МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)

НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

РАССМОТРЕНО
На заседании ПЦК ЭТД
Протокол № 7 «31» августа_2022г.
Председатель ПЦК
_____Тен М.Б.

УТВЕРЖДАЮ
Зам. директора по УВР
НефтИн (филиал) ФГБОУ ВО «ЮГУ»
«31» августа 2022 г.
_____Хайбулина Р.И

КОМПЛЕКТ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ (МЕЖДИСЦИПЛИНАРНОМУ КУРСУ)

МДК.01.05 — индекс
ЭКСПЛУАТАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ — (наименование учебной дисциплины, МДК)

программы подготовки специалистов среднего звена (ППССЗ)
по специальности СПО

10.02.05 — код
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ — (наименование)

базовой подготовки

г. Нижневартовск

-2022-

Комплект контрольно-измерительных материалов по междисциплинарному курсу
МДК.01.05. ЭКСПЛУАТАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

(наименование учебной дисциплины, МДК)

программы подготовки специалистов среднего звена (ППССЗ) по специальности СПО 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

(код, наименование специальности)

базового уровня разработан на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ,

(код, наименование специальности)

в соответствии с рабочей программой учебной дисциплины, профессионального модуля ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

(наименование учебной дисциплины, ПМ)

Разработчик:

Нефтяной институт (НефтИн (филиал) ФГБОУ ВО «ЮГУ»)	преподаватель	Е.А. Романцова
(место работы)	(занимаемая должность)	(инициалы, фамилия)

1. Паспорт комплекта контрольно-измерительных материалов по учебной дисциплине МДК.01.05 Эксплуатация компьютерных сетей

1.1. Область применения

Комплект контрольно-измерительных материалов предназначен для проверки результатов освоения междисциплинарного курса (далее - МДК) МДК.01.05 Эксплуатация компьютерных сетей программы подготовки специалистов среднего звена (ППССЗ) по специальности (специальностям) СПО
10.02.05 Обеспечение информационной безопасности автоматизированных систем

код наименование

Комплект контрольно-измерительных материалов позволяет оценивать:

1.1.1. Освоение профессиональных компетенций (ПК) и общих компетенций (ОК)

Профессиональные и общие компетенции	Средства проверки(№ задания)
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Практические работы №№30, 31, 32, 33
ПК 1.3. Обеспечивать бесперебойнуюработу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Практические работы №№27, 28, 29
ПК 1.4. Осуществлять проверку технического состояния, техническоеобслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособностьавтоматизированных (информационных) систем взащищенном исполнении.	Практические работы №№1-10
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Практические работы №№10,11,14,15-20
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Практические работы №№22-26
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Итоговый тест
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Практические работы №№37,38
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Практические работы №№31-34
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Практические работы №№42,43
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Практические работы №№34
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Практические работы №№35

ОК 09. Использовать информационные технологии в профессиональной деятельности.	Практические работы №№1-43
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	Практические работы №№1-43

1.1.2. Освоение умений и усвоение знаний

Освоенные умения, усвоенные знания	№№ заданий для проверки
1	2
У5. Настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.	Практические работы №№42,43
У6. Обеспечивать работоспособность, обнаруживать и устранять неисправности	Практические работы №№42,43
З5. Теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации.	Практические работы №№42,43
З6. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	

1.2. Система контроля и оценки освоения программы междисциплинарного курса

1.2.1. Формы рубежной аттестации по ППССЗ при освоении учебной дисциплины (междисциплинарного курса)

Учебная дисциплина (междисциплинарный курс)	Формы промежуточной аттестации
1	2
МДК 01.05. Эксплуатация компьютерных сетей	Экзамен (6 семестр)
МДК 01.05. Эксплуатация компьютерных сетей	ДФК (7 семестр)

1.2.2. Организация контроля и оценки освоения программы МДК 01.05 Эксплуатация компьютерных сетей

Промежуточный контроль по дисциплине осуществляется в форме экзамена в 6 семестре и ДФК в 7 семестре.

Условием допуска к экзамену является положительная оценка по всем практическим работам.

Экзамен выставляется по результатам тестирования.

Условием положительной аттестации по междисциплинарному курсу на экзамене является положительная оценка освоения всех умений, знаний, а также формируемых профессиональных компетенций по всем контролируемым показателям.

2. Задания для оценки освоения умений и усвоения знаний при изучении учебной дисциплины МДК.01.05 Эксплуатация компьютерных сетей

2.1. Комплект материалов для оценки освоения умений и усвоения знаний

2.1.1. Комплект заданий для обучающихся

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ И ЛАБОРАТОРНЫХ РАБОТ, ТЕМАТИКА ПО УЧЕБНОЙ ДИСЦИПЛИНЕ МДК.01.05 ЭКСПЛУАТАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Раздел	Номер и тема занятия	Количество аудиторных часов
1	**2**	**3**
1.	Практическое занятие №1 Изучение элементов кабельной системы.	2
1.	Практическое занятие №2 Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	2
1.	Практическое занятие №3 Сварка оптического волокна	2
1.	Практическое занятие №4 Разработка топологи сети небольшого предприятия	2
1.	Практическое занятие №5 Построение одноранговой сети	2
1.	Практическое занятие №6 Изучение адресации канального уровня. MAC-адреса.	2
1.	Практическое занятие №7 Создание коммутируемой сети	2

1.	Практическое занятие №8 Изучение IP-адресации.	2
1.	Практическое занятие №9 Настройка беспроводного сетевого оборудования	2
2.	Практическое занятие №10 Работа с основными командами коммутатора.	2
2.	Практическое занятие №11 Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	2
2.	Практическое занятие №12 Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	2
2.	Практическое занятие №13 Настройка VLAN на основе стандарта IEEE 802.1Q	2
2.	Практическое занятие №14 Настройка протокола GVRP.	2
2.	Практическое занятие №15 Настройка сегментации трафика без использования VLAN	2
2.	Практическое занятие №16 Настройка функции Q-in-Q (Double VLAN).	2
2.	Практическое занятие №17 Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.	2
2.	Практическое занятие №18 Настройка протоколов связующего дерева STP, RSTP, MSTP.	2
2.	Практическое занятие №19 Настройка функции защиты от образования петель LoopBackDetection	2
2.	Практическое занятие №20 Агрегирование каналов.	2
2.	Практическое занятие №21 Основные конфигурации маршрутизатора.	2
2.	Практическое занятие №22 Расширенные конфигурации маршрутизатора.	2
2.	Практическое занятие №23 Работа с протоколом CDP.	2
2.	Практическое занятие №24 Работа с протоколом TELNET. Работа с протоколом TFTP.	2
2.	Практическое занятие №25 Работа с протоколом RIP.	2
2.	Практическое занятие №26 Работа с протоколом OSPF.	2
2.	Практическое занятие №27 Конфигурирование функции маршрутизатора NAT/PAT.	2
2.	Практическое занятие №28 Конфигурирование PPP и CHAP.	2
2.	Практическое занятие №29 Настройка QoS. Приоритизация трафика. Управление полосой пропускания	2
2.	Практическое занятие №30 Списки управления доступом (AccessControlList)	2
2.	Практическое занятие №31 Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.	2
2.	Практическое занятие №32 Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	2
2.	Практическое занятие №33 Отслеживание трафика многоадресной рассылки.	2
2.	Практическое занятие №34 Отслеживание трафика Multicast	2
2.	Практическое занятие №35 Функции анализа сетевого трафика.	2
2.	Практическое занятие №36 Настройка протокола управления топологией сети LLDP.	2
3.	Практическое занятие №37 Основы администрирования межсетевого экрана	2
3.	Практическое занятие №38 Соединение двух локальных	2

	сетей межсетевыми экранами	
3.	Практическое занятие №39 Создание политики без проверки состояния.	2
3.	Практическое занятие №40 Создание политик для традиционного (или исходящего) NAT.	2
3.	Практическое занятие №41 Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing	2

ПРАКТИЧЕСКАЯ РАБОТА № 1

Изучение элементов кабельной системы

Цели: изучить элементы кабельной системы.

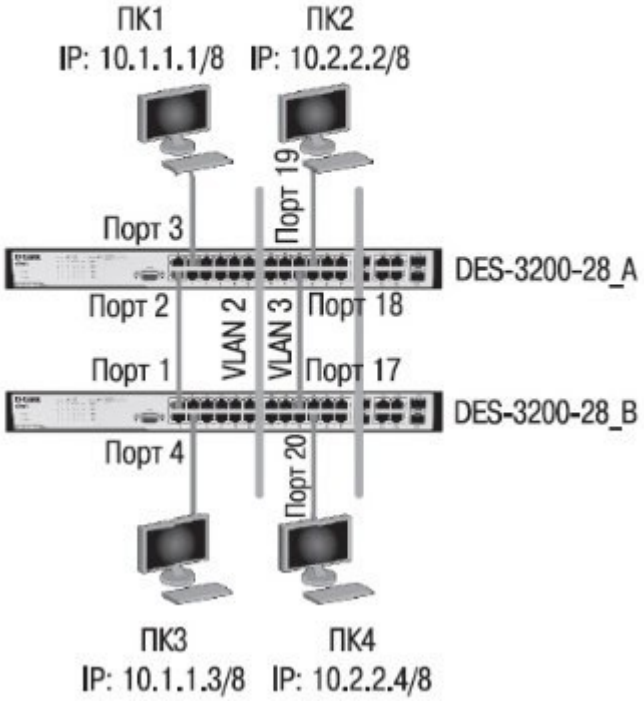
Теоретические вопросы

1. Типы VLAN.
2. VLAN на основе портов.
3. VLAN на основе стандарта IEEE 802.1Q.
4. Статические и динамические VLAN.
5. Протокол GVRP.
6. Q-in-Q VLAN.
7. VLAN на основе портов и протоколов – стандарт IEEE 802.1v.
8. Функция TrafficSegmentation

Задание 1. Изучите технологию VLAN и ее настройку на коммутаторах D-Link:

Оборудование:

DES-3200-28	2 шт.
Рабочая станция	8 шт.
Кабель Ethernet	10 шт.
Консольный кабель	2 шт.



Задание 2. Опишите команды настройки коммутаторов на основе портов:

Настройка DES-3200-28_A удалите порты из VLAN по умолчанию для использования в других VLAN config vlan default delete 1-24

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными

create vlan v2 tag 2

config vlan v2 add untagged 1-12 create vlan v3 tag 3

config vlan v3 add untagged 13-24

Настройка DES-3200-28_B

Удалите порты из VLAN по умолчанию для использования в других VLAN config vlan default delete 1-24

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными

create vlan v2 tag 2

config vlan v2 add untagged 1-12 create vlan v3 tag 3

config vlan v3 add untagged 13-24

Задание 3. Опишите команды настройки коммутаторов на основе стандарта IEEE 802.1Q:

Настройка DES-3200-28_A

Сбросьте настройки коммутатора к заводским настройкам по умолчанию

reset config

Удалите порты из VLAN по умолчанию для использования в других VLAN config vlan default delete 1-24

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными

create vlan v2 tag 2

config vlan v2 add untagged 1-10 config vlan v2 add tagged 24

Настройте порт 24 маркированным create vlan v3 tag 3

config vlan v3 add untagged 11-20 config vlan v3 add tagged 24

Настройка DES-3200-28_B

Сбросьте настройки коммутатора к заводским настройкам по умолчанию

reset config

Удалите порты из VLAN по умолчанию для использования в других VLAN config vlan default delete 1-24

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными.

create vlan v2 tag 2

config vlan v2 add untagged 1-10 config vlan v2 add tagged 24 Настройте порт 24 маркированным create vlan v3 tag 3

config vlan v3 add untagged 11-20
config vlan v3 add tagged 24

Задание 4. Проверьте настройки VLAN на обоих коммутаторах. Проверьте доступность соединения командой ping.

ПРАКТИЧЕСКАЯ РАБОТА № 2

Создание сетевого кабеля на основе неэкранированной витой пары (UTP)

Цели: научиться обжимать сетевой кабель на основе неэкранированной витой пары (UTP).

Теоретические вопросы

1. Понятие линии и канала связи.
2. Основные характеристики канала связи.
3. Методы совместного использования среды передачи канала связи.
4. Мультиплексирование и методы множественного доступа.
5. Стандарты кабелей. Электрическая проводка.

Задание 1. Подобрать и описать необходимые инструменты для создания сетевого кабеля на основе неэкранированной витой пары (UTP).

Задание 2. Опишите последовательность действий обжима кабеля.

Задание 3. Подготовьте сетевой кабель.

Задание 4. Проверьте кабель на работоспособность.

ПРАКТИЧЕСКАЯ РАБОТА № 3

Сварка оптического волокна

Цели: изучить способы соединения оптического волокна.

Теоретические вопросы

1. Понятие линии и канала связи.
2. Основные характеристики канала связи.
3. Методы совместного использования среды передачи канала связи.
4. Мультиплексирование и методы множественного доступа.
5. Стандарты кабелей. Электрическая проводка.
6. Оптоволоконные линии связи.

Задание 1. Изучите и опишите требования, предъявляемые к неразъемным соединениям.

Задание 2. Опишите способы соединения оптического волокна.

Задание 3. Изучите и опишите конструкции устройств, для оперативного подключения волокна.

Задание 4. Изучите и опишите назначение инструментов по разделке волоконно-оптических кабелей.

Задание 5. Ознакомьтесь с работой сварочного аппарата.

Задание 6. Произведите сварку оптического волокна.

ПРАКТИЧЕСКАЯ РАБОТА № 4

Разработка топологи сети небольшого предприятия

Цели: изучить виды топологий компьютерных сетей.

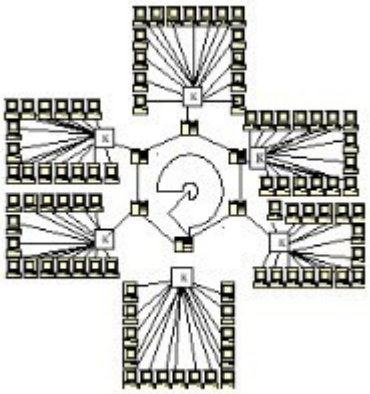
Теоретические вопросы

1. Понятие топологии сети.
2. Сетевое оборудование в топологии.
3. Обзор сетевых топологий**.**

Задание 1. Опишите топологии компьютерных сетей. Приведите схемы топологий компьютерных сетей.

Вид топологии	Достоинства	Недостатки
Сетевая топология «звезда»		
Сетевая топология «кольцо»		
Сетевая топология «шина»		

Задание 2. Изучите схему соединения компьютерной сети: Сервер 6 кольцо, ПК 15 звезда.



Задание 3. Создать схему соединения компьютерной сети согласно своему заданию.

Варианты заданий:

№	**Сервер**	**ПК**	**Топология**	
			Сервер	**ПК**
1	4	6	Общая шина	Кольцо
2	3	7	Звезда	Звезда
3	4	5	Звезда	Полносвязная
4	6	5	Звезда	Общая шина
5	3	7	Кольцо	Звезда
6	6	3	Звезда	Кольцо
7	4	11	Общая шина	Кольцо
8	5	4	Кольцо	Полносвязная
9	6	5	Звезда	Звезда
10	7	4	Общая шина	Полносвязная

11	5	6	Звезда	Кольцо
12	8	4	Звезда	Полносвязная
13	3	7	Общая шина	Общая шина
14	6	6	Общая шина	Кольцо
15	5	5	Полносвязная	Звезда
16	4	7	Полносвязная	Общая шина
17	5	6	Полносвязная	Кольцо
18	7	3	Общая шина	Звезда
19	8	4	Кольцо	Кольцо
20	5	6	Полносвязная	Полносвязная
21	8	5	Общая шина	Звезда
22	6	4	Кольцо	Полносвязная
23	5	5	Звезда	Полносвязная
24	4	6	Звезда	Звезда
25	5	6	Общая шина	Кольцо
26	8	5	Звезда	Полносвязная
27	5	7	Общая шина	Кольцо
28	8	4	Общая шина	Полносвязная
29	5	7	Полносвязная	Кольцо
30	3	8	Кольцо	Общая шина

Задание 4. Опишите построенную топологию.

ПРАКТИЧЕСКАЯ РАБОТА № 5

Построение одноранговой сети

Цель: **изучите способы построения одноранговых сетей.**

Теоретические вопросы

1. Типы локальных сетей.
2. Одноранговые сети.
3. Иерархические сети.

Задание 1. Опишите типы локальных сетей. Приведите схемы сетей.

Тип локальной сети	Достоинства	Недостатки
Одноранговая сеть		
Иерархическая сеть		

Задание 2. Описать одноранговую локальную сеть с топологией линейная шина. Проанализируйте описание локальной сети и сделайте выводы. Заполните таблицу.

Схема локальной сети	
Достоинства	
Недостатки	
Количество компьютеров в сети	
Оборудование, необходимое для создания сети и его стоимость	
Общая стоимость создания локальной сети	

Задание 3. Описать одноранговую локальную сеть с топологией звезда. Проанализируйте описание локальной сети и сделайте выводы. Заполните таблицу.

Схема локальной сети	
Достоинства	
Недостатки	
Количество компьютеров в сети	
Оборудование, необходимое для создания сети и его стоимость	
Общая стоимость создания локальной сети	

ПРАКТИЧЕСКАЯ РАБОТА № 6

Изучение адресации канального уровня. MAC-адреса

Цели: изучит команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы.

Теоретические вопросы

1. Средства управления коммутаторами.
2. Подключение к консоли интерфейса командной строки коммутатора.
3. Подключение к Web-интерфейсу управления коммутатора.
4. Начальная конфигурация коммутатора.
5. Загрузка нового программного обеспечения на коммутатор.
6. Загрузка и резервное копирование конфигурации коммутатора.

Задание 1. Изучите команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов коммутаторов D-Link:

Оборудование:

DES-3200-28 1 шт.

DGS-3612G 1 шт.

Рабочая станция 1 шт.

Кабель Ethernet 1 шт.

Консольный *кабель* 2 шт.

Схема 1

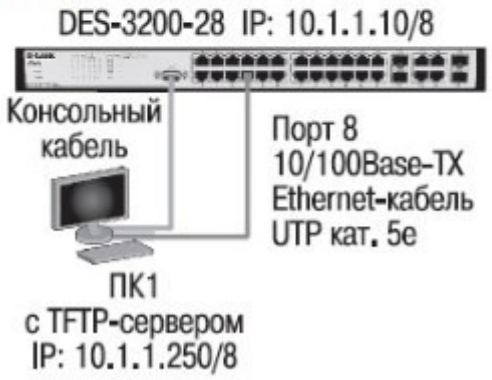
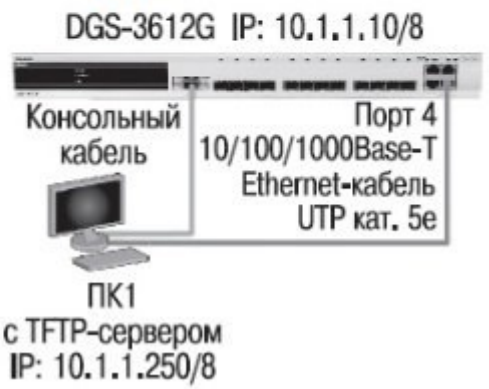


Схема 2



Задание 2. Опишите команды настройки DES-3200-28:

Настройка DES-3200-28

Изучение команд просмотра таблиц MAC-адресов

Посмотрите таблицу MAC-адресов show fdb

Найдите порт коммутатора, к которому подключено устройство с определенным MAC-адресом (например, 00-14-85-F2-D7-BE) show fdb macaddress 00-14-85-F2-D7-BE

Внимание! Замените указанные в командах MAC-адреса на реальные.

Посмотрите список MAC-адресов устройств, принадлежащих VLAN по умолчанию show fdb vlan default

Посмотрите MAC-адреса устройств, изученные портом 16 show fdb port 16

Посмотрите время нахождения записи в таблице MAC-адресов show fdb agingtime

Изучение команд управления таблицей MAC-адресов Создайте статическую запись в таблице MAC-адресов create fdb default 00-00-00-00-01-02 port 5

Удалите статическую запись из таблицы MAC-адресов delete fdb default 00-00-00-00-01-02

Измените время нахождения MAC-адреса в таблице до 350 секунд config fdb agingtime 350

Удалите все динамически созданные записи из таблицы MAC-адресов clear fdb all

Настройка DGS-3612G (работа с таблицей коммутации уровня 3 (IP FDB)) Изучение команд просмотра таблиц коммутации IP-адресов Посмотрите таблицу коммутации IP-адресов show ipfdb

Задание 3. Опишите команды настройки DES-3200-28 /DGS-3612G (управление ARP-таблицами):

Изучение команд просмотра ARP-таблиц Посмотрите ARP-таблицу show arpentry

Найдите в ARP-таблице сопоставления IP-MAC по указанному IP-адресу show arpentry ipaddress 10.1.1.250

Посмотрите в ARP-таблице все сопоставления IP-MAC на интерфейсе System show arpentry ipif System

Изучение команд управления ARP-таблицей Создайте статическую запись в ARP-таблице create arpentry 10.1.1.250 00-50-BA-00-07-36 Удалите запись из ARP-таблицы delete arpentry 10.1.1.250

Измените время нахождения записи в ARP-таблице до 30 минут (по умолчанию — 20 минут)

config arpaging time 30

Удалите все динамически созданные записи из ARP-таблицы clear arptable

Задание 4. Подключите станцию к любому порту коммутатора, как показано на схеме 1. Попробуйте найти соответствие IP-MAC-адресов подключенной станции в ARP-таблице.

ПРАКТИЧЕСКАЯ РАБОТА № 7
Создание коммутируемой сети

Цель: изучить состав аппаратного и программного обеспечения сетей ЭВМ, получить практические навыки базовой настройки сетевой системы.

Теоретические вопросы

1. Методы коммутации.
2. Технологии коммутации и модель OSI.
3. Конструктивное исполнение коммутаторов.
4. Физическое стекирование коммутаторов.
5. Программное обеспечение коммутаторов.

Задание 1. Охарактеризовать назначение, маркировку, функции и параметры следующего коммуникационного оборудования:

Повторитель Концентратор Коммутатор

Кабельная система «Витая пара» Оптоволоконный кабель Маршрутизатор

Брандмауэр Сетевая плата Модем

Мост

Задание 2. В соответствии с вариантом подобрать активное сетевое оборудование, способное удовлетворить всем требованиям задания. Каждый вариант состоит из трёх типов задач, требующих различных методов решения. Первая задача предельно формализована, т.е. явно указаны технологии, которые должен поддерживать прототип. Во второй и третьей задаче формализация падает. При подборе оборудования необходимо соблюдать принцип минимизации финансовых затрат. Ограничения по производителям оборудования нет, однако рекомендуется обратить внимание на оборудование LinkSys, CISCO, D-LINK, ASUS, HP.

Вариант 1

1. Подобрать коммутатор с 48 портами Fast Ethernet и двумя портами Gigabit Ethernet, поддерживающий технологию управления потоком IEEE 802.3x.

2. Подобрать коммутационное оборудование для сети небольшого офиса. В состав сети входят 15 компьютеров с равным уровнем доступа. В сети офиса установлена NAS(Network

Attached Storage) SYNOLOGY DS 412+. Требуется обеспечить получение данных с NAS на максимальной скорости. Для оценки производительности следует считать, что скорость чтения с NAS при подключении каждого нового клиента падает на 5%. Обеспечить возможность подключения существующей IDS (системы обнаружения вторжения), осуществляющей мониторинг всего передаваемого внутри локальной сети трафика.

3. Подобрать коммутационное оборудование для сети крупного автосервиса . Требуется создать инфраструктуру для обслуживания 6 ремонтных боксов. Необходимо обеспечить работоспособность специализированного программного обеспечения и доступность необходимых сетевых ресурсов пользователям. Сотрудник и имеют коммуникационные устройства (20 шт.) с беспроводным интерфейсом, которое служит для оповещения о поступивших заказах. Каждое из этих устройств должно работать на всей территории автосервиса. Доступ к беспроводной сети должен быть защищен с помощью авторизации на централизованном сервисе. Расстояние между наиболее удаленными точками ремонтных боксов 340 метров. Сервер баз данных расположен в аппаратной в офисных помещениях. Расстояние между коммуникационным шкафом в одном из ремонтных боксов, и коммуникационной стойки в аппаратной офисной части 240 м по кабельной трассе.

Вариант 2

1. Подобрать неуправляемый коммутатор с 16 портами 10/100/1000 Base-T и поддержкой технологии IEEE 802.1 p QoS.

2. Подобрать коммутационное оборудование для проведения чемпионата России по киберспорту. Необходимо обеспечить совместную работу минимум 90 компьютеров. Следует избежать ситуации задержек в игре из-за недостаточной производительности коммутационного оборудования. Пиковый трафик, генерируемый средней современной сетевой игрой, составляет 40 Мб\с. Предусмотреть возможность компактной установки коммутационного оборудования в стойку.

3. Подобрать коммутационное оборудование для телевизионной компании. Требуется обеспечить раздельную работу 4 студий. Количество компьютеров в студиях по 40 шт. Поставщик услуг телефонии предоставляет для оборудования студий 156 ip-телефонов D-Link DPH-150SE/F3 и сервер IP телефонии на базе Asterisk. Требуется обеспечить возможность приоритетной передачи данных IP-телефонии.

ПРАКТИЧЕСКАЯ РАБОТА № 8
Изучение IP-адресации

Цели: получить практические навыки по работе с пространством IP-адресов, масками и управления адресацией в IP сетях.

Теоретические вопросы

1. Сетевой уровень.
2. Протокол IP версии 4.
3. Общие функции классовой и бесклассовой адресации.
4. Выделение адресов.

5. Маршрутизация пакетов IPv4.

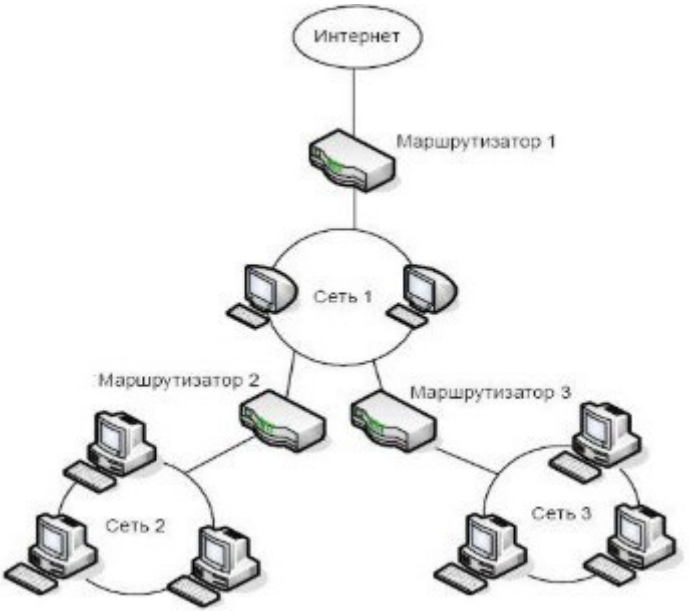
Задание 1. В работе даны 4 варианта задания (Табл. 1). Необходимо сделать все варианты. На приведенной схеме представлена составная локальная сеть. Отдельные локальные сети соединены маршрутизаторами. Для каждой локальной сети указано количество компьютеров. Провайдер, для вас выдал IP-сеть (данные о сети представлены в табл. 2). Ваша задача установить IP-адрес сети и допустимый диапазон адресов. Разделить вашу сеть на части, используя маски. Маску надо выбирать так, чтобы в отделяемой IP подсети было достаточно адресов. Помните, что и порт маршрутизатора, подключенный к локальной сети, имеет IP адрес! Некоторые маски представлены в табл.3.

Таблица1

Вариант	IP- адрес из сети
1	192.169.168.70
2	172.21.25.202
3	83.14.53.9
4	190.23.23.23

Таблица 2

маска	Сеть 1	Сеть 2	Сеть 3
255.255.248.0	500 комп.	16 комп.	19 комп.
255.255.255.224	1 комп.	4 комп.	2 комп.
255.255.255.128	10 комп.	12 комп.	8 комп.
255.255.255.192	5 комп	3 комп.	3 комп.



Маска	Количество двоичных 0	Количество всех адресов в IP сети с такой маской
255.255.255.252	00	4
255.255.255.248	000	8
255.255.255.240	0000	16
255.255.255.224	00000	32
255.255.255.192	000000	64
255.255.255.128	0000000	128
255.255.255.0	00000000	256
255.255.254.0	0.00000000	512

Задание 2. Заполните таблицу:

Вариант:	1		
Сеть	Сеть 1	Сеть 2	Сеть 3
IP-сети, маска			
Количество IP адресов в IP-сети			
Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров.			
Вариант:	2		
Сеть	Сеть 1	Сеть 2	Сеть 3
IP-сети, маска			
Количество IP адресов в IP-сети			
Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров.			
Вариант:	3		
Сеть	Сеть 1	Сеть 2	Сеть 3
IP-сети, маска			
Количество IP адресов в IP-сети			
Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров.			
Вариант:	4		
Сеть	Сеть 1	Сеть 2	Сеть 3
IP-сети, маска			
Количество IP адресов в IP-сети			
Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров.			

Задание 3. Сеть Internet 199.40.123.0 разбита на одинаковые подсети максимальной емкости маской 255.255.255.224. Назначить адреса интерфейсам подсетей и, по крайней мере, одной рабочей станции каждой подсети.

Задание 4. Разбить адресное пространство сети 199.40.123.0 на 4 одинаковые подсети с максимальным числом узлов в каждой и назначить IP – адрес этим подсетям. Как изменится результат, если сеть должна быть разбита на N=10 подсетей?

Задание 5. Сеть Internet 199.40.123.0 разбита на одинаковые подсети маской 255.255.255.240.

Какое максимальное число узлов и рабочих станций может иметь каждая подсеть и почему?

ПРАКТИЧЕСКАЯ РАБОТА № 9

Настройка беспроводного сетевого оборудования

Цели: изучить команды настройки маршрутизатора.

Теоретические вопросы

1. Информация, выводимая при запуске маршрутизатора.
2. Настройка последовательного интерфейса. Настройка Ethernet интерфейса.
3. Управление файловой системой.
4. Режимы конфигурирования маршрутизатора.
5. Настройка последовательного интерфейса.
6. Настройка Ethernet интерфейса.
7. Управление файловой системой.

Задание 1. Опишите процесс загрузки маршрутизатора.

Задание 2. Изучите процесс начала загрузки маршрутизатора:

```
System Bootstrap, Version 12.2(4r)XL, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 2001 by cisco Systems, Inc.
C1700 platform with 65536 Kbytes of main memory
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-K9O3SY7-M), Version 12.3(20)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Tue 08-Aug-06 17:59 by kesnyder
Image text-base: 0x8000816C, data-base: 0x810A3620
```

Задание 3. Поясните информацию о маршрутизаторе:

- Количество интерфейсов маршрутизатора;
- Перечисление типов интерфейсов маршрутизатора;
- Объем NVRAM памяти;
- Объем Flash памяти.

```
cisco 1760 (MPC860P) processor (revision 0x200) with 57462K/8074K bytes of memory.
Processor board ID FOC07110UK2 (2732403599), with hardware revision BB67
MPC860P processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
```

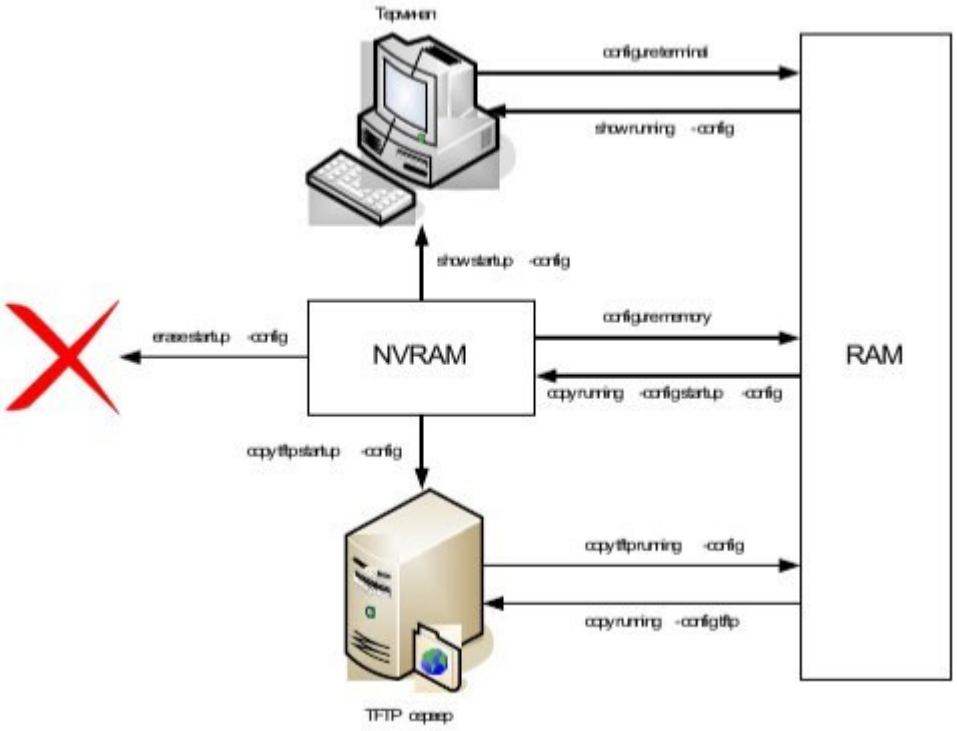
Задание 4. Опишите уровни доступа к командам маршрутизатора:

```
r1> - - - - - Пользовательский режим
r1>enable
Password:
r1# - - - - - Привилегированный режим
r1#disable
r1>
```

Задание 5. Поясните использование системой интерактивной помощи:

```
r1#
r1#clok
Translating "clok"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
r1#cl ?
% Ambiguous command:  "cl "
r1#cl?
clear  clock
r1#clock
% Incomplete command.
r1#clock ?
  set  Set the time and date
r1#clock set
% Incomplete command.
r1#clock set ?
  hh:mm:ss  Current Time
r1#clock set 04:53:00
% Incomplete command.
r1#clock set 04:53:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
r1#clock set 04:53:00 27 11
                          ^
% Invalid input detected at '^' marker.
r1#clock set 04:57:00 27 November
% Incomplete command.
r1#clock set 04:57:00 27 November ?
  <1993-2035>  Year
```

Задание 6. Изучите процесс конфигурирования маршрутизатора:



Задание 7. Опишите команды режимов конфигурирования маршрутизатора. Заполните таблицу:

Команда	Описание
configure terminal	
configure memory	
copy tftp running–config	
show running–config	
copy running–config startup–config	
copy running–config tftp	
show startup–config	
erase startup–config	

Задание 8. Опишите команды настройки:

- имени маршрутизатора,
- защиты маршрутизатора паролями,
- последовательного интерфейса,
- Ethernet интерфейса.

ПРАКТИЧЕСКАЯ РАБОТА № 10

Работа с основными командами коммутатора

Цель: изучить основные команды коммутатора.

Теоретические вопросы

1. Функционирование коммутаторов локальной сети.
2. Архитектура коммутаторов.
3. Типы интерфейсов коммутаторов.
4. Характеристики, влияющие на производительность коммутаторов.
5. Обзор функциональных возможностей коммутаторов.

