NETMandala2019 — слайды к вебинару

NETMandala2019 - «методология построение компьютерных сетей операторского и корпоративного типа».

Или

«чему, как, зачем и почему нужно учиться IT-специалисту»

вебинар

Москва, 27 февраля 2019 г

16:00-17:30

Спикер: Евстропов А.В.

EustroSoft.org

При участии АНО ДПО «МАСПК» http://maspk.ru

NETMandala2019 — слайды к вебинару

Программа

1. Причины и обстоятельства возникновения проекта NETMandala
2. Взаимодействие с RIPE NCC для получения сетевых ресурсов (политика ripe-587)
3. Как устроен Internet — Регулирующие органы и их БД, Автономные системы (AS), BGP
4. Как устроена сеть ISP и что из этого можно применить в корпоративной сети
5. Общие проблемы ISP, лицензирование, СОРМ, фильтрация трафика по Роскомнадзор, что из этого полезно применить в корпоративной сети
6. Обзор доступного оборудования и отечественных производителей - «динозавры», «наклейщики», «2000-ники».
7. Методология NETMandala и курс NETMandala2018
8. Программа курса NETMandala2018
9. Современная телефония SIP, E1, TDMoP, SIP<->E1 – за бортом NETMandala
10. Эталонная модель сети ISP, проблема описания топологии на разных уровнях L1,L2,L3
11. Простейшая сеть ISP, план VLAN, внутр. план адресации IPv4 (RFC1918 и RFC6598)
12. IPv4 vs IPv6 – проблемы и обоснованность внедрения IPv6
13. Динамическая маршрутизация OSPF vs BGP
14. Технологии канального уровня Ethernet, VLAN, Q-in-Q vs MPLS
15. Технологии физического уровня оптоволокно, WDM, CWDM, DWDM
16. Методика аттестации NETMandala2018
17. Вопросы

Проект NETMandala - моделирование сети оператора связи

- NETMandala — проект в котором мы долго и кропотливо собираем довольно сложную сеть, а потом быстро ее разбираем, и делаем вид, что так и было
- Символ проекта — «Песчаная Мандала*»

* Мандала - сакральное схематическое изображение Вселенной в буддийско-индуисткой религиозной практике, имеет форму картины подобной иконе в нашей традиции.
Песчаная Мандала — то-же самое из цветного песка, сто или тысяча монахов в закрытом помещении целый год рисуют это картину цветным песком, а потом, по завершению открывают двери ветру или зовут настоятеля с большим веером и картина снова становится песком. И можно начинать все заново.
Мы делаем приблизительно тоже самое.

NETMandala причины и обстоятельства возникновения проекта

- Суть проекта — построение с нуля на пустом месте сети оператора связи для исследовательский целей.
  - Исходная проблема — невозможность наработать этот опыт на реальной сети, находящийся в эксплуатации
- Эту сеть можно в короткое время пере-конфигурировать или перестроить под любую экспериментальную модель или под любое оборудование.
- На базе этого проекта можно подготовить методические материалы для обучения сетевых инженеров построению сетей на основе выбранного оборудования или на основе сформулированной модели и топологии.
  - И это сделано, в рамках курса NETMandala2018
- На базе NETMandala можно разработать и задокументировать методологию построения операторской сети из конкретного оборудования (например оборудования отечественного производства)
  - Мы зафиксировали наше понимание построения сетей на Mikrotik и успешно построили сеть на оборудовании NSG.RU
- В рамках такого моделирования можно разработать план перестройки реальной сети оператора для устранения архитектурных просчетов

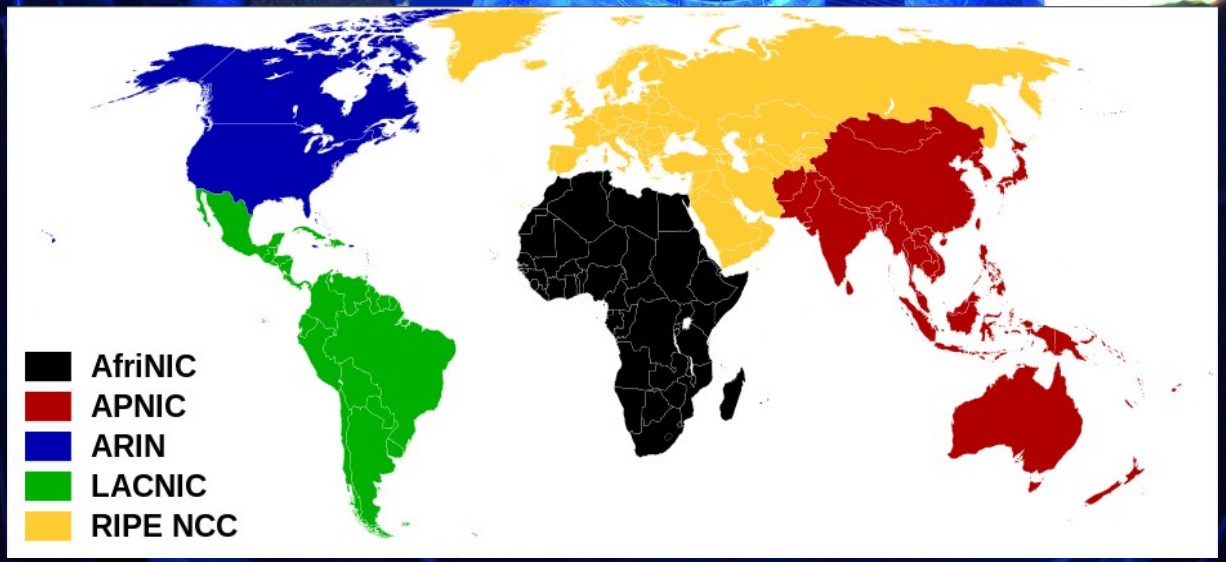
NETMandala Взаимодействие с RIPE NCC

- Взаимодействие с RIPE NCC (ripe.net) для получения временных ресурсов для академических исследований
  - ICANN → RIR → LIR → ISP → Пользователи
    - Номера AS, Адреса IP(v4,v6), домены (org,com,net,ru,su,...)
  - Политика ripe-587 — выделение временных ресурсов RIPE
  - РосНИИРОС (ripn.net) — координатор Internet в РФ (спасибо за содействие)

Ресурсы NETMandala

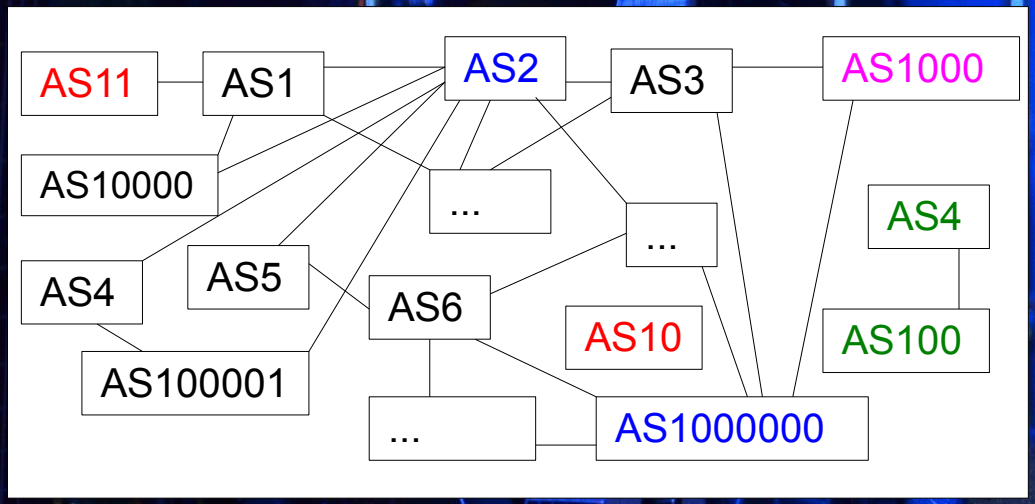
- AS58366
- IPv4: 151.216.0.0/22
- IPv6: 2001:7fc:4::/46

до 18 апреля 2019 г.



