МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИИ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛЬ-ХОРАЗМИЙ

Кафедра «Телекоммуникация инжиниринги»

Методическое пособие для практических занятий по предмету

"Широкополосные сети"

для студентов, обучающихся по направлениям образования 5350100 – Телекоммуникационные технологии (Телекоммуникация, телерадиовещание, мобильные системы)

Ташкент 2018

Авторы:Садчикова С.А., Абдужаппарова М.Б., Давлетова Х.Р.
Широкополосные сети. Методическое пособие для практических занятий /ТУИТ. 115 с. Ташкент, 2018

В данном методическом пособии представлены материалы для проведения практических занятий по дисциплине «Широкополосные сети». Дисциплина изучается студентами направления образования 5350100 - Телекоммуникационные технологии (Телекоммуникация, телерадиовещание, мобильные системы) в 8 семестре. Каждое занятие методического пособия содержит теоретические сведения, список литературы, контрольные вопросы, варианты заданий и описание виртуальной работы для проверки усвоения материала.

Методическое пособие призвано помочь студентам самостоятельно изучить основные положения широкополосных сетей, её структуру, оборудования для её построения и приобрести практические навыки по построению подсетей и фрагментов сети Интернет.

Методическое пособие рассмотрено и одобрено на заседании кафедры ТИ. Рекомендовано к тиражированию НМС в типографии ТУИТ.

Ташкентский университет информационных технологий
имени Мухаммада аль-Хоразмий, 2018

Практическое занятие №1

АРХИТЕКТУРА И ИСПОЛЬЗУЕМОЕ ОБОРУДОВАНИЕ ДЛЯ ПОСТРОЕНИЯ ШИРОКОПОЛОСНЫХ СЕТЕЙ

1. Цель и содержание занятия

Изучение структуры широкополосной сети, оборудования для её построения на примере учебной сети ТУИТ.

2. Заданиекзанятию

1.Изучитькомпоненты, входящиевсоставучебнойширокополосной сетиТУИТ (см.рис.1.1). Заполнить таблицу по каждому виду оборудования, которая включает – модель, назначение оборудования, техническое описание компонентов оборудования.

2.Привести технические характеристики оборудования, согласно варианту таблицы 1.1

Вариант	Тип оборудования
1.	Switch
2.	Huawei MC850
3.	DSLAM
4.	ZyXEL IP Express IES-1000
5.	IAD
6.	Huawei EchoLife MC820c
7.	Broadband MultiplayCenter
8.	Huawei U-SYS IAD208
9.	SIP-терминалMedia Phone
10.	D-Link xStack DES-3200-18

3. Порядоквыполнения

1. Нарисоватьархитектурусети
2. Изучитьтеоретическуючастьработы
3. Ответить на контрольные вопросы
4. Составить отчёт по работе

4. Содержаниеотчета

1.Краткое описание теоретической части
2. Блок-схемы устройств
3. Результаты настроек

5. Контрольныевопросы

1. Какиеустройствавходятвсоставширокополосной сети?
2. Каковоназначениеустройства D-Linkswitch?
3. ВчёмразницамеждуSIP-терминаломитрадиционнымтелефоннымаппаратом?
4. Каковоназначениеустройства SIP сервер?

5.КакимобразомоборудованиеLANподключаетсякучебной широкополосной сети ТУИТ?
6. КаковоназначениеDSLAM?
7. Каков принцип работы DSLAM?
8. КаковыфункцииIAD?
9. Какиевидысредыпередачииспользуютсявширокополосной сети?
10.КакимобразомSIP-терминаломподключается к традиционнойтелефонной сети?

6. Теоретическиесведения

Учебнаяширокополосная сетьТУИТ приведена на рис.1.1. Втаблице1.1 приведенооборудование, входящеевсоставсети.

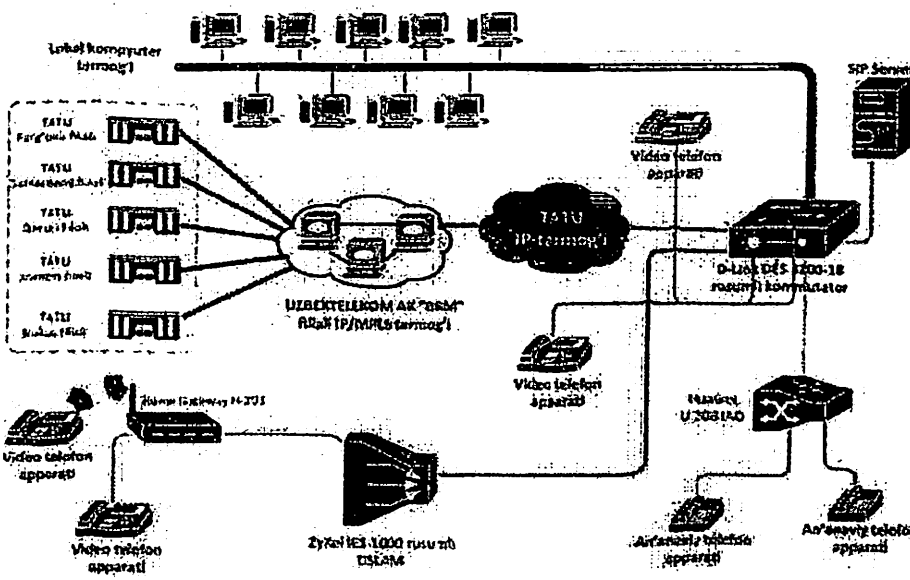


Рис.1.1. Учебнаяширокополосная сетьТУИТ

Таблица 1.1

Тип оборудования	Модель
Switch	D-Link xStack DES-3200-18
DSLAM	ZyXEL IP Express IES-1000
IAD	Huawei U-SYS IAD208
Broadband MultiplayCenter	HuaweiEchoLife MC820c
SIP-терминалMedia Phone	Huawei MC850

D-Link xStack DES-3200-18 Switch

КоммутаторD-LinkxStackDES-3200-18 Switch (рис.1.2) входитвсоставлинейкикоммутаторов 2 уровняD-Link'sTheDES-3200 SeriesLayer 2 xStackManagedSwitch, разработанныхдляETTX, FTTX.

DES-3200-18предоставляет 16 портов 10/100Мбит/cFastEthernetили дополнительные портыSFP или комбоGigabit/SFP. DES-3200-18упакованв 11-дюймовыйкожухдляустановкмнастоле или в сойке оборудования. ДополнительнокDES-3200-18могутбытьподключены 2 2ГбитSFPuplinkдляобеспечения гибкого выбора топологии сети (кольцо, дерево или смешанная).

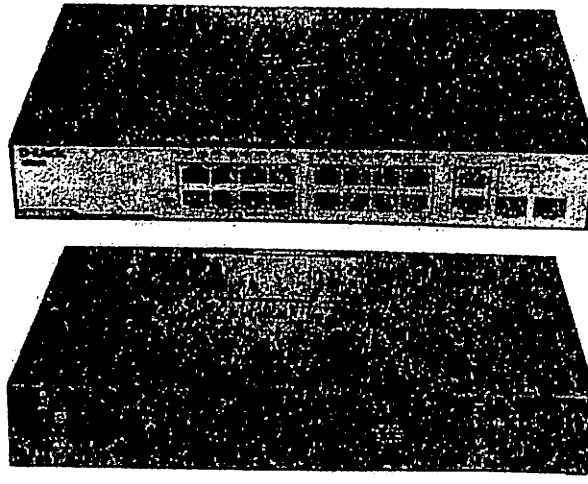


Рис.1.2. ВнешнийвидкоммутатораD-LinkxStackDES-3200-18 Switch

Безопасность и доступность

DES-3200-18 поддерживает 802.1X на основе портов / хоста управления доступом на основе, GuestVLAN и RADIUS / TACACS / XTACACS / TACACS + Аутентификация строгого контроля доступа по сети. Связывание Функция IP-MAC-Port позволяет администраторам связывать IP-адрес источника к соответствующему MAC-адресу для определенного

номера порта для усиления контроля доступа пользователей. Кроме того, с помощью функции DHCPSnooping, коммутатор автоматически пары в IP / MAC, отслеживая DHCP-пакеты и сохраняя их в белый список IMPB. Эти функции играют важную роль в поддержании безопасности сети. Встроенные D-LinkSafeguardEngine обеспечивает идентификацию и приоритезацию "CPU заинтересованные" пакеты для предотвращения злонамеренных атак на трафик в сети и защиты операций, выполняемых коммутатором. Кроме того, DES-3200-18 предоставляет различные многоуровневые правила списка управления доступом (ACL). Администраторы могут ограничить сетевые сервисы или права доступа, не влияя на производительность коммутатора.

Отказоустойчивость / Увеличение производительности

Для критически важных сред DES-3200-18 поддерживает 802.1D-2004 издание, 802.1w и 802.1sMultipleSpanningTree (MSTP). STPпозволяет настроить коммутатор на резервный маршрут, поэтому передача и прием пакетов может быть гарантировано в случае неисправности любого коммутатора в сети. Коммутаторы также поддерживают функцию 802.1AX и 802.3adLinkAggregation, что позволяет сгруппировать несколько портов параллельно с образованием одного порта, увеличивая пропускную способность и избыточность для более высокой доступности. Для управления качеством обслуживания (QoS), коммутатор поддерживает 802.1p и классификацию пакетов на передовую, основанную на TOS, DSCP, MAC-адрес, IP-адресов, VLANID, номера порта TCP / UDP, типа протокола и определяемого пользователем контента пакета. Это позволяет гибко конфигурировать для конкретных мультимедийных приложений, таких как VoIP или IPTV. Кроме того, DES-3200-18 поддерживает автоматическую и эффективную функцию QoS для голосового трафика. Голос VLAN1 включает в себя голосовые конечные точки автоматически к выделенной VLAN с более высоким приоритетом, чтобы гарантировать качество и безопасность голосового трафика.

Управление нагрузкой и полосой пропускания

Функция управления полосой пропускания позволяет сетевым администраторам определять / выход уровни пропускной способности Ingress для каждого порта с зернистостью до 8 Кбит. Коммутатор также поддерживает функцию управления шторм, который сводит к минимуму повреждения в сети. Зеркалирование портов помогает администраторам облегчить диагностику трафика или отслеживать производительность коммутатора и при необходимости внесите изменения. DES-3200-18 поддерживает два тарифа и SingleRateThreeColorMarker (TRTCM / srTCM) для классификации трафика потоков в соответствии и несоответствующей группы, чтобы гарантировать минимальную полосу пропускания для трафика.

Приложения Multicast

DES-3200-18 предоставляет полный спектр функций многоадресной рассылки L2, включая IGMPSnooping, фильтрация IGMP, быстрый отпуск и

конфигурации многоадресной рассылки трафика для конкретных портов. При поддержке L2 Multicast, DES-3200-18 демонстрирует свою способность справляться с растущей приложения IPTV. Принимающая сторона на основе протокола IGMP / MLDSnooping позволяет нескольким широковещательные абонентов на один физический интерфейс и ISMVLAN отправляет потоки групповой передачи в многоадресной VLAN, чтобы сохранить пропускную способность в магистральной сети. Профили ISMVLAN позволяют пользователям связываться / быстро и легко заменить предварительно определенную многоадресную регистрационную информацию подписки портов.

OAM

DES-3200-18 оснащён диагностическим кабелем для проверки состояния сетевых кабелей, чтобы точно определить причину любой неисправности в кабельной сети, не требуя на месте поддержки оператора. Функция 802.1agConnectivityFaultManagement (CFM) предоставляет инструменты для мониторинга и устранения неисправностей конец к концу сетей Ethernet, позволяя провайдерам услуг контролировать соединение, изолировать проблемные участки сети и идентифицировать клиентов, пострадавших от сетевых проблем. 802.3ahEthernetOAM, умирание издыхании и D-Link однонаправленный Обнаружение Link (DULD) функции может улучшить управление сетью на Ethernet и помогают поддерживать стабильную сетевое подключение и поддержка определения местоположения неисправностей.

Возможности управления

DES-3200-18 поддерживает стандартные протоколы управления, такие как аутентификация безопасности SNMP, RMON, Telnet, SSH / SSL и DHCP опция реле 82. переключатель серии также имеет веб-интерфейс, который обеспечивает удобный интерфейс и простое управление. DHCP автоматическое конфигурирование является функцией расширенного управления, которая позволяет администраторам предварительно настроить конфигурацию на сервере TFTP и применить к коммутаторам автоматически, когда переключатель пытается получить IP-адреса от DHCP. Это упрощает развертывание коммутатор и быстрее, особенно в больших масштабах сети. LLDP и LLDP-MED1 обеспечивают быстрое обнаружение оборудования Ethernet особенно для конечных устройств. Согласно результату обнаружения, администраторы могут легко раздвигать конфигураций соответствующих устройств и создать топологию рисования через систему управления сетью (NMS) быстро.

SingleIPManagementD-Link (SIM) упрощает и ускоряет задачи управления, позволяя нескольким коммутаторам настраиваться, контролироваться и поддерживаться с любой рабочей станции под управлением веб-браузера с помощью уникального IP-адреса. DES-3200-18 также работает с D-View 6.0 программное обеспечение D-Link. D-View 6.0 представляет собой систему управления сетью, которая позволяет осуществлять централизованное управление важнейшими характеристиками

сети, таких как доступность, надежность, устойчивость и безопасность. D-View 6.0 предоставляет полезный набор инструментов для сетевых администраторов, которые хотят эффективно управлять конфигурациями устройств, отказоустойчивости, производительности и безопасности.

IPv6

DES-3200-18 сертифицирован с IPv6 ReadyLogoPhase 2, которая гарантирует подключение и управляемость в сети IPv6. Кроме того, он поддерживает IPv4/v6 двойную функцию стека, которая позволяет коммутатору выступать в качестве моста между сетями IPv4 и IPv6. Поскольку сети растут и потребности в большей адресации и более высокий уровень защиты становится критической, серии DES-3200 поддерживает различные IPv6 ACL, IMPBv61 и функции L3 управления пакетами фильтрации для защиты сети от атак и отвечают требованиям к проектированию архитектуры IPv6.

КоммутаторDES-3200-18 (рис.1.3) обеспечивает достаточную производительность, отказоустойчивость и гибкуюмасштабируемуемость, надежную защиту, стандарт на основе взаимодействия и технологии для развертывания ведомственной и корпоративной сети на будущее. Список интерфейсов приведён в таблице 1.2.

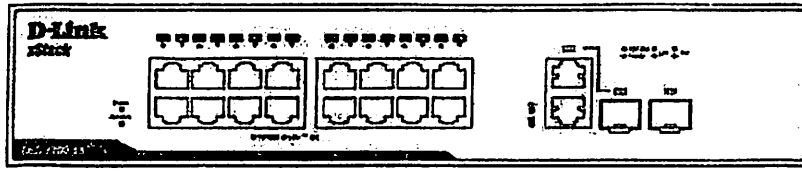


Рис.1.3. Передняя панельDES-3200-18

Табица 1.2

Типы интерфейсов

Описание	Количество
порт 10/100Mbps Copper	16
порт 100/1000Mbps SFP	1
портCombo 10/100/1000Мбит/с Copper / 100/1000 Мбит/с SFP	1
порт RJ-45 Console	1

Примечание: Светодиоды для питания, консоль, Link / Act для порта от 1 до 16 и Link/Act/Speed для порта 17 и 18 (рис.1.4).

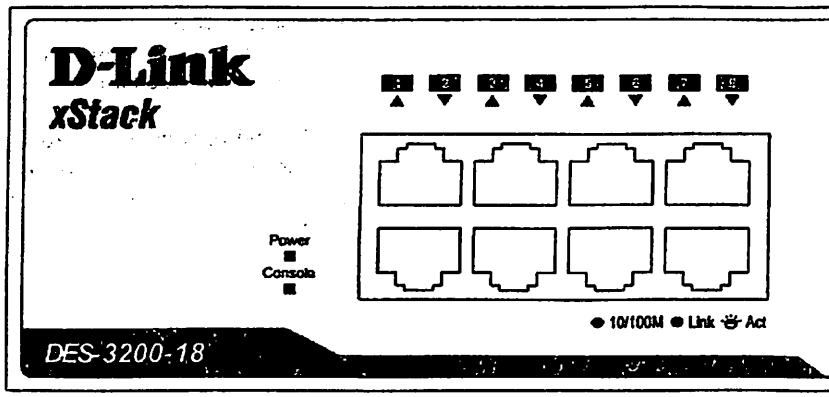


Рис.1.4. СветодиодыDES-3200-18

HuaweiIAD 208

Устройство интегрированного доступа IAD 208представляет собой шлюз IP на основе для доступа голосовых и факсимильных ресурсов. IAD208 предоставляет услуги голосовой связи высокой эффективности и высокого качества, основанные на Интернет или корпоративные сети.

В качестве шлюза доступа к среде передачи голоса поверх IP (VoIP) и факс поверх IP (FoIP) IAD208 применяется в сетях NGN или IPMultimediaSubsystem (IMS). IAD208 преобразует аналоговые речевые данные в IP-пакеты и передает данные через IP-сети.

IAD208 подключен к NGN/IMS через протокол управления медиа-шлюза (MGCP) или SessionInitiationProtocol (SIP). Он соединяет звонки между вызывающей и вызываемой сторонам через протокола MediaGatewayControl (MGC) или сервера SIP.

IAD208 может быть подключен к сети через xDSL абонентскую линию, коммутатор или Gigabit с поддержкой пассивной оптической сети (GPON) / Ethernet пассивной оптической сети (EPON).

IAD208 (рис.1.5) предоставляет различные возможности передачи голоса и данных и поддерживает следующие функции (таблица 1.3).

Таблица 1.3

Особенности IAD208

Наименование	Описание
Протокол/стандарт	SessionInitiationProtocol (SIP)
	Media Gateway Control Protocol (MGCP)
	Real-time Transport Protocol (RTP) / Real-time Transport Control Protocol (RTCP)
	Point-to-Point Protocol over Ethernet (PPPoE)
	Dynamic Host Configuration Protocol (DHCP) Client
	Domain Name Server (DNS) Client

Voice Features - обработкаголоса	Детектор голосовой активности (VoiceactivitydetectionVAD)
	Эхо (Echocancellation EC)
	ДетектированиеигенерацияDTMF кодов
	Кодеки G.711 и G.729
	Длительные вызовы
	Функция восстановления потерянных пакетов Packetlosscompensation (PLC)
	Длительностьголосовогокадраменее
DataFeatures – возможности по обработке данных	приоритет голоса над данными
	ПоддержкаVirtualLocalAreaNetwork (VLAN)иорганизацииотдельныхпакетовдляголоса, данныхисигналовпротоколовуправления

ИнтерфейсыIAD208 (см.рис.1.6.) приведеныв Таблице 1.4.

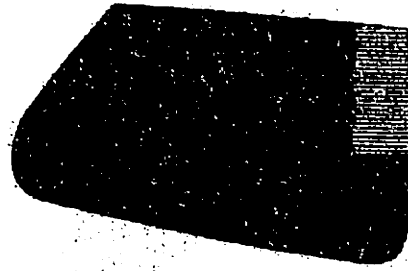


Рис.1.5. Внешнийвид IAD208

Рис.1.6.Внешнийвидинтерфейсов IAD 208

Таблица 1.4.

ИнтерфейсыIAD208

Тип интерфейса	Описание s
DC 12 V	Сокет питания
WAN	Uplink порт
LAN 1-8	8 портов для голоса и данных
CONSOLE	Последовательный порт для ТО

ZyXEL IP Express IES-1000 Remote MSAN/DSLAM

ZyXELIES-1000 серии (рис.1.7) представляет собой IP-узел доступа на основе мультисервисной (MSAN)выполненный в виде отдельной коробки. Он имеет два слота для различных комбинаций DSL и VoIP линейных карт, чтобы обеспечить ADSL2+, G.SHDSL и VoIP услуг частным и корпоративным клиентам. Он терминирует трафик ATM или EFM из DSL соединений и POTS голосовых сигналов, для упаковки их вIP-пакеты и маршрутрутизации через IP-сети.РазвертываниеZyXELIES-1000 вместе с DSL-модемами и маршрутизаторамиWAN образует комплексное решение для предоставления услуг широкополосного доступа к нескольким блокам.

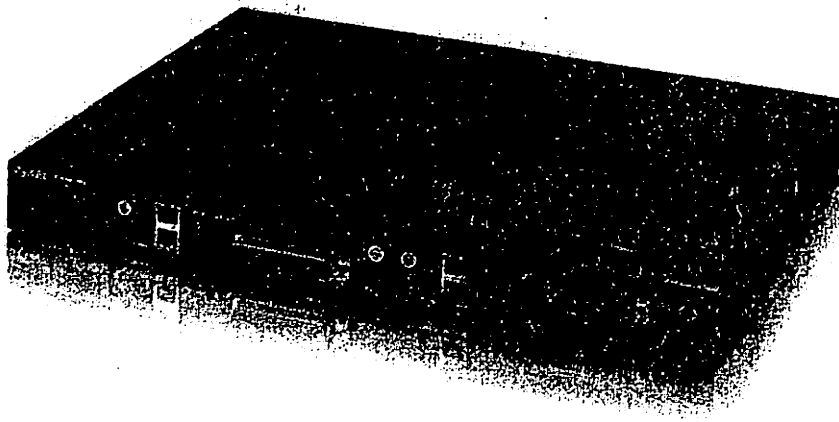


Рис.1.7. Внешний вид ZyXELIPExpressIES-1000

Сервис ADSL2 + для рассредоточенных пользователей

ИспользуяплатыADSL2+, провайдеры услуг могут предложить рассосредоточеннымпользователям жилых домовчерез одно подключение к сети высокую пропускную способность доступа в Интернет, услуги IPTV по запросу, развлекательные услуги. IES-1000 Series также предлагает абонентам объекты IP-подключения, VPN, видеоконференций высокого качества и услуг традиционной телефонии с пропускной способностью до 24Мбит/с на один порт. Кроме того, он поддерживает ATM на основе 2-х портов, чтобы обеспечить еще более высокую пропускную способность для

удаленных клиентов. ПлатаADSL2+ представляет собой сложное устройство полностью совместимо с существующими стандартами и современными функциями, как энергосбережение, отличная производительность и прозрачно назад для совместимости ADSL / ADSL2.

СервисарендованныелинииG.SHDSLдля предприятий

С помощью технологии G.SHDSL, MSAN/DSLAM серии IES-1000 применяется для замены аренды линии. Используя метод модуляции TC-PAM, IES-1000 Series совместим с другими существующими технологиями передачи, что позволяет сервис-провайдерам развернуть в тех местах, где уже существуют широкополосные услуги.

Платы G.SHDSL.bis обеспечивают скорость передачи данных до 5,7Мбит/с симметрично в одной паре. MSAN/DSLAMIES-1000 также поставляется с двумя 100Мбит/cEthernet-интерфейсами для агрегации Ethernet сети. Один IES-1000 Series может вместить двух SAM1316-22 модулей для поддержки 32 соединений SHDSL.

Платы VoIP для обеспечения функций медиа-шлюза

В дополнение к факс и модем услуги, плата VoIP обеспечивает параллельную и распределенную архитектуру медиа-шлюза для расширения возможностей VoIP услуг за счет использования POTS голосовых сигналов. С архитектурой, линейная карта обслуживает до 24 POTS портов. Медиа-шлюз обеспечивает кодеки G.711, G.723, G.726, G.729a/б и T.38 и сетевой протокол сигнализации SIP поддерживается.

Описание оборудования

IES-1000имеет 2 слотадляподключениясетевыхмодулей мультиплексоров.IES-1000 предоставляет:

- Подключениепоследнймилипосредствомethernet, совместимойстехнологиямисуществующихLAN
- Поддержкарасширенияконфигурацийсплатамиplug-and-play
- Приоретизация пакетов 802.1p (QoS)
- 802.1Q VLAN
- Multicast

ВозможностиплатыAAM1212-51/53

МодульAAM1212 (Рис. 1.8.) обеспечивает:

- 1Telco 50 коннектордля 12портовADSL/ADSL2/ADSL2+ икартусплиттерадляпортовтрадиционнойтелефонии(AAM1212-51) или ISDN (AAM1212-53)
- 1 портRJ11длямини-консолиуправления для локальных настроек
- 2 интерфейса 10/100Base-TX,дляuplink

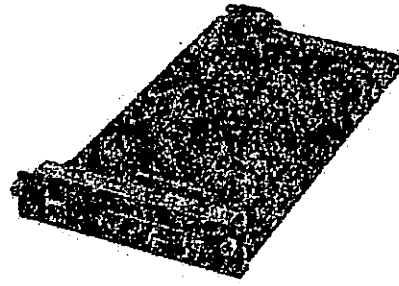


Рис.1.8. ВнешнийвидмодуляAAM1212

Плата AAM1212 обеспечивает:

- Адаптацию скорости подключения
- ADSL
- ADSL2
- ADSL2+

ВозможностиплатыSAM1316-22

SAM1316-22 (рис.1.9.) обеспечивает:

- 1 Telco 50 коннекторадля 16портовG.SHDSL.bis
- 1 портRJ11 длямини-консолиуправления для локальных настроек
- 2 интерфейса 10/100Base-TXдляuplink

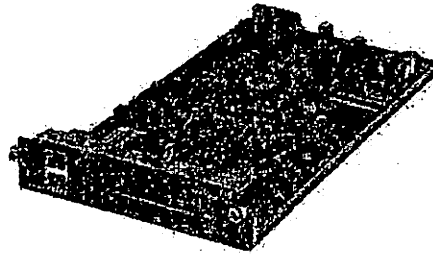


Рис.1.9. ВнешнийвидSAM1316-22

ПлатаSAM1316-22 обеспечивает:

- Режимыадаптациискорости – фиксированный, в зависимости от линии
- ФорматзаполненияSHDSL –ATMorEFM
- ПодключениеEthernetна «первоймиле» в соответствии cIEEE 802.3-2004
- SHDSL.bismакс. скорость 5.7Мбит/с

ВозможностиплатыVOP1224-61

VOP1224-61 (рис.1.10) обеспечивает:

- 1 Telco 50 коннектордля 24портовFXSтрадиционной телефонии
- 1 портRJ11 длямини-консолиуправления для локальных настроек
- 2 интерфейса 10/100Base-TXдляuplink

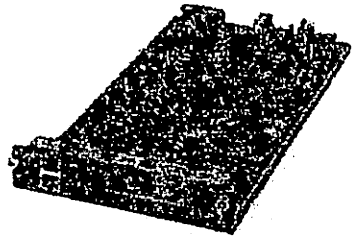


Рис.1.10. Внешнийвид SAM1316-22

- Плата VOP1224-61 поддерживает:
- Сигнальный протокол SIP
- КодекиG.711, G.726, G.729 a/b, G.723.1
- Эхо-компенсацию
- Детекторпаузи генерацию комфортного шума (ComfortNoiseGenerationCNG)
- Детектор голосовой активности (Voice Activity Detection VAD)
- Детеутированиецифрномеравызываемогоабонента (CallerID) дляIPпакетовизuplink
- Поддержкагенерацииакустических сигналов – ОС, вызов, КПВ, занято, извещение о неправильно положенной трубке
- ПоддержкаДВО – call waiting, call hold, call transfer, return and call back on busy

МодемZTE ZXHN H108N Broadband Access CPE

H108N (Рис.1.11.) беспроводный ADSL2+ модем с четырьмя интерфейсами Ethernet и IEEE 802.11 b/r/N(2x2) с Wi-Fi интерфейсом и одним USB-интерфейсом. Он используется для обеспеченияуслуг ШПД иIPTV дома. Интеграция с CWMP технологией (протокол управленияCPEWANManagementProtocol) облегчает автоматическую установку и автоматическая предоставление услуг

ВозможностиADSL2+

Модем H108N поддерживает ADSL2+ высокоскоростной доступ и совместим с модемом ADSL2 и ADSL. Со скоростью до 24Мбит/с (стандарт ADSL2+) или до 12 Мбит/с (стандарт ADSL2).

Улучшенная производительность беспроводной передачи 11n

Внедрение передовых **11n** технологий вH108N создает улучшенную производительность беспроводного подключения со скоростью до 300 Мбит/с.H108N полностью совместим с любыми стандарта

IEEE802.11b/gWiFi на сертифицированных устройствах.

USB функции

USB-порт может быть подключен с USB HDD, флэш-диск или принтеры, которые выступают в качестве файлового сервера и сервера печати, так что он может легко поддерживать конфигурации резервного копирования и восстановления файлов и сети обмена общей печати.

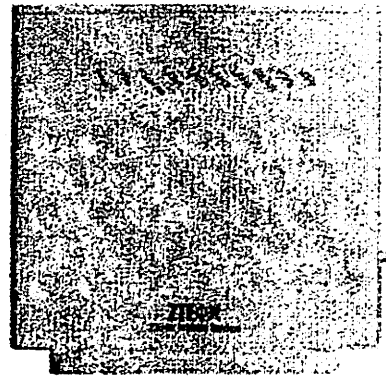


Рис.1.11. Внешний вид H108N

Поддержка IPv6

С поддержкой IPv4 и IPv6 двойного стека и DS-Lite, в H108N помогает операторам и конечным пользователям обеспечить будущее сети с плавной эволюции.

Технические возможностиH108N

В качестве ADSL модема споддержкойфункций маршрутизации, H108N модем поддерживает следующие технологии:

- ADSL (ADSL2, ADSL2+)
- Wi-Fi (IEEE 802.11b/g/n)
- USB Backup/Restore Configuration
- Networking
  - IPv4/IPv6 Dual Stack and DS-Lite
  - NAT/PAT
  - Статическая/динамическая маршрутизация
  - DHCP Client/Server
  - Динамическоеопределение DNS
- Безопасность
  - Stateful Packet Inspection (SPI)
  - Denial of Service (DOS) protection
  - Multiple VPN (IPSec, PPTP) pass-through

- Всетипыфильтрации(наосновеMACадреса, IPадреса, порта, протокола)

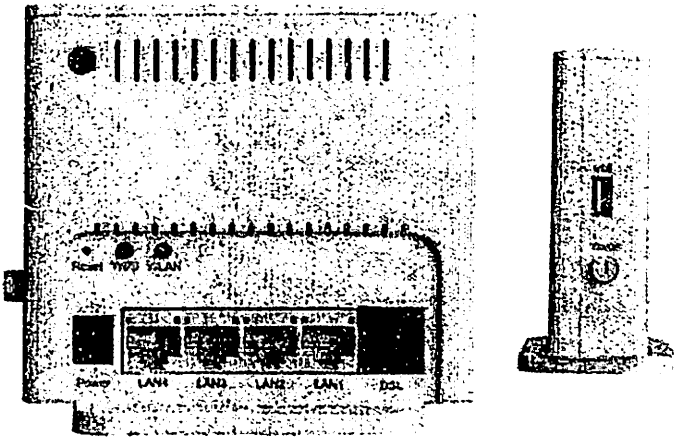


Рис.1.12. ВнешнийвидH108N

МодемH108N (рис.1.12.) обеспечивает:

- WAN: 1 порт RJ-11 ADSL
- LAN: 4 порта RJ-45 для FE
- USB: 1 USB 2.0 хост интерфейс
- Wi-Fi: 802.11b/g/n (2x2)
- WLAN, WPS Reset

ТерминалыVoIP

В учебной сети широкополосного доступа университета используются два типа терминалов.

