МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН
ФЕРГАНСКИЙ ФИЛИАЛ ТАШКЕНТСКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Телекоммуникационный инжиниринг»

ШИРОКОПОЛОСНЫЕ СЕТИ

Методическое указание по практики

Для студентов бакалавриатуры

Фергана 2017

1-Практическая занятия

Тема: Оборудование широкополосных сетей

Softswitch, шлюзы, терминальное оборудование – основные характеристики и требования к ним

1. Теоретическая часть

Основными типами оборудования, используемыми в сетях следующего поколения являются Softswitch, шлюзы, терминальное оборудование, рассмотрим основные характеристики и требования к ним.

Softswitch

Softswitch реализует функции по логике обработки вызова, доступу к серверам приложения, сбору статистической информации, сигнальному взаимодействию с сетью ТфОП и внутри пакетной сети, управлению установлением соединения и др.

Softswitch является основным устройством, реализующим функции уровня управления коммутацией и передачей информации. В оборудовании Softswitch должны быть реализованы следующие основные функции:

- функция управления базовым вызовом, обеспечивающая прием и обработку сигнальной информации и реализацию действий по установлению соединения в пакетной сети;
- функция аутентификации и авторизации абонентов, подключаемых в пакетную сеть как непосредственно, так и с использованием оборудования доступа ТфОП;
- функция маршрутизации вызовов в пакетной сети;
- функция тарификации, сбора статистической информации;
- функция управления оборудованием транспортных шлюзов;
- функция предоставления ДВО (дополнительных видов обслуживания). Реализуется в оборудовании Softswitch или совместно с сервером приложений;
- функция OAM&P: эксплуатация, управление (администрирование), техническое обслуживание и предоставление той информации, которая не нужна непосредственно для управления вызовом и может передаваться к системе управления элементами через логически отдельный интерфейс;
- функция менеджмента: обеспечивает взаимодействие с системой менеджмента сети[1].

1.1. Шлюзы (Gateways)

Шлюзы (Gateways) – устройства доступа к сети и сопряжения с существующими сетями. Оборудование *шлюзов* реализует функции по

преобразованию сигнальной информации сетей с коммутацией пакетов в сигнальную информацию пакетных сетей, а также функции по преобразованию информации транспортных каналов в пакеты IP / ячейки ATM и маршрутизации пакетов IP / ячеек ATM. ***Шлюзы*** функционируют на транспортном уровне / уровне доступа.

Для реализации возможности подключения к мультисервисной сети различных видов оборудования ТфОП используются различные программные и аппаратные конфигурации *шлюзового* оборудования:

- ***транспортный шлюз (Media Gateway (MG))*** – реализация функций преобразования речевой информации в пакеты IP / ячейки ATM и маршрутизации пакетов IP / ячеек ATM;
- ***сигнальные шлюзы (Signalling Gateway (SG))*** – реализация функции преобразования систем межстанционной сигнализации сети ОКС7 (квазисвязный режим) в системы сигнализации пакетной сети (SIGTRAN (MxUA));
- ***транкинговый шлюз (Trunking Gateway (TGW))*** – совместная реализация функций MG и SG;
- ***шлюз доступа (Access Gateway (AGW))*** – реализация функции MG и SG для оборудования доступа, подключаемого через интерфейс V5;
- ***резидентный шлюз доступа (Residential Access Gateway (RAGW))*** – реализация функции подключения пользователей, использующих *терминальное оборудование* ТфОП/ЦСИС к мультисервисной сети.

Оборудование *транспортного шлюза* должно выполнять функции устройства, производящего обработку информационных потоков среды передачи.

Оборудование *транспортного шлюза* должно реализовывать следующий перечень обязательных функций:

- функцию адресации: обеспечивает присвоение адресов транспортировки IP для средства приема и передачи;
- функцию транспортировки: обеспечивает согласованную транспортировку потоков среды передачи между доменом IP и доменом сети с коммутацией каналов, включая, например, выполнение процедур преобразования кодировок и эхокомпенсации;
- функцию трансляции кодека: маршрутизирует информационные транспортные потоки между доменом IP и доменом сети с коммутацией каналов;
- функцию обеспечения секретности канала среды передачи: гарантирует секретность транспортировки информации в направлении к *шлюзу* и от *шлюза*;
- функцию транспортного окончания сети с коммутацией каналов: включает реализацию процедур всех низкоуровневых аппаратных средств и протоколов сети;
- функцию транспортного окончания сети пакетной коммутации: включает реализацию процедур всех протоколов, задействованных в

распределении транспортных ресурсов, на сети пакетной коммутации, в том числе процедуры использования кодеков;

- функцию обработки транспортного потока с пакетной коммутацией / коммутацией каналов: обеспечивает преобразование между каналом передачи аудиоинформации, каналом передачи факсимильной информации или каналом передачи данных на стороне сети с коммутацией каналов и пакетами данных (например RTP/UDP/IP или ATM) на стороне сети пакетной коммутации;
- функцию предоставления канала для услуги: обеспечивает такие услуги, как передача уведомлений и тональных сигналов в направлении к сети с коммутацией каналов или к сети пакетной коммутации;
- функцию регистрации использования: определяет и/или регистрирует информацию о сигнализации и/или информацию о приеме или передаче сообщений, передаваемых в транспортных потоках;
- функцию информирования об использовании: сообщает внешнему объекту о текущем и/или зарегистрированном использовании (ресурсов);
- функцию OAM&P: эксплуатация, управление (администрирование), техническое обслуживание и предоставление той информации, которая не нужна непосредственно для управления вызовом и может передаваться к системе управления элементами через логически отдельный интерфейс;
- функцию менеджмента: обеспечивает взаимодействие с системой менеджмента сети.

Оборудование *сигнального шлюза* должно выполнять функции посредника при сигнализации между пакетной сетью и сетью с коммутацией каналов.

Оборудование *сигнального шлюза* сигнализации должно реализовывать следующий перечень обязательных функций:

- функцию окончания протоколов уровня, располагающегося ниже уровня протокола управления вызовом сети с коммутацией каналов;
- функцию секретности сигнальных сообщений: обеспечивает секретность сигнальных сообщений в направлении к *шлюзу* и от *шлюза*;
- функцию OAM&P: эксплуатация, управление (администрирование), техническое обслуживание и предоставление той информации, которая не нужна непосредственно для управления вызовом и может передаваться к системе управления элементами через логически отдельный интерфейс;
- функцию менеджмента: обеспечивает взаимодействие с системой менеджмента сети.

Терминальное оборудование

- ***Терминальное оборудование*** – терминальные устройства,

используемые для предоставления голосовых и мультимедийных услуг связи и предназначенные для работы в пакетных сетях.

- Существует два основных типа терминальных устройств, предназначенных для работы в пакетных сетях: SIP-терминалы и H.323-терминалы. Данное оборудование может иметь как специализированное аппаратное (standalone), так и программное исполнение (softphone).
- Также иногда используется *терминальное оборудование* на основе протокола MEGACO. Такое *терминальное оборудование* совмещает в себе функции аналогового телефонного аппарата и *шлюза доступа* в части преобразования сигнализации по аналоговым абонентским линиям. Его функциональные возможности ограничиваются возможностями аналогового аппарата, но оно может непосредственно подключаться к пакетной сети.
- Еще одним видом терминального оборудования являются интегрированные устройства доступа (IAD). Как правило, IAD обеспечивает подключение *терминального оборудования* сетей ТфОП (аналоговые ТА и терминалы ISDN) и терминального оборудования сетей передачи данных. В IAD реализуются функции по преобразованию протоколов сигнализации ТфОП в протоколы пакетных сетей (SIP/H.323) и преобразованию потоков пользовательской информации между сетями с коммутацией каналов и пакетными сетями. Ближайшая аналогия с IAD в сетях ТфОП — оборудование малых УПАТС.
- *Терминальное оборудование* поддерживает протоколы SIP или H.323 в направлении *Softswitch* для передачи информации сигнализации и управления коммутацией и протоколы RTP/RTCP для передачи пользовательской информации. Для подключения к сети, как правило, применяется Ethernet-интерфейс.

2-Практическая занятия

Тема: Структура протокола SIP применяющие при организации IP телефония

1. Теоретическая часть

Архитектура сети SIP

Протокол SIP работает по схеме клиент-сервер. Клиент выдает запросы, в которых указывает, что он желает получить от сервера. Сервер принимает запрос, обрабатывает его и выдает ответ, который может содержать уведомление об успешном выполнении запроса, уведомление об

ошибке или информацию, затребованную клиентом.

Рис.2.1. Схема "клиент-сервер"

Протоколом SIP предусмотрены 3 основных сценария установления соединения: с участием прокси-сервера, с участием сервера переадресации, и непосредственно между пользователями. Различие между перечисленными сценариями заключается в том, что по-разному осуществляется поиск и приглашение вызываемого пользователя. В первом случае эти функции возлагает на себя прокси-сервер, а вызывающему пользователю необходимо знать только постоянный SIP-адрес вызываемого пользователя. Во втором случае вызывающая сторона самостоятельно устанавливает соединение, а сервер переадресации лишь реализует преобразование постоянного адреса вызываемого абонента в его текущий адрес. И, наконец, в третьем случае вызывающему пользователю для установления соединения необходимо знать текущий адрес вызываемого пользователя[3].

Таким образом сеть SIP содержит основные элементы трех видов: агенты пользователя, прокси-серверы и серверы переадресации.

Агенты пользователя (User Agent или SIP client) являются приложениями терминального оборудования и включают в себя две составляющие: агент пользователя - клиент (User Agent Client - UAC) и агент пользователя - сервер (User Agent Server - UAS), иначе известные как клиент и сервер соответственно. Клиент UAC инициирует SIP-запросы, т.е. выступает в качестве вызывающей стороны. Сервер UAS принимает запросы и возвращает ответы, т.е. выступает в качестве вызываемой стороны.

