной сессии через каждые 3 минуты
   6. Настроить закрытие потока, если в течении 30 секунд не передаются данные.
   7. Указать в качестве источника отчета о трафике интерфейс E0/1.67
   8. Настроить Random Sampled Netflow cледующим образом:
      1. Наименование NETFLOW
      2. Настроить выборку в 1 пакет из 10
      3. Настроить ACL под названием R10\_R1:
         1. Разрешить трафик от IP адреса интерфейса Loopback0 маршрутизатора R10 к IP адресу интерфейса Loopback0 маршрутизатора R1
      4. Настроить Сlass Map под названием R10\_R1 и заматчить ACL R10\_R1
      5. Настроить Policy Map под названием NETFLOW:
         1. Применить Сlass Map под названием R10\_R1
         2. Применить Random Sampled Netflow под названием NETFLOW
      6. Применить Policy Map под названием NETFLOW на интерфейсе E0/1.67
      7. Настроить Netflow Aggregation Cache следующим образом:
         1. В качестве группировки указать Destination Prefix
         2. Разрешить кэш агрегации в 1024 записи
         3. Настроить таймаут активности в течении 15 минут
         4. Настроить таймаут неактивности в течении 1 минуту
         5. Применить на на входе в интерфейс E0/1.67
         6. Экспортировать кэш на удаленный коллектор, указанный в пункте 4с

## [Цикл 18, Лабораторная работа по теме 105: IPv4 Multicast Routing](http://ccie.linkmeup.ru/2017/03/10/laba-po-tsiklu-18-tema-105-ipv4-multicast-routing/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfYWp5M1ZCd1NUcnc) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На всех маршрутизаторах настроить Named EIGRP процесс 100 под названием AUTO-RP на всех интерфейсах
4. На всех маршрутизаторах настроить IP Multicast Routing
5. На всех маршрутизаторах настроить Sparse — Dense Mode на следующих интерфейсах:
   1. R1 — E0/1.12, Loopback0
   2. R2 — E0/1.12, E0/1.23, E0/1.235, Loopback0
   3. R3- E0/1.34, E0/1.23, E0/1.235
   4. R4 — E0/1.456, E0/1.34, Loopback0
   5. R5 — E0/1.456, E0/1.235
   6. R6 -E0/1.67, E0/1.456, Loopback0
   7. R7 — E0/1.78, E0/1.67
   8. R8 — E0/1.78, E0/1.89
   9. R9 — E0/1.89, Multilink 1
   10. R10 — Multilink 1, Loopback0
6. Настроить маршрутизатор R2 в качестве Mapping Agent’a следующим образом:
   1. Настроить команду аннонсирования RP Discovery:
      1. Источник- интерфейс Loopback 0
      2. Значение TTL= 255
      3. Частота отправки 5 секунд
7. Настроить маршрутизатор R4 в качестве RP следующим образом:
   1. Настроить команду аннонсирования RP Announce:
      1. Источник- интерфейс Loopback 0
      2. Значение TTL= 255
      3. Частота отправки 5 секунд
8. Настроить маршрутизатор R6 в качестве RP следующим образом:
   1. Настроить команду аннонсирования RP Announce:
      1. Источник- интерфейс Loopback 0
      2. Значение TTL= 255
      3. Частота отправки 5 секунд
9. На маршрутизаторе R2 изменить наименование DNS имен для R4 и R6 соотвественно на RP\_4 и RP\_6 и проверить применение DNS имен
10. Настроить маршрутизатор R6 качестве DR для маршрутизатора R7 с приоритетом равным 10
11. Настроить маршрутизатор R7 качестве DR для маршрутизатора R8 с приоритетом равным 10
12. Настроить маршрутизатор R8 качестве DR для маршрутизатора R9 с приоритетом равным 10
13. Настроить интерфейс Loopback0 маршрутизатора R1 в качестве клиента группы 224.1.1.1
14. Настроить обработку мультикастовой группы диапазоном 224.0.0.0/7 на R4 следущим образом:
    1. Изменить команду аннонсирования RP Announce:
       1. Источник- интерфейс Loopback 0
       2. Значение TTL= 255
       3. Создать ACL под номером 10, разрешить диапазон 224.0.0.0/7
       4. Частота отправки 5 секунд
15. Настроить обработку мультикастовой группы диапазоном 224.0.0.0/7 на R6 следущим образом:
    1. Изменить команду аннонсирования RP Announce:
       1. Источник- интерфейс Loopback 0
       2. Значение TTL= 255
       3. ACL 10, разрешить диапазон 232.0.0.0/7
       4. Частота отправки 5 секунд

## [Цикл 18, Лабораторная работа по теме 106: BGP 3.7](http://ccie.linkmeup.ru/2017/03/13/tsikl-18-laboratornaya-rabota-po-teme-106-bgp-3-7/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxUXdrUzQ3ZjFxdmc) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3, R5 настроить OSPF процесс 100 в Аrea 104 на всех интерфейсах:
   1. указать в качестве пассивных:
      1. R3- интерфейс E0/1.34
      2. R5- интерфейс E0/1.456
4. На маршрутизаторе R4 настроить OSPF процесс 100 в Аrea 4 на всех интерфейсах. Указать качестве пассивных:
   1. интерфейс E0/1.34
   2. интерфейс E0/1.456
5. На маршрутизаторах R6, R7, R8, R9, R10 настроить OSPF процесс 100 в Аrea 107 на всех интерфейсах:
   1. указать в качестве пассивных:
      1. интерфейс E0/1.456
6. На маршрутизаторах R1, R2, R3, R5 настроить внутренний и внешний BGP процесс следующим образом:
   1. Настроить внутренний bgp процесс:
      1. Номер AS — 51
      2. Создать bgp сессию следующим образом:
         1. Указать в качестве Remote AS номер 51
         2. Указать в качестве соседей IP адреса интерфейсов Loopback 0
         3. Настроить интервал задержки информирования BGP об изменениях в RIB в 6 секунд
         4. На R3 и R5 настроить команду, при которой все Next Hop адреса узнаются через OSPF
   2. Настроить внешний bgp процесс на R3 и R5:
      1. Номер AS — 51
      2. Создать bgp сессию следующим образом:
         1. Указать в качестве Remote AS номер 104
         2. Указать в качестве соседей IP адреса интерфейсов Loopback 0
         3. Настроить интервал задержки информирования BGP об изменениях в RIB в 6 секунд
         4. Позволить увеличение значения TTL только до 2 хопов
   3. На маршрутизаторе R4 настроить Confederation BGP процесс следующим образом:
   4. Номер AS — 4
   5. Создать внешнюю bgp сессию на R4 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 104
      2. Указать в качестве пира конфедерации 106
      3. Настроить Peer Group под названием EXTERNAL:
         1. Указать в качестве Remote AS номер 51
         2. Позволить увеличение значения TTL только до 2 хопов
         3. Указать в качестве соседей IP адреса интерфейсов Loopback 0
         4. Включить в группу маршрутизаторы R3 и R5
      4. Настроить Peer Group под названием CONF:
         1. Указать в качестве Remote AS номер 106
         2. Позволить увеличение значения TTL только до 2 хопов
         3. Указать в качестве соседей IP адреса интерфейсов Loopback 0
         4. Включить в группу маршрутизатор R6
7. Создать внешнюю bgp сессии на R6 следующим образом:
   1. Указать в качестве Remote AS номер
   2. Указать в качестве идентификатора конфедерации номер AS 104
   3. Позволить увеличение значения TTL только до 2 хопов
   4. Указать в качестве соседа IP адрес интерфейсов Loopback 0 маршрутизатора R4
   5. Создать внутренюю bgp сессию на R6 следующим образом:
      1. Указать в качестве Remote AS номер 106
      2. Указать в качестве соседей IP адреса интерфейсов Loopback
      3. Настроить команду, при которой все Next Hop адреса узнаются через OSPF
      4. Указать в качестве соседа IP адрес интерфейс Loopback 0 маршрутизатора R7
8. На маршрутизаторах R7, R8, R9, R10 настроить внутренний BGP процесс следующим образом:
   1. Номер AS — 106
   2. Настроить интервал задержки информирования BGP об изменениях в RIB в 6 секунд
   3. Настроить Peer Group под названием LOCAL:
      1. Указать в качестве Remote AS номер 106
      2. Указать в качестве соседей IP адреса интерфейсов Loopback 0
      3. Включить в группу:
         1. На R7 маршрутизаторы R6 и R8
         2. На R8 маршрутизаторы R7 и R9
         3. На R9 маршрутизаторы R8 и R10
         4. На R10 маршрутизатор R9
9. На маршрутизаторах R3 и R4 настроить статические маршруты к друг другу следующим образом:
   1. В качестве маршрута указать IP адрес Loopback0 интерфейса друг друга
   2. В качестве Next Hop указать IP адрес интерфейса E0/1.34 друг друга.
10. На маршрутизаторах R4 и R5 настроить статические маршруты к друг другу следующим образом:
    1. В качестве маршрута указать IP адрес Loopback0 интерфейса друг друга
    2. В качестве Next Hop указать IP адрес интерфейса E0/1.456 друг друга.
11. На маршрутизаторах R4 и R6 настроить статические маршруты к друг другу следующим образом:
    1. В качестве маршрута указать IP адрес Loopback0 интерфейса друг друга
    2. В качестве Next Hop указать IP адрес интерфейса E0/1.456 друг друга.

## [Цикл 18, Лабораторная работа по теме 107: DHCPv6](http://ccie.linkmeup.ru/2017/03/15/tsikl-18-laboratornaya-rabota-po-teme-107-dhcpv6/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfTGd2QURLM0hkQ2M) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Маршрутизатор R6 настроить в качестве Stateless DHCPv6 Server’a для R4 следующим образом:
   1. Включить IPv6 Unicast Routing
   2. DHCP пул под названием DHCP\_STATELESS
   3. DNS Server c адресом 2001:CC1E:1:45::100
   4. имя домена [ccie.linkmeup.ru](http://ccie.linkmeup.ru/)
   5. Настроить интерфейс E0/1.456 следующим образом:
      1. Указать пул для сервера — DHCP\_STATELESS с опцией Rapid Commit
      2. Указать, чтобы отправлялся флаг “other stateful configuration” в RA ipv6
4. На интерфейсе E0/1.34 маршрутизатора R4 включить работу и автонастройку IPv6.
5. Маршрутизатор R6 настроить в качестве Stateful DHCPv6 Server’a следующим образом для R7:
   1. DHCP пул под названием DHCP\_STATEFUL
   2. DNS Server c адресом 2001:CC1E:1:67::100
   3. имя домена [ccie.linkmeup.ru](http://ccie.linkmeup.ru/)
   4. Указать префикс 2001:CC1E:1:45::0/64
   5. Настроить интерфейс E0/1.67 следующим образом:
      1. Указать пул для сервера — DHCP\_STATEFUL с опцией Rapid Commit
      2. Указать, чтобы отправлялся флаг “other stateful configuration” в RA ipv6
6. На интерфейсе E0/1.67 маршрутизатора R7 включить работу IPv6 c опцией DHCP и Rapid Commit.
7. Настроить маршрутизаторы R5, R3 и R2 используя Prefix Delegation следующим образом:
   1. Настроить R5 в качестве DHCPv6 Server’a:
      1. DHCP пул под названием PREFIX\_DELEGATION
      2. Настроить время lifetime 1800 600
      3. DNS Server c адресом 2001:CC1E:1:235::100
      4. имя домена [ccie.linkmeup.ru](http://ccie.linkmeup.ru/)
      5. Настроить делегирование префикса /48 из диапазона 2001:CC1E:1::/40
      6. Настроить интерфейс E0/1.235 с указанием пула PREFIX\_DELEGATION для сервера
   2. Настроить R3 в качестве DHCPv6 Client’a:
      1. Настроить Unicast Routing
      2. Настроить интерфейс E0/1.235 следующим образом:
         1. включить работу IPv6
         2. включить автонастройку с опцией Default
         3. Настроить делегирование префиксов DHCP-клиенту от DHCP Server’a с наименованием PREFIX\_FROM\_SERVER
      3. Настроить интерфейс E0/1.23 таким образом, чтобы он отдавал первый адрес из диапазона пула PREFIX\_DELEGATION с префиксом /64
   3. Настроить интерфейс E0/1.23 маршрутизатора R2 в качестве DHCPv6 Client’a с автонастройкой

## [Цикл 18, Лабораторная работа по теме 108: BGP 3.7](http://ccie.linkmeup.ru/2017/03/17/tsikl-18-laboratornaya-rabota-po-teme-108-bgp-3-7/)

