

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

HLASOVÁ SLUŽBA V INTEGROVANÝCH SÍTÍCH

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. ALIAKSANDR YEFTSIFEYEU

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNologiÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

HLASOVÁ SLUŽBA V INTEGROVANÝCH SÍTÍCH

VOICE SERVICE WITHIN INTEGRATED NETWORKS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

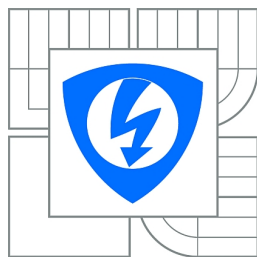
AUTHOR

Bc. ALIAKSANDR YEFTSIFEYEU

VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. VLADISLAV ŠKORPIL, CSc.



**VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ**

**Fakulta elektrotechniky
a komunikačních technologií**

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Aliaksandr Yeftsifeyeu

ID: 119805

Ročník: 2

Akademický rok: 2013/2014

NÁZEV TÉMATU:

Hlasová služba v integrovaných sítích

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se podrobně s problematikami směrování a VoIP v Cisco sítích. Nastudujte konfiguraci Cisco UCM, protokolů SCCP, SIP a využití MPLS v transportních sítích. Navrhněte topologii sítě tak, aby při přerušení fyzického propojení proběhlo přesměrování provozu s minimálním zpožděním. V transportní části sítě použijte MPLS. Do 3 přístupových směrovačů připojte 3 IP telefony Cisco, dále pak VoIP telefonní síť postavenou nad PBX SMC. Síť nakonfigurujte tak, aby bylo možno volat vždy v rámci PBX. Pomocí testů RFC 2544 a V-SAM proměřte QoS parametry transportní sítě. Použijte např. analyzátor VePAL TX300e nebo jiný vhodný.

DOPORUČENÁ LITERATURA:

- [1] WALLACE, K. Cisco VoIP, autorizovaný výukový průvodce. Computer Press, Brno 2009
- [2] ODOM, W., HEALY, R., MEHTA, N. Směrování a přepínání sítí, autorizovaný výukový průvodce. Computer Press, Brno 2009
- [3] PUŽMANOVÁ, R. Moderní komunikační sítě A-Z. Computer Press, Brno 2007

Termín zadání: 10.2.2014

Termín odevzdání: 28.5.2014

Vedoucí práce: doc. Ing. Vladislav Škorpil, CSc.

Konzultanti diplomové práce:

prof. Ing. Kamil Vrba, CSc.

Předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

Výzkum popsáný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Abstrakt

Diplomová práce se zabývá směrovacími protokoly, uvádí komunikaci protokolu SIP a SCCP, podrobně popisuje moderní VoIP technologie a její konfigurace. Na základě rozvoje globální sítě se zvětšuje použití její doplňujících služeb jako IP telefonie. Jedna z největších její výhod je především lacinost. Malé a velké podniky jsou schopni nastavením své privátní VoIP sítě rapidně snížit náklady použití vnitřního telefonování. Při využití této technologie, se přenáší obrovské množství dat, buď privátních nebo veřejných, které podle využití doplňujících služeb mohou být šifrované tj. zabezpečené. Přenos dat ovlivňuje šířku kanálu, proto signál musí být dostatečně komprimován, avšak komprese nesmí ovlivnit požadovanou kvalitu, proto je podstatné najít optimální řešení přenosu dat ve VoIP sítě.

Jedním z cílů diplomové práce bylo zaměření na transportní sítě používající protokol MPLS. Tento protokol je nezávislý na jiných směrovacích protokolech a dovoluje snadné vytváření virtuálních kanálů mezi uzly v síti. Díky spínání paketů podle číslovacího štítku a nezávislosti MPLS na řadě směrovacích protokolů, a tím použité technologie přenosu dat, v budoucnu, tento protokol je schopen přemístit všechny dřívější sady existujících protokolů.

V diplomové práci, bylo podrobně popsáno nastavení MPLS a OSPF na CISCO směrovači. Mezi nevýhody protokolu patří především drahé vybavení pro jeho instalaci a také dost náročná, a drahá obsluha sítě využívající MPLS. Nicméně, k výhodám patří vysoký výkon, spolehlivost, zaručena přenosová rychlost, také možnost společného využití MPLS s jinými protokoly, síťové a spojové vrstvy. Dále jsou podrobněji rozepsané výhody a nevýhody moderní telekomunikační sítě s využitím MPLS.

Teoretická část práce je věnovaná směrovacím protokolům a také protokolu SIP. Popsané rozdíly mezi statickým a dynamickým směrováním. V práci je podrobně popsán protokol SCCP, který se používá ve VoIP sítích a je součástí každého IP telefonu od společnosti CISCO. Dále je popsáno laboratorní vybavení, na kterém se tato práce provádí a rozebraná konfigurace veřejného programu Putty pro připojení na server. K popisu teorie byla použita doporučena odborná literatura a také elektronický články a webové citaci různých autorů.

V rámci diplomové práce byla nakonfigurována síť, s použitím CISCO směrovače s číslem modelů 2821. Dále byly použity 2 VoIP ústředny, připojené do sítě přes PE a CE směrovače. Pro rekonstrukce funkční smyčky byla popsána a použita telefonní ústředna společnosti SMC Networks. Ústředna SMC PBX10 – používá protokol SIP jak na straně koncových zařízení, tak i pro trunk. Konfigurace ústředny byla provedena přes webové rozhraní a směrovače, přes přímé připojení na směrovač pomocí veřejného programu Putty. Druhou použitou ústřednou byl Cisco Call Manager Express 7.1, instalovaný na jednom z Cisco směrovačů – v tomto případě byl na straně koncových zařízení použit zmíněný protokol SCCP, pro trunk byl použit signalizační protokol SIP. Do každé z ústředen byly připojeny cca 3 IP telefony. Každý z těchto telefonů má své vlastní číslo, které se dá libovolně zvolit a nastavit na směrovači a také na ústředně. Pro odchozí volání do jiné sítě bylo použito pravidlo

pro překlad telefonního čísla a následující odstranění přednastavené číslice, tím se vlastně dalo určit volající číslo zařízení.

V poslední části práce je popsáno testovací zařízení a návrh zapojení do laboratorní sítě. Pro testování síťových QoS parametrů byl použit analyzátor VePAL TX 300e. Tento analyzátor je schopen provádět testy dle standardu RFC 2544. Tento standard se používá za účelem testování Ethernet sítí a to tak, že zahrnuje spoustu drobných testů. Každý z těchto testů se provádí zvlášť, proto, se dá konfigurovat jednotlivé testy zvlášť, resp. nastavovat běžící délku a počet pokusů. Poté, dle těchto testů, byly testovány propustnost, zpoždění, ztrátovost rámců a jitter. Veškeré výsledky testů byly zadané do tabulek, aby došlo k zřehlednění. Po porovnání jednotlivých parametrů byla vybrána nejvhodnější délka rámce pro přenos hlasu a videa v reálném čase.

Závěr práce shrnuje všechny dosažené výsledky.

S časem vývoje lokálních sítí, pokračuje ve vývoji IP telefonie. V současné době, je zapotřebí umět konfigurovat integrované VoIP. Diplomová práce ukazuje možnosti nastavení podobných sítí.

Klíčová slova

VoIP, IP telefonie, CISCO, směrovací protokol, přenos dat, protokol MPLS, SIP.

Аннотация

Дипломная работа знакомит с протоколами маршрутизации, коммуникацией посредством протокола SIP, подробно описывает современную работу VoIP сетей и их настройку на оборудовании CISCO. Главный акцент делается на сети с протоколом MPLS. Описаны преимущества и недостатки современной сети построенной на данном протоколе. В рамках работы, была настроена сеть с использованием маршрутизатора от компании CISCO, на который был инсталлирован Cisco Call Manager Express 7.1. Для воссоздания полноценного телефонного узла также использовалась телефонная станция SMC PBX10 от компании SMC Networks. Конфигурация станции была проведена через веб браузер а маршрутизатора через прямое подключение с сервером с помощью программы Putty. Для межузлового соединения был создан и настроен SIP транк как на станции, так и на маршрутизаторе, к которому далее подключены и настроены три Cisco IP телефона. Каждый из телефонов имеет свой номер. Для звонков из одной сети в другую было настроено правило определения номера звонящего с помощью добавочной цифры.

Далее, описывается настройка протоколов MPLS и OSPF на одном из лабораторных маршрутизаторов. Измеряются QoS параметры рабочей сети с помощью тестера VePAL TX 300e согласно стандарту RFC 2544. Все результаты измерения присутствуют в таблицах.

Приводится описание лабораторного оборудования с которым ведётся работа.

Ключевые слова

VoIP, IP-телефония, протокол маршрутизации, протокол MPLS, SIP, CISCO.

Abstract

The master's thesis presents routing protocols, SIP handshake, describes modern VoIP networks and its features. Thesis is primary focused on networks with integrated MPLS. The most known advantages and disadvantages were described of modern network based on such technology. Further, networks and a router with installed Cisco Call Manager Express 7.1 were configured, which is provided by CISCO. For recreating of fully working telephone network IP PBX10 has been used from SMC Networks. For connection between different phones within these integrated networks, SIP trunk was configured on SMC PBX10 as well as on router, which is connecting three configured Cisco IP phones. Each phone has its own number according to the dial plan. For calls from one network to another the special pattern has been established, so the number of each caller can be easily identified by added digit.