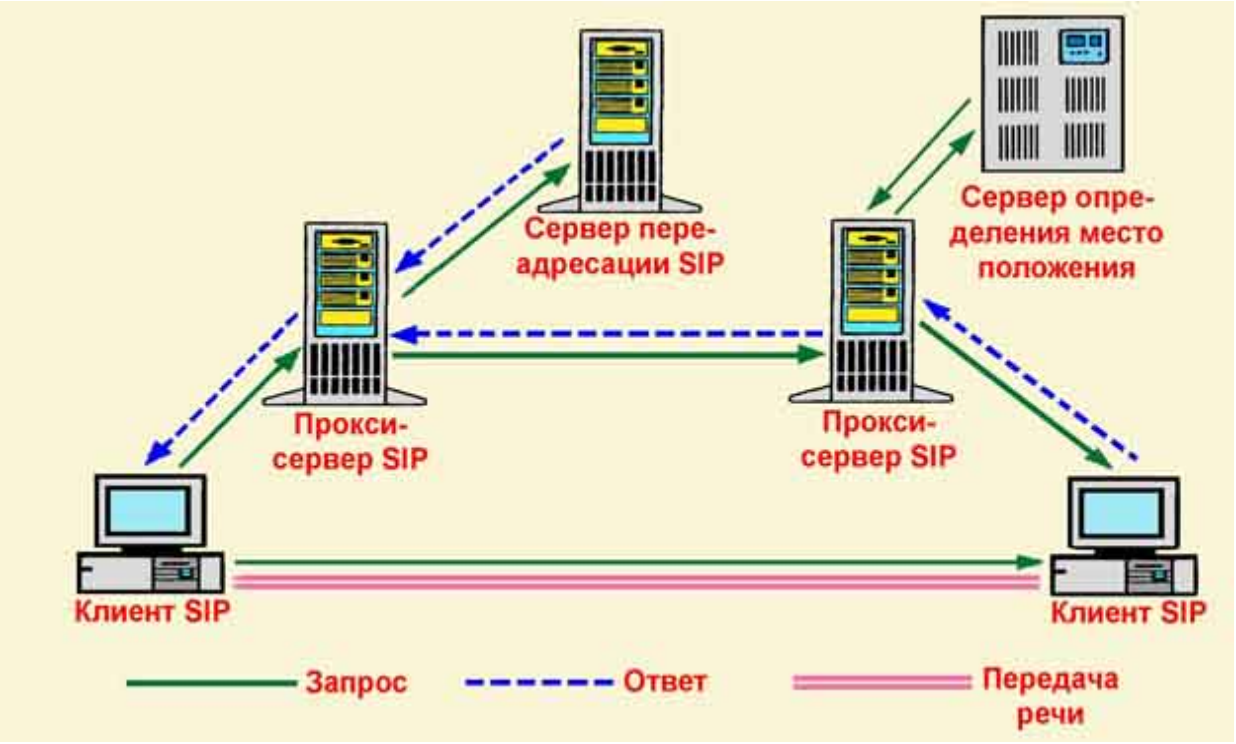


Рис.2.2. Архитектура SIP сети

Следует особо отметить, что сервер UAS и клиент UAC могут (но не обязаны) непосредственно взаимодействовать с пользователем, а другие клиенты и серверы SIP этого делать не могут. Если в устройстве присутствуют и сервер UAS, и клиент UAC, то оно называется агентом пользователя - User Agent (UA), а по своей сути представляет собой терминальное оборудование SIP.

Кроме терминалов определены два основных типа сетевых элементов SIP: прокси-сервер (proxy server) и сервер переадресации (redirect server).

Прокси-сервер (от английского proxy - представитель) представляет интересы пользователя в сети. Он принимает запросы, обрабатывает их и, в зависимости от типа запроса, выполняет определенные действия. Это может быть поиск и вызов пользователя, маршрутизация запроса, предоставление услуг и т.д. Прокси-сервер состоит из клиентской и серверной частей, поэтому может принимать вызовы, инициировать собственные запросы и возвращать ответы. Ответные сообщения следуют по тому же пути обратно к прокси-серверу, а не к клиенту.

Прокси - сервер может быть физически совмещен с сервером определения местоположения (в этом случае он называется registrar) или существовать отдельно от этого сервера, но иметь возможность взаимодействовать с ним.

Предусмотрено режима работы прокси-серверов - с сохранением состояний (stateful) и без сохранения состояний (stateless).

Сервер первого типа хранит в памяти входящий запрос, который явился причиной генерации одного или нескольких исходящих запросов. Эти исходящие запросы сервер также запоминает. Все запросы хранятся в памяти

сервера только до окончания транзакции, т.е. до получения ответов на запросы.

Сервер первого типа позволяет предоставить большее количество услуг, но работает медленнее, чем сервер второго типа.

Сервер без сохранения состояний просто ретранслирует запросы и ответы, которые получает. Он работает быстрее, чем сервер первого типа, так как ресурс процессора не тратится на запоминание состояний, вследствие чего сервер этого типа может обслужить большее количество пользователей. Недостатком такого сервера является то, что на его базе можно реализовать лишь наиболее простые услуги. Впрочем, прокси-сервер может функционировать как сервер с сохранением состояний для одних пользователей и как сервер без сохранения состояний - для других.

Сервер переадресации предназначен для определения текущего адреса вызываемого пользователя. Вызывающий пользователь передает к серверу сообщение с известным ему адресом вызываемого пользователя, а сервер обеспечивает переадресацию вызова на текущий адрес этого пользователя. Для реализации этой функции сервер переадресации должен взаимодействовать с сервером определения местоположения.

Сервер переадресации не терминирует вызовы как сервер RAS и не инициирует собственные запросы как прокси-сервер. Он только сообщает адрес либо вызываемого пользователя, либо прокси-сервера. По этому адресу инициатор запроса передает новый запрос. Сервер переадресации не содержит клиентскую часть программного обеспечения.

Но пользователю не обязательно связываться с каким-либо SIP-сервером. Он может сам вызвать другого пользователя при условии, что знает его текущий адрес.

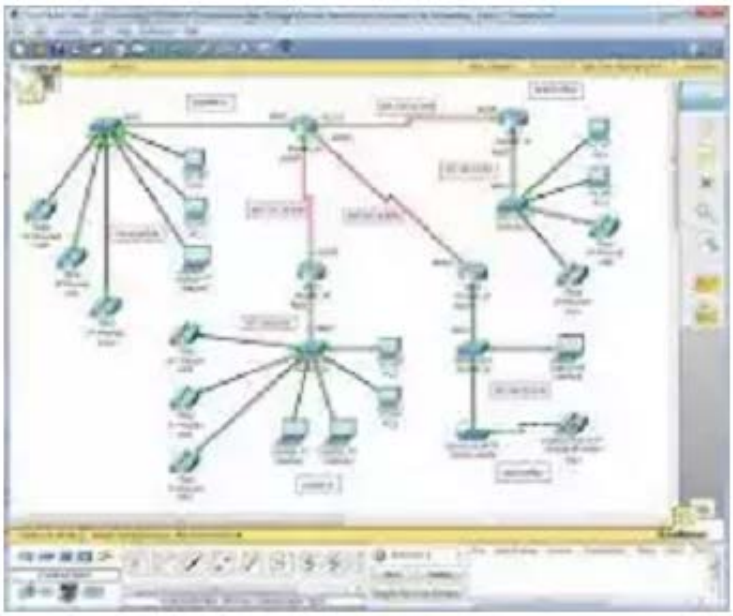
Сервер определения местоположения пользователей. Пользователь может перемещаться в пределах сети, поэтому необходим механизм определения его местоположения в текущий момент времени. Например, сотрудник предприятия уезжает в командировку, и все вызовы, адресованные ему, должны быть направлены в другой город на его временное место работы. О том, где он находится, пользователь информирует специальный сервер с помощью сообщения REGISTER.

Для хранения текущего адреса пользователя служит сервер определения местоположения пользователей, представляющий собой базу данных адресной информации. Кроме постоянного адреса пользователя, в этой базе данных может храниться один или несколько текущих адресов.

3-Практическая занятия

Тема: Постройка локалных сетей при помощью ПО Cisco Packet Tracer

Как настроить локальную сеть между двумя компьютерами



Cisco packet tracer -1 урок. Как настроить локальную сеть между двумя компьютерами-01. Всем привет сегодня хочу начать небольшой цикл статей посвященный работе с эмулятором сети Cisco packet tracer.

В первом уроке мы разберем как настроить локальную сеть между двумя компьютерами. Для начала нашего обучения нужно скачать Скачать Cisco packet tracer 6.2. Напомню, что с помощью него можно эмулировать работу реальных устройств таких как коммутаторы и компьютеры, и рисовать простые или сложные локальные сети. Далее вам нужно посмотреть Как установить Cisco Packet Tracer.

И так после установки сформулируем задачу, настроим сеть между двумя компьютерами на прямую. Открываем Cisco packet tracer и слева выбираем End Devices и перетаскиваем на верх двакомпьютера Generic

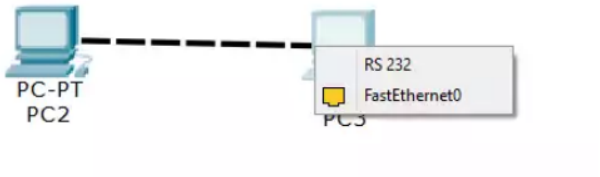
Как настроить локальную сеть в Cisco packet tracert-01 В итоге получаем вот такую картину

Как настроить локальную сеть в Cisco packet tracert-02 Далее нам нужно соединить два компьютера патч кордом. Для этого выбираем Connections и перекрестный кабель.

Как настроить локальную сеть в Cisco packet tracert-03

Щелкаем теперь по первому компьютеру и подключаем патч корд к FastEthernet0

Как настроить локальную сеть в Cisco packet tracert-04
Перетаскиваем связь на второй компьютер и выбираем тоже FastEthernet0