1. Для начальной конфигурации всех устройств используется конечная конфигурация лабораторной работы 106.
2. Для задания используется логическая и физическая топологии проекта.
3. Загрузить начальную конфигурацию всех устройств.
4. Для задания используется логическая и физическая топологии проекта.
5. На маршрутизаторе R4 переделать BGP процесс следующим образом:
   1. Исключить из Peer Group под названием EXTERNAL маршрутизатор R5:
   2. Применить к R5 следующие значения:
      1. Указать Remote AS 51
      2. Позволить увеличение значения TTL только до 2 хопов
      3. Указать в качестве соседей IP адреса интерфейсов Loopback 0
6. Редистрибьютить маршруты OSPF во внешнюю bgp сессию на R6 следующим образом:
   1. Создать ACL под названием FROM\_R6, где разрешить префикс 180.1.0.0/20
   2. Создать Route Map под названием FROM\_R6, где заматчить ACL под названием FROM\_R6
   3. Редистрибьютить OSPF процесс 100 Route Map под названием FROM\_R6 и метрикой 50
7. На маршрутизаторе R3 адвертайзить маршрут 188.1.23.0/24 в BGP процесс
8. На маршрутизаторе R4 настроить BGP Conditional Advertisement следующим образом:
   1. Создать ACL под номером 60, где разрешить префикс 0.0.0.0/0
   2. Создать ACL под номером 65, где разрешить префикс 180.1.23.0/24
   3. Создать Route Map под названием NON-EXIST, где заматчить ACL под номером 65
   4. Создать Route Map под названием ADVERTISE, где заматчить ACL под номером 60
   5. Настроить адвертайзинг префикс 0.0.0.0/0 в отношении R5, только в том случае, если от R3 перестанет приходить маршрут 188.1.23.0/24

# [**Цикл 19**](http://ccie.linkmeup.ru/2017/03/24/voprosy-po-tsiklu-18-tema-109-ospf/)

## [Цикл 19, Лабораторная работа по теме 109: OSPF 3.6](http://ccie.linkmeup.ru/2017/03/27/tsikl-19-laboratornaya-rabota-po-teme-109-ospf-3-6/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxRzdmNzN6Vnl6cG8) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3, R4, R5 настроить OSPF процесс 100 в Аrea 51 на следующих интерфейсах c типом сети Point-to-Point:
   1. R1 — E0/1.12, Loopback0
   2. R2- E0/1.12, Loopback0
   3. R3- E0/1.34, Loopback0
   4. R4- E0/1.34, Loopback0
   5. R5- E0/1.235, Loopback0
4. На маршрутизаторах R2, R3, R5 настроить OSPF процесс 100 в Аrea 51 на следующих интерфейсах c типом сети Broadcast:
   1. R2 — E0/1.235, E0/1.23
   2. R3- E0/1.235, E0/1.23
   3. R5- E0/1.235
5. На маршрутизаторах R4, R5 настроить OSPF процесс 100 в Аrea 0 на следующих интерфейсах c типом сети Point-to-Point:
   1. R4- E0/1.456
   2. R5 — E0/1.456
   3. Настроить аутентификацию MD5 с паролем OSPF\_EXT
6. На маршрутизаторах R6, R7, R8, R9, R10 настроить OSPF процесс 107 в Аrea 76 на следующих интерфейсах:
   1. R6 — E0/1.67, Loopback0
   2. R7- E0/1.67, E0/1.78, Loopback0
   3. R8- E0/1.78, E0/1.89, Loopback0
   4. R9- E0/1.89, Multilink1, Loopback0
   5. R10- Multilink1, Loopback0
7. На маршрутизаторе R6 настроить следующие статические маршруты:
   1. Маршрут по-умолчанию 0.0.0.0/0, в качестве Next Hop указать интерфейс Null0
   2. Маршрут 180.1.4.4/32, в качестве Next Hop указать IP адрес интерфейса E0/1.456 маршрутизатора R4
8. На маршрутизаторе R4 настроить следующие статические маршруты:
   1. Маршрут 180.1.6.6/32, в качестве Next Hop указать IP адрес интерфейса E0/1.456 маршрутизатора R6
9. На маршрутизаторе R6 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 107
   2. Создать ebgp сессию c маршрутизатором R4 следующим образом:
      1. Указать в качестве Remote AS номер 51
      2. Позволить увеличение значения TTL только до 2 хопов
      3. Указать в качестве Update Source интерфейс Loopback0
      4. Адвертайзить маршрут маршрут по-умолчанию
10. На маршрутизаторе R6 в процессе OSPF 107 редистрибьютить BGP процесс 107
11. На маршрутизаторе R4 настроить внешний BGP процесс следующим образом:
    1. Номер AS — 51
    2. Создать ebgp сессию c маршрутизатором R6 следующим образом:
       1. Указать в качестве Remote AS номер 107
       2. Позволить увеличение значения TTL только до 2 хопов
       3. Указать в качестве Update Source интерфейс Loopback0
       4. Редистрибьютить OSPF процесс 100 с метрикой 5
12. На маршрутизаторах R1, R2, R3, R4, R5 настроить внутренний BGP процесс следующим образом:
    1. Номер AS — 51
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название INTERNAL
          2. Указать в качестве Remote AS номер 51
          3. Указать в качестве Update Source интерфейс Loopback0
13. На маршрутизаторах R6, R7, R8, R9, R10 настроить внутренний BGP процесс следующим образом:
    1. Номер AS — 107
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название INTERNAL
          2. Указать в качестве Remote AS номер 107
          3. Указать в качестве Update Source интерфейс Loopback0
14. На интерфейсе E0/1.12 маршрутизаторов R1 и R2 отключить DoNotAge флаг в обновлениях OSPF.
15. Настроить интерфейсы E0/1.23 и E0/1.235 на маршрутизаторах R2, R3, R5 таким образом, чтобы транзитные маршруты от R2 до R4 не отображались в таблице маршрутизации R4.
16. На маршрутизаторах R1, R2, R6, R7, R8,R9, R10 настроить Incremental SPF
17. Настроить маршрутизатор R6 следующим образом:
    1. В LSDB должны сохраняться не более 5000 LSA
    2. Не более 5 маршрутов могут передаваться через редистрибьюцию
18. Настроить NSF на маршрутизаторах R4 и R5 следующим образом:
    1. R4 — включить NSF для Cisco:
       1. отключить Helper для Cisco
       2. включить IETF Helper
    2. R5 — включить NSF для IETF:
       1. включить Helper для Cisco
       2. отключить IETF Helper

## [Цикл 19, Лабораторная работа по теме 110: Miscellaneous Network Services 9.8](http://ccie.linkmeup.ru/2017/03/29/tsikl-19-laboratornaya-rabota-po-teme-110-miscellaneous-network-services-9-8/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0B8TdfSzCKkaxTF91M3d0eU5sUzQ) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Маршрутизатор R2 настроить следующим образом:
   1. Отключить IP Routing
   2. Настроить GDP IRDP
4. На маршрутизаторах R3 и R5 настроить IRDP следующим образом:
   1. R3 — E0/1.23, адресс 192.168.23.3 с приоритетом 100 и максимальной временем синхронизации 4 с
   2. R5 — E0/1.235 адресс 192.168.235.35 с приоритетом 200 и максимальной временем синхронизации 4 с
5. Настроить Proxy ARP на маршрутизаторах R3 и R5 на следующих интерфейсах:
   1. R3- E0/1.23
   2. R4- E0/1.235
6. На маршрутизаторах R3 и R4 настроить OSPF процесс 100 в Аrea 34 на следующих интерфейсах:
   1. R3 — E0/1.34, Loopback0
   2. R4- E0/1.34:
7. На маршрутизаторах R4, R5, R6 настроить OSPF процесс 100 в Аrea 0 на следующих интерфейсах:
   1. R4 — E0/1.456, Loopback0
   2. R5- E0/1.456, Loopback0
   3. R6- E0/1.456, Loopback0
8. На маршрутизаторах R7, R8, R9, R10 настроить OSPF процесс 100 в Аrea 107 на следующих интерфейсах:
   1. R7 — E0/1.78, Loopback0
   2. R8- E0/1.78, E0/1.89, Loopback0
   3. R9- E0/1.89, Multilink1, Loopback0
   4. R10 — Multilink1, Loopback0
9. На маршрутизаторе R6 настроить следующие статические маршруты:
   1. Маршрут по-умолчанию 0.0.0.0/0, в качестве Next Hop указать интерфейс Null0
   2. Маршрут 180.1.7.7/32, в качестве Next Hop указать IP адрес интерфейса E0/1.67 маршрутизатора R7
10. На маршрутизаторе R7 настроить следующие статические маршруты:
    1. Маршрут 180.1.6.6/32, в качестве Next Hop указать IP адрес интерфейса E0/1.67 маршрутизатора R6
11. На маршрутизаторе R6 настроить BGP процесс следующим образом:
    1. Номер AS — 6
    2. Адвертайзить маршрут по-умолчанию, не используя редистрибьюцию
    3. ID конфедерации — 456
    4. Указать в качестве пира конфедерации 2345
    5. Создать внутреннюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название INTERNAL
          2. Указать в качестве Remote AS номер 2345
          3. Указать в качестве Update Source интерфейс Loopback0
          4. Позволить увеличение значения TTL только до 2 хопов
          5. Применить к маршрутизаторам R4, R5, указав IP адреса их Loopback интерфейсов
    6. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EXTERNAL
          2. Указать в качестве Remote AS номер 107
          3. Указать в качестве Update Source интерфейс Loopback0
          4. Позволить увеличение значения TTL только до 2 хопов
          5. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R7
12. На маршрутизаторе R7 настроить BGP процесс следующим образом:
    1. Номер AS — 7
    2. Редистрибьютить OSPF процесс 100
    3. ID конфедерации — 107
    4. Указать в качестве пира конфедерации 8
    5. Создать внутренюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название INTERNAL
          2. Указать в качестве Remote AS номер 8
          3. Указать в качестве Update Source интерфейс Loopback0
          4. Позволить увеличение значения TTL только до 2 хопов
          5. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R8
    6. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EXTERNAL
          2. Указать в качестве Remote AS номер 456
          3. Указать в качестве Update Source интерфейс Loopback0
          4. Позволить увеличение значения TTL только до 2 хопов
          5. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R6
13. На маршрутизаторе R3 настроить BGP процесс следующим образом:
    1. Номер AS — 2345
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название INTERNAL
          2. Указать в качестве Remote AS номер 2345
          3. Указать в качестве Update Source интерфейс Loopback0
          4. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R4
14. На маршрутизаторах R4 и R5 настроить BGP процесс следующим образом:
    1. Номер AS — 2345
    2. ID конфедерации — 456
    3. Указать в качестве пира конфедерации 6
    4. Создать внутренюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название INTERNAL
          2. Указать в качестве Remote AS номер 2345
          3. Указать в качестве Update Source интерфейс Loopback0
          4. Позволить увеличение значения TTL только до 2 хопов
          5. В качестве соседа указать IP адреса Loopback интерфейсы следующих маршрутизаторов:
             1. На R4- R3 и R5
             2. На R5 — R4
    5. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EXTERNAL
          2. Указать в качестве Remote AS номер 6
          3. Указать в качестве Update Source интерфейс Loopback0
          4. Позволить увеличение значения TTL только до 2 хопов
          5. В качестве соседа указать IP адрес Loopback интерфейс маршрутизатора R6
15. На маршрутизаторах R6, R7, R8, R9, R10 настроить внутренний BGP процесс следующим образом:
    1. Номер AS — 107
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название INTERNAL
          2. Указать в качестве Remote AS номер 107
          3. Указать в качестве Update Source интерфейс Loopback0
16. Настроить DMVPN Phase 3 следующим образом:
    1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
       1. Настроить интерфейс Tunnel0:
          1. IP адрес — 188.1.100.7/24
          2. Аутентификация NHRP — PROXYARP
          3. Настроить динамическую поддержку мультикаста
          4. NHRP ID — 100
          5. Настроить NHRP Redirect
          6. Источник — интерфейс Ethernet 0/1.144
          7. Режим — GRE Multipoint
          8. Ключ туннеля 10000
    2. Настроить маршрутизаторы R3, R4, R6 качеcтве Spok’ов:
       1. Настроить интерфейс Tunnel0:
          1. IP адрес — использовать Overlay адрес топологии
          2. Аутентификация NHRP — PROXYARP
          3. Настроить маппинг мультикаста к R7
          4. NHRP ID — 100
          5. В качестве сервера NHRP NHS указать R7
          6. Настроить NHRP Shortcut
          7. Источник — интерфейс Ethernet 0/1.144
          8. Режим — GRE Multipoint
          9. Ключ туннеля 10000
17. На маршрутизаторах R3, R4, R6, R7 настроить EIGRP процесс следующим образом:
    1. Номер процесса 100
    2. Следующие интерфейсы устройств должны участвовать в процессе:
       1. R3 — Интерфейс Tunnel 0
       2. R4- Интерфейс Tunnel 0
       3. R6- Интерфейс Tunnel 0
       4. R7 — Интерфейс Tunnel 0
    3. Настроить редистрибьюцию на HUB’e из OSPF 100 в EIGRP 100 со следующими показателями метрики:
       1. BW- 1000000
       2. DLY-1
       3. Reliability — 255
       4. Loading — 1
       5. MTU — 1400