HuaweiEchoLifeMC820c

Приведен на рис.1.13, 1.14 и обеспечивает выполнение следующих функций:

• Совершать и принимать видео-звонки, IP-вызовов, и вызовы ТфОП

• Большие емкости для хранения контактов и звонков

До 400 контактов можно сохранить до 4 номеров могут быть сохранены для каждого контакта. Информация дя сохранения – набранные номера, принятые вызовы и пропущенные звонки.

• Функция управления группой

Вы можете создать до 20 групп и добавить контакты к разным группам.

• доступ к веб в одно касание (One-touchWebaccess)

• Воспроизведение потокового мультимедиа

На специальных веб-страницах Вы можете

режиме реального времени и программы по требованию.

Рис.1.13. Внешний вид MC820c

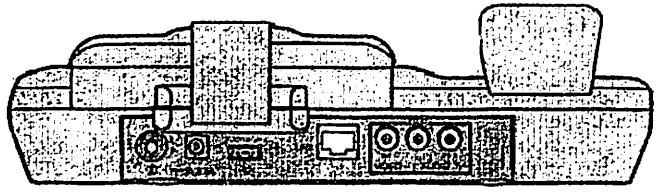


Рис.1.14. Задняя сторона MC820c

Таблица 1.4

Технические возможности MC820c

Стандарт	спецификация
Коммутикативный	SIP 2.0
Видео формат	H.263, H.263+, H264
Аудио формат	G.711A и G.711μ
Сетевые стандарты	TCP/IP, UDP, RTP, RTCP, DHCP, Telnet, DNS, PPPoE, HTTP, SNTP, RTSP

HuaweiMC850 MediaPhone

Приведённарис. 1.15, 1.16, предоставляетследующиевозможности:

- Приёмиинициированиевидео- иаудио- IP вызовов
- Функции цифровоефото
- Web browsing
- Потоковое видео

- Записьипроигрываниемультимедиафайловформатов MP4, MP3, 3GP, WMA и WMV
- переносная телефонная трубка
- накопители большой ёмкости для хранения контактов и записей о вызовах
- широкополосный доступ к сети

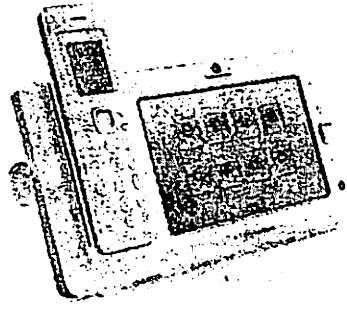


Рис.1.15. ВнешнийвидAppearance of the MC850

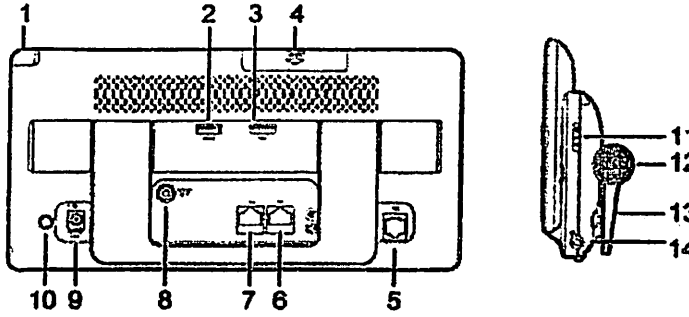


Рис.1.16. MC850 вид сзади и с боку

Таблица 1.5

MC850 вид сзади и с боку – описание компонентов

№	Description
1	Стилос для выбора элементов на экране и ввода информации
2,3	USB интерфейс
4	Слотдляподключения microSD card илиMultiMediaCard (MMC)
5	Телефонный интерфейс для подключения к ТфОП
6	Компьютерный интерфейс для подключения к сетевому интерфейсу компьютера
7	LANинтерфейсдляподключениякустройствам локальной сети
8	Интерфейсвидеовыхода для подключения к внешним устройствам
9	интерфейс для подключения к адаптеру питания
10	Кнопка питания
11	регулятор громкости

12	Стерео динамик
13	Support to adjust the inclination angle of the base unit
14	Headset Jack

Таблица 1.6

Подддерживаемые протоколы

Стандарт	Спецификации
Коммутикативный	SIP 2.0
Видео формат	H.263, H264
Аудио формат	G.711A и G.711μ
Сетевые стандарты	TCP/IP, UDP, RTP, RTCP, DHCP, Telnet, DNS, PPPoE, HTTP, SNTP, RTSP

Практическое занятие №2

ИЗУЧЕНИЕ ПРИНЦИПОВ РАБОТЫ ПРОТОКОЛА SIP ДЛЯ ОБЕСПЕЧЕНИЯ УСЛУГИ IP ТЕЛЕФОНИЯ

1. Цельисодержаниезанятия

Изучение структуры протокола SIP, структуры SIP заголовка, организации сессий между двумя пользователями.

2. Заданиекзанятию

Изучитьбазовую структуру SIP заголовка. Организации мультимедийной сессий между двумя пользователями для видео- или голосового вызова IP-телефонии (см.рис.2.1).

Вариант	Запрос команда SIP
1.	INVITE
2.	ACK
3.	BYE
4.	CANCEL
5.	OPTIONS
6.	REGISTER
7.	PRACK
8.	SUBSCRIBE
9.	NOTIFY
10.	PUBLISH
11.	INFO
12.	REFER
13.	MESSAGE
14.	UPDATE

3. Порядоквыполнения

1. Нарисоватьархитектурупротокола SIP
2. Изучитьтеоретическуючастьработы
3. Ответить на контрольные вопросы
4.Составить отчёт по работе

4. Содержаниеотчета

1.Краткое описание теоретической части
2. Блок-схемы устройств
3. Результаты настроек

5. Контрольныевопросы

1.Какие виды устройств участвуют в организации мультимедийной сессий между двумя пользователями? Краткоохарактеризуйтеих

2. Каковы основные функции протокола SIP?
3. В чём разница между SIP-терминалом и традиционным телефонным аппаратом?
4. Каково назначение прокси-сервера?
5. Каково назначение сервера переадресаций?
6. Каково назначение сервера определения местоположения?
7. Какие виды запросов используются для организации мультимедийной сессий между двумя пользователями для видео вызова?
8. Какие виды запросов используются для организации мультимедийной сессий между двумя пользователями для голосового вызова IP-телефонии?

6. Теоретическиесведения

Есть много приложений в Интернете, которые требуют создания и управления сеансом, где сессией является обмен данными между ассоциацией участников. Реализация этих приложений осложняется следующими факторами: пользователи могут перемещаться между конечными точками, они могут быть решены несколькими именами, и они могут общаться на нескольких разных носителях, иногда одновременно. Многочисленные протоколы являются источниками сообщений, которые несут различные формы мультимедийных данных в режиме реального времени, такие как голос, видео или текстовых сообщения. Протокол инициирования сеанса (SIP) работает совместно с этими протоколами, позволяя конечным точкам сети (которые называются агентами пользователя), узнать друг друга и договориться о характеристиках сессии. Для выявления потенциальных участников сессии и других функций, SIP дает возможность создания инфраструктуры сетевых узлов (так называемые прокси-сервера), к которым агенты пользователей могут отправлять запросы на регистрацию, приглашения на сессию, и другие запросы. SIP-это гибкий, универсальный инструмент для создания, изменения и прекращения сессий, который работает независимо от используемых протоколов транспортного уровня и от типа сеанса, который создается.

Протокол SIP - это протокол сигнализации, который для создания сессии соединения между двумя или более конечными точками IP-сети. Эти конечные точки могут быть IP-телефоны, клиенты обмена мгновенными сообщениями, или совместной конференции мультимедиа приложения.

SIP-это протокол управления уровня приложений, с помощью которого можно установить, внести изменения и завершить мультимедийные сеансы связи (конференции), такие как звонки через Интернет-телефонию. SIP также может предложить участникам уже существующих сессий, таких как конференций, рассылки. Средства массовой информации могут быть добавлены (или удалены от) существующей сессии. Протокол прозрачно поддерживает сопоставление имен и перенаправление услуг, поддерживает личную мобильность - пользователи могут сохранять единый внешний идентификатор, независимо от их расположения в сети.

Примерструктурыпротокола SIP

Полностью структура протокола SIP описана в RFC 3261.

Самый нижний слой-это транспортный уровень. Он определяет, как клиент посылает запросы и принимает ответы и как сервер получает запросы и отправляет ответы по сети. Все элементы SIP содержать транспортный уровень.

Второй слой называется уровнем транзакции (Transactionlayer). Транзакция-это запрос, отправленный клиентом транзакции (с помощью транспортного уровня) к серверу, а также все ответы на запрос, отправленные от сервера клиенту. Любые запросы, которые клиент агента пользователя (UAC) осуществляет, проходит через серию операций. Прокси-сервер без сохранения состояния (statelessproxy) не содержит уровня транзакций.

Уровень выше уровня транзакции называется пользователем транзакции (TransactionUserTU). Каждый из объектов SIP, за исключением Прокси-сервера без сохранения состояния, является пользователем транзакции.

На приведён рис.2.1 отказ в обслуживании первого запроса INVITE, затем действительный запрос INVITE, проанализируем содержимое запроса ACK для этих двух ситуаций. Предполагается, что оба прокси сервера Proxy 1 и Proxy 3 являются прокси-серверами с сохранением состояния (stateful).

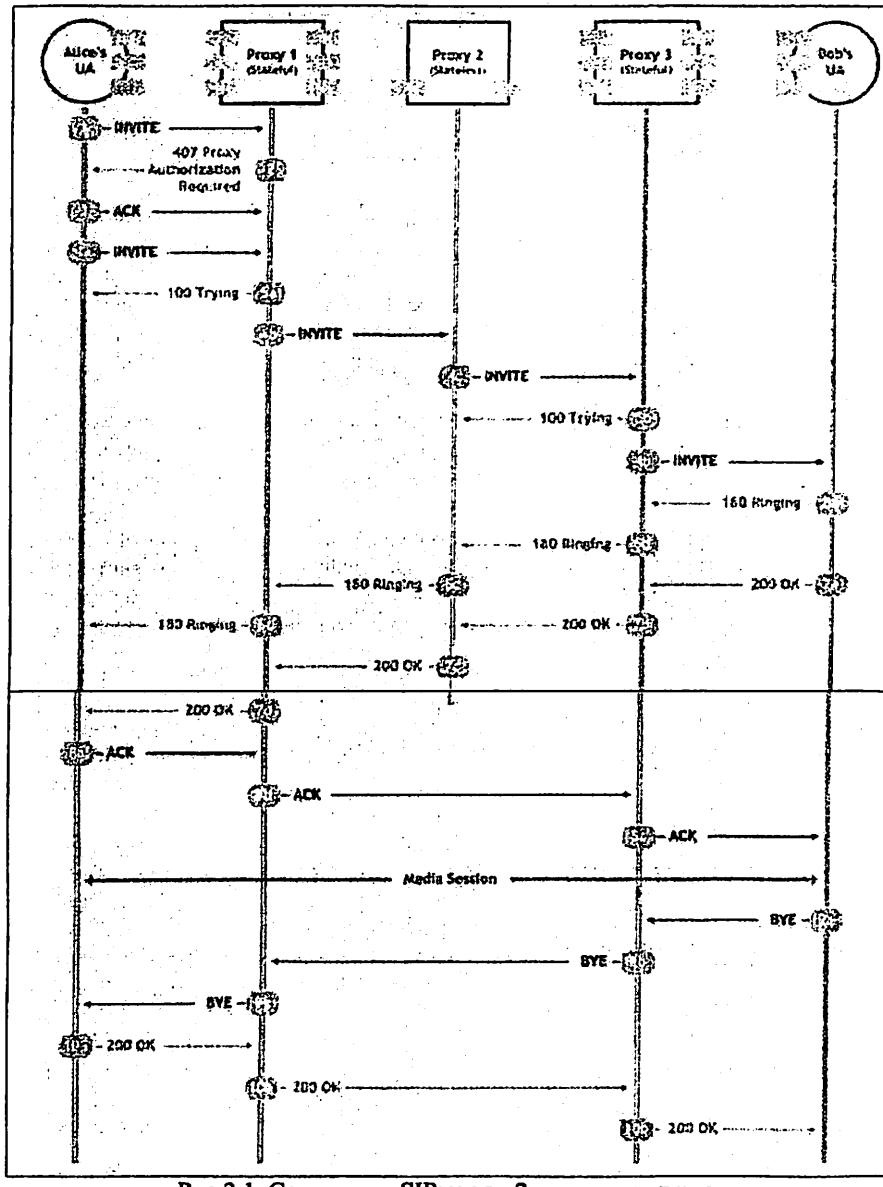


Рис.2.1. СоединениеSIPмежду 2 пользователями

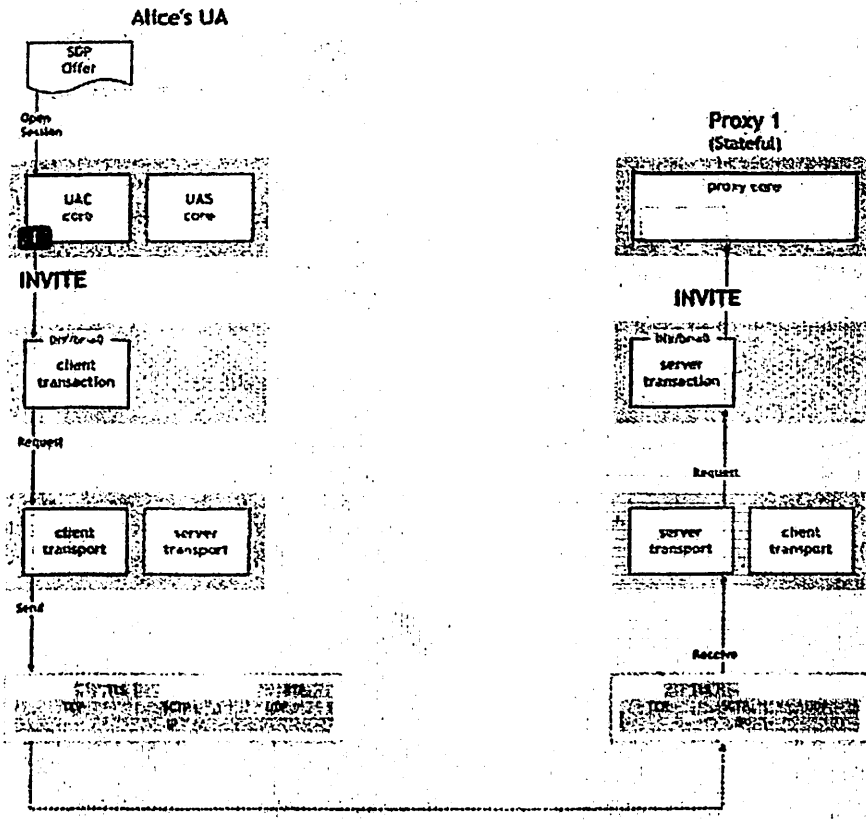


Рис.2.2. Инициирование вызова на прокси сервере

ДействиянаUAинициаторе:

- The UAC (User Agent Client) TU:
  - Создаётпервоначальныйзапрос INVITE;
  - СоздаётновуюклиентскуютранзакциюИ (науровнетранзакций) ипосылаетсообщениеINVITE, добавляякнемуIP адрес, порт услуги.
- НоваяклиентскаятранзакцияИ "INVITE" (состояние= «вызывающий» state="calling") идентифицируетсяCSeqвполезаголовкаипараметром "branch" вполеVia. ТаймерT1 запускается (еслиUDP), преждечемпередатьзапроснатранспортный уровень.
- Клиентский транспортный уровень (ClientTransport), перед отправкой запроса, вставляет 'sent-by' («отправили») на параметр Via в поле заголовка.

Действия наProxy 1:

• После получения запроса, ServerTransport, проверяя параметр'sent-by' в поле Via заголовка, сравнивает его с соответствующей транзакцией сервера и добавляет параметр "received" ("получил").

• Новаясервернаятранзакция "INVITE"(состояние="вобработке" state="proceeding") создаетсянапрокси сервере ядра.СерверТранзакциипередаетзапросINVITEнаTUивключаеттаймер 200мснаожиданиеответа 100 Trying.

• Прокси сервер ядра сначала проверяет валидностьзапросаINVITE. Он не может проверить подлинность отправителя, потому что нет данных. Он отказывает в обслуживании, отправив ответ в 407 ProxyAuthenticationRequired (407 требуется проверка подлинности прокси-сервера).

Обмен запросами и их маршрутизация

Диалог – это связь точка-точка между двумя агентами пользователей. Он представляет контекст, который облегчает последовательность обмена сообщениями между агентами пользователей и правильной маршрутизации запросов между ними. Следующая последовательность цифр иллюстрирует создание диалога, процесс обработки запросов во время этого диалога, и прекращение диалога.

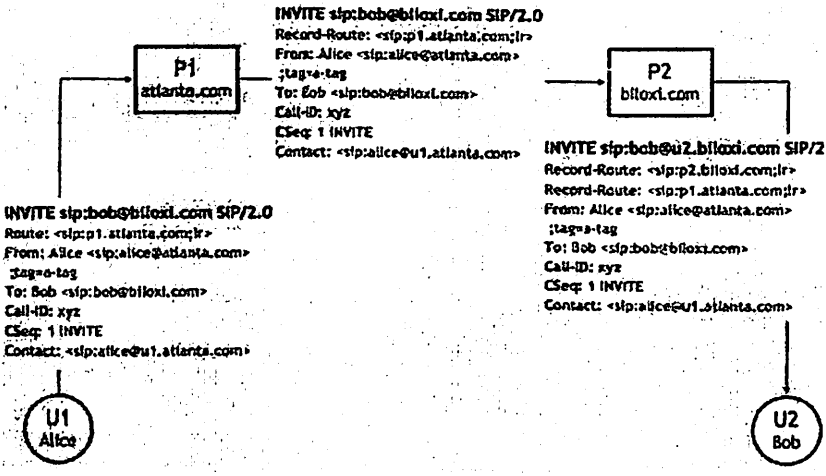


Рис.2.3.СигналINVITE впротоколе SIP

U1: генерируетзапросINVITE;

– DNSпроцедурыдляэтогоURIдляопределения, кудаотправлятьзапрос.

P1: проверяет запрос-URI (sip:bob@biloxi.com) и не меняет его, потому что он не несет ответственности за ресурсы, указанные в этом URI;

– видит, что это первое значение в поле заголовка маршрута, поэтому он

удаляет это значение;
– добавляет значение маршрута в поле заголовка;
– направляет запрос к ресурсу, указанному в заявке- URI (заданному маршруту в настоящее время пуст) путем применения процедуры DNS.

P2: проверяет запрос-URI: он отвечает за "biloxi.com" так он работает на сервере определения местоположения (locationservice) и переписывает запрос-URI (sip:bob@u2.biloxi.com);
– добавляет значение маршрута в поле заголовка;
– направляет запрос к ресурсу, указанной в заявке- URI (заданному маршруту пусто) путем применения процедуры DNS.

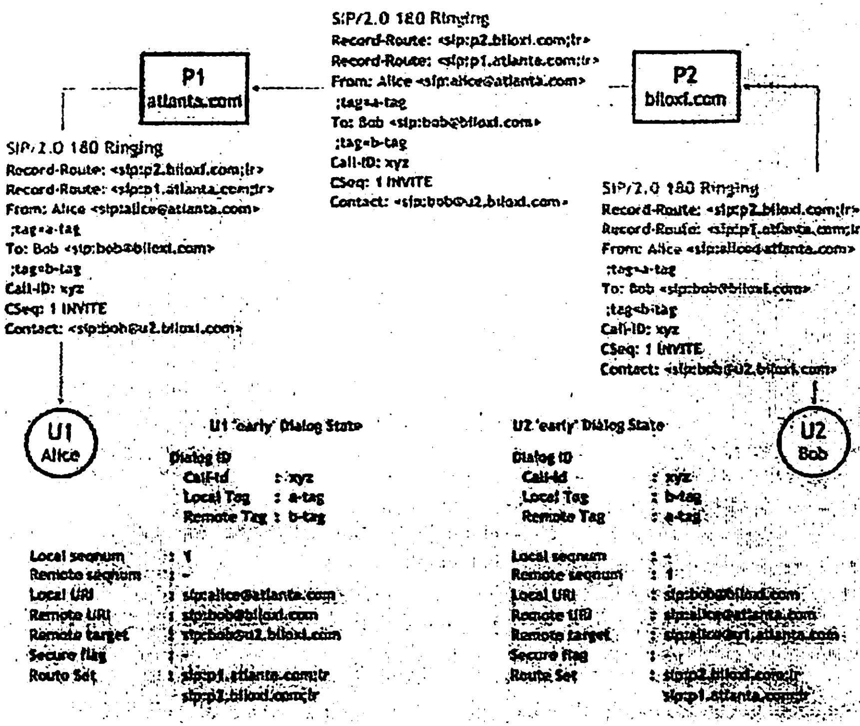


Рис.2.4. Ответ 180 Ringing

U2:- создает “ранний” диалогпосредствомответасвременнымответом, обладающимтегом “To”;
– копирует все заголовки Record-Route из запроса в ответ;
– добавляет поле заголовка Contact в ответ;
– создаетсостояниедиалога:
– набор маршрутов заносится в список URI, находящийся в полях

заголовка Record-Route, из запросов, принятого корректно и с сохранением всех параметров URI;
– удаленный пункт назначения задается в URIиз поля заголовка Contact в запросе;
– номер удаленной последовательность равен значению номера последовательности в поле заголовка CSeqзапроса;
– номерлокальнойпоследовательностипустой;
– компонент идентификатора вызова IDдиалога равен величине поля Call-IDв запросе
– компонент локального тэга IDдиалога равен тэгу в поле "To" ответа на запрос;
– компонент удаленного тэга IDдиалога равен тэгу из поля "From" запроса;
– удаленный URIравен URIв поле "From";
– локальный URIравен URIв поле "To".
– посылает ответ 180, используя поля заголовка Via (не показан)

P2: - передает ответ 180, используя поля заголовка Via (не показан).

P1: - передает ответ 180, используя поля заголовка Via (не показан).

U1: - устанавливает "ранний" диалог, когда получает временной ответ с тэгом "To";
– создаетсостояниедиалога:
– набор маршрутов задан в списке URI, находящемся в полях заголовка Record-Route в ответе, принятом в обратном направлении с сохранением всех параметров URI;
– удаленный пункт назначения задается в URI из поля заголовка Contactответа;
– номер локальной последовательности равен значению номера последовательности в поля заголовка CSeqзапроса;
– номерудаленнойпоследовательностипустой;
– компонент идентификатора вызова IDдиалога равен величине поля Call-IDв запросе;
– компонент локального тэга IDдиалога равен тэгу в поле "From" в запросе;
– компонент удаленного тэга IDдиалога равен тэгу в поле "To" в ответе;
– удаленный URIравен URIв поле "To";
– локальныйURIравен URIв поле "From".

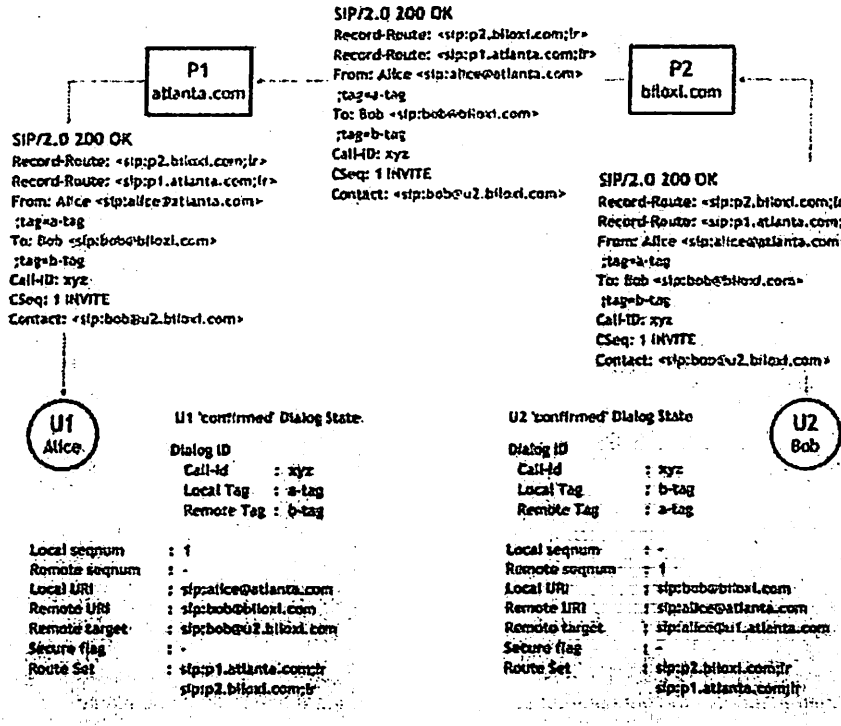


Рис.2.4 Сообщение 200 OK

U2 - подтверждает диалог посредство передачи финального ответа на запрос INVITE;

– передает ответ 200, используя поля заголовка Via (не показан).

P2: – передает ответ 200, используя поля заголовка Via (не показан).

P1: – передает ответ 200, используя поля заголовка Via (не показан).

U1:– меняет состояние диалога на "подтвержденный", когда получает финальный ответ на запрос INVITE.

U1 – генерирует запрос ACK, используя множество компонентов состояния, хранимого как часть диалога:

– URIв поле "To" запроса равно удаленному URIиз состояния диалога;

– тэг в поле заголовка "To" запроса равен удаленному тэгу IDдиалога;

– URIFromзапроса равен локальному URIиз состояния диалога;

– тэг поля заголовка "From" запроса равен локальному тэгу IDдиалога;

– Call-IDзапроса равен Call-IDдиалога;

– использует удаленный пункт назначения и набор маршрутов для построения Request-URIи поля заголовка Routeзапроса:

–

набормаршрутовнепустойипервыйURIнаборамаршрутовсодержитпара

метрlr (looserouting, свободнаямаршрутизация): UACпомещает удаленный целевой URIв Request-URIи включает поле заголовка Route, содержащего значения набора маршрутов по порядку, включая все параметры;

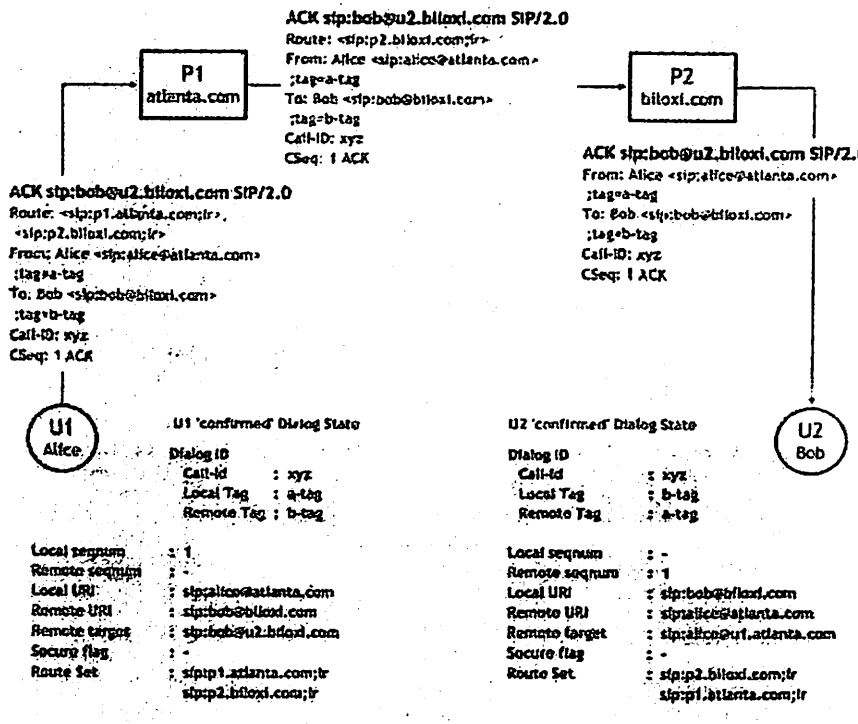


Рис.2.6. сообщение ACK

– заметка: если набор маршрутов был пуск, тогда UACвнесет удаленный целевой URIв Request-URIи не добавит поле заголовка Routeв запрос;

P1: - проверяетRequest-URI (sip:bob@u2.biloxi.com) и не меняет его потому, что он не несет ответственности за ресурсы, указанные в этом URI;

– замечает, что это первое значение в поле заголовка Route, поэтому он удаляет это значение;

– передает запрос в ресурс, указанный в самом верхнем поле заголовка Route, применяя процедуры DNS.

P2: - проверяет Request-URI: он не несет ответственности за "u2.biloxi.com" (он ответственный за "biloxi.com", а не "u2.biloxi.com"), поэтому он не меняет его;

– замечает, что это первое значение в поле заголовка Route, поэтому он удаляет это значение;

– передает запрос в ресурс, указанный в Request-URI (набор маршрутов

теперь пустой), применяя процедуры DNS.

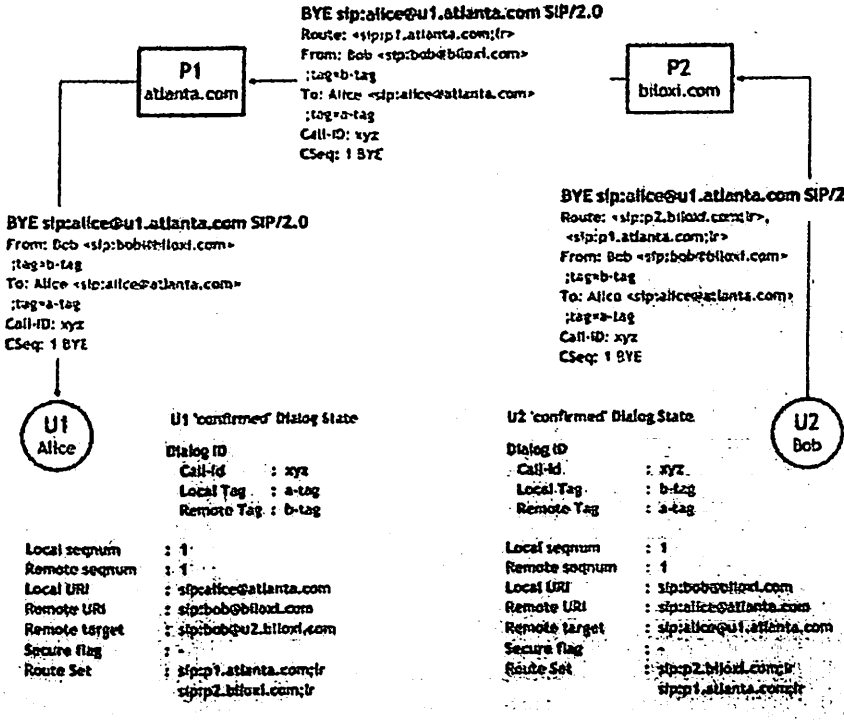


Рис.2.7 Сообщение BYE

U2: - генерирует запрос BYE, используя множество компонентов состояния, хранимого как часть диалога:

– URIв поле "To" запроса равно удаленному URIиз состояния диалога;
– тэг в поле заголовка "To" запроса равно удаленному тэгу IDдиалога;
– URIFromзапроса равен локальному URIиз состояния диалога;
– тэг в поле заголовка "From" запроса равен локальному тэгу IDдиалога;
– Call-IDзапроса равен Call-IDдиалога;
– использует удаленный пункт назначения и набор маршрутов для построения Request-URIи поля заголовка Routeзапроса:
–

набормаршрутовнепустойиперв ыйURIвнаборемаршрутовсодержитпараметрlr (looserouting, свободнаямаршрутизация): UACпомещает удаленый целевой URI в Request-URIи включает поле заголовка Route, содержащее значения набора маршрутов по порядку, включая все параметры;

– заметка: если набор маршрутов был пустой, тогда UACвнесет удалённый целевой URIв Request-URIи не добавит поле заголовка Routeв запрос;

P2: - проверяетRequest-URI (sip:alice@u1.atlanta.com) инеменяетегопотому, чтоонненесетответственностизаресурсы, указанныевэтомURI;

– замечает, что это первое значение в поле заголовка Route, поэтому он удаляет эту величину;

– передает запрос в ресурс, указанный в самом верхнем поле заголовка Route, применяя процедуры DNS.