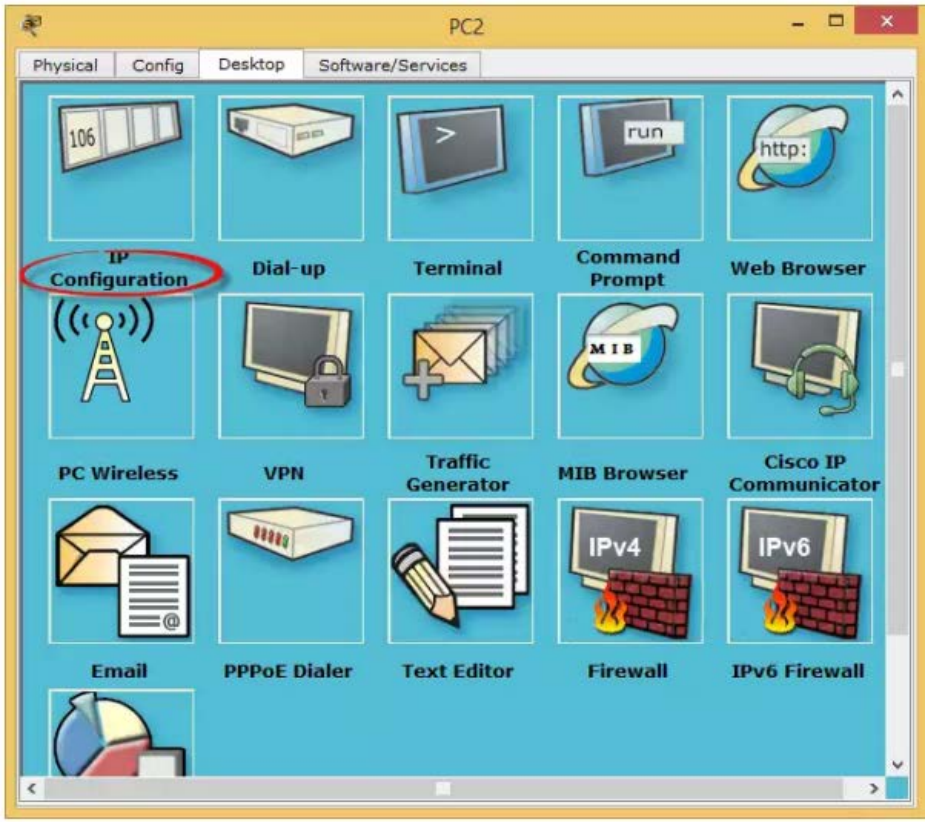


Как настроить локальную сеть в Cisco packet tracert-05

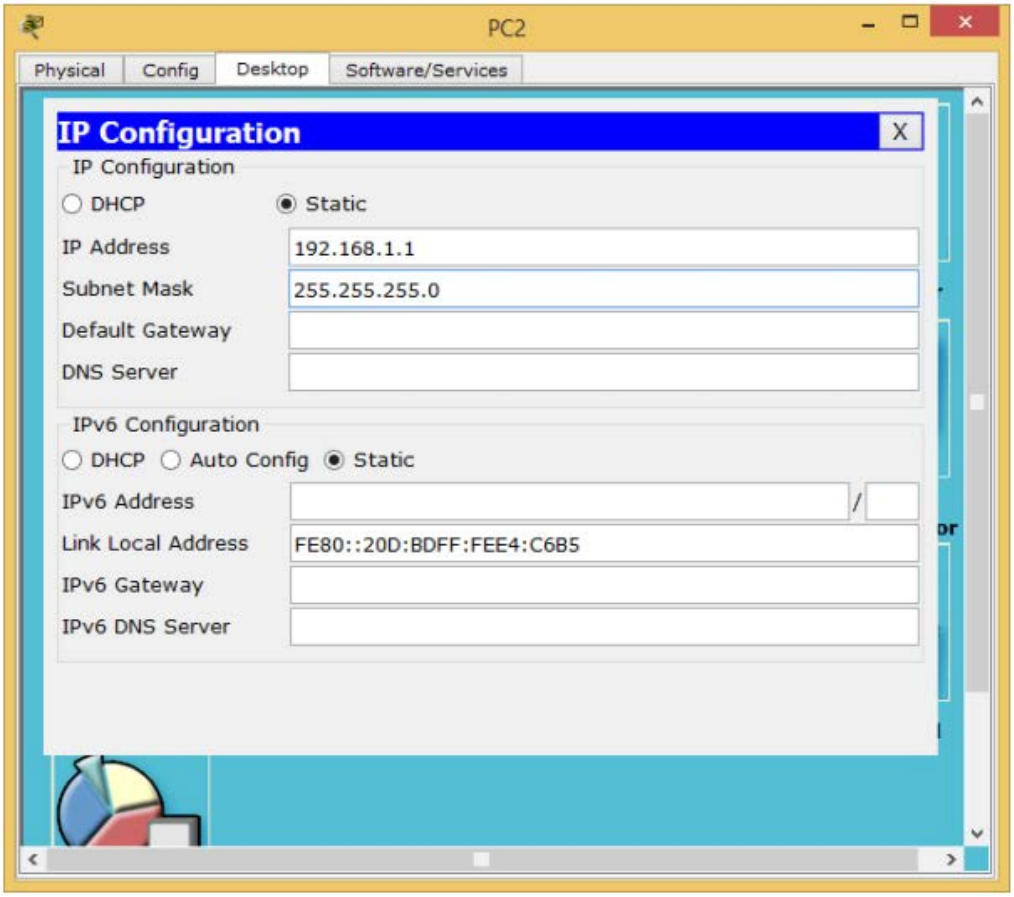
В итоге вы видите что локальная сеть между компьютерами заработала и загорелись зеленые лампочки

Как настроить локальную сеть в Cisco packet tracert-06

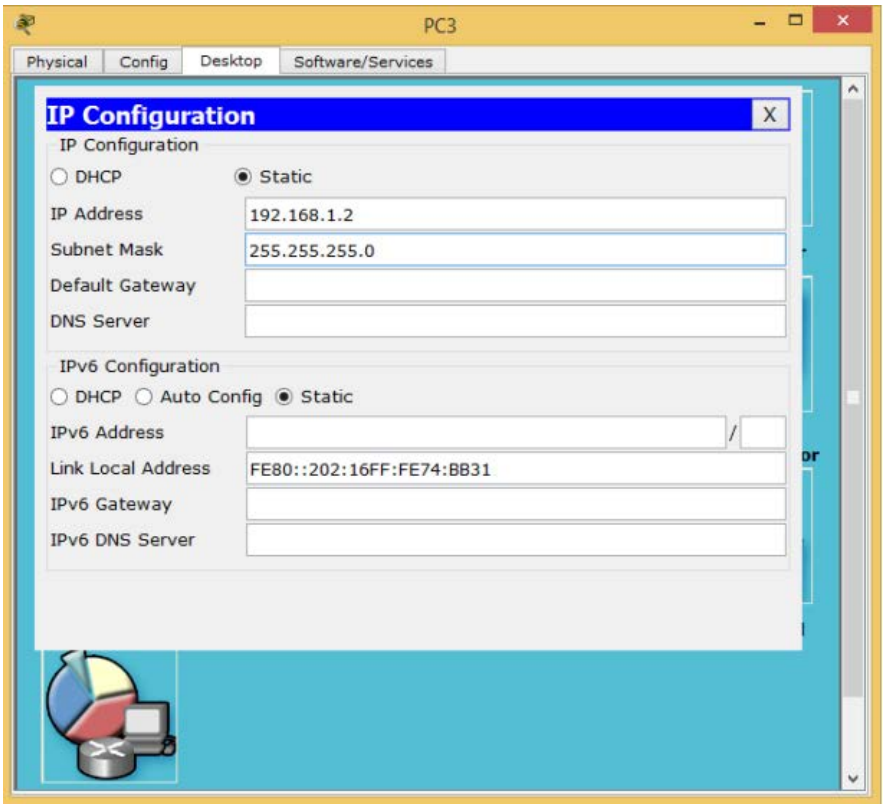
Теперь нужно настроить статический ip адрес у компьютера, для этого щелкаем по первому двойным кликом и переходим в меню Desktop и выбираем IP Configuration



Как настроить локальную сеть в Cisco packet tracert-07. Задаем ip адрес и маску, у меня это будет ip адрес 192.168.1.1

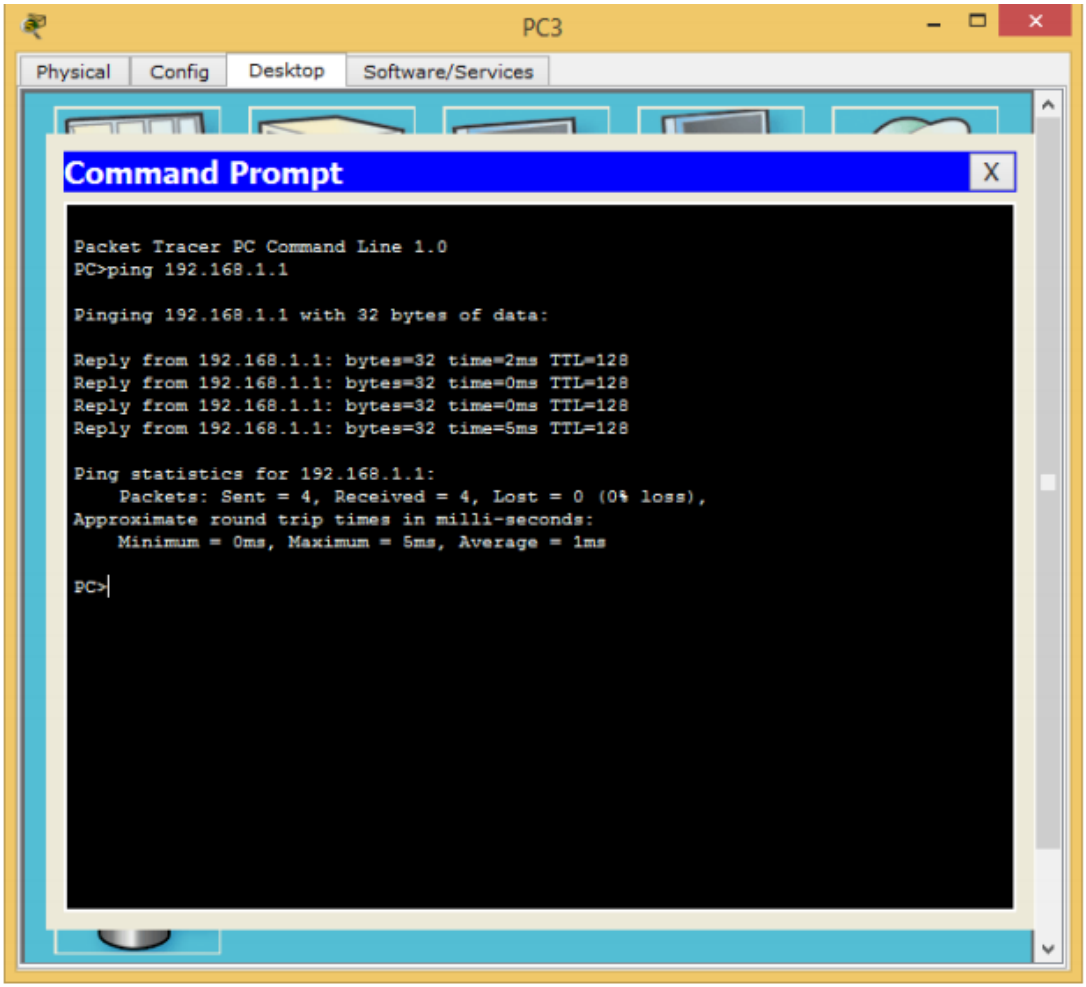


Как настроить локальную сеть в Cisco packet tracert-08. На втором делаем тоже самое но задаем ip адрес 192.168.1.2



Как настроить локальную сеть в Cisco packet tracert-09. Теперь на втором компьютере выбираем Command Promt

Как настроить локальную сеть в Cisco packet tracert-10. Откроется командная строка где пишем Ping 192.168.1.1, и видим что связь есть



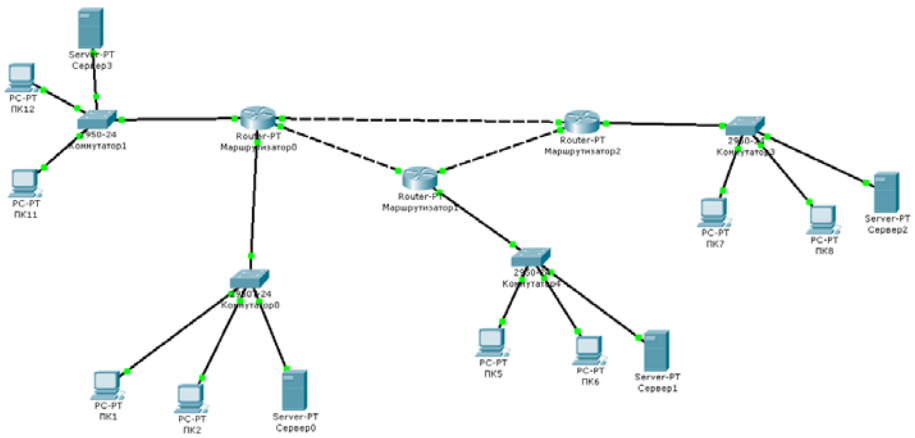
Как настроить локальную сеть в Cisco packet tracert-12. Вот так вот просто настроить простейшую локальную сеть между двумя компьютерами

4-Практическая занятия

Тема:Настройка DHCP при организации широкополосных сетей.

Практическая работа «Настройка DHCP адресации и OSPF маршрутизации в Cisco Packet Tracer».