Задание 1. Изучите команды настройки, контроля и устранения неполадок коммутаторов D- Link:

Оборудование:

DES-3200-28	1 шт.
Рабочая станция	1 шт.
Консольный кабель	1 шт.

Задание 2. Опишите команды коммутатора:

- просмотр списка команд конфигурирования;
- вывод команд просмотра настроек коммутатора;
- изменение IP-адреса интерфейса управления коммутатора;
- настройка IP-адреса шлюза по умолчанию;
- настройка IP-адреса шлюза по умолчанию;
- проверка настройки;
- создание учетной записи администратора;
- создание учетной записи пользователя;
- проверка настройки учетных записей пользователей;
- отключение режима администрирования;
- вход в режим администрирования;
- ввод данных для учетной записи администратора;
- изменение пароля пользователя;
- удаление учетной записи пользователя;
- проверка удаления учетной записи пользователя;
- настройка имя коммутатора;
- задание месторасположения (локализации) коммутатора;
- настройка времени на коммутаторе;
- настройка скорости и режима работы порта;
- просмотр режима работы портов;
- включение/отключение работы портов;
- задание имени порта;
- перегрузка коммутатора.

ПРАКТИЧЕСКАЯ РАБОТА № 11

Команды обновления программногообеспечения коммутатора и

сохранения/восстановления
конфигурационных файлов

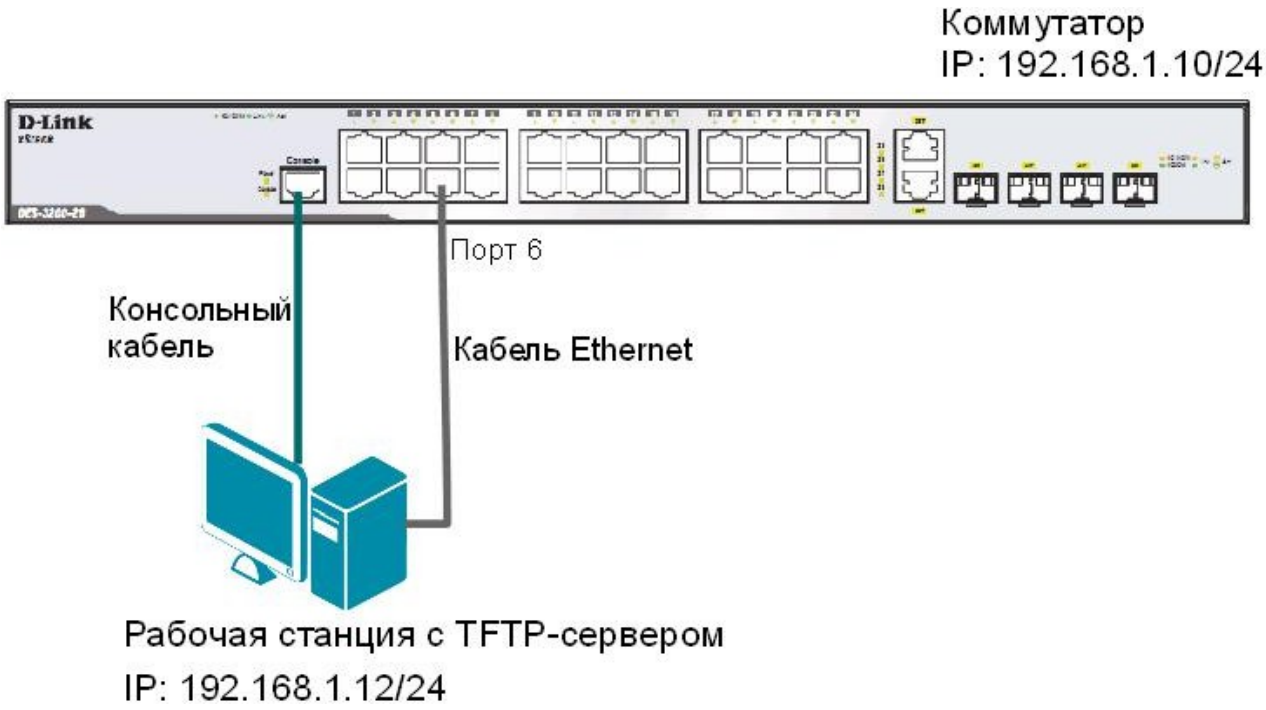
Обновление программного обеспечения (его иногда называют «прошивкой» коммутатора) может быть необходимо, когда доступна новая функциональность или требуется коррекция ошибок. Сохранять конфигурацию коммутатора необходимо при изменении его настроек, а также для упрощения восстановления функционирования коммутатора в результате сбоя его работы или поломки. Основным протоколом, применяемым для этих целей, служит протокол TFTP (Trivial File Transfer Protocol, простейший протокол передачи данных). Для передачи/загрузки программного обеспечения/конфигурации необходимо наличие в сети TFTP-сервера. Коммутаторы D-Link, поддерживают возможность хранения на коммутаторе двух версий программного обеспечения и конфигурации, причём любая из них может быть настроена как используемая при загрузке коммутатора. Это позволяет обеспечить отказоустойчивость оборудования при переходе на новое программное обеспечение или изменении конфигурации. Для изучения работы коммутатора, имеется возможность выгрузки через протокол TFTP журнала работы коммутатора.

Цель: изучить процесс обновления программного обеспечения и сохранения/восстановления конфигурации.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция с TFTP-сервером	1 шт.
Консольный кабель	1 шт.
Кабель Ethernet	1 шт.

Схема 2



2.1. Подготовка к режиму обновления и сохранения программного обеспечения коммутатора

Запустите на рабочей станции TFTP-сервер. В настройках программы выберите директорию приёма файлов:

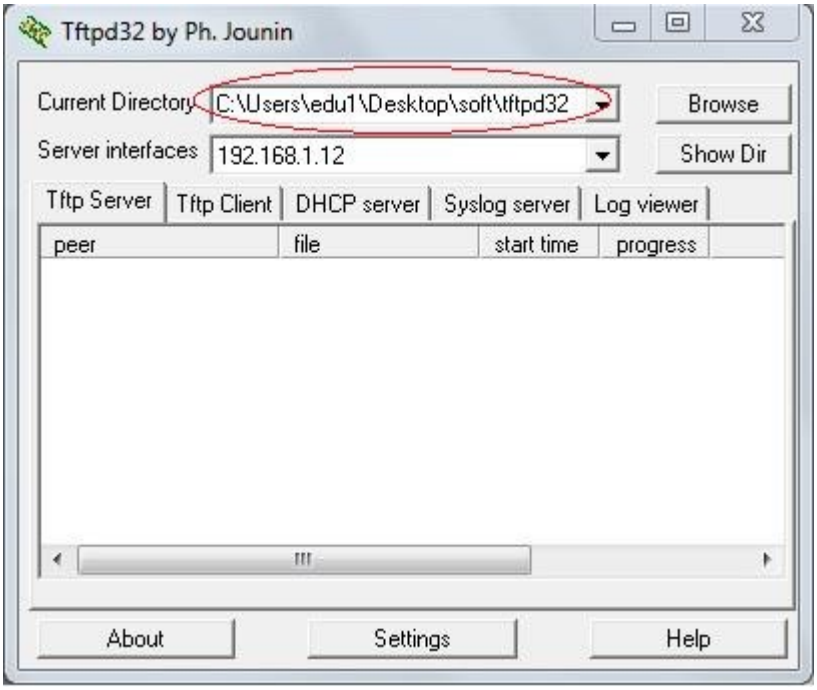


Рисунок 2.1 Выбор директории файлов

Подготовьте файл нового программного обеспечения коммутатора:
1. Найдите необходимый файл «прошивки» на сервере ftp://ftp.dlink.ru/;
2. Скачайте файл и перенесите его в директорию на TFTP-сервере;
3. Прочитайте файл сопровождения к «прошивке».

2.2. Загрузка файла программного обеспечения в память коммутатора

Все официальные версии ПО включают примечания, которые описывают новые функции и последние коррекции ошибок.

Внимание:
НЕ перезагружайте коммутатор во время обновления программного обеспечения.

Настройте IP-адрес интерфейса управления:

```
config ipif System ipaddress 192.168.1.10/24
```

Настройте TFTP-сервер:

```
Запустить TFTP-сервер, в настройках TFTP-сервера указать IP-адрес
рабочей станции 192.168.1.12/24, указать директорию с прошивкой
Current Directory.
```

Проверьте доступность TFTP-сервера с коммутатора:

```
ping 192.168.1.12
```

Проверьте информацию о текущем программном обеспечении коммутатора:

```
dir
```
Загрузите программное обеспечение на коммутатор (команда вводится в одну строку):
```
download firmware_fromTFTP 192.168.1.12 src_file DES-3200-26_28_C1_Run_v4.00.024.had dest_file DES_3200_runtime boot_up
```

Убедитесь, что программное обеспечение загружено:
```
dir
```

2.3. Настройка порядка загрузки программного обеспечения коммутатора

Задайте название файла программного обеспечения, которое будет загружаться при старте коммутатора:
```
config firmware image DES_3200_runtime boot_up
```

Сохраните изменения:
```
save
```

Обновлённая прошивка будет использована при следующей загрузке коммутатора.
Перезагрузите коммутатор:
```
reboot
```

После загрузки коммутатора проверьте информацию о программном обеспечении:
```
dir
```

Что вы наблюдаете?

_____
_____
_____
_____
_____

2.4. Выгрузка и загрузка конфигурации

Посмотрите текущую версию конфигурации коммутатора (находящуюся в RAM):
```
show config current_config
```

Проверьте информацию об имеющихся в NVRAM конфигурациях коммутатора:
```
dir
```

Выгрузите конфигурацию №1 на TFTP-сервер:
```
upload cfg_toTFTP 192.168.1.12 dest_file config.txt
```

Откройте выгруженный конфигурационный файл любым текстовым редактором, например блокнотом, и просмотрите его структуру.

Замените IP-адрес 192.168.1.**10**/24 на 192.168.1.**13**/24:
```
# IP
config ipif System ipaddress 192.168.1.10/24
disable autoconfig
```

Должно получиться так:

```
# IP
config ipif System ipaddress 192.168.1.13/24
disable autoconfig
```

Сохраните файл.

Загрузите изменённую конфигурацию на коммутатор в файл config_2:

```
download cfg_fromTFTP 192.168.1.12 src_file config.txt dest_file
config_2
```

Проверьте информацию об имеющихся в NVRAM конфигурациях коммутатора:

```
dir
```

Задайте номер конфигурации, которая будет загружаться при старте коммутатора:

```
config configuration config_2 boot_up
```

Чему будет равен IP-адрес после перезагрузки коммутатора? _____

Проверьте, изменился ли IP-адрес коммутатора:

```
show switch
```

Что вы наблюдаете?

_____

_____

2.5. Выгрузка log-файлов

Просмотрите журнал работы коммутатора:

```
show log
```

Выгрузите журнал работы на TFTP-сервер:

```
upload log_toTFTP 192.168.1.12 dest_file Logfiles.txt
```

Откройте выгруженный log-файл любым текстовым редактором, например блокнотом, и просмотрите его структуру.

ПРАКТИЧЕСКАЯ РАБОТА № 12

Команды управления таблицамикоммутации MAC- и IP-адресов, ARP-таблицы

Передача кадров коммутатором осуществляется на основе таблицы коммутации. Таблица коммутации может строиться коммутатором автоматически, на основе динамического изучения MAC-адресов источников поступающих на порты кадров, или создаваться вручную администратором сети. Коммутаторы третьего уровня также поддерживают таблицы коммутации IP-адресов, которые создаются динамически на основе изучения IP-адресов поступающих кадров.

ARP-таблица коммутатора хранит сопоставление IP- и MAC-адресов. ARP-таблица может строиться коммутатором динамически в процессе изучения ARP-запросов и ответов, передаваемых между устройствами подключёнными к его портам, или создаваться вручную администратором сети.

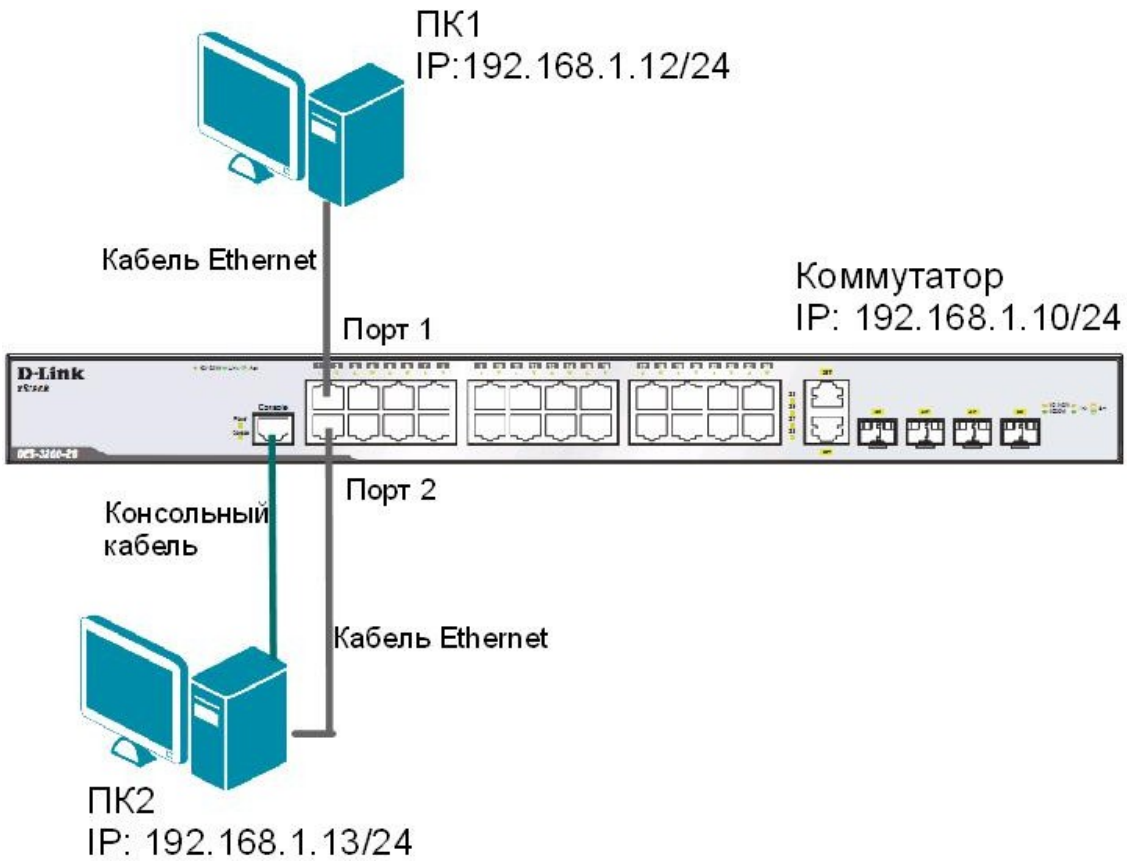
Умение работать с таблицами коммутации и ARP-таблицей позволяет диагностировать проблемы, возникающие в сети, например, атаки ARP Spoofing, а также отслеживать активность пользователей.

Цель: изучить процесс управления таблицей коммутации и ARP-таблицей.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция	2 шт.
Консольный кабель	2 шт.
Кабель Ethernet	2 шт.

Схема 3



3.1. Команды управления таблицей коммутации

Просмотрите содержимое таблицы MAC-адресов:
```
show fdb
```

Определите порт коммутатора, к которому подключено устройство с известным MAC-адресом (в качестве MAC-адреса введите реальный MAC-адрес ПК1):
```
show fdb mac_address 00-03-47-BD-3F-57
```

Посмотрите список MAC-адресов устройств, принадлежащих VLAN по умолчанию (default VLAN):
```
show fdb vlan default
```

Посмотрите MAC-адреса устройств, изученные портом 2:
```
show fdb port 2
```

Просмотрите время нахождения записи в таблице MAC-адресов:
```
show fdb aging_time
```

Измените время нахождения MAC-адреса в таблице до 350 секунд:
```
config fdb aging_time 350
```

Удалите все динамически созданные записи из таблицы MAC-адресов:
```
clear fdb all
```

Создайте статическую запись в таблице MAC-адресов (в качестве MAC-адреса введите реальный MAC-адрес ПК2) на порте 2:
```
create fdb default 00-03-47-BD-01-11 port 2
```

Просмотрите статические записи в таблице MAC-адресов:
```
show fdb static
```

Просмотрите статические записи таблицы MAC-адресов на порте 2:
```
show fdb static port 2
```

Удалите статическую запись из таблицы MAC-адресов:
```
delete fdb default 00-03-47-BD-01-11
```

Просмотрите содержимое таблицы MAC-адресов:
```
show fdb
```

3.2. Команды управления ARP-таблицей

Просмотрите ARP-таблицу:
```
show arpentry
```

Найдите в ARP-таблице сопоставления IP-MAC по указанному IP-адресу:
```
show arpentry ipaddress 192.168.1.12
```

Просмотрите в ARP-таблице все сопоставления IP-MAC на интерфейсе System:
```
show arpentry ipif System
```

Удалите все динамически созданные записи из ARP-таблицы:
```
clear arptable
```

Убедитесь, что все динамические записи из таблицы удалены:
```
show arpentry
```

Создайте статическую запись в ARP-таблице (в качестве MAC-адреса укажите MAC-адрес ПК2):
```
create arpentry 192.168.1.12 00-50-BA-00-07-36
```

Просмотрите созданную статическую запись в ARP-таблице:
```
show arpentry static
```

Удалите статическую запись из ARP-таблицы:
```
delete arpentry 192.168.1.12
```

Проверьте, что запись удалена:
```
show arpentry static
```

Измените время нахождения записи в ARP-таблице до 30 минут (по умолчанию 20 минут):
```
config arp_aging time 30
```

Проверьте выполненные настройки:
```
show arpentry
```

ПРАКТИЧЕСКАЯ РАБОТА № 13
Настройка VLAN на основе стандарта IEEE 802.1Q

Виртуальная локальная сеть (Virtual Local Area Netwrok, VLAN) представляет собой коммутируемый сегмент сети, который логически выделен по выполняемым функциям, рабочим группам или приложениям, вне зависимости от физического расположения пользователей. Виртуальные локальные сети обладают всеми свойствами физических локальных сетей, но рабочие станции можно группировать, даже если они физически расположены не в одном сегменте, т.к. любой порт любого коммутатора можно настроить на принадлежность определённой VLAN. При этом одноадресный, многоадресный и широковещательный трафик будет передаваться только между рабочими станциями, принадлежащими одной VLAN. Каждая VLAN рассматривается как логическая сеть. Кадры, предназначенные станциям не принадлежащим данной VLAN, должны передаваться через маршрутизирующее устройство (маршрутизатор или коммутатор 3-го уровня). Таким образом, с помощью виртуальных сетей решается проблема ограничений при передаче широковещательных кадров и вызываемых ими последствий, которые существенно снижают производительность сети, вызывают широковещательные штормы.

Основные определения IEEE 802.1Q:

- *Tag* (Тег) – дополнительное поле данных длиной 4 байта, содержащее информацию о VLAN (идентификатор VLAN (12 бит), поле приоритета (3 бита), поле индикатора канонического формата (1 бит), добавляемое в кадр Ethernet;
- *Tagging* (Маркировка кадра) – процесс добавления информации (тега) о принадлежности к 802.1Q VLAN в заголовок кадра;
- *Untagging* (Удаление тега из кадра) – процесс извлечения информации 802.1Q VLAN из заголовка кадра;

- *Ingress port* (Входной порт) – порт коммутатора, на который поступают кадры, и принимается решение о принадлежности VLAN;
- *Egress port* (Выходной порт) – порт коммутатора, с которого кадры передаются на другие сетевые устройства (коммутаторы, рабочие станции) и на нем, соответственно, принимается решение о маркировке кадра.

Любой порт коммутатора может быть настроен как *tagged* (маркированный) или как *untagged* (немаркированный). Функция *untagging* позволяет работать с теми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция *tagging* позволяет настраивать VLAN между несколькими коммутаторами, поддерживающими стандарт IEEE 802.1Q, подключать сетевые устройства, понимающие IEEE 802.1Q (например, серверы с сетевыми интерфейсами с поддержкой 802.1Q), обеспечивать возможность создания сложных сетевых инфраструктур.

Цель: понять технологию VLAN и её настройку на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

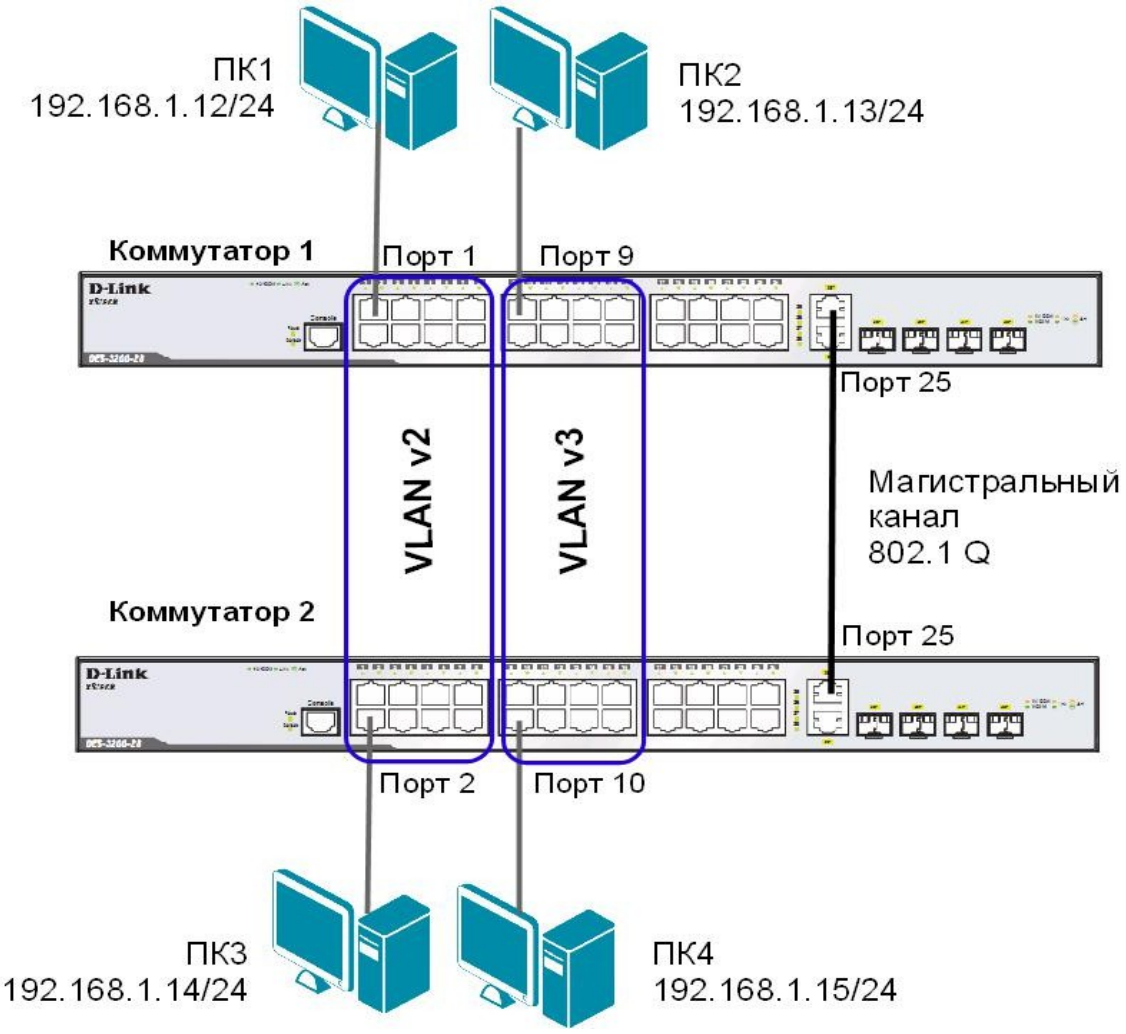
Коммутатор DES-3200-28	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.

Перед выполнением лабораторной работы необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

4.1. Настройка VLAN на основе стандарта IEEE 802.1Q

Схема 4.1



Внимание: перед созданием новой VLAN, используемые в ней порты необходимо удалить из VLAN по умолчанию, т.к. в соответствии со стандартом IEEE 802.1Q, немаркированные порты не могут одновременно принадлежать нескольким VLAN.

Проверьте и запишите доступность соединения между рабочими станциями командой ping:
`ping <IP-address>`

- от ПК1 к ПК 2, ПК 3 и ПК 4 _____
- от ПК2 к ПК 1, ПК 3 и ПК 4 _____

Настройка коммутатора 1
Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:
`config vlan default delete 1-16`

Настройте порт 25 маркированным в vlan default:
`config vlan default add tagged 25`

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порт 25 маркированным:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-8
config vlan v2 add tagged 25

create vlan v3 tag 3
config vlan v3 add untagged 9-16
config vlan v3 add tagged 25
```

Проверьте настройки VLAN:

```
show vlan
```

Повторите процедуру настройки для коммутатора 2.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК 3 _____
- от ПК2 к ПК4 _____
- от ПК1 к ПК2 и ПК4 _____
- от ПК2 к ПК1 и ПК3 _____

4.2. Настройка сегментации трафика внутри VLAN

Функция Traffic Segmentation (сегментация трафика) служит для разграничения доменов на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но имели доступ к разделяемым портам, используемым, например, для подключения серверов или магистрали сети. Функция сегментации трафика может использоваться с целью сокращения трафика внутри сетей VLAN 802.1Q, позволяя разбивать их на меньшие группы. При этом правила VLAN имеют более высокий приоритет при передаче трафика. Правила Traffic Segmentation применяются после них.

ЗАДАНИЕ

Используя функцию сегментации трафика, настроить порты 9-16 коммутатора 1, находящиеся в VLAN v3 таким образом, чтобы рабочие станции, подключённые к ним, не могли обмениваться данными между собой, но при этом могли передавать данные через магистральный канал.

Настройка коммутатора 1

Настройте сегментацию трафика:

```
config traffic_segmentation 9-16 forward_list 25
```

Проверьте выполненные настройки:

```
show traffic_segmentation
```

Подключите ПК1 к порту 9 коммутатора 1.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК 2 _____
- от ПК1 к ПК4 _____

Что наблюдаете? Запишите.

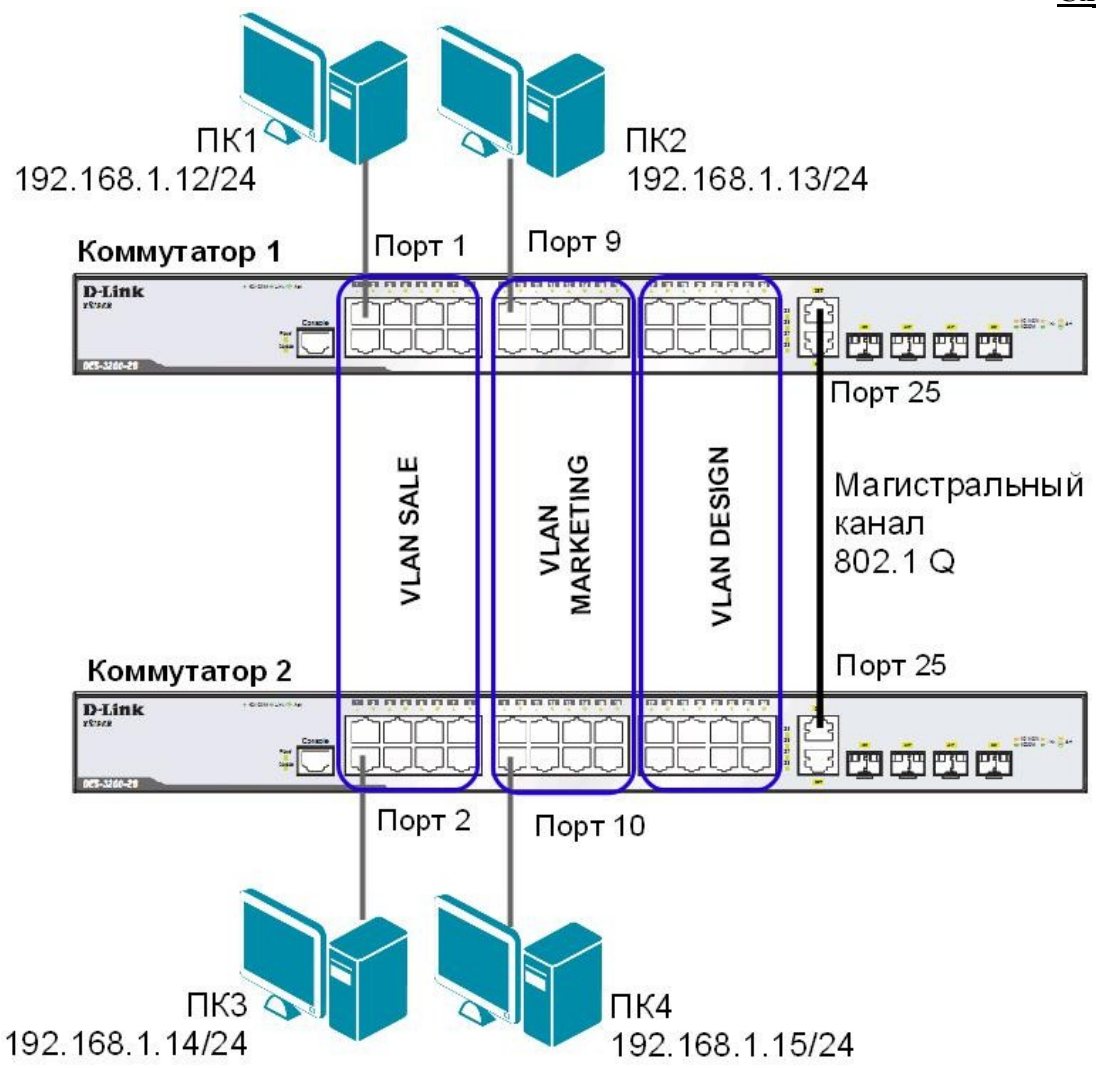
_____

_____

_____

4.3. Оптимизация настройки коммутаторов с большим количеством VLAN

Схема 4.2



Перед выполнением данной части лабораторной работы необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора 1

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

Создайте девять VLAN с тегами 2-10:

```
create vlan vlanid 2-10
```

Примечание: при создании VLAN без указания имени, имена присваиваются автоматически по шаблону (VLAN x, где x – тег создаваемой VLAN).

Измените имена в созданных VLAN и добавьте в них немаркированные порты:

```
config vlan vlanid 7 add untagged 1-8 name SALE
config vlan vlanid 8 add untagged 9-16 name MARKETING
config vlan vlanid 9 add untagged 17-24 name DESIGN
```

Добавьте маркированные порты сразу в несколько VLAN:

```
config vlan vlanid 2-10 add tagged 25-26
```

Проверьте настройки VLAN:

```
show vlan
```

Удалите порты из нескольких VLAN:

```
config vlan vlanid 2-10 delete 25-26
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте магистральный порт VLAN для передачи маркированных кадров с любыми VID:

```
config vlan_trunk ports 25 state enable
```

Активизируйте функционирование магистрального канала (выполнение коммутатором этой команды занимает некоторое время):

```
enable vlan_trunk
```

Проверьте выполненные настройки:

```
show vlan_trunk
```

Повторите процедуру настройки для коммутатора 2.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК 3 _____
- от ПК2 к ПК4 _____
- от ПК1 к ПК2 и ПК4 _____
- от ПК2 к ПК1 и ПК3 _____

Подключите ПК2 к порту 7 коммутатора 1, а ПК4 к порту 8 коммутатора 2.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК2 и ПК4 _____
- от ПК2 к ПК1 и ПК3 _____

Отключите магистральные каналы на обоих коммутаторах:

```
disable vlan_trunk
```

ПРАКТИЧЕСКАЯ РАБОТА № 14
Настройка протокола GVRP

Существуют два основных способа, позволяющих устанавливать членство в VLAN:

□ статические VLAN;

□ динамические VLAN.

В статических VLAN установление членства осуществляется вручную администратором сети. При изменении топологии сети или перемещении пользователя на другое рабочее место, администратору требуется вручную выполнять привязку порта к VLAN для каждого нового соединения.

Членство в динамических VLAN может устанавливаться динамически на основе протокола GVRP (GARP VLAN Registration Protocol). Протокол GVRP определяет способ, посредством которого коммутаторы обмениваются информацией о сети VLAN, чтобы автоматически зарегистрировать членов VLAN на портах во всей сети. Он позволяет динамически создавать и удалять VLAN стандарта IEEE 802.1Q на магистральных портах, автоматически регистрировать и исключать атрибуты VLAN (под регистрацией VLAN подразумевается включение порта в VLAN, под исключением – удаление порта из VLAN).

Протокол GVRP использует сообщения GVRP BPDU (GVRP Bridge Protocol Data Units), рассылаемые на многоадресный MAC-адрес 01-80-C2-00-00-21 для оповещения устройств-подписчиков о различных событиях.

Порт с поддержкой протокола GVRP подключается к сети VLAN только в том случае, если он непосредственно получает оповещение о ней. Если порт с поддержкой протокола GVPR передает оповещение, полученное от другого порта коммутатора, он не подключается к этой сети VLAN.

Главная цель протокола GVRP – позволить коммутаторам автоматически обнаруживать информацию о VLAN, которая иначе должна была бы быть вручную сконфигурирована на каждом коммутаторе. Наиболее рационально использовать протокол GVRP на магистральных коммутаторах для динамической передачи информации о статических VLAN на уровень доступа.