P1: – проверяетRequest-URI: онненесетответственностиза "u1.atlanta.com" (он ответственный за "atlanta.com", а не "u1.atlanta.com"), поэтому он его не меняет;

– замечает, что это первое значение в поле заголовка Route, поэтому он удаляет эту величину;

– передает запрос в ресурс, указанный в самом верхнем поле заголовка Request-URI, применяя процедуры DNS.

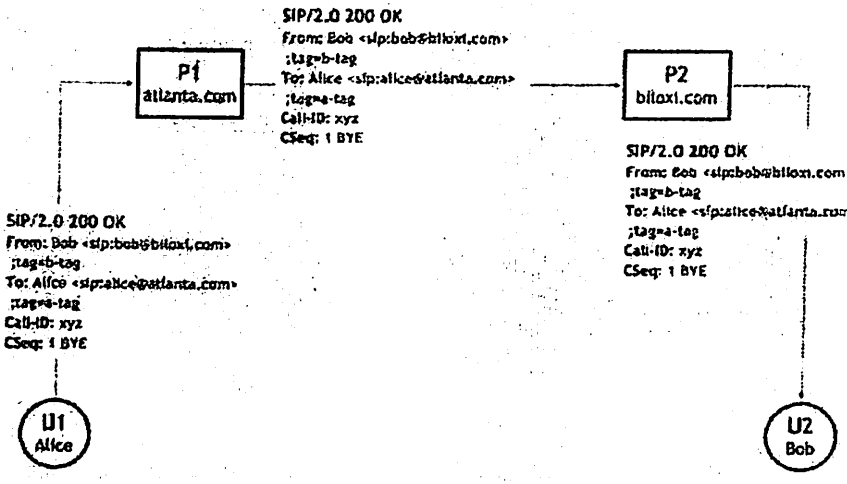


Fig. 2.8 BYEmessage

U1: – посылает ответ 200, используя поля заголовка Via (не показан).

P1: – передаетответ 200, используя поля заголовка Via (не показан).

P2: – передаетответ 200, используя поля заголовка Via (не показан).

Практическое занятие №3

НАСТРОЙКА МАРШРУТИЗАТОРА ЛОКАЛЬНОЙ СЕТИ С ПОМОЩЬЮ ПО CISCO PACKET TRACER

1. Цель и содержание занятия

Изучение структуры сети доступа с помощью ПО CiscoPacketTracer и конфигурирования устройств с помощью интерфейса командной строки.

2. Задание к занятию

Построить простейшую сеть доступа на основе маршрутизаторов в соответствии с рис.3.1. используя утилиту ping проверить связь между хостами.

Варианты заданий

вар	IP адрес сети доступа	IP default gateway	IP адреса между маршрутизаторами
0	192.168.0.0/30 192.168.0.4/30 192.168.0.8/30	192.168.0.1 192.168.0.5 192.168.0.9	R1 > R2 10.10.10.0/30 R1 > R3 10.10.10.4/30 R2 > R3 10.10.10.8/30
1	10.0.0.0/28 10.0.0.16/30 10.0.0.20/24	10.0.0.8 10.0.0.19 10.0.0.127	R1 > R2 1.1.1.0/29 R1 > R3 1.1.1.8/29 R2 > R3 1.1.1.16/30

3. Порядок выполнения

1. Изучить теоретическую часть работы
2. Выполнить практическую часть
3. Ответить на контрольные вопросы
4. Составить отчёт по работе

4. Содержание отчета

1. Краткое описание теоретической части
2. Блок-схемы устройств
3. Результаты настроек
1. Назначение
2. Сетевая модель построенная в ПО CiscoPacketTracer
3. Результаты утилиты ping каждого конечного узла
4. Заполненная управляющая таблица каждого маршрутизатора

5. Контрольныевопросы

1. Кратко охарактеризуйте устройства, используемые в модели локальной сети.
2. Каковы основные функции сетевого уровня в моделилокальной сети?
3. Какие сетевые протоколы используются в сети?
4. Напишите конфигурацию маршрутизатора.

5. Каким образом локальная сеть подключается к другим LAN?
6. Какие данные могут передаваться между двумя LAN?

6. Теоретическиесведения

CiscoPacketTracer– программа-симулятор для моделирования сети, которая позволяет студентам экспериментировать с поведением сети и получать ответы на вопросы "что если". В качестве неотъемлемой части сетевой Академии Cisco, ПО PacketTracer предоставляет моделирование, визуализацию, создание, оценку, а также возможности совместной работы и облегчает преподавание и изучение сложных понятий технологии локальных сетей.

ПОPacketTracer дополняет физическое оборудование в классе, позволяя студентам создавать сети с практически неограниченным количеством устройств, с целью получения практических навыков, обнаружения и устранения неполадок в сети.

Уровни	Протоколы, поддерживаемые CiscoPacketTracer
Прикладной	FTP, SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNTP, AAA, ISRVOIP, SCCP
Транспортный	TCP, UDP, алгоритм TCPNagle, IP фрагментация,RTP
Сетевой	BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSeq, RIPv1/v2/ng, Multi-area OSPF, EIGRP, Static Routing, Route Redistribution, Multilayer switching, L3QoS, NAT, CBAL, Zone-based policy firewall
Сетевого интерфейса/ доступа	Ethernet 802.3, 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.11q, PAgP, L2QoS, SLARP, Simple WEP, WPA, EAP

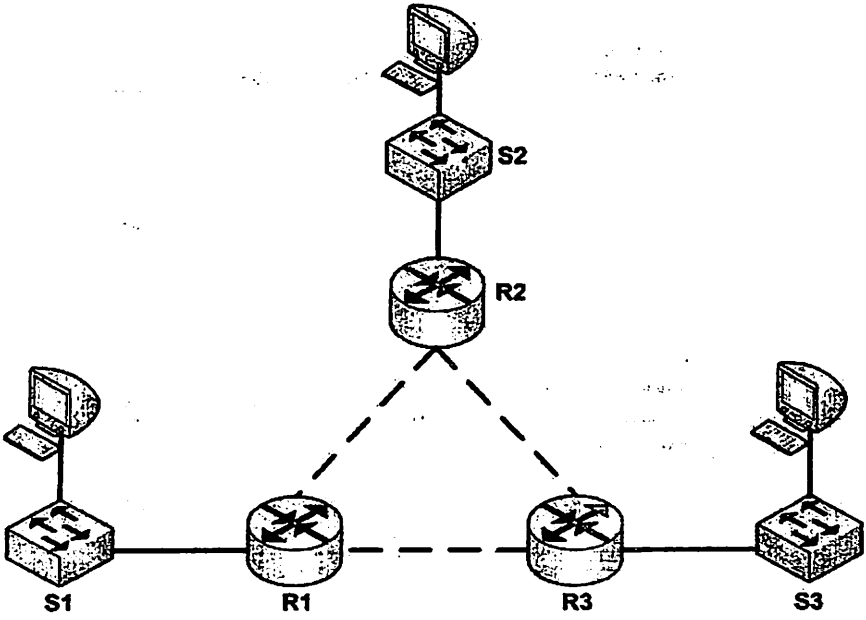


Рис.3.1. Модель сети

Руководство по использованию

Вданнойработеиспользуемустройство Cisco 2911 в качестве маршрутизатора, CiscoCatalyst 2960 в качествеLANswitchкомпьютеры Laptop в качестве оконеяных устройств.

Данныйтипустройствдолженподсоединятьсяспомощьюкабеля «витаяпара»(*CopperCross-Over*cable) черезEthernetинтерфейс или через*CopperStraight-Through*cable.

Прежде чем мы сможем установить коммуникативную связь между хостами (см.рис.3.2).

- сделайтеClick на компьютере/ноутбуке
- Выберите вкладку рабочий стол(desktop)
- Выберитеконфигурацию IP
- Настроить IP-адрес, маску подсети и шлюз по умолчанию в соответствии с вашим вариантом

IP-адрес R1	маску подсети	шлюз по умолчанию
192.168.0.1	225.225.0.0	192.168.0.17
192.168.0.2	225.225.0.0	192.168.0.21

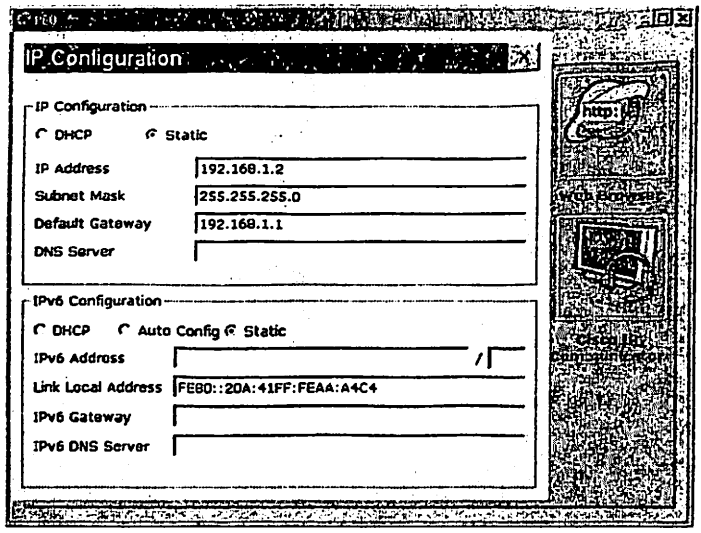


Рис.3.2. Конфигурирование хоста

Следующий шаг-настроить все маршрутизаторы в вашей сети (Рис. 3.3). Нам нужно определить IP-адреса всех активных интерфейсов и создать статические маршруты к сетям доступа.

- сделайте Click на маршрутизаторе
- Выберите вкладку config
- Настроить все интерфейсы (определить IP-адреса и маски подсети в соответствии с вашим вариантом)

Примечание: один из интерфейсов шлюза доступа к сети

- Создать статические маршруты к другим сетям доступа
  - Network– IP-адрес удаленного сетевого доступа
  - Mask– маска подсети удаленного доступа к сети
  - NextHop – IP-адрес соседнего маршрутизатора следующего перехода интерфейс

Примечание: для удобства настройки в заметках интерфейсов IP адрес и переключиться на показ порта надписи (параметры > настройки > всегда показывать порт ярлыки)

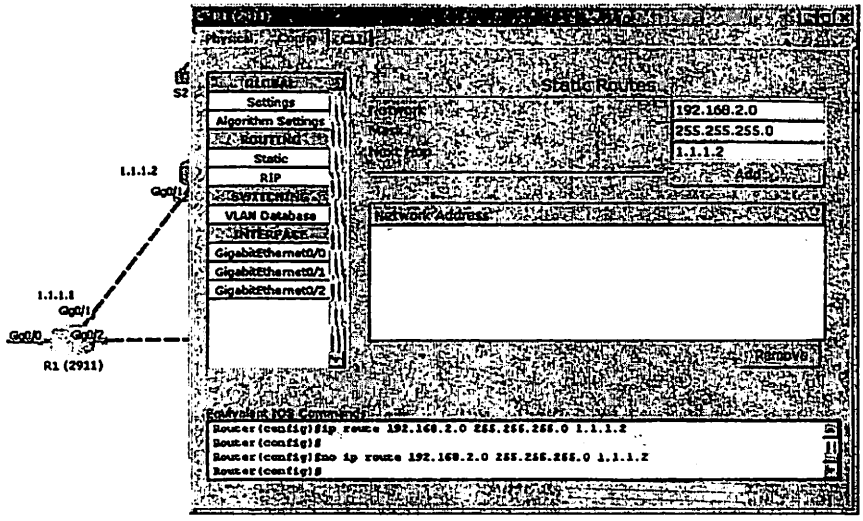


Рис.3.2. Конфигурированиемаршрутизатора

Используяутилитуpingпроверитьсвязьмеждухостами(рис.3.3).

- сделайте ClickPC/Laptop
- выберитевкладку*desktop*
- запустите*command promt*
- выполните команду Pingот каждого хоста к каждому из его хостов-соседей
  (ping *host_ip_address*)

Таблицакоманд

Операция	Синтаксис команды
Выбор интерфейса	
Конфигурирование IP адреса и масуи подсети на интерфейсе	
Включить (Switch ON) интерфейс	
Создать статический маршрут	

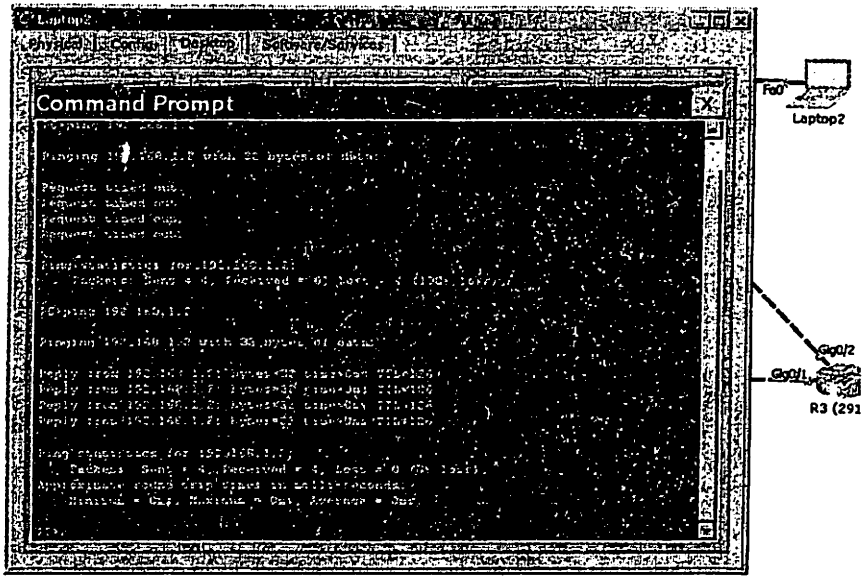


Рис.3.3. Использование утилитыPing

Практическое занятие №4

НАСТРОЙКА IP ТЕЛЕФОНОВ С ПОМОЩЬЮ ПО CISCO PACKET TRACER

4.1. Цель работы

Изучить построение сети IP-телефонии с помощью программыCiscoPacketTracer и настройка IP-телефонов, установление связи между ними и проверка связи.

4.2. Задание

При подготовке к лабораторной работе студент должен знать:

- Принципы построения сети IP;
- Назначение и применение устройств применяемых в сетях IP;
- Иметь навыки работы с программным обеспечением Ciscopackettracer;
- Иметь знания по IP адресации и классам IP.

Вариант	Количество Телефонов	Телефонларрақамлари
1	5	212,213,214,215,216
2	6	4861,4862,4863,4864,4865,4866
3	8	2221488-2221496
4	7	111,222,333,444,555,666,777
5	5	15660-15664
6	6	373-378
7	8	2368415-2388422

4.3. Контрольные вопросы

1. Назначение IP-телефонов
2. Из каких элементов состоит сеть IP-телефонии
3. Какие классы IP адресов вы знаете.
4. Назначение программного обеспечения CiscoPacketTracer.
5. Настройка IP-телефонов

4.4. Порядок выполнения работы

На рабочем столе настройте программное обеспечение *Ciscopackettracer*(рис.1.)

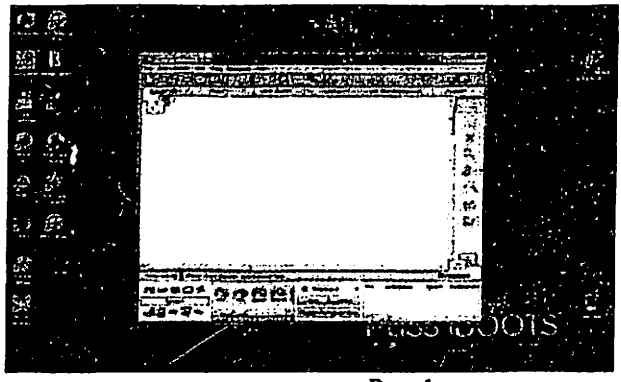


Рис. 1.

2. В нижней части меню Ciscopackettracer выбираем отдел Routers.После этого на рабочий стол устанавливаем роутер 2811(рис.2.).

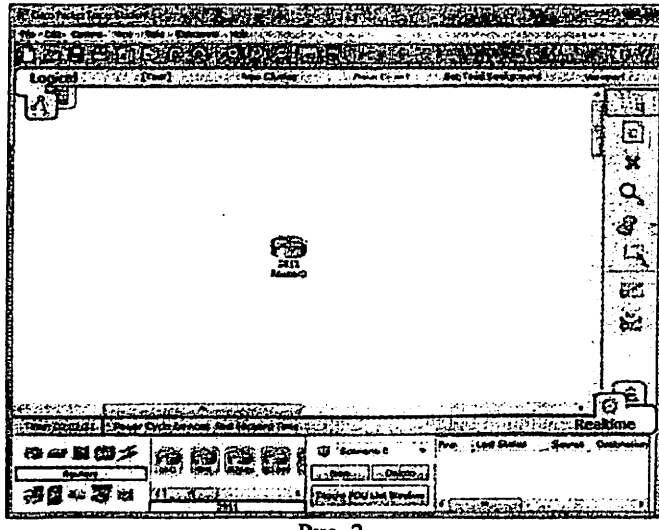


Рис. 2.

3. После этого на рабочий стол устанавливаем 7 шт. IPphoneиз отдела Enddevices и коммутаторы 2960 из отдела Switches (рис.3).

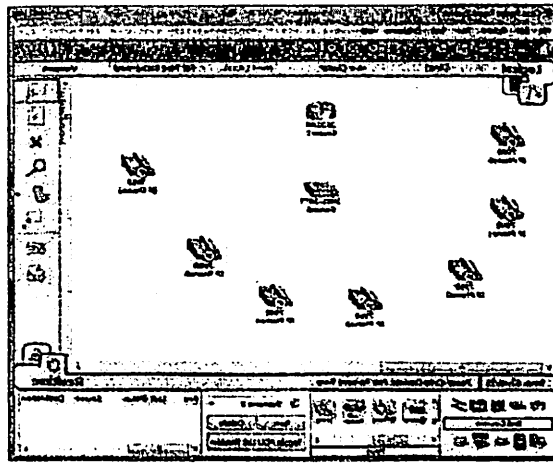


Рис.3.

4. Все устройства подключаются между собой выбранными кабелями из отдела ***Connections***. Коммутатор, роутер, IP-телефон подключаются кабелем ***Copper-straight-trough***. При подключениинеобходимо обратить внимание на последовательность соединяемых портов. Кабель подключается к порту ***Switch***IP-телефона.

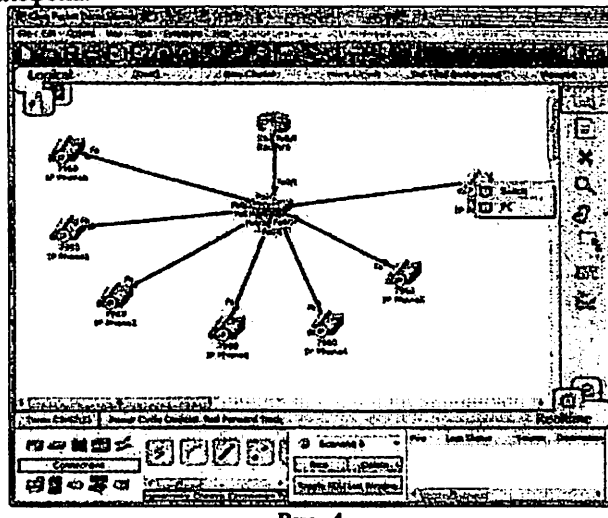


Рис. 4.

5. Теперь к каждому IP телефону подключаем питание. Для этого 2 раза нажимаем на IP телефон. Как показано на рисунке соединяем к телефону устройство питания нижней части справа.

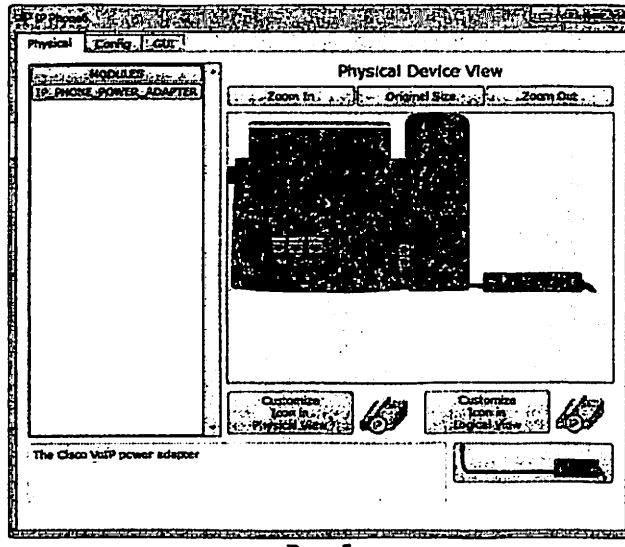


Рис. 5.

6. После этого загораются зеленым цветом все порты IP-телефонов и порты соединения IP-телефонов с коммутатором. (Рис.6)

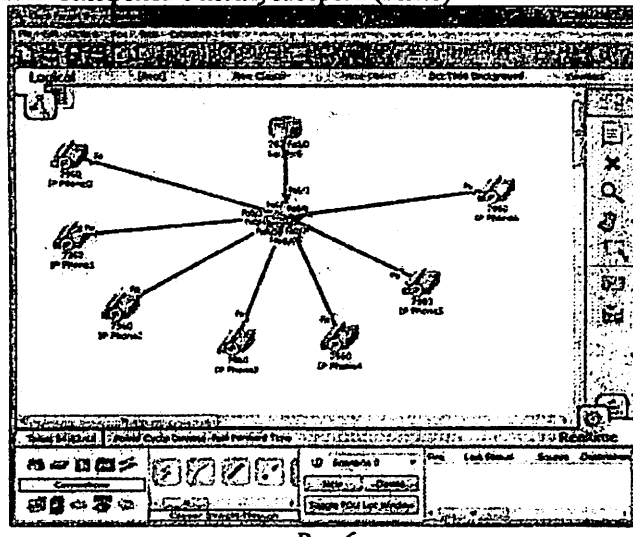


Рис.6

7. Теперь перейдем к настройке коммутатора. Для этого мы нажимаем два раза на коммутатор и верхнем меню выбираем меню CLI. (рис.7.)

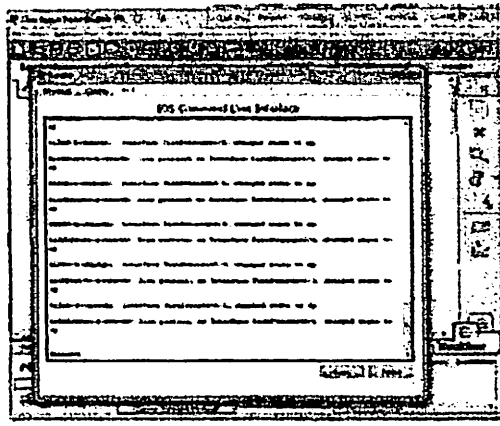


Рис.7.

8. Для настройки коммутатора начинаем писать команды. Слелующие команды набираем в окне коммутатора:

Switch>enable
Switch#configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 1
Switch(config-if-range)#exitit
Switch(config)#exitit
Switch(config)#write

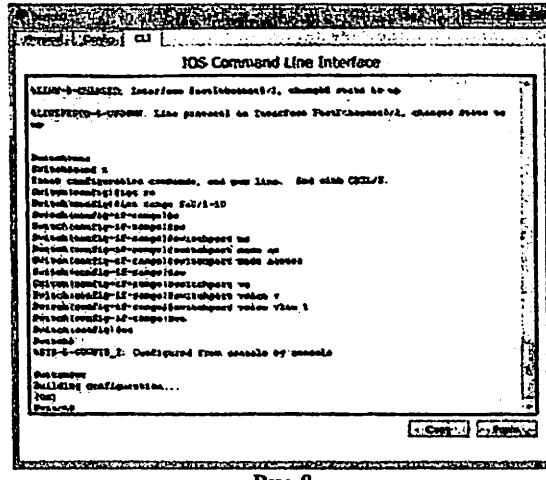


Рис.8.

9. После этого переходим к настройке Routera. Для этого нажимаем два раза на Router,выбираем в верхнем меню CLIинабираемследующиекоманды:

```
Continue with configuration dialog? [yes/no]: no
Router>enable
Router#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ipdhcp pool voice
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#exit
Router(config)#ipdhcp pool voice
Router(dhcp-config)#option 150 ip 192.168.1.1
Router(dhcp-config)#exit
Router(config)#telephony-service
Router(config-telephony)#max-dn 7
Router(config-telephony)#max-ephones 7
Router(config-telephony)#ip source-address 192.168.1.1 port 2000
Router(config-telephony)#auto assign 1 to 7
Router(config-telephony)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 111
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 222
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 3
Router(config-ephone-dn)#number 333
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 4
Router(config-ephone-dn)#number 444
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 4
Router(config-ephone-dn)#number 555
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 5
Router(config-ephone-dn)#number 666
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 6
Router(config-ephone-dn)#number 777
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 7
```

Router(config-ephone-dn)#number 888
Router(config-ephone-dn)#exit
Router(config)#exit
Router(config)#write

10. После этого два раза нажимаем на телефон и переходим к меню GUI. В верхнем углу IP телефона написан его номер

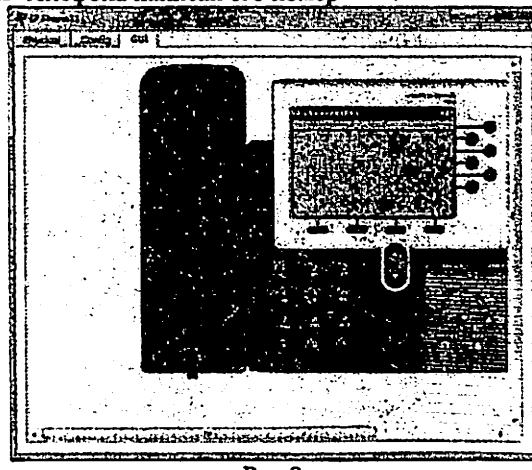


Рис.9.

11. Подняв трубку звоним другому IPтелефону. Например: звоним на номер 111.

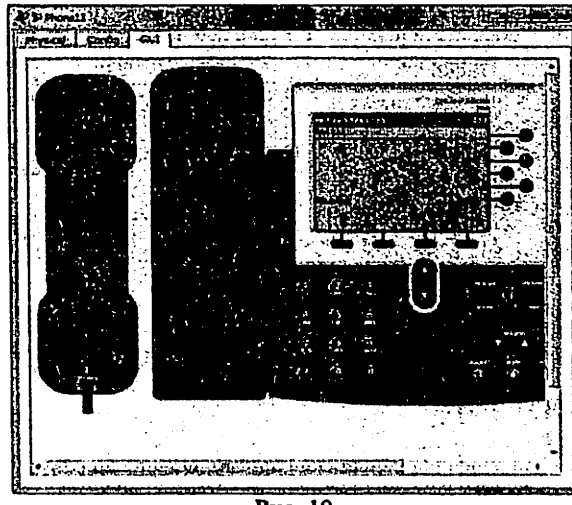


Рис. 10.

12. После этого входим в меню GUI вызываемого телефона. У него будет звенеть телефон.

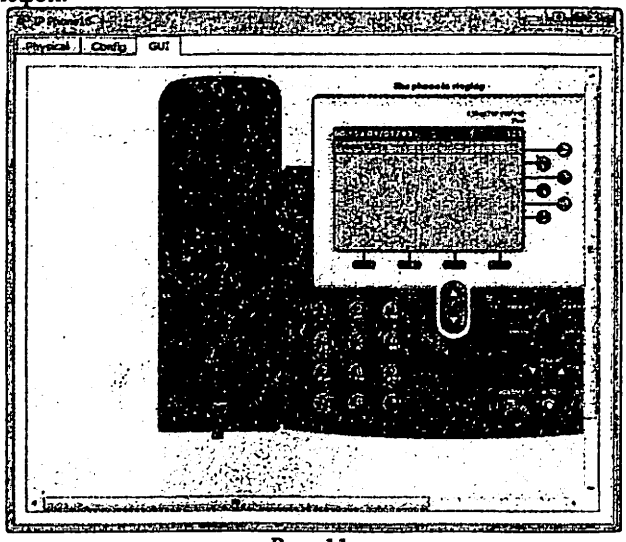


Рис. 11.

13. Подняв трубку второго телефона устанавливается связь между двумя телефонами.

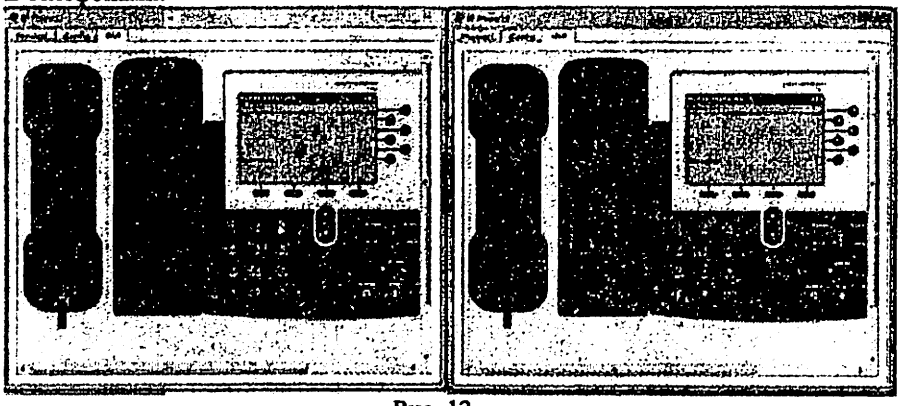


Рис. 12.

14. Положив одну из трубок связь заканчивается.

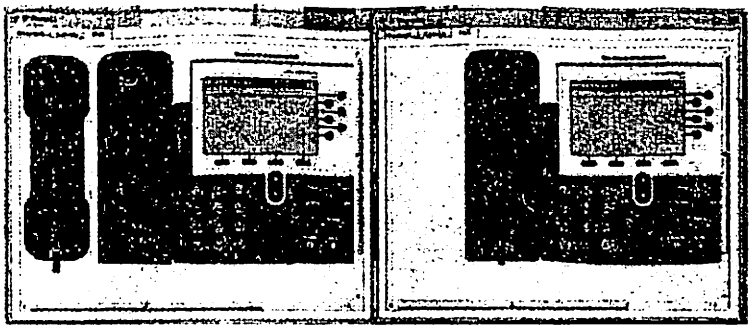


Рис. 13.