Часть №1. Настройка DHCP в простой сети. Топология сети:

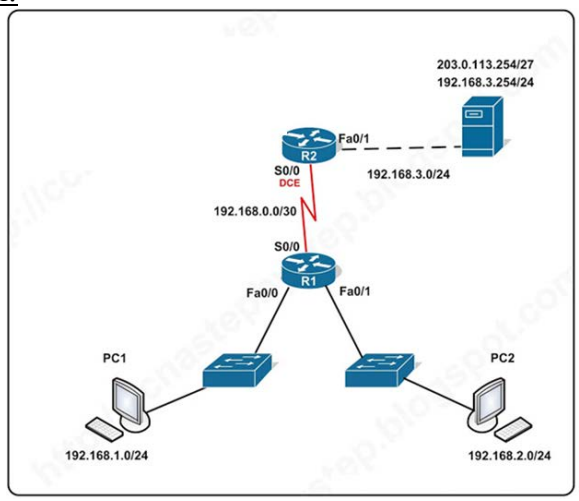


Постановка задачи:
Имеются 4 сети филиалов и 3 опорных сети (между маршрутизаторами).
Организовать в опорных сетях статическую адресацию, а в сетях филиалов (на рисунке – это сети с коммутаторами) – адресацию по DHCP. В каждой из сетей филиалов имеется свой DHCP сервер. Адресация во всех сетях различная.
Между сетями обеспечить маршрутизацию по OSPF.
Подсказка:

1) Перевести роутер в режим OSPF (router ospf 1)
2) Указать соседние сети (network адрес-сети обратная-маска area 1).

Предоставить отчёт, в котором необходимо описать выполнение каждого задания.

Задача №2.
Постановка задачи:
Необходимо настроить сеть из двух роутеров, связанных друг с другом.
Связать роутеры любым способом.
Имеется сеть между роутерами и есть две других сети организации.
У вас имеется только один DHCP-сервер.
Необходимо настроить раздачу адресов DHCP для двух сетей организации.
Используемая топология:



План адресации:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0	192.168.0.1	255.255.255.252	N/A
	Fa0/0	192.168.1.1	255.255.255.0	N/A
	Fa0/1	192.168.2.1	255.255.255.0	N/A
R2	S0/0	192.168.0.2	255.255.255.252	N/A
	S0/1	203.0.113.225	255.255.255.252	N/A
	Fa0/0	192.168.3.1	255.255.255.0	N/A
PC1		192.168.1.11	255.255.255.0	192.168.1.1
PC2		192.168.2.11	255.255.255.0	192.168.2.1
Server		192.168.3.254	255.255.255.0	192.168.3.1

1. Базовая конфигурация оборудования

- Настроить hostname на маршрутизаторах.
- Установить пароль на маршрутизатор.

2. Настроить адресацию оборудования согласно плана

- Проверить выполненные настройки командой show ip interface brief
- Настроить интерфейс Server в соответствии с таблицей
- Проверить выполненные настройки командой ping.
- Настроить интерфейсы PC1 и PC2 на автоматическое конфигурирование.
- Сконфигурировать протокол динамической маршрутизации OSPF на R1 и R2. Не включать сеть 203.0.113.224/27 в анонсы протокола OSPF.
- Добавить на R2 маршрут по умолчанию и настроить перераспределение в среду OSPF
- Проверить правильность выполненных настроек командой show ip route.

3. Настроить DHCP Server на R2
Настроить диапазоны исключаемых адресов
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
R2(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10

Создать пул адресов для сети 192.168.1.0/24, подключенной к R1.
Шлюз по умолчанию 192.168.1.1, DNS сервер 192.168.3.254

R2(config)#ip dhcp pool R1-pool-1.0
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#dns-server 192.168.3.254
R2(dhcp-config)#default-router 192.168.1.1

Создать пул адресов для сети 192.168.2.0/24, подключенной к R1.
Шлюз по умолчанию 192.168.2.1, DNS сервер 192.168.3.254

R2(config)#ip dhcp pool R1-pool-2.0
R2(dhcp-config)#network 192.168.2.0 255.255.255.0
R2(dhcp-config)#dns-server 192.168.3.254
R2(dhcp-config)#default-router 192.168.2.1

4. Настроить DHCP Relay на R1
Индивидуально для каждого интерфейса необходимо указать параметр ip helper-address
ip helper-address x.x.x.x заставляет пересылать широковещательные UDP сообщения различных протоколов.

R1(config)#interface fa0/0
R1(config-if)#ip helper-address 192.168.0.2
R1(config)#interface fa0/1
R1(config-if)#ip helper-address 192.168.0.2

Исключение IP-адресов
Исключить из пула адрес интерфейса маршрутизатора и DNS-сервера:
Router(config)# ip dhcp excluded-address 192.168.20.1
Router(config)# ip dhcp excluded-address 192.168.20.101

Ручное резервирование IP-адресов
Сопоставить определенный MAC-адрес с необходимым IP-адресом.
Router(config)# ip dhcp pool Test
Router(config-pool)#host 192.168.2.4 255.255.255.0
Router(config-pool)#client-identifier 0100.0476.106c.bc

Router(config-pool)#client-name Test

Т.е. необходимо указать:
адрес, который будет сопоставлен с физическим адресом: host address [mask | prefix-length]
физический адрес (идентификатор) сетевой карты: client-identifier unique-identifier
имя клиента: client-name name

Для microsoft сетей идентификатором данной сети является 01 ПЕРЕД MAC-адресом. Для UNIX сетей необходимо проставлять 00

То есть, для компьютера с MAC-адресом 00.04.76.10.6c.bc, который работает в среде Windows строчка client-identifier будет выглядеть как:
Router(config-pool)#client-identifier 0100.0476.106c.bc

Выполнить очистку таблицы соответствия динамически выданных адресов
Router#clear ip dhcp binding
Вывести таблицу соответствия DHCP -адресов после выполнения данной команды.

После выполнения заданий:

1) Просмотрите информацию об адресах, которые были выданы DHCP-сервером (show ip dhcp binding).
2) По указанному IP-адресу определите, использовался ли он при работе системы DHCP (show ip dhcp binding 10.84.130.42)
3) Выведите статистику
4) show ip dhcp server statistics

Предоставить отчёт, в котором необходимо описать выполнение каждого задания.

5-Практическая занятия

Тема:Создания новых пользова-телей в серевере Elastix SIP и настройка номера в IP телефонах.

1. Теоретическая сачть

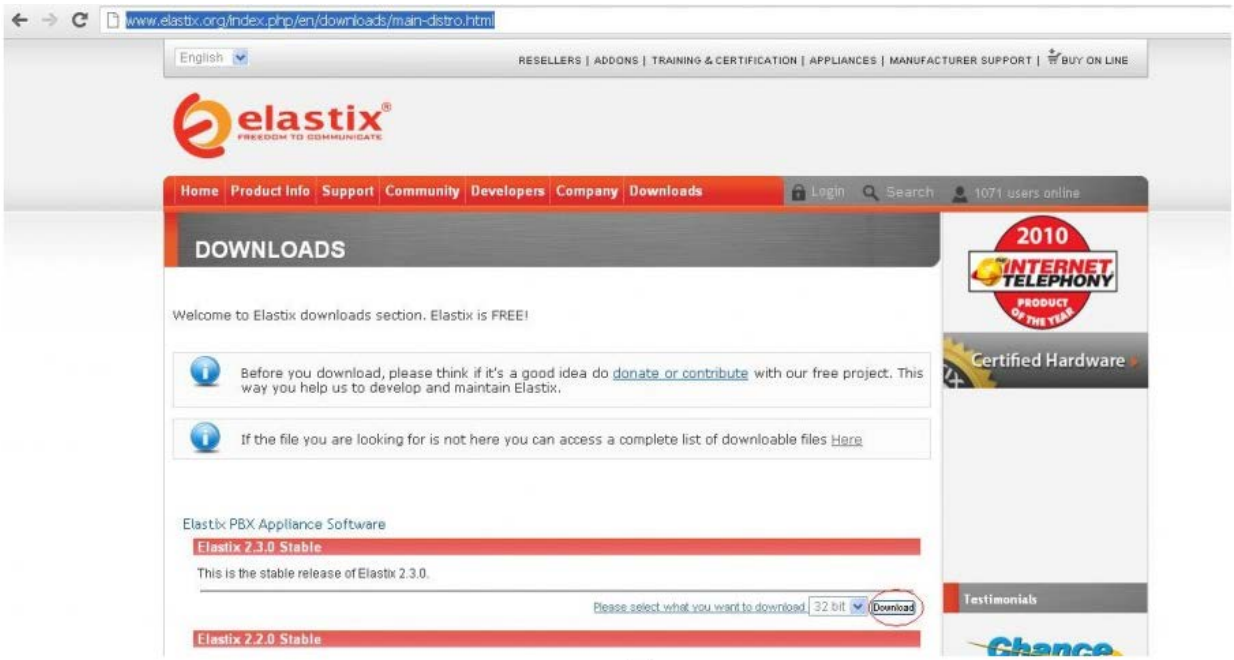
IP PBX Elastix http://www.elastix.org , пожалуй, один из самых удобных дистрибутивов для первоначального знакомства с системами , построеных на базе Asterisk, так как :

1) Установка и настройка не требует специальных знаний в области *nix систем.
2) Дистрибутив содержит все, что только можно себе представить , начиная от собственно Астериска и заканчивая факс- сервером , XMPP сервером , CRM системой и многое другое.

3) 99 процентов функционала можно сконфигурировать из WEB интерфейса, их там аж 2 штуки, собственно сам Elastix и FreePBX.Они похожи , правда, как близнецы братья, но тем неменее[5].

4)Время на установку и конфигурирование стандартных конфигураций, при наличии минимального опыта и знаний - 2-3 часа. Итак , часть №1 - базовая установка.

1. Идем по ссылке http://www.elastix.org/index.php/en/downloads/main-distro.html, скачиваем образ диска , на момент написания статьи предлагалась версия Elastix 2.3.0.Не забывайте, что для 32-х и 64-х битных систем идут разные дистрибутивы,выбираем нужный, жмем "Download":