## [Цикл 19, Лабораторная работа по теме 111: IPv4 Multicast Routing](http://ccie.linkmeup.ru/2017/04/03/tsikl-19-laboratornaya-rabota-po-teme-111-ipv4-multicast-routing/)

1. Для задания используется конечная конфигурация лабораторной работы 110.
2. На маршрутизаторах R2, R3, R4, R6, R7, R8, R9, R10 настроить IP Multicast Routing
3. На маршрутизаторах R2, R3, R4, R6, R7, R8, R9, R10 настроить Sparse-Dense Mode на следующих интерфейсах:
   1. R2 — E0/1.23, E0/1.235
   2. R3- E0/1.23, E0/1.34, Tunnel 0
   3. R4 — E0/1.34, Tunnel 0
   4. R5 — E0/1.456, E0/1.235
   5. R6 -E0/1.456, Tunnel 0
   6. R7 — E0/1.78, Tunnel 0
   7. R8 — E0/1.78, E0/1.89
   8. R9 — E0/1.89, Multilink 1
   9. R10 — Multilink 1, Loopback 0
4. Настроить маршрутизаторы R3 и R7 в качестве C-BSR таким следующим образом:
   1. Настроить в качестве RP кандидатов
   2. BSR адреса должы браться с интерфейса Loopback0
   3. Настроить таким образом, чтобы первые 4 группы мультикастовых адресов диапазона 224.1.1.0 назначались R7
5. Настроить интерфейс Loopback0 маршрутизатора R10 в качестве клиента группы 224.10.10.10

# 

## [Цикл 19, Лабораторная работа по темам 112 и 114: BGP](http://ccie.linkmeup.ru/2017/04/16/tsikl-19-laboratornaya-rabota-po-temam-112-i-114-bgp/)

1. Задание объединенное для тем 112 и 114
2. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfS3UxQzYzOWhVdXc) всех устройств.
3. Для задания используется логическая и физическая топологии проекта.
4. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 12, на следующих интерфейсах:
   1. R1- E0/1.12, Интерфейс Loopback0
   2. R2- E0/1.12
5. На маршрутизаторах R2, R3 настроить OSPF процесс 100 в Аrea 23, на следующих интерфейсах:
   1. R2- E0/1.23, Интерфейс Loopback0
   2. R3- E0/1.23, Интерфейс Loopback0
6. На маршрутизаторах R3, R4 настроить OSPF процесс 100 в Аrea 34, на следующих интерфейсах:
   1. R3- E0/1.34
   2. R4- E0/1.34
7. На маршрутизаторах R4, R6 настроить OSPF процесс 100 в Аrea 456 на следующих интерфейсах:
   1. R4 — E0/1.456, Интерфейс Loopback0
   2. R6 — E0/1.456, Интерфейс Loopback0
8. На маршрутизаторах R8,R9,R10 настроить OSPF процесс 100 в Аrea 108, на следующих интерфейсах:
   1. R8- E0/1.78, E0/1.89,Интерфейс Loopback0
   2. R9- E0/1.89, Интерфейс Loopback0, Интерфейс Multilink1
   3. R10- Интерфейс Loopback0, Интерфейс Multilink1
9. На маршрутизаторе R1 настроить BGP процесс следующим образом:
   1. Номер AS — 1
   2. Создать внешнюю bgp сессию следующим образом:
      1. Указать в качестве Remote AS номер 237
      2. Указать в качестве Update Source интерфейс Loopback0
      3. Позволить увеличение значения TTL только до 2 хопов
      4. Применить к маршрутизатору R2, указав IP адреса их Loopback интерфейсов
10. На маршрутизаторе R1 настроить статический маршрут к IP адресу интерфейса Loopback 0 маршрутизатора R2. В качестве Next Hop указать IP адрес интерфейса E0/1.12
11. На маршрутизаторе R2 настроить BGP процесс следующим образом:
    1. Номер AS — 237
    2. Редистрибьютить OSPF процесс 100 с метрикой 20
    3. Адвертайзить маршруты 188.1.235.0/24 и 180.1.1.1/32 не используя редистрибьютинг
    4. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R3
          4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Указать в качестве Update Source интерфейс Tunnel0
       3. В качестве соседа указать IP адрес Tunnel0 интерфейса маршрутизатора R7
    5. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R1, R5
12. На маршрутизаторе R2 настроить статические маршруты к IP адресам интерфейса Loopback 0 маршрутизаторов R1 и R5. В качестве Next Hop указать IP адреса интерфейсов E0/1.12 и E0/1.235 соответственно
13. На маршрутизаторе R3 настроить BGP процесс следующим образом:
    1. Номер AS — 237
    2. Редистрибьютить OSPF процесс 100 с метрикой 20
    3. Адвертайзить маршрут 188.1.235.0/24 не используя редистрибьютинг
    4. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R2
          5. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Указать в качестве Update Source интерфейс Tunnel0
       3. В качестве соседа указать IP адрес Tunnel0 интерфейса маршрутизатора R7
    5. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R4, R5
14. На маршрутизаторе R3 настроить статические маршруты к IP адресам интерфейса Loopback 0 маршрутизаторов R4 и R5. В качестве Next Hop указать IP адреса интерфейсов E0/1.34 и E0/1.235 соответственно
15. На маршрутизаторе R4 настроить BGP процесс следующим образом:
    1. Номер AS — 46
    2. Редистрибьютить OSPF процесс 100 с метрикой 20
    3. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R6
          5. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
    4. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R3, R5
       2. Указать в качестве Update Source интерфейс Tunnel0
       3. В качестве соседа указать IP адрес Tunnel0 интерфейса маршрутизатора R7
16. На маршрутизаторе R4 настроить статические маршруты к IP адресам интерфейса Loopback 0 маршрутизаторов R3 и R5. В качестве Next Hop указать IP адреса интерфейсов E0/1.34 и E0/1.456 соответственно
17. На маршрутизаторе R5 настроить BGP процесс следующим образом:
    1. Номер AS — 5
    2. Адвертайзить маршрут 188.1.235.0/24 не используя редистрибьютинг
    3. Создать внешние ebgp сессии следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP237
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R2, R3
       2. Создать BGP Peer Group:
          1. Название EBGP46
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R4, R6
18. На маршрутизаторе R5 настроить статические маршруты к IP адресам интерфейса Loopback 0 маршрутизаторов R2, R3, R4, R5. В качестве Next Hop указать IP адреса интерфейсов E0/1.235 и E0/1.456 соответственно
19. На маршрутизаторе R6 настроить BGP процесс следующим образом:
    1. Номер AS — 46
    2. Адвертайзить маршрут 188.1.45.0/24 не используя редистрибьютинг
    3. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R4
    4. Создать внешние ebgp сессии следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R5, R7
       2. Указать в качестве Update Source интерфейс Tunnel0
       3. В качестве соседа указать IP адрес Tunnel0 интерфейса маршрутизатора R7
20. На маршрутизаторе R6 настроить статические маршруты к IP адресам интерфейса Loopback 0 маршрутизаторов R5 и R7. В качестве Next Hop указать IP адреса интерфейсов E0/1.67 и E0/1.456 соответственно
21. На маршрутизаторе R7 настроить BGP процесс следующим образом:
    1. Номер AS — 237
    2. Адвертайзить маршруты 180.1.7.7/32, 188.1.67.0/24, 188.1.78.0/24 не используя редистрибьютинг
    3. Создать ebgp сессии следующим образом:
       1. Создать BGP Peer Group:
          1. Название GREEN
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседа указать IP адрес Loopback интерфейса маршрутизаторов R6, R8
       2. Настроить VRF под названием BLUE:
          1. Address-Family IPv4
          2. Создать BGP Peer Group:
             1. Название BLUE
             2. Указать в качестве Update Source интерфейс Tunnel0
             3. Позволить увеличение значения TTL только до 2 хопов
             4. В качестве соседа указать IP адрес интерфейса Tunnel0 маршрутизаторов R4, R6
       3. Настроить VRF под названием RED:
          1. Address-Family IPv4
          2. Создать BGP Peer Group:
             1. Название RED
             2. Указать в качестве Update Source интерфейс Tunnel0
             3. В качестве соседа указать IP адрес Tunnel0 интерфейса маршрутизаторов R2, R3
22. На маршрутизаторе R7 настроить статические маршруты к IP адресам интерфейса Loopback 0 маршрутизаторов R6 и R8. В качестве Next Hop указать IP адреса интерфейсов E0/1.67 и E0/1.78 соответственно
23. На маршрутизаторе R8 настроить BGP процесс следующим образом:
    1. Номер AS — 108
    2. Редистрибьютить OSPF процесс 100 с метрикой 20
    3. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейсов маршрутизатора R9
    4. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R7
24. На маршрутизаторе R8 настроить статические маршруты к IP адресу интерфейса Loopback 0 маршрутизатора R7. В качестве Next Hop указать IP адрес интерфейса E0/1.78 соответственно
25. На маршрутизаторе R9 настроить BGP процесс следующим образом:
    1. Номер AS — 108
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейсов маршрутизаторов R8, R10
26. На маршрутизаторе R10 настроить BGP процесс следующим образом:
    1. Номер AS — 108
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейсов маршрутизаторов R9
27. Настроить DMVPN Phase 3 следующим образом:
    1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
       1. Настроить интерфейс Tunnel0:
          1. Настроить VRF Forwarding под название BLUE
          2. IP адрес — 188.1.100.7/24
          3. Настроить значение MTU 1400
          4. Настроить Adjust MSS 1360
          5. Аутентификация NHRP — BGP
          6. Настроить динамическую поддержку мультикаста
          7. NHRP ID — 100
          8. Источник — интерфейс Ethernet 0/1.144
          9. Режим — GRE Multipoint
          10. Ключ туннеля 10000
       2. Настроить интерфейс Tunnel1:
          1. Настроить VRF Fotwarding под название RED
          2. IP адрес — 188.1.100.7/24
          3. Настроить значение MTU 1400
          4. Настроить Adjust MSS 1360
          5. Аутентификация NHRP — IBGP
          6. Настроить динамическую поддержку мультикаста
          7. NHRP ID — 200
          8. Источник — интерфейс Ethernet 0/1.144
          9. Режим — GRE Multipoint
          10. Ключ туннеля 20000
    2. Настроить маршрутизаторы R2, R3 качеcтве Spok’ов для VRF RED:
       1. Настроить интерфейс Tunnel0:
          1. IP адрес — использовать Overlay адрес топологии
          2. Аутентификация NHRP — IBGP
          3. Настроить динамическую поддержку мультикаста
          4. NHRP ID — 200
          5. В качестве сервера NHRP указать R7
          6. Источник — интерфейс Ethernet 0/1.144
          7. Ключ туннеля 20000
    3. Настроить маршрутизаторы R4, R6 качеcтве Spok’ов для VRF BLUE:
       1. Настроить интерфейс Tunnel0:
          1. IP адрес — использовать Overlay адрес топологии
          2. Аутентификация NHRP — EBGP
          3. Настроить динамическую поддержку мультикаста
          4. NHRP ID — 100
          5. В качестве сервера NHRP указать R7
          6. Источник — интерфейс Ethernet 0/1.144
          7. Ключ туннеля 10000
28. На маршрутизаторае R7 проверить таблицу маршрутизации BGP для VRF RED и BLUE
29. На маршрутизаторе R5 настроить приоритетность маршрутов пришедших от AS 108 следующим образом:
    1. Настроить IP AS-PATH ACL под номером 10 и разрешить AS 108
    2. Настроить Route Map под названием R4\_R5:
       1. Заматчить IP AS-PATH ACL под номером 10
       2. Применить значение Weigth равное 20000
    3. Настроить Route Map под названием R6\_R5:
       1. Заматчить IP AS-PATH ACL под номером 10
       2. Применить значение Weigth равное 50000
    4. Применить Route Map под названием R4\_R5 к соседу R4 в процессе BGP 5
    5. Применить Route Map под названием R6\_R5 к соседу R4 в процессе BGP 5
30. На маршрутизаторе R2 настроить приоритетность маршрута 180.1.2.2/32 в VRF RED R7 следующим образом:
    1. Настроить Prefix List’ы под названием Set\_Pref и номером 5, где разрешить 180.1.2.2/32
    2. Настроить Route Map под названием PREF:
       1. Заматчить Prefix List под названием Set\_Pref
       2. Применить значение Local Preference равное 500
       3. Применить на выходе к R7 в процессе BGP
31. На маршрутизаторе R3 настроить приоритетность маршрута 180.1.3.3/32 в VRF RED R7 следующим образом:
    1. Настроить ACL под номером 10, где разрешить 180.1.3.3/32
    2. Настроить Route Map под названием MED:
       1. Заматчить ACL под номером 10
       2. Применить значение MED 0
       3. Применить на выходе к R7 в процессе BGP
32. На маршрутизаторе R7 проверить результат.