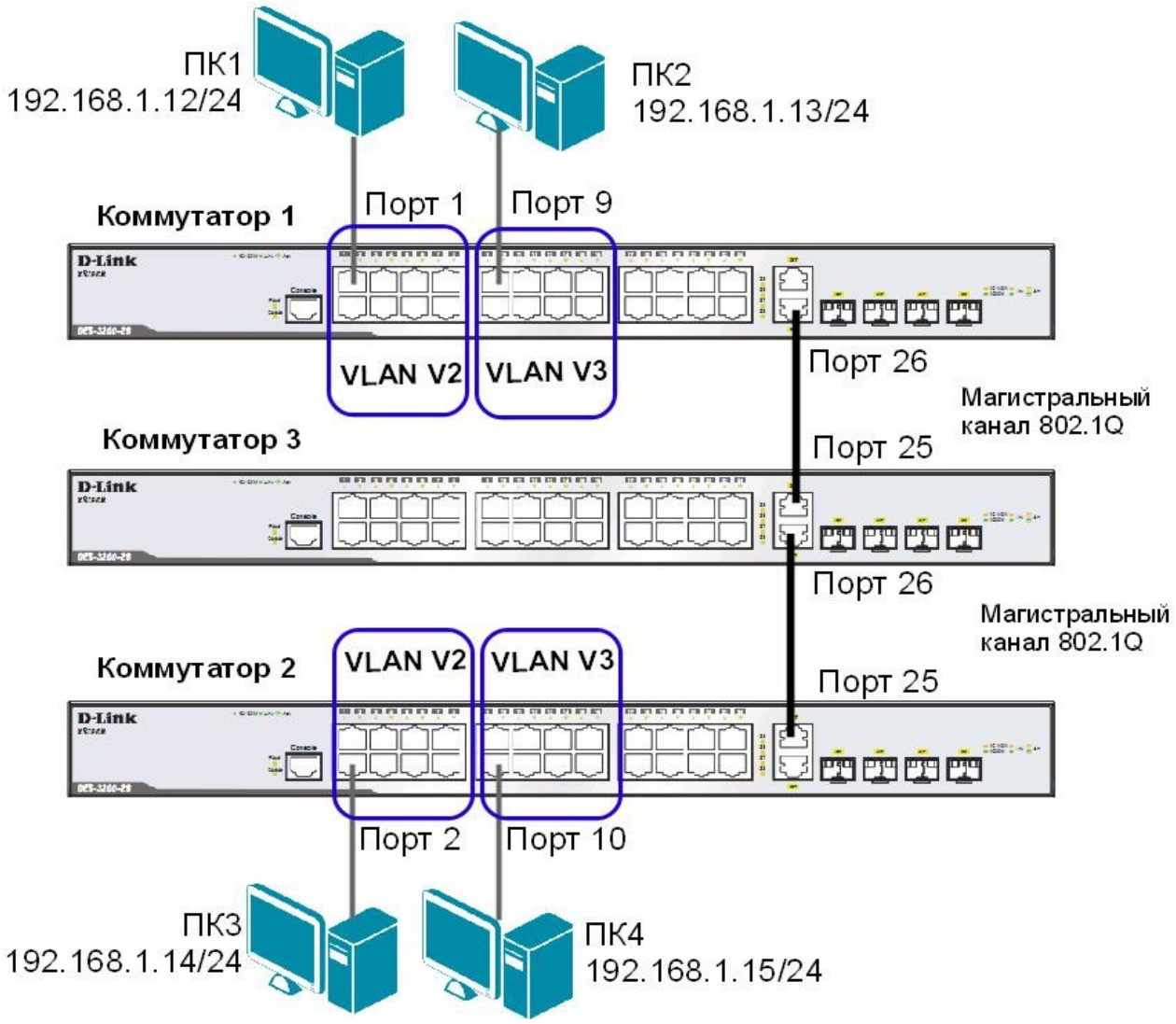
Примечание: при динамической передаче информации о VLAN через магистральные коммутаторы, рекомендуется передавать информацию только о пользовательских VLAN, а служебные VLAN и управляющие VLAN настраивать на магистральных коммутаторах статически.

Цель: изучить процесс динамического продвижения информации о VLAN в сети.

Оборудование (на 3 рабочих места):

Коммутатор DES-3200-28	3 шт.
Рабочая станция	4 шт.
Консольный кабель	3 шт.
Кабель Ethernet	6 шт.

Схема 5



Перед выполнением лабораторной работы необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора 1

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порты 25-26 маркированным:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-8
config vlan v2 add tagged 25-26

create vlan v3 tag 3
config vlan v3 add untagged 9-16
config vlan v3 add tagged 25-26
```

Проверьте настройки VLAN:
```
show vlan
```

Настройте объявление о VLAN v2 и v3:
```
config vlan v2 advertisement enable
config vlan v3 advertisement enable
```

Включите работу протокола GVRP:
```
enable gvrp
```

Установите возможность приёма и отправки информации о VLAN через порты 25-26 коммутатора:
```
config port_vlan 25-26 gvrp_state enable
```

Повторите процедуру настройки для коммутатора 2.

Настройка коммутатора 3
Включите работу протокола GVRP:
```
enable gvrp
```

Установите возможность приема и отправки информации о VLAN через все порты коммутатора:
```
config port_vlan all gvrp_state enable
```

Проверьте настройки VLAN на коммутаторе 3:
```
show vlan
```

Проверьте состояние GVRP на портах коммутаторов 1, 2, 3:
```
show port_vlan
```

Запишите ваши наблюдения:

_____
_____
_____
_____

Проверьте доступность соединения между рабочими станциями командой ping:
```
ping <IP-address>
```

- от ПК1 к ПК 3 _____
- от ПК2 к ПК4 _____

ПРАКТИЧЕСКАЯ РАБОТА № 15

Настройка сегментации трафика без использования VLAN

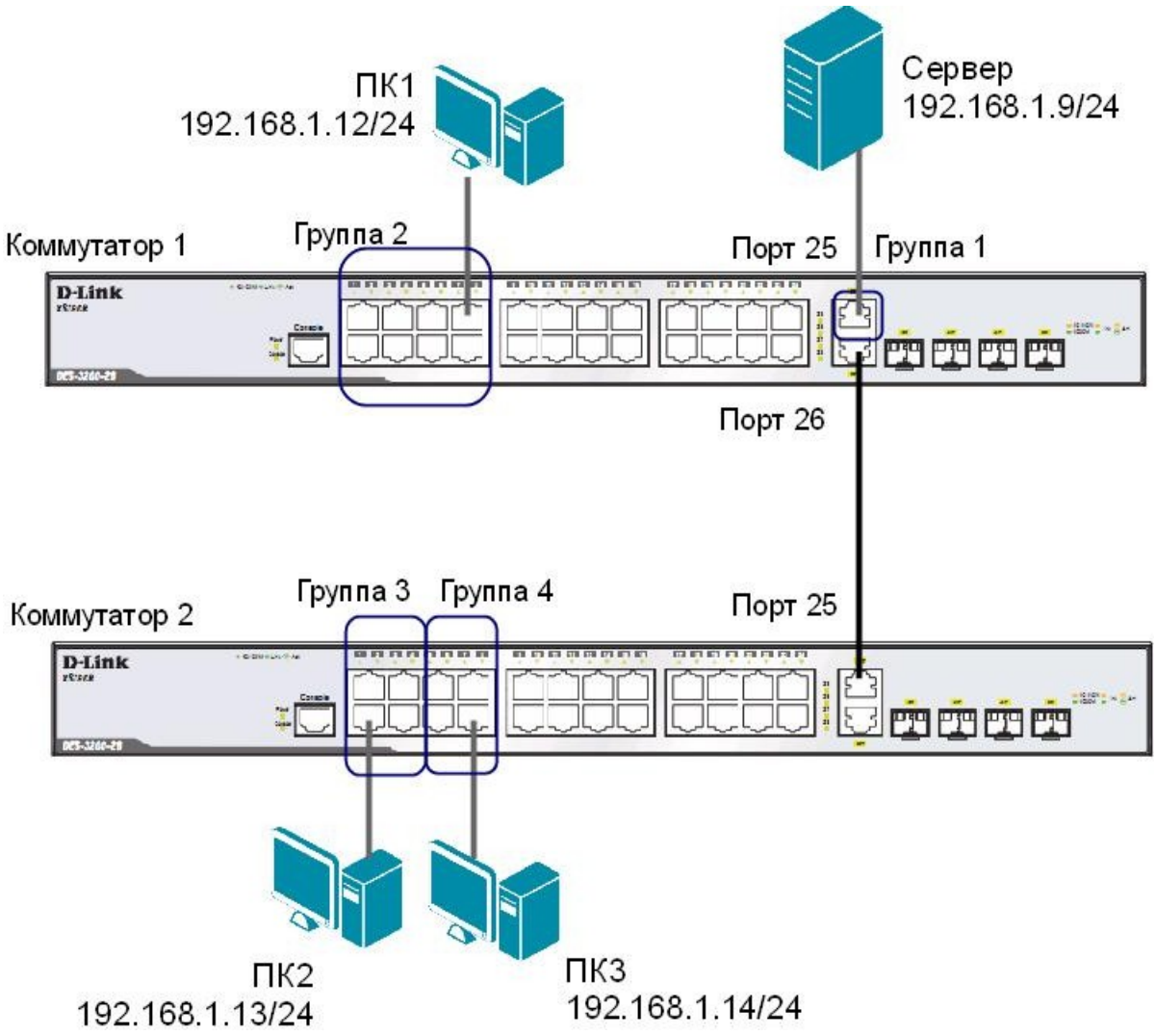
Функция Traffic Segmentation (сегментация трафика) служит для разграничения доменов на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения серверов или магистрали сети.

Цель: научиться выполнять сегментацию трафика на канальном уровне без использования технологии VLAN.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.

Схема 6



ЗАДАНИЕ

Используя функцию сегментации трафика, настройте коммутаторы таким образом, чтобы рабочие станции из разных групп получили доступ к совместно используемому серверу. При этом обмен данными между устройствами разных групп запрещён.

Сбросьте настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройте сегментацию трафика на коммутаторе 1:

```
config traffic_segmentation 1-8 forward_list 1-8,25
config traffic_segmentation 26 forward_list 25
config traffic_segmentation 25 forward_list 1-26
```

Настройте сегментацию трафика на коммутаторе 2:

```
config traffic_segmentation 1-4 forward_list 1-4,25
config traffic_segmentation 5-8 forward_list 5-8,25
config traffic_segmentation 25 forward_list 1-26
```

Проверьте настройки на обоих коммутаторах:

```
show traffic_segmentation
```

Проверьте доступность соединения между устройствами командой ping:

```
ping <IP-address>
```

- от ПК1 (Группа 2) к серверу (Группа 1) _____
- от ПК2 (Группа 3) к серверу (Группа 1) _____
- от ПК3 (Группа 4) к серверу (Группа 1) _____
- от ПК1 (Группа 2) к ПК2 (Группа 3) _____
- от ПК2 (Группа 3) к ПК3 (Группа 4) _____
- от ПК3 (Группа 4) к ПК1 (Группа 2) _____

ПРАКТИЧЕСКАЯ РАБОТА № 17

Самостоятельная работа по созданиюЛВС на основе стандарта IEEE 802.1Q

Цель: самостоятельно создать и настроить сеть на основе стандарта IEEE 802.1Q.

Оборудование (на 10 рабочих мест):

Коммутатор DES-3200-28	8 шт.
Коммутатор DES-3810-28	2 шт.
Рабочая станция	10 шт.
Консольный кабель	10 шт.
Кабель Ethernet	20 шт.

Перед выполнением данной лабораторной работы необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

ЗАДАНИЕ 1

Подключите устройства как показано на общей схеме сети 7. Задайте на всех ПК IP-адреса из подсети 192.168.1.0/24, в соответствии со схемой.

Проверьте соединение между рабочими станциями командой ping.

```
ping <IP-address>
```

В какой VLAN находятся ПК? Должна ли быть связь между всеми ПК и почему?

_____

_____

_____

Проверьте на каждом коммутаторе состояние таблицы коммутации:

```
show fdb
```

Проверьте таблицу ARP каждого компьютера:

```
arp -a
```

Сколько записей вы наблюдаете в этих таблицах? Есть ли в них одинаковые MAC-адреса?

_____

_____

_____

Если соединение до каких-либо ПК недоступно, необходимо выяснить причины и устранить их. Перейти к заданию 2 можно только после выявления и устранения причин отсутствия связи между ПК.

ЗАДАНИЕ 2

Создайте на каждом коммутаторе необходимые для работы сети VLAN.

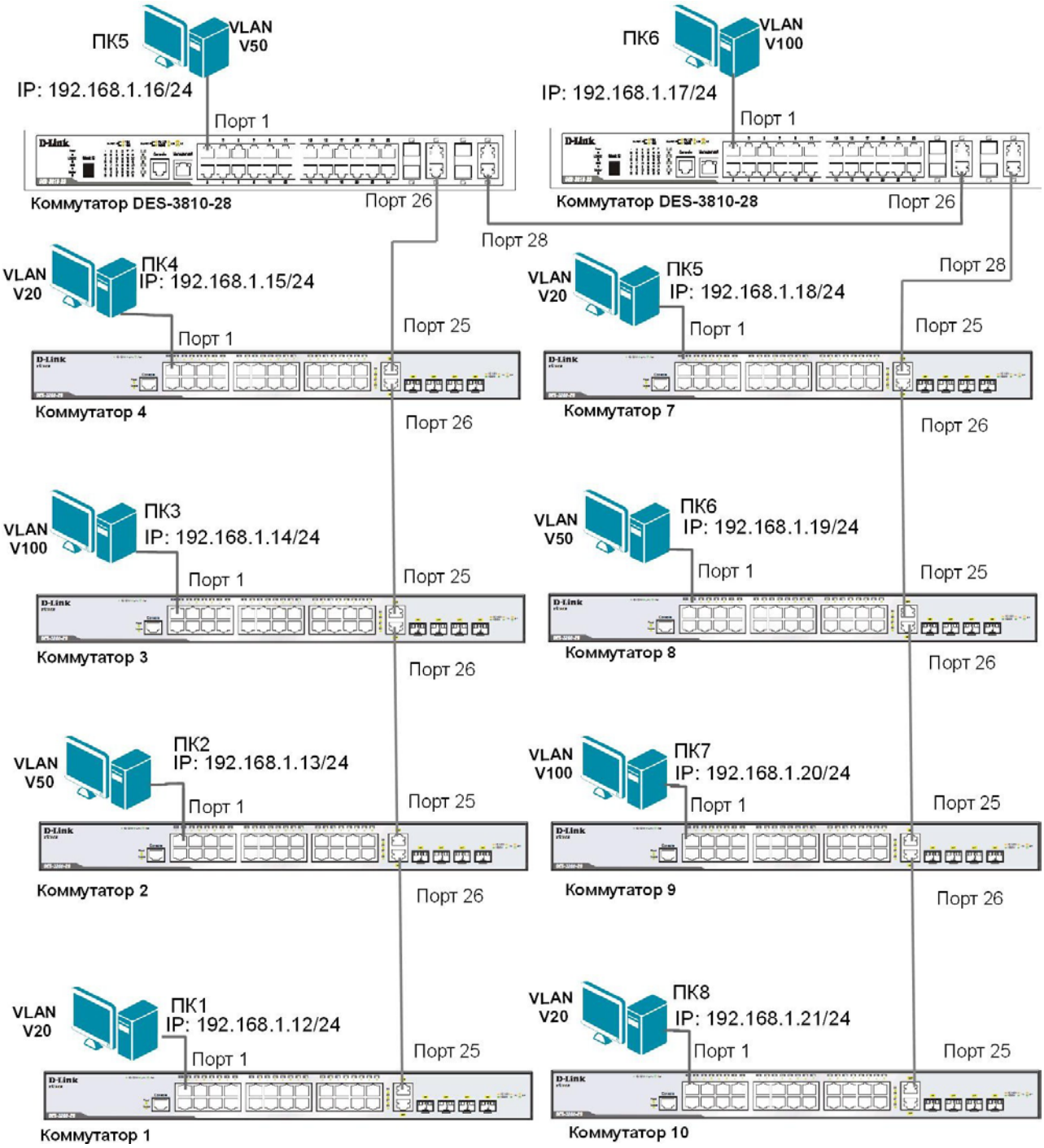
Какие VLAN необходимо создать на каждом коммутаторе?

_____

_____

_____

Схема 7 (общая схема сети)



Настройте магистральные порты коммутаторов как маркированные, а пользовательские порты как немаркированные, в соответствии со схемой 7.

Проверьте связь между всеми ПК командой ping.

Какие ПК доступны с вашего рабочего места, а какие нет? Почему?

_____

_____

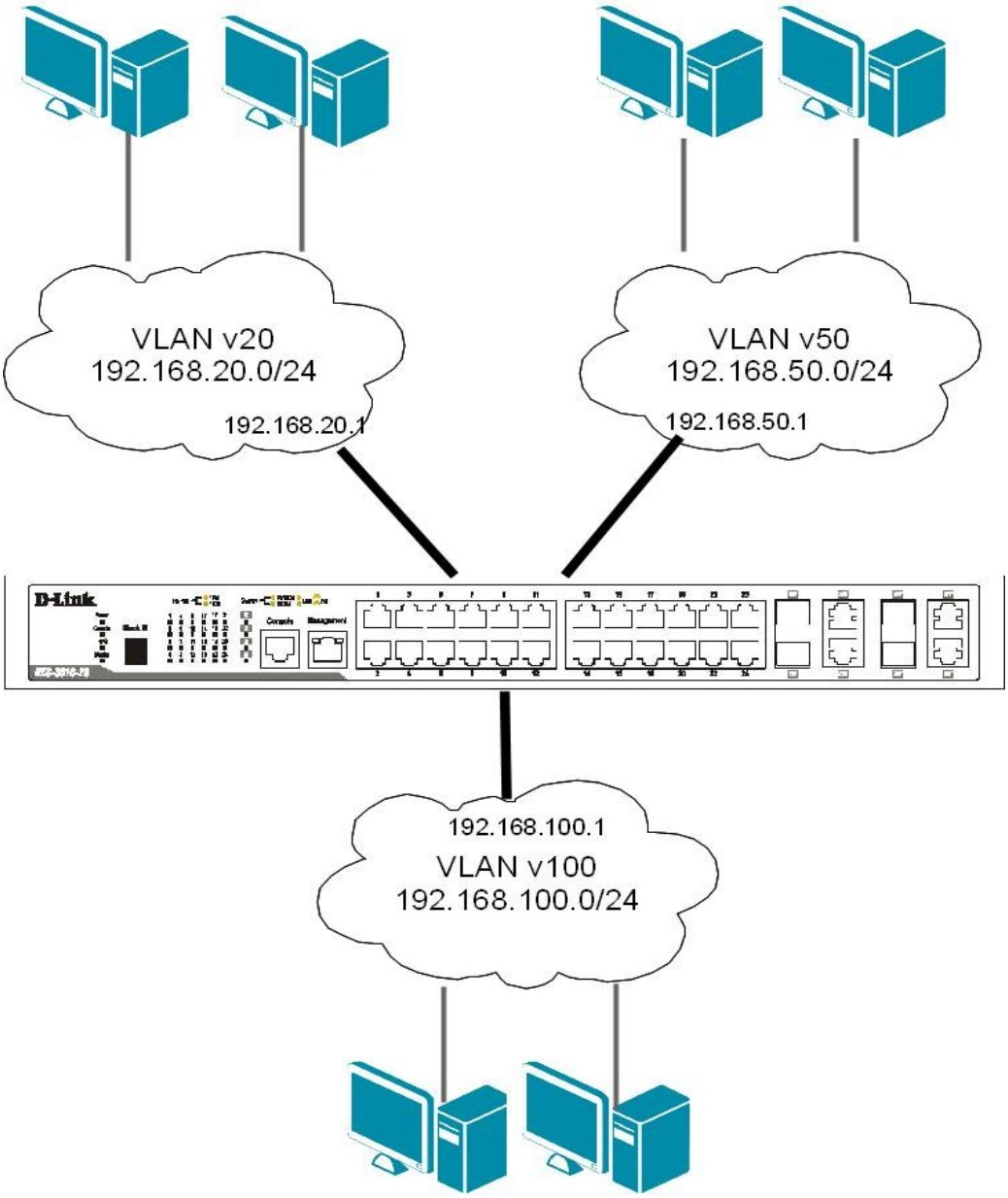
_____

ЗАДАНИЕ 3

На коммутаторе DES-3810-28 (только на одном!) необходимо настроить маршрутизацию для объединения разных VLAN в общую сеть. Логическая схема сети с маршрутизацией показана на схеме 7.1.

Примечание: в пределах одного коммутатора 3-го уровня маршрутизация между VLAN включается автоматически при настройке IP-интерфейсов.

Схема 7.1



Перед настройкой маршрутизации на коммутаторе DES-3810-28 уже должны быть созданы необходимые VLAN v20, v50, v100.

Введите на коммутаторе DES-3810-28 следующие команды, чтобы создать IP-интерфейс для каждой VLAN:

```
create ipif IPIF20 192.168.20.1/24 v20 state enable
create ipif IPIF50 192.168.50.1/24 v50 state enable
create ipif IPIF100 192.168.100.1/24 v100 state enable
```

Примечание: в этом примере IPIF20, IPIF50, IPIF100 – имена создаваемых IP-интерфейсов, а v20, v50, v100 – имена ранее созданных на этом коммутаторе VLAN (если имена VLAN другие, необходимо отредактировать вводимые команды).

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
show iproute
```

Задайте на всех ПК, принадлежащих к одной VLAN, IP-адреса из той IP-сети, которая назначена данной VLAN (значения IP-адресов рабочих станций выберите самостоятельно). В качестве шлюза по умолчанию (default gateway) укажите адрес IP-интерфейса маршрутизирующего коммутатора соответствующей VLAN. Командой ping проверьте связь между всеми ПК.

В какой VLAN находятся ПК? Должна ли быть связь между всеми ПК и почему?

_____
_____
_____

Проверьте на каждом коммутаторе состояние таблицы коммутации:

```
show fdb
```

Проверьте таблицу ARP каждого компьютера:

```
arp -a
```

Сколько записей вы наблюдаете в этих таблицах? Одинаковое ли количество записей в этих таблицах? Есть ли одинаковые MAC-адреса в них? Сравните с полученными результатами в задании 1.

_____
_____
_____
_____
_____

ПРАКТИЧЕСКАЯ РАБОТА № 18

Настройка протоколов связующего дерева STP, RSTP, MSTP

Протокол Spanning Tree Protocol (STP).

Протокол связующего дерева Spanning Tree Protocol (STP) является протоколом 2 уровня модели OSI, который позволяет строить древовидные, свободные от петель, конфигурации связей между коммутаторами локальной сети. Конфигурация связующего дерева строится коммутаторами автоматически с использованием обмена служебными пакетами, называемыми Bridge Protocol Data Units (BPDU).

Для построения устойчивой активной топологии с помощью протокола STP необходимо с каждым коммутатором сети ассоциировать уникальный идентификатор моста (Bridge ID), с каждым портом коммутатора ассоциировать стоимость пути (Path Cost) и идентификатор порта (Port ID).

Процесс вычисления связующего дерева начинается с выбора корневого моста (Root Bridge), от которого будет строиться дерево. Второй этап работы STP – выбор корневых портов (Root Port). Третий шаг работы STP – определение назначенных портов (Designated Port).

В процессе построения топологии сети каждый порт коммутатора проходит несколько стадий: Blocking (Блокировка), Listening (Прослушивание), Learning (Обучение), Forwarding (Продвижение), Disable (Отключен).

Протокол Rapid Spanning Tree Protocol (RSTP).

Протокол Rapid Spanning Tree Protocol (RSTP) является развитием протокола STP. Основные понятия и терминология протоколов STP и RSTP одинаковы. Существенным их отличием является способ перехода портов в состояние продвижения и то, каким образом этот переход влияет на роль порта в топологии. RSTP объединяет состояния Disabled, Blocking и Listening, используемые в STP, и создает единственное состояние Discarding («Отбрасывание»), при котором порт не активен. Выбор активной топологии завершается присвоением протоколом RSTP определённой роли каждому порту: корневой порт (Root Port), назначенный порт (Designated Port), альтернативный порт (Alternate Port), резервный порт (Backup Port).

Протокол RSTP предоставляет механизм предложений и соглашений, который обеспечивает быстрый переход корневых и назначенных портов в состояние Forwarding, а альтернативных и резервных портов в состояние Discarding. Для этого протокол RSTP вводит два новых понятия: граничный порт и тип соединения. *Граничным портом* (Edge Port) объявляется порт, непосредственно подключённый к сегменту сети, в котором не могут быть созданы петли. Граничный порт мгновенно переходит в состояние продвижения, минуя состояния прослушивания и обучения. Назначенный порт может выполнять быстрый переход в состояние продвижения в соединениях типа «точка — точка» (*Point-to-Point, P2P*), т.е. если он подключён только к одному коммутатору.

Администратор сети может вручную включать или выключать статусы Edge и P2P либо устанавливать их работу в автоматическом режиме, выполнив соответствующие настройки порта коммутатора.

Таблица 2 **Стоимость пути в соответствии с протоколом RSTP**

Скорость канала	Рекомендованное значение
<=100 Кбит/с	200 000 000
1 Мбит/с	20 000 000
10 Мбит/с	2 000 000
100 Мбит/с	200 000
1 Гбит/с	20 000
10 Гбит/с	2 000

* Коммутаторы, поддерживающие только стандарт STP должны использовать значения в соответствии со стандартом IEEE 802.1D-1998.

Протокол Multiple Spanning Tree Protocol (MSTP).

Протокол Multiple Spanning Tree Protocol (MSTP) является расширением протокола RSTP, который позволяет настраивать отдельное связующее дерево для любой VLAN или группы VLAN, создавая множество маршрутов передачи трафика и позволяя осуществлять балансировку нагрузки.

Протокол MSTP делит коммутируемую сеть на **регионы MST** (*Multiple Spanning Tree (MST) Region*), каждый из которых может содержать множество **копий связующих деревьев** (*Multiple Spanning Tree Instance, MSTI*) с независимой друг от друга топологией.

Для того чтобы два и более коммутатора принадлежали одному региону MST, они должны обладать одинаковой конфигурацией MST, которая включает: номер ревизии MSTP (*MSTP revision level number*), имя региона (*Region name*), карту привязки VLAN к копии связующего дерева (*VLAN-to-instance mapping*).

Внутри коммутируемой сети может быть создано множество MST-регионов.

Протокол MSTP определяет следующие типы связующих деревьев:

□ **Internal Spanning Tree (IST)** — специальная копия связующего дерева, которая по умолчанию существует в каждом MST-регионе. IST присвоен номер 0 (Instance 0). Она может отправлять и получать кадры BPDU и служит для управления топологией внутри региона. Все VLAN, настроенные на коммутаторах данного MST-региона, по умолчанию привязаны к IST;

□ **Common Spanning Tree (CST)** — единое связующее дерево, вычисленное с использованием протоколов STP, RSTP, MSTP и объединяющее все регионы MST и мосты SST;

□ **Common and Internal Spanning Tree (CIST)** — единое связующее дерево, объединяющее CST и IST каждого MST-региона;

□ **Single Spanning Tree (SST) Bridge** — это мост, поддерживающий только единственное связующее дерево, CST. Это единственное связующее дерево может поддерживать протокол STP или протокол RSTP.

Вычисления в MSTP

Процесс вычисления MSTP начинается с выбора **корневого моста CIST** (*CIST Root*) сети. В качестве CIST Root будет выбран коммутатор, обладающий наименьшим значением идентификатора моста среди всех коммутаторов сети.

Далее в каждом регионе выбирается **региональный корневой мост CIST** (*CIST Region Root*). Им становится коммутатор, обладающий наименьшей внешней стоимостью пути к корню CIST среди всех коммутаторов, принадлежащих данному региону.

При наличии в регионе отдельных связующих деревьев MSTI для каждой MSTI, независимо от остальных, выбирается **региональный корневой мост MSTI** (*MSTI Regional Root*). Им становится коммутатор, обладающий наименьшим значением идентификатора моста среди всех коммутаторов данной MSTI этого MST-региона.

При вычислении активной топологии CIST и MSTI используется тот же фундаментальный алгоритм, который описан в стандарте IEEE 802.1D-2004.

Роли портов

Протокол MSTP определяет роли портов, которые участвуют в процессе вычисления активной топологии CIST и MSTI аналогичные протоколам STP и RSTP. Дополнительно в MSTI используется ещё роль — мастер-порт (*Master Port*).

Счётчик переходов MSTP

При вычислении активной топологии связующего дерева IST и MSTI используется механизм счётчика переходов (Hop count), определяющий максимальное число переходов между устройствами внутри региона, прежде чем кадр BPDU будет отброшен. Значение счётчика переходов устанавливается региональным корневым мостом MSTI или CIST и уменьшается на 1 каждым портом коммутатора, получившим кадр BPDU. После того как значение счётчика станет равным 0, кадр BPDU будет отброшен и информация, хранимая портом, будет помечена как устаревшая.

Пользователь может установить значение счётчика переходов от 1 до 20. Значение по умолчанию — 20.

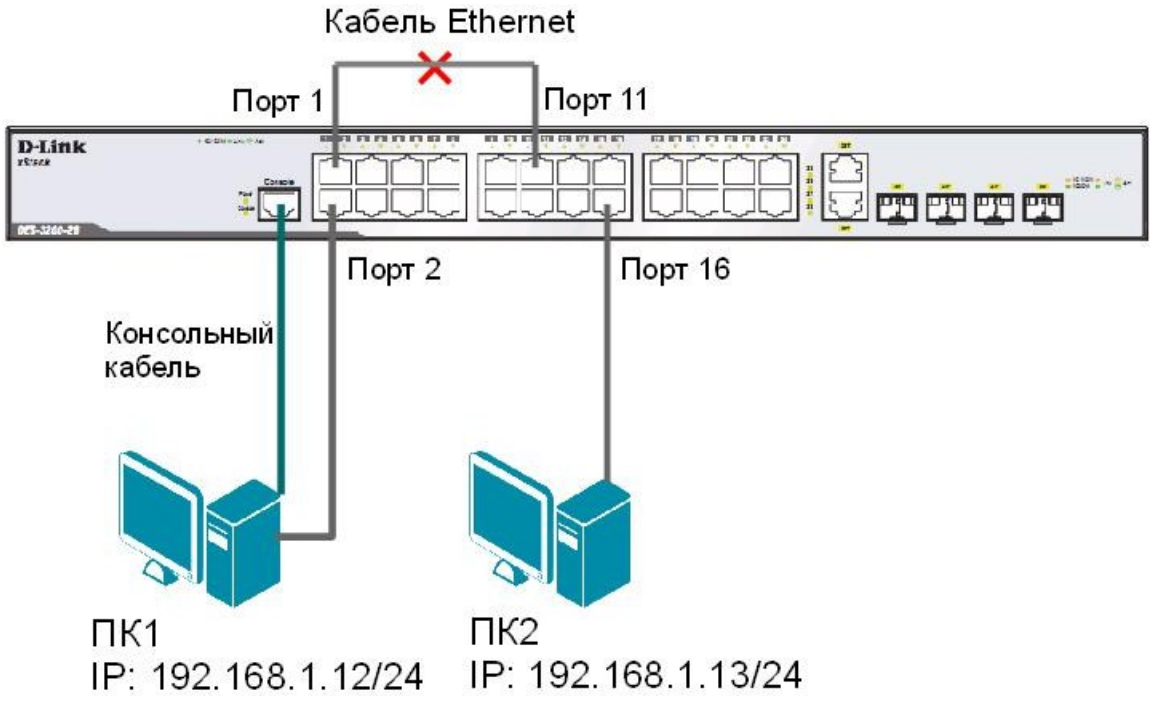
Цель: понять функционирование протоколов связующего дерева и изучить их настройку на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	8 шт.

8.1. Мониторинг и диагностика сети во время широковещательного шторма, вызванного наличием петли

Схема 8.1



Перед выполнением практического задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Просмотрите статистику о пакетах, передаваемых через порт 1:

```
show packet ports 1
```

Соберите схему и соедините кабелем Ethernet порты 1 и 11 коммутатора.

Выполните на рабочей станции ПК2 команду ping, и не останавливайте её до окончания выполнения задания 8.1:

```
ping 192.168.1.1 -t
```

Повторно просмотрите статистику о пакетах, передаваемых через порт 1:

```
show packet ports 1
```

Что вы наблюдаете? Возник широковещательный шторм? Почему?

_____

_____

_____

Что происходит при работе ping с не используемым в схеме IP-адресом?

_____

_____

Посмотрите загрузку ЦПУ коммутатора (CPU):

```
show utilization cpu
```

Просмотрите загрузку портов коммутатора:

```
show utilization ports
```

Какая загрузка портов, используемых в схеме?

Порт 1 (%) _____

Порт 2 (%) _____

Порт 11 (%) _____

Порт 16 (%) _____

Просмотрите загрузку ЦПУ на ПК1 и ПК2.

Выполните на рабочей станции ПК 1 команду:

```
ping 192.168.1.13
```

Что вы наблюдаете? Объясните почему.

_____

Отсоединив кабель от портов 1 и 11, удалите петлю.

Поместите порты 2 и 16 в новую VLAN:

```
config vlan default delete 2,16

create vlan v2 tag 2
config vlan v2 add untagged 2,16
```

Проверьте настройки VLAN:
```
show vlan
```

Просмотрите статистику о пакетах, передаваемых через порт 1:
```
show packet ports 1
```

Соедините кабелем порты 1 и 11 для повторного создания петли.

Просмотрите загрузку портов:
```
show utilization ports
```

Просмотрите загрузку ЦПУ на ПК1 и ПК2.

Что вы наблюдаете? Почему нет широковещательного шторма на портах 2 и 16?

_____
_____

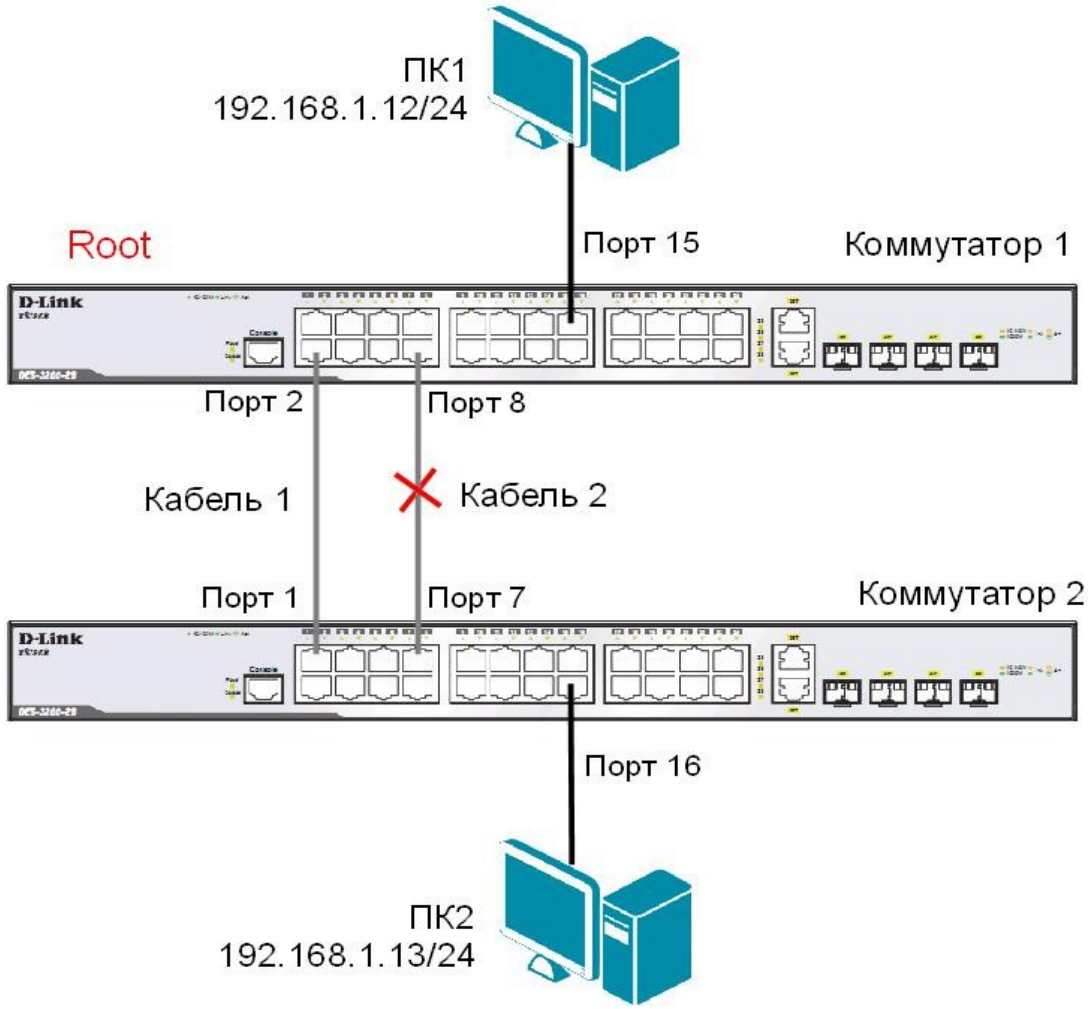
Выполните на рабочей станции ПК 1 команду:
```
ping 192.168.1.13
```

Что вы наблюдаете? Объясните почему.