On one of the CISCO routers was shown a configuration of MPLS and OSPF protocols. With an analyzer VePAL TX300e, the lab network has been measured to analyze QoS parameters of the network according to standard RFC 2544.

Thesis also gives references to lab devices, which have been used accordingly to the work.

Key words

VoIP, routing protocol, MPLS protocol, SIP handshake, integrated networks, CISCO.

YEFTSIFEYEU, A. *Hlasová služba v integrovaných sítích* . Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2014. 43 s. Vedoucí diplomové práce doc. Ing. Vladislav Škorpil, CSc..

Prohlášení

Prohlašuji, že svoji diplomovou práci na téma “Hlasová služba v integrovaných sítích” jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009Sb.

V Brně dne

.....
podpis autora

Poděkování

Děkuji svému vedoucímu diplomové práce doc. Ing. Vladislavu Škorpilovi, CSc. a také Ing. Michalu Polívkovi za odbornou a pedagogickou pomoc, za cenné rady při zpracování diplomové práce.

V Brně dne.....

.....
Aliaksandr Yeftsifeyeu

Оглавление

Список используемых иллюстраций	12
Список используемых таблиц	13
1. Представление современной, телефонной технологии	14
2. Многопротокольная коммутация по меткам	15
2.1. Преимущества коммутации по меткам	15
2.2. Описание протокола SIP	16
3. Протоколы маршрутизации	17
3.1. Статическая маршрутизация	17
3.2. Динамическая маршрутизация	17
3.2.1. Протокол RIP	17
3.2.2. Протокол OSPF	18
3.2.3. Протокол EIGRP	19
3.2.4. Протокол SCCP	19
4. Описание лаборатории	20
5. Реализация и решение курсового проекта	22
5.1. Инсталляция и конфигурация программы Putty	22
5.2. Настройка и работа с интерфейсом SMC IP PBX10 Networks	23
5.2.1. Описание телефонного интерфейса SMC IP PBX10	23
5.2.2. Конфигурация SMC IP PBX10	24
5.3. Работа с маршрутизатором CE-VOIP	28
5.3.1. Настройка телефонного сервиса	29
5.3.2. Настройка SIP транка на маршрутизаторе	31
5.3.3. Настройка MPLS	32
5.3.4. Тестирование по стандарту RFC 2544	33
5.3.5. Измеряемые параметры теста RFC 2544	33
5.3.6. Анализатор VePAL TX300e	34
5.3.7. Схема подключения тестера	34
5.3.8. Конфигурация тестера	35
5.3.9. Тест V-SAM	37
5.3.10. Результаты тестирования	38

6. Заключение	39
Список используемых сокращений	39
Список используемой литературы и цитат.....	42

СПИСОК ИСПОЛЬЗУЕМЫХ ИЛЛЮСТРАЦИЙ

Рис. 1: Соединение телефонного клиента SIP с ПК через прокси сервер.....	16
Рис. 2: Виртуальная топология лабораторной сети для наблюдения	20
Рис. 3: Логическая топология сети с подключённой IP PBX.....	21
Рис. 4: Интерфейс программы Putty с введёнными данными	22
Рис. 5: Устройство SMC IP PBX10, передняя панель	23
Рис. 6: SMC IP PBX10 задняя панель, расположение портов	23
Рис. 7: Меню локальных сетевых настроек	24
Рис. 8: Настройка WAN адреса	25
Рис. 9: Создание группы и ассоциирование с уже созданным SIP транком	25
Рис. 10: Настройка аккаунта пользователя	26
Рис. 11: Настройка плана набора номеров	26
Рис. 12: Процесс настройки телефонного аккаунта.....	27
Рис. 13: Настройка аналоговых телефонов в SMC IP PBX.....	27
Рис. 14: Создание SIP транка.....	28
Рис. 15: Настройка маршрутизации исходящих звонков	28
Рис. 16: Серверная консоль для подключения к маршрутизаторам сети	30
Рис. 17: Задняя панель анализатора VePAL TX300e.....	34
Рис. 18: Схема подключения тестера VePAL TX300e к лабораторной сети	35
Рис. 19: Настройки тестера после подключения к серверу DHCP	35
Рис. 20: Обработка трафика в процессе работы loopback	36

СПИСОК ИСПОЛЬЗУЕМЫХ ТАБЛИЦ

Табл. 1: Структура RIP Entry для протокола второй версии	18
Табл. 2: Используемые лабораторные устройства	20
Табл. 3: Основные параметры станции и поддерживаемые стандарты.....	24
Табл. 4: Измерение пропускной способности лабораторной сети тестом RFC 2544 ..	36
Табл. 5: Измерение сетевой задержки	37
Табл. 6: Измерение процентуального отношения потерянных пакетов	37
Табл. 7: Измерение джиттера лабораторной сети	37

1. ПРЕДСТАВЛЕНИЕ СОВРЕМЕННОЙ, ТЕЛЕФОННОЙ ТЕХНОЛОГИИ

С развитием глобальной сети интернет, появилось множество различных технологий позволяющих расширить спектр услуг и доступность получаемой информации из сети, тем самым позволив совместить сразу несколько разных по своей сути источников информации. На сегодняшний день мы способны общаться, играть с друзьями, просматривать развлекательные телевизионные программы не отходя от одного узла связи. Цифровая передача данных, позволила нам разделить одну линию создав множество каналов для взаимодействия информации. Кодирование, позволило существенно сократить используемые ресурсы сети и тем самым снизить нагрузку, что в свою очередь повлияло на снижение стоимости и повышению доступности услуг. Одной из таких услуг является IP-телефония или VoIP.

Идея передачи голосовой связи уже далеко не нова. VoIP, позволяет расширить и внедрить в услугу передачи голоса дополнительные возможности как видеотрансляции, проведение вебинаров¹, просмотр фильмов в режиме онлайн и многое другое. При этом, также расширяется возможности напрямую работать с телефонной линией, так как допускается передача более одного телефонного звонка в одном высокоскоростном телефонном подключении, что существенно бы увеличило затраты в телефонной сети общего доступа. Появляется услуга переадресации, создание конференций, автоматическое повторение номера а также определение номера звонящего абонента. Для поддержки работоспособности такого широкого рода услуг было создано множество различных программ и приложений, которые в свою очередь используют протоколы, позволяющие регистрировать сетевое телефонное оборудование, соединять абонентов и помогать решать сервисные задачи в процессе диалога. Одним из самых распространённых на сегодняшний день таких протоколов является SIP, который активно поддерживается компанией Cisco. Данный протокол не ограничен только предоставлением голосовых услуг но как и многие другие и уже включает в себя большой список возможностей, при этом может быть расширен в будущем.

Большую роль в процессе передачи информации также играет качество, безопасность. Поддержку шифрования помогают реализовать дополнительные программы а также транспортные протоколы, решая тем самым проблему несанкционированного доступа и прослушивания.

На сегодня, сложно себе представить обмен информации без живого общения. IP-телефония является ключом к эффективному использованию всех ресурсов, предоставляемых нам современной технологией, такой как Интернет.

¹ От английского webinar (веб-конференция)

2. МНОГОПРОТОКОЛЬНАЯ КОММУТАЦИЯ ПО МЕТКАМ

MPLS или многопротокольная коммутация по меткам является новой технологией, которая в будущем может быть внедрена в большое количество IP сетей и даже Internet. При этом, необходимо учесть все плюсы и минусы данного перехода чтобы с точностью оценить преимущества последующего внедрения.

Коммутация MPLS является усовершенствованным методом передачи трафика с использованием информации хранящийся в метках. В зависимости от типа коммутации, метки могут содержаться в:

1. IP-пакете
2. Внедряться между заголовками 2-го и 3-го уровней в случае если идёт передача фреймов²
3. В случае передачи ячеек содержаться в полях VPI и VCI

Это подтверждает многопротокольность данной технологии.

Использование MPLS обуславливается созданием гибкой сетевой структуры в которой первоначальную роль играет стабильность работы сети и обеспечение повышенной производительности.[42]

Процесс добавления метки является достаточно простым. При прохождении пограничного LSR маршрутизатора назначается метка и далее пакеты проходят по LSP маршруту с коммутацией уже по метке. Каждый последующий LSR маршрутизатор перенаправляет пакет основываясь на содержимом метки при этом значение метки меняется при каждом переходе, то есть происходит удаление и вставка новой метки, которая определяет направление последующего перехода по сети. На последнем граничном устройстве метка удаляется и происходит отправка к точке назначения пакета.

2.1. ПРЕИМУЩЕСТВА КОММУТАЦИИ ПО МЕТКАМ

Использование меток снижает общую нагрузку сети, так как решение об отправке пакетов принимается на основе содержимого меток, тем самым позволив упростить задачу маршрутизаторов, которые производят вычисление маршрута и в последующем определяют адресата по хранящемуся значению в таблице маршрутизации IP адреса. Преимущества данного метода:

1. Повышение качества обслуживания с надёжной гарантией QoS.
2. Интеграция IP и ATM путём передачи части функций ATM третьему уровню
3. Распределение потоков.

² От английского frame (рамка)

В частности при недостаточной загрузке маршрутов происходит перераспределение трафика, для оптимизированного использования полосы пропускания.

4. Создание дополнительных сетей VPN.

Использование технологии MPLS, позволяет провайдерам создавать на магистральных сетях 3-го уровня VPN сети для увеличения количества пользователей.