# 

# [**Цикл 20**](http://ccie.linkmeup.ru/2017/10/02/voprosy-po-tsiklu-20-tema-115-mpls-4-1/)

## [Цикл 20, Лабораторная работа по теме 115-116: MPLS, Miscellaneous Network Services](http://ccie.linkmeup.ru/2017/10/04/tsikl-20-laboratornaya-rabota-po-teme-115-116-mpls-miscellaneous-network-services/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfcjhObE9waHJMTFk) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. Настроить маршрутизатор R7 в качестве хаба DMVPN следующим образом:
   1. Настроить фазу 1 IPsec на R7 следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «VPN\_VRF» должен служить адрес 0.0.0.0/24
   2. Настроить фазу 2 IPsec на R7 следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием VPN\_VRF:
         1. применить Transform Set под названием ESP\_3DES\_SHA
4. На R7 на интерфесе Tunnel 0 применить IPSec Profile VPN\_VRF
   1. Настроить интерфейс Tunnel0:
      1. Настроить VFR Forwarding — GREEN
      2. IP адрес — 188.1.100.71/24
      3. Аутентификация NHRP — VRFGREEN
      4. Настроить динамическую поддержку мультикаста
      5. NHRP ID — 100
      6. Источник — интерфейс Ethernet 0/1.144
      7. Режим — GRE Multipoint
      8. Ключ туннеля 10000
      9. Применить профиль VPN\_VRF с ключом shared
5. На R7 на интерфесе Tunnel 1 применить IPSec VPN\_VRF
   1. Настроить интерфейс Tunnel1:
      1. Настроить VFR Forwarding — RED
      2. IP адрес — 188.1.100.72/24
      3. Аутентификация NHRP — VRF\_RED
      4. Настроить динамическую поддержку мультикаста
      5. NHRP ID — 200
      6. Источник — интерфейс Ethernet 0/1.144
      7. Режим — GRE Multipoint
      8. Ключ туннеля 20000
      9. Применить профиль VPN\_VRF с ключом shared
6. Настроить маршрутизаторы R2, R3 качеcтве Spok’ов VRF GREEN следующим образом:
   1. Настроить фазу 1 IPsec на R2 и R3 следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «VPN\_VRF» должен служить адрес 0.0.0.0/24
   2. Настроить фазу 2 IPsec на R2 и R3 следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием VPN\_VRF:
         1. применить Transform Set под названием ESP\_3DES\_SHA
   3. Настроить интерфейс Tunnel0:
      1. Настроить VFR Forwarding — GREEN
      2. IP адрес — использовать Overlay адрес топологии
      3. Аутентификация NHRP — VRFGREEN
      4. Настроить динамическую поддержку мультикаста
      5. NHRP ID — 100
      6. Сделать мапинг между Underlay и Overlay адресами хаба
      7. В качестве сервера NHRP указать R7
      8. Источник — интерфейс Ethernet 0/1.144
      9. Назначение — адрес R7
      10. Ключ туннеля 10000
      11. Применить профиль VPN\_VRF с ключом shared
7. Настроить маршрутизаторы R4, R6 качеcтве Spok’ов VRF RED следующим образом:
   1. Настроить фазу 1 IPsec на R4 и R6 следующим образом:
      1. Номер политики 10
      2. Шифрование 3 DES
      3. Хэш SHA 256
      4. Аутентификация PSK
      5. Diffie-Hellman 5
      6. Источником для пароля «VPN\_VRF» должен служить адрес 0.0.0.0/24
   2. Настроить фазу 2 IPsec на R4 и R6 следующим образом:
      1. Создать Transform Set под названием ESP\_3DES\_SHA:
         1. в качестве протокола использовать ESP
         2. в качестве шифрования 3DES
         3. в качестве аутентификации использовать HMAC SHA1
      2. Создать IPSec Profile под названием VPN\_VRF:
         1. применить Transform Set под названием ESP\_3DES\_SHA
   3. Настроить интерфейс Tunnel0:
      1. Настроить VFR Forwarding — RED
      2. IP адрес — использовать Overlay адрес топологии
      3. Аутентификация NHRP — VRF\_RED
      4. Настроить динамическую поддержку мультикаста
      5. NHRP ID — 200
      6. Ключ туннеля 20000
      7. Сделать мапинг между Underlay и Overlay адресами хаба
      8. В качестве сервера NHRP указать R7
      9. Источник — интерфейс Ethernet 0/1.144
      10. Назначение — адрес R7
      11. Применить профиль VPN\_VRF с ключом shared
8. На маршрутизаторах R2, R3, R4, R6, R7 настроить Named mode EIGRP следующим образом:
   1. Имя VRF
   2. Интерфейс Ethernet 0/1.144 должен участвовать в процессе EIGRP
   3. IP адрес 188.1.100.0/24 должен аннонсироваться в процессе EIGRP
   4. Настроить аутентификацию на интерфейсах R7, подключенных к VRF GREEN с следующим образом:
      1. Название ключа VPN\_VRF\_GREEN
      2. Режим HMAC
      3. Пароль VRF\_GREEN
   5. Настроить аутентификацию на интерфейсах R7, подключенных к VRF RED с следующим образом:
      1. VPN\_VRF\_RED
      2. Режим HMAC
      3. Пароль VRF\_RED
   6. Настроить аутентификацию на интерфейсах R2 и R3, подключенных к VRF GREEN с следующим образом:
      1. Название ключа VPN\_VRF\_GREEN
      2. Режим HMAC
   7. Пароль VRF\_GREEN Настроить аутентификацию на интерфейсах R4 и R6, подключенных к VRF RED с следующим образом:
      1. VPN\_VRF\_RED
      2. Режим HMAC
      3. Пароль VRF\_RED
9. На интерфейсах Tunnel0 и Tunnel1 маршрутизатора R7 настроить IP Event Dampening следующим образом:
   1. Маршрут по EIGRP не должен передаваться в течении 20 секунд после падения интерфейса
   2. При достижении значения Penalty ниже 1000 должна появляться возможность повторного использования интерфейса
   3. Каждое событие не должно демпфироваться более чем на 40 секунд.
   4. Значение рестарта по-умолчанию.
   5. Проверить работу IP Event Dampening на интерфейсах
10. На маршрутизаторе R7 настроить Сonditional Debug только для вывода crypto debug относительно R6 и R3.
11. На маршрутизаторе R7 настроить Embedded Packet Capture следующим образом:
    1. Цикличный буфер:
       1. Название EVERYTHING размером 1024
       2. Максимальный размер пакета 1500
       3. Применить ACL под названием R7\_R3
    2. Создать ACL под названием R7\_R3:
       1. разрешить от хоста 188.1.100.7 к 188.1.100.3
    3. Настроить точку сбора IPv4 CEF под названием CEF для интерфейса Tunnel0 в обоих направлениях
    4. Связать точку сбора с буфером
    5. Проверить настройки
12. Проанализировать пакеты.

## [Цикл 20, Лабораторная работа по теме 117: IPv4 Multicast Routing](http://ccie.linkmeup.ru/2017/10/06/tsikl-20-laboratornaya-rabota-po-teme-117-ipv4-multicast-routing/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfM1FnZW9aUENpWGc) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2, R3, R4, R5 настроить OSPF процесс 100 в Аrea 51 на следующих интерфейсах:
   1. R2- E0/1.12,E0/1.23, E0/1.235,Loopback 0
   2. R3- E0/1.34, E0/1.23, E0/1.235,Loopback 0
   3. R4-E0/1.34, Loopback 0
   4. R5- E0/1.235, Loopback 0
   5. R1 — настроить одной командой
4. На маршрутизаторах R4, R5, R6 настроить OSPF процесс 100 в Аrea 0 на на интерфейсе E0/1.456
5. На маршрутизаторах R6, R7, R8, R9, R10 настроить OSPF процесс 100 в Аrea 106 на следующих интерфейсах:
   1. R6- E0/1.67, Loopback 0
   2. R7, R8, R9, R10 — настроить одной командой
6. На всех маршрутизаторах настроить IP Multicast Routing
7. На всех маршрутизаторах настроить Sparse Mode на следующих интерфейсах:
   1. R1 — E0/1.12, Loopback0
   2. R2 — E0/1.12, E0/1.23, E0/1.235
   3. R3- E0/1.34, E0/1.23, E0/1.235
   4. R4 — E0/1.456, E0/1.23, E0/1.235
   5. R5 — E0/1.456, E0/1.235
   6. R6 -E0/1.67, E0/1.456, Loopback0
   7. R7 — E0/1.78, E0/1.67
   8. R8 — E0/1.78, E0/1.89
   9. R9 — E0/1.89, Multilink 1
   10. R10 — Multilink 1
8. На всех маршрутизаторах Source Specific Multicast на всех маршрутизаторах
9. Настроить интерфейс Multilink1 маршрутизатора R9 следующим образом:
   1. Настроить версию IGMP 3
   2. В качестве клиента группы 232.0.0.1
   3. В качестве источника указать IP адрес интверфейса E0/1.12 маршрутизатора R1
10. Проверить каким образом идет трафик.

## [Цикл 20, Лабораторная работа по теме 118: BGP](http://ccie.linkmeup.ru/2017/10/09/tsikl-20-laboratornaya-rabota-po-teme-118-bgp/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfUFA4cUxSUElwQlk) всех устройств.
   1. Для задания используется логическая и физическая топологии проекта.
   2. На маршрутизаторах R1, R2, R3, R4 настроить OSPF процесс 100 в Аrea 104 на всех интерфейсах:
      1. указать в качестве пассивных:
         1. R2- интерфейс E0/1.235
         2. R3- интерфейс E0/1.235
         3. R4- интерфейс E0/1.456
   3. На маршрутизаторах R5, R6, R7, R8, R9, R10 настроить OSPF процесс 100 в Аrea 105 на всех интерфейсах:
      1. указать в качестве пассивных:
         1. R5 — интерфейс E0/1.235
   4. На маршрутизаторах R1, R2, R3, R4 настроить внутренний BGP процесс следующим образом:
      1. Номер AS — 41
      2. Создать bgp сессию следующим образом:
         1. Настроить Peer Group под названием LOCAL:
            1. Указать в качестве Remote AS номер 41
            2. Позволить увеличение значения TTL только до 2 хопов
            3. Указать в качестве соседей IP адреса интерфейсов Loopback 0
         2. Настроить интервал задержки информирования BGP об изменениях в RIB в 6 секунд
   5. Создать внешнюю bgp сессии на R2 и R4 следующим образом:
      1. Номер AS — 41
      2. Адвертайзить маршрут по-умолчанию, используя команду Network
      3. Создать внешнюю bgp сессии на R4:
         1. Настроить Peer Group под названием REMOTE:
            1. Указать в качестве Remote AS номер 51
            2. Позволить увеличение значения TTL только до 2 хопов
            3. Указать в качестве соседей IP адреса интерфейсов Loopback 0
            4. Включить в группу маршрутизатор R5
   6. Создать внешнюю bgp сессии на R5 следующим образом:
      1. Номер AS — 51
      2. Адвертайзить маршрут по-умолчанию, используя команду Network
      3. Создать внешнюю bgp сессии на R4:
         1. Настроить Peer Group под названием REMOTE:
            1. Указать в качестве Remote AS номер 41
            2. Позволить увеличение значения TTL только до 2 хопов
            3. Указать в качестве соседей IP адреса интерфейсов Loopback 0
            4. Включить в группу маршрутизаторы R2 и R4
   7. На маршрутизаторах R5, R6, R7, R8, R9, R10 настроить внутренний BGP процесс следующим образом:
      1. Номер AS — 51
      2. Настроить интервал задержки информирования BGP об изменениях в RIB в 6 секунд
      3. Настроить Peer Group под названием LOCAL:
         1. Указать в качестве Remote AS номер 51
         2. Указать в качестве соседей IP адреса интерфейсов Loopback 0
         3. Включить в группу:
            1. На R5 маршрутизатор R6
            2. На R6 маршрутизаторы R5 и R7
            3. На R7 маршрутизаторы R6 и R8
            4. На R8 маршрутизаторы R7 и R9
            5. На R9 маршрутизаторы R8 и R10
            6. На R10 маршрутизатор R9
   8. На маршрутизаторах R2 и R5 настроить статические маршруты к друг другу следующим образом:
      1. В качестве маршрута указать IP адрес Loopback0 интерфейса друг друга
      2. В качестве Next Hop указать IP адрес интерфейса E0/1.235 друг друга.
   9. На маршрутизаторах R4 и R5 настроить статические маршруты к друг другу следующим образом:
      1. В качестве маршрута указать IP адрес Loopback0 интерфейса друг друга
      2. В качестве Next Hop указать IP адрес интерфейса E0/1.456 друг друга.
   10. На маршрутизаторах c R1 по R10 настроить BGP Router ID назначив номера ID с 1.1.1.1 по 10.10.10.10 соответственно
   11. На маршрутизаторе R3 настроить DMZ Link Bandwidth следующим образом:
       1. Маршрутизатор R3:
          1. Настроить DMZ Link Bandwidth в отношении BGP соседей R2 и R4
          2. Указать Maximum Path = 2
   12. На маршрутизаторах R2, R4 настроить DMZ Link Bandwidth следующим образом:
       1. Маршрутизатор R2:
          1. Настроить DMZ Link Bandwidth в отношении BGP соседа R3
          2. Настроить DMZ Link Bandwidth в отношении BGP соседа R5:
             1. Указать на интерфейсе E0/1.235 полосу пропускания 5000
       2. Маршрутизатор R4:
          1. Настроить DMZ Link Bandwidth в отношении BGP соседа R3
          2. Настроить DMZ Link Bandwidth в отношении BGP соседа R5:
             1. Указать на интерфейсе E0/1.456 полосу пропускания 6000
   13. На маршрутизаторе R5 настроить маршрут по-умолчанию указав в качестве Next Hop интерфейс Null0.