_____
_____

8.2. Настройка протокола RSTP

Схема 8.2



Примечание: не соединяйте коммутаторы одновременно двумя кабелями во время настройки до особого указания.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора 1

Включите протокол связующего дерева на коммутаторе:

```
enable stp
```

Проверьте текущую конфигурацию протокола связующего дерева:

```
show stp
```

Протокол RSTP используется по умолчанию.
Если нет, активизируйте его:

```
config stp version rstp
```

Установите на коммутаторе меньшее значение приоритета, чтобы он был выбран корневым мостом:

```
config stp priority 8192 instance_id 0
```

Просмотрите выполненные изменения:
`show stp instance 0`

Назначьте порты 1-24 граничными портами:
`config stp ports 1-24 edge true`

Активизируйте протокол связующего дерева на портах:
`config stp ports 1-24 state enable`

Настройка коммутатора 2
Активизируйте функцию связующего дерева:
`enable stp`

Проверьте текущую конфигурацию протокола связующего дерева:
`show stp`

Протокол RSTP используется по умолчанию.
Если нет, включите его:
`config stp version rstp`

Назначьте порты 1-24 граничными портами:
`config stp ports 1-24 edge true`

Активизируйте протокол связующего дерева на портах:
`config stp ports 1-24 state enable`

Соедините между собой коммутаторы 1 и 2 с помощью двух кабелей, как показано на схеме 8.2.

Проверьте настройки RSTP, состояние портов и их роли у обоих коммутаторов:
`show stp ports x, где x- номер порта`

Какой коммутатор является корневым? _____

Какие порты являются заблокированными? _____

Какая роль у заблокированных портов? _____
_____

Выполните от компьютера ПК1 до ПК2, и наоборот, команду ping, и не останавливайте её до окончания выполнения задания 8.2:
`На ПК1: ping 192.168.1.13 -t`
`На ПК2: ping 192.168.1.12 -t`

Отсоедините кабель от корневого порта.

Что происходит с тестом ping? _____

Превышен ли интервал ожидания для запроса?_____

Как долго пришлось ждать до появления ответа?_____

Проверьте состояние заблокированного порта, какая теперь у него роль?

_____

Подключите обратно кабель.

Поменяйте версию протокола связующего дерева с RSTP на STP на обоих коммутаторах командой:

```
config stp version stp
```

Отсоедините кабель от корневого порта.

Что происходит с тестом ping? _____

Превышен ли интервал ожидания для запроса?_____

Как долго пришлось ждать до появления ответа? _____

8.3. Настройка защиты от несанкционированного подключения корневых коммутаторов

ЗАДАНИЕ

Настройте на коммутаторе 1 защиту от несанкционированного подключения корневых коммутаторов.

Отключите кабели, соединяющие коммутаторы.

Настройка коммутатора 1

Включите на портах 1-8 защиту от перевыборов корневого коммутатора, активизировав параметр restricted_role:

```
config stp ports 1-8 restricted_role true
```

Настройка коммутатора 2

Измените значение приоритета коммутатора 2, так чтобы оно стало ниже значения приоритета коммутатора 1:

```
config stp priority 4096 instance_id 0
```

Соедините порты обоих коммутаторов кабелем 1, как показано на схеме 8.2.

На коммутаторе 1 посмотрите log-файл.

```
show log
```

Что вы наблюдаете? Запишите.

_____

_____

Какой коммутатор является корневым?_____

Какая роль у порта 2 коммутатора 1?_____

На коммутаторе 1 переключите кабель из порта 2 в порт 9.

На коммутаторе 1 посмотрите log-файл.
```
show log
```

Что вы наблюдаете? Запишите.

_____

_____

Какой коммутатор является корневым?_____

Какая роль у порта 9 коммутатора 1? _____

8.4. Настройка защиты от получения ложных кадров об изменении топологии

ЗАДАНИЕ

Настройте на коммутаторе 1 защиту от получения ложных кадров об изменении топологии (TCN BPDU).

Отключите кабели, соединяющие коммутаторы.

Настройка коммутатора 1

Включите на портах 1-8 коммутатора функцию защиты от получения ложных TCN BPDU:
```
config stp ports 1-8 restricted_tcn true
```

Настройка коммутатора 2

Настройте на коммутаторе приоритет по умолчанию:
```
config stp priority 32768 instance_id 0
```

Проверьте выполненные настройки:
```
show stp instance 0
```

Соедините между собой коммутаторы 1 и 2 с помощью двух кабелей, как показано на схеме 8.2.

Соедините порт 10 и порт 12 коммутатора кабелем Ethernet.

На коммутаторе 1 посмотрите log-файл.
```
show log
```

Что вы наблюдаете? Запишите.

_____

_____

На коммутаторе 2 посмотрите log-файл.
```
show log
```

Что вы наблюдаете? Запишите.

_____

_____

Отключите на коммутаторе 1 функцию защиты от получения ложных TCN BPDU:
```
config stp ports 1-8 restricted_tcn false
```

Отключите кабель, соединяющий порты 10 и 12 коммутатора 2.

На коммутаторе 1 посмотрите log-файл.

```
show log
```

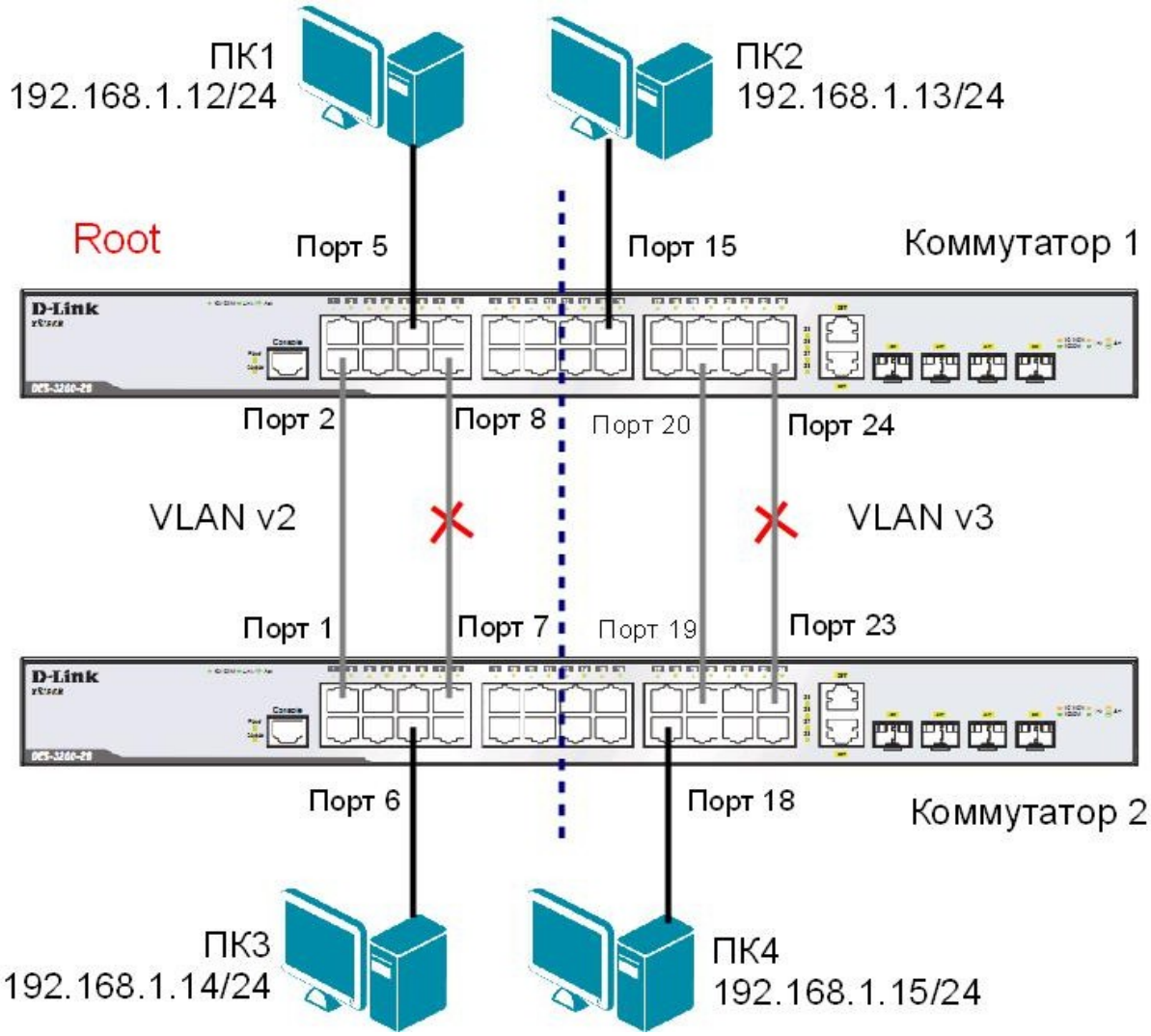
Что вы наблюдаете? Запишите.

_____

_____

8.5. Настройка протокола MSTP

Схема 8.3



Примечание: не соединяйте коммутаторы одновременно несколькими кабелями во время настройки до особого указания.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора 1

Удалите порты из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-12
create vlan v3 tag 3
config vlan v3 add untagged 13-24
```

Проверьте настройки VLAN:
```
show vlan
```

Включите протокол связующего дерева на коммутаторе:
```
enable stp
```

Проверьте текущую конфигурацию протокола связующего дерева на портах коммутатора:
```
show stp ports
```

Измените версию протокола связующего дерева на MSTP (по умолчанию используется RSTP):
```
config stp version mstp
```

Настройте имя MST-региона и ревизию:
```
config stp mst_config_id name abc
config stp mst_config_id revision_level 1
```

Создайте MSTI и карту привязки VLAN к MSTI:
```
create stp instance_id 2
config stp instance_id 2 add_vlan 2
create stp instance_id 3
config stp instance_id 3 add_vlan 3
```

Настройте приоритет STP так, чтобы коммутатор был выбран корневым мостом в MSTI 2:
```
config stp priority 4096 instance_id 2
config stp priority 32768 instance_id 3
```

Настройте порты как граничные:
```
config stp ports 1-24 edge true
```

Активизируйте протокол связующего дерева на портах:
```
config stp ports 1-24 state enable
```

Настройка коммутатора 2
Удалите порты из VLAN по умолчанию для их использования в других VLAN:
```
config vlan default delete 1-24
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:
```
create vlan v2 tag 2
config vlan v2 add untagged 1-12
create vlan v3 tag 3
config vlan v3 add untagged 13-24
```

Проверьте настройки VLAN:
```
show vlan
```

Включите протокол связующего дерева на коммутаторе:
```
enable stp
```

Проверьте доступность соединения между рабочими станциями командой ping:
```
ping <IP-address>
```

- от ПК1 к ПК 3 _____
- от ПК2 к ПК4 _____

Что вы наблюдаете? Запишите.

_____
_____
_____

Измените версию протокола связующего дерева на MSTP (по умолчанию используется RSTP):

```
config stp version mstp
```

Настройте имя MST-региона и ревизию:

```
config stp mst_config_id name abc
config stp mst_config_id revision_level 1
```

Создайте MSTI и карту привязки VLAN к MSTI:

```
create stp instance_id 2
config stp instance_id 2 add_vlan 2
create stp instance_id 3
config stp instance_id 3 add_vlan 3
```

Настройте приоритет STP так, чтобы коммутатор был выбран корневым мостом в MSTI 3:

```
config stp priority 32768 instance_id 2
config stp priority 4096 instance_id 3
```

Настройте порты как граничные:

```
config stp ports 1-24 edge true
```

Активизируйте протокол связующего дерева на портах:

```
config stp ports 1-24 state enable
```

Подключите коммутаторы как показано на схеме 8.3.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК 3 _____
- от ПК1 к ПК 2 _____
- от ПК1 к ПК 4 _____
- от ПК3 к ПК4 _____
- от ПК2 к ПК4 _____

Проверьте текущую конфигурацию протокола связующего дерева на портах коммутатора:

```
show stp ports
```

Какие порты являются корневым и альтернативным для VLAN v2? _____
Какие порты являются корневым и альтернативным для VLAN v3? _____
Какие порты являются назначенными для VLAN v2? _____
Какие порты являются назначенными для VLAN v3? _____

ПРАКТИЧЕСКАЯ РАБОТА № 19

Настройка функции защиты отобразования петель LoopBack Detection

Функция LoopBack Detection (LBD) обеспечивает дополнительную защиту от образования петель на уровне 2 модели OSI. Существует две реализации этой функции:

• STP LoopBack Detection;

• LoopBack Detection Independent STP.

Коммутатор, на котором настроена функция STP LoopBack Detection, определяет наличие петли, когда отправленный им кадр BPDU вернулся назад на другой его порт. В этом случае порт-источник кадра BPDU и порт-приемник будут автоматически заблокированы, и администратору сети будет отправлен служебный пакет-уведомление. Порты будут находиться в заблокированном состоянии до истечения таймера LBD Recover Timer.

Функция LoopBack Detection Independent STP не требует настройки протокола STP на портах, на которых необходимо определять наличие петли. В этом случае наличие петли обнаруживается путем отправки портом специального служебного кадра ECTP (Ethernet Configuration Testing Protocol). При получении кадра ECTP этим же портом, он блокируется на указанное в таймере время. Существуют два режима работы этой функции: Port-Based и VLAN-Based (начиная с LBD версии v.4.00).

В режиме Port-Based при обнаружении петли происходит автоматическая блокировка порта, и никакой трафик через него не передается.

В режиме VLAN-Based порт будет заблокирован для передачи трафика только той VLAN, в которой обнаружена петля. Остальной трафик через этот порт будет передаваться.

Цель: понять принципы работы функции LoopBack Detection Independent STP в режимах Port-Based и VLAN-Based.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	2 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.
Неуправляемый коммутатор	1 шт.

9.1. Настройка функции LoopBack Detection Independent STP в режиме Port-Based

В данном задании рассматривается блокирование порта управляемого коммутатора при обнаружении петли в подключённом сегменте.

Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Включите функцию LBD глобально на коммутаторе:

```
enable loopdetect
```

Активизируйте функцию LBD на всех портах коммутатора:

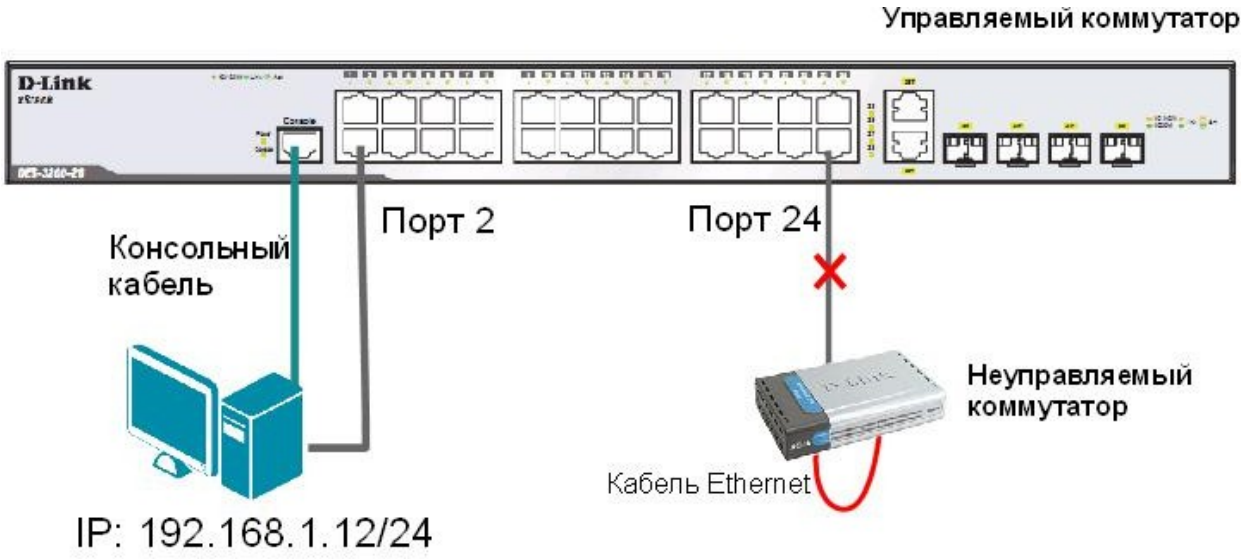
```
config loopdetect ports 1-24 state enabled
```

Сконфигурируйте режим Port-Based, чтобы при обнаружении петли отключался порт:

```
config loopdetect mode port-based
```

Внимание: При отключении порта трафик передаваться не будет ни из одной VLAN. Порт будет заблокирован.

Схема 9.1



Проверьте текущую конфигурацию функции LBD:
```
show loopdetect
```

Подключите неуправляемый коммутатор с петлей к управляемому коммутатору, как показано на схеме 9.1.

Посмотрите, обнаружена ли петля на управляемом коммутаторе:
```
show loopdetect ports
```

Что вы наблюдаете? Запишите.

_____

_____

Проверьте log-файл:
```
show log
```

Что вы наблюдаете? Запишите.

_____

_____

Проверьте загрузку портов:
```
show utilization ports
```

Отключите неуправляемый коммутатор с петлей от управляемого коммутатора.

Отключите функцию LBD глобально на коммутаторе:
```
disable loopdetect
```

Проверьте загрузку портов:
`show utilization ports`

Подключите неуправляемый коммутатор с петлей к управляемому коммутатору.

Что вы наблюдаете? Запишите.

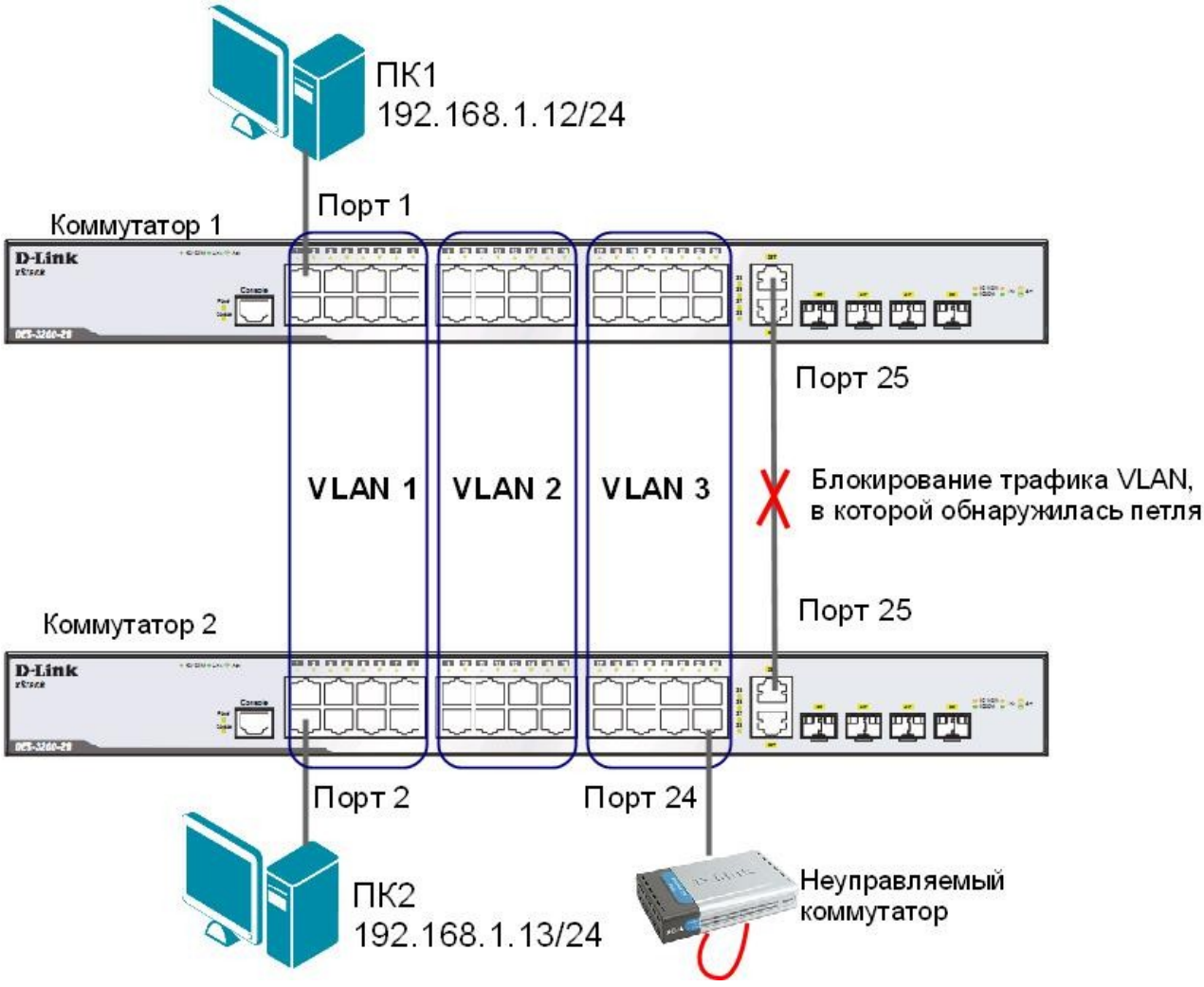
_____
_____

Отключите неуправляемый коммутатор с петлей от управляемого коммутатора.

9.2. Настройка функции LoopBack Detection Independent STP в режиме VLAN-Based.

В данном задании рассматривается блокирование порта управляемого коммутатора для передачи трафика только той VLAN, в которой обнаружена петля. Остальной трафик будет передаваться через этот порт.

Схема 9.2



Примечание: если при передаче пакетов порт 25 коммутатора 1 получит ECTP-кадр, который отправлял сам, передача трафика в VLAN 3, из которой он пришёл, будет заблокирована.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам командой:

```
reset config
```

Настройка коммутатора 1

Удалите порты из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 9-24
```

Создайте VLAN vlan2 и vlan3:

```
create vlan vlan2 tag 2
create vlan vlan3 tag 3
```

Добавьте в созданные VLAN v2 и v3 немаркированные порты. Добавьте порт 25 в VLAN default, v2 и v3 в качестве маркированного:

```
config vlan default add tagged 25
config vlan vlan2 add untagged 9-16
config vlan vlan2 add tagged 25
config vlan vlan3 add untagged 17-24
config vlan vlan3 add tagged 25
```

Проверьте настройки VLAN:

```
show vlan
```

Включите функцию LBD глобально на коммутаторе:

```
enable loopdetect
```

Активизируйте функцию LBD на всех портах коммутатора:

```
config loopdetect ports all state enabled
```

Сконфигурируйте режим VLAN-Based, в котором при обнаружении петли порт не сможет передавать трафик той VLAN, в которой обнаружена петля:

```
config loopdetect mode vlan-based
```

Настройка коммутатора 2

Удалите порты из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 9-24
```

Создайте VLAN vlan2 и vlan3:

```
create vlan vlan2 tag 2
create vlan vlan3 tag 3
```

Добавьте в созданные VLAN v2 и v3 немаркированные порты. Добавьте порт 25 в VLAN default, v2 и v3 в качестве маркированного:

```
config vlan default add tagged 25
config vlan vlan2 add untagged 9-16
config vlan vlan2 add tagged 25
config vlan vlan3 add untagged 17-24
config vlan vlan3 add tagged 25
```

Проверьте настройки VLAN:
`show vlan`

Отключите функцию LBD глобально на коммутаторе:
`disable loopdetect`

Подключите неуправляемый коммутатор с петлей к коммутатору 2, как показано на схеме 9.2.

Посмотрите, обнаружена ли петля на коммутаторах 1 и 2:
`show loopdetect ports 1-24`

Что вы наблюдаете? Запишите.
Коммутатор 1 _____
Коммутатор 2 _____

Проверьте log-файл коммутаторов:
`show log`

Что вы наблюдаете, запишите?
Коммутатор 1 _____

Коммутатор 2 _____

Проверьте загрузку портов:
`show utilization ports`

Что вы наблюдаете? Запишите.
Коммутатор 1 _____

Коммутатор 2 _____

Отключите неуправляемый коммутатор с петлей от коммутатора 2.

ПРАКТИЧЕСКАЯ РАБОТА № 20

. Агрегирование каналов

Агрегирование каналов связи (Link Aggregation) – это объединение нескольких физических портов в одну логическую магистраль на канальном уровне модели OSI с целью образования высокоскоростного канала передачи данных и повышения отказоустойчивости.

Все избыточные связи в одном агрегированном канале остаются в рабочем состоянии, а имеющийся трафик распределяется между ними для достижения балансировки нагрузки. При отказе одной из линий, входящих в такой логический канал, трафик распределяется между оставшимися линиями.

Включённые в агрегированный канал порты называются членами группы агрегирования (Link Aggregation Group). Один из портов в группе выступает в качестве мастера-порта (master port). Так как все порты агрегированной группы должны работать в одном режиме, конфигурация мастера-порта распространяется на все порты в группе.

Важным моментом при реализации объединения портов в агрегированный канал является распределение трафика по ним. Выбор порта для конкретного сеанса выполняется на основе выбранного алгоритма агрегирования портов, т.е. на основании некоторых признаков поступающих пакетов.

В коммутаторах D-Link по умолчанию используется алгоритм mac_source (MAC-адрес источника).

Программное обеспечение коммутаторов D-Link поддерживает два типа агрегирования каналов связи: статическое и динамическое, на основе стандарта IEEE 802.3ad (LACP).

При статическом агрегировании каналов (используется по умолчанию), все настройки на коммутаторах выполняются вручную, и они не допускают динамических изменений в агрегированной группе.

Для организации динамического агрегирования каналов между коммутаторами и другими сетевыми устройствами используется протокол управления агрегированным каналом – Link Aggregation Control Protocol (LACP). Протокол LACP определяет метод управления объединением нескольких физических портов в одну логическую группу и предоставляет сетевым устройствам возможность автосогласования каналов, путём отправки управляющих кадров протокола LACP непосредственно подключённым устройствам с поддержкой LACP. Порты, на которых активизирован протокол LACP, могут быть настроены для работы в одном из двух режимов: активном (active) или пассивном (passive). При работе в активном режиме порты выполняют обработку и рассылку управляющих кадров протокола LACP. При работе в пассивном режиме порты выполняют только обработку управляющих кадров LACP.

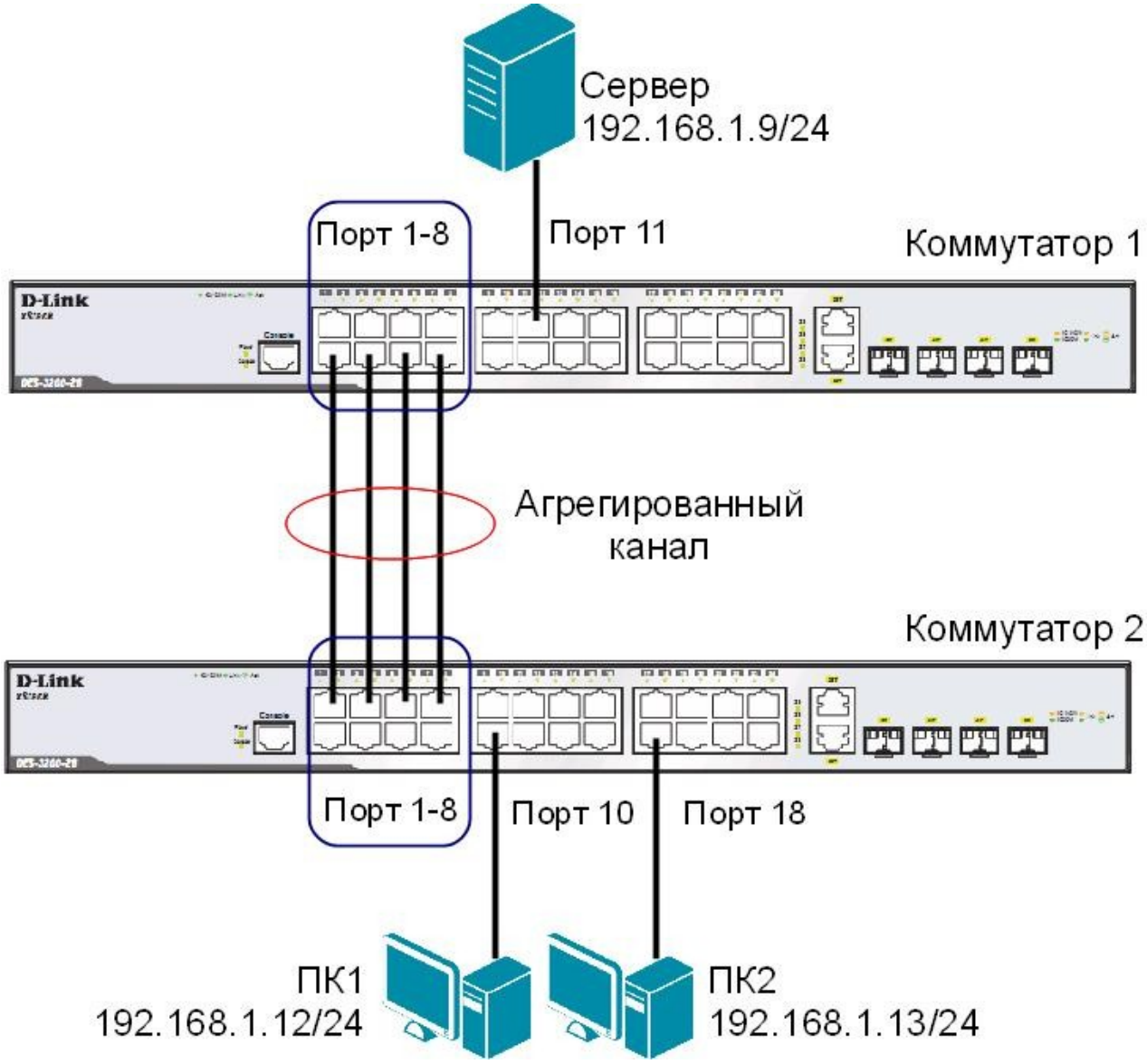
Для создания искусственной нагрузки на канал связи между коммутаторами, при выполнении лабораторной работы будет использоваться программа iperf.

Цель: изучить настройку динамического агрегирования каналов на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	3 шт.
Консольный кабель	2 шт.
Кабель Ethernet	7 шт.

Схема 10



<u>Примечание:</u> не соединяйте физически соответствующие порты коммутаторов до тех пор, пока не настроено агрегирование каналов, т.к. в коммутируемой сети может возникнуть петля.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора 1

Создайте группу агрегирования каналов:

```
create link_aggregation group_id 1 type lacp
```

Включите порты 1-8 в группу агрегирования каналов и выберите порт 1 в качестве мастера-порта:

```
config link_aggregation group_id 1 master_port 1 ports 1-8 state
enabled
```

Настройте порты на работу в пассивном режиме:
```
config lacp_port 1-8 mode passive
```

Проверьте выполненные настройки:
```
show link_aggregation
```

Проверьте режим работы LACP на портах коммутаторов:
```
show lacp_port
```

Посмотрите текущий алгоритм агрегирования каналов:
```
show link_aggregation algorithm
```

Настройка коммутатора 2
Создайте группу агрегирования каналов:
```
create link_aggregation group_id 1 type lacp
```

Включите порты 1-8 в группу агрегирования каналов и выберите порт 1 в качестве мастера-порта:
```
config link_aggregation group_id 1 master_port 1 ports 1-8 state
enabled
```

Настройте порты на работу в активном режиме:
```
config lacp_port 1-8 mode active
```

Проверьте выполненные настройки:
```
show link_aggregation
```

Проверьте режим работы LACP на портах коммутаторов:
```
show lacp_port
```

Подключите коммутаторы 4 кабелями, как показано на схеме 10. Из настроенной группы можно использовать любые порты.

Для создания искусственной нагрузки на канал связи между коммутаторами, используется утилита командной строки **iperf.** Iperf (для Windows) представляет собой небольшой исполняемый файл, который содержит клиентскую и серверную части. Программа не требует установки. Для запуска необходимо скопировать программу iperf на оба компьютера и запустить сначала серверную часть, а затем клиентскую.

Ключи, используемые при запуске программы iperf:
`-s` – устанавливает режим сервера;
`-c` - устанавливает режим клиента и задает адрес сервера;
`-i` - задает интервал вывода отчета о скорости;
`-t` - время длительности теста в секундах;
`-r` - режим двустороннего тестирования;
`-u` - режим тестирования по протоколу UDP, а не TCP;
`-b10M` - задает полосу генерации трафика в 10 Мбит/с;
`-P5` - запускает одновременно 5 тестовых потоков.