- О проблемах взаимодействия с RIPE NCC (языковые, валютные)
- Благодарность RIPE NCC

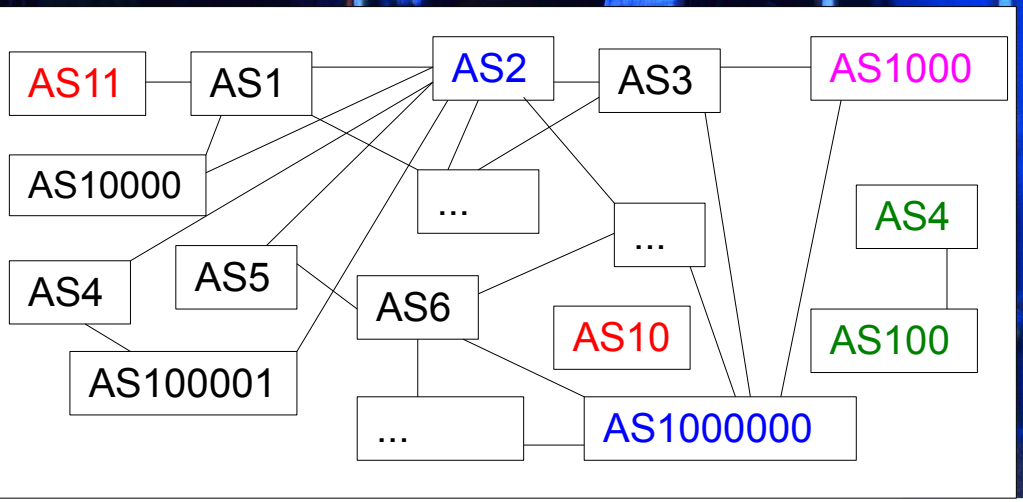
NETMandala — как устроен Internet

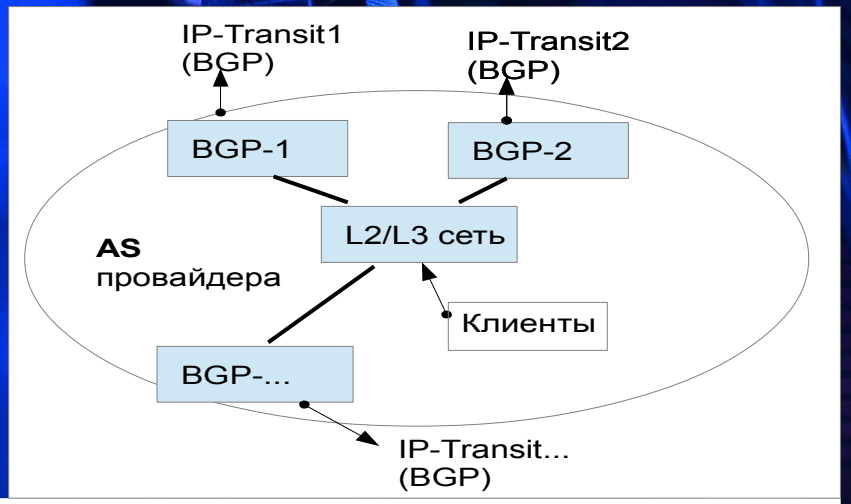


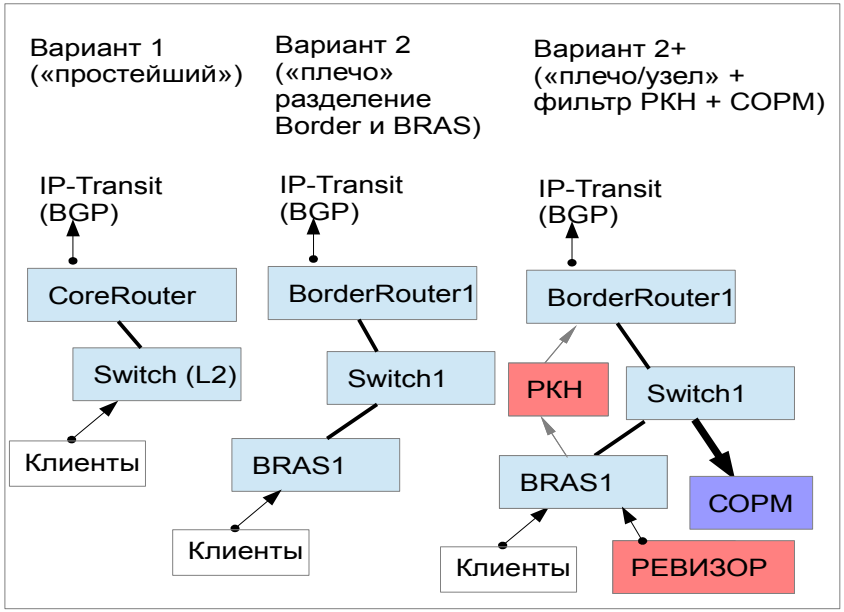
Здесь могла-бы быть картинка с устройством отдельной AS
Но этому вопросу посвящен отдельный слайд, не будем отвлекаться

- Internet — совокупность AS
- AS — это сеть провайдера или [не]крупного предприятия
- AS — это 16-битное или 32-битное число (большая часть полезного Internet была построена на первых 65536 AS)
- AS взаимодействуют через «пограничные маршрутизаторы» по протоколу BGP, понятие IP-transit, peering, Internet eXchange (IX)
- Минимально маршрутизируемая сеть IPv4 - /24 (256 адресов), IPv6 - /48 (2^16=65536 сетей /64)
- Оптимальный маршрут — самый короткий, т. е. проходящий через минимум транзитных AS

NETMandala — как устроена сеть ISP







- Варианты — эволюция от «простейшего»
- разделение функция L2 (коммутация) и L3 (маршрутизация),
- разделены функций пограничного маршрутизатора (BGP) и маршрутизатора доступа (BRAS)
- Маршрутизация внутренняя и внешняя
- Внедрение фильтрации и СОРМ
- Применение опыта в корпоративной сети

NETMandala2019 —Общие проблемы ISP

1. 'Телематические услуги связи'
2. 'Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации'

1. 'Услуги связи по предоставлению каналов связи'

1. 'Услуги местной телефонной связи, за исключением услуг местной телефонной связи с использованием таксофонов и средств коллективного доступа'
2. 'Услуги внутризоновой телефонной связи'
3. 'Услуги междугородной и международной телефонной связи'
4. 'Услуги связи по передаче данных для целей передачи голосовой информации'

1. 'Услуги связи для целей кабельного вещания'
2. 'Услуги связи для целей проводного радиовещания'
3. 'Услуги связи для целей эфирного вещания'

1. 'Услуги местной телефонной связи с использованием средств коллективного доступа'
2. 'Услуги местной телефонной связи с использованием таксофонов'
3. 'Услуги подвижной радиосвязи в выделенной сети связи'
4. 'Услуги подвижной радиосвязи в сети связи общего пользования'
5. 'Услуги подвижной радиотелефонной связи'
6. 'Услуги подвижной радиотелефонной связи (при использовании бизнес-модели виртуальных сетей подвижной радиотелефонной связи)'
7. 'Услуги подвижной спутниковой радиосвязи'
8. 'Услуги почтовой связи'
9. 'Услуги связи персонального радиовызова'
10. 'Услуги телеграфной связи'
11. 'Услуги телефонной связи в выделенной сети связи'

1. Закон о связи, лицензирование, понятие «узла», биллинг, СОРМ, РЕВИЗОР, фильтрация трафика по Роскомнадзор
2. «Операторский налог» (1.2% с выручки)
3. Телефония, местная, зона, МГ-МН, биллинг, присоединение, ОКС7, E1, SIP (слайд в конце)
4. Регулирующие и контролирующие органы (Минкомсвязи, РКН, ФСБ, Россвязь, ГКРЧ, Ростехнадзор,МВД, ...)
5. Сертификаты на оборудование, электробезопасность и ССС
6. Аттестация персонала (электробезопасность)
7. Проблема профессионального роста кадров (проблема «каст»)

NETMandala2019 — обзор оборудования

Обзор доступного оборудования и отечественных производителей - «динозавры», «наклейщики», «2000-ники».