2.2.ОПИСАНИЕ ПРОТОКОЛА SIP

SIP является простым коммуникационным протоколом, построенным на запросах и ответах для установки соединения между различными компонентами или частями сети, либо создания конференции с двумя либо несколькими конечными узлами сети. Каждый пользователь сети имеет свой регистрационный SIP номер вида *userID@gateway.com*. Соединение в протоколе SIP начинается с отправки сообщения INVITE переводящему серверу, либо прокси если таковой имеется. Запрос включается также в себя адрес вызываемого и запрашиваемого устройства. В последующем сервер определяет местонахождение и путь вызываемого, после этого отправляет ответ назад. Протокол SIP работает как с IPv4 так и с IPv6.[9]

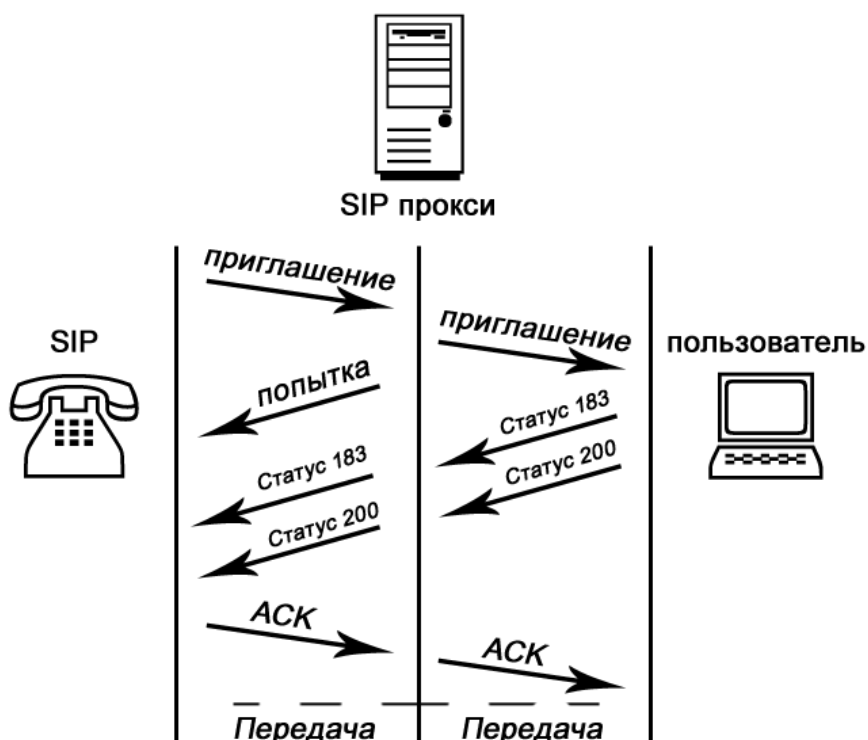


Рис. 1: Соединение телефонного клиента SIP с ПК³ через прокси сервер

³ ПК – Персональный Компьютер

3. ПРОТОКОЛЫ МАРШРУТИЗАЦИИ

Для успешной работы маршрутизатора в большой сети необходим чёткий алгоритм, позволяющий в кратчайшее время найти оптимальный маршрут и произвести доставку пакетов в пункт назначения. Все существующие протоколы объединяет поиск оптимального маршрута, однако алгоритм поиска у каждого может существенно отличаться.

В процессе работы маршрутизатора необходимо точно определить все устройства в сети, т.е. иметь информацию для поиска оптимального маршрута. Компьютерная сеть это динамическая среда, которая постоянно изменяется, поэтому важно что бы каждый маршрутизатор имел актуальную таблицу маршрутизации, которая составляется на основе информации полученной с помощью протокола маршрутизации либо в ручную. Изменения в сети также могут иметь разные последствия, будь то подключение дополнительного маршрутизатора или пользователя до полного выхода из строя целого участка сети. Ниже рассмотрены основные на сегодняшний день используемые протоколы и типы маршрутизации.

3.1. СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Загрузка сети играет большую роль в процессе передачи трафика. Если сеть является сравнительно небольшой, имеет смысл в ручную настраивать маршруты на каждом отдельно взятом маршрутизаторе. Это разгружает сеть что в свою очередь влияет на конечную задержку пакетов. В этом случае необходим администратор сети, который производит все сетевые настройки. Также повышается стоимость администрирования такой сети. Человеческий фактор не может быть исключен. В случае не правильной конфигурации, можно вызвать проблемы на целом участке сети что приведёт к задержке и даже неработоспособности целого сетевого сегмента.

3.2. ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ

В сети с большим количеством пользователей как правило применяется динамическая маршрутизация. В такой сети маршрутизаторы автоматически изучают маршрут от своих ближайших соседей и составляют таблицу маршрутизации. С повышением трафика эффективность данной сети падает, тем не менее административные затраты являются низкими, что позволяет дополнительно сосредоточиться на качестве обслуживания сети.[2]

3.2.1. ПРОТОКОЛ RIP

RIP является одним из первых и самых простых протоколов маршрутизации. Используется алгоритм Беллмана-Форда и являясь протоколом дистанционно-векторной маршрутизации, то есть находит маршрут основываясь на конечном

числе переходов (метрике) максимум которых 15, тем самым может использоваться в небольших по размерам сетях, его преимуществом является простота конфигурирования. Уступает более современным протоколам.

Обновления в сети по умолчанию происходят каждые 30 секунд, когда RIP раздает в сеть свою таблицу маршрутизации происходит дополнительная загрузка низкоскоростных сетей. Обмен информацией происходит с помощью протокола UDP и порта 520.

Протокол имеет две версии. Первая была унифицирована и описана в документе RFC 1058, вторая в RFC 2453 соответственно.[11][12]

Формат протокола RIPv2 идентичен формату RIP за исключением дополнительно введенных параметров для второй версии.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	...
Адресный индикатор										Тег маршрута											
Адрес IPv4																					
Маска подсети																					
Следующий хоп																					
Метрика																					

Табл. 1: Структура RIP Entry для протокола второй версии

Отличие версий заключается в нескольких параметрах, прежде всего это поддержка маски подсети, которая позволяет решить проблему классовой адресации и упростить маршрутизацию в сети и тем самым использовать данный протокол в разных подсетях. Также была добавлена безопасность протокола. Тем не менее, ограничение по метрике делает данный протокол нежелательным для использования в больших сетях.[3][4]

3.2.2. Протокол OSPF

Протокол основан на отслеживании состояния канала и использует для нахождения кратчайшего пути алгоритм Дейкстры⁴. Имеет преимущества в высокой скорости сходимости перед остальными дистанционно-векторными протоколами маршрутизации. Поддержка сетевых масок переменной длины а также использование оптимальной пропускной способности линии при нахождении кратчайшего пути по средствам применения алгоритмов Дейкстры.

В протоколе маршрут выбирается по так называемой стоимости канала. Метрика показывают данную стоимость и вычисляется на основе пропускной способности интерфейса, чем больше пропускная способность тем ниже стоимость маршрута тем ниже метрика.

цена= 100 000 000/пропускная способность в bps
--

Не смотря на простоту практической реализации алгоритма и высокой скорости сходимости протокол не избавляет от проблем связанных

⁴ Алгоритм Дейкстры - Dijkstra's algorithm

с перегрузкой сети, избыточную пропускную способность предлагается распределять что бы бороться с излишней перегруженностью.[3][5][6]

3.2.3. Протокол EIGRP

EIGRP разработан на базе протокола IGRP. Вычисление оптимального маршрута основывается на минимальной пропускной способности интерфейса, однако также учитываются другие параметры как:

1. Общая задержка
2. Надёжность маршрута
3. Загрузка маршрута
4. Предполагаемое расстояние
5. Заданное расстояние

Выбор оптимального маршрута рассчитывается по формуле:

$\text{метрика} = [K1 * \text{пропускная способность} + (K2 * \text{пропускная способность}) / (256 - \text{загрузка}) + K3 * \text{задержка}] * [K5 / (\text{надёжность} + K4)]$

Комплексная формула вычисления метрики приводит к дополнительным системным требованиям маршрутизатора. Повышается нагрузка процессора и оперативной памяти, тем самым увеличивая время просчёта оптимального маршрута в объёмной сети. Тем не менее, протокол успешно справляется с нахождением кратчайшего пути во всех типах сетей. Единственным существенным недостатком протокола является его совместимость только с маршрутизаторами компании Cisco.[7][8]

3.2.4. Протокол SCCP

Данный протокол используется компанией Cisco для VoIP сетей. Является сигнальным протоколом, используя при этом для передачи данных TCP/IP, допускается передача медиа данных транспортным протоколом UDP. Протокол SCCP был создан на базе клиента Skinny как расширяющий возможности сигнальных функций этого протокола. Появилась поддержка создания конференции, перевода и перехвата текущего звонка, а также создания голосовой почты. [10]

4. ОПИСАНИЕ ЛАБОРАТОРИИ

Реализация проекта осуществлялась в учебной лаборатории SC 5.35. Лаборатория оснащена новейшим оборудованием Cisco, в том числе 7 маршрутизаторов и 1 свич. Далее в рамках проекта использовались следующие устройства:

Название устройства	Модель
P1,P2,PE1,PE2,CE-VOIP,CE-E1	Cisco 2821
3x Cisco IP телефон	Cisco 7975 G
2x IP телефон	SMC DSP205
2x аналоговый телефон	Sagem C95
IP PBX интерфейс	SMC IP PBX10

Табл. 2: Используемые лабораторные устройства

Интерфейс SMC PBX10 может быть наконфигурирован через веб браузер после подключения к сетевой карте компьютера либо через подключение к консоли интерфейса.