Лабораторная работа № 5

НАСТРОЙКА УСЛУГИ TRIPLEPLAY С ПОМОЩЬЮ ПО CISCO PACKET TRACER

1. Цель работы

Настроить модель сети для предоставления услуги Triple Play (доступ в интернет,телефония, IPTV) в программе CiscoPacketTracer.

2. Задание к работе

1.При подготовке к практическому занятию изучить вопросы:

- назначение и состав услуг TriplePlay
- схемы реализация услуг TriplePlay на основе IP сети

2. Построить сеть для реализации услуг TriplePlay как показано на рис.5.1. Настроить элементы сети.

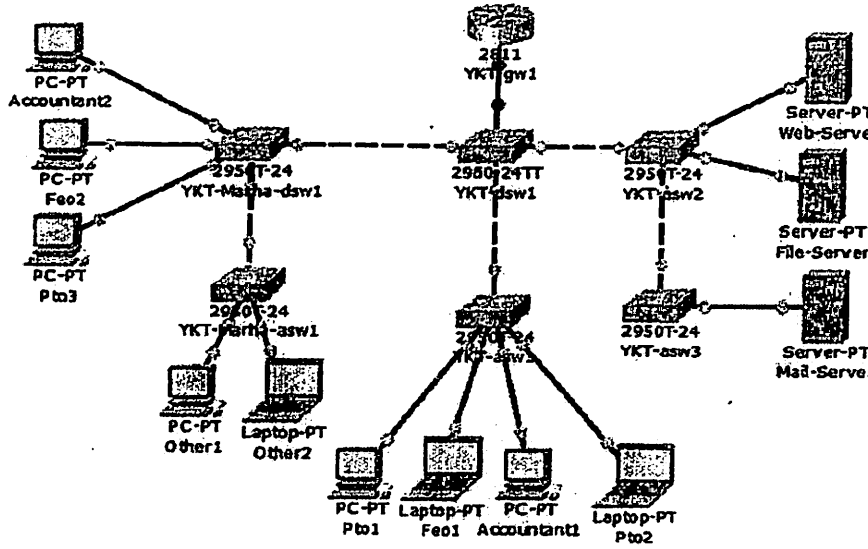


Рис.5.1. Пример сети

3. Содержание отчета

1. Теоретическая схема сети, выполненная в тетради согласно варианту
2. Сетевая модель, построенная в ПО CiscoPacketTracer
3. Ответы на контрольные вопросы

4. Контрольные вопросы

1. Что обозначает термин TriplePlay?
2. Какие услуги входят в состав TriplePlay?
3. Как классифицируются виды услуг TriplePlay?
4. Каким образом происходит реализация услуги «высокоскоростной доступ в интернет»?
5. Какреализуется услуга«телефонная связь»?
6. Что входит в состав понятия «широкополосные мультимедийные приложения»?
7. Каково назначение VoIP-платформ?
8. Каково назначение DSLAM?
9. Каково назначение BRAS?
10. Каково назначение AAA-сервера?
11. Каково назначениеDNS/ENUM-сервера?
12. Что входит в понятие ТВ-контент?
13. Что показывает физический адрес?
14. Что показывает сетевой адрес?
15. Какие протоколы входят в состав прикладного уровня?
16. Какие устройства принадлежат прикладному уровню?
17. Какие протоколы входят в состав транспортного уровня?
18. Какие устройства принадлежат транспортному уровню?
19. Какие протоколы входят в состав сетевого уровня?
20. Какие устройства принадлежат сетевому уровню?
21. Какие протоколы входят в состав уровня сетевого интерфейса?
22. Какие устройства принадлежат уровню сетевого интерфейса?

5.Литература

1. Chris Hellberg, Dylan Greene, Truman Boyes. Broadband Network Architectures designing and deploying Triple-play services. Pearson Education 2007.
2. CISCO Packet Tracer – Сетевая академия. – официальный сайт.– URL:https://www.netacad.com/ web/about-us/cisco-packet-tracer.

6.Порядок выполнения виртуальной работы

НастройкаVLAN (локальной сети учета) состоит из трёх этапов:

1. создание модели сети, т.е. установка устройств на основе топологии, приведенной на рис.5.1.
2. создание VLAN.
3. настройка портов доступа и соединительных линий для обеспечения услуги

6.1.Создание сети

1.В рабочей области CiscoPacketTracer Установить маршрутизатор2811 из панели «Routers» (см.рис.5.2).

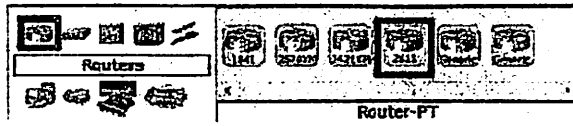


Рис.5.2. Выбормаршрутизатора

2.ВыберитеSwitch модели 2960(см.рис.5.3).

Рис.5.3. Выбор коммутатора

3.Подключите Switchк сети, используя медный кабель CopperStraightThrough. Требуемый кабель выбирается из панели «Соединения» (см.рис.5.4).

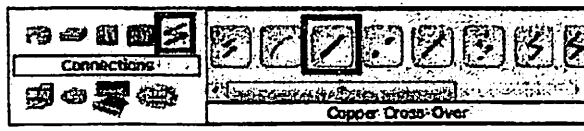


Рис.5.4. Выбор кабеля

4.Чтобы подключить кабель к устройству, нажмите маршрутизатор левой кнопкой мыши и выберите нужный порт. Тип и номер порта показаны в таблице 5.1. Соедините коммутатор с маршрутизатором. Для этого переместите левую кнопку мыши в коммутатор и выберите порт, показанный в таблице 5.1.

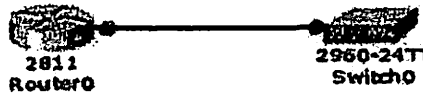


Рис.5.5.Соединение коммутатора с маршрутизатором

5.Переименуйте устройство в соответствии с таблицей 5.1 (2 и 3 колонки)

6.Подключите коммутатор 2950T к другим 5 распределительным устройствам и переименуйте устройства в соответствии с таблицей 5.1, как показано на рис.5.6.

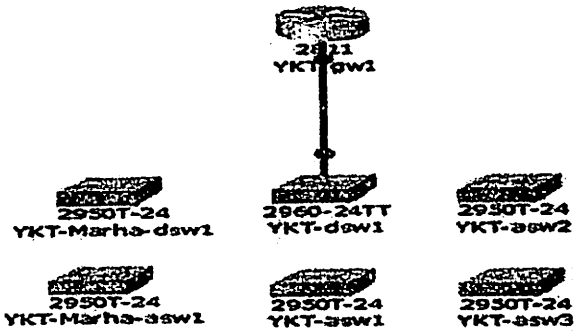


Рис.5.6.Подключение пяти коммутаторов

7.Используя кабель CopperCross-over, подключите порт YKT-dsw1 коммутатора к порту YKT-asw1 коммутатора. Номера портов показаны в таблице 5.1 (см.рис.5.7).

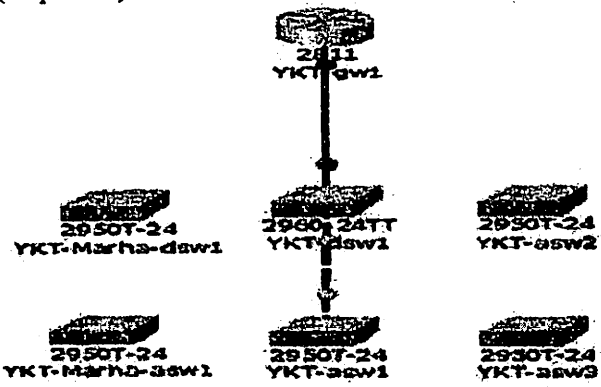


Рис.5.7. Соединение YKT-asw1

8.Переключите Подключение к YKT-asw1 (EndDevices). Для этого выберите 2PC-PT и 2Laptop-PT с EndDevices в нижнем левом углу окна (см.рис.5.8).

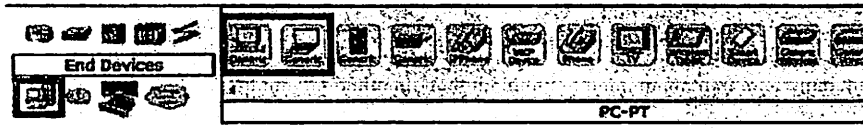


Рис.5.8. Выбор абонентских устройств

9.Используйте емкости CopperStraight-Through. Таблица 5.1,столбцы 3, 4 и 5

(см.рис.5.9)

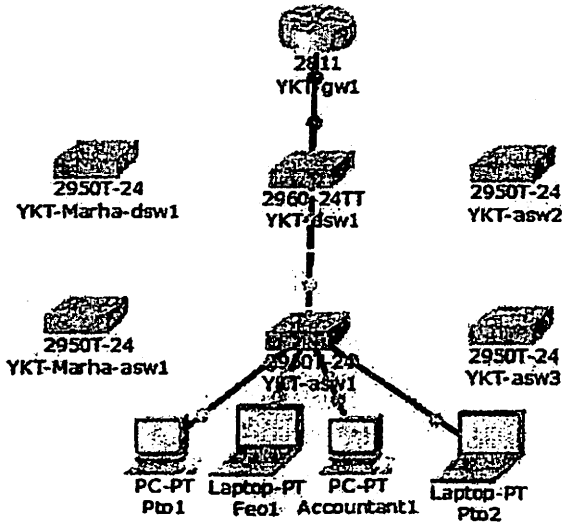


Рис.5.9. Использование емкостиCopperStraightThrough

10.Установите и настройте остальные устройства из таблицы 5.1. Получиться сеть, показанная на рис.5.10.

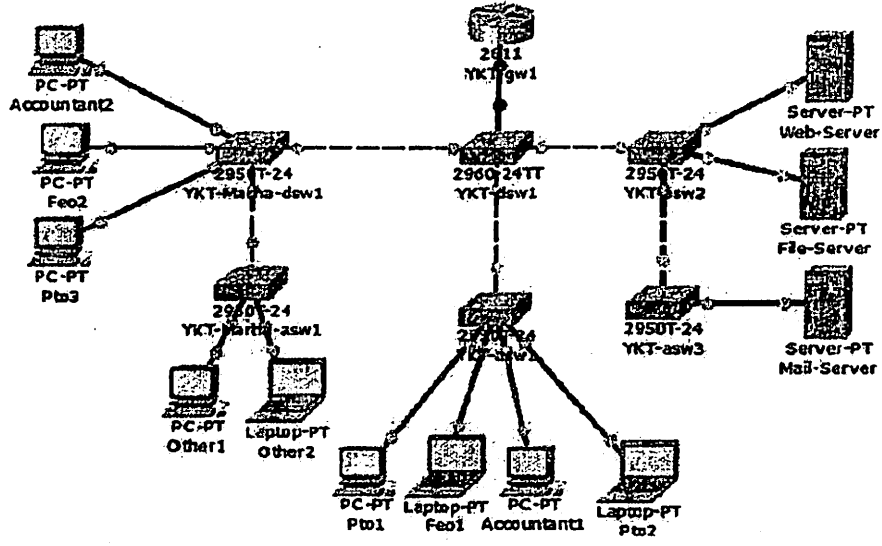


Рис.5.10. Полная топология сети

6.2.Создание VLAN

1.Откройте интерфейс командной строки IOS, переключившись на коммутатор (YKT-dsw1) и выбрав приложение CLI. Введите команду

Enable(Switch>enable)

мы перейдем к льготному режиму.

Наберите

Configureterminal (Switch#configureterminal)

длявходаврежимглобальныхнастроек.

(Switch(config)#hostnameYKT-dsw1) инастройте с помощью командой hostname (см.рис.5.11).

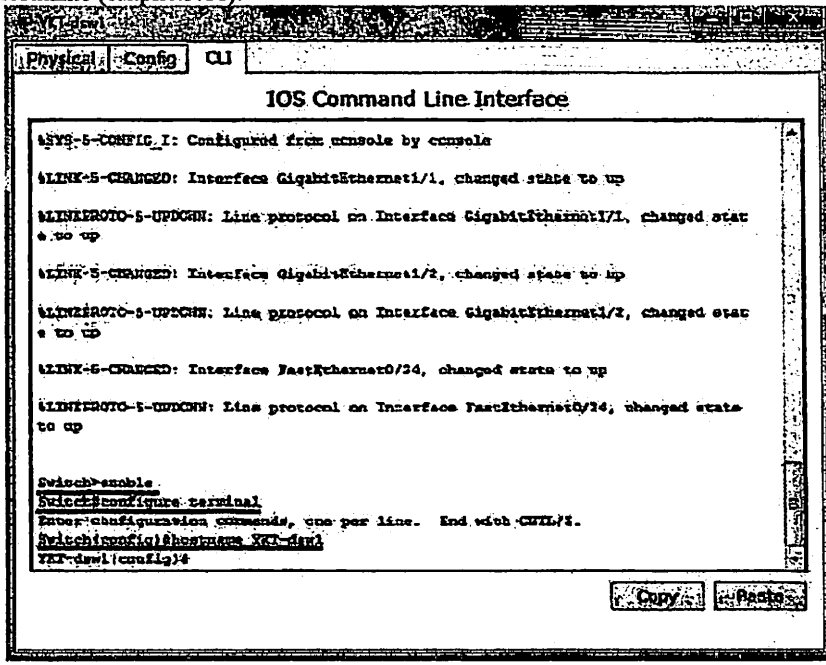


Рис.5.11.Окно командной строки

2.Для создания VLAN в режиме
YKT-dsw1 (config) #
в командной строке введите имя VLAN и ее номер. Например, для YKT-dsw1 введите (см. Таблица 5.2)

YKT-dsw1 (config) # Vlan 2

После этого имя будет присвоено с помощью команды YKT-dsw1 (config-vlan) # после имени метки (имени) будет введено имя VLAN, например YKT-dsw1 (config-vlan) #name Серверы (см.рис.5.11).

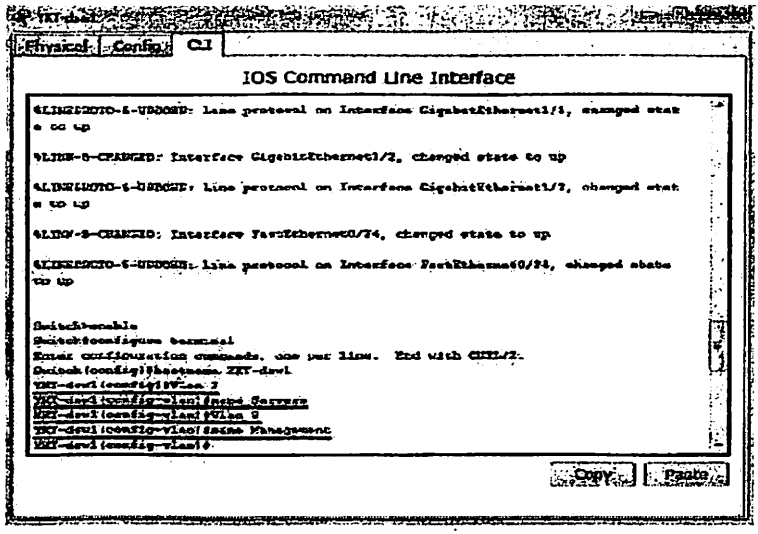


Рис.5.11. Настройка VLAN

3.Повторите действия п.2 для создания остальных VLAN для коммутатора YKT-dsw1.Остальные VLAN для коммутатора YKT-dsw1 (таблица 5.1, столбец 7) (3,151 - 154) создаются в соответствии с таблицей 5.2. Когда вы создаете все VLAN на коммутаторе YKT-dsw1, окно интерфейса командной строки IOS закрывается.

4.Переключитесь на режим коммутатор-коммутатор YKT-asw1 и настройте VLAN 3, 151, 223, 154. (Таблица 5.1, столбец 7), имена VLAN показаны в таблице 5.2.

5.Настройка остальных коммутаторов (YKT-asw2, YKT-asw3, YKT-Marha-dsw1, YKT-Marha-asw1) производиться с использованием таблиц 5.1,5.2.Для организации эффективного управления сетью, коммутатор VLAN 3 выделяется для функций управления потоками (Management Управление).

6.Выберите нужный коммутатор из схемы и выберите IP-адрес для управления сетью во всех коммутаторах.

7.Используя **YKT-dsw1(config)#** , мы создаем виртуальный интерфейс для YKT-dsw1. Из метки сети введите номер строки командной строки (номер VLAN). Это соответствует VLAN 3.

YKT-dsw1(config-if)#description По определению мы описываем виртуальный интерфейс VLAN 3 для текущей ситуации с помощью команды, а адрес **YKT-dsw1(config-if)#ip** (0.0.0.0) отображается его IP-адрес. IP-адрес показан на рис.5.12.

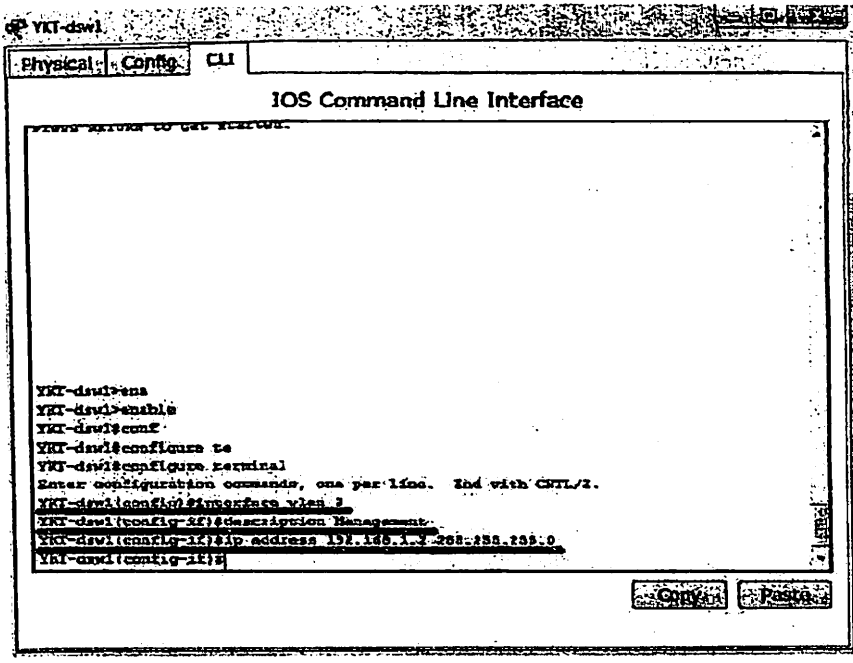


Рис.5.12. Виртуальныйинтерфейс

8.Наберите Exit длявыходаизглобальногорежима(#), перейдитекрежиму**ViralInterfaceSetup.YKT-dsw1 #copyrunning-config.**Сохраните конфигурацию коммутатора**YKT-dsw1** с помощью команды **startup-config.**В соответствии с таблицами 5.2,5.3 создайте виртуальный интерфейс для других коммутаторов.Переключатель #, сконфигурируйте команду **configstartup-config,** чтобы настроить конфигурацию каждого коммутатора.Сохраните созданный макет с полной топологией сети и IP-адресами с вашей фамилией.

Таблица 5.1.

Взаимодействие сетевых устройств

Router1	Router2811	YKT-gw1	Fe0/0	YKT-dsw1		
			Fe0/1	UpLink		
Switch1	Switch2960	YKT-dsw1	Fe0/1	YKT-gw1		2,3,151,152,153,154
			Gig1/1	YKT-asw1		3,152,153, 154
			Fe0/24	YKT-Morha-dsw1		3,151,152, 153,154
			Gig1/2	YKT-asw2		2,3
Switch1	Switch2950T	YKT-asw1	Fe0/1	Pto1(PC-PT)	154	
			Fe0/2	Feo1(Laptop-PT)	153	
			Fe0/3	Accountant1(PC-PT)	152	
			Fe0/4	Pto2(Laptop-PT)	154	
			Gig1/1	YKT-dsw1		3,152,153, 154
Switch1	Switch2950T	YKT-asw2	Fe0/1	Web-Server	2	
			Fe0/2	File-Server	2	
			Gig1/2	YKT-asw3		2,3
			Gig1/1	YKT-dsw1		2,3
Switch1	Switch2950T	YKT-asw3	Fe0/1	Mail-Server	2	
			Gig1/2	YKT-asw2		2,3
Switch1	Switch2950T	YKT-Marha-dsw1	Fe0/1	YKT-dsw1		3,151,152,153,154
			Fe0/2	Accountant2(PC-PT)	152	
			Fe0/3	Feo2(PC-PT)	153	
			Fe0/4	PTo3(PC-PT)	154	
			Gig1/1	YKT-Morha-asw1		3,151
Switch1	Switch2950T	YKT-Marha-asw1	Fe0/1	Other1	151	
			Fe0/2	Other2	151	
			Gig1/1	YKT-Morha-dsw1		3,151

Таблица 5.2.

Список VLAN

Номер VLAN	VLAN name	Описание
1	Default	не используется
2	Servers	для серверной фирмы
3	Management	для управления устройствами
4-150		резерв
151	Other	для других пользователей
152	Accountant	для пользователей учетных записей
153	FEO	для пользователей FEO
154	PTO	для пользователей PTO

Таблица 5.3.

План IPадресов

IP адрес	Описание	VLAN
192.168.1.0/24	**Management**	**3**
192.168.1.1	Defaultgateway	
192.168.1.2	YKT-dsw1	
192.168.1.3	YKT-asw1	
192.168.1.4	YKT-asw2	
192.168.1.5	YKT-asw3	
192.168.1.6	YKT-Morha-dsw1	
192.168.1.7	YKT-Morha-asw1	
192.168.1.8 - 192.168.1.254	резерв	

Таблица 5.4.

Маска подсети

Маска	CIDR режим расширения маски	Количество IP-адресов в сети
255.255.255.255	/32	0
255.255.255.254	/31	2
255.255.255.252	/30	4
255.255.255.248	/29	8
255.255.255.240	/28	16
255.255.255.224	/27	32
255.255.255.192	/26	64
255.255.255.128	/25	128
255.255.255.0	/24	256
255.255.254.0	/23	512
255.255.252.0	/22	1024

6.3.Настройка портов доступа и соединительных линий

Настройка портов доступа и соединительных линий состоит из двух шагов:
1) установка портов доступа и соединительных линий;
2) настройка IP-адресов.

Выполните следующие действия по настройке компьютерной сети для обеспечения услуги.

1.Откройте построенную сеть (см.рис.5.10) .

2.Установите порты доступа для всех команд. Для этого:
Перейдите к Глобальной настройке интерфейса с помощью коммутатора

Switch(config)#interfacefastEthernet 0/N

в команде номерN-порта изтаблицы 5.1. Для YKT-asw1 это выглядит следующим образом(таблица 5.1, столбец 4).:

YKT-asw1(config)#interface fastEthernet0/1

Мыописываеминтерфейс. Как видно из таблицы 5.1, RS01 добавляется в порт Fe0/1 коммутатора YKT-asw1. Используйте команду

YKT-asw1(config-if)#descriptionPTO

В связи с тем, что порт доступа подключен к этому порту, укажите режим порта доступа с помощью команды доступа

YKT-asw1 (config-if) #switchport. Switch (config-if) #switchportaccessvlan #

«Подключиться» к этому порту с помощью команды VLAN. В этом коммутаторе вы увидите(см.рис.5.13):

YKT-asw1 (config-if) #switchportaccessvlan 154

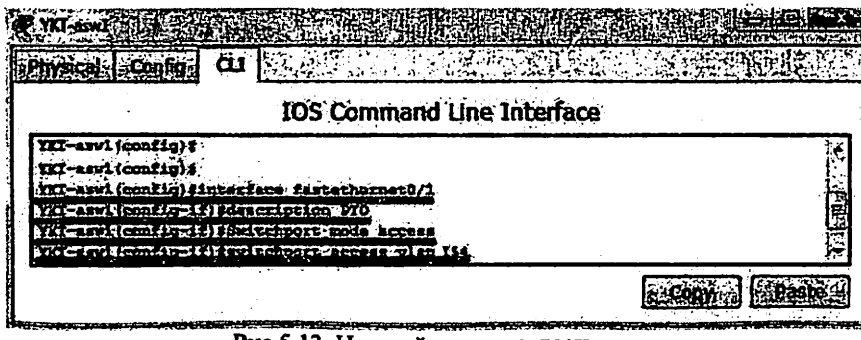


Рис.5.13. Настройка портов доступа

Номер VLAN показан в таблице 5.1 (столбец 6).Установите порты доступа на основе топологии, указанной в таблице 5.1.

3.Перейдите к настройке порта внешней линии, для которой требуются два взаимосвязанных коммутатора.

Чтобы настроить порт внешней линии, введите глобальный режим настройки для параметров порта внешней линии от YKT-dsw1 до YKT-asw1. В режиме настройки интерфейса, команду

YKT-dsw1 (config) # interfaceGig1 / 1

Просмотрите режим порта с помощью команды

#switchportmodetrunk. Switch (config-if) #switchporttrunkallowedVLAN

Добавитьэлемент #VLAN. Длязтойтопологии: YKT-dsw1 (config-if) #switchporttrunkразрешенVLAN 3,152-154.

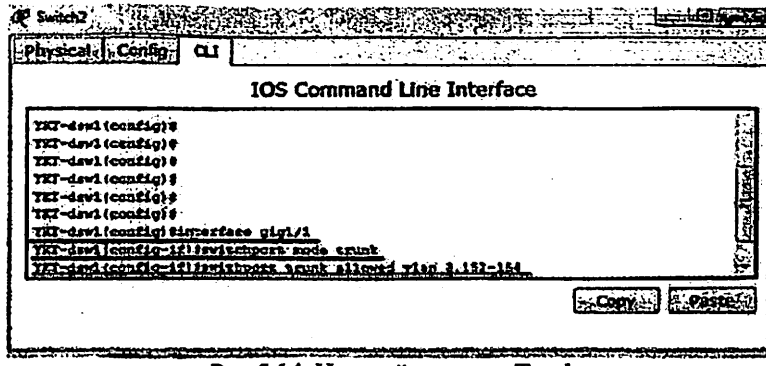


Рис.5.14. Настройка портовTrunk

Мы передаем магистральные порты в YKT-ASW1 (таблица 5.1).
Установите магистральные порты в других сетевых коммутаторах.

4.Настройте IP-адреса следующим устройствам.
Выделите устройство ПК-СТ (Pto1), выберите закладку «Desktop» и нажмите «IP addressconfiguration». Во всплывающем окне выберите «Static» и введите IP-адрес, указанный в таблице 5.3. Для нашего устройства 192.168.2.2, 255.255.255.0. Маска подсети и Шлюз по умолчанию - IP 192.168.2.1 (см.рис.5.15, 5.16).

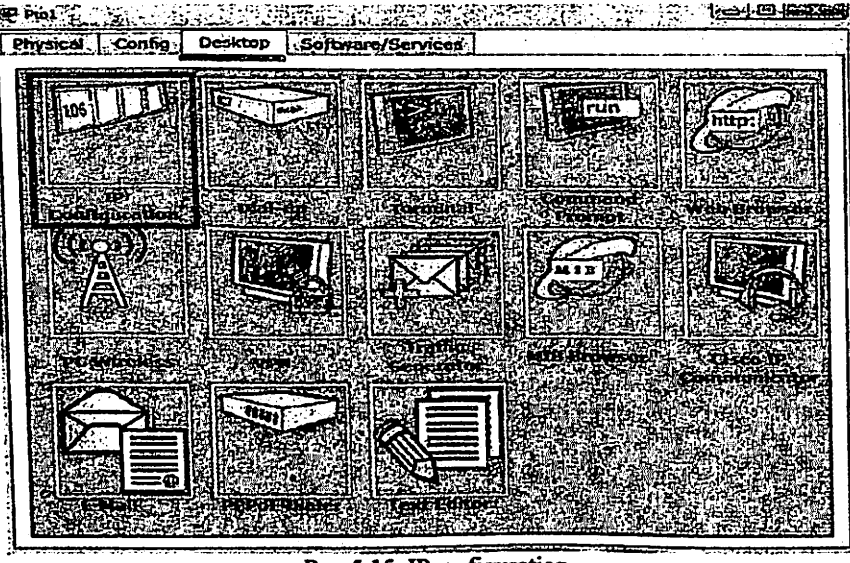


Рис.5.15. IPconfiguration

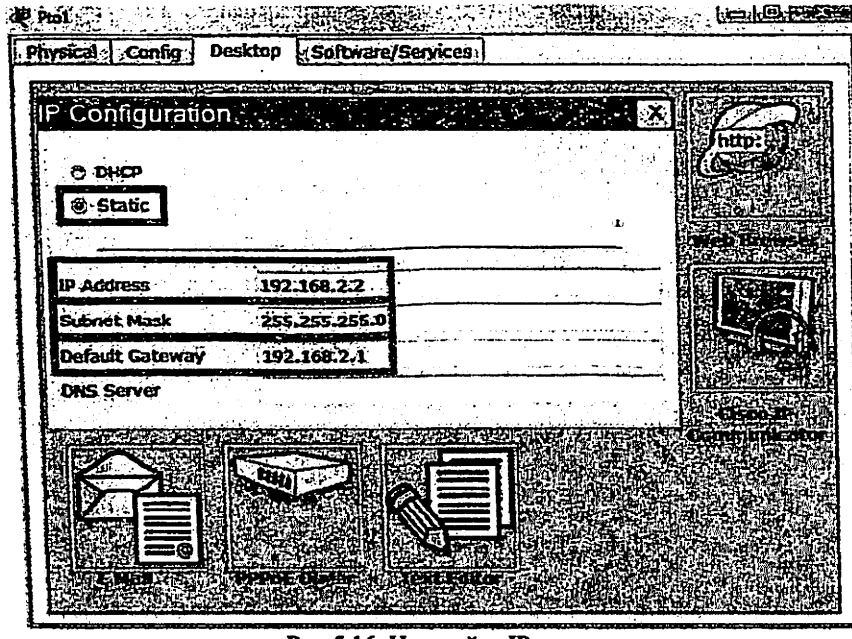


Рис.5.16. Настройка IP-адреса

Переключитесь в режим #copyrun-configstartup-config, чтобы настроить файлы конфигурации. Новый план IP приведён в таблице 5.5.

Таблица 5.5.

План IP

IP адрес	Описание	VLAN
192.168.0.0/24	**Servers**	**2**
192.168.0.1	Defaultgateway)	
192.168.0.2	Web	
192.168.0.3	File	
192.168.0.4	Mail	
192.168.0.5- 192.168.0.254	Резерв	
192.168.1.0/24	**Manegement**	**3**
192.168.1.1	Defaultgateway	
192.168.1.2	YKT-dsw1	
192.168.1.3	YKT-asw1	
192.168.1.4	YKT-asw2	
192.168.1.5	YKT-asw3	
192.168.1.6	YKT-Morha-dsw1	
192.168.1.7	YKT-Morha-asw1	
192.168.1.8- 192.168.1.254	Резерв	
192.168.2.0/24	**PTO**	**154**
192.168.2.1	Defaultgateway	
192.168.2.2- 192.168.2.254	Диапазон для пользователя	
192.168.4.0/24	**Другие пользователи(Other)**	**151**
192.168.3.1	Defaultgateway	
192.168.3.2- 192.168.3.254	Диапазон для пользователя	
192.168.4.0/24	**accountant**	**152**
192.168.4.1	Defaultgateway	
192.168.4.2- 192.168.4.254	Диапазон для пользователя	
192.168.5.0/24	**ФЭО(FEO)**	**153**
192.168.5.1	Defaultgateway	
192.168.5.2- 192.168.5.254	Диапазон для пользователя	

Практическое занятие №6

НАСТРОЙКА ПРОТОКОЛА DHCP В КОММУТАТОРАХ СЕТЕВОГО УРОВНЯ

1. Цель и содержание занятия

Изучение конфигурирования протоколаDHCPв коммутаторах сетевого уровня с помощью ПО CiscoPacketTracer.