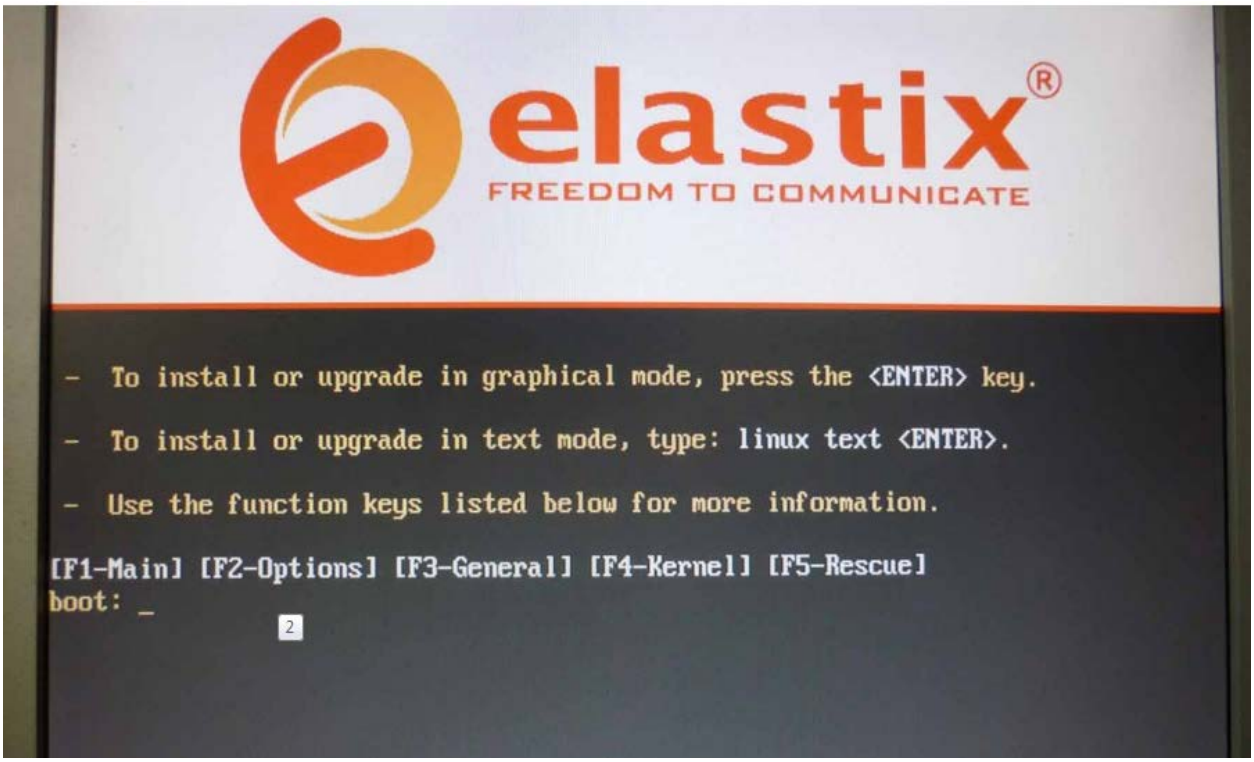


1

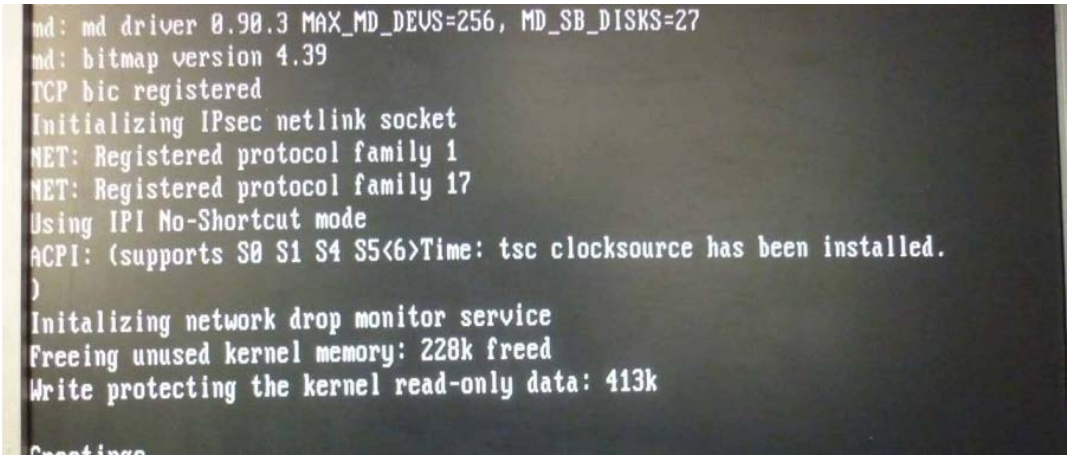
2. После того , как образ скачался нарезаем CD-R с дистрибутивом, например при помощи программы "Nero".

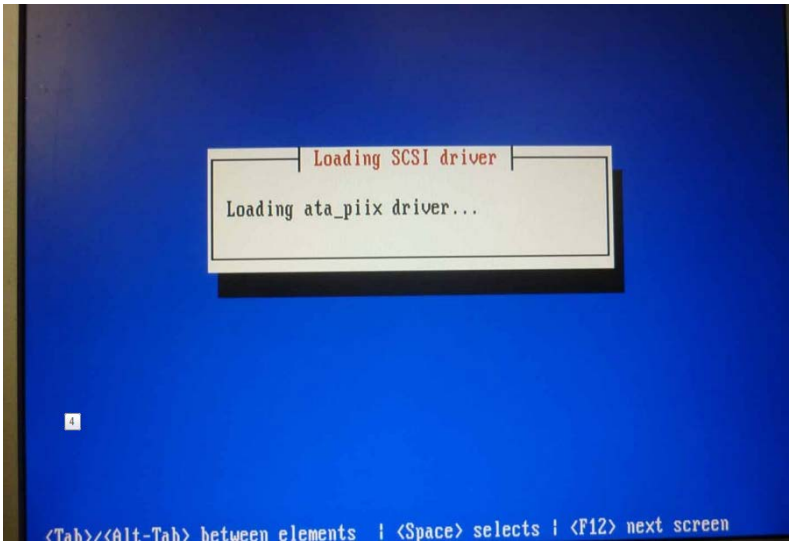
3. Устанавливаем диск в привод, не забывая включить в BIOS загрузку с CDROM.

4. После появления экрана с приглашением начать установку нажимаем "ENTER":

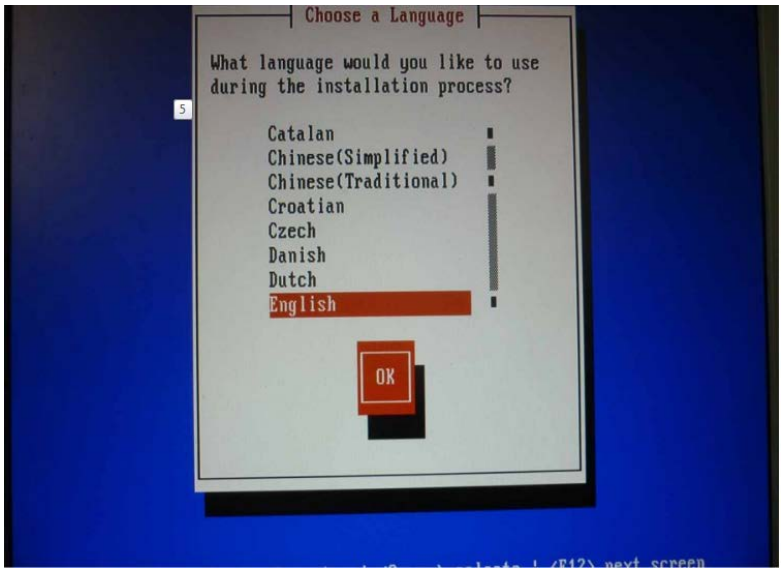


5. Установка началась:

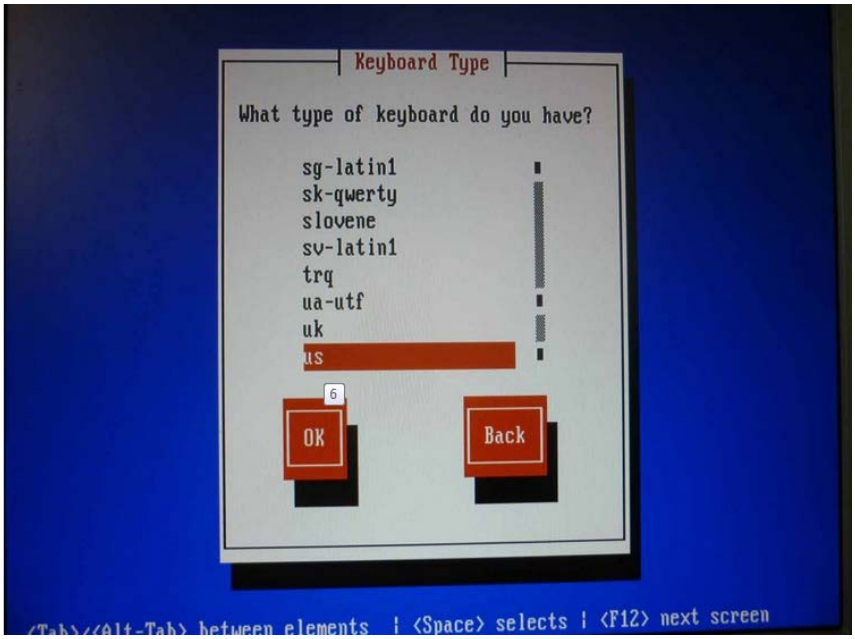




7.Выбираем английский язык.Перемешение по меню осуществляется клавишами - "вверх" , "вниз","TAB".Нажимаем "OK" :



8.Выбираем раскладку клавиатуры "US", нажимаем "OK":



6-Практическая занятия

Тема:Управление данные пользо-вателья в серевере Elastix SIP

7-Практическая занятия

Тема: Настройка номера аналоговых телефонов в IAD концентраторе.

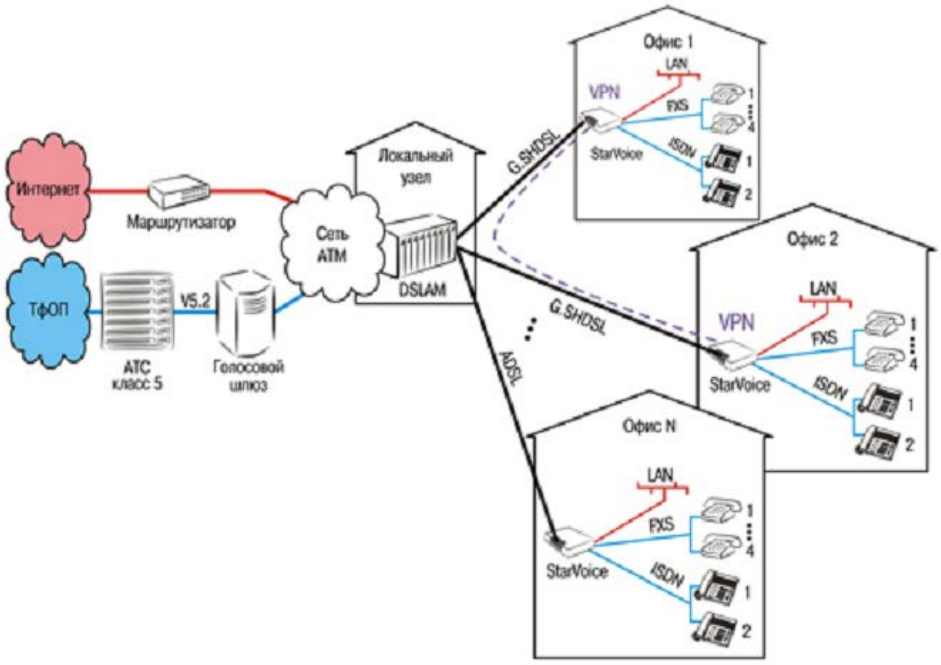
Семейство Starvoice включает устройства интегрированного доступа (IAD), разработанные для приложений малого и среднего бизнеса. IAD

Starvoice обеспечивают передачу по одной медной паре данных (Ethernet) и 2-4 голосовых каналов (FXS и/или ISDN) с применением технологии ADSL (серия SV10xx) или G. SHDSL (серия SV20xx). Разнообразие моделей IAD позволяет оператору предоставить абоненту требуемые услуги по минимальной цене.