В лаборатории используется 3 сети, из которых 2 являются внутренними и 1 внешней. Одна из внутренних сетей обслуживает сервер контроля на котором изображена данная топология:

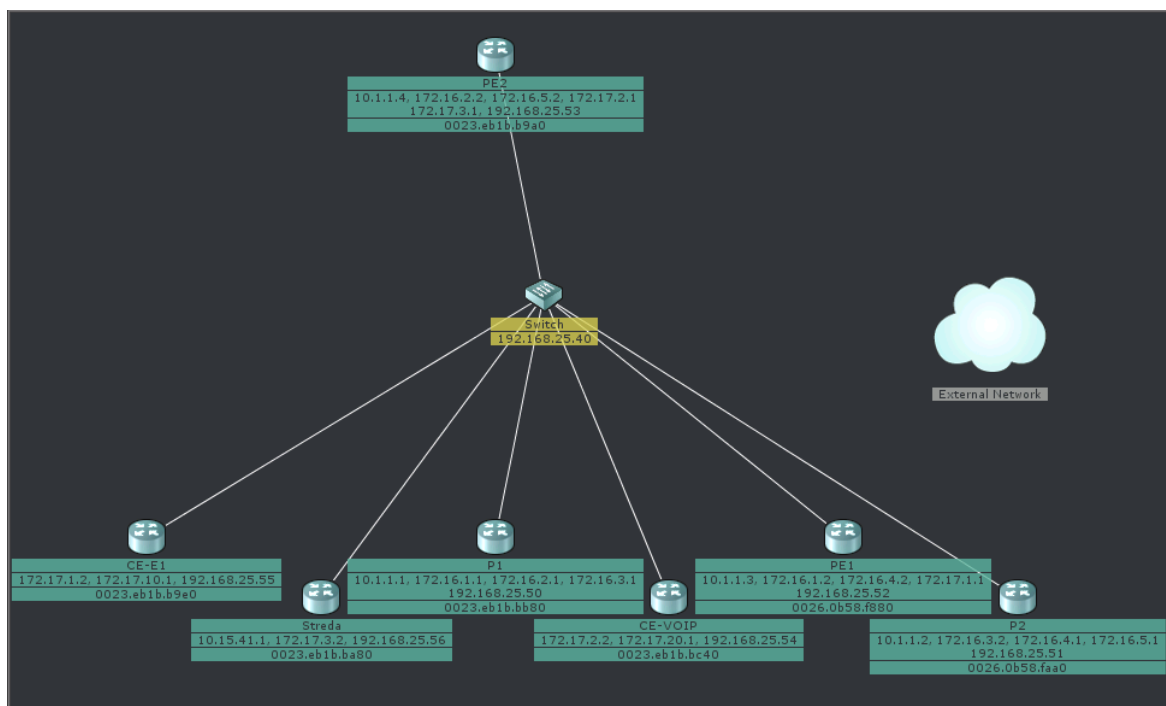


Рис. 2: Виртуальная топология лабораторной сети для наблюдения

Логическая топология всей сети показана на следующем рисунке:

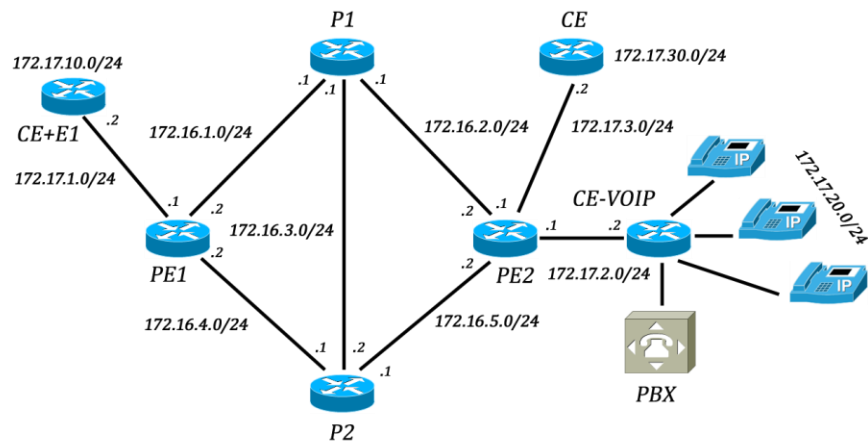


Рис. 3: Логическая топология сети с подключённой IP PBX

Телефонная станция подключена прямо к маршрутизатору CE-VoIP. В лаборатории его обслуживают следующие LAN разъёмы: L.14a-d.

5. РЕАЛИЗАЦИЯ И РЕШЕНИЕ КУРСОВОГО ПРОЕКТА

5.1. ИНСТАЛЛЯЦИЯ И КОНФИГУРАЦИЯ ПРОГРАММЫ PUTTY

В рамках реализации проекта для подключения к удалённому серверу использовалась программа Putty, которая является бесплатной для платформ Windows и Unix. Программа поддерживает работу с протоколами Telnet а также SSH, обеспечивая тем самым необходимое шифрование данных при подключении к консоли маршрутизатора. Данная консоль доступна на адресе `ccs.utko.feec.vutbr.cz` с номером порта 22. Имеется возможность прямого подключения к консоли через асинхронный интерфейс UART.

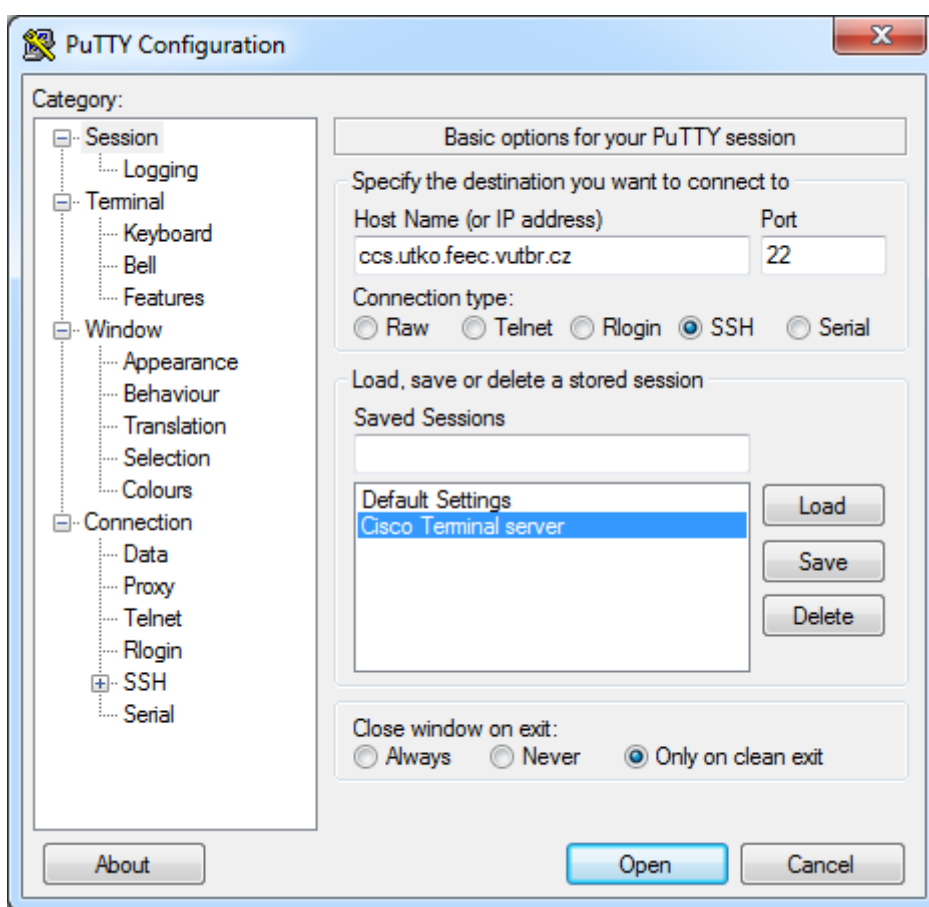


Рис. 4: Интерфейс программы Putty с введенными данными

После успешного подключения к серверу необходимо пройти процесс аутентификации пользователя. Логинем является user и пароль user535.

В Putty, также имеется встроенная возможность сохранять файлы конфигурации по настройке роутера и которые, в последующем, возможно использовать для продолжения конфигурации маршрутизатора.

5.2. НАСТРОЙКА И РАБОТА С ИНТЕРФЕЙСОМ SMC IP PBX10 NETWORKS



Рис. 5: Устройство SMC IP PBX10, передняя панель

5.2.1. ОПИСАНИЕ ТЕЛЕФОННОГО ИНТЕРФЕЙСА SMC IP PBX10

Данный интерфейс используется для интеграции и обслуживания телефонных сетей основанных на технологиях SIP и VoIP, тем самым объединяя их в одно, при этом являясь легко конфигурируемым устройством. Поддерживает до 30 регистрируемых пользователей с широкими возможностями создания и настройки плана набора номера, создания в количестве до пяти SIP транков. Существует встроенная возможность прямого подключения к ITSP для снижения стоимости звонков.