- **OpenSource Unix: 4.4BSD - FreeBSD, NetBSD, OpenBSD; GNU, Linux**
- **Мировые лидеры**
  - **Cisco Systems (US, $49 bln)**
  - **Juniper Networks (US, $5 bln)**
  - **D-Link Corporation (TW, $? bln)**
  - **Huawei Technologies Co., Ltd (CN, $92 bln)**
  - **DIGITAL CHINA NETWORKS LIMITED (CN, $? bln)**
- **«Новая волна»**
  - **Mikrotik (Латвия, $0.3 bln)**
  - **Ubiquiti Networks (US, $1 bln)**
- **Отечественное**
  - **SNR (г. Екатеринбург) – Ethernet Switches, SFP модули**
  - **Eltex (г. Новосибирск) – полная линейка оборудования**
  - **RDP.ru (г. Москва, Сколково) – маршрутизаторы и NAT,**
  - **NSG.ru (г. Москва) 30% банкоматов - через маршрутизаторы NSG**
  - **GarantPlus (г. Ярославль) - Шлюзы SIP-E1 Alvis-GW**
  - **VASExperts.ru (СПБ) – ПО для DPI**

Методология NETMandala

Курс NETMandala2018[v2019] - «Экстремальный курс построения операторской сети за 5 дней... или за 3 дня?»

1. **Сверху вниз и от сложного к простому — от присоединения к Internet к развитию внутренней сети, от того, что написано в конце учебника, к тому, что написано в его начале**
2. **Экстремальность — в понимании методологий «экстремального программирования» (от быстрого первоначального решения, через рефакторинг к выработке решения оптимального)**
3. **Импровизация — лучше импровизировать, чем играть по нотам, если получится красиво — можно записать ноты и импровизировать на их основе**
4. **Принцип 30/70 — 30% теории 70% практики**
5. **Поэтичность - Хорошая теория должна быть больше похожа на поэму, чем на роман; на роман, чем на словарь; на словарь, чем на азбуку**
6. **Человека ничему нельзя научить, он всему учится сам, ему можно в этом только помочь, создав необходимые условия и предоставив карту прохождения маршрута**
7. **По Гамбургскому счету — лучшая оценка, которую можно поставить в диплом, это оценка, которую поставят тебе коллеги**

Программа курса NETMandala2018 (5 дней)

День 1 — понедельник 50/50
0) Причины и обстоятельства возникновения курса
1) Общие проблемы ISP, обзор доступного оборудования
2) как устроен Internet и как устроен ISP, БД RIPE
3) Эталонная модель сети ISP
4) Простейшая сеть ISP, план VLAN, внутр. план адресации IPv4
5) лабораторная работа построение простейшей сети ISP

День 2 — вторник 50/50
1) глобальная маршрутизация BGP, Transit, IX, пиринг
2) локальная маршрутизация, статическая, динамическая, OSPF
3) IPv4 vs IPv6
4) практическое применение MPLS (MPLS vs OSPF)
5.1) лабораторная работа построение сети ISP — эталонная модель
5.2) продолжение лабораторной работы — внедрение OSPF и MPLS

День 3 — среда 50/50
1) типовые сервисы ISP (DNS, Mail, NTP, LookingGlass)
2) детали DNS
3) почтовый сервер ISP
4) Looking Glass
5.1) лабораторная работа по развертыванию типовых сервисов ISP
5.2) продолжение лабораторной работы — Looking Glass, анализ сети

День 4 — четверг 100% практическая работа по заданному плану
День 5 — пятница 100% практическая работа по собственному выбору

Программа курса NETMandala2018v2019 (3 дня)

День 1

0) Причины и обстоятельства возникновения курса, введение (20 мин)

1) Общие проблемы ISP, обзор доступного оборудования 1.1) обзор построения телефонной сети, лицензирование, СОРМ 1.2) обзор распространенного сетевого оборудования, мировых и отечественных производителей, перспективных разработок (45 мин)

2) как устроен Internet и как устроен ISP, БД RIPE (45 мин)

3) Эталонная модель сети ISP – пограничный маршрутизатор, BRAS (45 мин)

4) Простейшая сеть ISP, план VLAN, внутр. план адресации Ipv4 (20 мин)

5) типовые UNIX сервисы ISP – NTP, DNS, почтовый сервер, LookingGlass и другие (45 мин)

6) лабораторная работа построение простейшей сети ISP (3 часа)

6.1) работа с удаленным Looking Glass, для анализа видимости своей сети (1 час)

День 2

1) глобальная маршрутизация BGP, Transit, IX, пиринг (45 мин)

2) локальная маршрутизация, статическая, динамическая, OSPF (45 мин)

3) Ethernet, VLAN, Q-in-Q, IPv4 vs IPv6, GRE (45 мин)

4) применение MPLS для резервирования каналов L2 (MPLS vs OSPF) (20 мин)

5) небольшой обзор технологий оптоволоконной связи: кабель, муфта, волокно, лямбда - WDM, CWDM, DWDM, PON (45 мин)

6.1) лабораторная работа построение сети ISP — эталонная модель (3 часа)

6.2) продолжение лабораторной работы — внедрение OSPF (1 час)

День 3

1) Свободная практика

2) Аттестация

Телефония - за бортом NETMandala

Современная телефония SIP, E1, TDMoP, SIP<->E1 – за бортом NETMandala

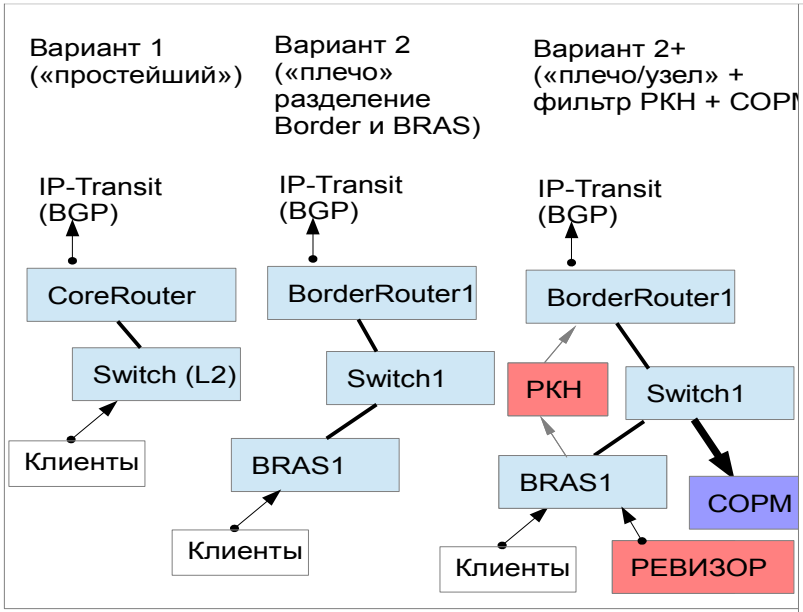
1. **Присоединение (телефония на операторском уровне)**
   - **Биллинг и ФРОД**
   - **Проблема резервирования входящих звонков**
   - **Проблемы введения в эксплуатацию новых номерных емкостей**
2. **Виды телефонной связи - местная, зоновая и МГ-МН**
3. **Классическая телефония (TDM, E1, FXS/FXO)**
4. **Современная телефония (VoIP/SIP)**
5. **Проблемы передачи телефонии по пакетным сетям и их решения**
   - **Задержки, джиттер, эхо, односторонняя слышимость**
   - **Проблемы прохождения факсимильных сообщений (проблема кодеков)**
   - **Проблема маленьких пакетов (<512 байт) на 1G Ethernet**
   - **Перейти на SIP, проблемы старых АТС, шлюзы SIP<->E1 (Alvis-GW-2E1)**
   - **TDMoP — передача синхронных потоков E1 поверх асинхронных сетей Ethernet/IP - костыли**
6. **Перспективы отдельного проекта TDMandala ;)**