## [Цикл 20, Лабораторная работа по теме 119: First Hop Redundancy Protocols 9.2 (IPv6)](http://ccie.linkmeup.ru/2017/10/11/tsikl-20-laboratornaya-rabota-po-teme-119-first-hop-redundancy-protocols-9-2-ipv6/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfQV9BTko4S3FldWs) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На всех маршрутизаторах настроить IPv6 Unicast Routing
4. На R5 и R6 настроить HSRP следующим образом:
   1. На интерфейсе E 0/1.456 маршрутизатора R5:
      1. Standby версии 2
      2. Виртуальный ipv6 адрес fe80::45
      3. Приоритет 101
      4. Настроить маршрутизатор таким образом, чтобы он автоматически забирал роль Aсtive на себя если их приоритет выше чем у действующего Active в данный момент.
   2. На интерфейсе E 0/1.456 маршрутизатора R6:
      1. Standby версии 2
      2. Виртуальный ipv6 адрес fe80::45
      3. Приоритет 99
      4. Настроить маршрутизатор таким образом, чтобы он автоматически забирал роль Aсtive на себя если их приоритет выше чем у действующего Active в данный момент.

## [Цикл 20, Лабораторная работа по теме 120: BGP](http://ccie.linkmeup.ru/2017/10/13/tsikl-20-laboratornaya-rabota-po-teme-120-bgp/)

1. Для данного задания в качестве начальной конфигурации использовать конечную конфигурацию лабораторного задания 118.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторе R2 и R4 настроить редистрибьюцию OSPF маршрутов из AS 41 в AS 51
4. На маршрутизаторах R2 и R4 агрегацию всех IP адресов Loopback0 интерфейсов с маской /21 из AS 41 в AS 51 c опцией Summary Only и опцией восстановления избегания петель.
5. На маршрутизаторе R5 агрегацию всех IP адресов Loopback0 интерфейсов с маской /20 из AS 41 в AS 51 c опцией NO\_EXPORT следующим образом:
   1. Создать Prefix List под названием AGGREGATE
   2. Создать Route Map под названием NO\_EXPORT
      1. Заматчить Prefix List под названием AGGREGATE
      2. Установить Community c опцией NO\_EXPORT
   3. Применить Route Map под названием NO\_EXPORT

# [**Цикл 21**](http://ccie.linkmeup.ru/2017/10/16/tsikl-21-laboratornaya-rabota-po-teme-121-mpls/)

## [Цикл 21, Лабораторная работа по теме 121: MPLS](http://ccie.linkmeup.ru/2017/10/16/tsikl-21-laboratornaya-rabota-po-teme-121-mpls/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfNmdBSnU4OVF4cms) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 21 на следующих интерфейсах c типом сети Point-to-Point:
   1. R1 — E0/1.12, Loopback0
   2. R2- E0/1.12
   3. Между маршрутизаторами настроить тип аутентификации Type 2
      1. Алгоритм MD5
      2. Пароль MPLS21
4. На маршрутизаторах R2 и R3 настроить OSPF процесс 100 в Аrea 23, на следующих интерфейсах:
   1. R2- E0/1.23, Loopback 0
   2. R3- E0/1.23, Loopback 0
   3. Между маршрутизаторами настроить тип аутентификации Type 2
      1. Алгоритм MD5
      2. Пароль MPLS23
5. На маршрутизаторах R3 и R4 настроить OSPF процесс 100 в Аrea 34, на следующих интерфейсах:
   1. R2- E0/1.34
   2. R3- E0/1.34
   3. Между маршрутизаторами настроить тип аутентификации Type 1
      1. Пароль MPLS34
6. На маршрутизаторах R2, R3, R5 настроить OSPF процесс 100 в Аrea 52, на следующих интерфейсах:
   1. R2- E0/1.235
   2. R3- E0/1.235
   3. R3- E0/1.235
   4. Между маршрутизаторами настроить тип аутентификации Type 2
      1. Название ключа MPLS52
      2. Номер ключа 1
      3. Пароль SHA\_256
      4. алгоритм SHA256
7. На маршрутизаторах R4, R5, R6 настроить OSPF процесс 100 в Аrea 0, на следующих интерфейсах:
   1. R4- E0/1.456, Loopback 0
   2. R5- E0/1.456, Loopback 0
   3. R6- E0/1.456, Loopback 0
   4. Между маршрутизаторами настроить тип аутентификации Type 2
      1. Название ключа MPLS0
      2. Номер ключа 1
      3. Пароль SHA\_256
      4. алгоритм SHA256
8. На маршрутизаторах R6, R7, R8, R9, R10 настроить OSPF процесс 107 в Аrea 107 на следующих интерфейсах:
   1. R6 — E0/1.67
   2. R7- E0/1.67, E0/1.78, Loopback0
   3. R8- E0/1.78, E0/1.89, Loopback0
   4. R9- E0/1.89, Multilink1, Loopback0
   5. R10- Multilink1, Loopback0
   6. Между маршрутизаторами настроить тип аутентификации Type 2
      1. Название ключа MPLS107
      2. Номер ключа 1
      3. Пароль SHA\_256
      4. алгоритм SHA256
9. Настроить MPLS на маршрутизаторах R2, R3, R4, R5, R6, R7 следующим образом:
   1. Настроить MPLS глобально на всех маршрутизаторах
   2. На маршрутизаторе R2:
      1. Ограничить диапазон MPLS заголовков от 200 до 299
      2. Настроить интерфейсы E0/1.23, E0/1.235 таким образом, чтобы они принимали участие в MPLS Label Switching
   3. На маршрутизаторе R3:
      1. Ограничить диапазон MPLS заголовков от 300 до 399
      2. Настроить интерфейсы E0/1.34, E0/1.235 таким образом, чтобы они принимали участие в MPLS Label Switching
   4. На маршрутизаторе R4:
      1. Ограничить диапазон MPLS заголовков от 400 до 499
      2. Настроить интерфейсы E0/1.34, E0/1.456 таким образом, чтобы они принимали участие в MPLS Label Switching
   5. На маршрутизаторе R5:
      1. Ограничить диапазон MPLS заголовков от 500 до 599
      2. Настроить интерфейсы E0/1.235, E0/1.456 таким образом, чтобы они принимали участие в MPLS Label Switching
   6. На маршрутизаторе R6:
      1. Ограничить диапазон MPLS заголовков от 600 до 699
      2. Настроить интерфейсы E0/1.67, E0/1.456 таким образом, чтобы они принимали участие в MPLS Label Switching
   7. На маршрутизаторе R7:
      1. Ограничить диапазон MPLS заголовков от 700 до 799
      2. Настроить интерфейсы E0/1.67 таким образом, чтобы они принимали участие в MPLS Label Switching

## [Цикл 21, Лабораторная работа по теме 122: BGP](http://ccie.linkmeup.ru/2017/10/18/tsikl-21-laboratornaya-rabota-po-teme-122-bgp/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfWUlSR1pCbDZSR0k) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 12, на следующих интерфейсах:
   1. R1- E0/1.12, Интерфейс Loopback0
   2. R2- E0/1.12, Интерфейс Loopback0
4. На маршрутизаторах R2, R3 настроить OSPF процесс 100 в Аrea 23, на следующих интерфейсах:
   1. R2- E0/1.23
   2. R3- E0/1.23
5. На маршрутизаторах R4, R6, R7 настроить OSPF процесс 100 в Аrea 764 на следующих интерфейсах:
   1. R4 — E0/1.456, Интерфейс Loopback0
   2. R6 — E0/1.456, E0/1.67, Интерфейс Loopback0
   3. R7 — E0/1.67, Интерфейс Loopback0
6. На маршрутизаторах R8,R9,R10 настроить OSPF процесс 100 в Аrea 108, на следующих интерфейсах:
   1. R8- E0/1.78, E0/1.89,Интерфейс Loopback0
   2. R9- E0/1.89, Интерфейс Loopback0, Интерфейс Multilink1
   3. R10- Интерфейс Loopback0, Интерфейс Multilink1
7. На маршрутизаторе R3 настроить BGP процесс следующим образом:
   1. Номер AS — 3
   2. Создать внешнюю bgp сессию следующим образом:
      1. Указать в качестве Remote AS номер 764
      2. Указать в качестве Update Source интерфейс Loopback0
      3. Позволить увеличение значения TTL только до 2 хопов
      4. Применить к маршрутизатору R4, указав IP адрес Loopback интерфейса
8. На маршрутизаторе R3 настроить статический маршрут к IP адресу интерфейса Loopback 0 маршрутизатора R4. В качестве Next Hop указать IP адрес интерфейса E0/1.34
9. На маршрутизаторе R1 настроить BGP процесс следующим образом:
   1. Номер AS — 21
   2. Создать внутренюю bgp сессию следующим образом:
      1. Создать BGP Peer Group:
         1. Название IBGP
         2. Указать в качестве Update Source интерфейс Loopback0
         3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R2
         4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
10. На маршрутизаторе R2 настроить BGP процесс следующим образом:
    1. Номер AS — 21
    2. Редистрибьютить маршруты из OSPF 100 c метрикой 20
    3. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R1
          4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
    4. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Позволить увеличение значения TTL только до 2 хопов
          3. Указать в качестве Update Source интерфейс Tunnel0
          4. В качестве соседа указать IP адрес Tunnel0 интерфейса маршрутизатора R7
11. На маршрутизаторе R5 настроить BGP процесс следующим образом:
    1. Номер AS — 5
    2. Создать внешнюю bgp сессию следующим образом:
       1. Указать в качестве Remote AS номер 764
       2. Указать в качестве Update Source интерфейс Loopback0
       3. Позволить увеличение значения TTL только до 2 хопов
       4. Применить к маршрутизатору R6, указав IP адрес Loopback интерфейса
12. На маршрутизаторе R5 настроить статический маршрут к IP адресу интерфейса Loopback 0 маршрутизатора R6. В качестве Next Hop указать IP адрес интерфейса E0/1.456
13. На маршрутизаторе R6 настроить статический маршрут к IP адресу интерфейса Loopback 0 маршрутизатора R5. В качестве Next Hop указать IP адрес интерфейса E0/1.456
14. На маршрутизаторе R4 настроить BGP процесс следующим образом:
    1. Номер AS — 764
    2. Редистрибьютить статический маршрут с мерикой 10
    3. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R6
          4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Указать в качестве Update Source интерфейс Tunnel0
       3. В качестве соседа указать IP адрес Tunnel0 интерфейса маршрутизатора R7
    4. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R3
15. На маршрутизаторе R6 настроить BGP процесс следующим образом:
    1. Номер AS — 764
    2. Редистрибьютить статический маршрут с метрикой 10
    3. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R4
          4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Указать в качестве Update Source интерфейс Tunnel0
       3. В качестве соседа указать IP адрес Tunnel0 интерфейса маршрутизатора R7
    4. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R5
16. На маршрутизаторе R7 настроить BGP процесс следующим образом:
    1. Номер AS — 764
    2. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Указать в качестве Update Source интерфейс Tunnel0
       3. В качестве соседей указать IP адрес Tunnel0 интерфейса маршрутизатора R4, R6
    3. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R8
          5. Указать в качестве Update Source интерфейс Tunnel0
          6. В качестве соседей указать IP адрес Tunnel0 интерфейса маршрутизатора R2
17. На маршрутизаторе R8 настроить BGP процесс следующим образом:
    1. Номер AS — 108
    2. Редистрибьютить OSPF процесс 100 с метрикой 20
    3. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейсов маршрутизатора R9
    4. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R7
18. На маршрутизаторе R9 настроить BGP процесс следующим образом:
    1. Номер AS — 108
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейсов маршрутизаторов R8, R10
19. На маршрутизаторе R10 настроить BGP процесс следующим образом:
    1. Номер AS — 108
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейсов маршрутизаторов R9
20. На маршрутизаторе R7 настроить статические маршруты к IP адресу интерфейса Loopback 0 маршрутизатора R8. В качестве Next Hop указать IP адреса интерфейса E0/1.78
21. На маршрутизаторе R8 настроить статические маршруты к IP адресу интерфейса Loopback 0 маршрутизатора R7. В качестве Next Hop указать IP адреса интерфейса E0/1.78
22. На маршрутизаторе R6 настроить статический маршрут к IP адресу интерфейса Loopback 0 маршрутизатора R5. В качестве Next Hop указать IP адреса интерфейса E0/1.456
23. Настроить DMVPN Phase 3 следующим образом:
    1. Настроить маршрутизатор R7 в качестве хаба DMVPN:
       1. Настроить интерфейс Tunnel0:
          1. IP адрес — 188.1.100.7/24
          2. Аутентификация NHRP — STANDARD
          3. Настроить динамическую поддержку мультикаста
          4. NHRP ID — 100
          5. Настроить NHRP Redirect
          6. Источник — интерфейс Ethernet 0/1.144
          7. Режим — GRE Multipoint
          8. Ключ туннеля 10000
    2. Настроить маршрутизаторы R2, R4, R6 качеcтве Spok’ов:
       1. Настроить интерфейс Tunnel0:
          1. IP адрес — использовать Overlay адрес топологии
          2. Аутентификация NHRP — STANDARD
          3. Настроить маппинг мультикаста к R7
          4. NHRP ID — 100
          5. В качестве сервера NHRP NHS указать R7
          6. Настроить NHRP Shortcut
          7. Источник — интерфейс Ethernet 0/1.144
          8. Режим — GRE Multipoint
          9. Ключ туннеля 10000
24. На маршрутизаторах R4, R6, R7 настроить Named mode EIGRP следующим образом:
    1. Имя Tunnel
    2. Номер процесса 72
    3. Следующие интерфейсы устройств должны участвовать в процессе:
       1. R2 — Интерфейс Tunnel 0
       2. R4- Интерфейс Tunnel 0
       3. R6 — Интерфейс Tunnel 0
       4. R7 — Интерфейс Tunnel 0