Рис.6.1.Устройство IAD

Модель	Технология доступа	Eth 10/100	POTS	BRI
SV1004	ADSL	1	0	4
SV1040	ADSL	1	4	0
SV1042	ADSL	1	4	2
SV2004	SHDSL	1	0	4
SV2040	SHDSL	1	4	0
SV2042	SHDSL	1	4	2

IAD, устройства интегрированного доступа ADSL и SHDSL (Aethra)



Интерфейсы:

- ADSL или SHDSL технологии
- Аналоговые порты POTS (0 или 4 RJ-11)
- ISDN-BRI порты (0, 2 или 4)
- Ethernet 10/100BaseT (RJ-45)
- Консольный порт RS232 (все модели)

ATM

- до 10 VCC
- Настраиваемые конфигурации CBR, VBR-rt и UBR
- Уровни адаптации ATM: AAL-2 и AAL-5

Сетевые интерфейсы

- ShDSL: ETSI TS 101 524, ITU G.991.2 скорость линии до 2304 кбит/с (от 3до 36 DS0 каналов)
- ADSL: ITU-T G.992.1 (g.dmt), ITU-T G.992.2 (g.lite) Скорость по направлению к абоненту 8192 кбит/
- с, от абонента 832 кбит/с

Функции моста и маршрутизатора

- IP-маршрутизация с поддержкой RIP1, RIP2
- Статическая маршрутизация
- Поддержка функции прозрачного моста
- Поддержка Spanning Tree алгоритма

Сервисные возможности

- Улучшенный NAPT с шлюзами (H.323, ICMP, passive FTP, GRE,IPSec, и т.д.)
- DHCP сервер, DNS сервер
- VPN (PPTP сервер/клиент, GREinIP, IPinIP)

Протоколы доступа

- IP over AAL-5, Ethernet over AAL-5 (RFC2684)
- PPPoA (RFC2364) и PPPoE (RFC2516)
- LLC/SNAP и VC инкапсуляция

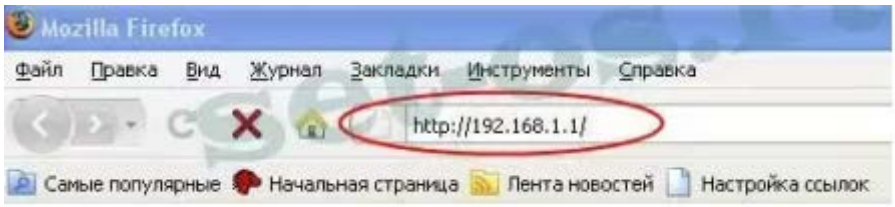
8-Практическая занятия

Тема: Настройка Home Gateway (модем) через Web-интерфейс для WiFi.

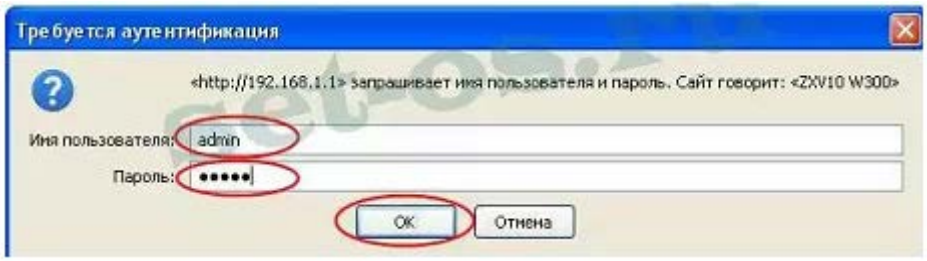
Настройка Wi-Fi На ZTE ZXV10 W300

Инструкция по настройке Wi-Fi на ZTE ZXV10 W300

Для настройки Wi-Fi на роутере ZTE ZXV10 W300, надо сначала подключится к нему через сетевой шнур. 1. Запускаем браузер и заходим в веб-интерфейс роутера по адресу http://192.168.1.1 (IP-адрес роутера 192.168.1.1). Если веб-интерфейс недоступен, смотрите статью Как зайти в настройки роутера.

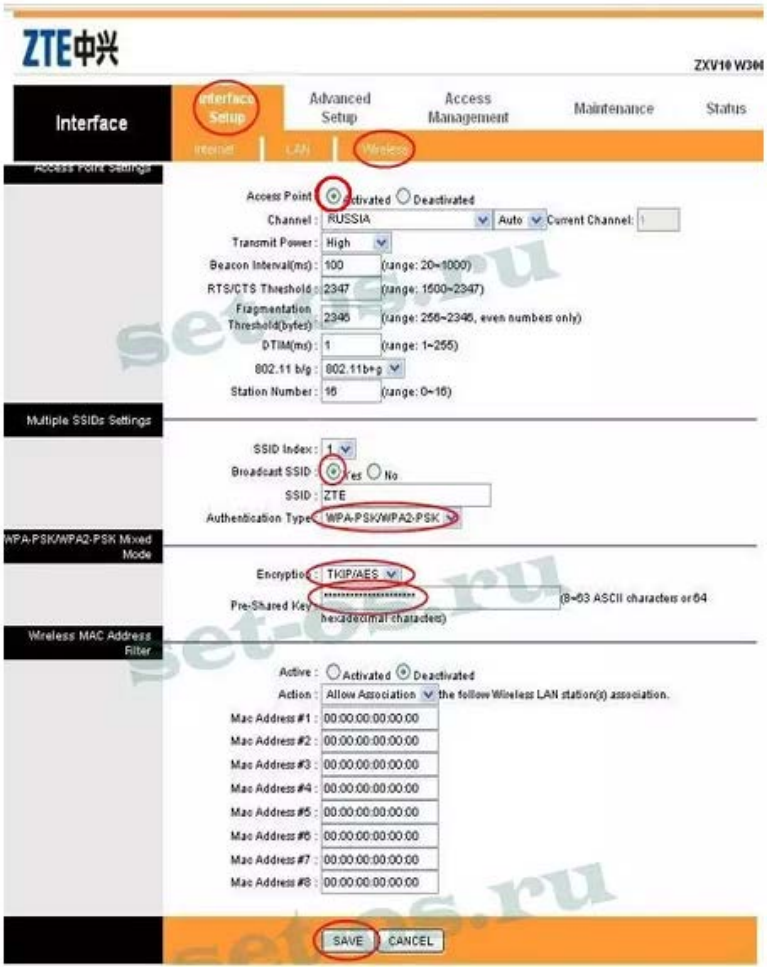


Если роутер доступен, Вы увидите запрос авторизации:



Стандартный логин на доступ в интерфейс ZTE ZXV10 W300 — admin. Пароль поумолчанию — admin. Нажимаем ОК.

2. Попав в веб-интерфейс настройки роутера, переходим в раздел Interface Setup >>> Wireless:



3. Настраиваем следующие параметры настройки беспроводной сети Wi-Fi:
Access Point — Activated;
Authentication Type — WPA-PSK/WPA2-PSK mixed;
Encryption — TKIP/AES;

В поле Pre-Shared Key надо прописать пароль на сеть Wi-Fi. Это может быть любая последовательность символов, но не менее 8 знаков.

4. Нажимаем кнопку Save. Настройка Wi-Fi на ZTE ZXV10 W300 завершена, можно работать.

9-Практическая занятия

Тема: Управление данные пользо-вателья D-Link DES 3200-18 коммутаторе.

1. Теоретическая часть

Cisco D-link DES-3200-18

DES-3200 коммутаторлари D-Link нинг OSI моделининг иккинчи поғонасида ишловчи бошқариладиган коммутаторлари қаторига киради ва бундай коммутаторлар Metro Ethernet (ETTX ва FTTX) ва корпоратив тармоқларида қўллашга мўлжалланган.

Бундай сериядаги коммутаторлар 8/16/24/48 тагача бўлган 10/100 Мбит/с тезликли Fast Ethernet, шунингдек 1/2/4 гача бўлган комбопорт Gigabit Ethernet/SFP портларига эга.

DES-3200-10/18 коммутаторлари столга жойлашувчи, шунингдек телекоммуникация ва тарқатиш шкафларига ўрнатиш учун мўлжалланган версиялари ҳам мавжуд.

DES-3200-26,28,28/ME,28F,52 коммутаторлари мис ёки оптик кабеллар ёрдамида (24/48 портлар) 100 Мбит/с тезликда маълумот узатишни таъминлайди.

Мазкур сериядаги барча коммутаторлар 1, 2 ёки 4 тагача комбо-порт Gigabit Ethernet/SFP ларга эгалар ва бу портлар орқали 4 Гбит/с гача ўтказиш қобилиятини таъминлаш мумкин ва бу мазкур коммутаторлар ёрдамида халқали тармоқ қуриш имкониятини беради.

DES-3200-28P/52P коммутаторлари PoE стандартини қўллаб қувватлайди (электр таъминотни Ethernet-кабели орқали) ва IEEE 802.3af ва IEEE 802.3at стандартлари 15,4 Вт ва 30 Вт гача қувватни таъминлайди.

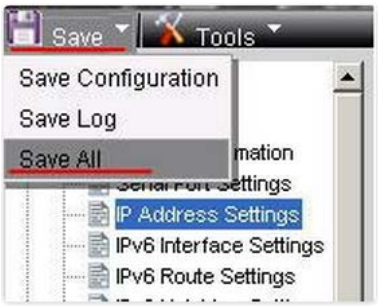
Настройка Cisco D-link DES-3200-18

В качестве примера для базовой настройки рассмотрим модификацию DES-3200-10, имеющую 8 медных 10/100 портов RG-45 и 2 комбинированных 1000BASE-T/SFP порта. Адрес Web-интерфейса коммутатора — http://10.90.90.90, соответственно для того чтобы попасть на него — Вам необходимо прописать на сетевой плате IP-адрес из той же подсети что и сам свитч — например: 10.90.90.91.

По умолчанию на коммутаторе нет пользователя и пароля на доступ к интерфейсу настройки, поэтому в окне запроса логина и пароля не пишем ничего а просто нажимаем OK. Самый первый шаг который следует сделать — настроить доступ к управлению свитчем для этого прописываем IP-адрес коммутатора из своей сети. Для этого идём в раздел «Configuration» пункт «IP Address Settings»:

Если после настройки управления устройство недоступно в сети по управляющему Vlan'у (хотя прописано всё верно) либо после непродолжительного времени сбрасывает настройки управления — обновите прошивку коммутатора с официального сервера. Четвертый шаг — настроим доступ к настройке DES-3200 через авторизацию. Для этого переходим в раздел «Configuraton» -> «User Accounts»:

Создаем нового пользователя с полными правами Администратора — для этого в поле «User Name» вводим имя — например admin, права «Access Rights» — Admin и дважды вводим пароль в поля «Password» и «Commit Password». Нажимаем «Apply». В качестве завершающего шага обязательно сохраните настройки нажатием кнопки «Save» -> «Save All» верхнем левом углу веб-интерфейса коммутатора:



на этом базовая настройка L2-коммутатора DES-3200 завершена.

10-Практическая занятия

Тема:Изучение технические данные ва ZyXel IES-1000 DSLAM, и настройка параметров. Настройка Статик VLAN и управление MAC адрес.

Модульный IP xDSL-коммутатор на 8 - 32 порта

Описание

ZyXEL IES-1000 - это G.shdsl Ethernet Switch, идеальное решение для для обеспечения доступаклиентов к магистральным сетям на базе протокола IP. В качестве клиентов могут выступать: офисныесети, учебные заведения, различные производственные структуры и другие. Это также прекрасноерешение для обеспечения высокоскоростного доступа к услугам сети Internet по стандартное меднойпаре проводов - что делает этот концентратор доступа идеальным решением для существующейинфраструктуры телефонной сети.