NETMandala, эталонная модель сети ISP, топологии L1-L3

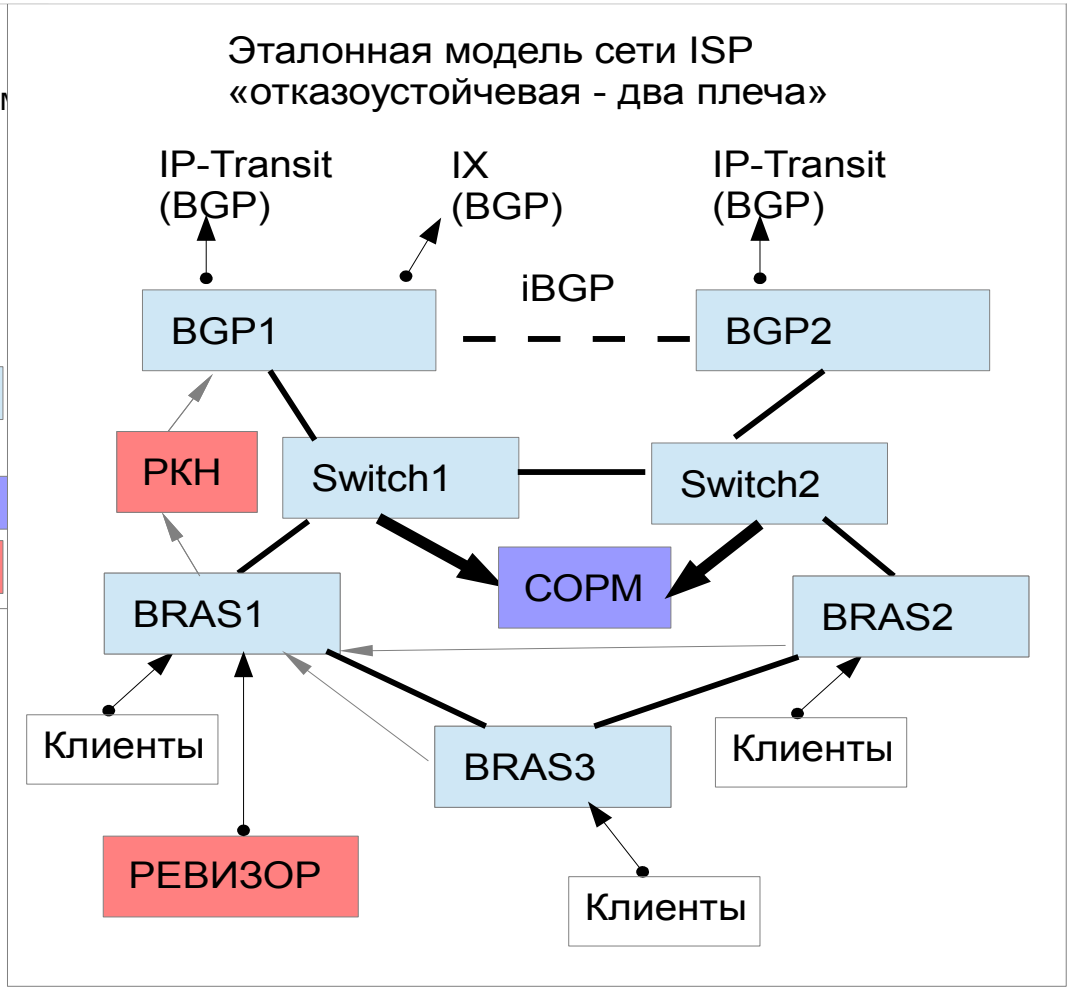
Эталонная «двухплечевая» модель сети

1) Цель импровизационного моделирования

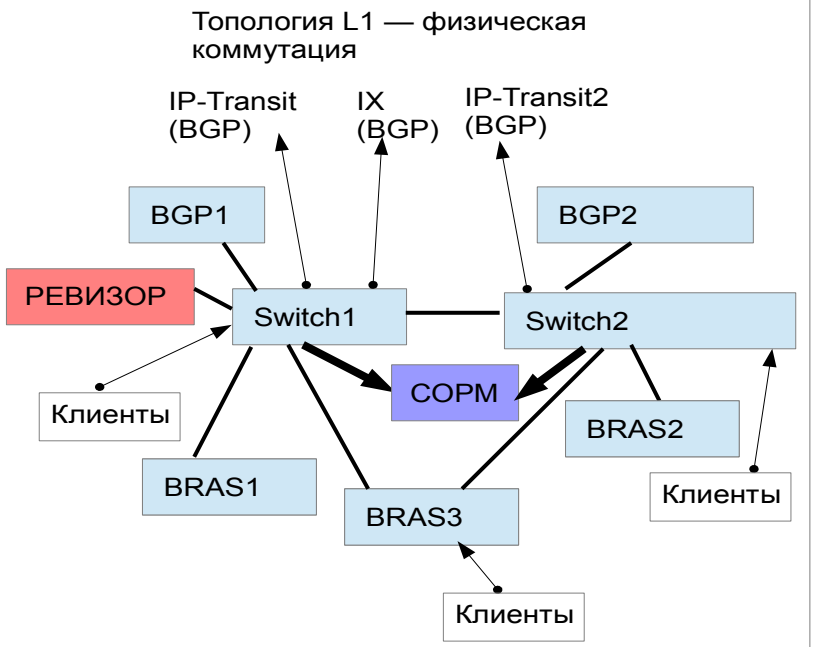
2) средство моделирования и изучения

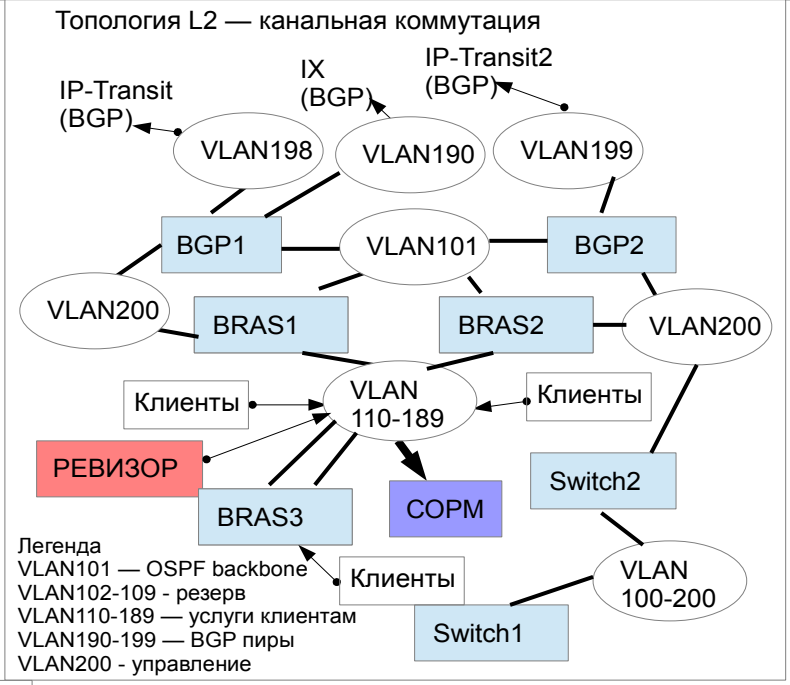


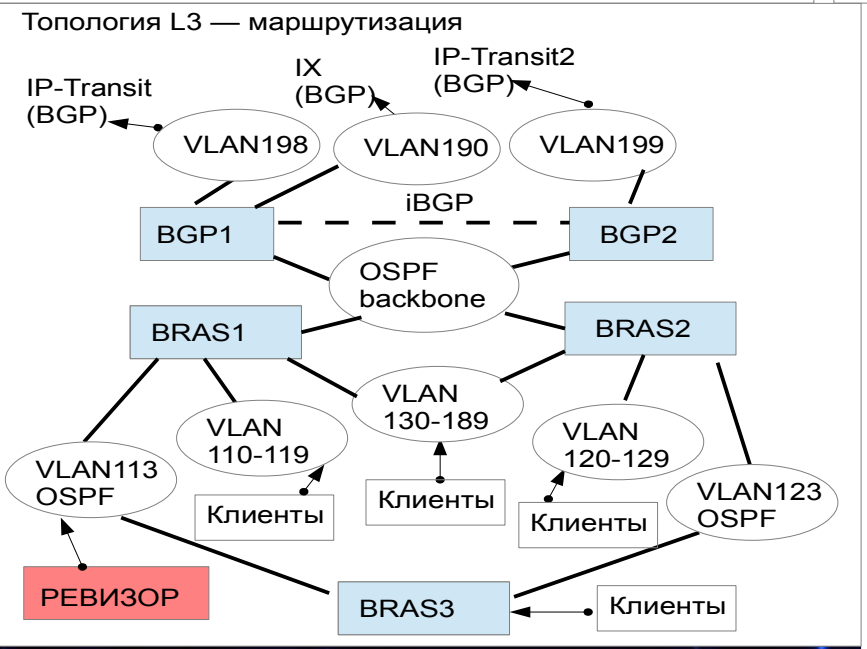
3) проблема описания топологии сети на разных уровнях «модели OSI» (следующий слайд)