2. Задание к занятию

В ПО CiscoPacketTracer построить модель сети в соответствии с рис.6.1. используя утилиту ping проверить связь между хостами. Проверить функциональные возможности **DHCP** сервера

1.	Создайте 2 сегмента сети с 13 хостами
2.	Создайте 2 сегмента сети с 12 хостами
3.	Создайте 2 сегмента сети с 11 хостами
4.	Создайте 2 сегмента сети с 10 хостами
5.	Создайте 2 сегмента сети с 9 хостами
6.	Создайте 2 сегмента сети с 8 хостами
7.	Создайте 2 сегмента сети с 7 хостами
8.	Создайте 2 сегмента сети с 6 хостами
9.	Создайте 3 сегмента сети с 14 хостами
10.	Создайте 3 сегмента сети с 12 хостами
11.	Создайте 3 сегмента сети с 11 хостами
12.	Создайте 3 сегмента сети с 10 хостами
13.	Создайте 3 сегмента сети с 9 хостами
14.	Создайте 3 сегмента сети с 8 хостами
15.	Создайте 3 сегмента сети с 7 хостами
16.	Создайте 3 сегмента сети с 6 хостами
17.	Создайте 4 сегмента сети с 17 хостами
18.	Создайте 4 сегмента сети с 16 хостами
19.	Создайте 4 сегмента сети с 15 хостами

20.	Создайте 4 сегмента сети с 14 хостами
21.	Создайте 4 сегмента сети с 13 хостами
22.	Создайте 4 сегмента сети с 12 хостами
23.	Создайте 4 сегмента сети с 11 хостами
24.	Создайте 4 сегмента сети с 10 хостами
25.	Создайте 4 сегмента сети с 9 хостам
26.	Создайте 4 сегмента сети с 8 хостами
27.	Создайте 4 сегмента сети с 7 хостами
28.	Создайте 4 сегмента сети с 6 хостами

3. Порядок выполнения

1. построить модель сети, сконфигурировать DHCP сервер, проверить соединения
2. Изучить теоретическую часть работы
3. Ответить на контрольные вопросы
4.Составить отчёт по работе

4. Содержание отчета

1. Задание
2. Сетевая модель построенная в ПО CiscoPacketTracer
3. Результаты утилиты ping каждого конечного узла
4. Принтскрины конфигурации DHCP-сервера
5.Принтскрины настройки IP-адресакаждого узла

5. Контрольные вопросы

1. Кратко охарактеризуйте устройства, используемые в модели локальной сети.
2. Каковы основные функции канального уровня модели?
3. Какие протоколы канального уровня используются в сети?
4. Напишите конфигурацию по DHCP.
5. Сколько существует сообщений DHCP и каковы их функции?
6. Какие данные могут передаваться между сервером и клиентом?

6. Теоретические сведения

Протокол DHCPv4 отвечает задинамическое назначениеIPv4-адресов и других сетевых конфигураций. Т.к. клиенты настольных компьютеров, как правило, составляют большую часть сетевых узлов, DHCPv4 является

чрезвычайно полезным и экономящим время инструментом для сетевых администраторов.

DHCPv4 включает в себя три различных механизма распределения адресов, обеспечивающие гибкость при присвоении IP-адресов:

• Ручное распределение - администратор назначает предварительно выделенный IPv4-адрес клиента, и DHCPv4 общается только IPv4-адреса для устройства.

• Автоматическое распределение - DHCPv4 автоматически присваивает статический адрес IPv4 постоянно на устройстве, выбрав его из пула доступных адресов. Нет аренды, и адрес постоянно присвоенный устройству.

• Динамическое распределение - DHCPv4 динамически распределяет, или арендует, IPv4-адрес из пула адресов в течение ограниченного периода времени выбранного сервера, или пока клиент больше не нуждается в адресе.

Динамическое распределение является наиболее часто используемым механизмом DHCPv4. При использовании динамического распределения, клиенты арендуют информации от сервера к административной определенного периода времени, как показано на рисунке 4.1. Администраторы настраивают сервера DHCPv4 установить сдает раз в разные промежутки времени. Договор аренды, как правило, колеблется от 24 часов до недели или больше. Когда срок аренды истекает, клиент должен попросить еще адреса, хотя клиент обычно переназначены тому же адресу.

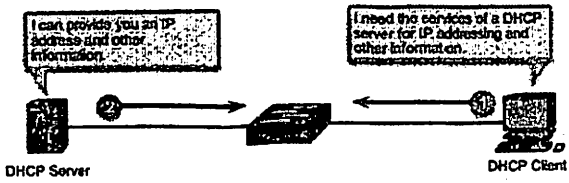


Рис. 4.1. Схема работыDHCP

DHCPv4 работает в клиент-серверном режиме. Когда клиент общается с сервером DHCPv4, сервер назначает или аренда IPv4-адреса клиента. Клиент подключается к сети с тем, что арендованный IP-адрес до истечения срока аренды. Клиент должен периодически обращаться к DHCP-серверу в продлении аренды. Этот механизм лизинга гарантирует, что клиенты, которые движутся или отключение питания не держать адресов, которые они больше не нужны. Когда истекает срок аренды, DHCP-сервер возвращает адрес в пул адресов, где он может быть перераспределен по мере необходимости.

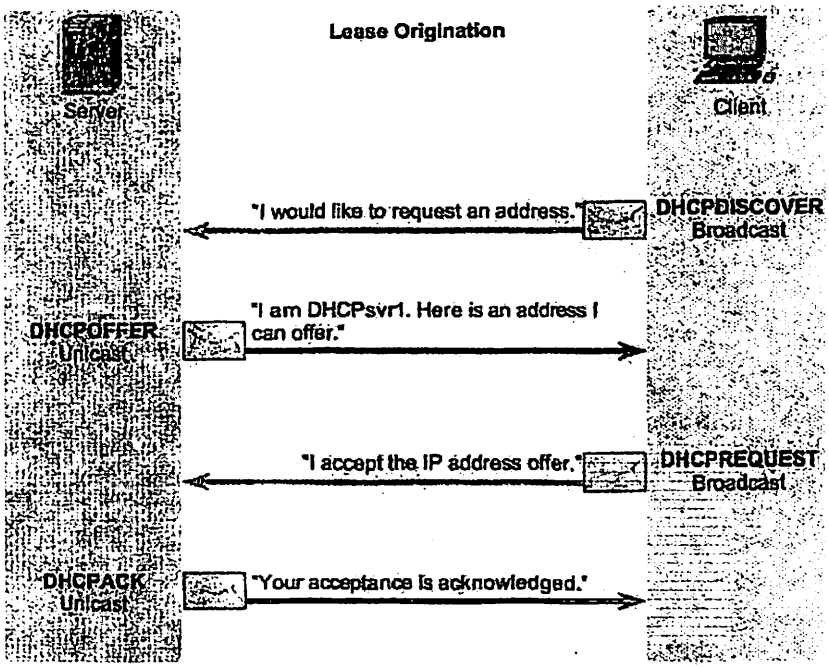


Рис.4.2. Механизмлизингаадресов

При загрузке сетевого клиентского ПО компьютера (когда компьютер хочет присоединиться к сети), происходит четыре этапа для получения аренды адреса. Клиент запускает процесс с широковещательным сообщениемDHCPDISCOVER с собственным MAC-адресом в поиск доступных серверов DHCPv4.

DHCP обнаружен (DHCPDISCOVER)

Сообщение DHCPDISCOVER находит сервераDHCPv4 в сети. Поскольку клиент имеет достоверную информацию для IPv4 при загрузке, он использует уровень 2 и уровень 3 широковещательные адреса для связи с сервером.

Предложение DHCP (DHCPOFFER)

Когда сервер DHCPv4 получает сообщение DHCPDISCOVER, он назначаетодин из свободных адресов IPv4 в аренду клиенту. Сервер также создает запись ARP, состоящей из MAC-адреса запрашивающего клиента и арендованногоIPv4-адреса клиента. Сервер DHCPv4 отправляет сообщение DHCPOFFER запрашивающему клиенту. Сообщение DHCPOFFER отправляется как одноадресное, используя 2 уровеньMAC-адрес сервера в качестве адреса источника и уровень 2 MAC-адреса клиента в качестве места назначения.

Запрос DHCP (DHCPREQUEST)

Когда клиент получает DHCPOFFER от сервера, он отправляет обратно сообщение DHCPREQUEST. Это сообщение используется для предоставления в аренду и продления аренды. При использовании для возникновения лизинга, DHCPREQUEST служит обязательным уведомлением о его принятии к выбранному серверу параметры, он предложил и неявное снижение на любые другие сервера, которые могут предоставить клиенту максимально выгодное предложение.

Подтверждения DHCP (DHCPACK)

Получив сообщение DHCPREQUEST, сервер проверяет сведения об аренде с ICMP-пинг на этот адрес, чтобы убедиться, что он не уже используется, создает новую запись ARP для аренды клиента, и отвечает сообщением DHCPACK одноадресной передачи. Сообщение DHCPACK является дубликатом DHCPOFFER, за исключением изменений в поле типа сообщения. Когда клиент получает сообщение DHCPACK, он записывает сведения о конфигурации и выполняет поиск ARP для адреса. Если нет ответа на АРП, клиент знает, что IPv4-адрес является действительным, и начинает использовать его как свой собственный.

Продление Аренды

Запрос DHCP (DHCPREQUEST)

Когда срок аренды истек, клиент посылает сообщение DHCPREQUEST напрямую к серверу DHCPv4, что изначально предлагал IPv4-адрес. Если DHCPACK не получен в течение указанного времени, клиент транслирует другой DHCPREQUEST так, что один из других серверов DHCPv4 может продлить договор аренды.

Подтверждения DHCP (DHCPACK)

Получив сообщение DHCPREQUEST, сервер проверяет сведения об аренде, возвращая DHCPACK

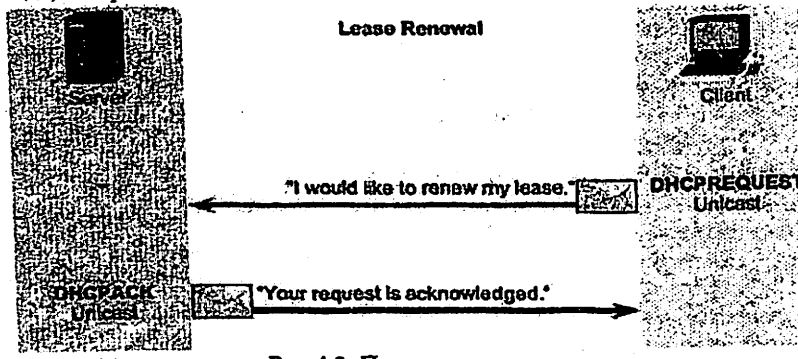


Рис.4.3. Продление аренды

Описание программы CiscoPacketTracer

CiscoPacketTracer (см.рис.4.4)– программа-симулятор для моделирования сети, которая позволяет студентам экспериментировать с поведением сети и получать ответы на вопросы "что если". В качестве неотъемлемой части сетевой Академии Cisco, ПО PacketTracer предоставляет моделирование, визуализацию, создание, оценку, а также возможности совместной работы и облегчает преподавание и изучение сложных понятий технологии локальных сетей.

ПОPacketTracer дополняет физическое оборудование в классе, позволяя студентам создавать сети с практически неограниченным количеством устройств, с целью получения практических навыков, обнаружения и устранения неполадок в сети.

CiscoPacketTracerподдерживаетследующиетипыпротоколов (табл.4.1).

Таблица 4.1

Уровни	Протоколы, поддерживаемые CiscoPacketTracer
Прикладной	FTP, SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNTP, AAA, ISRVOIP, SCCP
Транспортный	TCP, UDP, алгоритм TCPNagle, IP фрагментация,RTP
Сетевой	BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSeq, RIPv1/v2/ng, Multi-area OSPF, EIGRP, Static Routing, Route Redistribution, Multilayer switching, L3QoS, NAT, CBAL, Zone-based policy firewall
Сетевого интерфейса/ доступа	Ethernet 802.3, 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.11q, PAgP, L2QoS, SLARP, Simple WEP, WPA, EAP

Основные Характеристики

Рабочая область PacketTracer: CiscoPacketTracer имеет две рабочие области – логическую (рис.4.4.) и физическую (рис.4.5.). Логическое пространство позволяет пользователям строить логические сетевые топологии размещения, подключения и кластеризация виртуальных сетевых устройств. Физическое рабочее пространство предоставляет графический Физический размер логическую сеть, дающих ощущение масштаба и размещения в сети устройств, таких как маршрутизаторы, коммутаторы и узлы выглядели бы в реальной среде. Физическое представление также предоставляет географические представления сетей, включая несколько городов, зданий и коммутационных шкафов.

Режимы PacketTracer: CiscoPacketTracer обеспечивает два режима работы для визуализации поведения сети—режим реального времени и режим моделирования. В режиме реального времени в сети ведет себя как реальные устройства, с немедленной реакцией в режиме реального времени для всех сетевых операций. Режим реального времени дает студентам

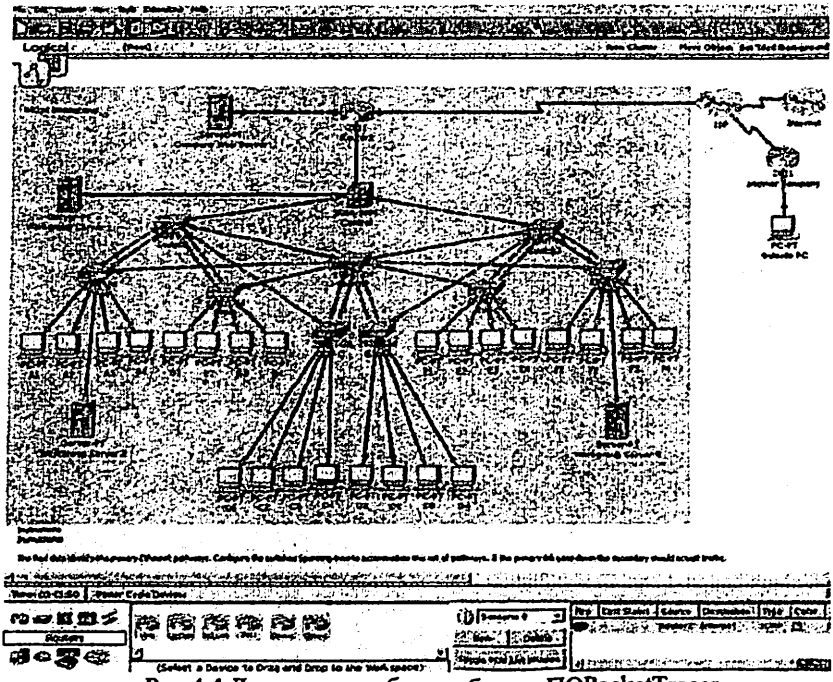


Рис.4.4.Логическая рабочая область ПОPacketTracer

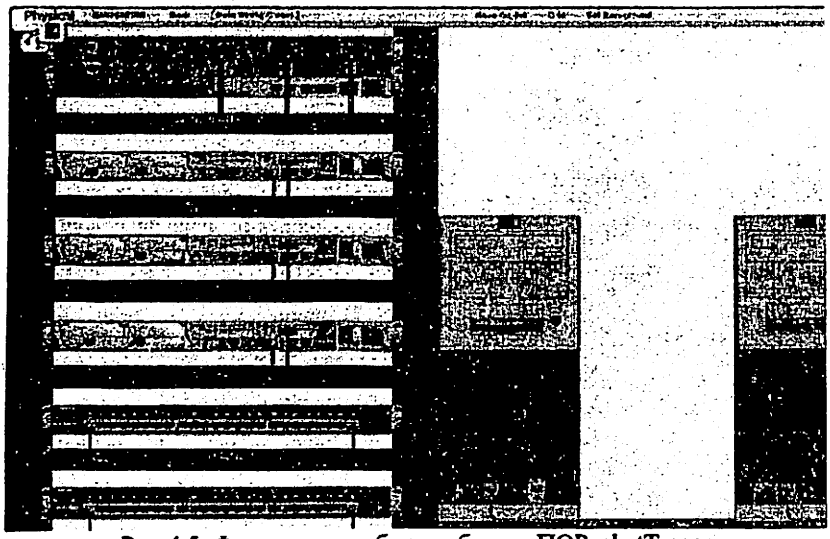


Рис.4.5. Физическая рабочая область ПОPacketTracer

реальную альтернативу реальным оборудованием и позволяет им набраться опыта настройки перед началом работы с реальным оборудованием.

В режиме моделирования пользователь может видеть и контролировать интервалы времени, внутреннее устройство передачи данных и распространения данных по сети. Это помогает студентам понять основные концепции сетевых операций. Твердое понимание основ сетей может помочь ускорить изучение взаимосвязанных понятий.

Modular Devices: Graphical representations visually simulate hardware and offer the ability to insert interface cards into modular routers and switches, which then become part of the simulation.

Модульные устройства: графические изображения оборудования для визуального моделирования, предлагают возможность вставить адаптеры в модульные маршрутизаторы и коммутаторы, которые затем становятся частью моделирования.

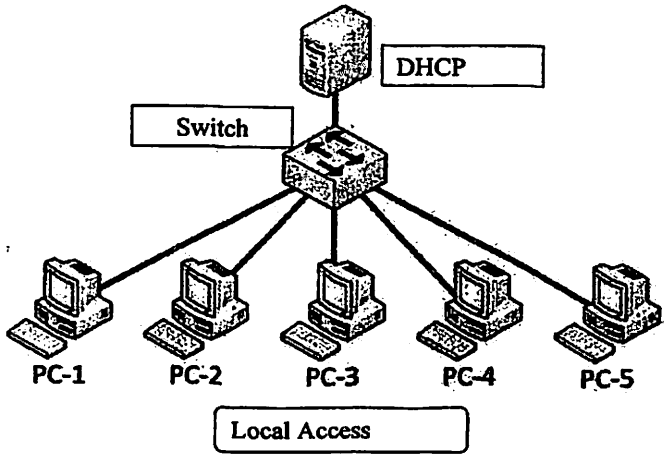


Рис.4.6. Модель сети

Практическое занятие №7,8

СОЗДАНИЕ НОВЫХ ПОЛЬЗОВАТЕЛЕЙ В СРЕДЕ ELASTIXSIP

1. Цельисодержаниезанятия

Ознакомление с основными принципами организации сети IP-телефонии на базе протокола SIP. Получение базовых навыков работы с сервером ElastixSIP.

2. Заданиекзанятию

1. При подготовке к лабораторной работе необходимо изучить следующие вопросы:

- Типы архитектуры в сетях IP-телефонии
- Структура сети передачи данных на основе стека протоколов TCP/IP
- Структура сети на базе протокола SIP

2. Сконфигурировать рабочую станцию, подключаемую к SIP-серверу, для работы в локальной сети на основе стека протоколов TCP/IP
3. Настроить пользователей соответственно варианту сервере ElastixSIP.
4. Настроить IP-телефоны компании Huawei, Softphone 3CXPhone, а так же доступ на IAD208 для аналогового абонента.
5. Подключить телефонные аппараты к шлюзу через порты
6. Проверить прохождение вызова и листинг команд в CLI оболочке Asterisk:
   - этап «ответ станции»
   - этап «абонент Б свободен»
   - проверка прохождения разговора
   - этап «абонент Б занят»

3. Порядоквыполнения

При выполнении лабораторной работы рекомендуется соблюдать следующую последовательность:

1. Изучить методические указания к данной лабораторной работе. Ознакомиться с видами соединений в сети IP-телефонии, структурой сети передачи данных на основе стека протоколов TCP/IP и SIP
2. Получить у преподавателя задание
3. Выполнить практическую часть.

- настроить рабочую станцию SIP-клиента для работы в локальной сети LAN по протоколу TCP/IP
- в программе Elastix:
- настроить IP адресацию и SIP параметры шлюза в таблице QuickSetup
- настроить таблицу TeltoIPRouting шлюза для внешнего соединения
- настроить таблицу EndpointPhoneNumberTable шлюза для привязки телефонных номеров к портам шлюза
- настроить username и password в таблице ProtocolManagement – EndpointSettings –Authentication для аутентификации пользователей

- Проверить этапы прохождения вызова

4. Ответить на контрольные вопросы.

Варианты заданий

N		PC0	PC1	IP Phone0	IP Phone1	AnalogPhone
1	Тел. Номер	201101	201102	201103	201104	201105
	IP-адрес	192.168.201.101	192.168.201.102	192.168.201.103	192.168.201.104	192.168.201.90
2	Тел. Номер	201111	201112	201113	201114	20115
	IP-адрес	192.168.201.111	192.168.201.112	192.168.201.113	192.168.201.114	192.168.201.90
3	Тел. Номер	201121	201122	201123	201124	201125
	IP-адрес	192.168.201.121	192.168.201.122	192.168.201.123	192.168.201.124	192.168.201.90
4	Тел. Номер	201131	201132	201133	201134	201135
	IP-адрес	192.168.201.131	192.168.201.132	192.168.201.133	192.168.201.134	192.168.201.90
5	Тел. Номер	201141	201142	201143	201144	201145
	IP-адрес	192.168.201.141	192.168.201.142	192.168.201.143	192.168.201.144	192.168.201.90
6	Тел. Номер	201151	201152	201153	201154	201155
	IP-адрес	192.168.201.151	192.168.201.152	192.168.201.153	192.168.201.154	192.168.201.90
7	Тел. Номер	201161	201162	201163	201164	201165
	IP-адрес	192 168.201.161	192.168.201.162	192.168.201.163	192.168.201.164	192.168.201.90
8	Тел. Номер	201171	201172	201173	201174	201175
	IP-адрес	192.168.201.171	192.168.201.172	192.168.201.173	192.168.201.174	192.168.201.90
9	Тел. Номер	201181	201182	201183	201184	201185
	IP-адрес	192.168.201.181	192.168.201.182	192.168.201.183	192.168.201 184	192.168.201.90
10	Тел. Номер	201191	201192	201193	201194	201195
	IP-адрес	192.168.201.191	192.168.201.192	192.168.201.193	192.168.201.194	192.168.201.90
11	Тел. Номер	201201	201202	201203	201204	201205
	IP-адрес	192.168.201.201	192.168.201.202	192.168.201.203	192.168.201.204	192.168.201.90
12	Тел. Номер	201211	201211	201211	201211	201211
	IP-адрес	192.168.201.211	192.168.201.212	192.168.201.213	192.168.201.214	192.168.201.90

4. Содержаниеотчета

1. Схема сети SIP с кратким описанием компонентов.
2. Схема лабораторного макета по варианту.
3. Краткая характеристика шлюза с объяснением параметров.
4. Алгоритм обмена сигнальными сообщениями по протоколу SIP при прохождении вызова через прокси-сервер и шлюз.
5. Ответы на контрольные вопросы

5. Контрольныевопросы

1. Какие компоненты входят в состав сети на основе протокола SIP?
2. Зачем нужен протокол SIP?
3. Основные принципы, положенные в основу протокола SIP, кто егостандартизировал?
4. Какое место занимает протокол SIP в стеке протоколов TCP/IP?
5. Какой тип адресации используется в протоколе SIP?
6. Перечислить типы SIP-адресов, что значат их элементы?

7. Что такое план нумерации E.164?
8. Что такое DTMF набор номера (тоновый набор)?
9. Что такое IP адрес?
10. Что такое Web-браузер?
11. Что означает термин «параметры по умолчанию»?
12. Что означает термин «авторизация пользователя»?
13. Что означает термин «аутентификация пользователя»?
14. Функциональных возможностей программы ElasticSIP?

6. Теоретическиесведения

1. Описание лабораторного макета

Схема лабораторного макета приведена на рис.1. Лабораторный макет использует программу Elastix в качестве сервера SIP, которая осуществляет функции пакетной УАТС, программу 3CX Phone установленную на ПК, эмулирующую IP-телефон на ПК, два IP телефона и один аналоговый телефон, подключенный через IAD208e.

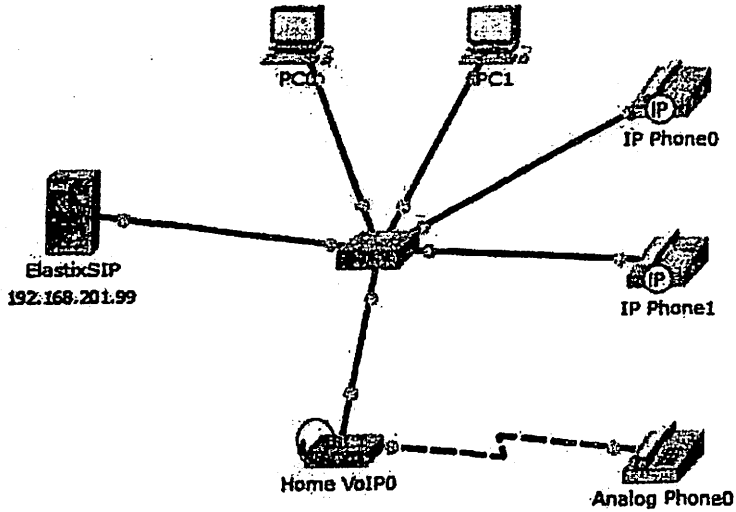


Рис.1. Схема лабораторного макета.

Серверное приложение Elastix установлено на отдельном сервере ElastixSIP. Клиентские части в виде программы 3CX SoftPhone установлены на PC0 и PC1. К сети подключены IP телефоны IPPhone0 и IPPhone1. **IP адрес ElasticSIP сервера 192.168.201.99 маска подсети 255.255.255.0.** К серверу SIP подключён IAD208e, поддерживающий сигнализацию по протоколу SIP. К шлюзу подключен аналоговый телефон

AnalogPhone0.

2. Конфигурация рабочей станции SIP-клиента для работы в локальной сети на основе стека протоколов TCP/IP

1. Собрать схему лабораторного макета в соответствии с рис. 1.
2. На компьютерах PC0 и PC1 необходимо настроить сетевую карту в соответствии с IP планом, в соответствии с вариантом. Для этого на рабочих станциях необходимо зайти в настройки сетевой карты (Пуск – Панель управления – Сетевые подключения – Подключение по локальной сети – ПКМ – Свойства – Протокол Интернета (TCP/IP) (см. рис.2.)
3. В открывшемся окне произвести настройку IP адреса и принять изменения, нажав ОК. (см. рис.3.)
4. Осуществить проверку работоспособности параметров сети при помощи процедуры ping до адреса 192.168.201.99 (Пуск – Выполнить – cmd, в открывшемся окне ввести ping 192.168.201.99). В случае отсутствия соединения проверить соединение кабелей а так же IP адреса на предмет совпадения с другим компьютером.

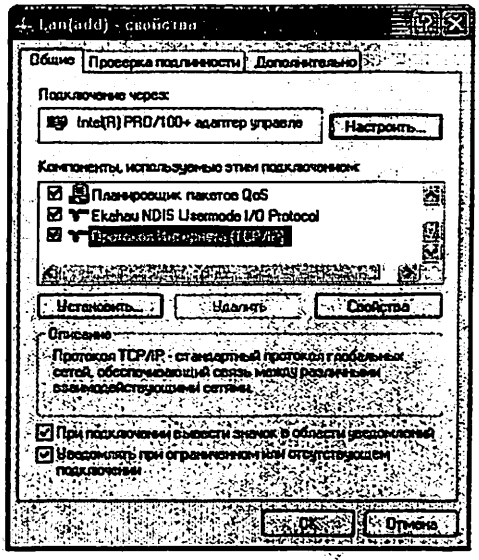


Рис. 2. Окно свойства.

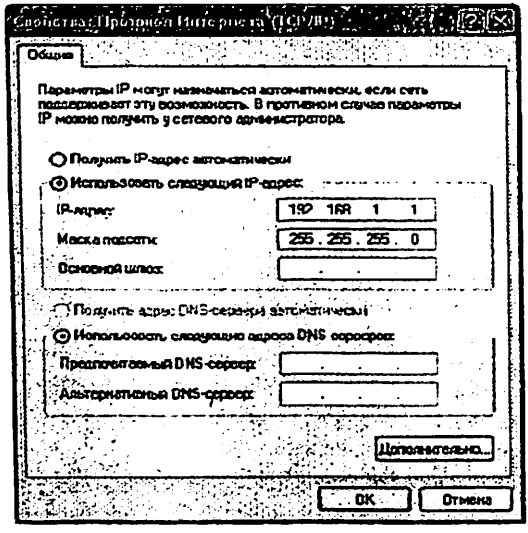


Рис.3. Настройки протокола Интернет TCP/IP

3. Вход в Web-интерфейс приложения Elastix.

1. Для доступа к Web-интерфейсу Elastix необходимо открыть любой браузер.
2. В браузере введите в строке адреса **IP адрес** сервера Elastix.
3. В окне авторизации (см.рис.4) вводятся данные для доступа к ресурсу:
   User name = Admin
   Password = q1w2e3
4. НажмитекнопкуOK.

Если **Login** и **Password** введены правильно, появляется стартовое окно Elastix (см.рис.5)

Рис.4. Вход на сервер ElastixSIP

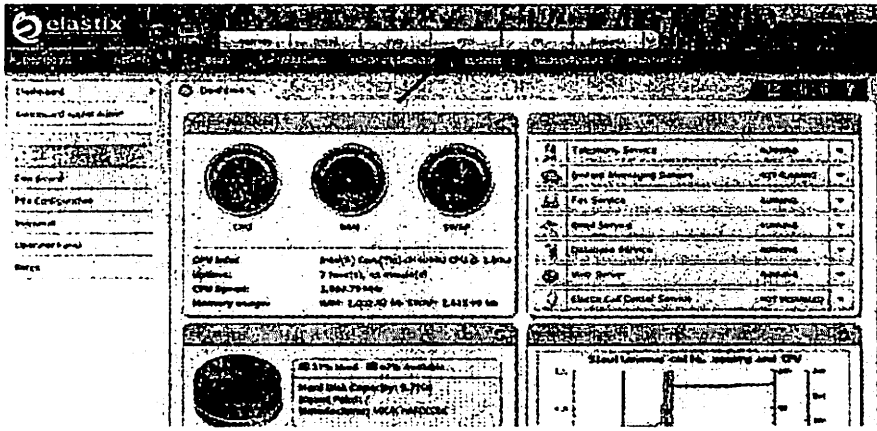


Рис.5. Стартовое окно программы Elastix

4. Создание абонентов в среде ElastixSIP

Для создания абонентов необходимо выполнить следующие действия:

1. В стартовом окне Elastix зайти во вкладку PBX, расположение которой указано на рис.5.
2. В открывшемся окне (см. рис.6) выбираем тип устройства (Device) «GenericSIPDevice» и нажимаем Submit

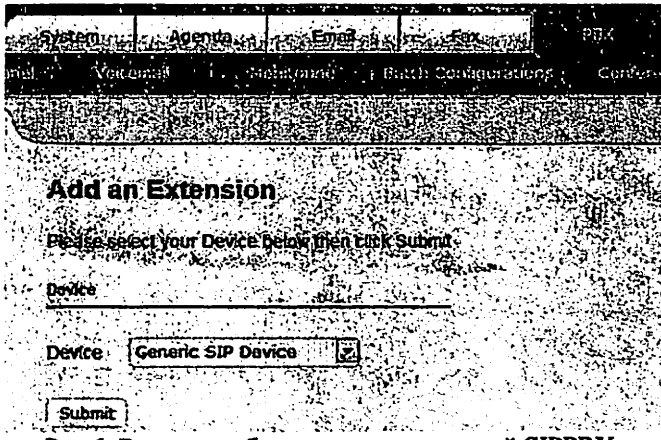


Рис.6. Вкладка добавления пользователей SIPPBX.