Также имеется ряд дополнительных функций таких как: встроенная голосовая почта, создание и управление конференциями, автоматическое определение подключаемых телефонов, что позволяет не настраивать каждый подключённый аппарат отдельно, система способна самостоятельно определить подключаемое устройство и на основе уже зарегистрированного аккаунта предоставляет данные к регистрации телефона. Данная опция работает только с SIP телефонами.

Телефонная станция имеет встроенную систему безопасности NAT Firewall.[16]



Рис. 6: SMC IP PBX10 задняя панель, расположение портов

Основные функции	Управление	Дополнительные возможности	Поддерживаемые стандарты
До 30 регистрируемых аккаунтов, SIP прокси, настройка 5 SIP транков, поддержка кодеков G.711u-	Веб ориентированное управление интерфейсом (HTTP/HTTPS), TFTP Сервер, CDR, Системные	Перевод звонков, режим ожидания на музыку, Голосовая почта, Создание конференций, Перенаправление	RFC 3261, RFC 3311, RFC 3515, RFC 3265, RFC 3892, RFC 3361, RFC 3842, RFC 3389, RFC 3489, RFC 3428, RFC 2327, RFC 2833, RFC 2976, RFC 3263, RFC 3264

/a-law, G.726,
G.729, G.723.1,
DHCP сервер, STUN
клиент, QoS

логи, Удалённое
обновление
программного
обеспечения

звонков (IVR),
Автоматическая
конфигурация
аккаунтов

Табл. 3: Основные параметры станции и поддерживаемые стандарты

5.2.2. Конфигурация SMC IP PBX10

Для начала конфигурации интерфейса необходимо вернуть заводские настройки. Для этого надо перезагрузить устройство (IP Service->Restore Default) и в последующим подключить к одному из находящихся в лаборатории компьютеров (нижняя сетевая карта). С помощью команды ipconfig в командном меню Windows 7 можно увидеть настройки сетевой карты. В верхней сетевой карте должны остаться предыдущие данные для выхода в интернет вида (147.229.*.*). После перезагрузки и возвращения интерфейса SMC в заводское состояние его локальный IP адрес должен быть 192.168.2.1 с маской 255.255.255.0. Интерфейс доступен через веб браузер, необходимые поля для заполнения в пользовательскую часть логин и пароль соответственно admin/smcadmin. Конфигурирование SMC IP PBX10 возможно провести через кабель RS232 а также через Telnet, при этом для подключения через асинхронный интерфейс требуется установить скорость передачи на 115200. Для того, чтобы аутентифицироваться в системе необходимо ввести логин и пароль **estcli** два раза соответственно. После этого можно входить в привилегированный режим управления командой enable. Система запрашивает пароль, что является прежним паролем доступа для управления из интерфейса - smcadmin.

После входа в систему через веб интерфейс, можно переходить к конфигурации сетевых параметров.

LAN Setup	
Interface MAC	00:13:F7:62:80:41
IP Address	192.168.2.1
Netmask	255.255.255.0
APPLY	

Рис. 7: Меню локальных сетевых настроек

В меню LAN можно настроить адрес локальной сети и маску подсети, с которого будет доступна конфигурация данной станции.

Следующим этапом является настройка WAN адреса, для доступности телефонной станции в глобальной сети для исходящих и входящих звонков. Тип IP адреса нужно переключить в статический и в адресном поле задать

172.17.20.2 с маской 255.255.255.0. При этом как шлюз указать маршрутизатор 172.17.20.1 к которому и будет подсоединено устройство.

:: Setup Management

WAN Setup

Type: Static IP ▼

☐ LAN Only

Interface MAC: 00:13:F7:62:80:40

☐ MAC Clone

IP Address: 172.17.20.2

Netmask: 255.255.255.0

Gateway: 172.17.20.1

DNS 1:

DNS 2:

DNS 3:

APPLY

Рис. 8: Настройка WAN адреса

В закладке User Group Management настраивается новая группа пользователей. В данном случае Group ID 1.

:: User Group Management

ADD

DEL

	Group ID	Description	Associated SIP Trunks	Associated PSTN Trunk
☐	1		SIPTrunk	
☐	UG_DEF			

1

Рис. 9: Создание группы и ассоциирование с уже созданным SIP транком

Все зарегистрированные пользователи в меню User Management. Два IP телефона и два аналоговых подключённых напрямую к PBX.

:: User Management

User Add New

Search :

DEL

	Login ID	Name	Description	Usergroup	E-mail Address	Extensions
☐	501	501	501	1		501
☐	502	502	502	1		502
☐	503	503	503	1		503
☐	504	504	504	1		504
☐	admin	admin		UG_DEF		

1

Рис. 10: Настройка аккаунта пользователя

Далее следует регистрация IP телефонов. Здесь же настраивается план набора или диал план. Все ранее созданные пользователи привязываются к телефонному номеру.

:: IP Phone Management

Device ID Device Administration URL

DEL

	Device ID	Associated Extension	Device Administration URL
☐	501	501	LINK
☐	502	502	LINK

1

Рис. 11: Настройка плана набора номеров

Настроить телефоны можно в меню Extension of IP Phone Management. Указанные параметры необходимо также будет настроить на самом телефоне, чтобы устройство смогло пройти регистрацию по предварительно созданному аккаунту.

:: Extension of IP Phone Management

Extensions

Update

Extension Number	501
Associated Device	501 ▾
Password	...
User	501(501) ▾
Pickup Group	1 ▾ ☒ Include Reachables
Voicemail	Disable ▾
Voicemail PIN	
Max Voicemail Space	KBytes
Unavailable Timeout	20 ▾ sec.
☐ Allow LAN Use Only	
☐ Disable NAT Traversal	
☐ Call Keep Alive	
☐ Registered Keep Alive	
☐ Disable Fast Bridging	
Try Peer-to-peer RTP	NO ▾
DTMF Mode	RFC2833 ▾
☐ Advanced Settings	

Рис. 12: Процесс настройки телефонного аккаунта

Аналогично настраиваются аналоговые телефоны с одним лишь исключением, а именно номера напрямую задаются к соответствующему порту (POTS Port) в устройстве PBX.

:: Analog Phone Management

Extensions

Add New

DEL

	POTS Port	Extension Number	Pickup Group	Unavailable Timeout
☐	3	503	1	20
☐	4	504	1	20

1

Рис. 13: Настройка аналоговых телефонов в SMC IP PBX

Настройка SIP транка. Здесь за прокси сервер выступает маршрутизатор 172.17.20.1 и порт 5060.

The screenshot shows the 'SIP Trunk Management' interface. At the top, there are tabs for 'Trunks' and 'Add New'. Below these is a search bar with a 'GO' button. A 'DEL' button is also present. The main part of the interface is a table with the following columns: Trunk Identifier, Description, Dynamic Peer, SIP Proxy IP, and SIP Proxy Port. There is one entry in the table with the identifier 'SIPtrunk', a description of 'no', and a SIP Proxy IP of '172.17.20.1' and port '5060'. A blue number '1' is displayed at the bottom right of the table area.

	Trunk Identifier	Description	Dynamic Peer	SIP Proxy IP	SIP Proxy Port
☐	SIPtrunk		no	172.17.20.1	5060

Рис. 14: Создание SIP транка

Исходящие звонки в рамках глобальной сети настраиваются в меню управления маршрутизации. В случае заданного номера вида 8XXX и Number Stripped 1 имеется ввиду, что при наборе трёхзначного номера после 8, которая будет изыматься, SIP пошлёт первое сообщение INVITE с набранным номером. Если такой номер зарегистрирован, то произойдёт звонок телефона на другой линии. При этом, предварительно создаётся GroupID (в нашем случае route1). После этого созданное SIProute необходимо добавить в ассоциированные маршруты.

The screenshot shows the 'Route Management' interface. It has a form with fields for 'Route ID', 'Description', 'Destination Number Pattern', and 'Prefix'. Below the form is a 'DEL' button. The main part of the interface is a table with the following columns: Route ID, Description, Destination Number Pattern, and Num. There is one entry in the table with the identifier 'SIProute', a description of '8XXX', and a value of '1' in the 'Num' column. A blue number '1' is displayed at the bottom right of the table area.

	Route ID	Description	Destination Number Pattern	Num
☐	SIProute		8XXX	1

Рис. 15: Настройка маршрутизации исходящих звонков

5.3. РАБОТА С МАРШРУТИЗАТОРОМ CE-VOIP

Необходимо выбрать для работы маршрутизатор. В целях проверки работоспособности коммуникации сначала был выбран маршрутизатор CE-VOIP. Для подключения сервер запрашивает авторизацию, логином

и паролем является соответственно admin/admin. Маршрутизатор CE-VOIP обслуживается протоколом EIGRP. На данном маршрутизаторе создано 2 сети, одна из которых является виртуальной, её IP адрес 172.17.20.0. Далее виртуальная сеть для наблюдения 192.168.25.0. Данному маршрутизатору был присвоен адрес 192.168.25.54.

Для начала необходимо настроить CISCO телефоны, которых всего 3. После подключения к маршрутизатору протокол DHCP автоматически присвоит каждому из телефонов IP адрес так как шлюз по умолчанию уже поднастроен. Настройка TFTP сервера не проводилась так как конфигурация уже проведена.