## [Цикл 21, Лабораторная работа по теме 123: BGP](http://ccie.linkmeup.ru/2017/10/20/tsikl-21-laboratornaya-rabota-po-teme-123-bgp/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfdFE4SFVPV3JDMDA) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1 и R2 настроить OSPF процесс 21 в Аrea 21 на всех интерфейсах:
4. На маршрутизаторах R3, R4, R5, R6 настроить OSPF процесс 6543 в Аrea 6543 на всех интерфейсах:
5. На маршрутизаторах R7, R8, R9, R10 настроить OSPF процесс 10987 в Аrea 10987 на всех интерфейсах.
6. На маршрутизаторах R1, R2 настроить внутренний BGP процесс следующим образом:
   1. Номер AS — 21
   2. Создать bgp сессию следующим образом:
      1. Указать в качестве Remote AS номер 21
      2. Указать в качестве соседей IP адреса интерфейсов Loopback 0
      3. Настроить команду, при которой все Next Hop адреса узнаются через OSPF
      4. На R2 указать R1 в качестве клиента Route Reflector’a
7. На маршрутизаторе R2 настроить внешний BGP процесс следующим образом:
   1. Номер AS — 21
   2. Создать bgp сессию следующим образом:
      1. Указать в качестве Remote AS номер 6543
      2. Указать в качестве соседей IP адреса интерфейсов Loopback 0
      3. Позволить увеличение значения TTL только до 2 хопов
      4. Адвертайзить маршрут 180.1.0.0/22 с помощью команды network
8. На маршрутизаторах R3, R4, R5, R6 настроить Confederation BGP процесс следующим образом:
   1. R3 — номер AS — 3
   2. R4, R5 — номер AS — 54
   3. R6 — номер AS — 6
   4. Создать внешнюю bgp сессию на R3 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 6543
      2. Указать в качестве пиров конфедерации 54
      3. Указать в качестве Remote AS номера AS 21 и 54
      4. Указать в качестве соседей IP адреса интерфейсов Loopback 0
      5. Позволить увеличение значения TTL только до 2 хопов
      6. Для соседа в AS 54 настроить команду, при которой все Next Hop адреса узнаются через OSPF
      7. Адвертайзить маршрут по-умолчанию с помощью команды network
   5. Создать внешнюю и внутреннюю bgp сессии на R4 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 6543
      2. Указать в качестве пиров конфедерации AS номера 3 и 6
      3. Для внешней bgp сессии:
         1. Создать пир группу под названием CONFEDERATION:
            1. Позволить увеличение значения TTL только до 2 хопов
            2. Для соседей настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номера AS R3 и R6
         3. Указать в качестве членов группы IP адреса интерфейсов Loopback 0 R3 и R6
      4. Для внутренней bgp сессии:
         1. Создать пир группу под названием REFLECT:
            1. На R4 указать R5 в качестве клиента Route Reflector’a
            2. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номер AS 54
         3. Указать в качестве члена группы IP адрес интерфейса Loopback 0 R5
   6. Создать внутреннюю bgp сессию на R5 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 6543
      2. Указать в качестве Remote AS номер AS 54
      3. Для соседа R4 настроить команду, при которой все Next Hop адреса узнаются через OSPF
   7. Создать внешнюю и внутреннюю bgp сессии на R6 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 6543
      2. Указать в качестве пиров конфедерации AS номер 54
      3. Для внешней bgp сессии конфедерации:
         1. Создать пир группу под названием CONFEDERATION:
            1. Позволить увеличение значения TTL только до 2 хопов
            2. Для соседей настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номер AS R4
         3. Указать в качестве членов группы IP адрес интерфейса Loopback 0 R4
      4. Для внешней bgp сессии:
         1. Указать в качестве Remote AS номер AS 10987
         2. Указать в качестве члена группы IP адрес интерфейса Loopback 0 R7
         3. Позволить увеличение значения TTL только до 2 хопов
         4. Адвертайзить маршрут по-умолчанию с помощью команды network
9. На маршрутизаторах R7, R8, R8, R10 настроить Confederation BGP процесс следующим образом:
   1. R7 — номер AS — 7
   2. R8, R9, R10 — номер AS — 1098
   3. Создать внешнюю bgp сессию на R7 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 10987
      2. Указать в качестве пиров конфедерации 1098
      3. Указать в качестве Remote AS номера AS 6543 и 1098
      4. Указать в качестве соседей IP адреса интерфейсов Loopback 0
      5. Позволить увеличение значения TTL только до 2 хопов
      6. Для соседа в AS 1098 настроить команду, при которой все Next Hop адреса узнаются через OSPF
      7. Адвертайзить маршрут 180.1.0.0/20 с помощью команды network
   4. Создать внешнюю и внутреннюю bgp сессии на R8 следующим образом:
      1. Указать в качестве идентификатора конфедерации номер AS 10987
      2. Указать в качестве пиров конфедерации AS номер 7
      3. Для внешней bgp сессии:
         1. Создать пир группу под названием CONFEDERATION:
            1. Позволить увеличение значения TTL только до 2 хопов
            2. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номер AS R7
         3. Указать в качестве членов группы IP адреса интерфейсов Loopback 0 R7
      4. Для внутренней bgp сессии:
         1. Создать пир группу под названием REFLECT:
            1. Указать R9 в качестве клиента Route Reflector’a
            2. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
         2. Указать в качестве Remote AS номер AS 1098
         3. Указать в качестве члена группы IP адрес интерфейса Loopback 0 R9
   5. Создать внутреннюю bgp сессию на R9 следующим образом:
      1. Создать пир группу под названием REFLECT:
         1. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
      2. Указать в качестве Remote AS номер AS 1098
      3. Указать в качестве членов группы IP адреса интерфейсов Loopback 0 R8 и R9
   6. Создать внутреннюю bgp сессию на R10 следующим образом:
      1. Создать пир группу под названием REFLECT:
         1. Для соседа настроить команду, при которой все Next Hop адреса узнаются через OSPF
      2. Указать в качестве Remote AS номер AS 1098
      3. Указать в качестве члена группы IP адрес интерфейса Loopback 0 R9
10. На маршрутизаторах R2 и R3 настроить статические маршруты к друг другу следующим образом:
    1. В качестве маршрута указать IP адрес Loopback0 интерфейса друг друга
    2. В качестве Next Hop указать IP адрес интерфейса E0/1.23 друг друга.
11. На маршрутизаторах R6 и R7 настроить статические маршруты к друг другу следующим образом:
    1. В качестве маршрута указать IP адрес Loopback0 интерфейса друг друга
    2. В качестве Next Hop указать IP адрес интерфейса E0/1.67 друг друга.
12. На маршрутизаторе R3 настроить маршрут по-умолчанию указав в качестве Next Hop интерфейс Null0.
13. На маршрутизаторе R6 настроить маршрут по-умолчанию указав в качестве Next Hop интерфейс Null0.
14. На маршрутизаторе R2 настроить статический маршрут 180.1.0.0/22 указав в качестве Next Hop интерфейс Null0.
15. На маршрутизаторе R7 настроить статический маршрут 180.1.0.0/20 указав в качестве Next Hop интерфейс Null0.
16. На всех маршрутизаторах настроить IP Multicast Routing
17. На всех маршрутизаторах настроить Sparse Mode на следующих интерфейсах:
    1. R1 — E0/1.12, Loopback0
    2. R2 — E0/1.12, E0/1.23, E0/1.235
    3. R3- E0/1.34, E0/1.23, E0/1.235
    4. R4 — E0/1.456, E0/1.23, E0/1.235
    5. R5 — E0/1.456, E0/1.235
    6. R6 -E0/1.67, E0/1.456, Loopback0
    7. R7 — E0/1.78, E0/1.67
    8. R8 — E0/1.78, E0/1.89
    9. R9 — E0/1.89, Multilink 1
    10. R10 — Multilink 1
18. Настроить интерфесы E0/1.67 R6 и R7 в качестве BSR EDGE, роли BSR Candidate и RP, используя при этом Lo интерфейс маршрутизаторов с условием не адвертайзить BSR информацию за пределы настраивомого линка.
19. Настроить интерфейс Multilink1 маршрутизатора R9 качестве клиента группы 224.2.2.2