NETMandala, эталонная модель сети ISP, топологии L1-L3







Недостающие уровни «Эталонной сетевой модели OSI»

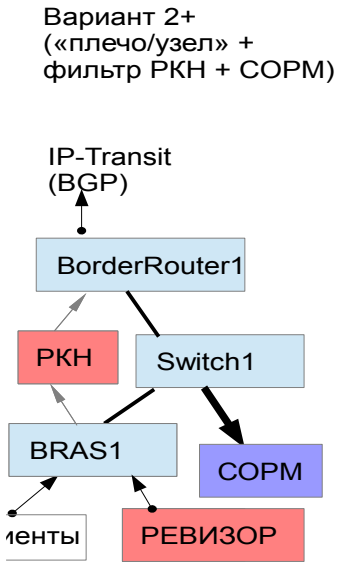
- -1 частотно-временной (длины волн, тайм-слоты)
- -2 уровень среды (оптические волокна, в которых распространяется сигнал)
- -3 кабельный уровень (кабеля, в которых находятся волокна)
- -4 канализационный (коллекторы, в которых лежат кабеля)
- 0 - уровень неопределенности

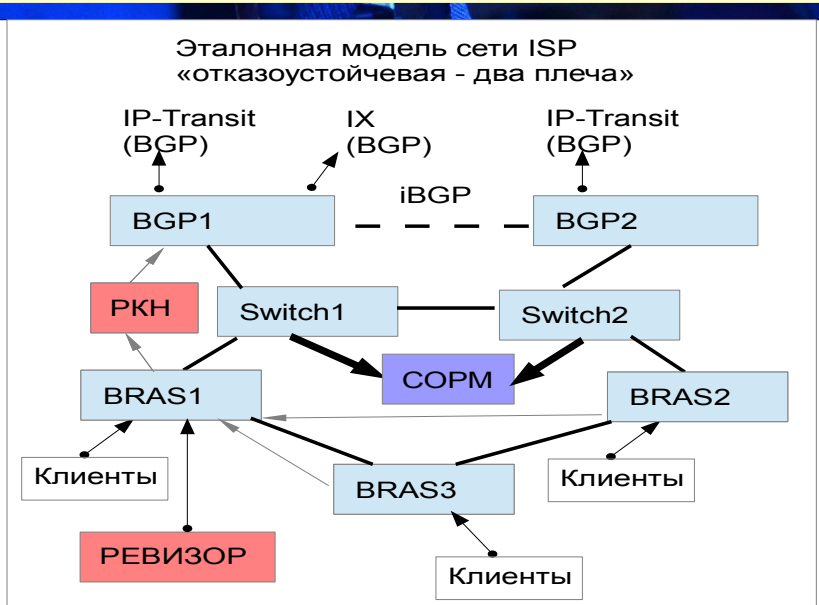
NETMandala, эталонная модель сети ISP, топологии L1-L3

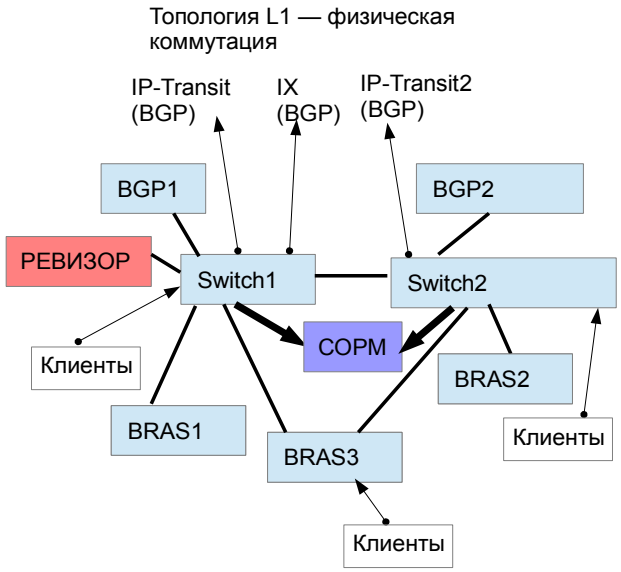
Эталонная «двухплечевая» модель сети

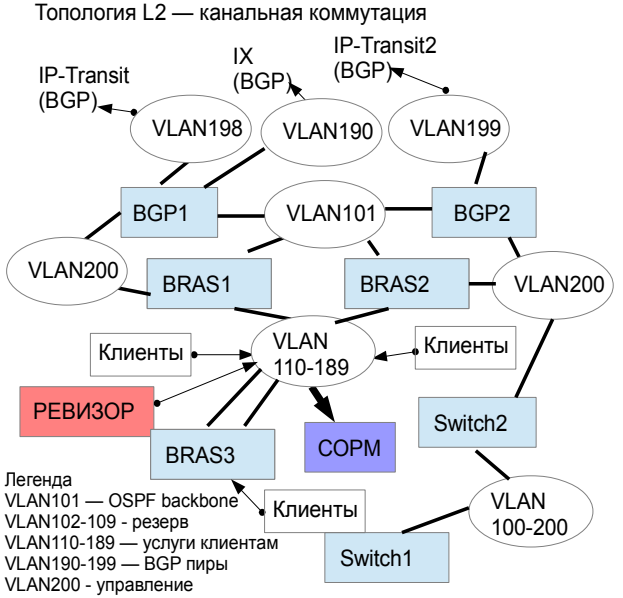
1) Цель и средство моделирования и изучения