5.3.1. НАСТРОЙКА ТЕЛЕФОННОГО СЕРВИСА

Данные команды предназначены для настройки телефонного сервиса на маршрутизаторе (вводятся в конфигурационном режиме **conf t**):

telephony-service

задать настройки, которые будут применимы ко всем телефонам

max-ephones 5

максимальное количество IP телефонов

max-dn 10

максимальное количество внутренней адресации

ip source-address

IP адрес для обработки регистрации телефонов

exit

Следующие команды задаются в консольной панели маршрутизатора для настройки IP телефонов:

ephone-dn 1(2-3) dual-line⁵

проводит конфигурацию первой и последующих линий

number 601(2-3)

привязка телефонного номера к аппарату

exit

⁵ Dual-line позволяет обслуживать одновременно два вызова, появляются доп. возможности как ожидание вызова, перевод звонка и подобное.

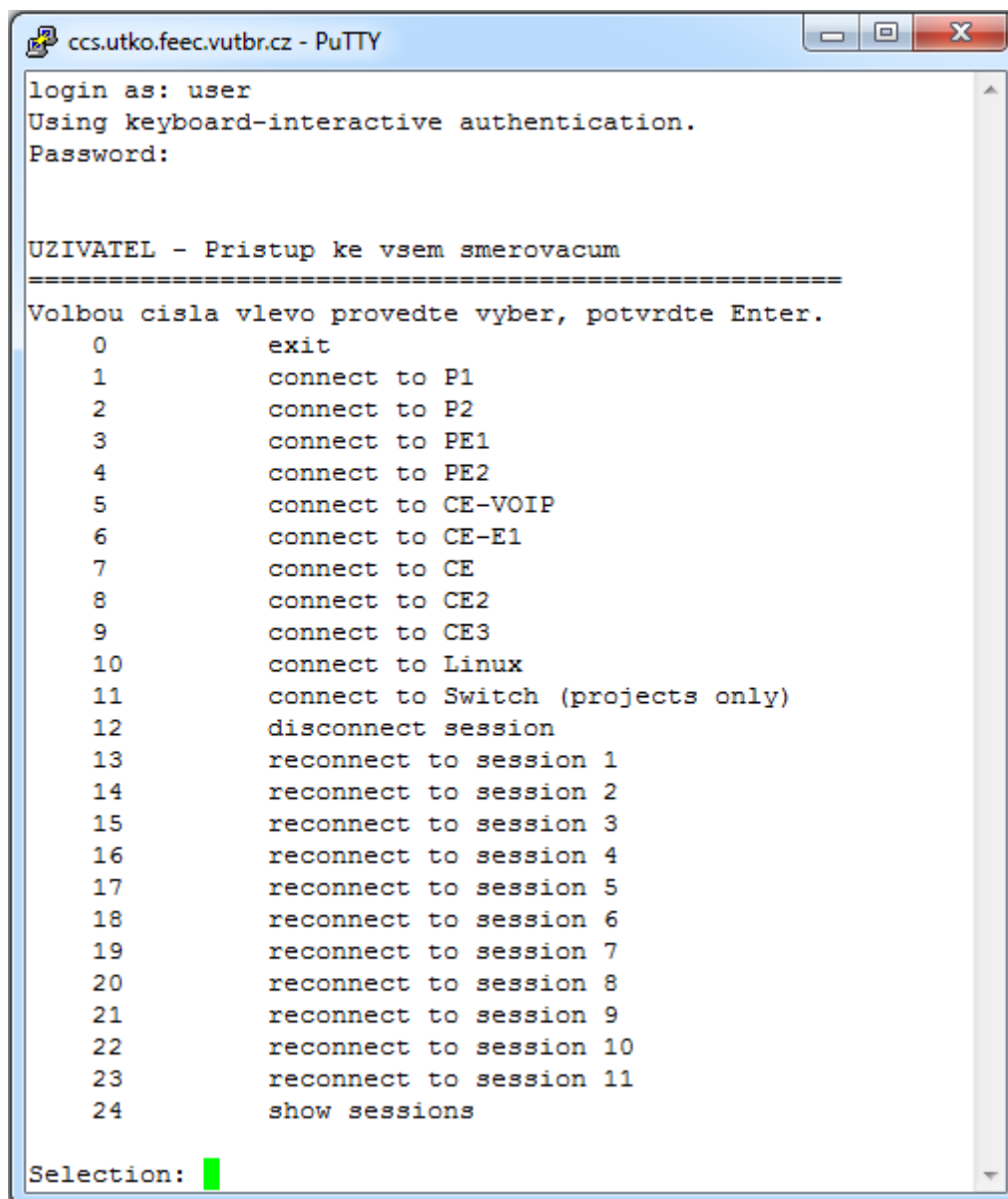


Рис. 16: Серверная консоль для подключения к маршрутизаторам сети

Также необходимо привязать физический IP телефон к его виртуальному прототипу:

ephone 1(2-3)

привязка первого телефона

mac-address 0024.9734.0FC4

(mac-address 0024.9734.0EEB)

(mac-address 0024.9734.844F)

уникальный мак адрес один для каждого из аппаратов

button 1:1

назначение ephone-dn 1 на кнопку 1 виртуального ephone 1

restart

перезагрузка телефона

5.3.2. НАСТРОЙКА SIP ТРАНКА НА МАРШРУТИЗАТОРЕ

Для настройки SIP также команды вводятся в режиме конфигурации **conf t**.

```
voice service voip  
вход в конфигурацию службы voip  
allow-connections sip to sip  
разрешить подключение через SIP  
exit
```

Создание правила перевода номера входящих-исходящих звонков:

```
voice translation-rule 1  
установка первого правила для перевода телефонного номера  
rule 1 /^5\(.*\)/ /\0/6  
создание правила  
exit  
voice translation-profile profile1  
установка профиля перевода номера  
translate calling 1  
для исходящего звонка  
translate called 1  
для входящего звонка  
exit
```

Далее настройка входящих звонков с телефонной станцией SMC PBX10:

```
dial-peer voice 1 voip  
конфигурация телефонных номеров с пометкой 1  
translation-profile outgoing profile1  
активация созданного перевода телефонных номеров  
destination-pattern 9...  
настройка формата телефонных номеров  
session protocol sipv2  
настройка протокола связи  
session target ipv4:172.17.1.2  
целевой SIP прокси сервер  
dtmf-relay rtp-nte  
определение DTMF тонов
```

После проведения данных настроек телефоны могут звонить навзаем в рамках использованного маршрутизатора.

Для дебага и обзора уже готовой конфигурации можно использовать следующие команды:

```
debug ccsip error/events/messages/calls  
определение конфигурации и решение возникающих ошибок
```

⁶ Для тестирования созданного правила используется команда **test voice translation-rule**

5.3.3. НАСТРОЙКА MPLS

В рамках дипломной работы была произведена конфигурация протокола MPLS поверх OSPF и протестирована на маршрутизаторах в лаборатории CISCO. Также данная конфигурация может быть протестирована в программе Packet Tracer.

Настройка маршрутизатора P1 (по аналогии настраиваются P2, PE1, PE2, за исключением сетевого адреса.):

```
P1(config)#int loopback 0  
настройка логического интерфейса  
P1(config-if)#ip address 10.1.1.1 255.255.255.255  
P1(config-if)#exit  
P1(config)#int fa 0/1  
P1(config-if)#ip address 172.16.1.1 255.255.255.0  
P1(config-if)#no sh  
P1(config-if)#exit  
P1(config)#int fa 0/0  
P1(config-if)#ip address 172.16.2.1 255.255.255.0  
P1(config-if)#no sh  
P1(config)#router ospf 1  
P1(config-router)#network 10.1.1.0 0.0.0.255 area 0  
P1(config-router)#network 172.16.0.0 0.0.255.255 area 0  
P1(config-router)#exit  
P1(config-if)#exit  
P1(config)#exit  
P1#wr  
сохранение конфигурации
```

Далее следует сама настройка протокола MPLS:

```
P1(config)#ip cef  
включение Cisco Express Forwarding, является технологией ускоренной коммутации пакетов на сетевом уровне OSI  
P1(config)#mpls ip  
включение процесса коммутации по меткам  
P1(config)#mpls label protocol ldp  
выбор протокола по которым происходит обмен метками LSR (ELSR) друг с другом  
P1(config)#mpls ldp router-id loopback 0  
определение интерфейса для ID маршрутизатора в процессе MPLS  
P1(config)#int fa 0/1  
Router_1(config-if)#mpls ip  
включение протокола MPLS на данном интерфейсе  
Router_1(config-if)#mpls mtu 1512
```

для избежания фрагментации кадров

P1(config)#exit

P1#wr

Настройка MPLS на одном из маршрутизаторов завершена. Маршруты будут отныне помечены метками. Проверить данную конфигурацию можно с помощью команды **show mpls forwarding-table**.

5.3.4. ТЕСТИРОВАНИЕ ПО СТАНДАРТУ RFC 2544

Документ RFC 2544 включает в себя серию тестов для измерения и определения производительности сетевых устройств. Результатом данного теста являются данные характеристик оборудования, для их последующего сравнения с предоставленными данными от производителя, после чего можно провести подробный анализ работоспособности сетевого устройства. Данный стандарт также используется производителем для описания сетевых характеристик выпускаемой продукции.

Стандарт заключается в серии тестов, при этом, не все из них могут быть применены к любому из сетевых устройств, в зависимости от типа тестируемого оборудования.