## [Цикл 21, Лабораторная работа по теме 124: MPLS](http://ccie.linkmeup.ru/2017/10/23/tsikl-21-laboratornaya-rabota-po-teme-124-mpls/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=0ByVf6yfX4EBfM2RhWjM5cG11VHc) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2 настроить OSPF процесс 100 в Аrea 21 на следующих интерфейсах c типом сети Point-to-Point:
   1. R1 — E0/1.12, Loopback0
   2. R2- E0/1.12, Loopback0
4. На маршрутизаторах R2 и R3 настроить статические маршруты к IP адресам Loopback 0 интерфесов друг друга, указав в качестве Next Hop IP адреса E0/1.23 интерфесов.
5. На маршрутизаторах R3, R4, R6, R7 настроить OSPF процесс 100 в Аrea 37, на следующих интерфейсах:
   1. R3- E0/1.34, Loopback0
   2. R4- E0/1.34, E0/1.456, Loopback0
   3. R6 — E0/1.67, E0/1.456, Loopback0
   4. R7 — E0/1.67, Loopback0
6. На маршрутизаторах R7, R8 настроить OSPF процесс 100 в Аrea 78 на следующих интерфейсах:
   1. R7- E0/1.78
   2. R8- E0/1.78
7. На маршрутизаторах R7 и R8 настроить статические маршруты к IP адресам Loopback 0 интерфесов друг друга, указав в качестве Next Hop IP адреса E0/1.78 интерфесов.
8. На маршрутизаторах R2, R5, R8 и настроить RIPv2:
   1. Настроить Passive интерфейсы по дефолту, кроме:
      1. На R2 — E0/1.23
      2. На R5 — E0/1.235
      3. На R8 — E0/1.78
   2. Настроить сети 180.1.0.0, 188.1.0.0
   3. Убрать автосуммирование
9. На маршрутизаторах R8, R9, R10 настроить OSPF процесс 100 в Аrea 108 на следующих интерфейсах:
   1. R8- E0/1.89, Loopback0
   2. R9- E0/1.89, Multilink1, Loopback0
   3. R10- Multilink1, Loopback0
10. На маршрутизаторe R7 настроить OSPF процесс 100 в Аrea 7 на следующем интерфейсе:
    1. R7- E0/1.7
11. На маршрутизаторе R1 настроить BGP процесс следующим образом:
    1. Номер AS — 21
    2. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R2
          4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
12. На маршрутизаторе R2 настроить BGP процесс следующим образом:
    1. Номер AS — 21
    2. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R1
          4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
    3. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Позволить увеличение значения TTL только до 2 хопов
          3. Указать в качестве Update Source интерфейс Loopback0
          4. В качестве соседа указать IP адрес Loopback0 интерфейса маршрутизатора R3
13. а маршрутизаторе R3 настроить BGP процесс следующим образом:
    1. Номер AS — 73
    2. Редистрибьютить маршруты из протокола RIP
    3. Создать внешнюю bgp сессию следующим образом:
       1. Указать в качестве Remote AS номера 21 и 5 соотвественно
       2. Указать в качестве Update Source интерфейс Loopback0
       3. Позволить увеличение значения TTL только до 2 хопов
       4. Применить к маршрутизаторам R2 и R5, указав IP адрес Loopback интерфейса
       5. Создать внутренюю bgp сессию следующим образом:
          1. Создать BGP Peer Group:
             1. Название IBGP
             2. Указать в качестве Update Source интерфейс Loopback0
             3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R7
             4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
          2. Настроить VPN следующим образом:
             1. Настроить Address Family VPNv4
             2. Активировать соседа R7
             3. Испольховать Extended Community
          3. Настроить VRF BLUE следующим образом:
             1. Настроить Address Family VPNv4 VRF BLUE
             2. Редистрибьютить RIP
          4. Настроить VRF GREEN следующим образом:
             1. Настроить Address Family VPNv4 VRF GREEN
             2. Редистрибьютить RIP
14. На маршрутизаторе R5 настроить BGP процесс следующим образом:
    1. Номер AS — 5
    2. Создать внешнюю bgp сессию следующим образом:
       1. Указать в качестве Remote AS номер 73
       2. Указать в качестве Update Source интерфейс Loopback0
       3. Позволить увеличение значения TTL только до 2 хопов
       4. Применить к маршрутизатору R3, указав IP адрес Loopback интерфейса
15. На маршрутизаторе R7 настроить BGP процесс следующим образом:
    1. Номер AS — 73
    2. Редистрибьютить маршруты из протокола RIP
    3. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Указать в качестве Update Source интерфейс Loopback0
       3. В качестве соседей указать IP адрес Loopback0 интерфейса маршрутизатора R3
          1. Настроить VPN следующим образом:
             1. Настроить Address Family VPNv4
             2. Активировать соседа R3
             3. Испольховать Extended Community
          2. Настроить VRF BLUE следующим образом:
             1. Настроить Address Family VPNv4 VRF BLUE
             2. Редистрибьютить RIP
          3. Настроить VRF GREEN следующим образом:
             1. Настроить Address Family VPNv4 VRF GREEN
             2. Редистрибьютить RIP
    4. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R8
16. На маршрутизаторе R8 настроить BGP процесс следующим образом:
    1. Номер AS — 108
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейсов маршрутизатора R9
    3. Создать внешнюю ebgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название EBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. Позволить увеличение значения TTL только до 2 хопов
          4. В качестве соседей указать IP адрес Loopback интерфейса маршрутизаторов R7
17. На маршрутизаторе R9 настроить BGP процесс следующим образом:
    1. Номер AS — 108
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейсов маршрутизаторов R8, R10
18. На маршрутизаторе R10 настроить BGP процесс следующим образом:
    1. Номер AS — 108
    2. Создать ibgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейсов маршрутизаторов R9
19. Настроить MPLS на маршрутизаторах R3, R4, R6, R7 следующим образом:
    1. Настроить MPLS глобально на всех маршрутизаторах
    2. На маршрутизаторе R3:
       1. Ограничить диапазон MPLS заголовков от 300 до 399
       2. Настроить интерфейсы E0/1.34 таким образом, чтобы они принимали участие в MPLS Label Switching
    3. На маршрутизаторе R4:
       1. Ограничить диапазон MPLS заголовков от 400 до 499
       2. Настроить интерфейсы E0/1.34, E0/1.456 таким образом, чтобы они принимали участие в MPLS Label Switching
    4. На маршрутизаторе R6:
       1. Ограничить диапазон MPLS заголовков от 600 до 699
       2. Настроить интерфейсы E0/1.67, E0/1.456 таким образом, чтобы они принимали участие в MPLS Label Switching
    5. На маршрутизаторе R7:
       1. Ограничить диапазон MPLS заголовков от 700 до 799
       2. Настроить интерфейсы E0/1.67 таким образом, чтобы они принимали участие в MPLS Label Switching
20. На маршрутизаторах R3 и R7 настроить RIPv2 через VRF следующим образом:
    1. Настроить VRF под названием BLUE
       1. Route Distinguisher 1:1
       2. Route Target (Export/Import) 1:1
       3. На R3 применить на интерфейсе E0/1.235
       4. На R7 применить на интерфейсе E0/1.7
    2. Настроить VRF под названием GREEN
       1. Route Distinguisher 1:2
       2. Route Target (Export/Import) 1:2
       3. На R3 применить на интерфейсе E0/1.23
       4. На R7 применить на интерфейсе E0/1.78
    3. Настроить Address Family VRF BLUE:
       1. Network 188.1.0.0
       2. Редистрибьютить маршруты из BGP 73
       3. Указать Default Metric 2
    4. Настроить Address Family VRF GREEN:
       1. Network 188.1.0.0
       2. Редистрибьютить маршруты из BGP 73
       3. Указать Default Metric 2

## [Цикл 21, Лабораторная работа по теме 125: Data Plane Security (IPv6)](http://ccie.linkmeup.ru/2017/10/27/tsikl-21-laboratornaya-rabota-po-teme-125-data-plane-security-ipv6/)

1. В качестве [начальной конфигурации](https://drive.google.com/open?id=0ByVf6yfX4EBfY1FEbjBjMktMTmM) использовать конечную конфигурацию лабораторной работы 119.
2. Для задания используется логическая и физическая топологии проекта.
3. Маршрутизатор R6 настроить в качестве Stateful DHCPv6 Server’a следующим образом для R7:
   1. DHCP пул под названием DHCP\_STATEFUL
   2. DNS Server c адресом 2001:CC1E:1:67::100
   3. имя домена [ccie.linkmeup.ru](http://ccie.linkmeup.ru/)
   4. Указать префикс 2001:CC1E:1:45::0/64
   5. Настроить интерфейс E0/1.67 следующим образом:
      1. Указать пул для сервера — DHCP\_STATEFUL с опцией Rapid Commit
      2. Указать, чтобы отправлялся флаг “other stateful configuration” в RA ipv6
      3. Указать клиенту, чтобы он использовал только DHCP сервер для получения IP адреса, вместо SLAAC
4. Настроить интерфейс E0/1.67 маршрутизатора R7 следующим образом:
   1. включить работу IPv6 c опцией DHCP и Rapid Commit.
5. На свиче SW1 настроить DHCP GUARD следующим образом:
   1. Создать префикс лист под названием PREFIX разрешить только адрес 2001:CC1E:1:67::/64
   2. Создать ACL под названием TRUSTED\_ROUTER где разрешить только хост IPv6 адрес интерфейса E0/1.67 маршрутизатора R6
   3. Создать DHCP Guard Policy под названием TRUSTED:
      1. Применить роль устройства в качестве сервера
      2. заматчить ACL под названием TRUSTED\_ROUTER
      3. Заматчить префикс лист под названием PREFIX
   4. Применить DHCP Guard Policy к VLAN67
6. На свиче SW1 настроить RA Guard следующим образом:
   1. Настроить IPv6 RA Guard Policy под названием TRUST\_ROUTER
      1. применить роль маршрутизатора
   2. Настроить IPv6 RA Guard Policy под названием TRUST\_HOST
      1. применить роль хоста
   3. Включить логирование сброшенных пакетов
   4. Применить к VLAN67 политику под названием TRUST\_HOST
   5. Применить на интерфейсе E0/2 политику TRUST\_ROUTER
7. На свиче SW1 применить к VLAN67 ND Inspection

## [Цикл 21, Лабораторная работа по теме 126:](http://ccie.linkmeup.ru/2017/10/27/tsikl-21-laboratornaya-rabota-po-teme-126/)

1. В качестве начальной конфигурации использовать конечную конфигурацию лабораторного задания 122.
2. Для задания используется логическая и физическая топологии проекта.
3. R3 и R5 выступают в качестве Транзитных маршрутизаторов, трафик которых может проходить через AS 764 от одного транзитного маршрутизатора к другрму, но внутренние префиксы AS 764 не передаются ни одному Транзитному маршрутизатору.
4. R2 и R8 выступают в качестве Клиентских маршрутизаторов, которые могут достигать внутренних префиксов AS 764, также могут проходить через AS 764 и достигать префиксов Транзитных маршрутизаторов. Также префиксы Клиентских маршрутизаторов могут передаваться Транзитным маршрутизаторам. Но трафик от одного Клиентского маршрутизатора не может передаваться к другому.
5. Настроить R4, R6 и R7 в качестве маршрутизаторов ISP следующим образом:
   1. Настроить команду при которой десятичный формат Community преобразуется в вид AA:NN, где AA — это номер автономной системы, а NN — это произвозльное число
   2. На маршрутизаторе R7:
      1. Настроить Route Map под названием customer-21:
         1. проставить community 21:3
      2. Настроить Route Map под названием customer-108:
         1. проставить community 108:3
      3. Применить Route Map под названием customer-21 по отношению к R2 на входе
      4. Применить Route Map под названием customer-108 по отношению к R8 на входе
      5. Применить в настройках протокола BGP комманду send-community по отношению к R2 и R8
      6. Настроить AS -path ACL под номером 10, где разрешить все маршруты с пустым списком AS\_PATH
      7. Настроить Expanded Community List под названием Permit\_transit, где разрешить любой префикс, который адвертайзится от Транзитных маршрутизаторов.
      8. Настроить Route Map под названием Customers:
         1. Разрешить и заматчить AS -path ACL под номером 10
         2. Разрешить и заматчить Expanded Community List под названием Permit\_transit
         3. Запретить все остальные маршруты
      9. Применить под названием Customers по отношению к R2 и R8 на выходе
   3. На маршрутизаторе R4:
      1. Настроить Route Map под названием transit-3:
         1. проставить community 3:1
      2. Применить Route Map под под названием transit-3 по отношению к R3 на входе
      3. Применить в настройках протокола BGP комманду send-community по отношению к R3
      4. Настроить Community List под номером 200 для идентифицирования префиксов, принадлежащих Клиентским маршрутизаторам AA:3 и Транзитным маршрутизаторам АА:1.
      5. Настроить Route Map под названием Transit\_Partners:
         1. Разрешить и заматчить Community List под номером 200
         2. Запретить все остальные маршруты
      6. Применить Route Map под под названиемTransit\_Partners по отношению к R3 на выходе
   4. На маршрутизаторе R6:
      1. Настроить Route Map под названием transit-5:
         1. проставить community 3:1
      2. Применить Route Map под под названием transit-5 по отношению к R5 на входе
      3. Применить в настройках протокола BGP комманду send-community по отношению к R5
      4. Настроить Community List под номером 200 для идентифицирования префиксов, принадлежащих Клиентским маршрутизаторам AA:3 и Транзитным маршрутизаторам АА:1.
      5. Настроить Route Map под названием Transit\_Partners:
         1. Разрешить и заматчить Community List под номером 200
         2. Запретить все остальные маршруты
      6. Применить Route Map под под названиемTransit\_Partners по отношению к R5 на выходе
6. На маршрутизаторе R2 редистрибьютить все Connected маршруты в BGP процессе 21.
7. На маршрутизаторе R3 редистрибьютить все Connected маршруты в BGP процессе 3.
8. На маршрутизаторе R5 редистрибьютить все Connected маршруты в BGP процессе 5.
9. Проверить выполнение условий задания.