ЗАДАНИЕ

Запустите программу iperf на ПК, выполняющего роль сервера (запускается из командной строки, где указывается путь к программе и ключи):

```
iperf –s -u
```

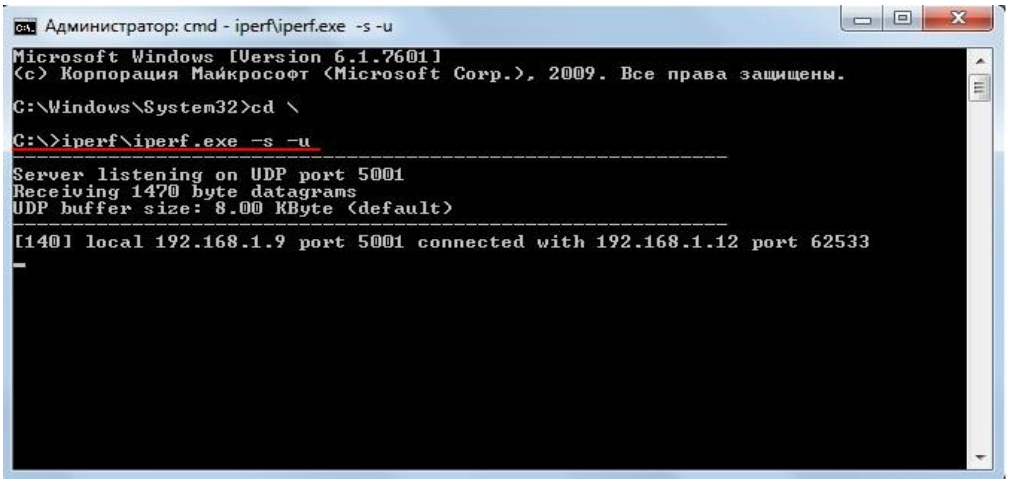


Рисунок 10.1 Запуск программы iperf на ПК,
выполняющего роль сервера

Запустите программу iperf на ПК1 и ПК2:

```
iperf -c 192.168.1.9 -i 1 -t 1000 -r -u -b10M -P5
```

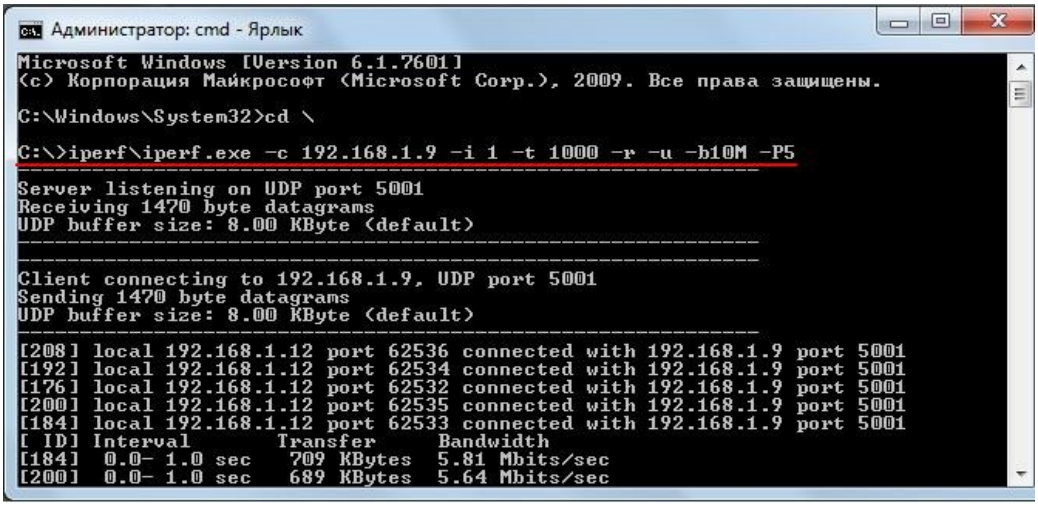


Рисунок 10.2 Запуск программы iperf на ПК,
выполняющего роль клиента

Во время теста проверьте загрузку портов на обоих коммутаторах:

```
show utilization ports
```

Что вы наблюдаете? Загрузка трафика перераспределяется между каналами? Сколько одновременно соединений участвует в передаче? Почему?

_____

_____

_____

ПРАКТИЧЕСКАЯ РАБОТА № 30

Списки управления доступом (Access Control List)

Списки управления доступом (Access Control List, ACL) являются средством

фильтрации потоков данных без потери производительности, так как. проверка содержимого пакетов данных выполняется на аппаратном уровне. Фильтруя потоки данных, администратор может ограничить типы приложений, разрешённых для использования в сети, контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS, путём классификации трафика и переопределения его приоритета.

ACL представляют собой последовательность условий проверки параметров пакетов данных. Когда сообщения поступают на входной интерфейс, коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определёнными в ACL и выполняет над пакетами одно из действий: Permit (Разрешить) или Deny (Запретить).

Списки управления доступом состоят из профилей доступа (Access Profile) и правил (Rule). Профили доступа определяют типы критериев фильтрации, которые должны проверяться в пакете данных (MAC-адрес, IP-адрес, номер порта, VLAN и т.д.), а в правилах указываются непосредственные значения их параметров. Каждый профиль может состоять из множества правил.

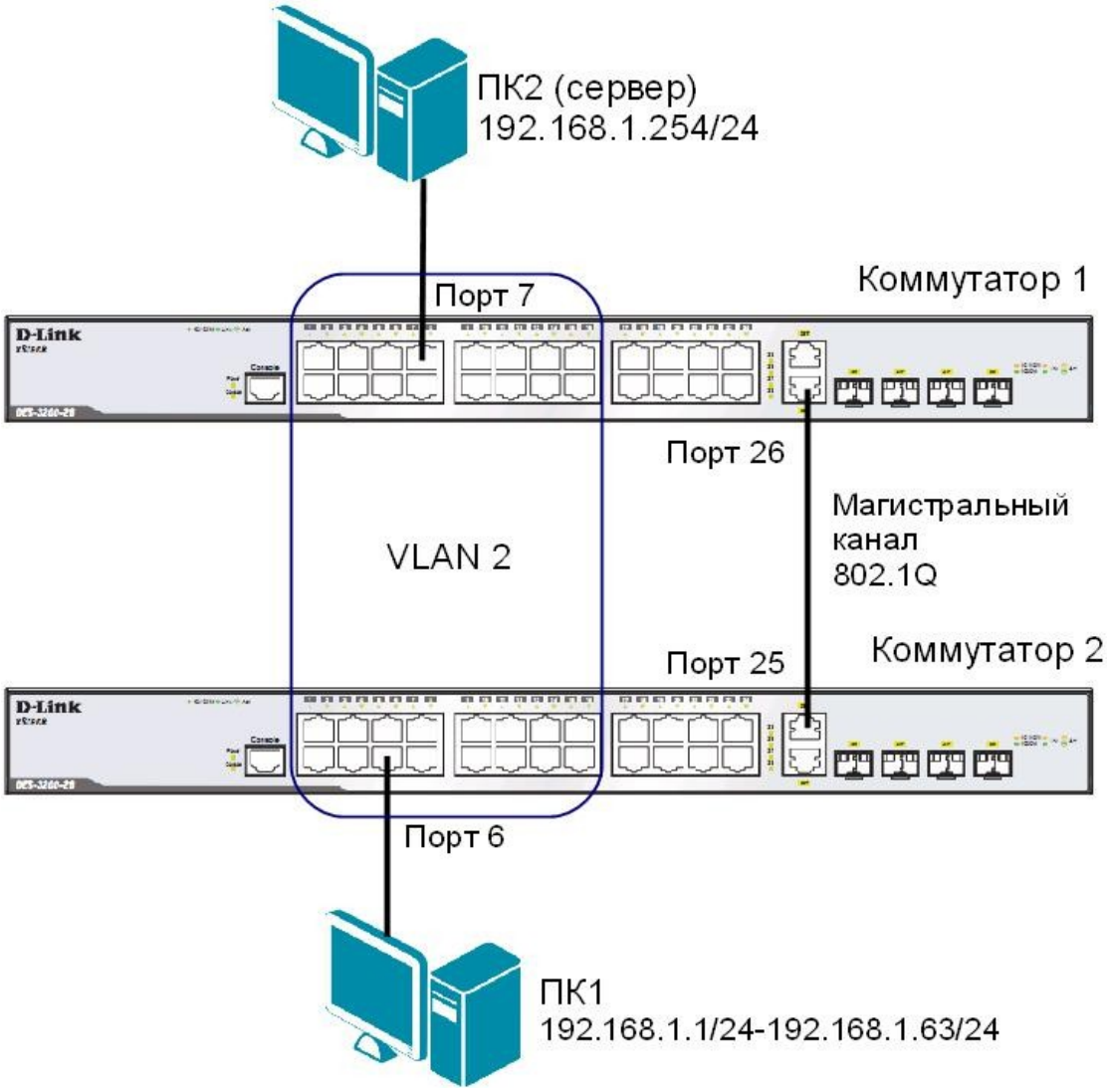
Цель: на коммутаторе D-Link настроить списки управления доступом, используя в качестве критериев фильтрации MAC и IP-адреса.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	3 шт.

12.1. Настройка ограничения доступа пользователей к серверу по IP-адресам

Схема 12.1



ЗАДАНИЕ

Разрешить доступ к серверу пользователям с IP-адресами с 192.168.1.1/24 по 192.168.1.63/24. Остальным пользователем сети 192.168.1.0/24, с адресами не входящими в разрешённый диапазон, доступ к серверу запретить.

Правила:
Правило 1:
Если IP-адрес источника = IP-адресам из диапазона с 192.168.1.1 по 192.168.1.63 (подсеть 192.168.1.0/26) — разрешить (permit);
Правило 2:
Если IP-адрес источника принадлежит сети 192.168.0.0/24, но не входит в разрешенный диапазон адресов — запретить (deny).
Правило 3:
Иначе, по умолчанию разрешить доступ всем узлам.

Примечание: максимальное количество профилей, которое поддерживает коммутатор DES-3200-28 равно 4.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам командой:

```
reset config
```

Настройка коммутатор 2

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-16
```

Создайте VLAN 2 и добавьте соответствующие порты, которые необходимо настроить немаркированными. Настройте порт 25 маркированным:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-16
config vlan v2 add tagged 25
```

Проверьте настройки VLAN:

```
show vlan
```

Повторите процедуру настройки для коммутатора 1

Проверьте доступность соединения между ПК1 и ПК2 командой ping:

```
ping <IP-address>
```

от ПК1 к ПК2 _____

Настройка коммутатора 1

Создайте профиль доступа с номером 4, осуществляющий фильтрацию трафика по IP-адресам:

```
create access_profile profile_id 4 profile_name 4 ip
source_ip_mask 255.255.255.255
```

Правило 1.

Создайте правило для профиля доступа 4, разрешающее доступ для подсети 192.168.1.0/26 (узлам с 1 по 63):

```
config access_profile profile_id 4 add access_id 1 ip source_ip
192.168.1.0 mask 255.255.255.192 port 26 permit
```

Примечание: созданное правило разрешает прохождение трафика IP-подсети 192.168.1.0/26 через 26 порт.

Правило 2

Создайте правило для профиля доступа 4, запрещающее остальным станциям доступ к серверу:

```
config access_profile profile_id 4 add access_id 2 ip source_ip
192.168.1.0 mask 255.255.255.0 port 26 deny
```

Примечание: созданное правило запрещает прохождение через 26 порт трафика, который принадлежит сети 192.168.1.0/24, но не входит в разрешенный диапазон.

Правило 3

Разрешите все остальное:

Выполняется по умолчанию

Проверьте созданные профили:
```
show access_profile
```

Что вы наблюдаете? Сколько профилей создано, сколько в них правил?

_____

_____

Подключите рабочую станцию ПК1 как показано на схеме 12.1 (адрес из диапазона 192.168.1.1-192.168.1.63/24) к коммутатору 2.

Протестируйте командой ping соединение с сервером 192.168.1.254/24.

Что вы наблюдаете? Запишите.

_____

_____

Измените IP-адрес рабочей станции ПК1 (адрес из диапазона 192.168.1.64-192.168.1.254/24)

Протестируйте командой ping соединение с сервером 192.168.1.254/24.

Что вы наблюдаете? Запишите.

_____

_____

Удалите профиль ACL:
```
delete access_profile profile_id 4
```

Проверьте соединение с сервером командой ping:
```
ping 192.168.1.254
```

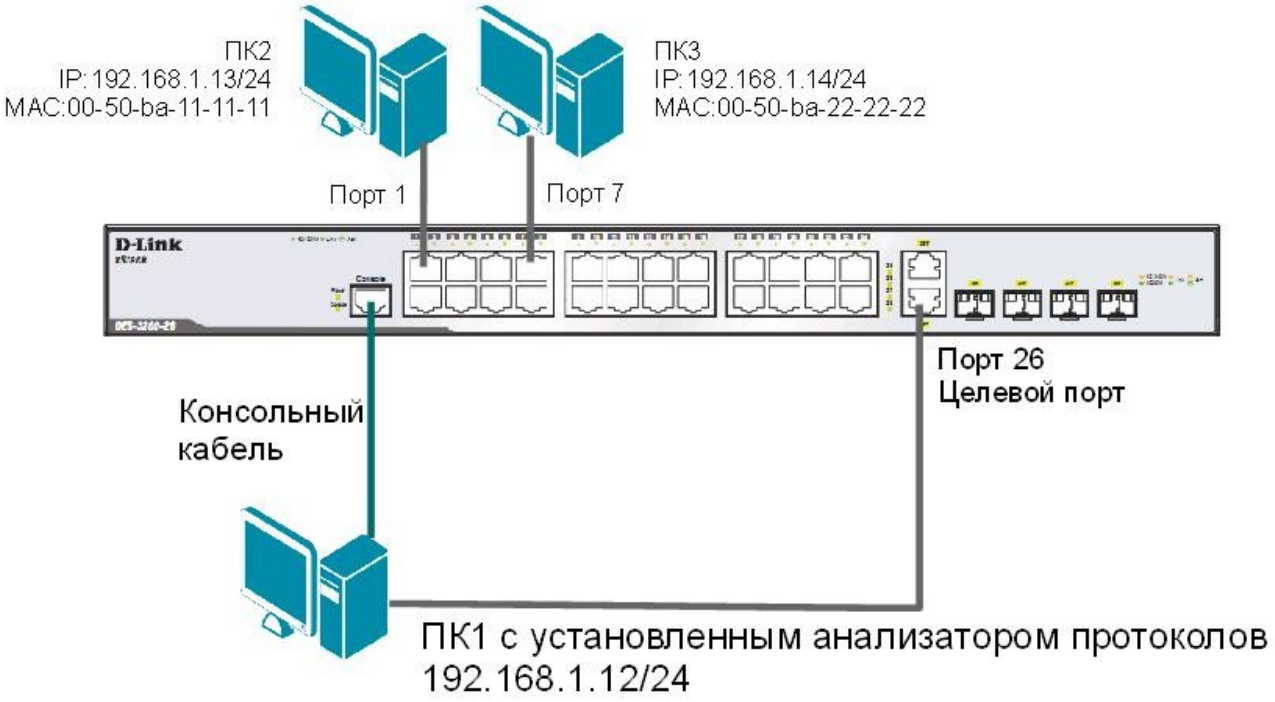
Что вы наблюдаете? Запишите.

_____

_____

12.2. Настройка фильтрации кадров по MAC-адресам

Схема 12.2



ЗАДАНИЕ

Настроить профиль доступа так, чтобы кадры, принимаемые на любой порт коммутатора от ПК3 (с MAC-адресом 00-50-ba-22-22-22) зеркалировались (копировались) на целевой порт коммутатора, к которому подключено устройство мониторинга сети.

Правило:
Если MAC-адрес источника = MAC-адресу ПК3 (00-50-ba-22-22-22) — копировать кадры на целевой порт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам командой:

```
reset config
```

Внимание! Замените указанные в командах MAC-адреса на реальные MAC-адреса рабочих станций.

Создайте профиль доступа 4:

```
create access_profile profile_id 4 profile_name 4 ethernet
source_mac FF-FF-FF-FF-FF-FF
```

Создайте правило для профиля доступа 4, в результате выполнения которого кадры, принимаемые на любой порт коммутатора с ПК3 будут зеркалироваться на целевой порт:

```
config access_profile profile_id 4 add access_id 1 ethernet
source_mac 00-50-ba-22-22-22 mask FF-FF-FF-FF-FF-FF port all
mirror
```

Проверьте созданный профиль:

```
show access_profile
```

Включите функцию зеркалирования портов глобально на коммутаторе:
```
enable mirror
```

Укажите целевой порт:
```
config mirror port 26
```

Проверьте настройки функции:
```
show mirror
```

Подключите рабочие станции ПК2 и ПК3 как показано на схеме 12.2

Выполните тестирование соединения между ПК2 и ПК3 с помощью команды:
```
ping <IP address>
```

- от ПК2 к ПК3 _____
- от ПК3 к ПК2 _____

Запустите на рабочей станции ПК1 анализатор протоколов Wireshark (настройка программы описана в лабораторной работе №15).

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Что вы наблюдаете? Запишите.

_____
_____

Подключите рабочую станцию ПК3 к порту 10 коммутатора.

Выполните тестирование соединения между ПК2 и ПК3 и наоборот командой ping.

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Что вы наблюдаете? Что изменилось? Запишите.

_____
_____

Удалите все профили ACL:
```
delete access_profile all
```

Отключите функцию зеркалирования портов:
```
disable mirror
```

ПРАКТИЧЕСКАЯ РАБОТА № 31

Контроль над подключением узлов кпортам коммутатора. Функция Port Security

Функция Port Security позволяет настроить какой-либо порт коммутатора так, чтобы доступ к сети через него мог осуществляться только определёнными устройствами. Устройства, которым разрешено подключаться к порту определяются по MAC-адресам. MAC-адреса могут быть изучены динамически или вручную настроены администратором сети. Помимо этого функция Port Security позволяет ограничивать количество изучаемых портом MAC-адресов, тем самым, ограничивая количество подключаемых к нему узлов.
Существует три режима работы функции Port Security:

- *Permanent* (Постоянный) – занесённые в таблицу коммутации MAC-адреса никогда не устаревают, даже если истекло время, установленное таймером Aging Time или коммутатор был перезагружен.
- *Delete on Timeout* (Удалить при истечении времени) – занесённые в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером Aging Time и будут удалены.
  Если состояние канала связи на подключённом порте изменяется, MAC-адреса, изученные на нем, удаляются из таблицы коммутации, что аналогично выполнению действий при истечении времени, установленного таймером Aging Time.
- *Delete on Reset* (Удалить при сбросе) – занесённые в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора (этот режим используется по умолчанию).

Функция Port Security оказывается весьма полезной при построении домовых сетей, сетей провайдеров Интернет и локальных сетей с повышенным требованием по безопасности, где требуется исключить доступ незарегистрированных рабочих станций к услугам сети.

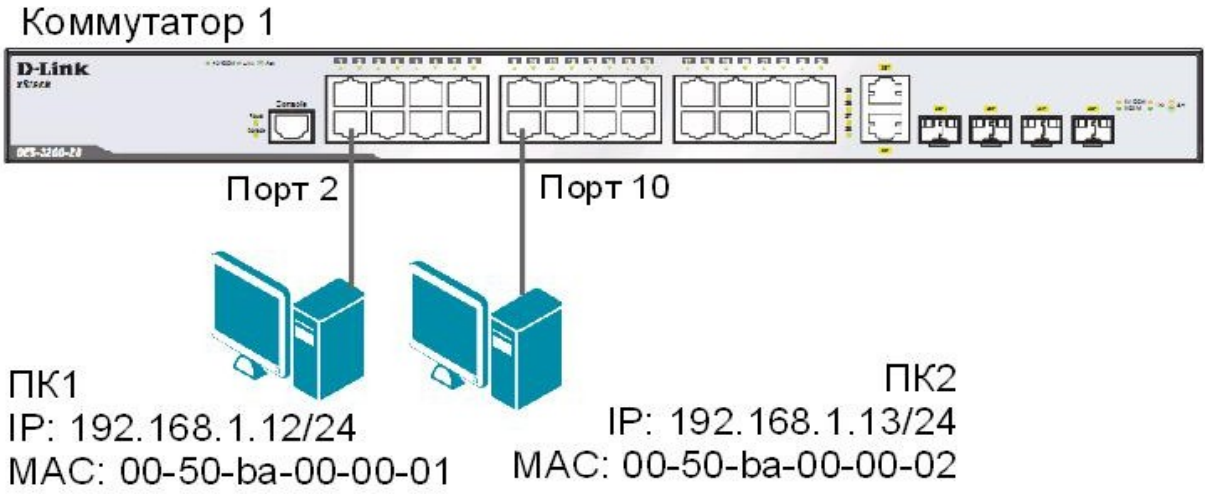
Используя функцию Port Security можно полностью запретить динамическое изучение MAC-адресов указанными или всеми портами коммутатора. В этом случае доступ к сети получат только те пользователи, MAC-адреса которых указаны в статической таблице коммутации.

Цель: научиться управлять подключением узлов к портам коммутатора и изучить настройку функции Port Security на коммутаторах D-Link.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.

Схема 13



13.1. Управление количеством подключаемых к портам коммутатора пользователей, путём ограничения максимального количества изучаемых MAC-адресов

Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Проверьте информацию о настройках Port Security:

```
show port_security
```

Установите максимальное количество изучаемых каждым портом MAC-адресов равным 1, и включите функцию на всех портах:

```
config port_security ports all admin_state enable
max_learning_addr 1
```

Подключите ПК1 и ПК2 к портам 2 и 10 коммутатора соответственно.

Посмотрите MAC-адреса, которые стали известны портам 2 и 10:

```
show fdb port 2
show fdb port 10
```

Проверьте, соответствуют ли зарегистрированные адреса адресам рабочих станций:_____

Проверьте информацию о настройках Port Security на портах коммутатора:

```
show port_security ports 1-24
```

Включите запись в журнал работы коммутатора MAC-адресов, подключающихся к порту станций и отправку сообщений SNMP Trap:

```
enable port_security trap_log
```

Выполните тестирование доступности узлов командой ping от ПК1 к ПК2 и наоборот.

Подключите ПК1 к порту 10, а ПК2 к порту 1.

Повторите тестирование соединения между рабочими станциями командой ping.

Проверьте информацию в журнале работы коммутатора:
```
show log
```

Какой вы сделаете вывод?_____
_____
_____

Сохраните конфигурацию и перезагрузите коммутатор:
```
save
reboot
```

Выполните тестирование соединения между рабочими станциями командой ping.

Какой вы сделаете вывод? Сохраняется ли информация о привязке MAC-порт?
_____
_____

Настройте на порте 2 работу функции Port Security в режиме Permanent и максимальное количество изучаемых адресов равное 1:
```
config port_security ports 2 admin_state enable max_learning_addr
1 lock_address_mode permanent
```

Сохраните конфигурацию и перезагрузите коммутатор:
```
save
reboot
```

Проверьте информацию о настройках Port Security на портах коммутатора:
```
show port_security ports 1-24
```

Какой вы сделаете вывод? Сохраняется ли информация о привязке MAC-порт?
_____
_____
_____

Очистите информацию о привязке MAC-порт на порте 2:
```
clear port_security_entry port 2
```

Отключите работу функции Port Security на порте 2 и приведите настройки в исходное (по умолчанию) состояние:
```
config port_security ports 2 admin_state disable max_learning_addr
1 lock_address_mode deleteonreset
```

Посмотрите время таймера блокирования (он соответствует времени жизни MAC-адреса в таблице коммутации):
```
show fdb aging_time
```

Изменить время действия таймера можно с помощью настройки времени жизни MAC-адреса в таблице коммутации (время указано в секундах):
```
config fdb aging_time 20
```

Измените режим работы функции Port Security на Delete on Timeout:

```
config port_security ports 2 admin_state enable max_learning_addr
1 lock_address_mode deleteontimeout
```

Проверьте MAC-адреса, которые стали известны порту 2:

```
show fdb port 2
```

Проверьте информацию о настройках Port Security на портах коммутатора:

```
show port_security ports 1-24
```

Выполните тестирование соединения между ПК1 и ПК2 командой ping.

Какой вы сделаете вывод? Сохраняется информации о привязке MAC-порт?

_____

_____

_____

Отключите работу функции Port Security на портах:

```
config port_security ports 1-24 admin_state disable
```

Отключите функцию записи в log-файл и отправки SNMP Trap:

```
disable port_security trap_log
```

Примечание: после выполнения обучения имеется возможность отключить функцию динамического изучения MAC-адресов, тогда в таблице коммутации сохранятся изученные адреса. Таким образом, текущая конфигурация сети будет сохранена, и дальнейшее подключение новых устройств без ведома администратора будет невозможно. Новые устройства можно добавить путём создания статических записей в таблице коммутации.

13.2. Настройка защиты от подключения к портам, основанной на статической таблице MAC-адресов

Сбросьте настройки коммутатора к заводским настройкам командой:

```
reset system
```

Активизируйте функцию Port Security на всех портах и запретите изучение MAC-адресов, установив параметр *max_learning_addr* равным 0 (команда вводится в одну строку):

```
config port_security ports 1-24 admin_state enable
max_learning_addr 0
```

Проверьте состояние портов:

```
show ports
```

Проверьте соединение между ПК1 и ПК2 командой ping.

Проверьте состояние таблицы коммутации:

```
show fdb
```

Имеются ли там записи? _____

В таблице коммутации вручную создайте статические записи для MAC-адресов рабочих станций, подключённых к портам 2 и 10.

Внимание! **Замените указанные в командах MAC-адреса на реальные адреса рабочих станций, подключаемых к коммутатору.**

```
create fdb default 00-50-ba-00-00-01 port 2
create fdb default 00-50-ba-00-00-02 port 10
```

Проверьте созданные статические записи в таблице коммутации:
```
show fdb
```

Проверьте информацию о настройках Port Security на портах коммутатора:
```
show port_security ports 1-24
```

Проверьте соединение между ПК1 и ПК2 командой ping.

Подключите ПК1 к порту 8, а ПК2 к порту 2.

Повторите тестирование командой ping.

Какой вы сделаете вывод?_____

_____

_____

Удалите ранее созданную статическую запись из таблицы MAC-адресов на порте 2:
```
delete fdb default 00-50-ba-00-00-02 port 2
```

ПРАКТИЧЕСКАЯ РАБОТА № 32

Контроль над подключением узлов кпортам коммутатора. Функция IP-MAC-Port Binding

Функция IP-MAC-Port Binding (IMPB), реализованная в коммутаторах D-Link, позволяет контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, а также порта подключения. Администратор сети может создать записи («белый лист»), связывающие MAC- и IP-адреса компьютеров с портами подключения коммутатора. На основе этих записей, в случае совпадения всех составляющих, клиенты будут получать доступ к сети со своих компьютеров. В том случае, если при подключении клиента, связка IP-MAC-порт будет отличаться от параметров заранее сконфигурированной записи, то коммутатор заблокирует MAC-адрес соответствующего узла с занесением его в «чёрный лист».

Функция IP-MAC-Port Binding включает три режима работы: ARP mode (по умолчанию), ACL mode и DHCP Snooping mode.

ARP mode является режимом, используемым по умолчанию, при настройке функции IP-MAC-Port Binding на портах. При работе в режиме ARP коммутатор анализирует ARP-пакеты и сопоставляет параметры IP-MAC ARP-пакета с предустановленной администратором связкой IP-MAC. Если хотя бы один параметр не совпадает, то MAC-адрес узла будет занесён в таблицу коммутации с отметкой «Drop» (Отбрасывать). Если все параметры совпадают, MAC-адрес узла будет занесён в таблицу коммутации с отметкой «Allow» (Разрешён).

При функционировании в *ACL mode,* коммутатор на основе предустановленного администратором «белого листа» IMPB создает правила ACL. Любой пакет, связка IP-MAC которого отсутствует в «белом листе», будет блокироваться ACL.

Режим *DHCP Snooping* используется коммутатором для динамического создания записей IP-MAC на основе анализа DHCP-пакетов и привязки их к портам с включённой функцией IMPB (администратору не требуется создавать записи вручную). Таким образом, коммутатор автоматически создает «белый лист» IMPB в таблице коммутации или аппаратной таблице ACL (при включении режима ACL). При этом для обеспечения корректной работы, сервер DHCP должен быть подключён к доверенному порту с выключенной функцией IMPB. Администратор может ограничить максимальное количество создаваемых в процессе автоизучения записей IP-MAC на порт, следовательно, ограничить для каждого порта с активизированной функцией IMPB количество узлов, которые могут получить IP-адрес с DHCP-сервера. При работе в режиме DHCP Snooping коммутатор не будет создавать записи IP-MAC для узлов с IP-адресом установленным вручную.

При активизации функции IMPB на порте администратор должен указать режим его работы:

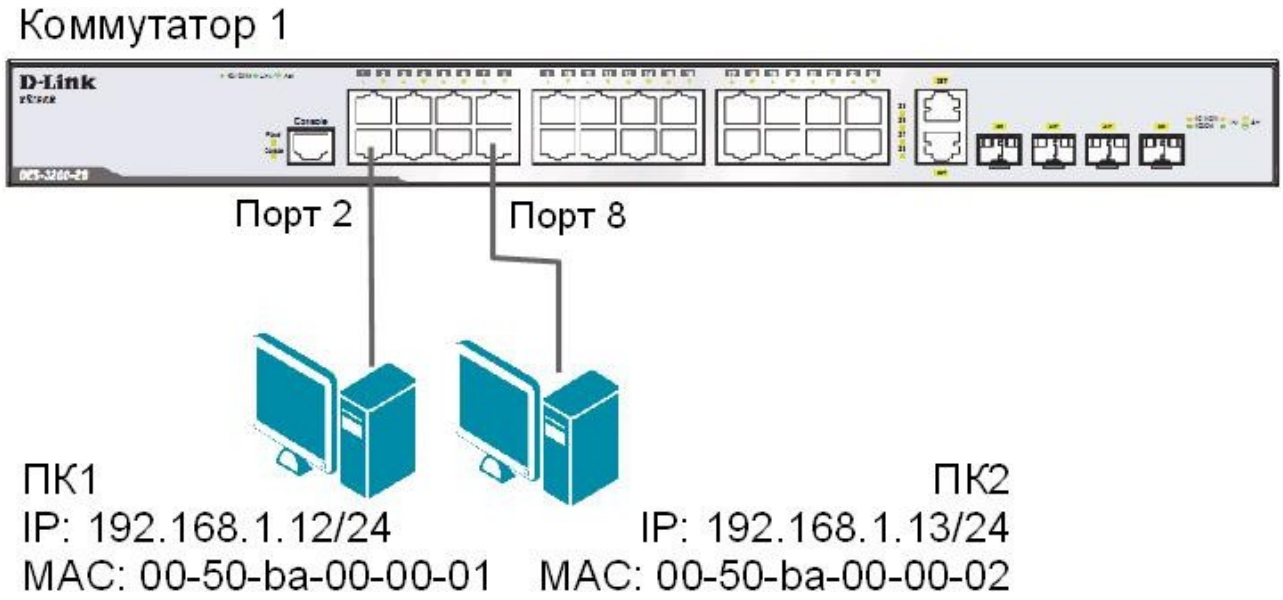
- **Strict Mode** – в этом режиме порт по умолчанию заблокирован.
- **Loose Mode** – в этом режиме порт по умолчанию открыт.

Цель: научиться управлять подключением узлов к портам коммутатора и изучить настройку функции IP-MAC-Port Binding на коммутаторах D-Link.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.

Схема 14



14.1. Настройка работы функции IP-MAC-Port Binding в режиме ARP

Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Внимание! Замените указанные в командах MAC-адреса на реальные MAC-адреса рабочих станций, подключаемых к коммутатору.

Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес рабочей станции ПК1 с портом 2 (по умолчанию режим работы функции ARP):

```
create address_binding ip_mac ipaddress 192.168.1.12 mac_address
00-50-ba-00-00-01 ports 2
```

Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес рабочей станции ПК2 с портом 8:

```
create address_binding ip_mac ipaddress 192.168.1.13 mac_address
00-50-ba-00-00-02 ports 8
```

Активизируйте функцию на портах 2 и 8 (по умолчанию режим работы портов strict):

```
config address_binding ip_mac ports 2,8 arp_inspection strict
```

Проверьте созданные записи IP-MAC-Port Binding:

```
show address_binding ip_mac all
```

Проверьте порты, на которых настроена функция и их режим работы:

```
show address_binding ports
```

Подключите рабочие станции ПК1 и ПК2 к коммутатору как показано на схеме 14.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

Включите запись в log-файл и отправку сообщений SNMP Trap в случае несоответствия ARP-пакета связке IP-MAC:

```
enable address_binding trap_log
```

Подключите ПК1 к порту 8, а ПК2 к порту 2.

Повторите тестирование соединения между рабочими станциями командой ping.

Проверьте заблокированные рабочие станции:

```
show address_binding blocked all
```

Проверьте наличие заблокированных станций в log-файле:

```
show log
```

Какой вы сделаете вывод?_____

_____

Удалите адрес ПК1 из списка заблокированных адресов:

```
delete address_binding blocked vlan_name default mac_address 00-
50-ba-00-00-01
```

Удалите адрес ПК2 из списка заблокированных адресов:

```
delete address_binding blocked vlan_name default mac_address 00-
50-ba-00-00-02
```

Удалите запись IP-MAC-Port Binding:

```
delete address_binding ip_mac ipaddress 192.168.1.12 mac_address
00-50-ba-00-00-01

delete address_binding ip_mac ipaddress 192.168.1.13 mac_address
00-50-ba-00-00-02
```

Отключите функцию IP-MAC-Port Binding на портах 2 и 8:

```
config address_binding ip_mac ports 2,8 arp_inspection disable
```

14.2. Настройка работы функции IP-MAC-Port Binding в режиме ACL

Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес станции ПК1 с портом 2:

```
create address_binding ip_mac ipaddress 192.168.1.12 mac_address
00-50-ba-00-00-01 ports 2
```

Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес станции ПК2 с портом 8:

```
create address_binding ip_mac ipaddress 192.168.1.13 mac_address
00-50-ba-00-00-02 ports 8
```

Активизируйте функцию на портах 2 и 8 (по умолчанию режим работы портов Strict) и установите работу функции IMPB в режиме ACL:

```
config address_binding ip_mac ports 2,8 ip_inspection enable
```

Примечание: по умолчанию автоматически включается режим allow_zeroip, благодаря которому коммутатор не будет блокировать узлы, отправляющие ARP-пакеты с IP-адресом источника 0.0.0.0.

Проверьте созданные записи IP-MAC-Port Binding:
```
show address_binding ip_mac all
```

Проверьте порты, на которых настроена функция и их режим работы:
```
show address_binding ports
```

Проверьте, созданные профили доступа ACL:
```
show access_profile
```

Подключите рабочие станции ПК1 и ПК2 к коммутатору как показано на схеме 14.

Проверьте доступность соединения между рабочими станциями командой ping:
```
ping <IP-address>
```

Подключите ПК1 к порту 8, а ПК2 к порту 2.

Повторите тестирование соединения между рабочими станциями командой ping.

Проверьте заблокированные рабочие станции:
```
show address_binding blocked all
```

Какой вы сделаете вывод?_____
_____

Удалите адрес из списка заблокированных адресов:
```
delete address_binding blocked vlan_name default mac_address 00-50-ba-00-00-01
```

Удалите все заблокированные адреса:
```
delete address_binding blocked all
```

Удалите все записи IP-MAC-Port Binding:
```
delete address_binding ip_mac ipaddress 192.168.1.12 mac_address 00-50-ba-00-00-01

delete address_binding ip_mac ipaddress 192.168.1.13 mac_address 00-50-ba-00-00-02
```

Отключите функцию IP-MAC-Port Binding на портах 2 и 8:
```
config address_binding ip_mac ports 2,8 ip_inspection disable
```

Какой можно сделать вывод о работе функции IP-MAC-Port Binding в режиме ACL?
_____
_____
_____

ПРАКТИЧЕСКАЯ РАБОТА № 33

Функции анализа сетевого трафика

Коммутаторы улучшают производительность и надёжность сети, передавая трафик только на те порты, которым он предназначен. При этом анализ критичных данных – сложная задача, поскольку инструментальные средства сетевого анализа физически изолированы от анализируемого трафика.

В коммутаторах D-Link реализована поддержка функции Port Mirroring (Зеркалирование портов), которая полезна администраторам для мониторинга и поиска неисправностей в сети.