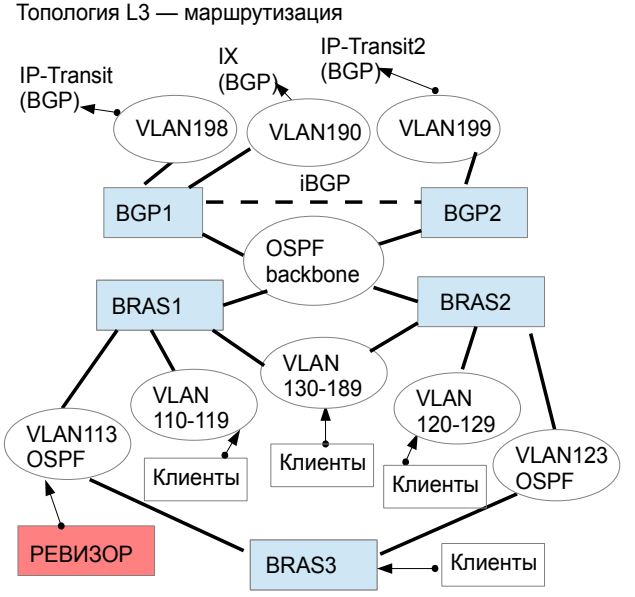
2) Проблема топологии







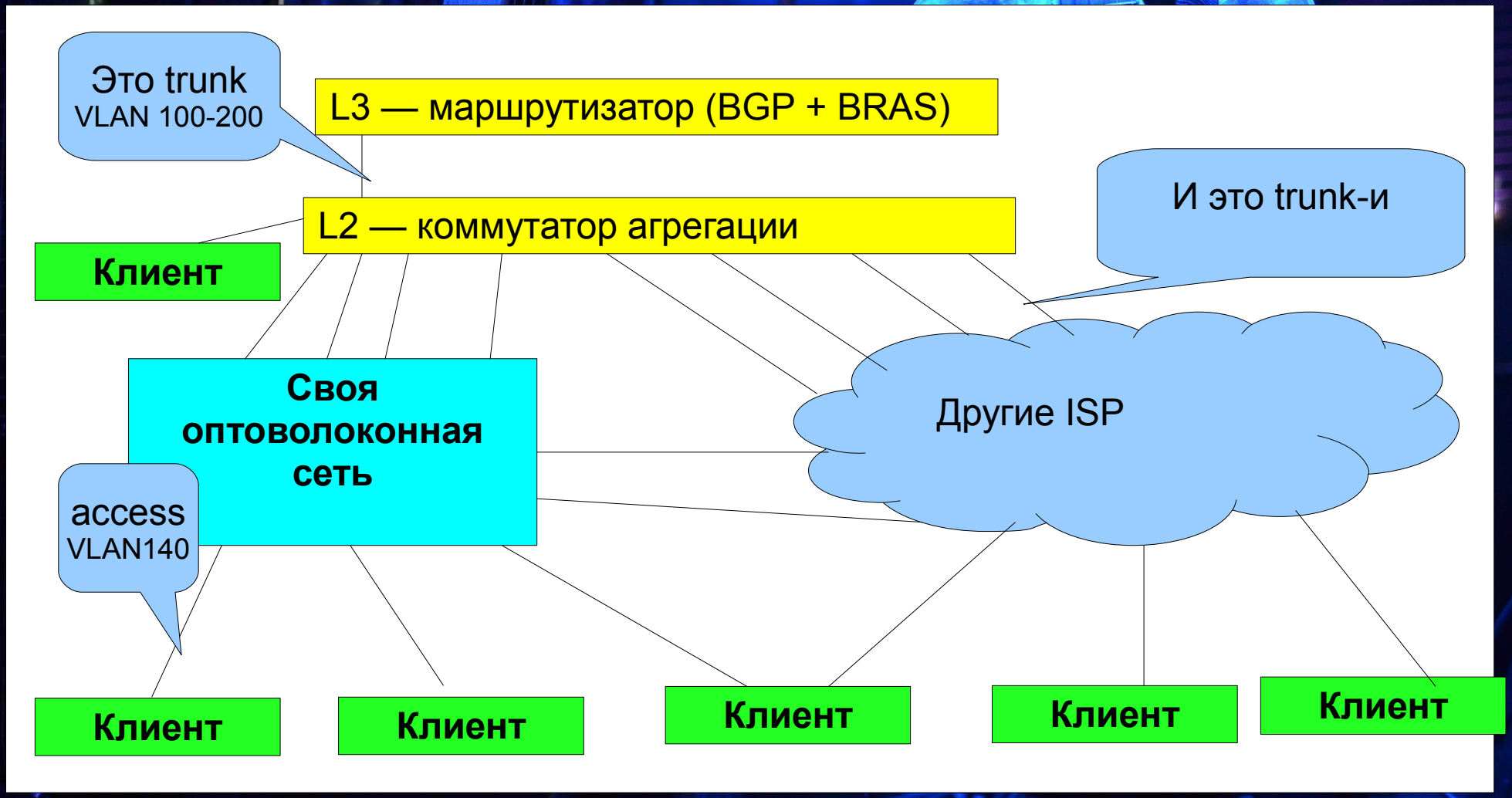




- Недостающие уровни «Эталонной сетевой модели OSI»
- -1 частотно-временной, -2 среда, -3 кабель, -4 канализация

NETMandala — простейшая сеть ISP

- План VLAN — выбираем произвольный диапазон из 4094 (напр 100-200)
- IPv4 — внутренние адреса (внешние на следующем слайде)
  - Корп сеть - RFC1918 (10./8, 192.168./16, 172.16/12 или **172.16.0.0-172.31.255.255**)
  - Сеть ISP — RFC6598 (100.64.0.0/10 или **100.64.0.0-100.127.255.255**)



NETMandala — Распределение пространства /23 (ISP)

IPv4 Network1 /24

xxx.xxx.yyy.0/28 Public services DNS,mail,ntp and so on (primary)
xxx.xxx.yyy.16/28 VoIP services
xxx.xxx.yyy.32/27 Collocation service
xxx.xxx.yyy.64/26 Client network
xxx.xxx.yyy.128/27 NAT-6-to-4 Service
xxx.xxx.yyy.160/27 Hosting service
xxx.xxx.yyy.192/29 client network (reserved)
xxx.xxx.yyy.200/29 client network (reserved)
xxx.xxx.yyy.208/29 client network (reserved)
xxx.xxx.yyy.216/29 client network (reserved)
xxx.xxx.yyy.224/29 client network (reserved)
xxx.xxx.yyy.232/29 client network (reserved)
xxx.xxx.yyy.240/29 client network (reserved)
xxx.xxx.yyy.248/29 client network (reserved)

IPv4 Network2 /24

xxx.xxx.zzz.0/28 Public services (secondary)
xxx.xxx.zzz.16/28 VoIP services (secondary)
xxx.xxx.zzz.32/27 VPS/VDS service
xxx.xxx.zzz.64/26 SOHO clients
xxx.xxx.zzz.128/26 NAT for home network clients
xxx.xxx.zzz.192/26 home network clients with public IP

NETMandala — публичные сервисы ISP (/28)

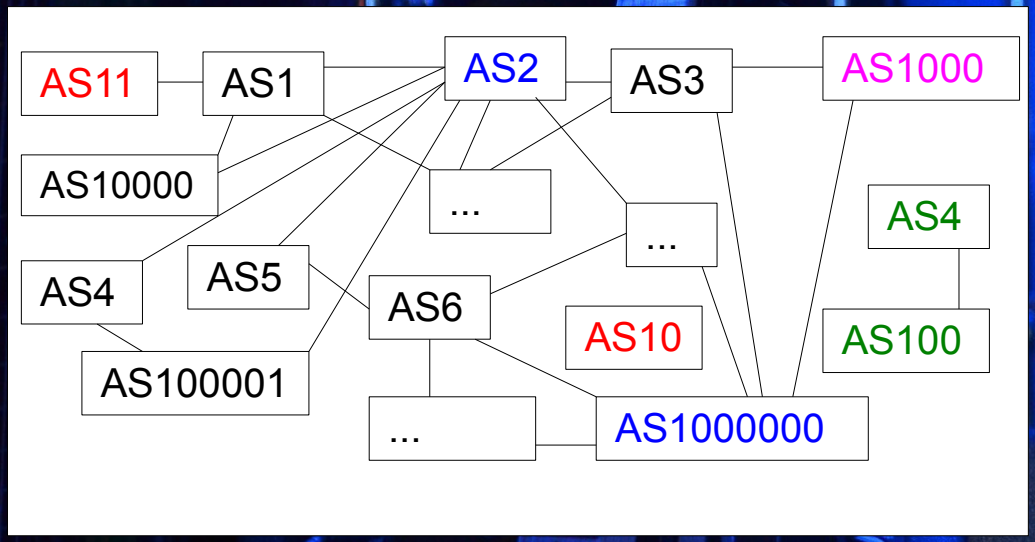
xxx.xxx.{yyy|zzz}.1	gw1	default-gateway
xxx.xxx.{yyy|zzz}.2	ns	DNS сервер
xxx.xxx.{yyy|zzz}.3	mail	SMTP сервер (прием/отправка почты)
xxx.xxx.{yyy|zzz}.4	nat	NAT (для внутренних нужд)
xxx.xxx.{yyy|zzz}.5	web	HTTP/HTTPS сервер
xxx.xxx.{yyy|zzz}.6	nagios	Система мониторинга
xxx.xxx.{yyy|zzz}.7		(reserved)
xxx.xxx.{yyy|zzz}.8	mix	Все службы «в одном флаконе»
xxx.xxx.{yyy|zzz}.9	lg	Looking Glass (если у вас своя AS)
xxx.xxx.{yyy|zzz}.10	ntp	NTP сервер (точное время stratum3)
xxx.xxx.{yyy|zzz}.11	intra	(reserved) intra https/pop/imap
xxx.xxx.{yyy|zzz}.12	ftp	FTP сервер (reserved)
xxx.xxx.{yyy|zzz}.13		(reserved)
xxx.xxx.{yyy|zzz}.14	gw14	default-gateway2