Оценка данного теста является объективной только в том случае, если проводится необходимое количество тестов для определения среднего показателя в рамках тестируемой цепи, то есть для наиболее качественного результата надо провести разное количество измерений в зависимости от загруженности измеряемой сети.[13]

5.3.5. ИЗМЕРЯЕМЫЕ ПАРАМЕТРЫ ТЕСТА RFC 2544

Всего тест основывается на шести различных измерениях:

➤ Пропускная способность

Измеряется в битах за секунду (bps). Показывает величину, с которой было успешно доставлено количество информации через коммуникационный канал за единицу времени, то есть количество успешно отправленных и принятых пакетов за отведённое время, при этом не должно возникнуть ошибки либо потери пакета.

Тестирование этого параметра начинается на максимально доступной пропускной способности сети и в случае возникновения ошибки, либо утраты пакета, пропускная способность снижается на половину, и тест будет повторён. Если же при повторном цикле не возникла ошибка, то тест автоматически увеличивает пропускную способность на половину от предыдущего измерения.

Результатом измерения является таблица в которой приведены максимальная пропускная способность в секунду (Mbps). Так же график, показывающий зависимость пропускной способности от величины пакета.[14][15]

➤ Потеря кадров

Характеризует процент всех отправленных кадров сетевым устройством в процессе тестирования, но которые так и не были доставлены по назначению из-за недостатка сетевых ресурсов. В зависимости от перегрузки сети, этот параметр определяет производительность конкретной сети и значение её перегруженности. Показывает потенциальную производительность конкретного сетевого устройства в условиях перегрузки сети.[15]

➤ Задержка

Показывает величину времени, за которое тестируемый кадр пройдёт по сети и вернётся обратно в порт из которого был отправлен. Для измерения задержки в сети на ОС⁷ Windows, как правило используются несколько приложений, такие как ping и tracert.

5.3.6. АНАЛИЗАТОР VePAL TX300e

Для измерения сетевых параметров использовался анализатор VePAL TX300e. Данный анализатор обладает всем набором инструментов для измерения телекоммуникационной сети с первого по четвёртый уровень базовой модели OSI. Он способен анализировать следующие типы сетей: Ethernet, Fiber Channel, PDH, SDH.[17]



Рис. 17: Задняя панель анализатора VePAL TX300e

5.3.7. СХЕМА ПОДКЛЮЧЕНИЯ ТЕСТЕРА

Одной из целей дипломной работы являлось измерение параметров всей сети, поэтому было необходимо подключить тестер наиболее подходящим способом чтобы измерить трафик целиком внутри лабораторной сети. Для измерения параметров существует несколько способов подключения тестера к сети. Был выбран наиболее оптимальный способ:

⁷ ОС- Операционная Система

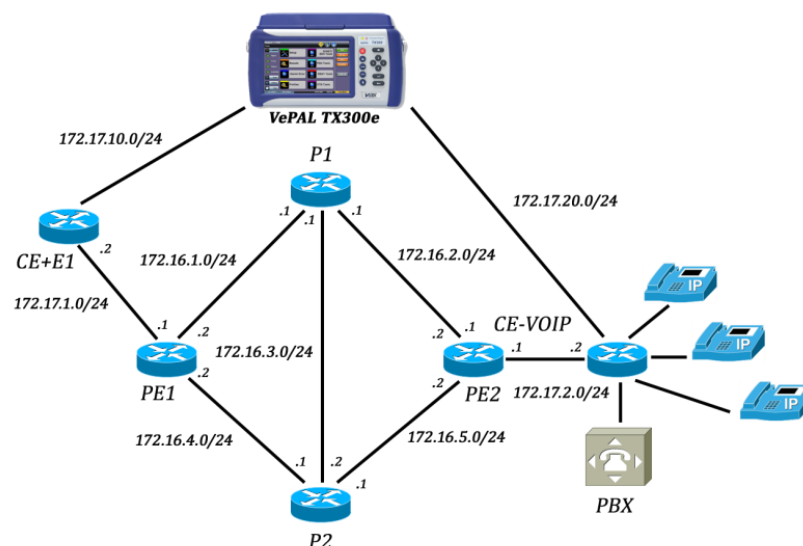


Рис. 18: Схема подключения тестера VePAL TX300e к лабораторной сети

Были выбраны наиболее удалённые от себя маршрутизаторы, в частности CE+E1 и CE-VOIP. Подключение реализовано с помощью дополнительных модулей на HWIC-4ESW-POE. Данный модуль предоставляет 4 дополнительных высокоскоростных порта. Тестер был подключён через 2 порта обозначенных как Cu P1 и Cu P2 (максимальная скорость сети 10/100/1000-T).

5.3.8. КОНФИГУРАЦИЯ ТЕСТЕРА

Перед тем как приступить к тесту, необходимо проконтролировать настройки тестера, задать IP адреса для определения подсети и сконфигурировать параметры теста.

Прежде всего в закладке Setup->Network надо удалить локальный IP адрес настроенный по умолчанию и перевести в режим DHCP на обоих портах тестера. После этого нажав кнопку Connect, тестер автоматически подключится к сети. Проверить работоспособность можно с помощью утилиты ping, которая находится в тех же настройках.

Setup	Status	Ping	Trace Route	ARPWiz
DHCP server		172.17.20.1:67		
DHCP Lease Time		1 days		
Local IP		172.17.20.25		
Subnet Mask		255.255.255.0		
Gateway		172.17.20.1		
DHCP:		PASS		
IP:		PASS		
Gateway:		PASS		

Рис. 19: Настройки тестера после подключения к серверу DHCP

Теперь необходимо переключиться в меню теста RFC 2544. Тестируется соответственно сетевой уровень, поэтому в закладке Setup->Header нужно переключить тестируемый уровень с канального по умолчанию на сетевой. Далее для того чтобы анализатор смог найти конечный порт приёма пакета необходимо задать MAC Destination в закладке ARP Gateway. Настройку самого теста RFC 2544 можно не проводить, по умолчанию каждый тест проводится в течении 5 секунд. Для увеличения результата точности теста можно повысить данный параметр до 15, однако полное время теста может быть увеличено на часы. Так же, здесь можно выбрать размер измеряемых кадров от 64 до 1518 Байт. По умолчанию, в тесте уже поднастроена измерение 128, 256 и 512 Байт. Сюда же добавим ещё 2 кадра с длиной 64 и 1028 Байт. Одному из подключённых портов надо назначить loopback на сетевом уровне, после этого нажать кнопку Start.

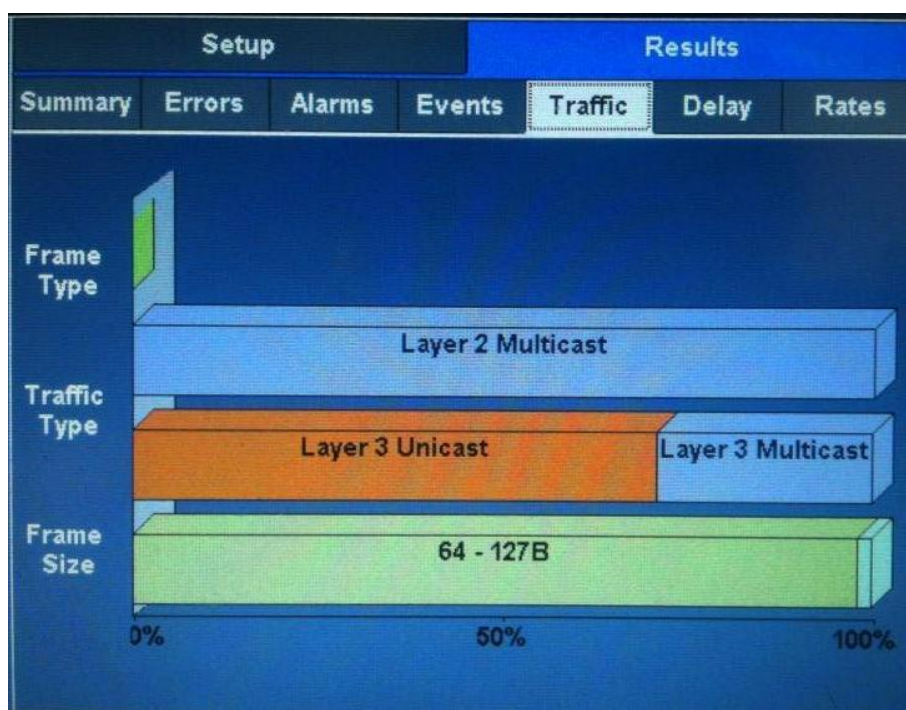


Рис. 20: Обработка трафика в процессе работы loopback

На другом порту Si 1-2 можно начать тест RFC 2544. Результаты теста будут доступны через специальную закладку о статусе теста. Там же можно посмотреть уже имеющиеся результаты не дожидаясь окончания серии.

Следующие результаты актуальны для первого сета теста:

Длина пакета [Б]	[Мбзс]	[ФЗС]
64	29,64	56076
128	53,98	52565
256	83,23	44651
512	95,66	23689
1024	98,50	12038

Табл. 4: Измерение пропускной способности лабораторной сети тестом RFC 2544

Тест показывает, что с увеличением размера кадра, увеличивается пропускная способность, из-за высокой нагрузки на маршрутизатор.

Длина пакета [Б]	Задержка [мкс]	[Мбзс]
64	1615,08	29,64
128	1998,56	53,98
256	1896,14	83,23
512	2101,13	95,66
1024	3519,69	98,50

Табл. 5: Измерение сетевой задержки

Задержка стремительно растёт с увеличением пропускной способности.