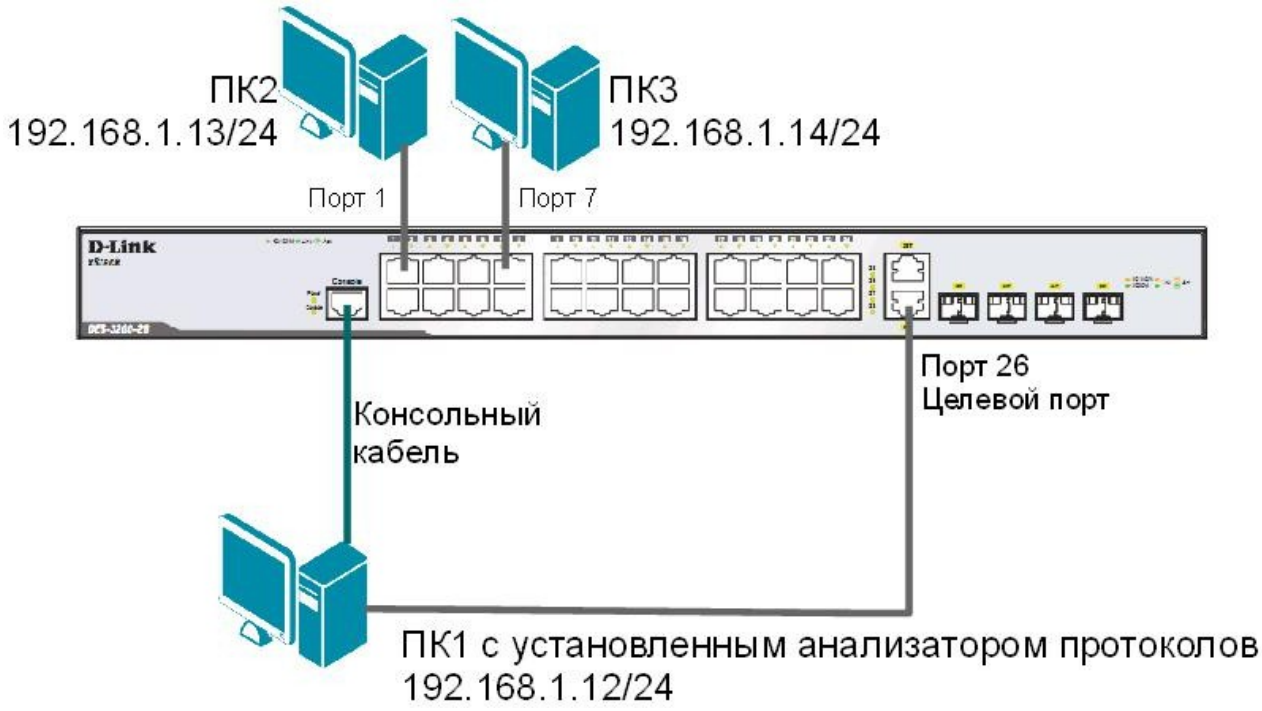
Функция Port Mirroring позволяет отображать (копировать) кадры, принимаемые в порт-источник (Source port) и отправляемые на целевой порт (Target port) коммутатора, к которому подключено устройство мониторинга с целью анализа проходящих через интересующий порт-источник пакетов.

Цель: изучить настройку функций зеркалирования портов и анализа сетевого трафика.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция	3 шт.
Консольный кабель	1 шт.
Кабель Ethernet	3 шт.

Схема 15



Укажите порты, трафик которых будет пересылаться на целевой порт 26:

```
config mirror port 26 add source ports 1,7 both
```

Включите функцию зеркалирования портов глобально в коммутаторе:

```
enable mirror
```

Проверьте настройки функции:

```
show mirror
```

Внимание: целевой порт и порт-источник должны принадлежать одной VLAN и иметь одинаковую скорость работы. В том случае, если скорость порта-источника будет выше скорости целевого порта, то коммутатор снизит скорость порта-источника до скорости работы целевого порта. Также целевой порт не может быть членом группы агрегированных каналов.

Запустите на рабочей станции ПК1 анализатор протоколов Wireshark. Интерфейс программы представлен ниже.

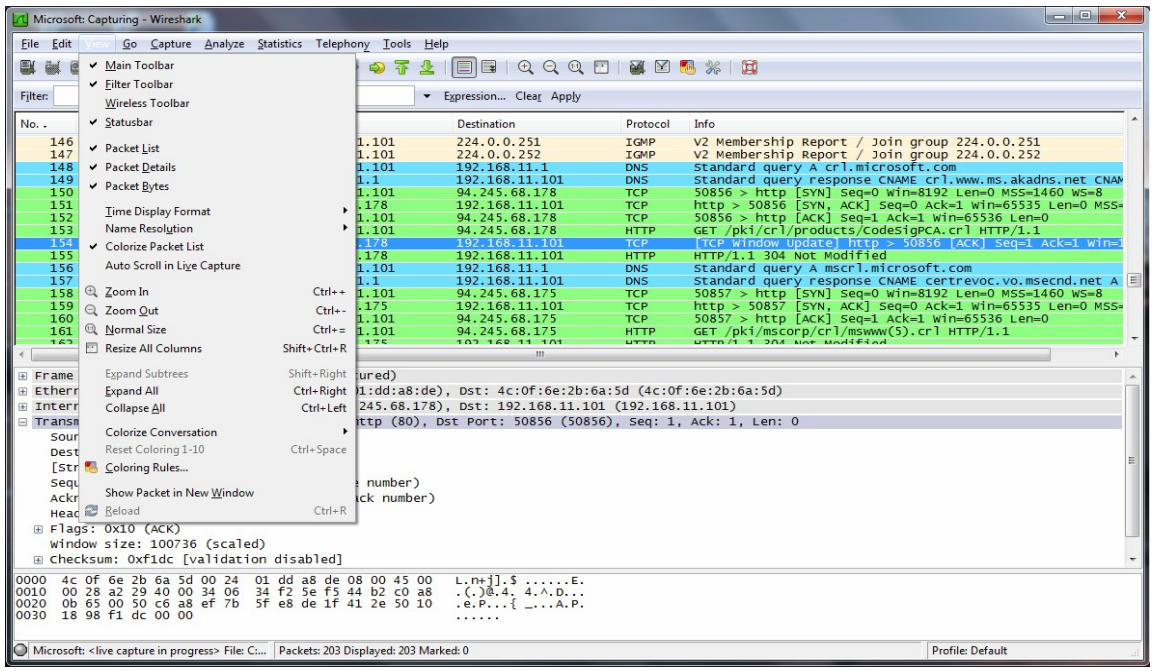


Рисунок 15. 1 Интерфейс программы Wireshark

Чтобы начать перехват трафика нужно выбрать правильный сетевой интерфейс. Чтобы выбрать сетевой адаптер, с которого будет выполняться перехват, необходимо нажать на кнопку **Interfaces** на тулбаре, либо меню **Capture > Interfaces:**

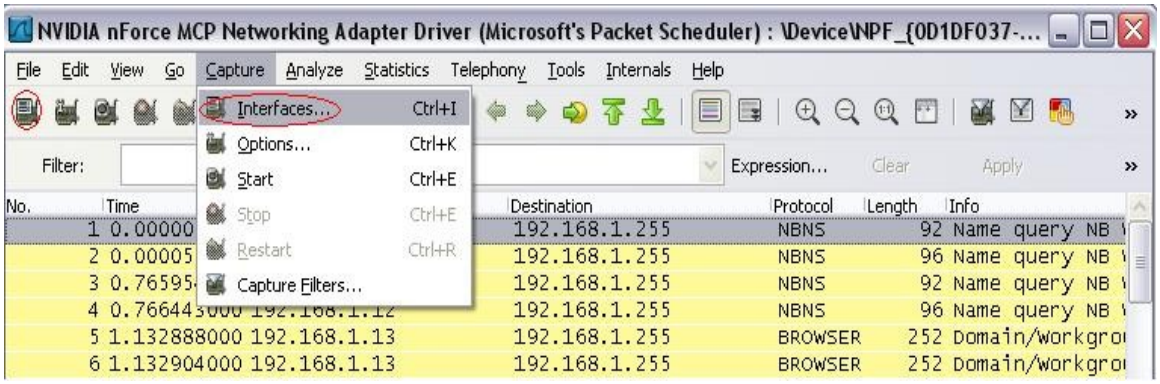


Рисунок 15. 2 Выбор интерфейса для перехвата трафика

После нажатия одной из этих кнопок появится окно со списком сетевых интерфейсов, доступных системе:

Рисунок 15. 3 Список сетевых интерфейсов

После нажатия кнопки **Start** начнется захват трафика.

ЗАДАНИЕ

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Выполните тестирование соединения между ПК2 и ПК3 и наоборот командой ping.

Наблюдаете ли вы трафик, передаваемый портами коммутатора? Какой еще трафик вы наблюдаете?_____
_____

Отключите функцию зеркалирования портов:

```
disable mirror
```

Проверьте настройки функции:

```
show mirror
```

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Выполните тестирование соединения между ПК 2 и ПК 3 и наоборот командой ping.

Что вы наблюдаете теперь? Сравните с предыдущими результатами?

_____
_____
_____
_____

ПРАКТИЧЕСКАЯ РАБОТА № 36

Настройка протокола управления топологией сети LLDP

Согласованная работа различных узлов в локальной сети (LAN) требует корректной конфигурации протоколов и приложений, которые выполняются и поддерживаются ими. По мере того как число различных типов устройств в сети растет, сетевым администраторам все труднее становится отслеживать правильность конфигурации каждого из них, одновременно все большее количество времени затрачивается на то, чтобы обнаружить и устранить проблемы. Стандарт 802.1ab, или Link Layer Discovery Protocol (LLDP), обеспечивает решение проблем конфигурации, вызванных расширением LAN.

Link Layer Discovery Protocol (LLDP) – протокол канального уровня, позволяющий сетевому оборудованию (коммутаторам, маршрутизаторам, IP-телефонам, беспроводным точкам доступа, узлам и т.д.) оповещать локальную сеть о своем существовании и характеристиках, а также собирать такие же оповещения, поступающие от соседнего оборудования. Информация, собранная посредством LLDP накапливается в устройствах, и может быть запрошена с помощью протокола SNMP. Таким образом, топология сети, в которой используется LLDP, может быть получена с управляющего компьютера, посредством последовательного опроса каждого устройства, на предмет собранной им информации. При этом получаемая информация содержит следующие параметры:

- Имя устройства (System Name);
- Описание устройства (System Description);
- Идентификатор порта (Port ID);
- Описание порта (Port Description);
- Возможности устройства (System Capabilities);
- Управляющий адрес (Management Address) и т.д.

Протокол LLDP передает информацию в сообщениях, которые называются *LLDP Data Unit (LLDPDU)*. Протоколом предусматривается передача данных только в одном направлении, то есть LLDP-устройства не обмениваются информацией в режиме запрос-ответ, а так же не подтверждают ее получения.

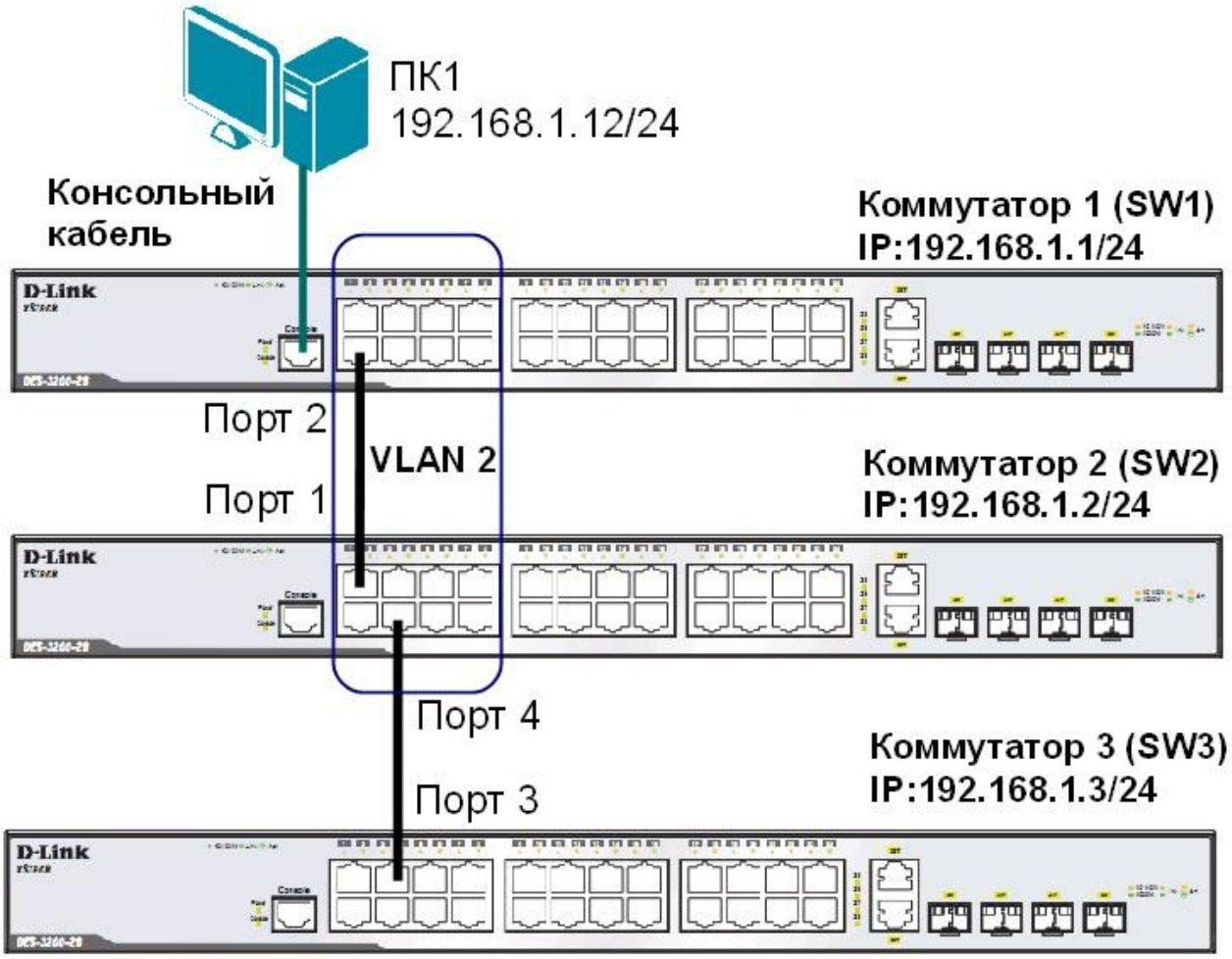
Таким образом, сам по себе LLDP не управляет трафиком – он только распространяет информацию, относящуюся к конфигурации на канальном уровне. Данный протокол, поддерживается всеми основными производителями активного сетевого оборудования. Используя эту информацию, и опрашивая MIB базы данных обнаруженных устройств, системы управления могут динамически моделировать и отслеживать состояния локальных сетей передачи данных, а также строить их визуальные схемы для пользователей и администраторов.

Цель: понять функционирование протокола LLDP и изучить его настройку на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	3 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.

Схема 16



Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора 1 (SW1)

Настройте IP-адрес коммутатора:

```
config ipif System ipaddress 192.168.1.1/24
```

Настройте имя коммутатора:

```
config snmp system_name SW1
```

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-9
```

Создайте VLAN v2, добавьте в соответствующий VLAN порты, которые необходимо настроить немаркированными.

```
create vlan v2 tag 2
config vlan v2 add untagged 1-9
```

Проверьте настройки VLAN:

```
show vlan
```

Включите работу протокола LLDP глобально на коммутаторе:
```
enable lldp
```

Проверьте информацию о настройках LLDP:
```
show lldp
```

Включите продвижение пакетов LLDP:
```
config lldp forward_message enable
```

Настройте интервал передачи информационных пакетов LLDP:
```
config lldp message_tx_interval 20
```

Примечание: с помощью данной команды можно регулировать частоту отправки LLDP-сообщений соседним устройствам с активных портов коммутатора. По умолчанию интервал 30 секунд.

Настройте время переинициализации LLDP:
```
config lldp reinit_delay 3
```

Примечание: данная команда позволяет установить интервал времени ожидания, после которого повторно активизированные LLDP-порты начнут передачу пакетов LLDP. По умолчанию 2 секунды.

Проверьте информацию о настройках LLDP:
```
show lldp
```

Что вы наблюдаете? Запишите_____
_____

Настройте на всех портах возможность приема и передачи LLDP пакетов:
```
config lldp ports all admin_status tx_and_rx
```

Включите передачу в оповещениях LLDP информации об IP-адресе управления коммутатора:
```
config lldp ports all mgt_addr ipv4 192.168.1.1 enable
```

Включите передачу в оповещениях основных информационных данных протокола LLDP:
```
config lldp ports all basic_tlvs all enable
```

Включите передачу в оповещениях LLDP информации о 802.1Q (VLAN):
```
config lldp ports all dot1_tlv_vlan_name vlan all enable
```

Проверьте настройку оповещений на портах:
```
show lldp ports 1-24
```

Что вы наблюдаете? Запишите_____
_____

Повторите процедуру настройки для коммутатора 2 и коммутатора 3

На коммутаторе 2 (SW2):

Проверьте полную информацию о портах, используемых для отправки оповещений LLDP:
```
show lldp local_ports 1-24 mode detailed
```

Проверьте расширенную информацию о соседних устройствах:
```
show lldp remote_ports 1-24 mode detailed
```

Что вы наблюдаете? Запишите_____

_____

_____

_____

Отключите кабель, соединяющий коммутатор 1 и коммутатор 2.

Проверьте расширенную информацию о соседних устройствах:
```
show lldp remote_ports 1-24 mode detailed
```

Что вы наблюдаете? Что изменилось? Запишите_____

_____

_____

Отключите протокол LLDP глобально на коммутаторе:
```
disable lldp
```

Проверьте информацию о настройках LLDP:
```
show lldp
```

ПРАКТИЧЕСКАЯ РАБОТА № 37
Основы администрирования межсетевого экрана

Цель

Рассмотрим общие вопросы администрирования межсетевого экрана.

1. Вход с использованием различных интерфейсов в консоль управления межсетевым экраном.
2. Перезапуск межсетевого экрана, сброс к заводским настройкам по умолчанию, установка даты и времени, DNS, активация и применение изменений.
3. Сброс и загрузка новой конфигурации устройства, автоматическое обновление ПО.
4. Поиск неисправностей.

Описание практической работы

Управление межсетевым экраном с помощью различных интерфейсов

Доступ к межсетевому экрану с рабочей станции

Новому межсетевому экрану D-Link NetDefend с заводскими настройками по умолчанию система NetDefendOS автоматически назначает внутренний IP-адрес по умолчанию на интерфейсе **`lan1`** (или интерфейс **`lan`** на моделях с одним локальным интерфейсом). IP-

адрес, назначаемый интерфейсу управления, зависит от модели межсетевого экрана NetDefend:

- Для моделей межсетевых экранов NetDefend DFL-210, 260, 800, 860, 1600 и 2500, IP-адрес интерфейса управления, назначаемый по умолчанию - **`192.168.1.1`**.
- Для моделей межсетевых экранов NetDefend DFL-1660, 2560, 2560G и 260E/860E, IP-адрес интерфейса управления, назначаемый по умолчанию - **`192.168.10.1`**.

IP-адреса интерфейса межсетевого экрана, который соединен с рабочей станцией, и интерфейс самой рабочей станции, которая должна выполнять управление межсетевым экраном, должны быть в одной и той же сети. Поэтому интерфейсу рабочей станции вручную должен быть назначен статический IP-адрес из подсети 192.168.1.0/24 и основной шлюз 192.168.1.1:

IP-адрес: 192.168.1.30

Маска подсети: 255.255.255.0

Основной шлюз: 192.168.1.1

Веб-интерфейс

Система NetDefendOS предоставляет *веб-интерфейс* (WebUI) для управления системой с помощью стандартного веб-браузера.

Первоначальная регистрация в веб-интерфейсе и Мастер установки

Для первоначального доступа к веб-интерфейсу межсетевого экрана с заводскими настройками по умолчанию следует использовать URL **`https://192.168.1.1`**.

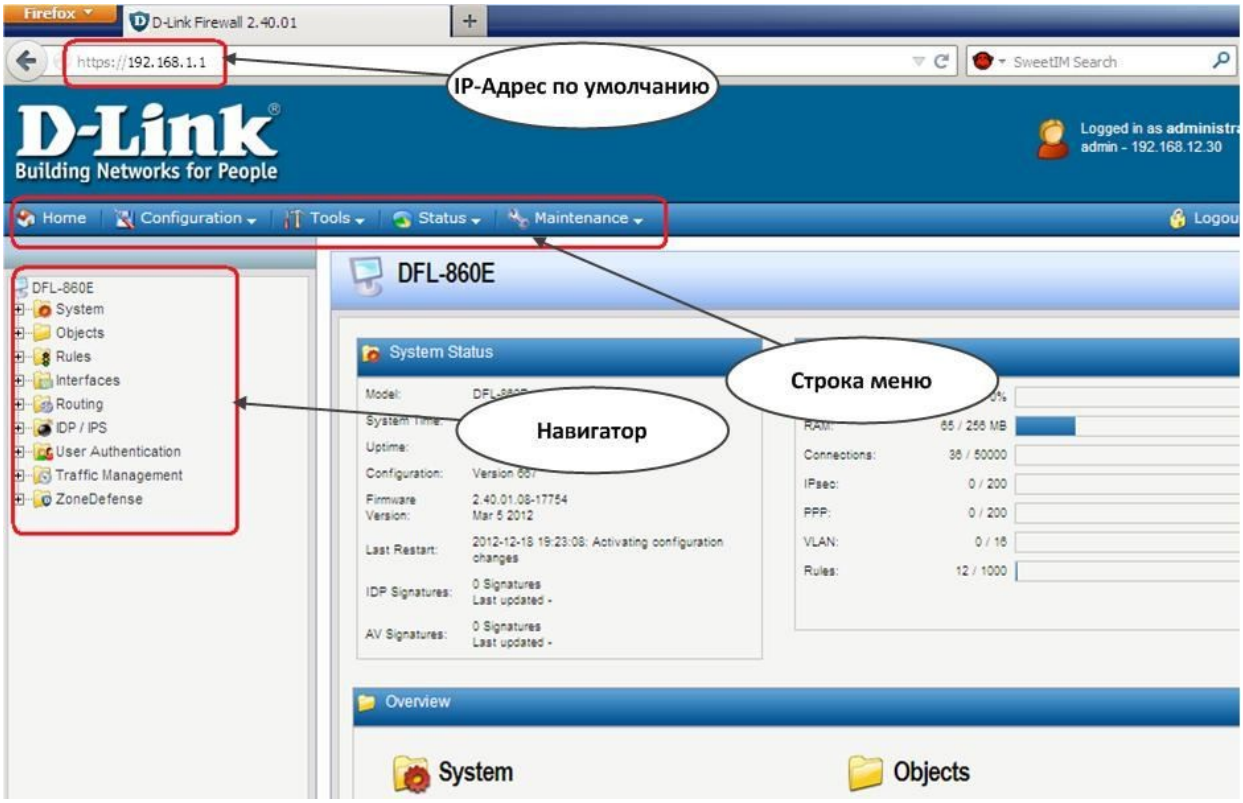
После этого появится диалоговое окно аутентификации пользователя.

Имя пользователя по умолчанию – **`admin`,** пароль по умолчанию – **`admin`.**

Диалоговое окно регистрации в веб-интерфейсе предоставляет возможность выбрать язык интерфейса. Поддержка языка реализована с помощью набора ресурсных файлов.

Если изменения в настройках не были сделаны, запускается Мастер установки, и администратор может выполнить все необходимые шаги по установке публичного доступа к интернет.

Общий вид веб-интерфейса:



Доступ к веб-интерфейсу регулируется настраиваемой политикой удаленного управления. По умолчанию, система разрешает доступ к веб-интерфейсу только из сети, которая подсоединена к интерфейсу **`lan`**. Будем называть эту сеть внутренней.

Строка меню содержит кнопки и выпадающие меню, используемые для редактирования различных настроек, а также для доступа к различным инструментальным средствам и

просмотру текущих статусов соединений, интерфейсов, аутентифицированных пользователей и т.п.

Home – Возврат на главную страницу веб-интерфейса.

Configuration

Save and Actvate – Сохранение и активация настроек.

Discard changes – Отмена изменений в настройках, выполненных во время текущей сессии.

View Changes – Список изменений в настройках с момента последнего сохранения.

Tools – Инструментальные средства, необходимые для обслуживания системы.

Status – Текущие статусы, используемые для диагностики текущего состояния системы.

Maintenance – Обслуживание.

Update Center – Обновление сигнатур антивируса и определения вторжений, которое может выполняться как вручную, так и по расписанию.

License – Просмотр лицензии и ввод кода активации.

Backup – Создание резервной копии настроек на рабочей станции и восстановление предварительно созданной резервной копии.

Reset – Перезапуск межсетевого экрана или сброс к заводским настройкам по умолчанию.

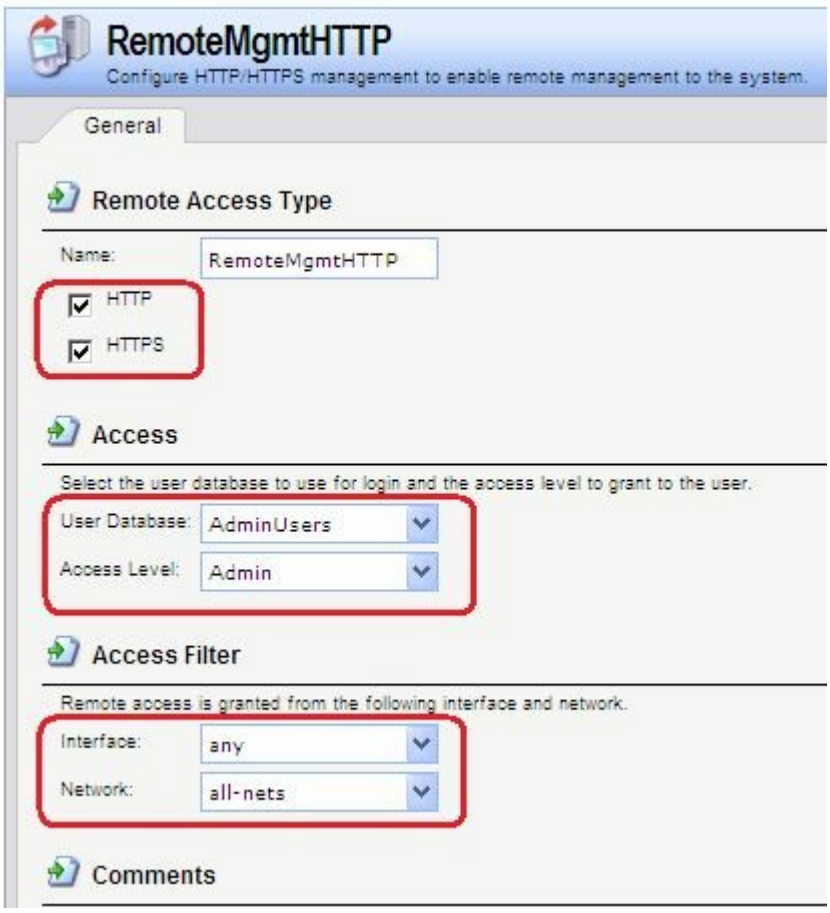
Upgrade – Обновление программного обеспечения межсетевого экрана.

Technical support – Создание на рабочей станции файла, содержащего различные статистические данные о работе межсетевого экрана. Этот файл может быть изучен локально или отправлен специалисту технической поддержки для оказания помощи в исследовании проблемы. Это является крайне важным, так как автоматически собираемая информация содержит множество деталей, которые требуются при поиске и устранении неисправностей.

По умолчанию, доступ к веб-интерфейсу открыт только из внутренней сети. Если необходимо включить доступ с других интерфейсов, кроме интерфейса **lan**, требуется изменить политику удаленного управления.

Веб-интерфейс:

System → Remote Management → Add → HTTP/HTTPS Management



Командная строка:

```
add RemoteManagement RemoteMgmtHTTP https Network=all-nets Interface=any
LocalUserDatabase=AdminUsers HTTPS=Yes
```

После завершения работы необходимо выйти из веб-интерфейса, чтобы предотвратить доступ других пользователей к межсетевому экрану. Выход из системы осуществляется нажатием кнопки **`Logout`**, расположенной справа в строке меню.

Интерфейс командной строки CLI

Система NetDefendOS предоставляет *интерфейс командной строки (CLI)*, который доступен локально через серийный консольный порт (соединение с которым описывается ниже) или удаленно через один из интерфейсов межсетевого экрана с помощью клиента протокола *Secure Shell* (SSH).

CLI предоставляет набор команд, обеспечивающих отображение и изменение настроек, а также отображение работы системы и выполнение задач по обслуживанию системы.

Наиболее часто используемые команды CLI:

- **`add`** – Добавление объекта, например, IP-адреса или правила в настройки межсетевого экрана.
- **`set`** – Изменение какого-либо свойства объекта.
- **`show`** – Отображение текущих категорий или значений объекта.
- **`delete`** – Удаление объекта.

Структура команд

Большинство команд имеют следующую структуру:

```
<command> [<object_category>] <object_type> <object_name>
[<object_properties>]
```

Например, для отображения IP-адреса объекта **my_address** используется команда:

```
gw-world:/> show Address IP4Address my_address
```

Все настраиваемые сущности (IP-адреса, интерфейсы, правила фильтрования и маршрутизации и т.п.) межсетевого экрана называются объектами. Каждый объект принадлежит определенному типу (**IP4Address**, **Ethernet**, **IPsecTunnel**, **IPRule**, **RoutingRule** и т.п.). Несколько типов могут быть сгруппированы в категорию (**Address**, **Interface**, **Settings** и т.п.).

Команда

```
gw-world:/> help help
```

выводит справочную информацию о системе.

История команд

Навигация по списку использованных команд в интерфейсе командной строки выполняется с помощью клавиш «стрелка вниз» и «стрелка вверх» (аналогично консоли в большинстве версий Microsoft Windows™ и UNIX™). Например, нажатие клавиши «стрелка вверх» вызовет появление последней выполненной команды в текущей строке CLI. После этого ее можно отредактировать и выполнить.

Функция Tab Completion

Система NetDefendOS предоставляет возможность, которая называется *tab completion.* Нажатие клавиши **tab** вызовет автоматическое завершение текущего идентификатора. Если однозначное завершение невозможно, то нажатие клавиши **tab** приведет к автоматическому отображению возможных завершений или опций команды.

Возможность tab completion можно также использовать для автоматического заполнения параметров команды значениями по умолчанию. Для этого в качестве значения следует ввести символ "." и нажать клавишу **tab**. Например, если при наборе незаконченной команды:

```
set Address IP4Address lan_ip Address=
```

ввести "." и нажать клавишу **tab**, то отобразится текущее значение параметра **Address**. Если данным значением является, например, **10.6.58.10** будет автоматически создана следующая команда:

```
set Address IP4Address lan_ip Address=10.6.58.10
```

После этого ее можно при необходимости отредактировать и выполнить.

Категории объектов

Ранее упоминалось, что объекты группируются по *типу*, например, **IP4Address**. Типы могут группироваться по *категориям*. Тип **IP4Address** принадлежит категории **Address**. При использовании в категориях функция tab completion применяется для поиска типа объекта, который необходимо использовать.

При вводе команды, например **add**, и нажатии клавиши **tab**, отображаются доступные для использования с этой командой категории. После выбора категории и повторного нажатия клавиши **tab**, будут отображены все типы объектов для данной категории.

Не все типы объектов принадлежат категориям. В этом случае после ввода команды и нажатия **tab** будет появляться список возможных типов объектов.

Выбор категории объектов

Для некоторых команд сначала с помощью команды **cc** необходимо указать категорию и экземпляр, прежде чем отдельные объекты могут создаваться или редактироваться. Это касается, например, правил маршрутизации или фильтрования. Если существует более одной таблицы маршрутизации, для добавления или изменения маршрута необходимо использовать команду **cc** для указания используемой таблицы маршрутизации.

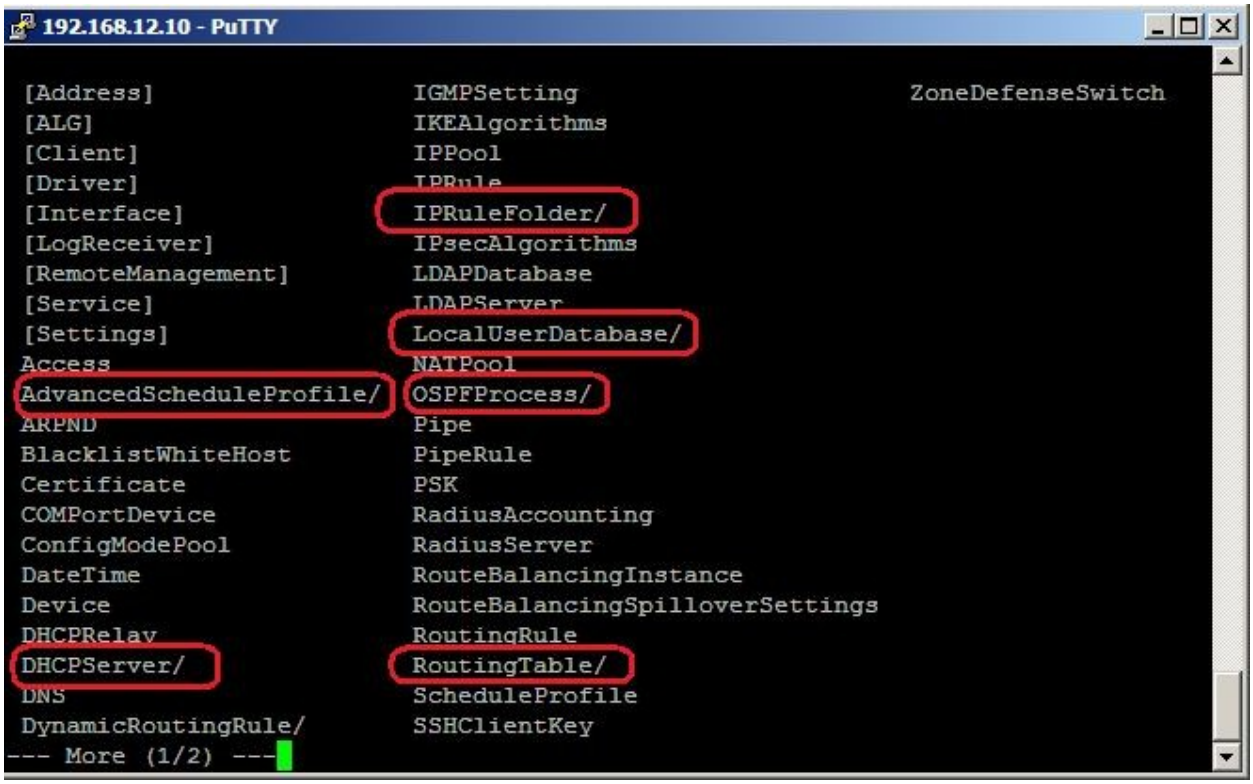
```
gw-world:/> cc RoutingTable main
gw-world:/main>
```

Обратите внимание, что приглашение изменяется. Теперь можно добавить маршрут:

```
gw-world:/main> add Route Name=new_route1 Interface=lan Network=lannet
```

Для отмены указания текущей категории следует использовать команду **cc** без параметров.

В категориях, в которых перед созданием или редактированием объектов требуется указать экземпляр с помощью команды **cc**, в списке, показываемом командой **show**, после имени категории следует символ «/».



Определение нескольких значений параметров

Иногда параметр команды может иметь несколько значений. Эти значения должны разделяться запятой. Например:

```
AccountingServers=server1,server2,server3
```

Добавление нового правила в список правил

Порядок правил в списке, например, набор правил фильтрования, является важным. По умолчанию новое правило добавляется в конец списка. Если упорядоченность важна, то может быть добавлен параметр **Index=<Номер позиции в списке правил>**.

Использование уникальных имен

Для удобства рекомендуется назначать всем объектам уникальные имена, чтобы эти имена можно было использовать в качестве ссылки на объект. Это особенно часто используется при написании сценариев.

Имена должны быть уникальными в пределах одного типа объекта. По причинам совместимости с более ранними выпусками NetDefendOS существует исключение, связанное с IP-правилами, у которых могут быть двойные имена, тем не менее, рекомендуется избегать этого. Если дублированное имя IP-правила используется в двух IP-правилах, в таком случае только значение **`Index`** может однозначно определить каждое IP-правило в командах. Ссылка на IP-правило с дублированным именем приведет к сообщению об ошибке.

Использование dns-имени вместо IP-адреса

В некоторых командах адрес в виде dns-имени, а не IP-адреса. В этом случае перед именем должен стоять префикс **`dns:`**, указывающий на то, что необходимо использовать сервис DNS для поиска IP-адреса по имени хоста. Например, dns-имя **`host.company.com`** следует указывать в командной строке как **`dns:host.company.com`**.

Параметры, в которых могут употребляться dns-имена в командной строке:

- Удаленная конечная точка для IPsec-, L2TP- и PPTP-туннелей.
- Хост для LDAP-серверов.

Если необходимо использовать сервис DNS, то следует настроить хотя бы один DNS-сервер, который будет выполнять преобразования dns-имена в IP-адреса.

Локальный доступ к интерфейсу командной строки

Серийный порт консоли – это порт RS-232 межсетевого экрана NetDefend, обеспечивающий локальный доступ к интерфейсу командной строки. Порт RS-232 существует на старших моделях DFL 1660/2560. На новых младших моделях DFL консольный порт выполнен в виде Ethernet-разъема.

Доступ к интерфейсу командной строки по протоколу SSH (Secure Shell)

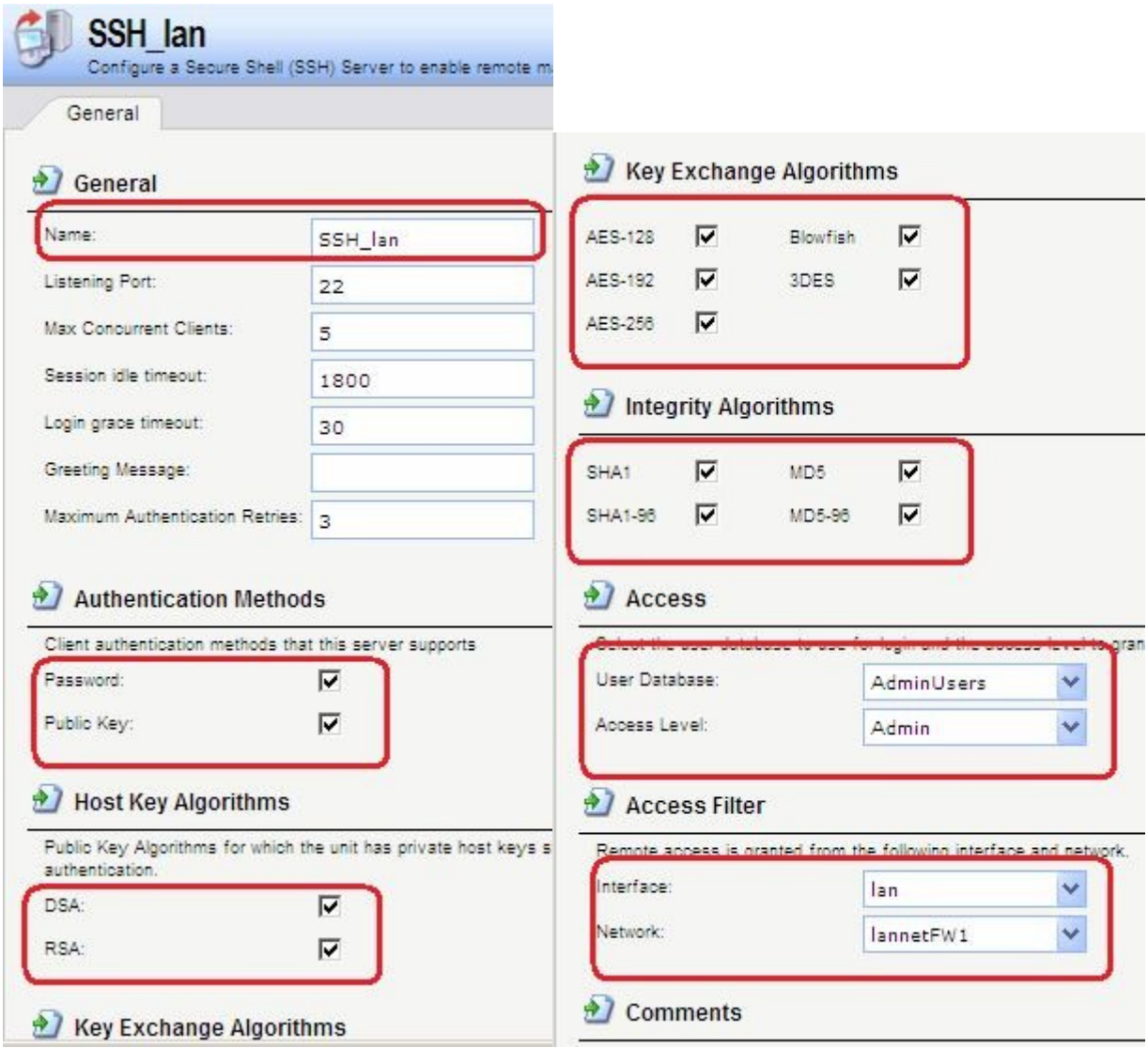
Протокол SSH (Secure Shell) используется для доступа к интерфейсу командной строки с удаленной рабочей станции. Протокол SSH обеспечивает безопасные коммуникации по незащищенным сетям, а также сильную аутентификацию обеих сторон. SSH-клиенты доступны для большинства платформ.

Система NetDefendOS поддерживает версии 1, 1.5 и 2 протокола SSH. Разрешение доступа по протоколу SSH предоставляется с помощью политики удаленного управления, и по умолчанию разрешения доступа по протоколу SSH нет.

Веб-интерфейс:

`System > Remote Management > Add > Secure Shell Management`

`Name: SSH_lan`



Командная строка:

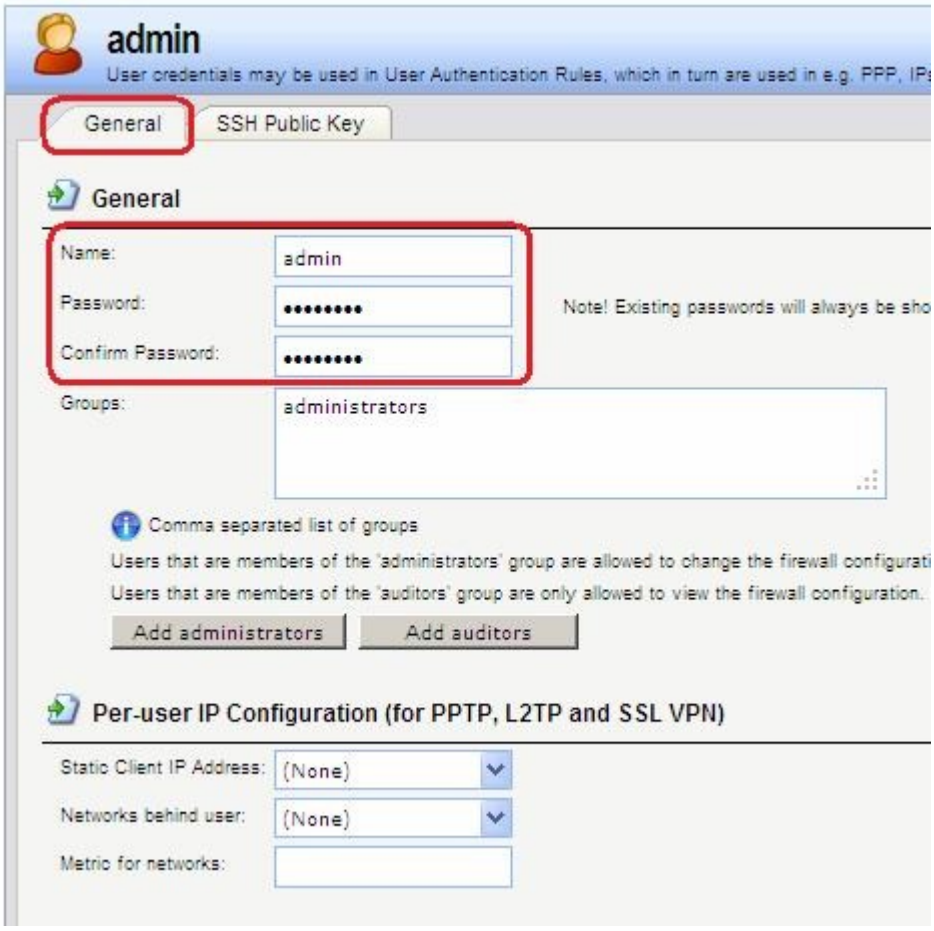
```
add RemoteManagement RemoteMgmtSSH ssh Network=lannetFW1 Interface=lan LocalUserDatabase=AdminUsers
```

Изменение пароля пользователя admin

После первоначального запуска рекомендуется как можно скорее изменить пароль по умолчанию **admin** на любой другой. Пароль пользователя может быть любой комбинацией символов и не может содержать более 256 символов.

Веб-интерфейс:

User Authentication → Local User Databases → AdminUsers



Командная строка:

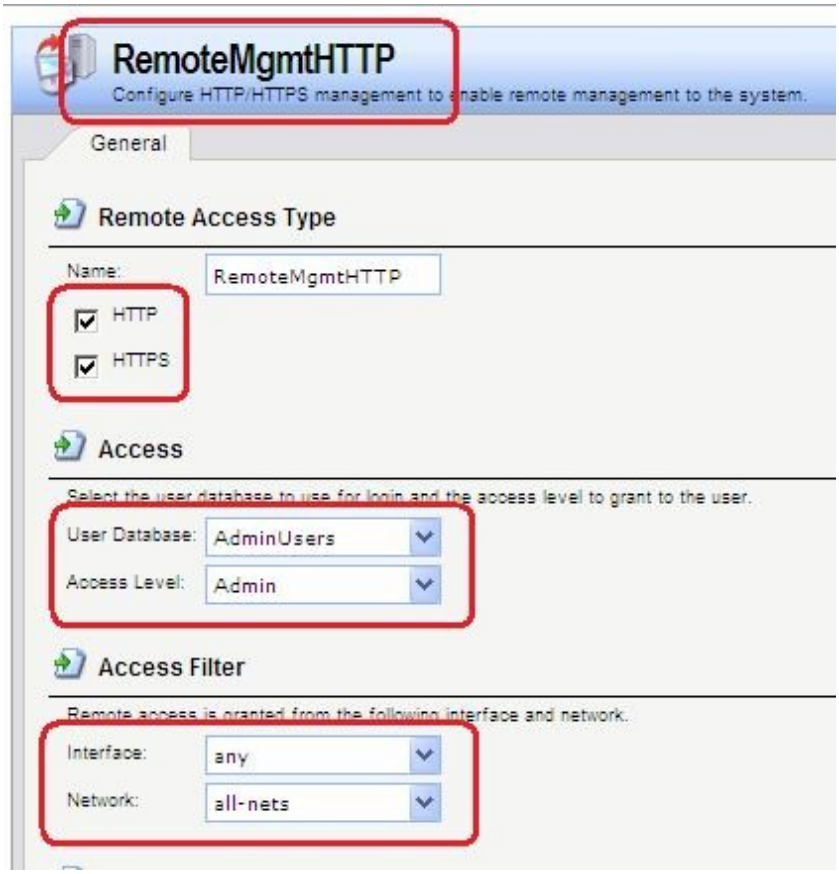
```
cc LocalUserDatabase AdminUsers
set User admin Password=admin
```

Учетные записи для администрирования межсетевого экрана

Для администрирования межсетевого экрана используются учетные записи пользователей, которые хранятся в локальной базы данных.

По умолчанию имеется локальная база данных **`AdminUsers`**, которая содержит учетную запись **`admin`**. Пароль данной учетной записи – **`admin`**.

Какая именно база данных используется для хранения учетных записей администраторов межсетевого экрана и с каких интерфейсов и сетей возможно администрирование, определяется конфигурационными параметрами.



Для управления межсетевым экраном определены две группы: **`Administrators`** и **`Auditors`**.

Учетные записи, принадлежащие группе **`Administrators`**, обладают правами по чтению и записи всех настроек межсетевого экрана.

Учетные записи, принадлежащие группе **`Auditors`**, обладают только правами по чтению всех настроек межсетевого экрана.

Если требуется, можно создать дополнительные учетные записи для администрирования межсетевого экрана, указав какой из групп принадлежат создаваемые учетные записи.

Система NetDefendOS запрещает одновременный вход более одной учетной записи с правами администратора. Если выполнен вход под одной учетной записью с правами администратора, то вход под второй учетной записи возможен, но при этом предоставляются права только аудита. Другими словами, вторая учетная запись будет обладать только правами чтения настроек без возможности их изменения.

Сценарии командной строки

Для простоты хранения и выполнения команд администратором, NetDefendOS поддерживает функцию *CLI scripting*. *CLI script* – это записанная в файл последовательность команд, которые можно выполнить после загрузки файла на межсетевой экран.

Для создания CLI script следует выполнить следующие шаги:

1. Создать текстовый файл, содержащим последовательность команд, по одной команде в строке. Для этих файлов рекомендуется использовать расширение **.sgs** (S*ecurity* G*ateway* S*cript*). Имя файла, включая расширение, не должно содержать более 16 символов.
2. Загрузить файл на межсетевой экран, используя Secure Copy (SCP). Файлы-сценарии должны храниться в папке **scripts**.
3. Использовать команду CLI **script -execute** для выполнения команд из файла.

Команда **script** – это инструментальное средство, используемое для выполнения определенной последовательности команд. Полный синтаксис команды описан в *Руководстве по интерфейсу командной строки CLI. Р*ассмотрим некоторые примеры использования данной команды.

В сценариях можно использовать следующие четыре команды: **add, set, delete, cc.**

Если в сценарии появляется любая другая команда, она игнорируется, при этом генерируется сообщение с предупреждением. Например, команда **ping** будет проигнорирована.

С помощью команды **script -execute** запускается указанный в параметре **–name** файл сценария.

```
script -execute -name=my_script.sgs
```

Файл сценария может содержать любое количество *переменных сценария,* которые обозначаются следующим образом:

```
$1, $2, $3, $4   $n
```

Фактические параметры этих переменных указываются в командной строке **script -execute**.

Если в выполняемом файле сценария возникает ошибка, то по умолчанию сценарий будет прерван. С помощью опции **–force** сценарий будет продолжен даже при возникновении ошибки.

```
script -execute -name=my_script2.sgs -force
```

Все выходные данные выполненного сценария появляются в консоли командной строки. По умолчанию эти выходные данные состоят из сообщений обо всех ошибках, которые произошли во время выполнения. Для вывода на консоль подтверждения выполнения каждой команды используется опция **–verbose.**

```
script -execute -name=my_script2.sgs -verbose
```

При загрузке файла сценария на межсетевой экран, сначала он хранится только в памяти RAM. При перезапуске NetDefendOS все загруженные сценарии будут уничтожены в энергозависимой памяти, и для их следующего выполнения потребуется повторная загрузка. Для сохранения сценариев после перезапусков следует переместить их в энергонезависимую память с помощью команды **script -store**.

```
script  -store   -name=my_script.sgs
```

Если требуется переместить в энергонезависимую память все сценарии, то используется команда.

```
script -store -all
```

Для удаления сценария используется команда **script –remove**.

Команда **script** без параметров отображает список всех сценариев, размер каждого сценария и тип памяти, в которой хранится сценарий (**Disk** или **Memory**).

Для вывода на консоль содержимого файла сценария используется команда.

script -show -name=<имя файла>

Автоматическое создание сценариев

Когда необходимо выполнить создание одних и тех же объектов конфигурации на нескольких межсетевых экранах, следует создать файл сценария и запустить его на каждом устройстве.

Команда

script -create <object_type>

автоматически создает файл сценария, который содержит команду **add** всех объектов указанного типа, существующих в межсетевом экране.

Например, для создания всех объектов **IP4Address** с одними и теми же параметрами на нескольких межсетевых экранах следует выполнить команду.

script -create Address IP4Address -name new_script.sgs

Файл **new_script_sgs** может быть загружен на локальную рабочую станцию и затем скачен и активирован на других межсетевых экранах. После этого у всех устройств в адресных книгах будут находиться одни и те же объекты **IP4Address.**

Некоторые параметры конфигурации, зависящие от аппаратного обеспечения, не могут быть автоматически записаны в сценарий с помощью параметра **-create**.

Строка в файле сценария, которая начинается с символа #, является комментарием.

Сценарии, вызывающие другие сценарии

Один сценарий может вызывать другой. Например, сценарий **my_script.sgs** может содержать строку.

script -execute -name my_script2.sgs

Максимальное количество вложенных сценариев – 5.

Дата и время

Обзор

Корректная установка даты и времени важны для правильной работы системы межсетевого экрана. Политики по расписанию, авто-обновления IDP и баз данных антивируса, а также других функций продукта требуется точно установленное системное время.

Кроме того, сообщения журнала отмечаются временной меткой для того, чтобы указать, когда произошло определенное событие. Кроме того, время должно быть синхронизировано с другими устройствами в сети.

Протоколы синхронизации времени

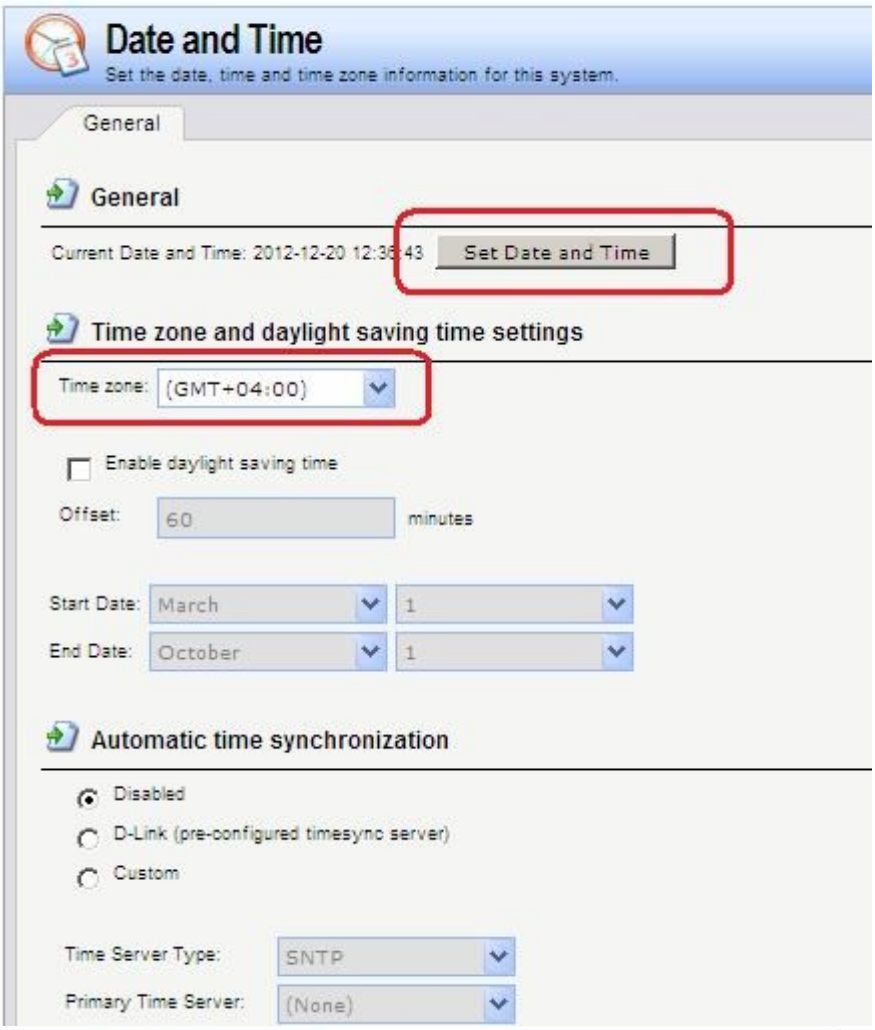
Поддерживается использование протоколов синхронизации времени для автоматической регулировки системных часов с помощью ответов на запросы, отправляемые через интернет, на специальные внешние серверы, которые называют сервера времени (Time Servers).

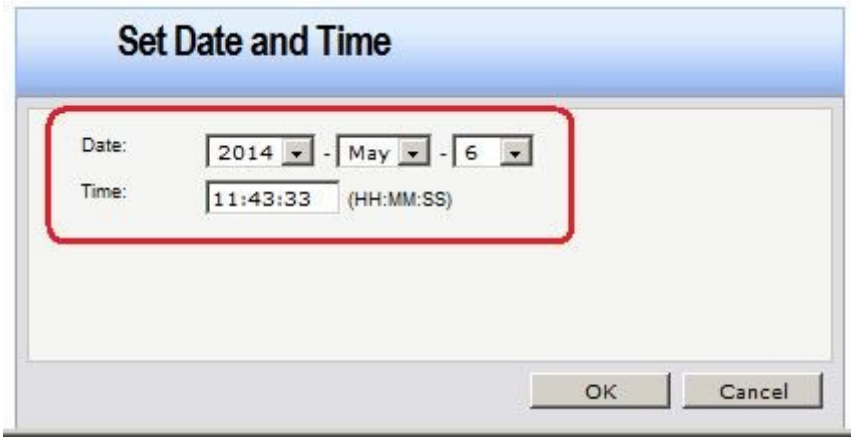
Установка даты и времени и установка часового пояса

Установить дату и время можно вручную, это рекомендуется при первоначальном запуске системы.

Веб-интерфейс:

`System → Date and Time`





Командная строка:

`time -set YYYY-mm-DD HH:MM:SS`

`set DateTime Timezone=GMTplus4`

Серверы времени (Time Servers)
Для корректировки аппаратных часов используются сервера времени, с помощью которых возможна автоматическая настройка времени, полученного от одного или нескольких серверов, которые предоставляют точное время.

Поддерживаются следующие протоколы синхронизации времени:

- **SNTP**

Определяется стандартом RFC 2030, простой сетевой протокол синхронизации времени – реализация NTP (RFC 1305). NetDefendOS использует данный протокол для запросов к NTP-серверам.

- **UDP/TIME**

Протокол времени - Time Protocol (UDP/TIME) – более ранний протокол, также обеспечивающий синхронизацию времени через интернет.

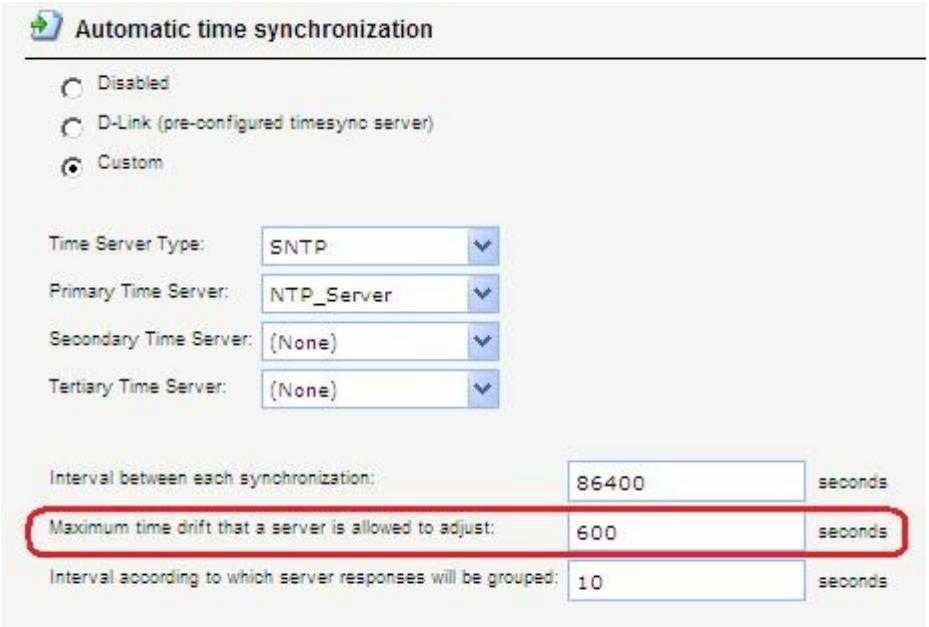
Большинство серверов времени поддерживают NTP или SNTP-протоколы.

Могут быть указаны максимально три сервера времени. Если используется более одного сервера для синхронизации времени, то можно избежать ситуации. Когда синхронизация невозможна из-за недоступности одного из серверов. Система получает информацию со всех доступных серверов и вычисляет среднее время.

Максимальная величина корректировки времени
Чтобы избежать установления некорректного времени, которое может произойти при синхронизации с неисправным сервером, можно установить максимальную величину корректирования времени (*Maximum Adjustment)* (в секундах). Если разница между текущим временем системы и временем, полученным с сервера, будет больше заданной максимальной величины, то данные, полученные с сервера, будут отклонены. Например, значение максимального времени установки равно 60 секунд и текущее время системы NetDefendOS составляет 16:42:35. Если время, полученное с сервера: 16:43:38, то разница составляет 63 секунды, что превышает максимальную величину, т.е. текущее время не будет обновлено.

Веб-интерфейс:

`System → Date and Time`



Командная строка:

```
set DateTime TimeSyncMaxAdjust=40000
```

Значение максимальной регулировки времени можно отключить.

```
time -sync –force
```

При необходимости можно изменить интервал между попытками синхронизации. По умолчанию интервал равен 86 400 секунд (1 день).

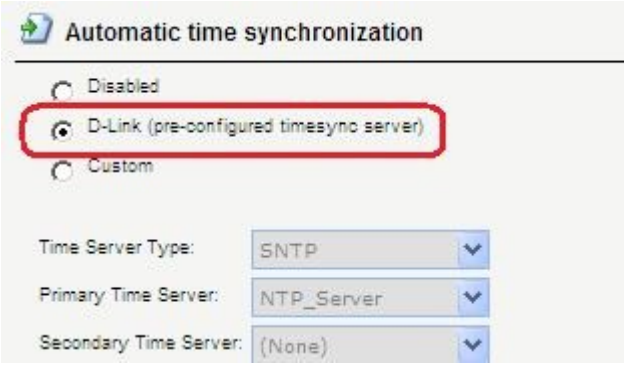
Серверы синхронизации времени D-Link

При работе с системой NetDefendOS для синхронизации времени рекомендуется использовать серверы синхронизации времени D-Link, путь к которым прописан в опциях системы. Серверы D-Link взаимодействуют с системой по протоколу SNTP.

Когда опция D-Link Server включена, синхронизация осуществляется автоматически.

Веб-интерфейс:

System → Date and Time



Командная строка:

```
set DateTime TimeSynchronization=D-Link
```

Следует помнить, что для работы с серверами синхронизации времени D-Link необходимо настроить сервис DNS.

Серверы DNS

Если в системе настроены DNS-сервера, то вместо IP-адреса можно указывать соответствующее доменное (FQDN) имя.

Система NetDefendOS является DNS-клиентом и может использовать три DNS-сервера: Primary Server (первичный сервер), Secondary Server (вторичный сервер) и Tertiary Server (третий сервер).

Настройка хотя бы одного DNS-сервера необходима для функционирования следующих модулей системы NetDefendOS:

- Автоматическая синхронизация времени.
- Доступ к CA для получения сертификатов.
- Доступ к внешним сервисам, содержащим различные базы данных сигнатур, используемые в системе (антивирусные или IDP).

Веб-интерфейс:

System → DNS

Командная строка:

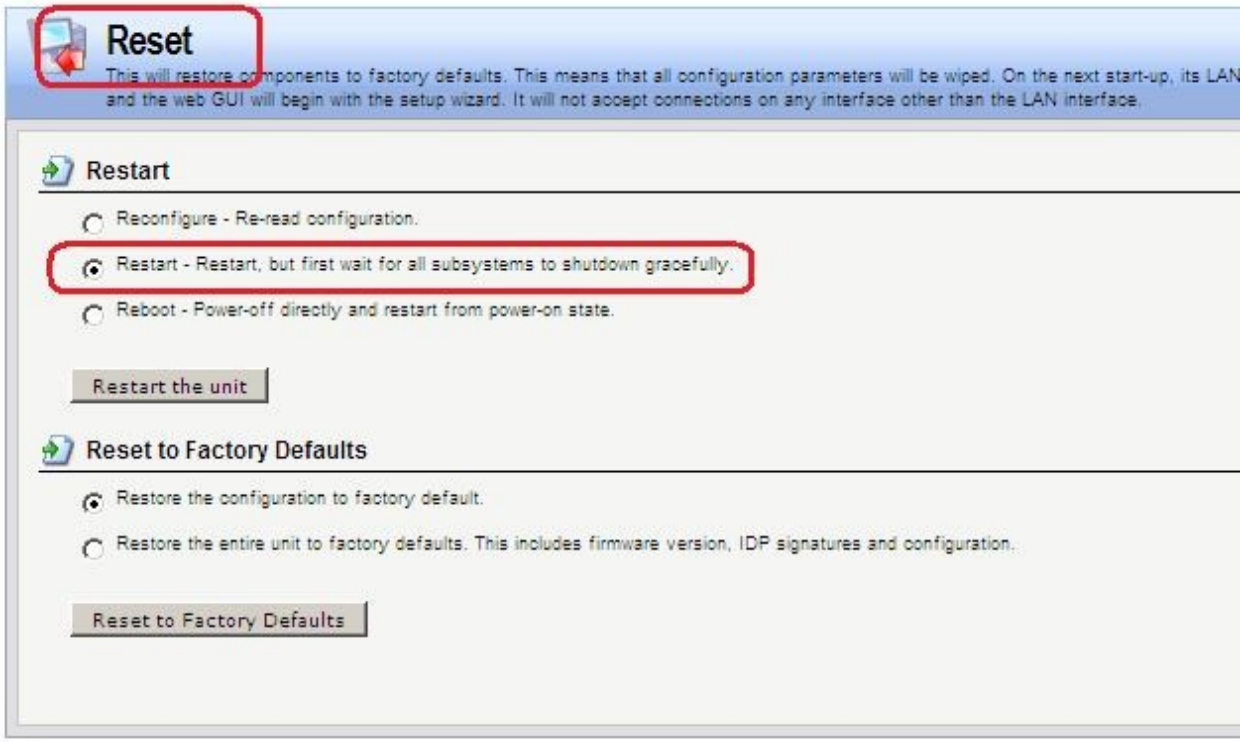
```
set DNS DNSServer1=wan1/wan1_dns1
```

Перезапуск межсетевого экрана, сброс к заводским настройкам по умолчанию

Сброс к заводским настройкам по умолчанию выполняется для возврата к первоначальным настройкам межсетевого экрана. При выполнении сброса настроек все данные, такие, как база данных провайдера и антивирусная база данных, будут утеряны и должны быть повторно загружены.

Веб-интерфейс:

`Maintenance → Reset`



Командная строка:

```
reset -unit
```

Активация и применение изменений

После внесения изменений в конфигурацию следует выполнить команды **`activate`** и **`commit`**.

Если в течение 30 секунд (по умолчанию) не выполнена команда **commit**, выполненные изменения автоматически отменяются, и происходит восстановление прежних настроек.

Управление сессиями с помощью команды ***sessionmanager***

Интерфейс командной строки предоставляет команду **sessionmanager** для управления сессиями. Команда используется для управления всеми типами сессий:

- Сессии командной строки, созданные при использовании протокола SSH.
- Сессия командной строки, созданные через интерфейс серийной консоли RS232.
- Сессии, созданные при использовании протокола Secure Copy (SCP).
- Сессии веб-интерфейса, созданные при использовании протокола HTTP или HTTPS.

Команда без каких-либо опций предоставляет краткую информацию о текущих открытых сессиях. Для просмотра списка всех сессий используется опция **-list**.

Командная строка:

```
sessionmanager
```

```
sessionmanager -list
```

Если пользователь обладает правами администратора, можно завершить любую сессию с помощью опции **-disconnect**.

Поиск неисправностей - команда pcapdump

Важным инструментом диагностики является анализ пакетов, проходящих через интерфейсы межсетевого экрана. Для этого используется команда **pcapdump**, которая позволяет записать поток пакетов, проходящих через интерфейсы, и выполнить фильтрацию этих потоков в соответствии с определенными критериями.

Примеры использования **pcapdump**:

1. Освобождение памяти, использованной командой **pcapdump** и удаление всех файлов, которые были ранее сохранены с помощью команды **pcapdump**.

```
pcapdump –cleanup
```

2. Запись в буфер в оперативной памяти межсетевого экрана всех пакетов, проходящих через интерфейс **lan**. Если интерфейс не указан, то будет выполнен перехват всех пакетов, проходящих через все интерфейсы.

```
pcapdump  -start lan
```

3. Запись всех пакетов, прошедших через интерфейс **lan**, из буфера в оперативной памяти в файл **lan_int.cap**. Данные файлы находятся в корневой папке межсетевого экрана.

```
pcapdump -write lan -filename=lan_int.cap
```

4. Отображение перехваченных пакетов в консоли.

```
pcapdump –show
```

5. Останов перехвата пакетов, проходящих через интерфейс **lan**. Если интерфейс не указан, то будет выполнен останов перехвата пакетов, проходящих через все интерфейсы.