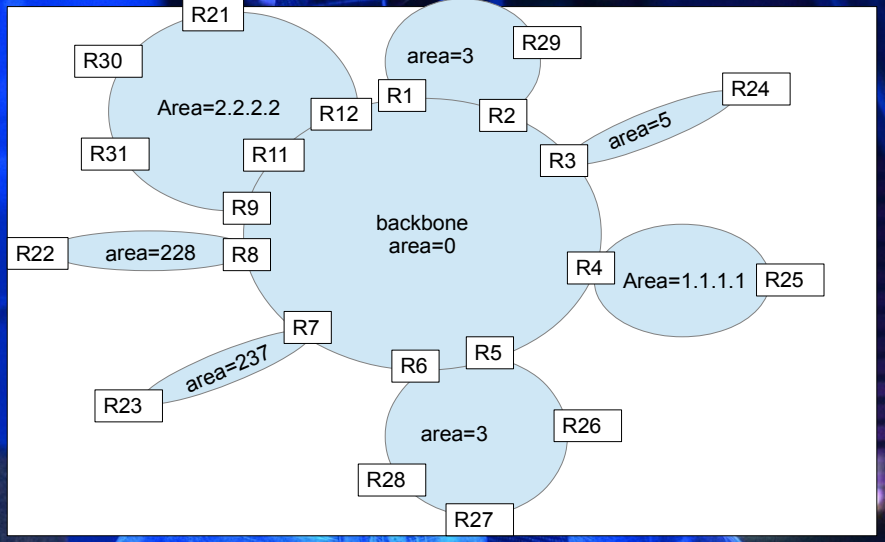
NETMandala2019 — IPv4 vs IPv6

Дискуссионная тема

1. **IPv4 vs IPv6 – проблемы и обоснованность внедрения IPv6**
2. **Дискуссионная тема, мои тезисы:**
    1. **Провайдеру необходимо внедрять у себя IPv6, однозначно**
        1. **чтобы быть готовым его предоставить клиентам**
        2. **Чтобы быть в курсе текущих трендов**
        3. **Чтобы иметь свое мнение по этому вопросу**
    2. **IT-специалисту стоит его изучать**
        1. **Это интересно**
        2. **Internet v6 сейчас по атмосфере похож на Internet v4 в 199x**
        3. **Чтобы разобраться, чем грозит его внедрение и подготовиться к этому**
            1. **Например, представьте, готовы-ли Вы, чтобы на каждом устройстве в вашей офисной сети был публичный адрес Ipv4, доступный со всего Internet**
    3. **Для корпоративной сети — внедрение на усмотрение ЛПР**
    4. **Возможно, что вместо Ipv6 появится и получит повсеместное распространение другой протокол, также как в свое время стек TCP/IP полностью вытеснил протоколов OSI**
    5. **Возможно, что Ipv6 проявление тезиса «генералы всегда готовятся к прошедшей войне» в применении к сетевым технологиям**

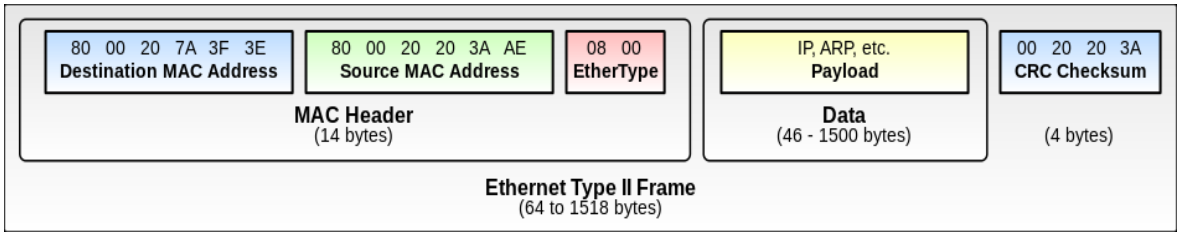
Динамическая маршрутизация OSPF vs BGP





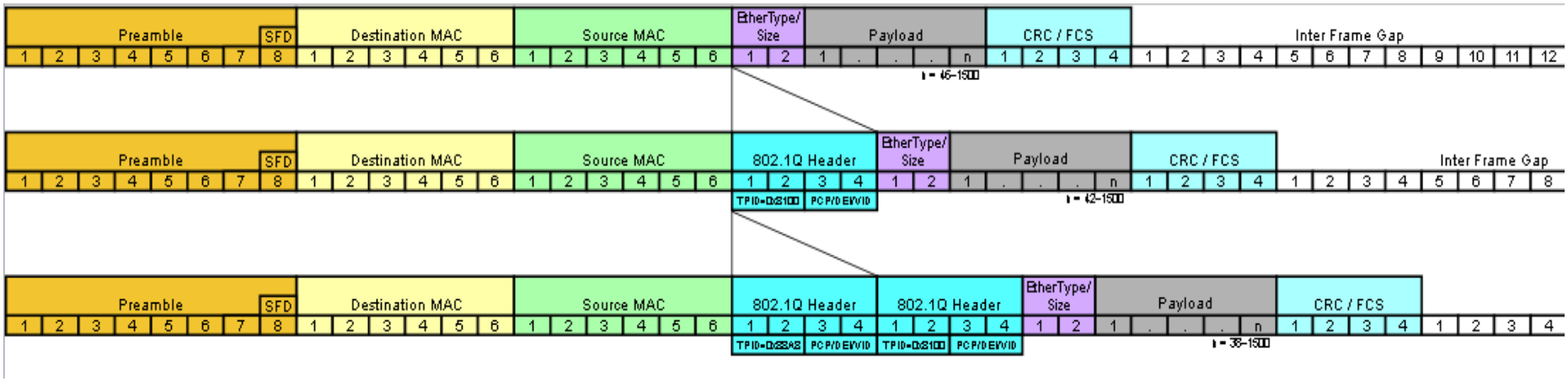
1. **Наша методология начинается с присоединения к Internet и изучения eBGP**
2. **Внутри AS, если более одного border используется iBGP**
3. **Можно построить внутреннюю маршрутизацию на BGP, но iBGP для этого не предназначен**
4. **Но есть номера AS, зарегистрированных для внутреннего использования (64512 – 65535)**
5. **Достоинства BGP — развитая система фильтров, нет предела масштабируемости**
    1. **Недостатки — накладные расходы на настройку каждого соединения**
6. **Достоинства OSPF — простота настройки каждого нового маршрутизатора**
    1. **Недостатки — более сложная, «нелинейная» логика работы, меньше возможностей для «ручного» контроля, проблемы с масштабируемостью и поиском ошибок, чувствительность к прохождению multicast**
7. **EIGRP – хороший протокол от Cisco, но слишком долго был пропертарным**
8. **RIP – R.I.P.**

Технологии канального уровня Ethernet, VLAN, Q-in-Q vs MPLS



802.1Q tag format

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID



MPLS Label

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Label																				TC: Traffic Class (QoS and ECN)			S: Bottom-of-Stack	TTL: Time-to-Live							

1.