Преимущества Высокая скорость работы до 2.3 Мбит по одной паре проводов, а такжеиспользование линейного кодирования TC-PAM делает IES-1000 совместимым со многими стандартами xDSL и позволяет организовывать мощные узлы исключая взаимное влияние на соседние системыпередачи, что приобретает большую актуальность в нынешней ситуации бурного развития xDSL.

IES-1000 поддерживает высокоскоростную передачу данных до 2.3 Мбит и объединяет в одномустройстве 16 портов G.shdsl, имеет стандартный размер 1U что делает его очень компактным решениемпри построении узлов высокой плотности. Каждое устройство имеет в своем составе 8 портовый G.shdslмодуль с поддержкой "горячей замены". 10/100M Ethernet интерфейс

обеспечивает uplink к коммутаторам2 или3 уровня или к удаленным узлам магистральной сети.

IES-1000 также дает возможность эффективного сетевого управления с использованием системыуправления и мониторинга сети ZyXEL NetaVista. Информация о конфигурации, статусе системы , загрузкуустройства, сообщения об ошибках и многое другое передается от IES-1000 на систему NetaVista, котораяв свою очередь производит анализ данных с последующей выдачей отчетов. Кроме того имеется вналичии консольный порт для локального управления устройством.

Состав:

- G. SHDSL концентратор доступа
- Поддержка IP поверх ATM
- Обеспечение IP DSLAM приложений
- Организация приложений для центрального офиса
- Организация MTU приложений
- Поддержка L2 Switch

Составные части решений на базе IES-1000

- IES- 1000
- Маршрутизатор/мост Prestige 782
- Синхронный модем Prestige 724 CSU/DSU
- Система управления и мониторинга сети NetaVista

Характеристики IES-1000

- G. SHDSL + Ethernet Switch
- IP DSLAM, ATM коммутатор в одном устройстве IES- 1000
- Симметричная передача данных на расстояния свыше 3.3 км на скорости 2. 3 Мбит с шагом в
- 64 кбит поверх обычной медной пары проводов
- Линейная модуляция - TC- PAM
- 2 модуля с поддержкой "горячей замены в одном устройстве 1U.
- Каждый модуль имеет поддержку IGMP Snooping - для IP multicast
- Поддержка IEEE 802.1d (прозрачный мост)
- Поддержка IEEE 802.1Q тэгов для идентификации клиентов
- Поддержка VLAN защиты
- Поддержка протоколов : 802.1p, 802.1Q (вскоре будет реализована)

- Поддержка SNMP
- Поддержка MIB: RFC 1213, 1493, 1757, 2674, SHDSL line MIB

11-Практическая занятия

Тема: Изучение ZyXel IES-1000 DSLAM CLI через консол. орқали созлашни ўрганиш.

Заводские настройки по умолчанию

В данном разделе описываются настройки IES-1000, выполненные по умолчанию на заводе.

Параметры IP

- IP-адрес = 192.168.1.1
- Маска подсети = 255.255.255.0
- Шлюз по умолчанию = 192.168.1.254

Консольный порт

- Скорость (в бодах) = 9600 бит/с
- Биты данных = 8
- Контроль четности = отсутствует
- Стоп-бит = 1
- Управление потоком = отсутствует

Пароль при подключении через консоль, Telnet и FTP

Интерфейс командной строки (CI)

IES-1000 использует текстовые командные строки в качестве интерфейса пользователя для конфигурирования программного обеспечения. Перед тем, как приступать к конфигурированию, следует ознакомиться с общими правилами ввода команд, приведенными ниже.

Ключевые слова команды пишутся обычным шрифтом «Courier».

1. Ключевые слова команды должны вводится точно так, как показано, никакие сокращения не допускаются.
2. Поля команды, обязательные для заполнения, заключены в угловые скобки (<>), напр.,

   ```
   list port <port #>
   ```

   означает, что Вы должны указать номер порта для данной команды.
3. Поля команды, необязательные для заполнения, заключены в квадратные скобки ([]), напр.,

Использование команд, не упомянутых в настоящем Руководстве пользователя, может повредить модуль и привести его в негодность.

Подключение консоли

Первоначальное конфигурирование производится через консольный порт. По завершении первоначального конфигурирования можно подключиться к системе через

Далее в настоящем Руководстве пользователя рассматриваются команды CI, предназначенные для конфигурирования сетевых модулей.

Функция справки

Система содержит функцию справки, с помощью которой можно получить оперативную помощь.

- Можно в любой момент ввести help или ? , и система выдаст список всех доступных команд.
- Можно ввести help с именем какой-либо команды для получения подробной информации об этой команде, напр., команда

Telnet для выполнения дополнительных функций управления. Подсоединить один конец кабеля RS-232 к консольному порту IES8SHDSL, а другой конец - к последовательному порту (COM1, COM2 или другой порт COM) компьютера.

Можно использовать любую программу-эмулятор терминала (напр., терминальную программу HyperTerminal из состава Windows) со следующими параметрами:

- эмуляция терминала VT100
- скорость передачи 9600 бод
- без контроля четности, 8 бит данных, 1 стоп-бит
- без управления потоком

Командная структура

Система использует двухуровневую командную структуру. Команды, относящиеся к одной подсистеме, группируются под первичной командой данной подсистемы. Напр., чтобы сконфигурировать параметры G.SHDSL, необходимо сначала войти в подсистему G.SHDSL, введя команду gshdsl в командной строке. После входа в подсистему в командной строке появится имя подсистемы, напр.,

```
192.168.1.1 gshdsl>
```

Для возврата из подсистемы к подсказке верхнего уровня используется команда home .

```
192.168.1.1> help version
```

дает

```
version - show system software version
```

В ответ система выдает описание команды version.

Сохранение конфигурации

Следует обязательно сохранить созданную конфигурацию с помощью следующей команды:

```
192.168.1.1> config save
```

Данная команда предназначена для сохранения всей системной конфигурации в энергонезависимой памяти. Рекомендуется сохранять любые изменения в конфигурации с помощью данной команды, в противном случае при перезапуске IES-1000 вернется к настройкам по умолчанию.

Не выключать IES-1000 в процессе сохранения конфигурации.

Команда Version

Синтаксис:

```
192.168.1.1> version
```

Данная команда предназначена для вывода версии и даты выпуска системного встроенного программного обеспечения.

Команда Restart

Синтаксис:

```
192.168.1.1> restart
```

Данная команда дает указание системе произвести «горячий» перезапуск, то есть перезапустить систему без выключения и повторного включения питания.

Команда Passwd

Синтаксис:

```
192.168.1.1> passwd
```

Данная команда предназначена для изменения пароля доступа к управлению. Этот пароль используется для аутентификации при подключении через консоль или Telnet. Данная команда работает только в локальных сеансах управления. Длина пароля должна составлять от 1 до 8 символов, допускаются любые символы. По умолчанию установлен пароль «1234».

Очень важно помнить свой пароль. Если Вы все же забудете его, следует обратиться к разделу Устранение неисправностей *за справкой.*

Команда Config Print

Синтаксис:

```
192.168.1.1> config print
```

Данная команда предназначена для вывода всех текущих параметров конфигурации системы.

12-Практическая занятия

Тема: Ознокомление способом мультиплексированые пользова-тельские данные в широко-полосных сетях.

1. Теоритическая часть

Термин широкополосная (broadband) передача изначально использовался в системах телефонной связи, где им обозначался аналоговый канал с диапазоном частот (шириной полосы пропускания) более 4 КГц. С целью экономии ресурсов при передаче большого числа телефонных сигналов с полосой частот 0,3-3,4 КГц были разработаны различные схемы уплотнения (мультиплексирования) этих сигналов, обеспечивающие их передачу по одному кабелю.

В высокоскоростных сетевых приложениях широкополосная передача означает, что для передачи данных используется не импульсная, а аналоговая несущая. По аналогии термин «широкополосный Интернет» означает, что вы используете канал с пропускной способностью более 128 Кбит/с (в Европе) или 200 Кбит/с (в США).

Широкополосная система обладает высокой пропускной способностью, обеспечивает высокоскоростную передачу данных и мультимедийной информации (голос, видео, данные). Примером являются сети ATM, B-ISDN, Frame Relay, сети кабельного вещания CATV.

Термин «мультиплексирование» используется в компьютерной технике во множестве аспектов. Мы под этим будем понимать объединение нескольких коммуникационных каналов в одном канале

передачи данных. Перечислим основные техники мультиплексирования: частотное уплотнение – Frequency Division Multiplexing (FDM), временное уплотнение – Time Division Multiplexing (TDM) и спектральное или уплотнение по длине волны (волновое) – Wavelength Division Multiplexing (WDM).

WDM применяется только в оптоволоконных системах. Кабельное телевидение, например, использует FDM.

FDM

При частотном мультиплексировании каждому каналу выделяется своя аналоговая несущая. При этом в FDM может применяться любой вид модуляции или их комбинация. Например, в кабельном телевидении по коаксиальному кабелю с шириной полосы пропускания 500 МГц обеспечивается передача 80 каналов по 6 МГц каждый. Каждый из таких каналов в свою очередь получен мультиплексированием подканалов для передачи звука и видеоизображения.

TDM

При этом виде мультиплексирования низкоскоростные каналы объединяются (сливаются) в один высокоскоростной, по которому передается смешанный поток данных, образованный в результате агрегирования исходных потоков. Каждому низкоскоростному каналу присваивается свой временной слот (отрезок времени) внутри цикла определенной длительности. Данные представляются, как биты, байты или блоки бит или байт. Например, каналу А отводятся первые 10 бит внутри

временного отрезка заданной длительности (фрейм, кадр), каналу В – следующие 10 бит и т.д. Кроме бит данных фрейм включает служебные биты для синхронизации передачи и других целей. Фрейм имеет строго определенную длину, которая обычно выражается в битах (например, 193 бита) и структуру. Устройства сети, которые выполняют мультиплексирование потоков данных низкоскоростных каналов (tributary, компонентные потоки) в общий агрегированный поток (aggregate) для передачи по одному физическому каналу, называются мультиплексорами (multiplexer, mux, мукс). Устройства, выполняющие разделение агрегированного потока на компонентные потоки, называются демультиплексорами.

Синхронные мультиплексоры используют фиксированное разделение на временные слоты. Данные, принадлежащие определенному компонентному потоку, имеют одну и ту же длину и передаются в одном и том же временном слоте в каждом фрейме мультиплексированного канала. Если от некоторого устройства информация не передается, то его тайм слот остается пустым. Статистические мультиплексоры (stat muxes) решают эту проблему, динамически присваивая свободный временной слот активному устройству.

WDM

WDM использует различные длины волн светового сигнала для организации каждого канала. Фактически это особый вид частотного уплотнения на очень высоких частотах. При этом виде мультиплексирования передающие устройства работают на разных длинах волн (например, 820нм и 1300нм). Затем лучи объединяются и передаются по одному оптоволоконному кабелю. Принимающее устройство разделяет передачу по длинам волн и направляет лучи в разные приемники. Для слияния/разделения каналов по длинам волн используются специальные устройства – каплеры (coupler). Ниже приведен пример такого мультиплексирования.