3. На следующем этапе производится указание номера абонента, указанного в таблице заданий в поле «**UserExtension**», имя, которое

будет отражаться при звонке от данного абонента, указывается в поле «**DisplayName**», в данном поле указываются имена студентов, состоящих в группе по исполнению данной лабораторной работы. (см. рис.7) .

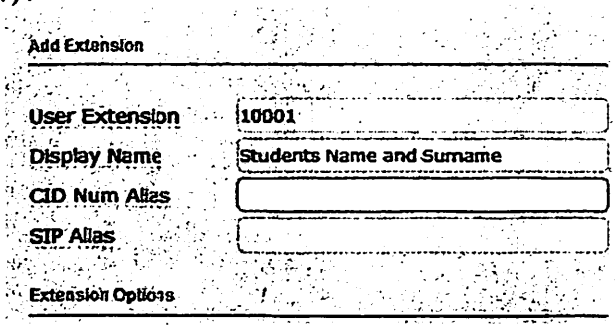


Рис.7. Пример создания абонента

4. Для более точной идентификации абонента необходимо назначить пароль для данного юзера. Для этого в поле Secret указываем пароль (см. рис.8). После данных действий нажимаем кнопку Submit, находящуюся в самом конце списка.

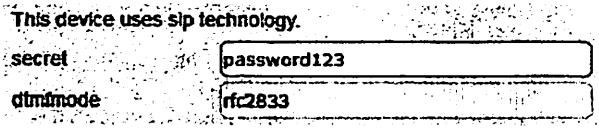


Рис.8. Пример присвоения пароля для данного абонента

5. Повторяем шаги 2-5 для оставшихся абонентов, после чего нажимаем на **ApplyConfigurationChangesHere**(рис .9).

6.

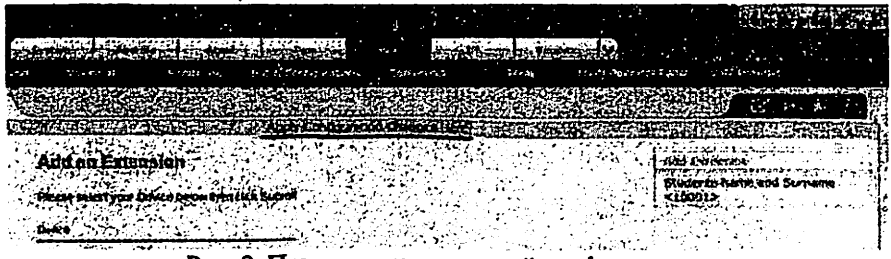


Рис. 9. Применение изменений конфигурации

5. Просмотр учетной записи абонента в CLI режиме ElastixSIP.

1. Для того, чтобы подключиться непосредственно к серверу Elastix необходимо открыть приложение Putty, В поле HostName указать IP-адрес Elastix сервера, в поле Port – 22 (порт по умолчанию для протокола SSH),и Connectiontype – SSH, как показано на рис. 10.

2. В открывшемся окне вводим в качестве логина «root», пароль – «q1w2e3».
3. Далее в качестве набираем «asterisk -vvvvvvvvvr» (9 знаков «v» и одну «r»), что позволяет зайти в CLI режим программы Elastix. (рис.11).
4.

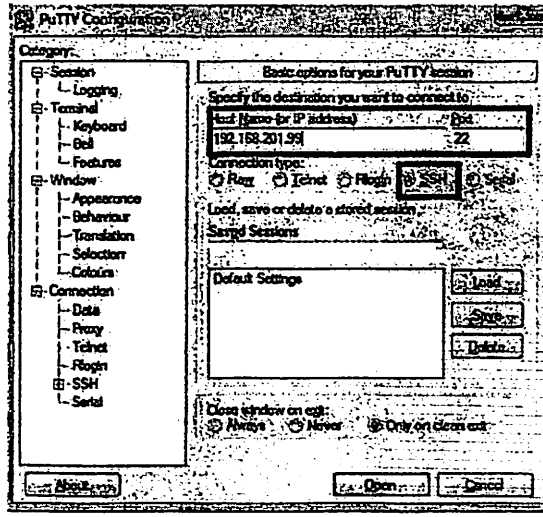


Рис.10. Настройки Putty для подключения к серверу Elastix по протоколу SSH

5. Режиме CLI вводим команды **sipshowusers**, которая показывает всех прописанных абонентов на данном SIP сервере, и **sipshowuser "Extension"** (например sipshowuser 10001), которая выводит информацию о пользователе, хранящуюся в БД Elastix (рис. 12). Оставляем после данных действий окно Putty открытым, в дальнейшем через него мы будем наблюдать процесс обработки вызовов.

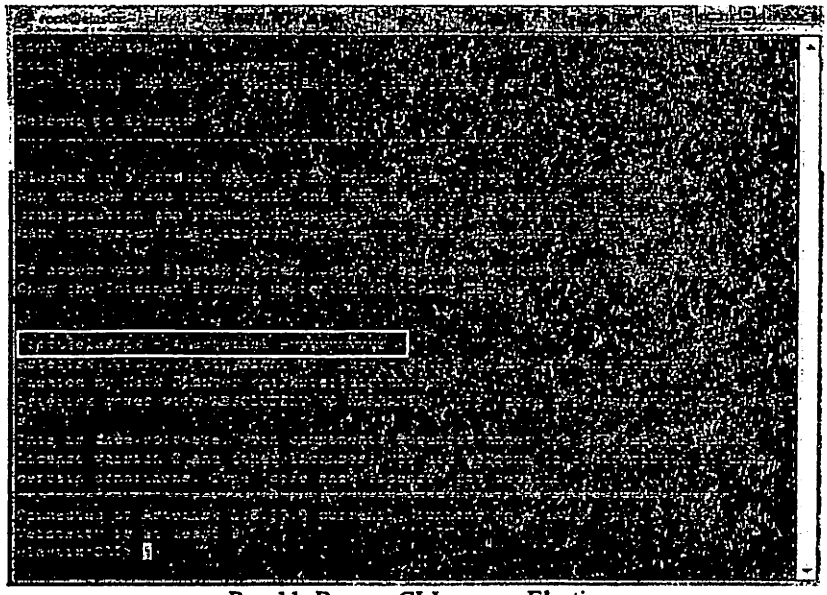


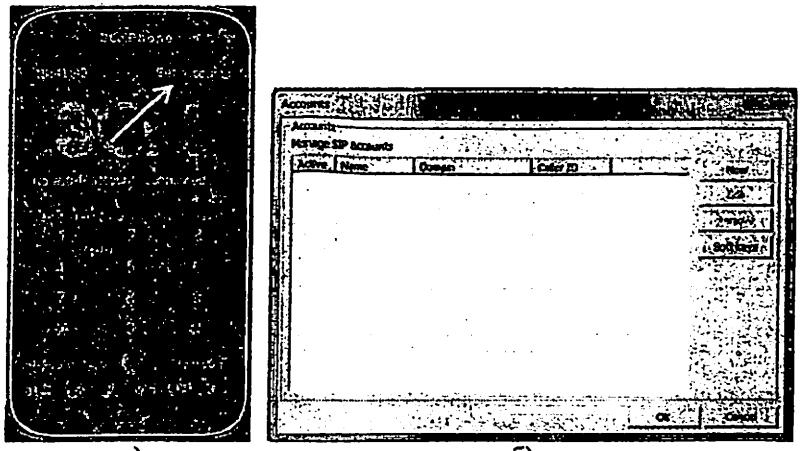
Рис.11. Вход в CLI режим Elastix

Рис. 12. Результат команд

6. Настройка приложения SoftPhone 3CXPhone для работы с ElastixSIP

Для настройки приложения 3CX Phone на компьютерах PC0 и PC1 необходимо выполнить следующие действия:

1. Открыть приложение 3CXPhone и щелкнуть на надписи «SetAccounts». (рис. 13 а). В открывшемся окне «Accounts» (рис. 13 б) выбрать пункт «New».



а) б)

Рис.13. Настройка 3CX Phone

2. В окне «Accountsettings» заполняются следующие поля «Accountname» (имя абонента), «CallerID» (телефонный номер абонента) в полях «Extension» и «ID» также вводится номер абонента, в поле «Password» указывается пароль, установленный администратором для данного номера. В поле «SpecifytheIPofyourPBX/SIPserver» указывается IP адрес сервера Elastix. Подтверждаем настройки. Пример заполнения пояснен на рисунке 14.
3. В случае правильной настройки всех параметров можно увидеть состояние телефона «Onhook», обозначающее, что телефон произвел авторизацию и готов к работе. В случае состояния «Notconnected» проверьте правильность параметров. Пример настроенного терминала 3CXPhone показан на рисунке 15.

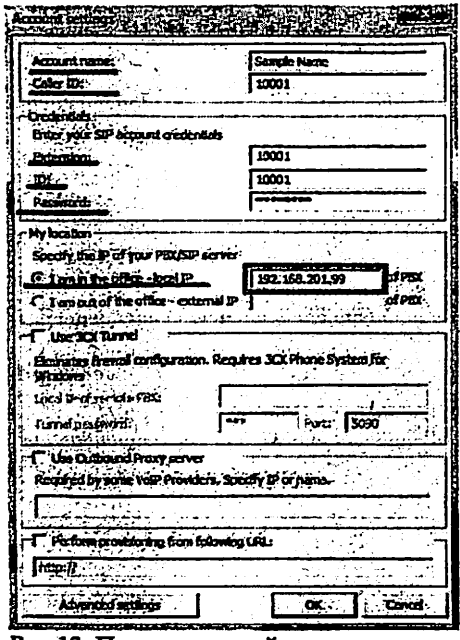


Рис.13. Пример настройки аккаунта в программе 3CXPhone

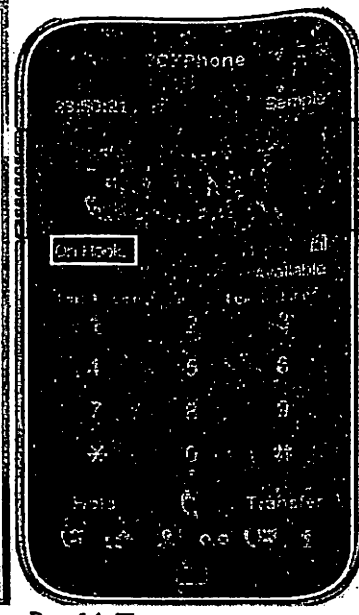


Рис.14. Пример готового к работе терминала 3CXPhone

7. Настройка IP-телефона MC850 компании Huawei для работы с ElastixSIP

Для того, чтобы настроить MC850 следуйте следующим указаниям:

1. Для настройки IP адреса для терминала выбираются по порядку следующие пункты: More (на рабочем столе телефона) – Settings – Network . В поле Networktype выбираем Ethernet. В поле Accessmode нажимаем на клавишу Set.
2. Настройте параметры IP-телефона в соответствии с IP-планом для вашего варианта. (пример на рис.15). После введения всех параметров сохраните параметры и вернитесь на рабочий стол устройства.

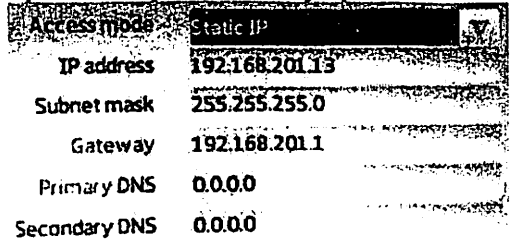


Рис.15. настройка IP-адреса телефона MC850

3. Откройте панель набора номера, выбрав пункт «Dialer» на рабочем столе телефона.
4. В открывшемся окне введите код *62820*, для открытия диалогового окна настроек данного телефонного аппарата, (в случае использования IP-телефона модели MC820c данный код необходимо набирать в окне выбора настроек). Пример открывающегося таким образом диалогового окна показан на рис. 16.
5. Выберите пункт «Serviceserver» и указываем в поле «Registrarserver» IP-адрес сервера Elastix, после сохранения настройки выберете раздел «Serviceaccount», где необходимо ввести номер телефона и пароль аутентификации, пример показан на рис.17. Сохранив внесенные изменения телефон потребуется перезагрузить.
6. Проверьте работоспособность телефона, в случае отсутствия регистрации в сети проверьте настройки для данного пользователя.
7. Конфигурирование IP-телефона MC850 завершено.

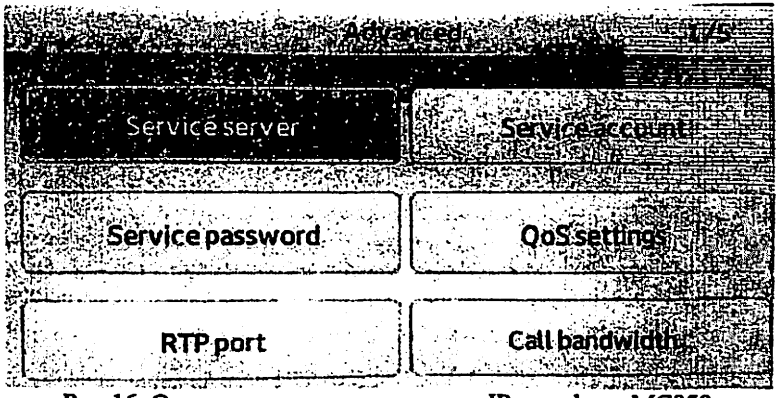


Рис.16. Окно расширенных настроек IP-телефона MC850

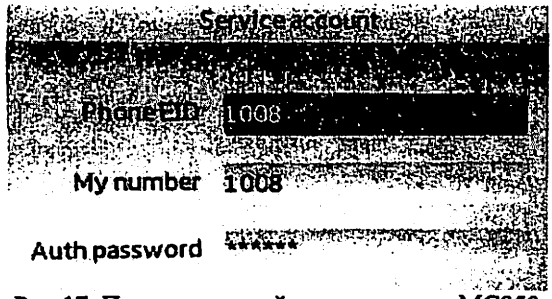


Рис.17. Пример настройки аккаунта на MC850

8. Настройка шлюза IAD208E(M) компании Huawei для подключения аналогового телефона к IP сети ElastixSIP.

Для того, чтобы подключить стандартный аналоговый телефон к SIP сети необходимо использовать шлюз интегрированного доступа, в составе лабораторной работы применяется IAD208E(M) компании Huawei. Для настройки IAD следуйте следующей инструкции:

1. Откройте InternetExplorer (в других браузерах Web-интерфейс работает некорректно), и в адресной строке введите IP-адрес 192.168.201.90 (IP-адрес IAD). Для авторизации введите логин root, пароль – admin (см. рис.18).

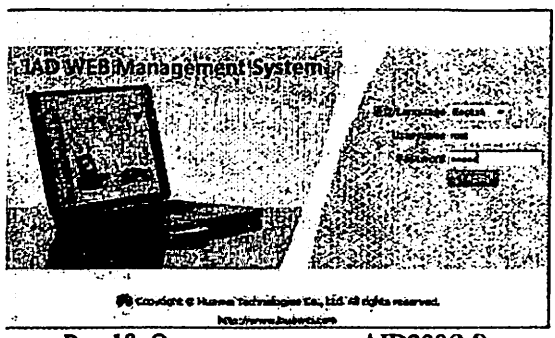


Рис.18. Окно авторизации AID208(M)

2. Выбираем последовательно SIPServiceConfiguration – FXSUser, в появившемся окне производим настройку для абонентского аналогового терминала следующим образом Ставим выделение напротив требуемого SN (соответствует номеру порта, к которому подключен AT)В полях UserID вводим номер телефона в соответствии с вариантом задания.
3. В Поле Username вводятся фамилия и имя студента «обладателя» данного номера. В поле Password вводится пароль, установленный для этого абонента в программе Elastix. В случае необходимости указать в поле CurrentSIPServerIP адрес сервера Elastix (рис.19). Нажать OK и сохранить конфигурацию. Проверить работу терминала.

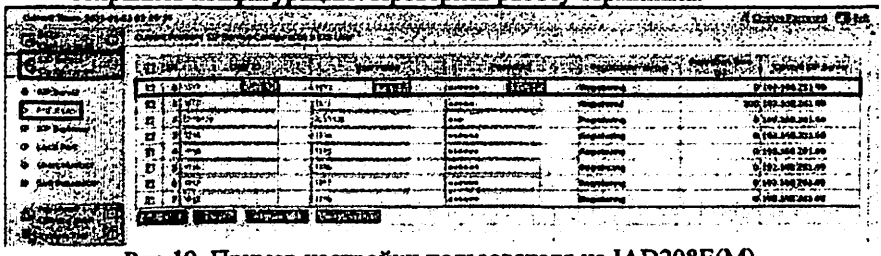


Рис.19. Пример настройки пользователя на IAD208E(M)

Практическое занятие №9

ИЗУЧЕНИЕ И НАСТРОЙКА ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ В КОММУТАТОРЕ D-LINK DES 3200-18. НАСТРОЙКА VLAN НА ПОРТАХ. СОСТАВ РЕК.802.1Q

1. Цель и содержание занятия

Изучение конфигурирования пользовательских данных в коммутаторе D-link с помощью Web-интерфейса. Изучение коммутаторов сетевого и канального уровня.

2. Заданиекзанятию

Сконфигурировать пользовательский порт в коммутаторе D-link с помощью Web-интерфейса. Изучить характеристики и поддерживаемые протоколы коммутаторов сетевого и канального уровня.

5. Изучение VLAN (Virtual local area network) в одном или в двух коммутаторах в программе Cisco Packet Tracer.

№	ВАРИАНТ
1.	Создать виртуальные пути между VLAN1(через 5 порт) и VLAN2 (через 6 порт).
2.	Создать виртуальный путь между VLAN1(через 6 порт) и VLAN2 (через 2 порт).
3.	Создать виртуальный путь между VLAN1(через 2 порт) и VLAN2 (через 3 порт).
4.	Создать виртуальный путь между VLAN1(через 6 порт) и VLAN2 (через 2 порт).
5.	Создать виртуальный путь между VLAN1(через 7 порт) и VLAN2 (через 4 порт).
6.	Создать виртуальный путь между VLAN1(через 7 порт) и VLAN2 (через 9 порт).
7.	Создать виртуальный путь между VLAN1(через 6 порт) и VLAN2 (через 8 порт).
8.	Создать виртуальный путь между VLAN1(через 6 порт) и VLAN2 (через 2 порт).
9.	Создать виртуальный путь между VLAN1(через 6 порт) и VLAN2 (через 1 порт).
10.	Создать виртуальный путь между VLAN1(через 8 порт) и VLAN2 (через 3 порт).
11.	Создать виртуальный путь между VLAN1(через 9 порт) и VLAN2 (через 12 порт).
12.	Создать виртуальный путь между VLAN1(через 2 порт) и VLAN2 (через 7 порт).
13.	Создать виртуальный путь между VLAN1(через 5 порт) и VLAN2

	(через6 порт).
14.	Создать виртуальный путь между VLAN1(через 8 порт) и VLAN2 (через 12 порт).
15.	Создать виртуальный путь между VLAN1(через 2 порт) и VLAN2 (через 3 порт).
16.	Создать виртуальный путь между VLAN1(через 5 порт) и VLAN2 (через 9 порт).
17.	Создать виртуальный путь между VLAN1(через 3 порт) и VLAN2 (через 4 порт).
18.	Создать виртуальный путь между VLAN1(через 7 порт) и VLAN2 (через 4 порт).
19.	Создать виртуальный путь между VLAN1(через 7 порт) и VLAN2 (через 11 порт).
20.	Создать виртуальный путь между VLAN1(через 1 порт) и VLAN2 (через 8 порт).
21.	Создать виртуальный путь между VLAN1(через 3 порт) и VLAN2 (через 9 порт).
22.	Создать виртуальный путь между VLAN1(через 5 порт) и VLAN2 (через 7 порт).
23.	Создать виртуальный путь между VLAN1(через 8 порт) и VLAN2 (через 9 порт).
24.	Создать виртуальный путь между VLAN1(через 4 порт) и VLAN2 (через 12 порт).
25.	Создать виртуальный путь между VLAN1(через 8 порт) и VLAN2 (через 7 порт).
26.	Создать виртуальный путь между VLAN1(через 11 порт) и VLAN2 (через 6 порт).
27.	Создать виртуальный путь между VLAN1(через 12 порт) и VLAN2 (через 3 порт).
28.	Создать виртуальный путь между VLAN1(через 1 порт) и VLAN2 (через 8 порт)

3. Порядоквыполнения

1. Сконфигурировать пользовательский порт в коммутаторе D-link для различных пользователей и сконфигурироватьVLAN
2. Изучить теоретическую часть работы
3. Ответить на контрольные вопросы
4.Составить отчёт по работе

4. Содержаниеотчета

1. Краткая характеристика коммутатора и шаги конфигурирования.
2. Протоколы коммутатора на канальном и сетевом уровне.
3. Результаты конфигурации коммутатора и VLAN порты.
4. Напишите краткое описание функций коммутатора.

5. Контрольныевопросы

1. Какие функции выполняеткоммутатор DES 3200-18?
2. Каковы основные функции алгоритма CSMA коллизий в коммутаторах канального уровня?
3. Какие протоколы канального уровня используются в коммутаторе?
4. Что такое VLAN?
5. Какие приложения могут использоваться для настройки?
6. Как осуществляется процесс коммутации пакетов в коммутаторе D-LINK?

6. Теоретическиесведения

КонфигуртрованиеD-LinkDES-3200-18 Switch

Все программные функции коммутатора можно управлять, настраивать и контролировать через встроенный web-интерфейс (HTML-код). Коммутатором можно управлять с удаленных станций в любой точке сети с помощью стандартного браузера, такого как FireFox или InternetExplorer. Браузер действует как универсальное средство доступа и вы можете общаться напрямую с коммутатором с помощью протокола http.

Login to Web Manager – Войдитев Web-менеджер

Чтобы начать управление коммутатора, просто запустите браузер, установленный на вашем компьютере и укажитеIP-адрес, определенный для устройства.

Примечание: заводской IP-адрес по умолчанию для коммутатора 10.90.90.90.

Чтобы открыть модуль управления, необходимо пройти процедуру аутентификации (рис. 6.1.).

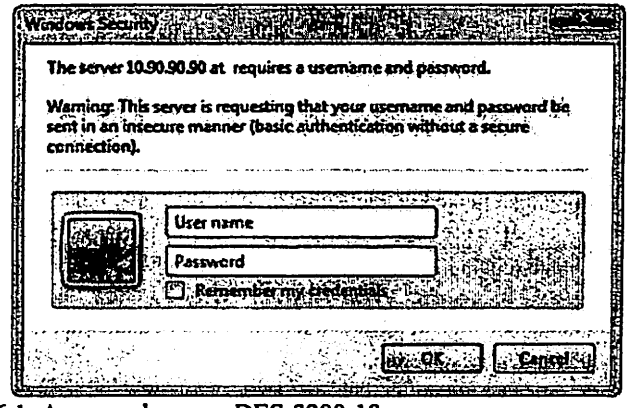


Рис. 6.1. АутентификацияDES-3200-18

Web-basedUserInterface – Веб-интерфейспользователя

Пользовательский интерфейс обеспечивает доступ к различным настройки конфигурации и управления Windows, позволяет просматривать статистику производительности, и позволяет наглядно контролировать состояние системы (рис. 6.2.).Пользовательский интерфейс можно разделить на три отдельные зоны, как описано в таблице 6.1.

Главная папки доступными в веб-интерфейсе:

- Configuration – настройка возможностей коммутатора
- L2 Features– настройка функциональных возможностей коммутатора уровня L2
- QoS – настройка характеристик в отношении качества обслуживания коммутатора.
- ACL – для настройки функций относительно функциональности списка контроля доступа коммутатора
- Security – настройки, касающиеся безопасности коммутатора
- Monitoring – настройки мониторинга для отслеживания конфигурации и статистики коммутатора

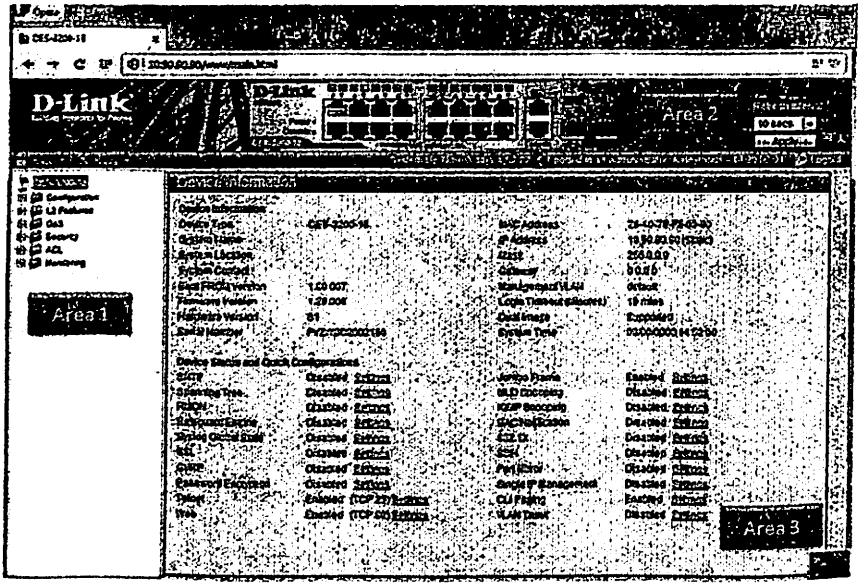


Рис.6.2. Главная страницаWeb-Manager

Таблица 6.1

Зоны пользовательского интерфейса

Номер зоны	Функции
Area 1	выборменюилиокнадляпоказа
Area 2	показываетпортыкоммутатора, консольипортуправления, показываетсостояниепорта некотоорыефункцииуправления – save, reboot, download,upload – находятся здесь
Area 3	Представлена информация коммутатора на основе выбора пользователя и ввода данных конфигурации

System Information configuration

ДляхарактериистикикоммутаторамыможемввестиSystem Name, System Location, System Contact (рис.6.3.).

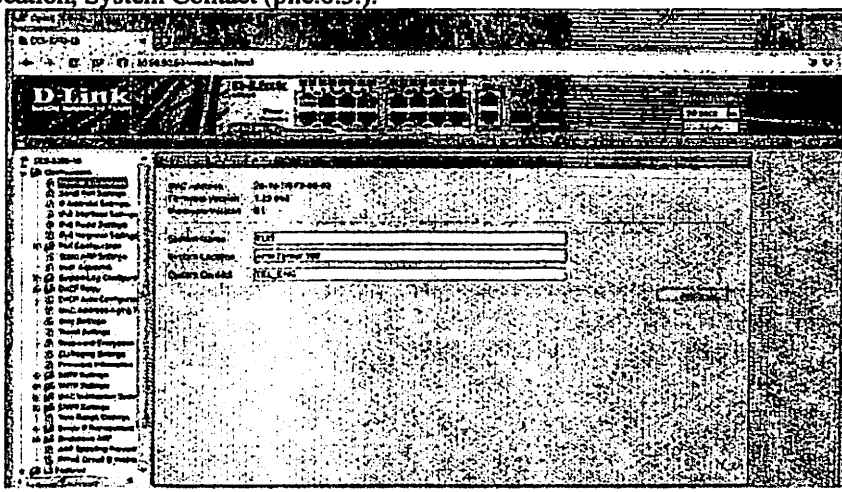


Рис.6.3. Окно System Information settings

- SystemName – определяетимякоммутаторавсети
- SystemLocation – определяетрасположениекоммутаторавсети
- System Contact – определяет контактную информацию

КонфигурированиепортаPort Configuration

Чтобыоткрытьэтоокновыберите**Configuration > Port Configuration > Port Settings** (рис. 6.4.)

Для конфигурирования порта коммутатора:

• Выбрать порт или последовательный диапазон портов, используя параметры **FromPort и ToPortв** выпадающем меню

• Использовать выпадающее меню для настройки параметров (Таблица 6.2)

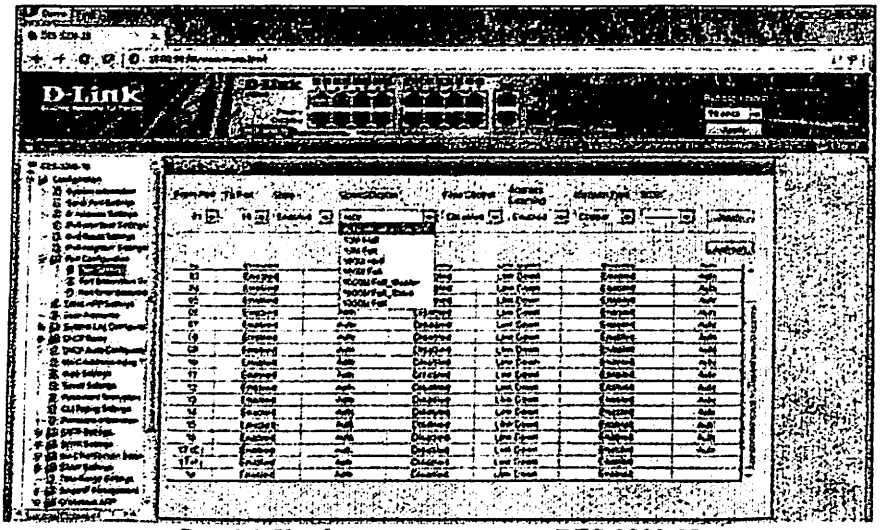


Рис.6.4. КонфигурированиепортаDES-3200-18

Table 6.2

Port Configuration fields

параметр	описание
From Port/To Port	Выборсоответствующегодиапазонапортовдляконфигурирования
State	СостояниепортаилигруппыпортовEnable(включен)orDisable (отключен)
Speed/Duplex	Выборскоростиирежимаработыпортадуплексный/полудуплексныйt
Flow Control	Показывет схему контроля потока
Address Learning	ОпределениеMAC-адресов для выборанных портов
Medium Type	ОпределениетипасредыпередачидляиспользованияComboports
MDIX	Выбор типа кабеля (прямой или перекрестный)

ОписаниеконфигурациипортаPort Description configuration

Коммутаторы DES-3200-18 поддерживает функцию описание порта. Чтобыпросмотретьследующееокно, щелкните

Configuration > Port Configuration > Port Description Settings(Рис. 6.5.)