Технологии физического уровня (WDM, CWDM, DWDM)

1. **Типы оптического волокна (MM, SM)**
2. **Оптические коннекторы (ST,SC,FC,LC)**
3. **Тип полировок и их совместимость PC,UPC и APC**
4. **Окна прозрачности и затухание**
5. **Simplex передача (односторонняя)**
6. **Duplex передача (модули SFP, SFP+, QSFP…)**
    1. **По двум волокнам MM – 850nm**
    2. **По двум волокнам SM – 1310nm**
    3. **По одному волокну SM 1310/1550nm (WDM)**
7. **Спектральное уплотнение каналов**
    1. **Более одного дуплексного канала по одному волокну (CWDM – 8 каналов, 16 “лямбд” 1271, 1291,1311, 1331 nm, …, 1491, 1511, 1531, 1551 nm)**
    2. **Более чем 8 каналов по одному волокну – DWDM (40 и более каналов)**
    3. **Оптические мультиплексоры (OADM - Optical add-drop multiplexer)**
8. **Технология PON — другой способ организации множества каналов по одному волокну**

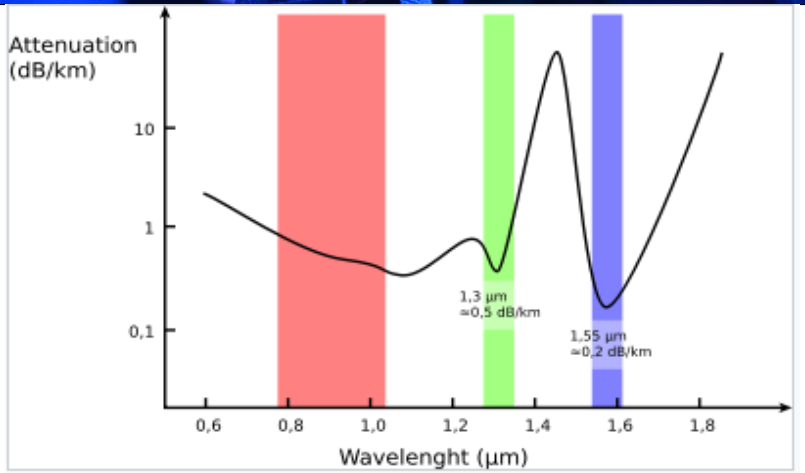
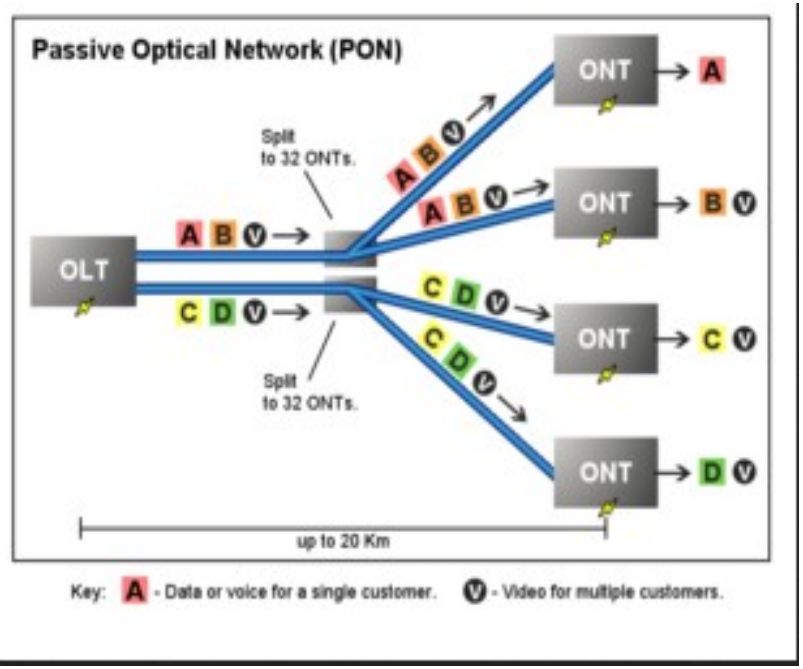


График зависимости затухания в кварцевом волокне от длины волны излучения и три окна прозрачности



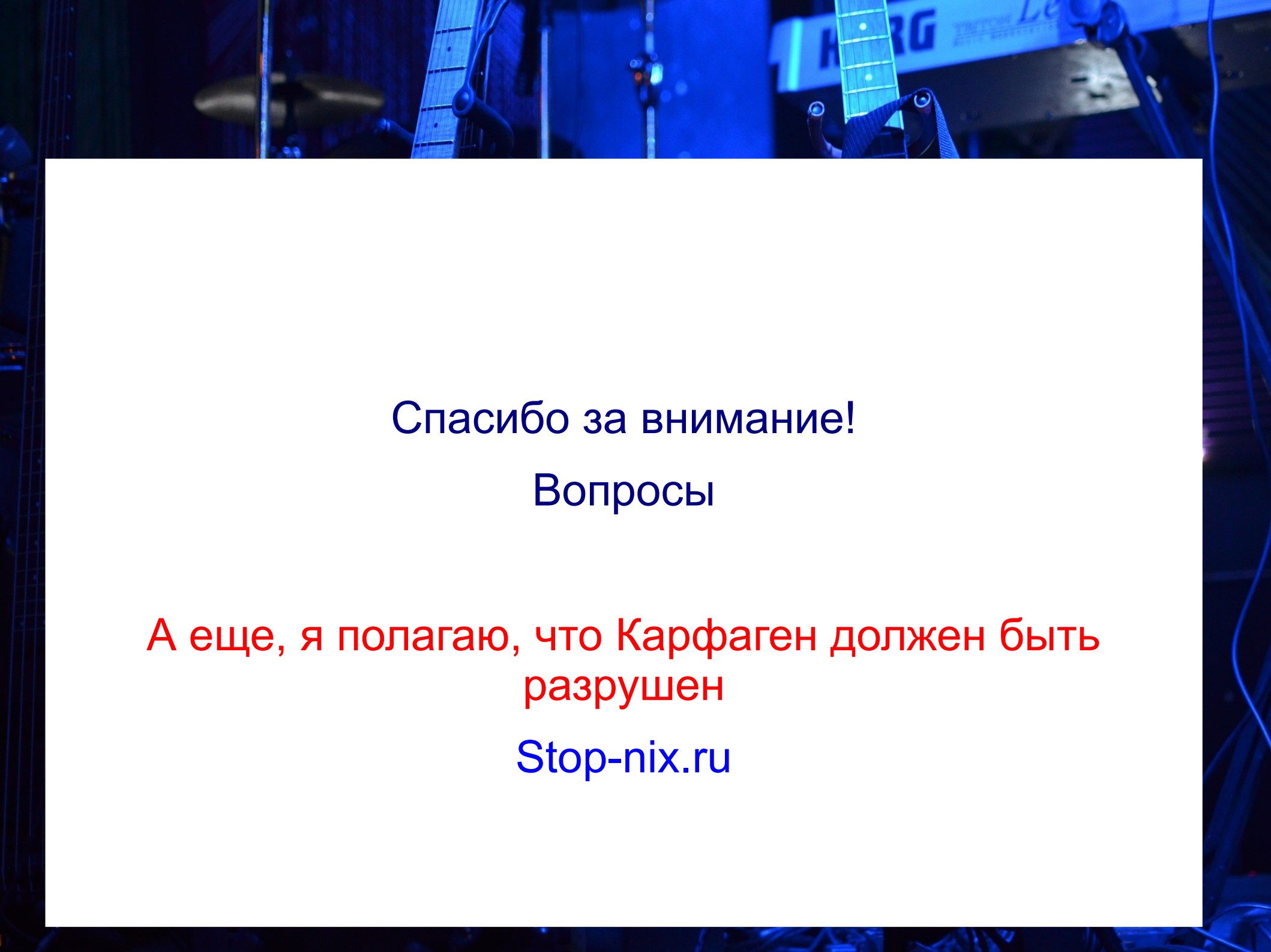
Методика аттестации NETMandala2018

NETMandala2018
Категории оценок, «По Гамбургскому счету»

0 — ничего не знает, можно поставить продажником
1 — монтажник, 1 ЛП (при наличии соотв. навыков)
2 — L2 OSI, 2 ЛП (управление свичами)
3 — L3 OSI, сетевой инженер (маршрутизаторы)
4 — Главный сетевой инженер, преподавание курса
5 — настоящий технический директор, архитектор
6 — знает больше, чем этот курс
7 — все знает, но overqualified

Принцип формирования оценки

После 3-4 дней совместной работы, каждый участник выставляет оценку каждому (в т.ч. себе и преподавателю), среднее арифметическое, если с ним согласен преподаватель, идет в диплом



Спасибо за внимание!

Вопросы

А еще, я полагаю, что Карфаген должен быть разрушен

Stop-nix.ru