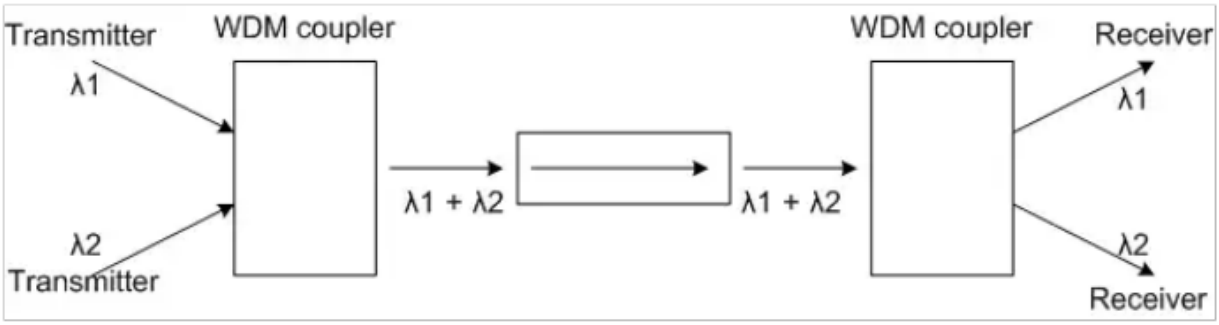


Рис.12.1. WDM мультиплексирование

Среди основных конструкций каплеров различают отражающие каплеры и центрально-симметричные отражающие каплеры (SCR). Отражающие каплеры представляют собой крошечные “перекрученные” в центре кусочки стекла в виде звезды. Количество выходных лучей соответствует количеству портов каплера. А число портов определяет количество устройств, передающих на разных длинах волн. Далее показаны два вида отражающих каплеров.

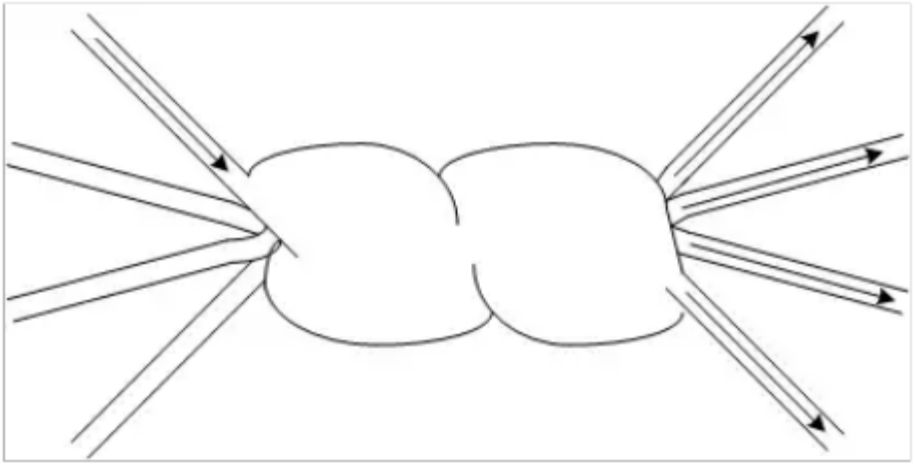


Рис.12.2. Передающая звезда

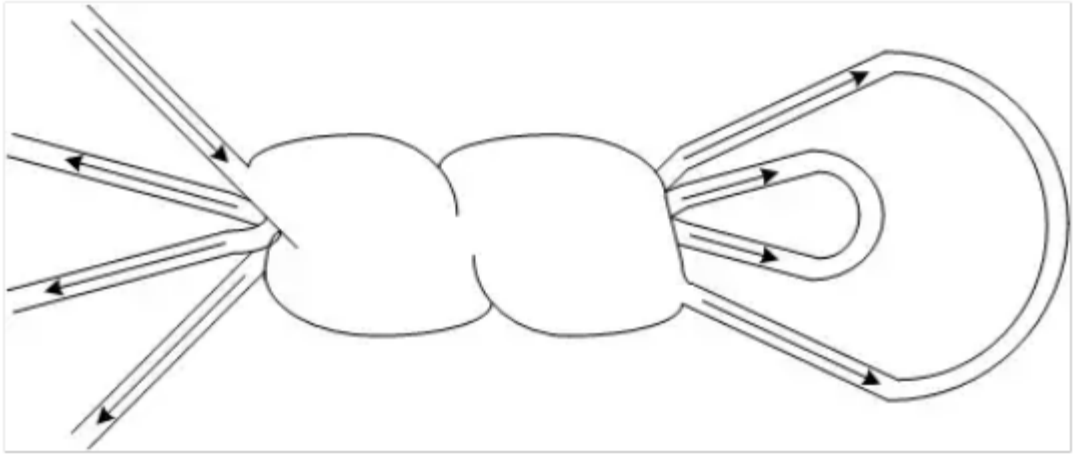


Рис.12.3. Отражающая звезда

Центрально-симметричный отражающий каплер использует отражение света от сферического зеркала. При этом поступающий луч разделяется на два луча симметрично центра изгиба сферы зеркала. При повороте зеркала меняется положение изгиба сферы и соответственно путь отраженного луча. Можно добавить третий оптоволоконный кабель (fiber) и перенаправить отраженный луч еще на один порт. На этой идее основана реализация WDM – мультиплексоров и оптоволоконных коммутаторов.

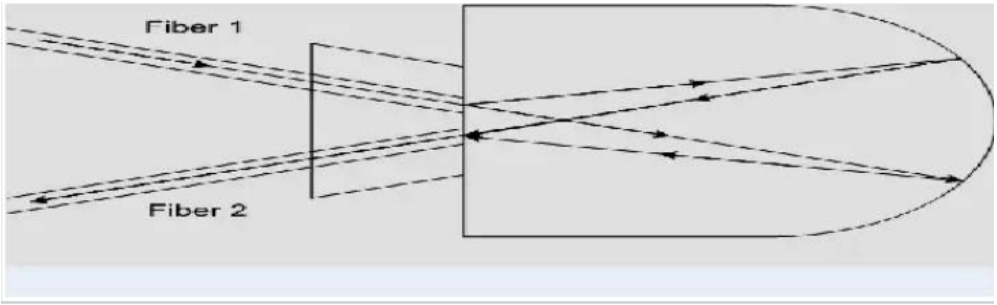


Рис.12.4. Центрально-симметричный отражающий каплер

Оптические мультиплексоры могут реализовываться не только при помощи CSR-каплеров, но и при помощи отражающих фильтров и дифракционных решеток. В данном учебном пособии они не рассматриваются. Основными факторами, определяющими возможности различных реализаций, являются мешающие наводки и разделение каналов. Величина наводки определяет, насколько хорошо разделены каналы, и, например, показывает, какая часть мощности 820-нм луча оказалась на 1300-нм порту. Наводка в 20 ДБ означает, что 1% сигнала появился на непредназначенном порту. Чтобы обеспечить надежное разделение сигналов длины волн должны быть разнесены “широко”. Трудно распознать близкие длины волн, например 1290 и 1310 нм. Обычно используют 4 схемы мультиплексирования: 850/1300, 1300/1550, 1480/1550 и 985/1550 нм. Лучшими характеристиками пока обладают CSR-каплеры с системой зеркал, например, двумя (рис.5.5).

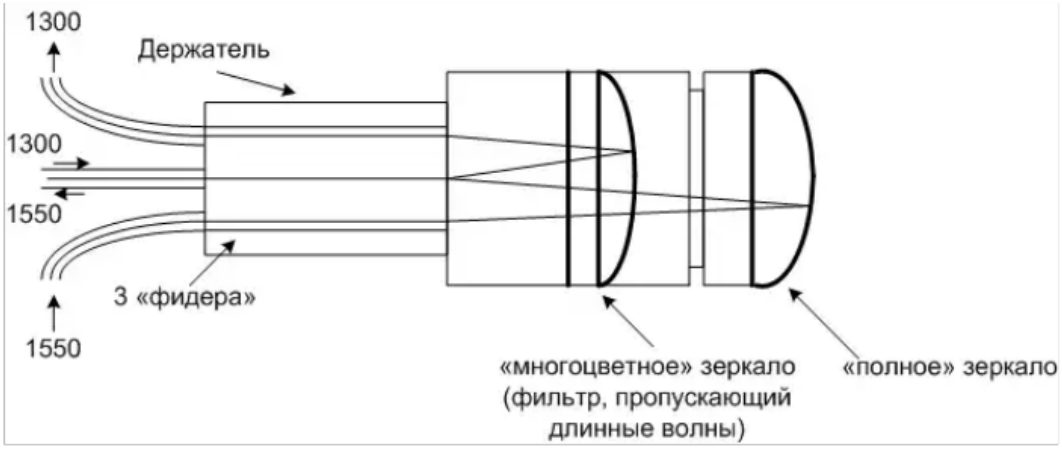


Рис.12.5. SCR-каплер с двумя зеркалами

Технология WDM, представляющая собой одну из трех разновидностей спектрального уплотнения, занимает среднее положение в смысле эффективности использования спектра. В системах WDM объединяются спектральные каналы, длины волн которых отличаются одна от другой на 10 нм. Самой производительной является технология DWDM (Dense WDM). Она предусматривает объединение каналов, разнесенных по спектру не более чем на 1 нм, а в некоторых системах даже на 0,1 нм. Вследствие такого плотного размещения сигналов по спектру стоимость оборудования DWDM обычно очень высока. Наименее эффективно спектральные ресурсы используются в новых системах на основе технологии CWDM (Coarse WDM, разреженные системы WDM). Здесь спектральные каналы разнесены не менее чем на 20 нм (в некоторых случаях эта величина достигает 35 нм). Системы CWDM обычно используются в городских сетях и в LAN, где низкая цена оборудования является важным фактором и требуется организация 8-16 каналов WDM. Оборудование CWDM не ограничено одним участком спектра и может

работать в диапазоне от 1300 до 1600 нм, в то время как аппаратура DWDM привязана к более узкому диапазону 1530 - 1565нм.

Литература

1. Семенов А.В. Сети нового поколения. СПб: Наука и техника, 2005.
2. Материалы курса «Сети связи следующего поколения» сайта Интернет-Университета Информационных Технологий http://www.INTUIT.ru
3. А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева. IP-телефония. ИТЦ Эко-Трендз. 2002.
4. Б.С. Гольштейн, А.В. Пинчук, А.Л. Суховицкий. IP-телефония. Москва. Радио и связь. 2003.
5. Гольдштейн Б.С., Гольдштейн А.Б. SoftSwitch. СПб.: БХВ - Санкт-Петербург, 2006.
6. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS. СПб.: БХВ - Санкт-Петербург, 2005.
7. Крук Б.И. Папантанопуло В.Н. Шувалов В.П Телекоммуникационные сети и системы: Современные технологии. М.: Горячая линия - Телеком, 2003.
8. Современные телекоммуникации. Технологии и экономика. Под ред. Довгого С.А. –М.: Эко-Трендз, 2003.
9. Садчикова С.А. IP-телефония. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. Ташкент. ТУИТ.2008
10. С. Илич. FTTC: решение для широкополосных сетей доступа с оптимальной стоимостью. Вестник связи, №10, 2010
11. Доступ следующего поколения – Комбинирование широкополосного доступа FTTC и FTTB. Описание технического решения Iskratel FTTx