# [**Цикл 22**](http://ccie.linkmeup.ru/2017/11/08/voprosy-po-tsiklu-22-tema-127-mpls/)

## [Цикл 22, Лабораторная работа по теме 127:MPLS](http://ccie.linkmeup.ru/2017/11/08/tsikl-22-laboratornaya-rabota-po-teme-127-mpls/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=1TH9KIl701UETAqrzvoRnjHiJHwzY8ru6) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R1, R2 настроить OSPF процесс 1289 в Аrea 0 на следующих интерфейсах:
   1. R1 — E0/1.12, Loopback0, Router ID — 180.1.1.1
   2. R2- E0/1.12, E0/1.23, Loopback0 — Router ID — 180.1.2.2
   3. Network point-to-point
4. На маршрутизаторе R3 настроить OSPF процесс 1289 следующим образом:
   1. Наименование VRF — GREEN:
   2. Router ID — 3.3.2.2
   3. Интерфейс- E0/1.23
   4. Редистрибьютить BGP процесс 73
   5. Network point-to-point
5. На маршрутизаторе R3 настроить OSPF процесс 57 следующим образом:
   1. Наименование VRF — BLUE:
   2. Router ID — 3.3.5.5
   3. Интерфейс- E0/1.235
   4. Редистрибьютить BGP процесс 73
6. На маршрутизаторе R5 настроить OSPF процесс 57 в Аrea 0, на следующих интерфейсах:
   1. R5- E0/1.235, Loopback0, Router ID — 180.1.5.5
7. На маршрутизаторах R3, R4, R6, R7 настроить OSPF процесс 37 в Аrea 0, на следующих интерфейсах:
   1. R3- E0/1.34, Loopback0, Router ID — 180.1.3.3
   2. R4- E0/1.34, E0/1.456, Loopback0 , Router ID — 180.1.4.4
   3. R6 — E0/1.67, E0/1.456, Loopback0, Router ID — 180.1.5.5
   4. R7 — E0/1.67, Loopback0, Router ID — 180.1.7.7
8. На маршрутизаторах R7, R8, R9, R10 настроить OSPF процесс 1289 в Аrea 0 на следующих интерфейсах:
   1. R8- E0/1.89, Loopback0, Router ID -180.1.8.8
   2. R9- E0/1.89, Multilink1, Loopback0, Router ID -180.1.9.9
   3. R10- Multilink1, Loopback0, Router ID -180.1.10.10
9. На маршрутизаторе R7 настроить OSPF процесс 1289 следующим образом:
   1. Наименование VRF — GREEN:
   2. Router ID — 7.7.8.8
   3. Интерфейс- E0/1.78
   4. Редистрибьютить BGP процесс 73
10. На маршрутизаторе R7 настроить OSPF процесс 57 следующим образом:
    1. Наименование VRF — BLUE:
    2. Router ID — 7.7.7.7
    3. Интерфейс- E0/1.7
    4. Редистрибьютить BGP процесс 73
11. На маршрутизаторе R3 настроить BGP процесс следующим образом:
    1. Номер AS — 73
    2. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R7
          4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Настроить VPN следующим образом:
          1. Настроить Address Family VPNv4
          2. Активировать соседа R7
          3. Испольховать Extended Community
       3. Настроить VRF BLUE следующим образом:
          1. Настроить Address Family VPNv4 VRF BLUE
          2. Редистрибьютить OSPF процесс 57
       4. Настроить VRF GREEN следующим образом:
          1. Настроить Address Family VPNv4 VRF GREEN
          2. Редистрибьютить OSPF процесс 1289
12. На маршрутизаторе R7 настроить BGP процесс следующим образом:
    1. Номер AS — 73
    2. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Указать в качестве Update Source интерфейс Loopback0
       3. В качестве соседей указать IP адрес Loopback0 интерфейса маршрутизатора R3
          1. Настроить VPN следующим образом:
             1. Настроить Address Family VPNv4
             2. Активировать соседа R3
             3. Испольховать Extended Community
       4. Настроить VRF BLUE следующим образом:
          1. Настроить Address Family VPNv4 VRF BLUE
          2. Редистрибьютить OSPF процесс 57
       5. Настроить VRF GREEN следующим образом:
          1. Настроить Address Family VPNv4 VRF GREEN
          2. Редистрибьютить OSPF процесс 1289
13. Настроить MPLS на маршрутизаторах R3, R4, R6, R7 следующим образом:
    1. Настроить MPLS глобально на всех маршрутизаторах
    2. На маршрутизаторе R3:
       1. Ограничить диапазон MPLS заголовков от 300 до 399
       2. Настроить интерфейсы E0/1.34 таким образом, чтобы они принимали участие в MPLS Label Switching
    3. На маршрутизаторе R4:
       1. Ограничить диапазон MPLS заголовков от 400 до 499
       2. Настроить интерфейсы E0/1.34, E0/1.456 таким образом, чтобы они принимали участие в MPLS Label Switching
    4. На маршрутизаторе R6:
       1. Ограничить диапазон MPLS заголовков от 600 до 699
       2. Настроить интерфейсы E0/1.67, E0/1.456 таким образом, чтобы они принимали участие в MPLS Label Switching
    5. На маршрутизаторе R7:
       1. Ограничить диапазон MPLS заголовков от 700 до 799
       2. Настроить интерфейсы E0/1.67 таким образом, чтобы они принимали участие в MPLS Label Switching
14. На маршрутизаторах R3 и R7 настроить VRF следующим образом:
    1. Настроить VRF под названием BLUE
       1. Route Distinguisher 1:1
       2. Route Target (Export/Import) 1:1
       3. На R3 применить на интерфейсе E0/1.235
       4. На R7 применить на интерфейсе E0/1.7
    2. Настроить VRF под названием GREEN
       1. Route Distinguisher 2:2
       2. Route Target (Export/Import) 2:2
       3. На R3 применить на интерфейсе E0/1.23
       4. На R7 применить на интерфейсе E0/1.78

## [Цикл 22, Лабораторная работа по теме 128:BGP](http://ccie.linkmeup.ru/2017/11/22/tsikl-22-laboratornaya-rabota-po-teme-128-bgp/)

1. В качестве начальной конфигурации использовать конечную конфигурацию лабораторного задания 126.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторе R7 настроить Maximum Prefix следующим образом:
   1. R7 должен принимать максимум 7 префиксов от R2
   2. При достижении 65 % (4 префикса) должно быть сгененировано лог сообщение
   3. После превышения максимума в 7 префиксов, сессия должна переустанавливаться
   4. Поиграиться с разными значениями Maximum Prefix
4. На маршрутизаторе R7 настроить Soft Reconfiguration по отношению к R2 следующим образом:
   1. Указать, что вся маршрутная информация сохраняется в таблице adj-RIB-in
   2. Создать Route Map под названием PREF:
      1. Указать локальный префикс равный 800
      2. Применить по отношению к R2
   3. Проверить, каким образом изменилась таблица adj-RIB-in
5. На маршрутизаторах R2 и R7 настроить ORF по отношению друг к другу следующим образом:
   1. На маршрутизаторе R2 настроить Prefix List под названием INBOUND:
      1. Разрешить только маршруты 180.1.5.5/32 и 180.1.6.6/32
      2. Применить в BGP процессе 21 на входе по отношению к R7
   2. На маршрутизаторе R2 настроить ORF на выходе по отшению к R7
   3. На маршрутизаторе R7 настроить ORF на входе по отшению к R2
   4. Проверить как отрабатывает ORF

## [Цикл 22, Лабораторная работа по теме 130:MPLS](http://ccie.linkmeup.ru/2017/11/30/tsikl-22-laboratornaya-rabota-po-teme-130-mpls/)

1. Загрузить [начальную конфигурацию](https://drive.google.com/open?id=1eSFyyH4qsKYDbIgs_ycWWTTM1iaEIF1l) всех устройств.
2. Для задания используется логическая и физическая топологии проекта.
3. На маршрутизаторах R3 и R7 настроить VRF следующим образом:
   1. Настроить VRF под названием BLUE
      1. Route Distinguisher 2:2
      2. Route Target (Export/Import) 2:2
      3. На R3 применить на интерфейсе E0/1.235
      4. На R7 применить на интерфейсе E0/1.7
   2. Настроить VRF под названием GREEN
      1. Route Distinguisher 1:1
      2. Route Target (Export/Import) 1:1
      3. На R3 применить на интерфейсе E0/1.23
      4. На R7 применить на интерфейсе E0/1.78
4. На маршрутизаторах R1, R2 настроить EIGRP процесс следующим образом:
   1. Наименование GREEN
   2. Номер автономной системы 1289
   3. Адвертайзить префиксы 180.1.0.0 и 188.1.0.0
5. На маршрутизаторе R3 настроить настроить EIGRP процесс следующим образом:
   1. Наименование CORE:
      1. Address Family IPv4:
         1. AS — 73
         2. Network 180.1.0.0 и 188.1.0.0
         3. Редистрибьютить BGP процесс 73
      2. Address Family VRF GREEN:
         1. AS — 1289
         2. Network 180.1.0.0 и 188.1.0.0
         3. Редистрибьютить BGP процесс 73
      3. Address Family VRF BLUE:
         1. AS — 57
         2. Network 180.1.0.0 и 188.1.0.0
         3. Редистрибьютить BGP процесс 73
6. На маршрутизаторе R5 настроить EIGRP процесс следующим образом:
   1. Наименование BLUE
   2. Номер автономной системы 57
   3. Адвертайзить префиксы 180.1.0.0 и 188.1.0.0
7. На маршрутизаторе R7 настроить настроить EIGRP процесс следующим образом:
   1. Наименование CORE:
      1. Address Family IPv4:
         1. AS — 73
         2. Network 180.1.0.0 и 188.1.0.0
         3. Редистрибьютить BGP процесс 73
      2. Address Family VRF GREEN:
         1. AS — 1289
         2. Network 180.1.0.0 и 188.1.0.0
         3. Редистрибьютить BGP процесс 73
      3. Address Family VRF BLUE:
         1. AS — 57
         2. Network 180.1.0.0 и 188.1.0.0
         3. Редистрибьютить BGP процесс 73
8. На маршрутизаторе R4, R6 настроить EIGRP процесс следующим образом:
   1. Наименование CORE:
      1. Address Family IPv4:
         1. AS — 73
         2. Network 180.1.0.0 и 188.1.0.0
9. На маршрутизаторах R8, R9, R10 настроить EIGRP процесс следующим образом:
   1. Наименование GREEN
   2. Номер автономной системы 1289
   3. Адвертайзить префиксы 180.1.0.0 и 188.1.0.0
10. На маршрутизаторе R3 настроить BGP процесс следующим образом:
    1. Номер AS — 73
    2. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Указать в качестве Update Source интерфейс Loopback0
          3. В качестве соседа указать IP адрес Loopback интерфейса маршрутизатора R7
          4. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Настроить VPN следующим образом:
          1. Настроить Address Family VPNv4
          2. Активировать соседа R7
          3. Испольховать Extended Community
       3. Настроить VRF BLUE следующим образом:
          1. Настроить Address Family VPNv4 VRF BLUE
          2. Редистрибьютить EIGRP процесс 57
       4. Настроить VRF GREEN следующим образом:
          1. Настроить Address Family VPNv4 VRF GREEN
          2. Редистрибьютить EIGRP процесс 1289
11. На маршрутизаторе R7 настроить BGP процесс следующим образом:
    1. Номер AS — 73
    2. Создать внутренюю bgp сессию следующим образом:
       1. Создать BGP Peer Group:
          1. Название IBGP
          2. Настроить марщрутизатор таким образом, чтобы он менял атрибут BGP NEXT\_HOP на свой собственный Loopback адрес.
       2. Указать в качестве Update Source интерфейс Loopback0
       3. В качестве соседей указать IP адрес Loopback0 интерфейса маршрутизатора R3
          1. Настроить VPN следующим образом:
             1. Настроить Address Family VPNv4
             2. Активировать соседа R3
             3. Испольховать Extended Community
       4. Настроить VRF BLUE следующим образом:
          1. Настроить Address Family VPNv4 VRF BLUE
          2. Редистрибьютить EIGRP процесс 57
       5. Настроить VRF GREEN следующим образом:
          1. Настроить Address Family VPNv4 VRF GREEN
          2. Редистрибьютить EIGRP процесс 1289
12. Настроить MPLS на маршрутизаторах R3, R4, R6, R7 следующим образом:
    1. Настроить MPLS глобально на всех маршрутизаторах
    2. На маршрутизаторе R3:
       1. Ограничить диапазон MPLS заголовков от 300 до 399
       2. Настроить интерфейсы E0/1.34 таким образом, чтобы они принимали участие в MPLS Label Switching
    3. На маршрутизаторе R4:
       1. Ограничить диапазон MPLS заголовков от 400 до 499
       2. Настроить интерфейсы E0/1.34, E0/1.456 таким образом, чтобы они принимали участие в MPLS Label Switching
    4. На маршрутизаторе R6:
       1. Ограничить диапазон MPLS заголовков от 600 до 699
       2. Настроить интерфейсы E0/1.67, E0/1.456 таким образом, чтобы они принимали участие в MPLS Label Switching
    5. На маршрутизаторе R7:
       1. Ограничить диапазон MPLS заголовков от 700 до 799
       2. Настроить интерфейсы E0/1.67 таким образом, чтобы они принимали участие в MPLS Label Switching
13. На маршрутизаторах R3 и R7 настроить VRF следующим образом:
    1. Настроить VRF под названием BLUE
       1. Route Distinguisher 1:1
       2. Route Target (Export/Import) 1:1
       3. На R3 применить на интерфейсе E0/1.235
       4. На R7 применить на интерфейсе E0/1.7
    2. Настроить VRF под названием GREEN
       1. Route Distinguisher 2:2
       2. Route Target (Export/Import) 2:2
       3. На R3 применить на интерфейсе E0/1.23
       4. На R7 применить на интерфейсе E0/1.78

# [**Цикл 23**](http://ccie.linkmeup.ru/2017/12/15/voprosy-po-tsiklu-22-tema-133-mpls-4-1/)

# [**Цикл 24**](http://ccie.linkmeup.ru/2017/12/25/voprosy-po-tsiklu-24-tema-139-mpls/)

# [**Цикл 25**](http://ccie.linkmeup.ru/2017/12/25/voprosy-po-tsiklu-24-tema-145-ipv4-multicast-routing/)

# [**Цикл 26**](http://ccie.linkmeup.ru/2017/12/25/voprosy-po-tsiklu-26-tema-151-network-programmability-sdn/)