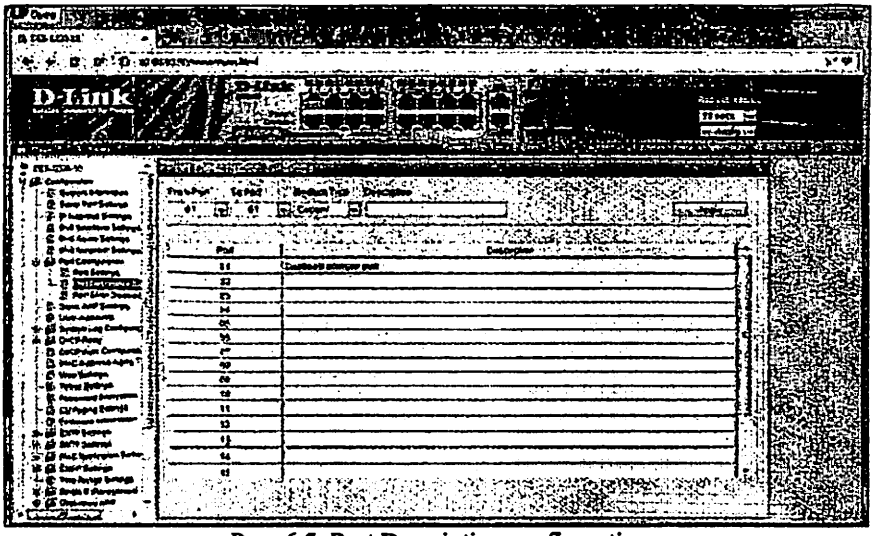


Рис. 6.5. Port Description configuration

КонфигурацияучетнойзаписипользователяUserAccountconfiguration

Чтобыпросмотретьследующееокно, щелкните**Configuration>UserAccountSettings** (Рис. 6.6.) Для добавления нового пользователя введите имя пользователя, пароль и повторно введите тот же пароль. Выберите уровень привилегий (Администратор, Оператор, Пользователь или Пользователь) из доступ выпадающего меню.

Таблица 6.3

Права доступа для разных уровней привилегий

Management	Admin	Operator	Power User	User
конфигурирование	Read/Write чтение/запись	Read/Write (partly) чтение/запись (частично)	Read/Write (partly) Read/Write (partly) чтение/запись (частично)	No нет
Мониторинг	Read/Write чтение/запись	Read/Write чтение/запись	Read-only Только чтение	Read-only Только чтение

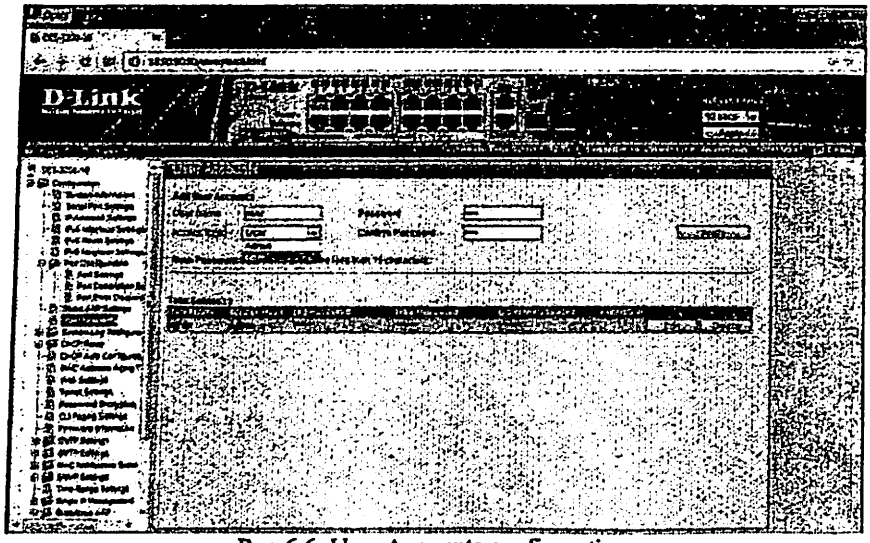


Рис.6.6. User Accounts configuration

System IP Address configuration

ПоумолчаниюкоммутаторуприсвоенIPадрес 10.90.90.90 смаскойподсети (subnetmask) 255.0.0.0 идefaultgatewayof 0.0.0.0.Чтобыоткрытьокнощёлкните**Configuration>IPAddressSettings** (рис. 6.7.)

Таблица 6.4

Получение параметров IP-адреса

Параметр	Описание
Static	Ручнаяустановка IP адреса
DHCP	назначение параметров IP-адреса с помощью DHCP-сервера
BOOTP	назначения параметров IP-адреса с помощью BOOTP -сервера

Таблица 6.5

ПолядлянастройкиSystemInterface

параметр	описание
Interface Name	Определяет имя системного интерфейса
Management VLAN Name	Определяет имя VLAN
Interface AdminState	Установкавкл/выкл (enable/disable) на интерфейсе
IPv4 Address	Связывает IP адрес с данным интерфейсом
Subnet Mask	Связываетмаскуподсетис данным интерфейсом
Gateway	Определяетшлюз по умлчанию для удалённого соединения коммутатора

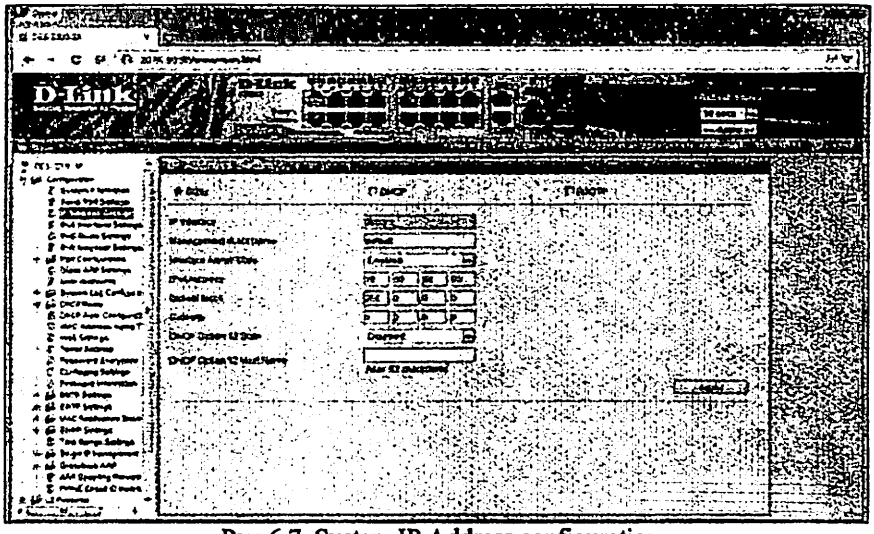


Рис.6.7. System IP Address configuration

802.1QVLANConfiguration

Чтобыоткрытьокнощёлкните**L2 Features> 802.1QStaticVLAN** (рис. 6.8.)

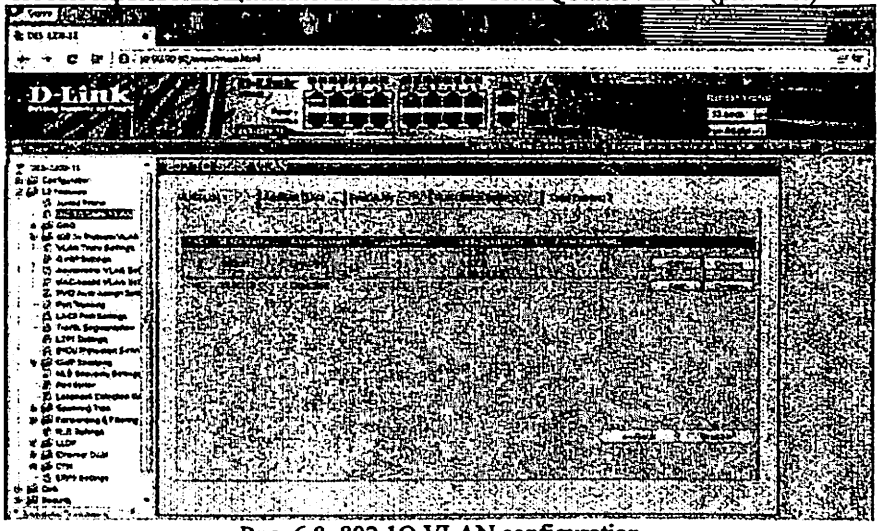


Рис. 6.8. 802.1Q VLAN configuration

Длясозданиянового802.1QVLANилимодификациисуществующего802.1QVLANщёлкните**Add/EditVLAN**tab (рис. 6.9.)

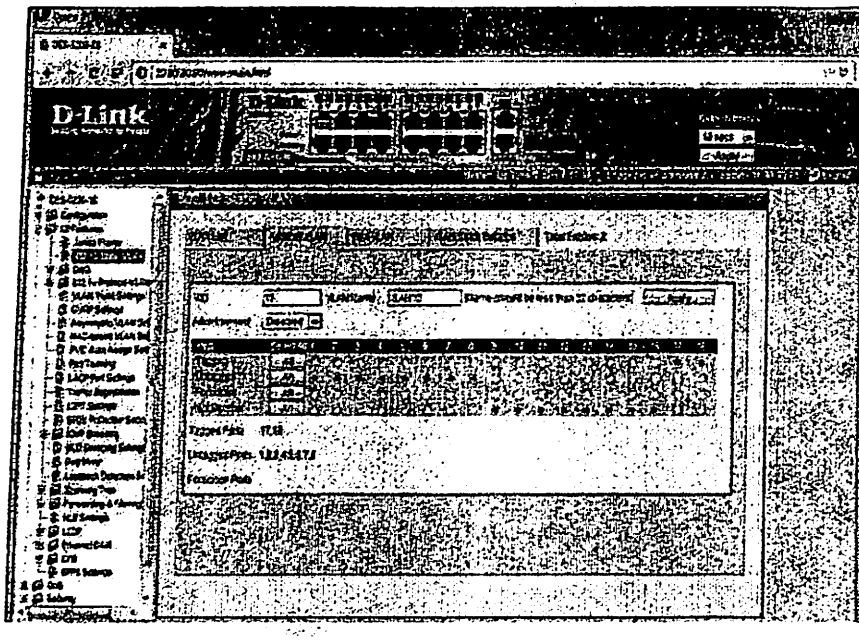


Рис. 6.9.ОкноAdd/EditVLAN

Таблица6.6

ПарметрыAdd/Edit VLAN

параметр	описание
VID	Ввести VLAN ID
VLAN Name	Ввести имя VLAN
Advertisement	ПосылкаGVRP пакетов разрешена
Tagged	Определить портв виде 802.1Qtagged (с тэгами)
Untagged	Определить портв виде 802.1Quntagged (без тэгов)
Forbidden	ЗапретитьпортубытьчленомVLAN(динамически)
Not Member	Позволить порту бытьпоп-VLANmember

Для поиска VLAN, перейдите на вкладку **FindVLAN.**

Чтобы создать, удалить и настроить пакета записейVLAN перейдите на вкладку **VLANBatchSettings** (рис. 6.10.)

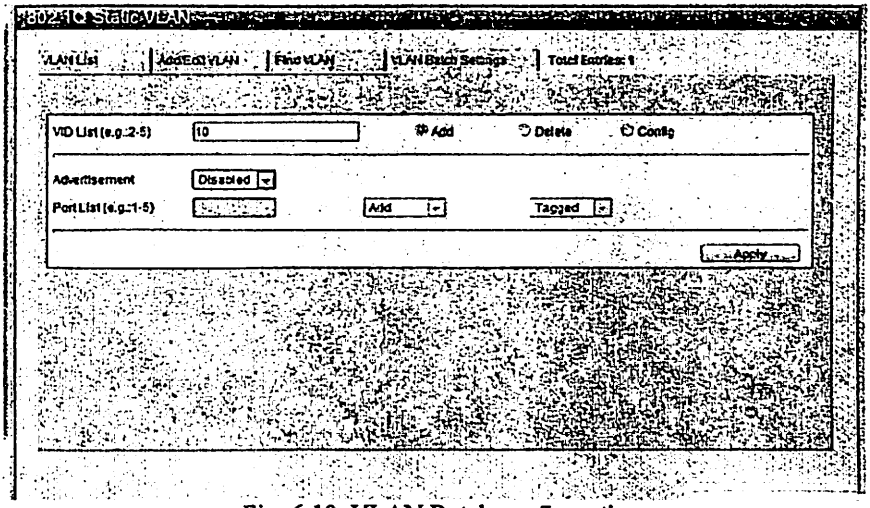


Fig. 6.10. VLAN Batch configuration

ПараметрыLoopbackDetectionSettings

Функция LoopbackDetection (LBD) используется для обнаружения петель на определенном порту. Эта функция используется, чтобы временно закрыть порт на коммутаторе CTP пакет (ConfigurationTestingProtocol) проходит по петле обратно к коммутатору.Для просмотра этого окна, щелкните функции **L2 Features>LoopbackDetectionSettings** (Рис. 6.11.)

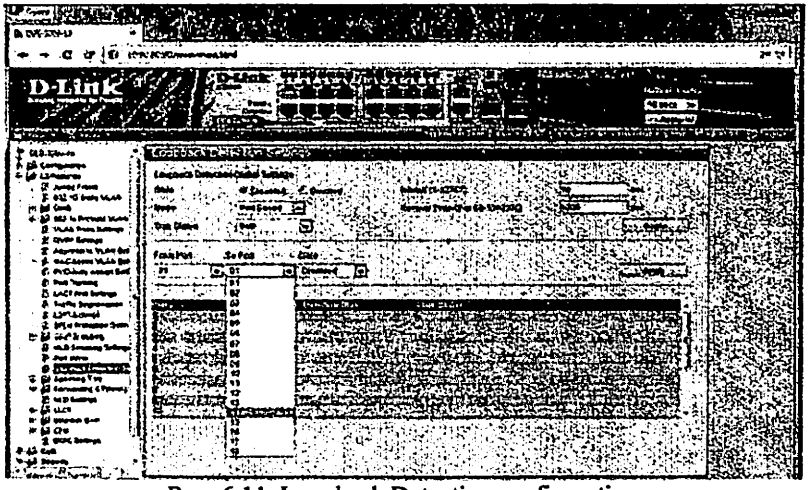


Рис. 6.11. Loopback Detection configuration

Мониторинг (Ping Test)

Pingэтомаленькаяпрограмма, котораяпосылаетICMPEchoпакеты по направлению к указанному Вами IP адресу.Узел назначения отвечает или "Эхо" пакеты, отправленные с коммутатору. Это очень полезно для проверки подключения между коммутатором и другими узлами в сети.

Дляпросмотраокнавыполните**Monitoring>PingTest**(рис. 6.12.)

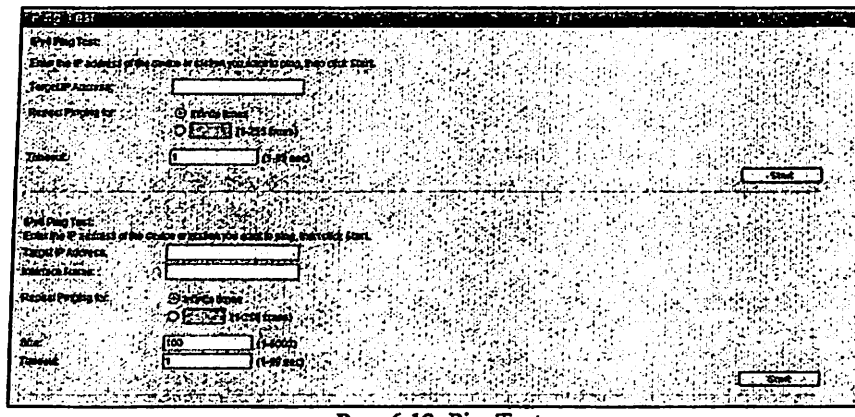


Рис. 6.12. PingTest

Изучение технических характеристик оборудования ZyXel IES-1000 DSLAM и настройка параметров порта xDSL - VPI/VCI. Создание статического VLAN. Управление подключением на основе MAC-адресов

Практическое занятие №10,11

ИЗУЧЕНИЕ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК ОБОРУДОВАНИЯ ZYXEL IES-1000 DSLAM И НАСТРОЙКА ПАРАМЕТРОВ ПОРТА XDSL - VPI/VCI. СОЗДАНИЕ СТАТИЧЕСКОГО VLAN. УПРАВЛЕНИЕ ПОДКЛЮЧЕНИЕМ НА ОСНОВЕ MAC-АДРЕСОВ

1. Цель и содержание занятия

Изучение конфигурирования интерфейсов DSLAM, конфигурирования коммутатора через веб-интерфейс, настройки VLAN на портах коммутатора и управление соединениями с MAC-адресами.

2. Заданиекзанятию

Сконфигурировать интерфейс DSLAM с помощью Web-интерфейса. Изучить характеристики и поддерживаемые протоколы DSLAM.

3. Порядоквыполнения

1. Сконфигурировать интерфейс DSLAMи сконфигурироватьVLAN
2. Изучить теоретическую часть работы
3. Ответить на контрольные вопросы
4.Составить отчёт по работе

4. Содержаниеотчета

1. Краткая характеристика DSLAMи шаги конфигурирования.
2. Сервисы DSLAMсети доступа.
3. Результаты конфигурации DSLAMи VLAN порты.

5. Контрольныевопросы

1. Какие функции выполняетDSLAM?
2. Что такое VPI/VCI в порты?
3. Как настроить xDSL порты?
4. Что такое MAC-адресDSLAM?
5. Какие приложения можно использовать для настройки DSLAM?
6. Как осуществляется процесс мультиплексирования в DSLAM?

6. Теоретическиесведения

ZyXELIES-1000 configuration

IES-1000 поддерживает web-интерфейс для конфигурирования модулей DSL. По умолчанию IP-адрес модуля DSL является 192.168.1.1
Для доступа к WebConfiguratorнеобходим любой веб-браузер (рис. 7.1.) и информация для процедуры аутентификации (Рис. 7.2.).
Примечание: имя пользователя по умолчанию (admin) и пароль (1234)

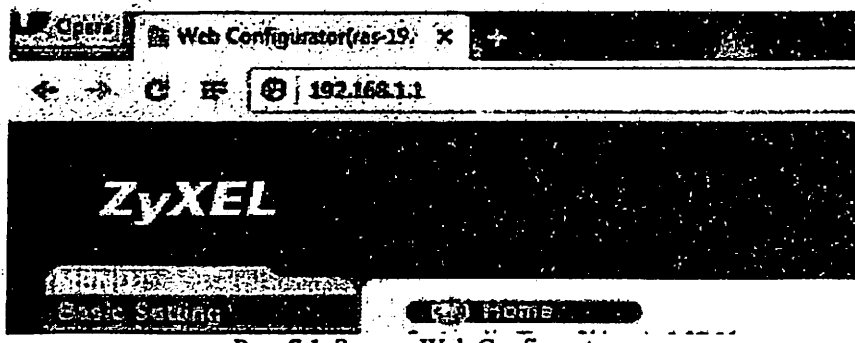


Рис. 7.1. Запуск Web Configurator

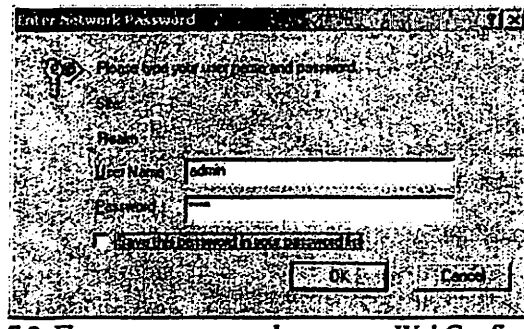


Рис. 7.2. ПроцедурааутентификациинаWebConfigurator

Информация о Системе SystemInformation

Чтобы настроить характеристики системы, выберите **BasicSettings>GeneralSetup** (Рис. 7.3.)

Общие установки **GeneralSetup** состоят из двух областей:

- SystemInformation (Area 1) – настройки информация о системе
- SystemTime (Area 2) – для настройки времени/даты синхронизации системы

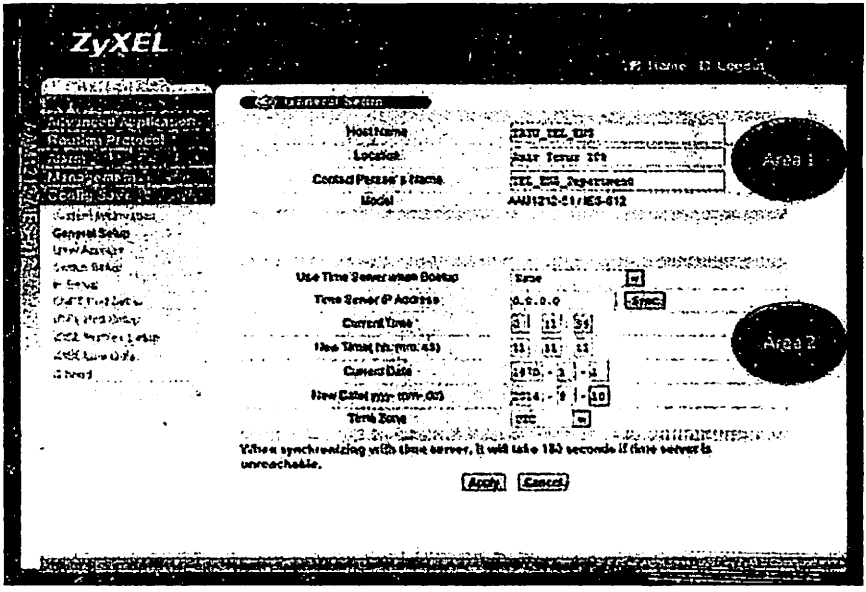


Рис. 7.3. IES-1000 General configuration

КонфигурацияУчетнойЗаписиПользователяUserAccountConfiguration

Чтобы настроить сведения о проверке подлинности пользователей, выберите **UserAccount** в панели навигации (Рис. 7.4.)

Для добавления нового пользователя необходимо заполнить все обязательные поля (имя, пароль, пароль для подтверждения) и выбрать уровень привилегий.

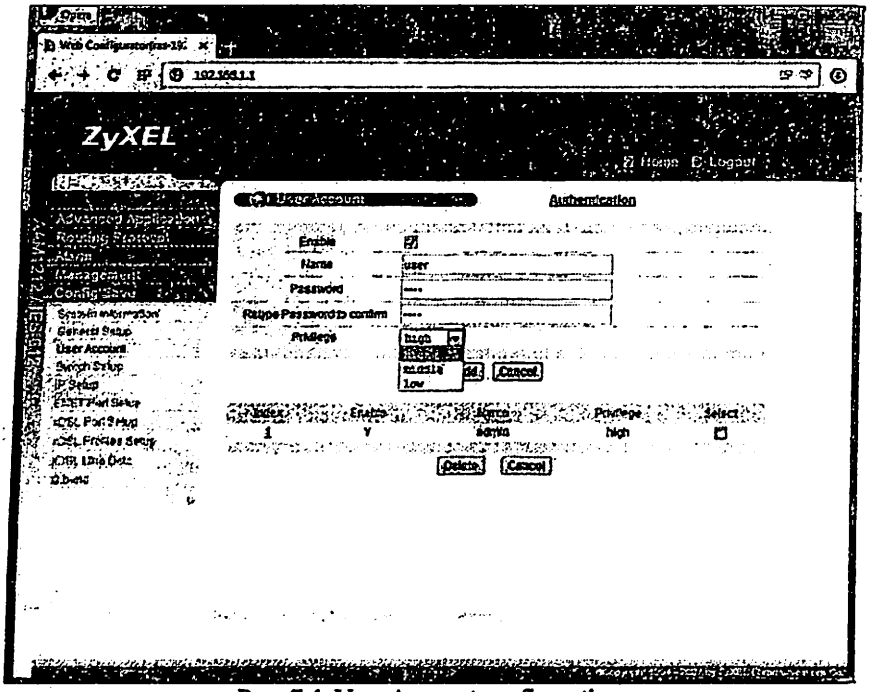


Рис. 7.4. User Account configuration

Management IP Address Configuration

Дляизмененияустановок IP адреса, выбранныхпоумолчанию, выберите **IP Setup** на панели навигации (рис. 7.5.)

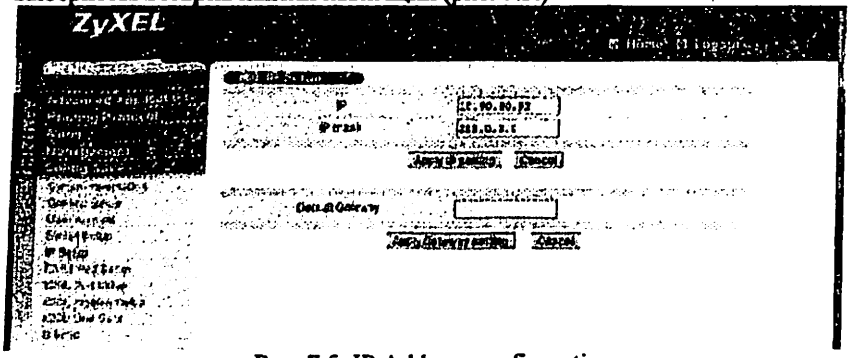


Рис. 7.5. IP Address configuration

ПоумолчаниюIPадрес 192.168.1.1/24 идefaultgateway 192.168.1.254

НастройкаxDSLпортовxDSLPortSetup

Чтобыоткрытьэтотэкран (Рис.7.5.), нажмитекнопку**BasicSetting>xDSLPortSetup**

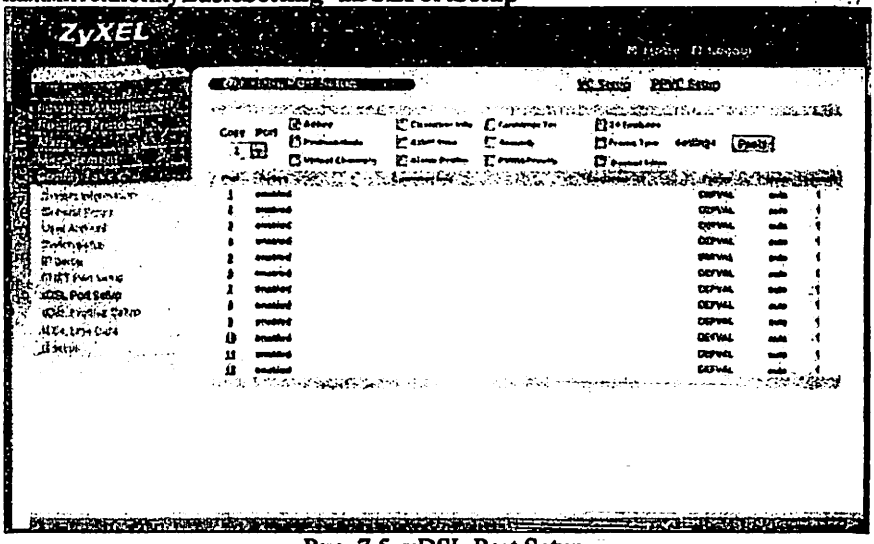


Рис. 7.5. xDSL Port Setup

Выберитеномерпортадляиндивидуальнойнастройкикаждогопорта (Рис. 7.6.)

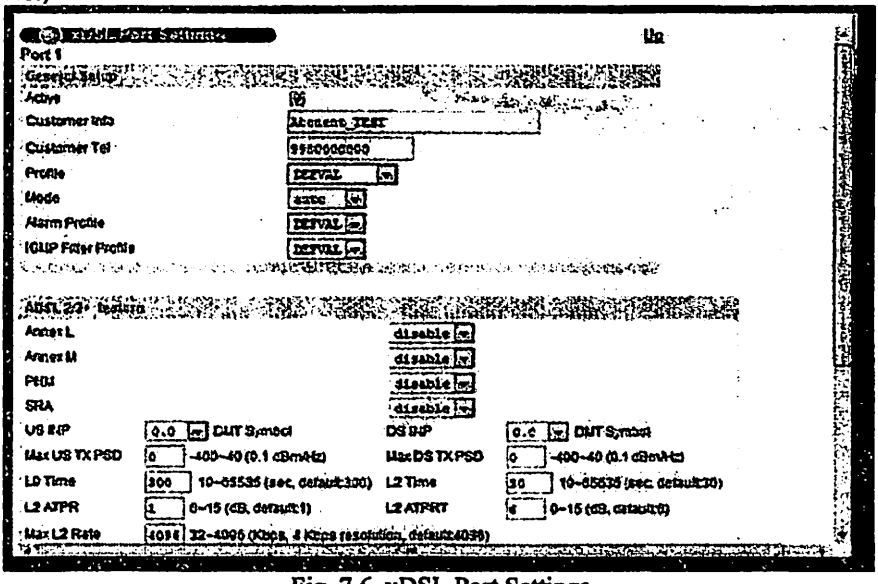


Fig. 7.6. xDSL Port Settings

НастройкаxDSLпрофилякxDSL Profiles Setup

Профиль представляет собой список предварительно настроенных параметров ADSL, который может быть назначен один или несколько отдельных портов. Чтобы открыть этот экран (Рис. 7.7.), нажмите **BasicSetting>xDSLProfilesSetup**

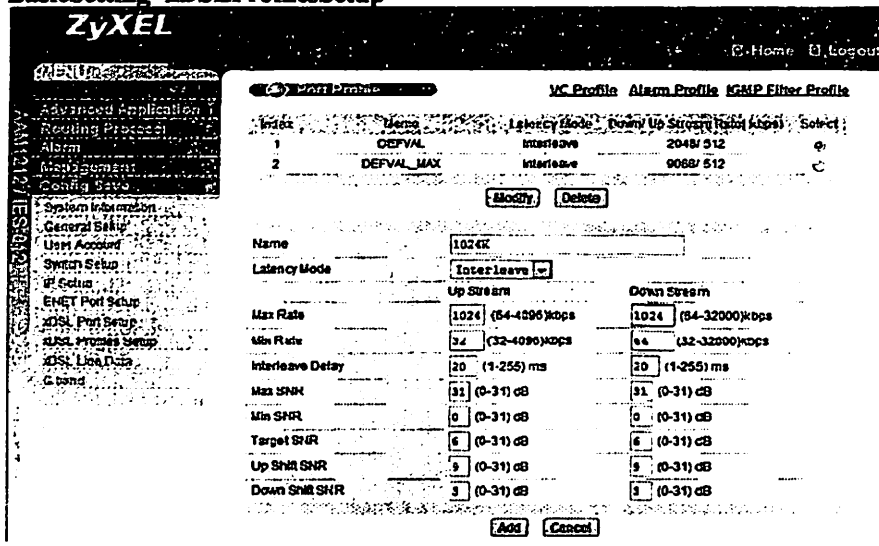


Рис. 7.7. Port Profile configuration

ВыберитеVCProfileURLдляконфигурированияпрофилявиртуальнойцеп и (рис. 7.9.)

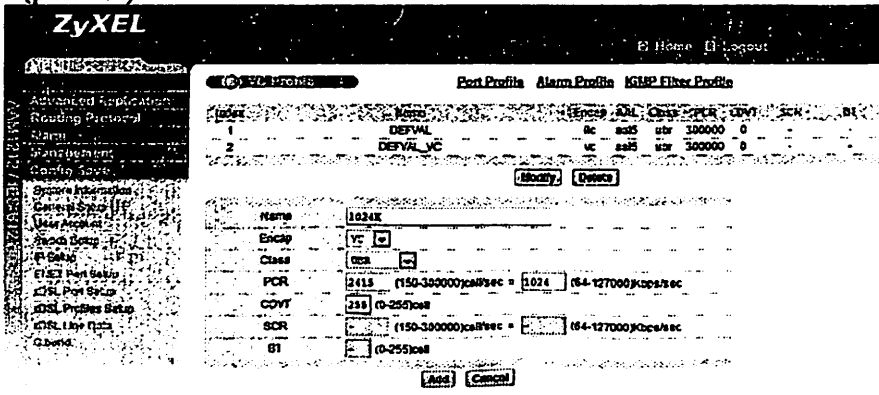


Рис. 7.9. Virtual Circuit Profile configuration

Virtual Circuit configuration

Дляконфигурированияпорта PVCвыберитеBasic Setting >xDSL Port Setup > VC Setup (рис. 7.10.)