Длина пакета [Б]	Потеря пакетов [%]	[Мбзс]
64	0	29,64
128	0	53,98
256	0	83,23
512	0	95,66
1024	0	98,50

Табл. 6: Измерение процентуального отношения потерянных пакетов

В ходе теста все отправленные пакеты успешно прошли по сети, потери пакетов не произошло.

5.3.9. ТЕСТ V-SAM

Данный тест соответствует стандарту ITU-T Y.1564. В отличие от RFC 2544, тест Y.156sam нацелен на измерение параметров QoS сети, прежде всего Ethernet линий мобильного трафика. Тестируются следующие характеристики:

➤ Переменная задержка кадров

Так же называется как джиттер, это величина промежуточной задержки между доставкой двух кадров. Проходя через сеть, пакеты по умолчанию имеют одинаковый приоритет, поэтому, вследствие загруженности сети, мультимедийные пакеты могут задерживаться на своём пути, то есть иметь нерегулярный интервал прибытия по месту отправки. Измерение джиттера позволяет выявить этот интервал.[15]

Длина пакета [Б]	Джиттер [мкс]	[Мбзс]
64	40,01	29,64
128	12,16	53,98
256	0,93	83,23
512	1,02	95,66
1024	0,96	98,50

Табл. 7: Измерение джиттера лабораторной сети

5.3.10. РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

После проведённых измерений, можно предположить, исходя из наилучшего результата у кадра с длиной в 256 Байт, что именно он подходит для отправки мультимедийных данных в режиме реального времени, таких как голосовая связь либо видео.

6. ЗАКЛЮЧЕНИЕ

Дипломная работа позволяет рассмотреть конфигурацию VoIP сети и телефонной станции IP PBX10 от производителя SMC Networks. В первом разделе, описывается введение в современную технологию VoIP. Во второй главе описывается сразу два протокола, с которыми велась работа это MPLS и SIP. Были рассмотрены преимущества и недостатки MPLS а также, описан принцип работы и анализирован протокол SIP. В следующей главе, приведено полное описание протоколов маршрутизации, некоторые из которых были использованы в рамках данной работы. Была анализирована и описана топология лабораторной сети и доступного оборудования для решения поставленной задачи. Далее следует решение дипломной работы. Приведены и описаны необходимые программы, для подключения и работы с лабораторными маршрутизаторами от компании Cisco. Приведено полное описание и настройка мобильной телефонной станции IP PBX10 и конфигурация IP телефонов, подключённых к ней, создание диал плана. В дипломной работе приводится командная настройка протоколов MPLS и OSPF на маршрутизаторе P1, а также телефонного сервиса на CE-VoIP, как и Cisco IP телефонов. Каждый из подключенных телефонов может дозвониться до любого последующего подключенного устройства двух отдельных локальных сетей. В работе приводится описание настройки SIP транка для обеих станций.

В последней части реализации проекта, описывается тестер VePAL TX300e и схема его подключения к лабораторной сети для измерения параметров QoS, теста V-SAM. Измеряемые данные описаны исходя из самого теста по стандарту RFC 2544. По результатам тестирования, был сделан вывод о подходящей длине кадра в байтах, для передачи мультимедийных данных, таких как голосовые службы и видео сигнал в реальном времени. Все измеренные результаты записаны в соответствующие таблицы.

Недостаток данной работы, заключается лишь в ограниченности оборудования конкретного производителя, хотя это и замещается простотой, и доступностью данного девайса, в условиях современной IP телефонии, этого уже недостаточно. В будущем, производители телефонных устройств, возможно, пойдут на увеличение доли присутствия в данном оборудовании сервисов и программ с открытым исходным кодом.

С развитием локальных сетей, развивается IP телефония. Всё чаще необходимо уметь настраивать VoIP сети, данная дипломная работа иллюстрирует возможности конфигурирования таких сетей.

СПИСОК ИСПОЛЬЗУЮЩИХСЯ СОКРАЩЕНИЙ

ATM	Asynchronous Transfer Mode
Cisco UCM	Unified Communications Manager
CDR	Call Detail Record
DHCP	Dynamic Host Configuration Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
HTTP(S)	Hypertext Transfer Protocol (Secure)
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
ITSP	Internet Telephony Service Provider
IVR	Interactive Voice Response
LSR	Label-Switched Router
LSP	Label-Switched Path
LAN	Local Area Network
MPLS	Multiprotocol Label Switching
MAC	Media Access Control
NAT	Network Resolution Protocol
OSPF	Open Shortest Path First
OSI	Open System Interconnection basic reference model
PBX	Private Branch Exchange
QoS	Quality of Service
POTS	Plain Old Telephony Service
PDH	Plesiochronous Digital Hierarchy
RIP	Routing Information Protocol
SDH	Synchronous Digital Hierarchy
SIP	Session Initiation Protocol
SSH	Secure Shell
SCCP	Skinny Client Control Protocol
STUN	Session Traversal Utilities
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UART	Universal Asynchronous Receiver-Transmitter
VoIP	Voice over Internet Protocol

VPI	Virtual Path Identifier
VCI	Virtual Channel Identifier
VPN	Virtual Private Network
WAN	Wide Area Network

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ И ЦИТАТ

- [1] ВИБЕК, Олвейн. *Структура и реализация современной технологии MPLS*. Издательский дом "Вильямс". Москва: Cisco press 2002, 2004. ISBN 5-8459-0633-4.
- [2] DYE, Mark A., Rick MCDONALD a Antoon W. RUF. COPYRIGHT© 2008 CISCO SYSTEMS, Inc. *Network fundamentals : CCNA exploration companion guide*. Cisco Press, 800 East 96th Street, Indianapolis, IN 46240 USA. Indianapolis: Cisco, 2008. ISBN 978-1-58713-208-7.
- [3] GRAZIANI, Rick a Allan JOHNSON. COPYRIGHT© 2008 CISCO SYSTEMS, Inc. *Routing protocols and concepts : CCNA exploration companion guide*. Cisco Press, 800 East 96th Street, Indianapolis, IN 46240 USA. Indianapolis: Cisco, 2008. ISBN 978-1-58713-206-3.
- [4] Routing Information Protocol. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-10-29]. Доступно с WWW: http://ru.wikipedia.org/wiki/Routing_Information_Protocol
- [5] Open Shortest Path First. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-10-29]. Доступно с WWW: <http://ru.wikipedia.org/wiki/OSPF>
- [6] OSPF Design Guide. CISCO. [Http://www.cisco.com](http://www.cisco.com) [online]. 2005 [cit. 2013-10-29]. Доступно с WWW: http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml#t6
- [7] Enhanced Interior Gateway Routing Protocol. CISCO. [Http://www.cisco.com](http://www.cisco.com) [online]. 2005, Sep 09, 2005 [cit. 2013-10-29]. Доступно с WWW: http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094cb7.shtml
- [8] EIGRP. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-10-29]. Доступно с WWW: <http://ru.wikipedia.org/wiki/EIGRP>
- [9] *VC-365 Cisco IOS Voice, Video, and Fax Configuration Guide Configuring Session Initiation Protocol for Voice over IP* [online]. San Jose: Cisco Inc., 2006, s. 1-20, 18.1.2008 [cit. 2013-12-01]. Доступно с WWW: http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/vvfsip.pdf
- [10] Skinny Call Control Protocol. In: *Wikipedia: the free encyclopedia* [online]. 2008. vyd. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-12-27]. Доступно с WWW: http://en.wikipedia.org/wiki/Skinny_Call_Control_Protocol
- [11] HEDRICK, C. Internet Standart: Routing Information Protocol. *RFC 1058* [online]. 1988, s. 31 [cit. 2014-05-08]. Доступно с WWW: <http://tools.ietf.org/html/rfc1058>
- [12] MALKIN, G. Internet Standart: Routing Information Protocol version 2. *RFC 2453* [online]. 1998, s. 39 [cit. 2014-05-08]. Доступно с WWW: <https://tools.ietf.org/html/rfc2453>

- [13] BRADNER, S. a J. MCQUAID. Internet Standart: Benchmarking Methodology for Network Interconnect Devices. *RFC 2544* [online]. 1999, s. 31 [cit. 2014-14-05]. Доступно с WWW: <http://tools.ietf.org/html/rfc2544>
- [14] Throughput. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2011-11-18, 2014-05-3 [cit. 2014-05-14]. Доступно с WWW: <http://en.wikipedia.org/wiki/Throughput>
- [15] ITU-T Y.156sam. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2010-12-30, 2013-06-04 [cit. 2014-05-14]. Доступно с WWW: <http://en.wikipedia.org/wiki/Y.156sam>
- [16] SMC IP PBX10 *e-Manual* [online]. Tiget VoIP: IP PBX Systems 2010 [cit. 2014-04-15]. Доступно с WWW: http://www.smc-asia.com/tw/files/DS_SMCPBX10.pdf
- [17] VePAL TX300 *e-Manual* [online]. VeEX Inc.: Portable SONET/Ethernet Test 2010 [cit. 2014-0-05]. Доступно с WWW: http://www.southeastdatacom.com/images/TX300_D05-00-022P_D01.pdf
- [18] EXFO. *Блок тестирования IP сервисов: RTU-310*. Canada, 2010. Доступно с WWW: <http://www.exforus.ru/pdf/RTU-310-rusHR.pdf>