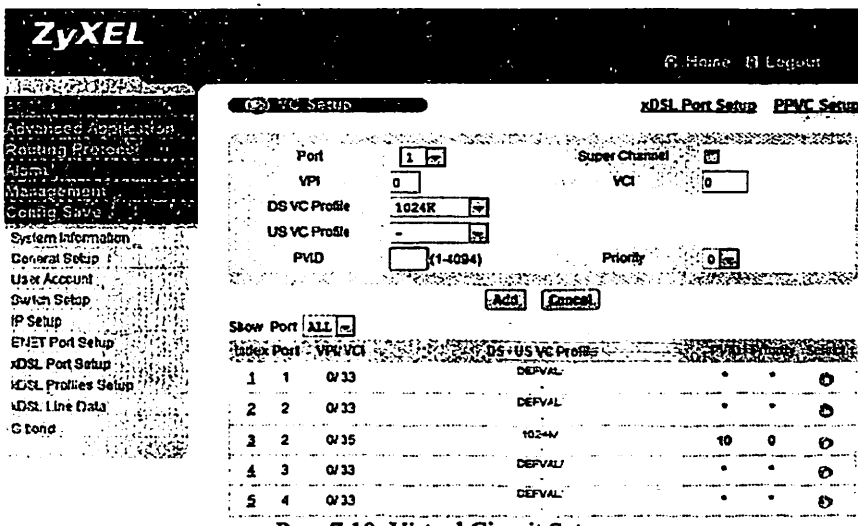


Рис. 7.10. Virtual Circuit Setup

Virtual Local Area Network (VLAN) configuration

ДляконфигурированияVLANs, выберитеAdvanced Application > VLAN (рис. 7.11.)

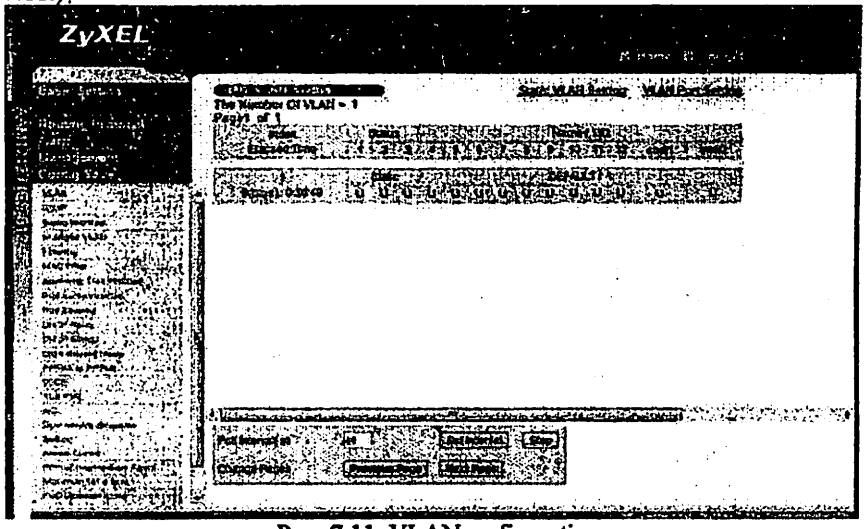


Рис. 7.11. VLANconfiguration

Длятого, чтобыпривязатьпорткгруппеVLANилизапретитьпортуприсоединятьсякгруппеVLANвыберитеStaticVLANSettingURL (рис.7.12.)

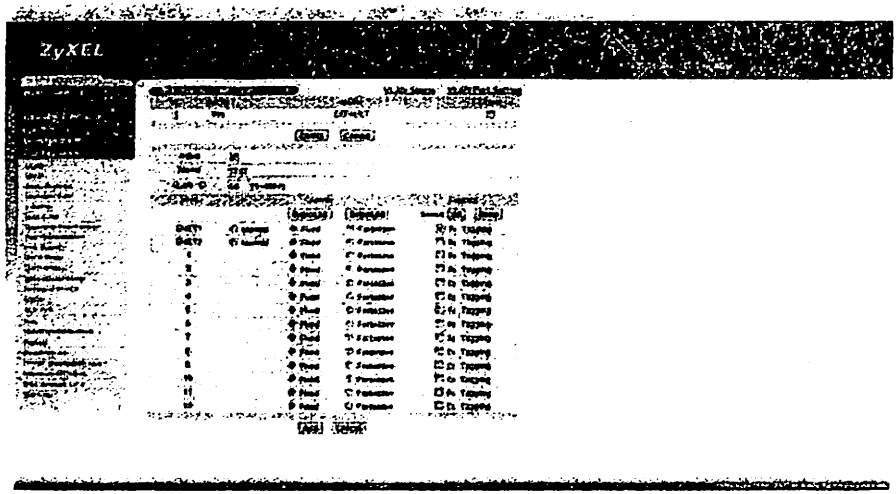


Рис. 7.12. Статическое конфигурированиеVLAN

Чтобы указать порт VLANID и установить, является ли онEthernet-портом или нет, распространить информацию о VLAN на другие устройства, выберите VLANPortSettingURL (Рис. 7.13.)

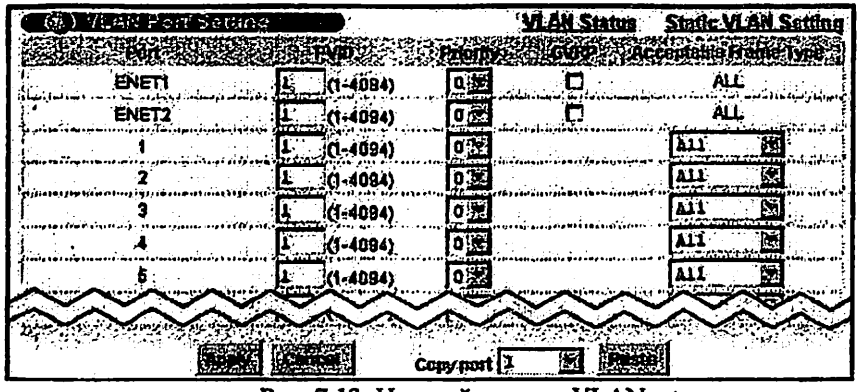


Рис. 7.13. Настройки портаVLAN

Настройки фильтра по MAC-адресуMACFilterconfiguration

Для того, чтобыпроконтролировать может или нет кадр с данногоMAC-адресапоступать в порт, выберите AdvancedApplication>MACFilter (Рис.7.14.)

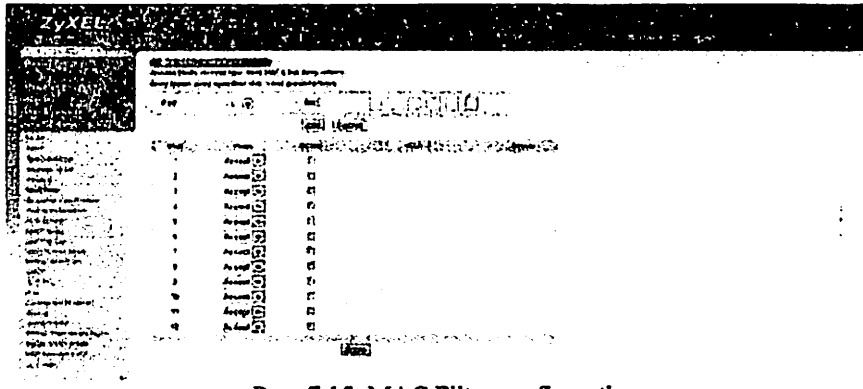


Рис. 7.15. MAC Filter configuration

PVC Upstream Limit Configuration

Дляограниченияскоростипередачиupstream потокачерезPVCвыберите**Advanced Application > PVC Upstream Limit** (рис. 7.16.)

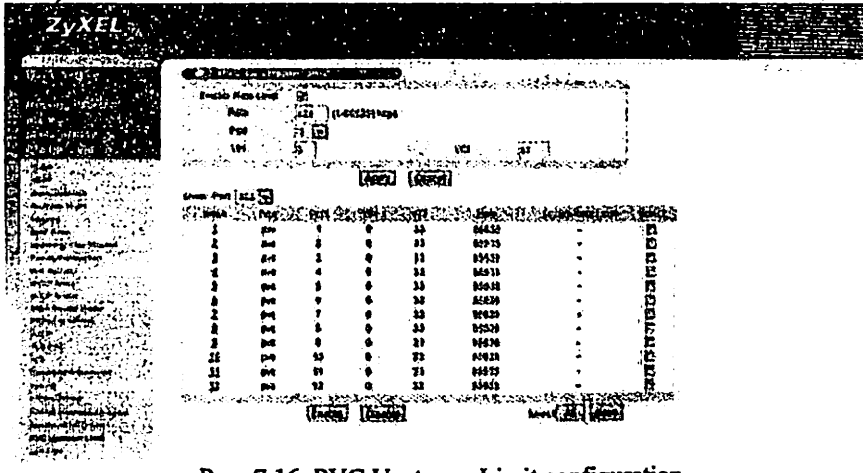


Рис. 7.16. PVC Upstream Limit configuration

Процедурыдиагностики Diagnostic procedure

Дляпроверкисистемныхлогов, результатовоперации ping IP addresses илизапускаloopback testsвыберите**Management > Diagnostic** (рис. 7.17.)

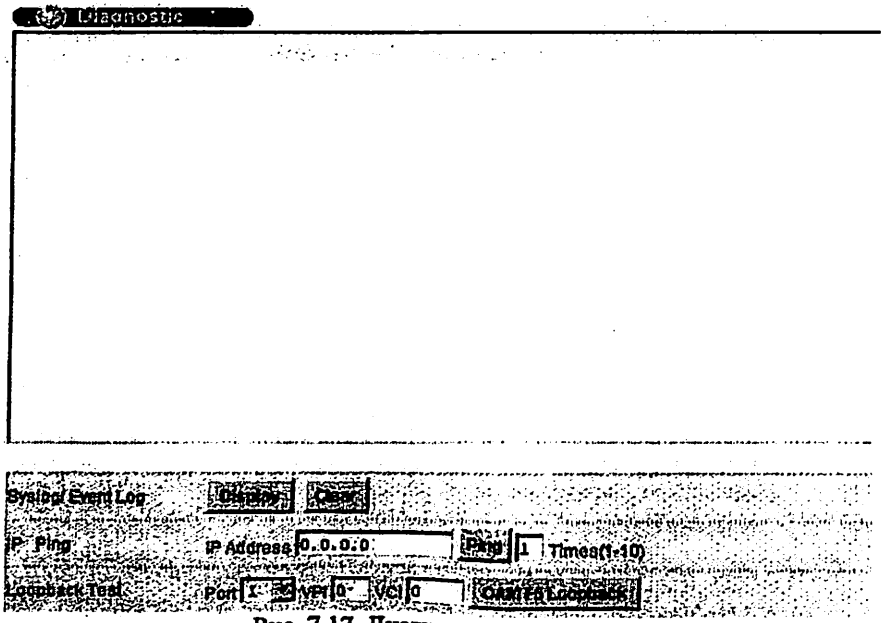


Рис. 7.17. Диагностический тест

Практическое занятие №12

ИЗУЧЕНИЕ АЛГОРИТМА КАНАЛЬНОГО УРОВНЯ 802.11 CSMA/CD И ПЕРЕДАЧА ИНФОРМАЦИИ НА ФИЗИЧЕСКОМ УРОВНЕ НА ОСНОВЕ MAC-АДРЕСОВ

1. Цельисодержаниезанятия

Изучениеконфигурирования IAD208 и алгоритма CSMA/CDв проводной сети доступа.

2. Заданиекзанятию

Сконфигурировать интерфейс IAD208 с помощью Web-интерфейса. Изучить характеристики и поддерживаемые протоколы IAD208, беспроводного модема ADSL2+.

3. Порядоквыполнения

1. Сконфигурировать интерфейс IAD208, беспроводного модема ADSL2+
2. Изучить теоретическую часть работы
3. Ответить на контрольные вопросы
4.Составить отчёт по работе

4. Содержаниеотчета

1. Краткая характеристика интерфейс IAD208, беспроводного модема ADSL2+и шаги конфигурирования.
2. Сервисы интерфейс IAD208, беспроводного модема ADSL2+сети доступа.

5. Контрольныевопросы

1. Какие функции выполняетIAD208?
2. Какие функции выполняетбеспроводный модемADSL2+?
3. Как настроить портыIAD208, беспроводного модема ADSL2+?
4. Что такое MAC-адресDSLAM?
5. Какие приложения можно использовать для настройки интерфейсаIAD208, беспроводного модема ADSL2+?
6. Как осуществляется процесс пакетизации в IAD208?

6. Теоретическиесведения

Конфигурирование IAD208 фирмыHuawei

IAD208 предоставляет пользователям веб-систему управления. Система запускает страницу поддержки только в InternetExplorer. Страница является простой в использовании. Вы можете настроить большинство функций в веб-режиме.

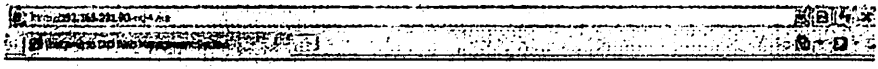
Входввеб-интерфейссистемыуправления Logging In to the Web Management

Перед входом в веб-интерфейс системы управления, необходимо создать среду конфигурации.

Используйте перекрестный кабель для подключения сетевого порт компьютера к порту WANIAD208E(M). Если сетевой порт ПК поддерживает самоадаптацию, вы можете использовать прямой кабель. Набор IP-адресов ПК и IAD одинаков в сегменте сети. Например, IP-адрес по умолчанию IAD является 192.168.100.1, то адрес ПК может быть установлен на 192.168.100.2.

Для входа в систему введите IP-адрес IAD (Рис. 8.1), далее введите имя пользователя и пароль и нажмите кнопку **Login**.

Примечание: по умолчанию имя пользователя**root** и пароль **admin**



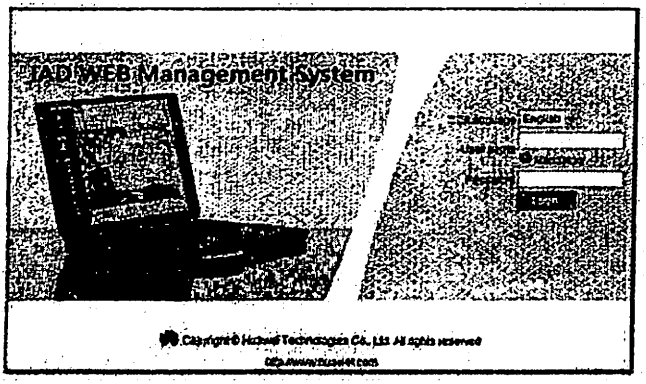


Рис. 8.1. Вход в Web интерфейс IAD

Network Parameter Settings

Для конфигурирования параметров сети выберите **Basic Configuration > Network Parameter** (рис. 8.2.)

В следующей таблице описаны ярлыки на этом экране (Таблица 8.1)

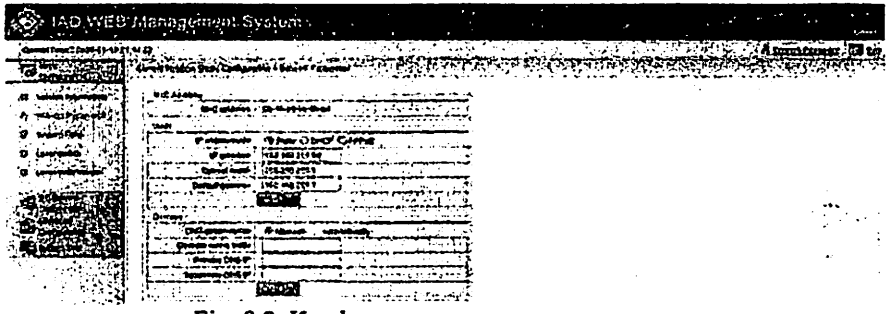


Fig. 8.2. Конфигурирование параметров сети

Таблица 8.1

Network Parameters

Параметр	Описание
IP obtain mode	Определяетметодполучения IP адреса IAD
IP address	Устанавливает статический IP адрес
Subnet Mask	Устанавливает статическую маску подсети
Default Gateway	Устанавливает статический default gateway
DNS obtain mode	Определяетметодполучения IP адреса от DNS
Domain name suffix	Определяетсуффиксдоменногоименидляускоренияпоиска
Primary DNS IP	Устанавливает IP адресот PrimaryDNS
Secondary DNS IP	Устанавливает IP адресотSecondaryDNS

НастройкаSIP сервераSIP Server Settings

Дляконфигурированияпараметровтелефонногосервера SIP, выберитеSIPServiceConfiguration>SIPServer (рис. 8.3.)

В таблице 8.2 описаны ярлыки на этом экране.

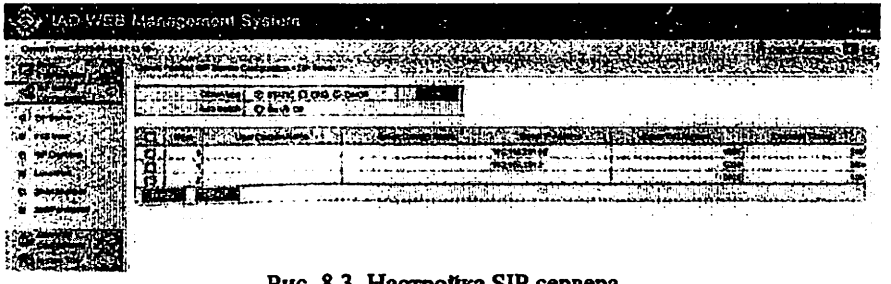


Рис. 8.3. Настройка SIP сервера

Таблица 8.2

Настройка SIP сервера

Параметр	Описание
Obtain type	Определяетметодполучения информации SIPсервера
Auto switch	IADавтоматическипереключаетсямеждуSIPсерверами
User Domain Name	Установка доменного имени пользователя
Server Domain Name	Установка доменного имени от SIPсервер
Server IP Address	УстановкаIPадреса для SIP сервера
ServerPort Number	Установка номера порта под сервер
Expiration Time	SIPServerregistrationexpirationtimeдлительность времени регистрации на SIP сервере

Конфигурирование пользователей FXS– FXSUsersConfiguration

ДлярегистрацииипользователейSIPвыберитеSIPServiceConfiguration>FXSUser (рис. 8.4.)

The following table describes the labels in this screen (Table 8.3)

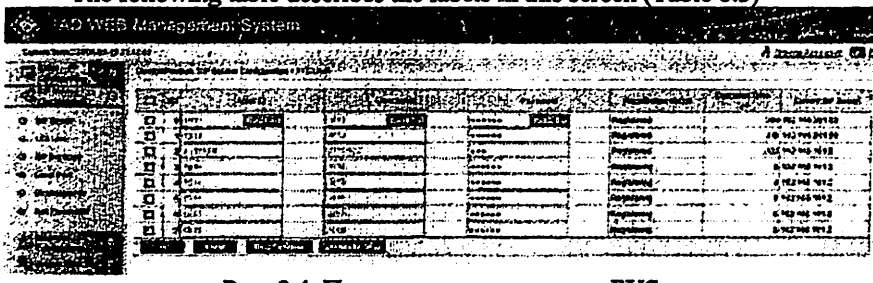


Рис. 8.4. Параметры пользователя FXS

Таблица 8.3

Параметры пользователя FXS

Параметр	Описание
User ID	Идентификатор пользователя
User name	alias-адрес пользователя
Password	пароль пользователя для аутентификации
Expiration Time	Срокдействиярегистрации
Current SIP Server	IPадрес текущего SIP сервера

Конфигурирование устройства широкополосного доступа H108Nфирмы ZTE

IP-адресаПКиZXHNH108Nдолжныналодитсяводномсегментесети.ПоумолчаниюZXHN H108N имеет следующие установки:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

Вход в систему управления Logging In to the Device

ДляначалаконфигурированияH108Nчерезweb-интерфейсвойдитенаweb-страницу (рис. 8.5.). Web страницаобеспечиваетразличныевидыконфигурации(таблица 8.4)

Таблица 8.4

Права пользователей

Role	Username/Password	Права Permission
Administrator	1234/1234	Разрешенывседействиянастранице
Common users	user/user	Имеется разрешение на просмотр некоторых конфигураций

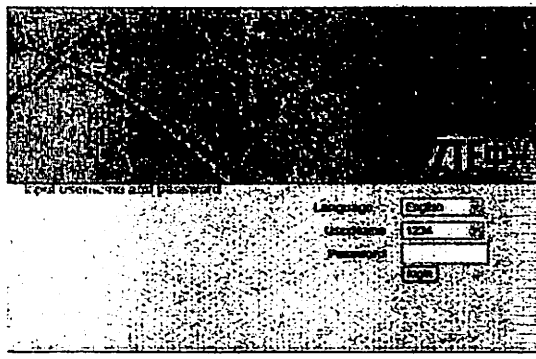


Рис. 8.5. H108N Login Page

КонфигурированиелокальнойсетиConfiguring the Local Network

Для конфигурирования локальной сетимаршрутизаторавыберитеSetup>LocalNetwork (рис. 8.6.)

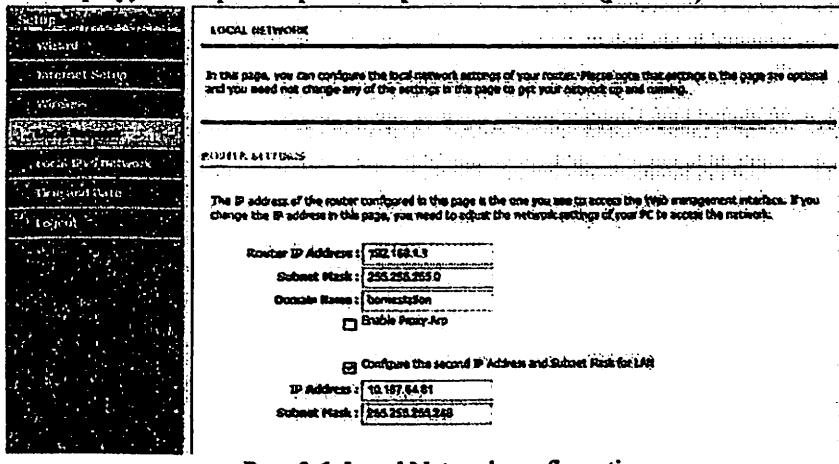


Рис. 8.6. Local Network configuration

Configuring Basic Wireless Parameters

Дляконфигурированияпарметровбеспроводногодоступавыберите **Setup>Wireless>WirelessBasic** (рис. 8.6.)

Таблица 8.6 содержит описание базовых параметров беспроводной сети.

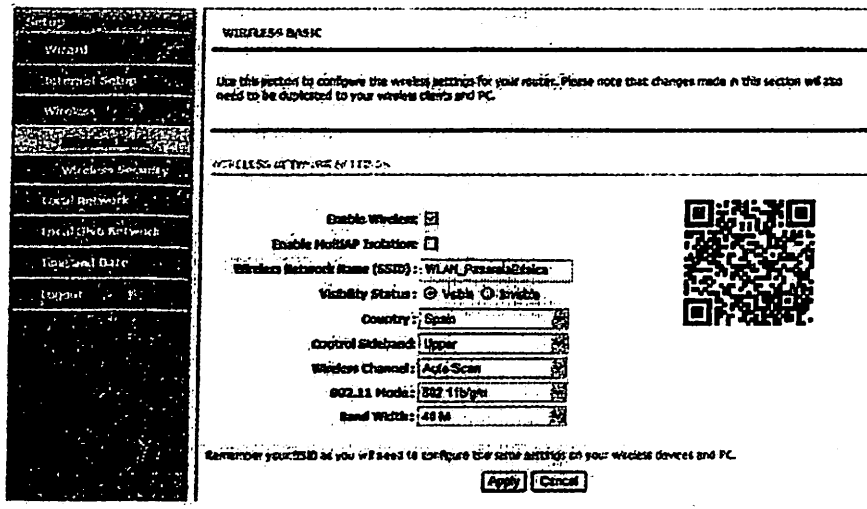


Рис. 8.6. конфигурирование базовых параметров беспроводной сети

Таблица 8.6

Описаниебазовыхпараметровбеспроводнойсети

Параметр	Описание
MultiAP Isolation	To isolate multiple SSIDs
SSID	Установка имени беспроводной сети
Control Sideband	задать направление полосы для канала управления
Wireless Channel	выбрать определенный канал для развертывания беспроводной сети
802.11 Mode	Установить режимWi-Fi
Bandwidth	Установитьдиапазондо 40МГцили 20МГц

ConfiguringaStaticRoute

Дляконфигурированиястатическоймаршрутизациивыберите**Advanced> Routing>StaticRoute** (рис. 8.7.). Таблица 8.7 содержитописаниебазовыхпараметровстатическоймаршрутизации.

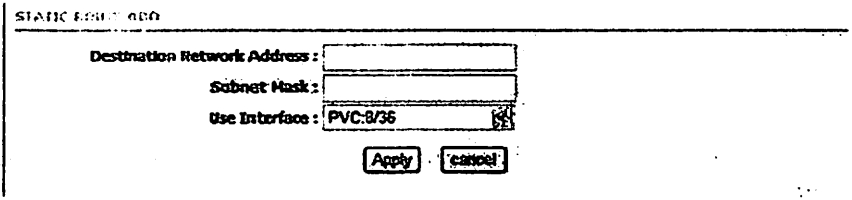


Рис.8.7. Конфигурированиястатическоймаршрутизации

Таблица 8.7

Параметры статическоймаршрутизации

Параметр	Описание
Destination address	Установить адрес назначения
Subnet Mask	Установитьмаску подсетиназначения
Use Interface	Определить широкополосный канал для пересылки

Список литературы

Основная литература

1. J.Kurose, K.Ross. Computer networking. Sixth edition. Pearson Education, 2013.
2. В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы4-е издание Москва, Санкт-Петербург, 2010.
3. Ўзбекистон Республикасини янада ривожлантириш бўйича харакатлар стратегияси тўғрисида. Ўзбекистон Республикаси Президентининг ПФ-4749-сон фармони. Тошкент, 2017 йил 7 феврал.
4. В.П. Комагоров. Технологии сети Интернет: протоколы и сервисы. – Томск: Томский политехнический университет, 2009. – 107с.
5. Таненбаум Э. Компьютерные сети. Изд.4./Изд. ПИТЕР, 2003
6. Садчикова С.А. IP-ТЕЛЕФОНИЯ. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. Ташкент. ТУИТ.2008

Дополнительная литература

1. Мирзиёев Ш.М. Буюк келажагимизни мард ва олижаноб халқимиз билан бирга қурамиз. 2017.
2. Мирзиёев Ш.М. Қонун устуворлиги ва инсон манфаатларини таъминлаш юрт тараққиёти ва халқ фаровонлигининг гарови. 2017.
3. Мирзиёев Ш.М. Танқидий таҳлил, қатъий тартиб-интизом ва шахсий жавобгарлик – ҳар бир раҳбар фаолиятининг кундалик қоидаси бўлиши керак. Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2016 йил якунлари ва 2017 йил истиқболларига бағишланган мажлисидаги Ўзбекистон Республикаси Президентининг нутқи. // Халқ сўзи газетаси. 2017 йил 16 январь, №11.
4. Мирзиёев Ш.М. "Тошкент ахборот технологиялари университетининг фаолиятини янада такомиллаштириш чора-тадбирлари тўғрисида" га қарори. ПҚ-2834, 15.03.2017.
5. Хомоненко А.Д. Основы современных компьютерных технологий: Учебник для ВУЗ. – С-Пб.: КОРОНА-принт, 2006 г.
6. ШаттСтэн Мир компьютерных сетей, пер. с англ. - К.: BHV, 2004 г.
7. Галкин В.А., Ю.А. Григорьев. Телекоммуникации и сети. Учебник для бакалавров направлений «Информационные технологии». Москва, МГТУ им.Н.Э.Баумана, 2003
8. Еркинбаева Л.Т., Садчикова С.А., Каюмова Г.А. Телекоммуникационные системы и сети. Методическое пособие для проведения практических занятий. ТУИТ. Ташкент 2012.
9. Chris Hellberg, Dylan Greene, Truman Boyes. Broadband Network Architectures designing and deploying Triple-play services. Pearson Education

2007.
10. CISCO Packet Tracer – Сетевая академия. – официальный сайт.– URL:https://www.netacad.com/ web/about-us/cisco-packet-tracer.
11. 1. Broadband Network Architectures designing and deploying Triple-play services. Chris Hellberg, Dylan Greene, Truman Boyes. Pearson Education 2007.
12. 2. Packet Broadband Network Handbook. The McGraw-Hill Companies. 2004
13. 3. Broadband optical access networks. Leonid g. Kazovsky. A john wiley & sons, inc., publication. 2011
14. 4. Broadband Access Networks. Technologies and Deployments. Abdallah Shami, Martin Maier. Springer Science 2009.
15. 5. Computer Networking A Top Down Approach. James. F. Kuross. Pearson Education 2013.
16. http://www.intuit.ru/studies/courses/509/365/info
17. Материалы курса «IP-телефония в компьютерных сетях» сайта Интернет-Университета Информационных Технологий
18. http://www.intuit.ru/studies/courses/8/8/info
19. Шарифов Р.А. Садчикова С.А. Тилляев С.Д. IP-телефония. Методическое пособие лабораторных работ по дисциплине «IP-телефония» для магистрантов специальностей 5А522202, 5А522203, 5А522205, 5А522216. Ташкент, ТУИТ. 2008.http://www.teic.uz/lib
20. Шарифов Р.А., Садчикова С.А. Методическое пособие для практических занятий по предмету «IP-телефония». Ташкент, ТУИТ, 2008
21. http: // www. teic.uz/ lib

ОГЛАВЛЕНИЕ

«Широкополосные сети»
Методическое пособие для практических работ
для студентов, обучающихся по направлениям образования
5350100 – Телекоммуникационные технологии
(Телекоммуникация, телерадиовещание, мобильные системы)

Рассмотрено и одобрено на заседании каф. ТИ. Протокол заседания кафедры ТИ № 34 от 27.03.2018 г.

Рассмотрено и одобрено на заседании НМС факультета ТТ. Протокол заседания НМС ф-та ТТ № 8 от 03.04.2018г.

Рекомендовано к тиражированию НМС в типографии ТУИТ. Протокол заседания НМС № 9 от 20.04.2018г.

Авторы издания: Садчикова С.А., Абдужаппарова М.Б., Давлетова Х.Р.

Ответственный редактор:Гультураев Н.Х.

Корректор: Хамдам-Зода Л.Х.

Бичими 60x84 1/16. Босма табоғи 14,5
Адади 30. Буюртма - № 242
Тошкент ахборот технологиялари университети
"Мухаррирлик нашр" бўлимида чоп этилди.
Тошкент ш, Амир Темур кўчаси, 108-уй