```
pcapdump -stop lan
```

Загрузка выходного файла
После того, как сохранены в файле межсетевого экрана, их следует переписать, например, с помощью программы **scp**, на рабочую станцию.

Для дальнейшего анализа пакетов рекомендуется использовать программу **Wireshark** (ранее известную как *Ethereal*). Данная программа является приложением с открытым исходным кодом и использует библиотеку *Pcap*.

Для получения более подробной информации о программе **Wireshark**, см сайт http://www.wireshark.org.

Практическая работа №38.

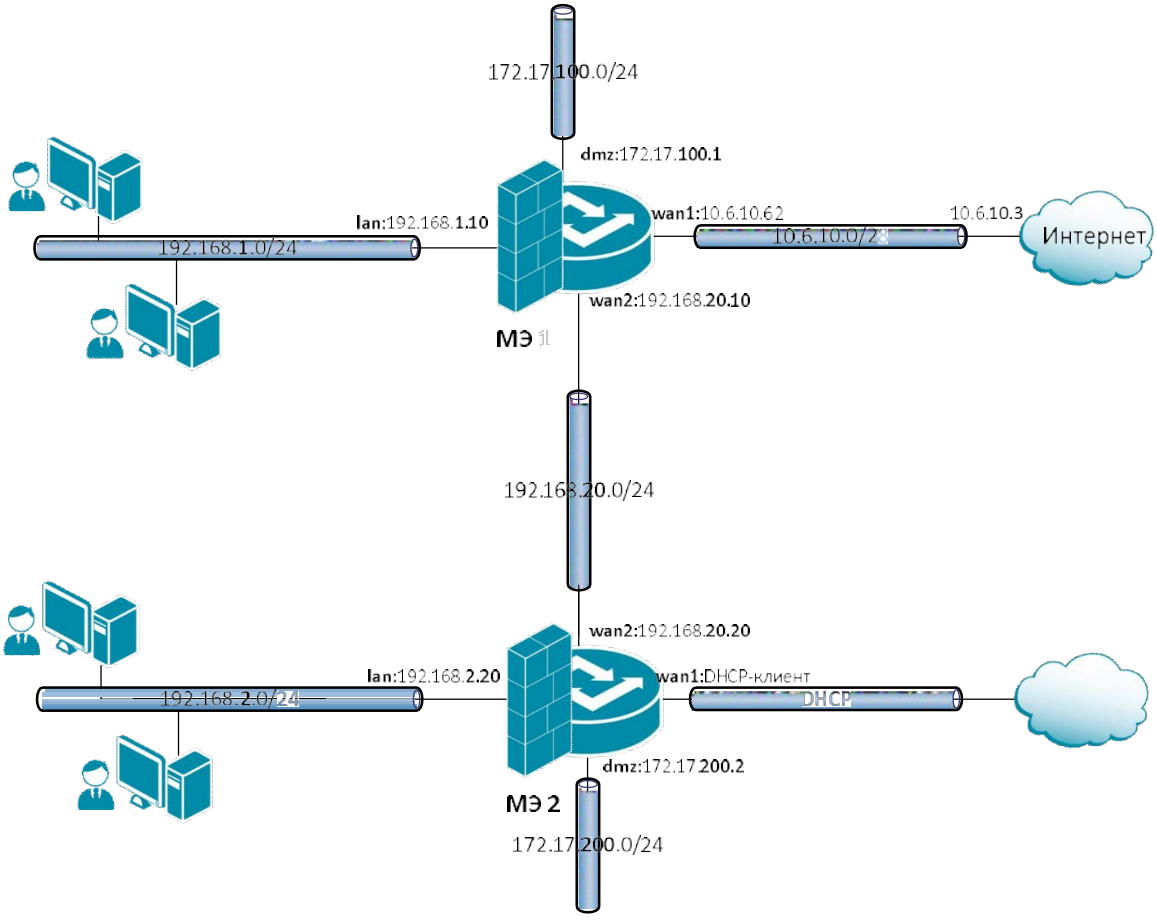
Соединение двух локальных сетей,

расположенных за межсетевыми экранами

Цель
Создать топологию сети, в которой два межсетевых экрана соединяют локальные сети, обеспечивая доступ в локальные сети друг друга и доступ в интернет через одного провайдера.

1. Настроить сервисы DNS на обоих межсетевых экранах.
2. Разрешить доступ из обеих локальных сетей в интернет.
3. Разрешить доступ из локальных сетей к lan-интерфейсам каждого межсетевого экрана и к рабочим станциям в локальных сетях.

Топология сети



Интернет

На Межсетевом Экране 1 (**МЭ 1**) используются четыре интерфейса, которые обозначены **`lan`**, **`dmz`**, **`wan1`** и **`wan2`**.

Интерфейс **lan** имеет IP-адрес 192.168.**1.10** и соединен с подсетью 192.168.**1**.0/24, в которой расположены рабочие станции пользователей.

Интерфейс **dmz** имеет IP-адрес 172.17.**100.1**, в текущей топологии к нему не подсоединена никакая сеть.

Интерфейс **wan1** имеет IP-адрес 10.6.10.62 и соединен с подсетью 10.6.10.0/28 со шлюзом провайдера, который обеспечивает выход в интернет и имеет IP-адрес 10.6.10.3.

Интерфейс **wan2** имеет IP-адрес 192.168.**20.10** и соединен с подсетью 192.168.**20**.0/24, в которой расположен Межсетевой Экран 2 (**МЭ 2**) с IP-адресом 192.168.**20.20**.

На Межсетевом Экране 2 (**МЭ 2**) используются четыре интерфейса, которые обозначены **lan**, **dmz**, **wan1** и **wan2**.

Интерфейс **lan** имеет IP-адрес 192.168.**2.20** и соединен с подсетью 192.168.**2**.0/24, в которой расположены рабочие станции пользователей.

Интерфейс **dmz** имеет IP-адрес 172.17.**200.2**, в текущей топологии к нему не подсоединена никакая сеть.

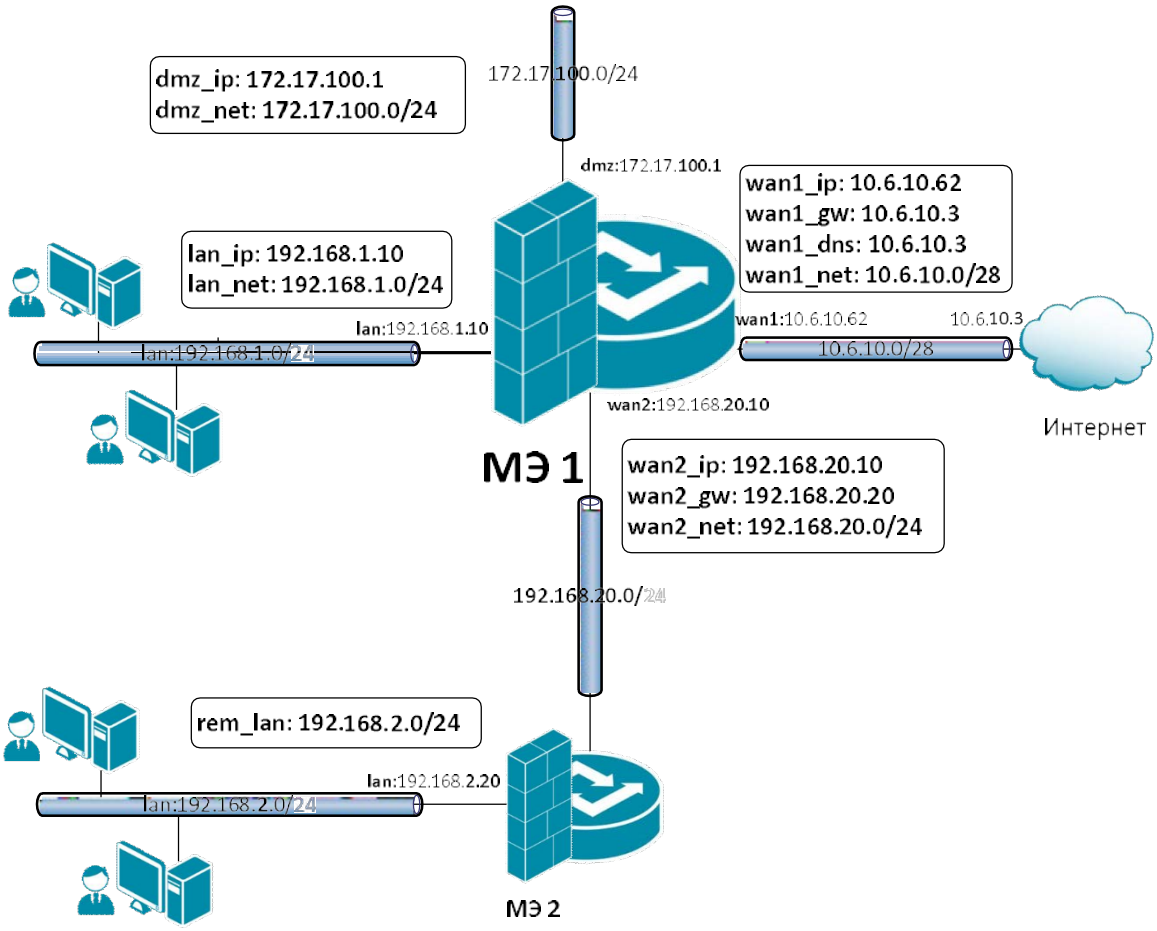
Интерфейс **wan1** является DHCP-клиентом, который получает IP-адрес, маску подсети, шлюз по умолчанию и IP-адрес DNS-сервера от DHCP-сервера провайдера.

Интерфейс **wan2** имеет IP-адрес 192.168.**20.20** и соединен с подсетью 192.168.**20**.0/24, в которой расположен Межсетевой Экран 1 (**МЭ 1**) с IP-адресом 192.168.**20.10**.

Описание практической работы

Сервисы DNS

Межсетевой Экран 1



На МЭ1 весь DNS-трафик из своей локальной сети и удаленной локальной сети должен перенаправляться на DNS-сервер провайдера, поэтому Межсетевой Экран 1 должен знать IP-адрес DNS-сервера провайдера. Необходимо выполнить следующие настройки:

1. В Адресной Книге создать необходимые объекты.
2. Для удобства конфигурирования объединить в одну группу интерфейсы, которые требуют одинаковых Правил фильтрования.
3. Создать Правила фильтрования, перенаправляющие DNS-трафик из локальной сети и dmz-сети к DNS-серверу.
4. При необходимости в таблицу маршрутизации добавить маршруты.

Объекты Адресной Книги

В Адресной Книге создать необходимые объекты.

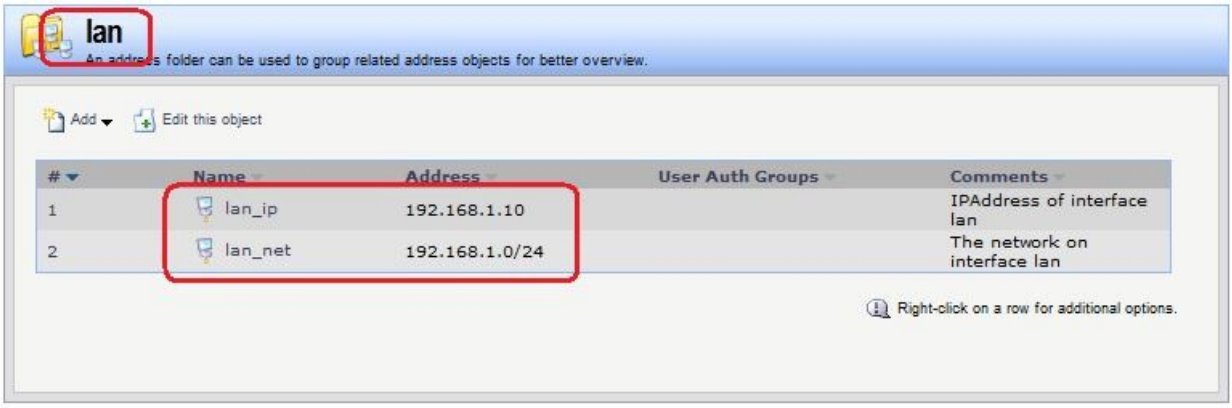
1. Объекты интерфейса **lan**.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: lan

Object → Address Book → lan



Командная строка:

```
add Address AddressFolder lan Comments=lan
cc Address AddressFolder lan
add IP4Address lan_ip Address=192.168.1.10 Comments='IPAddress of interface lan'
add IP4Address lan_net Address=192.168.1.0/24 Comments='The network on interface lan'
```

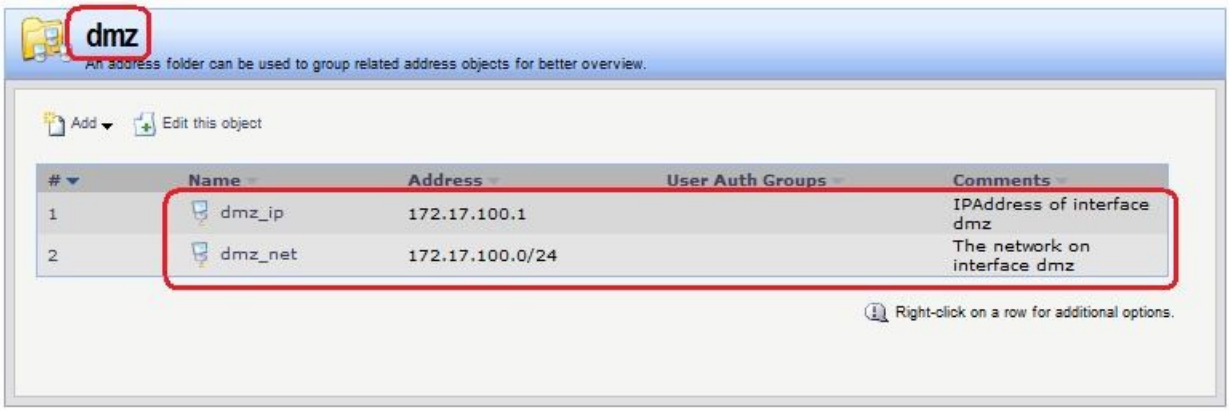
2. Объекты интерфейса **dmz**.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: dmz

Object → Address Book → lan



Командная строка:

```
add Address AddressFolder dmz Comments=dmz
cc Address AddressFolder dmz
add IP4Address dmz_ip Address=172.17.100.1 Comments='IPAddress of interface dmz'
add IP4Address dmz_net Address=172.17.100.0/24 Comments='The network on interface dmz'
```

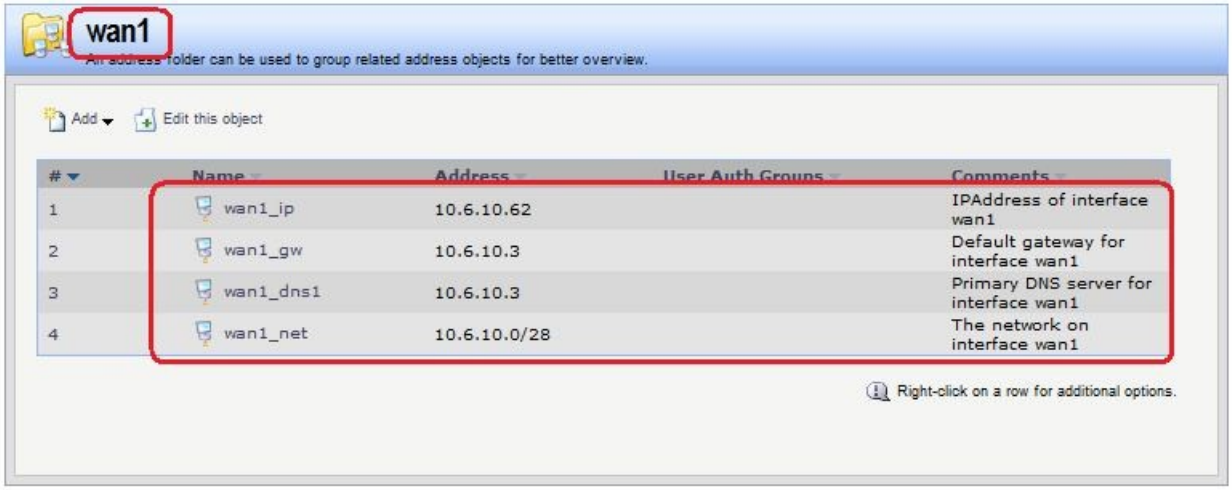
3. Объекты интерфейса **wan1**.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: wan1

Object → Address Book → wan1



Командная строка:

```
add Address AddressFolder wan1 Comments=wan1
cc Address AddressFolder wan1
add IP4Address wan1_ip Address=10.6.10.62 Comments='IPAddress of interface wan1'
add IP4Address wan1_gw Address=10.6.10.3 Comments='Default gateway for interface wan1'
add IP4Address wan1_dns1 Address=10.6.10.3 Comments='Primary DNS server for interface wan1'
add IP4Address wan1_net Address=10.6.10.0/28 Comments='The network on interface wan1'
```

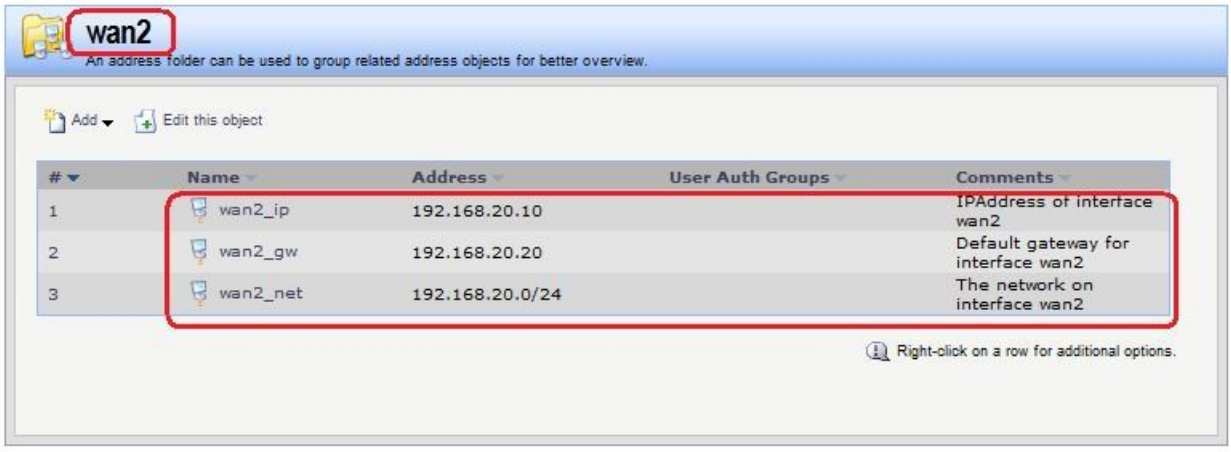
4. Объекты интерфейса **wan2**.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: wan2

Object → Address Book → wan2



Командная строка:

```
add Address AddressFolder wan2 Comments=wan2
cc Address AddressFolder wan2
```

add IP4Address wan2_ip Address=192.168.20.10 Comments='IPAddress of interface wan2'

add IP4Address wan2_gw Address=192.168.20.20 Comments='The network on interface wan2'

add IP4Address wan2_net Address=192.168.20.0/24 Comments='The network on interface wan2'

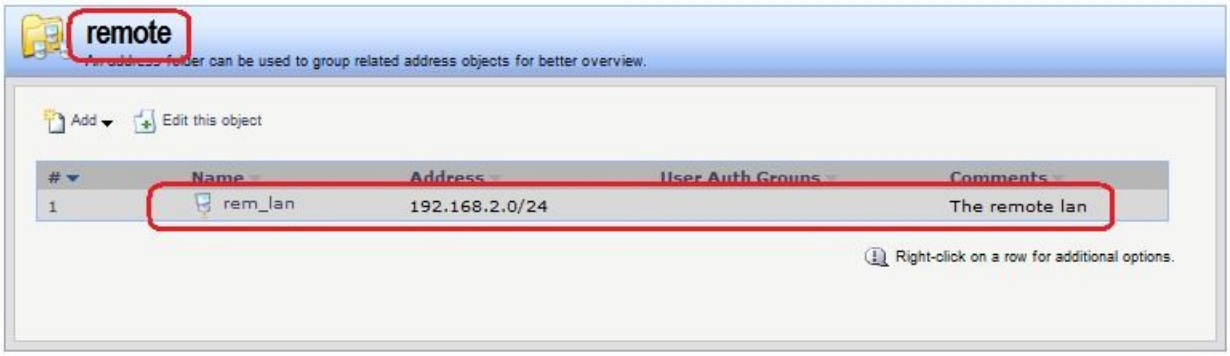
5. Объекты, описывающие LAN-сеть, расположенную за МЭ 2.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: remote

Object → Address Book → rem_lan



Командная строка:

add Address AddressFolder remote Comments='The remote objects'

cc Address AddressFolder remote

add IP4Address rem_lan Address=192.168.2.0/24 Comments='The remote lan'

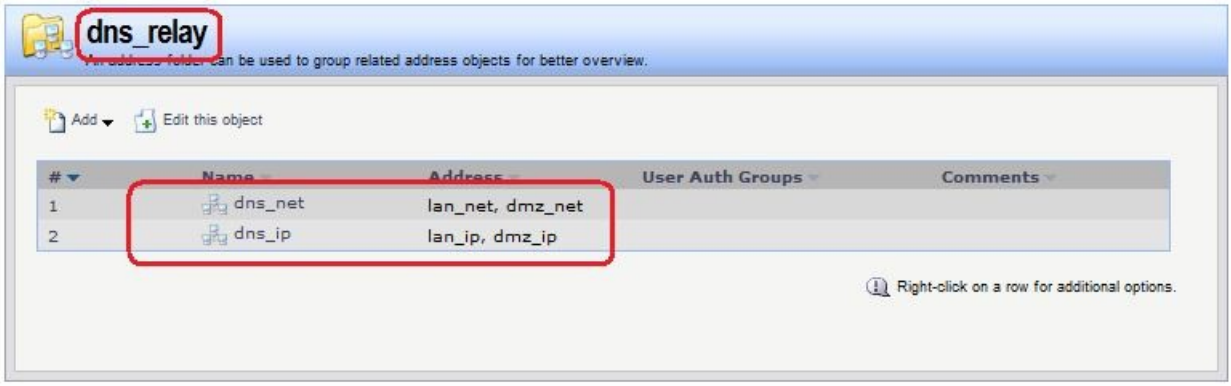
6. Дополнительные объекты, необходимые для удобства администрирования и объединяющие в одну группу сети и IP-адреса, которые необходимы одинаковые сервисы DNS.

Веб-интерфейс:

Object → Address Book → InterfaceAddresses → Add

add Address AddressFolder dns_relay Comments='DNS services'

cc Address AddressFolder dns_relay



Командная строка:

add Address AddressFolder dns_relay Comments='DNS services'

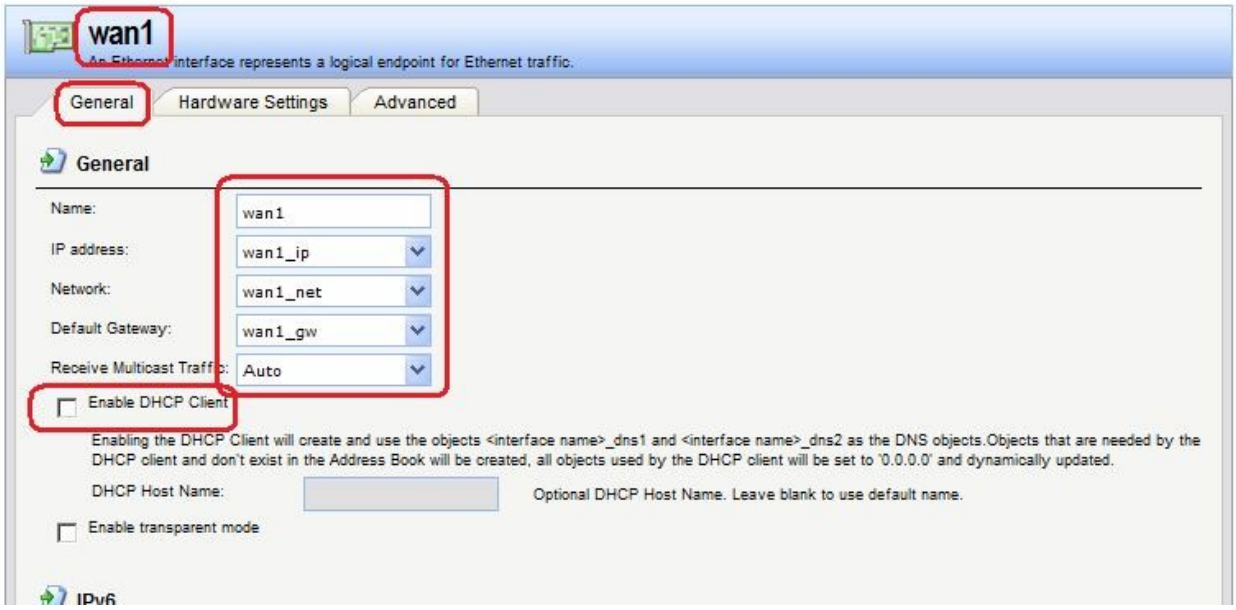
cc Address AddressFolder dns_relay

```
add IP4Group dns_net Members =lan/lan_net, dmz/dmz_net
add IP4Group dns_ip Members = lan/lan_ip, dmz/dmz_ip
```

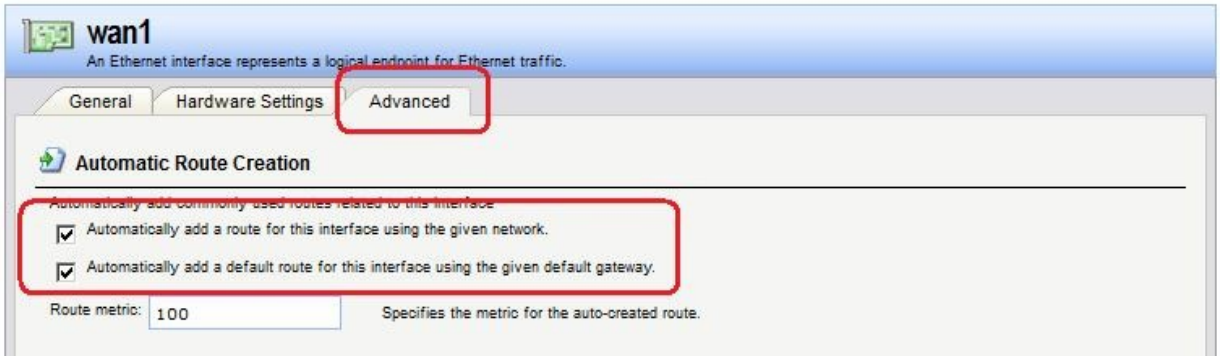
Привязка созданных объектов Адресной Книги к интерфейсам
Объекты, созданные в пунктах 1, 2, 3 и 4, должны быть привязаны к соответствующим Ethernet-интерфейсам.

Веб-интерфейс:

`Interfaces → Ethernet → wan1`



Если IP-адрес данного интерфейса должен быть получен по протоколу DHCP, то следует установить соответствующий флаг «**`Enable DHCP Client`**».



На вкладке **`Advanced`** рекомендуется добавить флаг автоматического добавления маршрута к указанной сети, используя данный интерфейс. Для интерфейса **`wan1`** следует также установить флаг добавления маршрута по умолчанию к указанному шлюзу через данный интерфейс.

Аналогично привязать созданные объекты к другим интерфейсам.

Командная строка:

```
set Interface Ethernet lan IP=lan/lan_ip Network=lan/lan_net
AutoInterfaceNetworkRoute=yes
set Interface Ethernet dmz IP=dmz/dmz_ip Network=dmz/dmz_net
AutoInterfaceNetworkRoute=yes
```

```
set Interface Ethernet wan1 IP=wan1/wan1_ip Network=wan1/wan1_net
DefaultGateway=wan1/wan1_gw Name=wan1 AutoInterfaceNetworkRoute=yes
AutoDefaultGatewayRoute=yes

set Interface Ethernet wan2 IP=wan2/wan2_ip Network=wan2/wan2_net
DefaultGateway=wan2/wan2_gw Name=wan2 AutoInterfaceNetworkRoute=yes
```

В результате заданы следующие параметры интерфейсов:

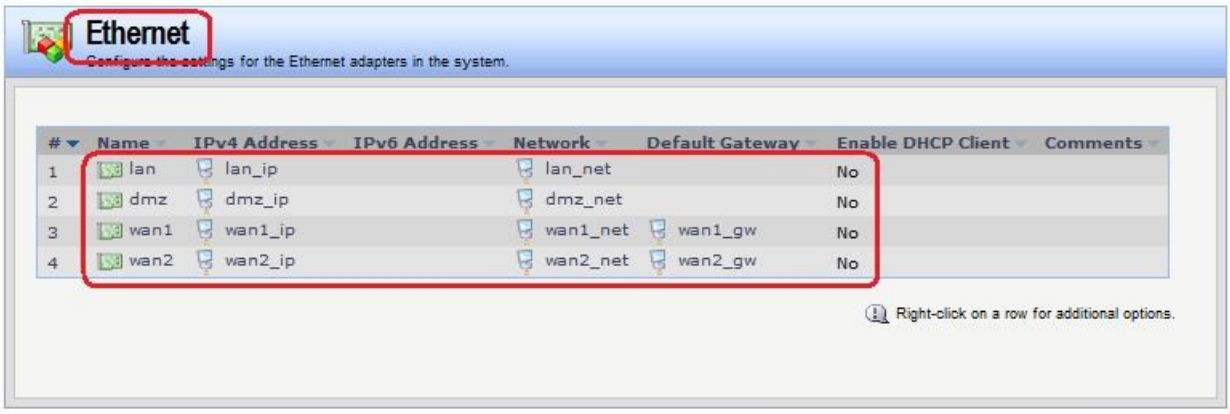
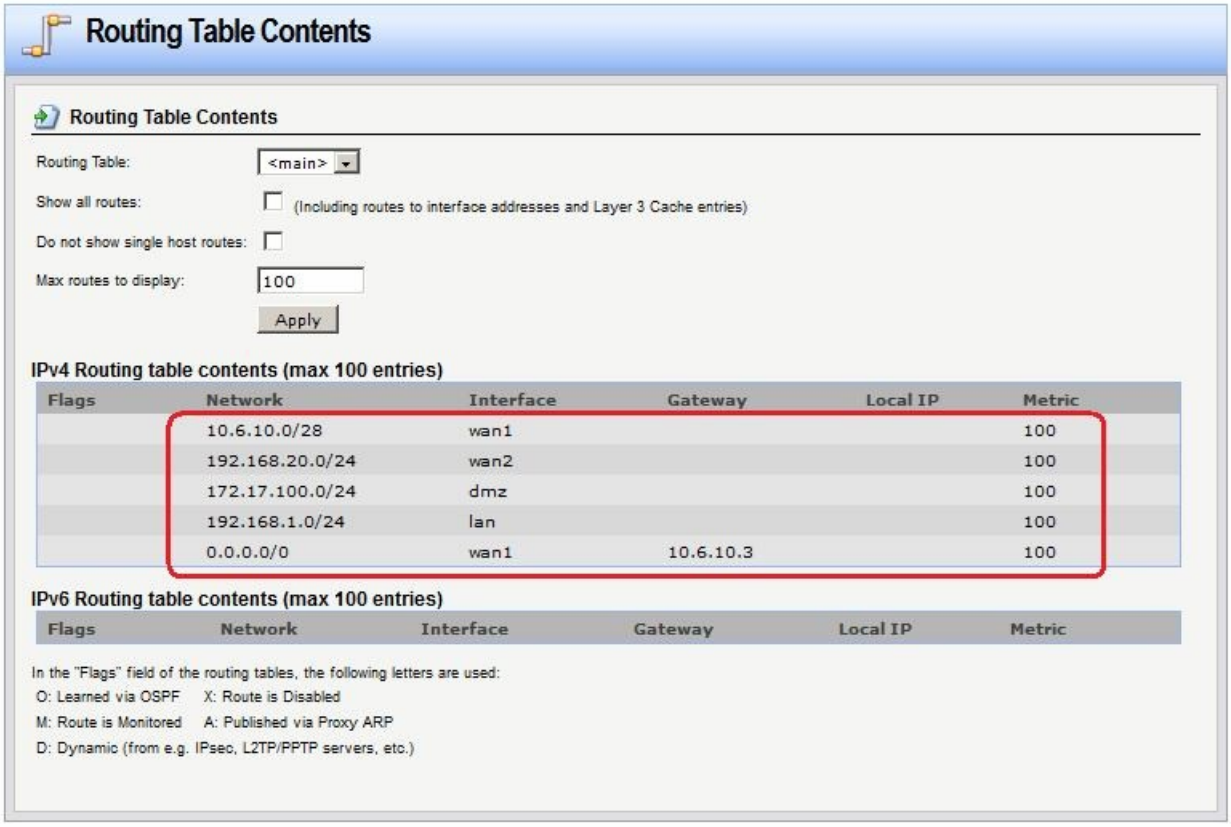


Таблица маршрутизации следующая:

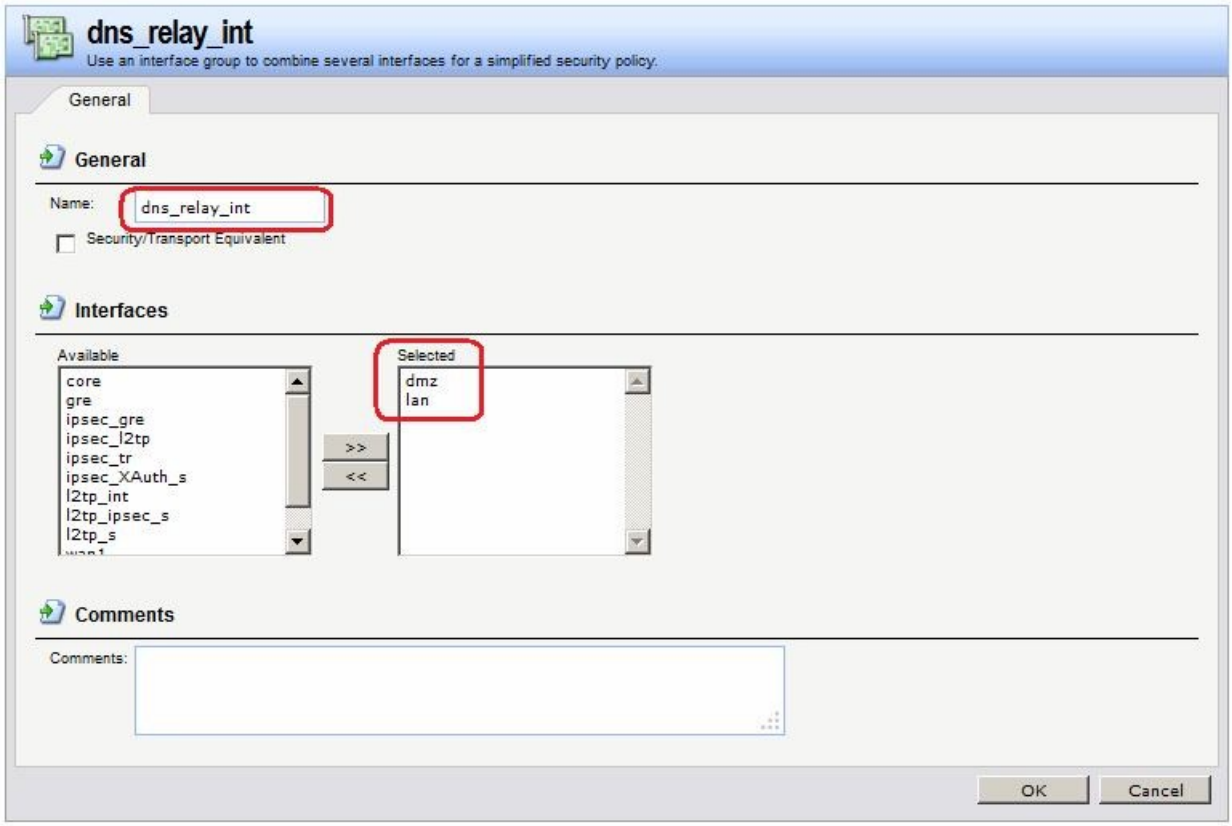


Группа интерфейсов

Объединить интерфейсы в Группу, чтобы несколько интерфейсов можно было указывать одним параметром в Правилах фильтрования.

Веб-интерфейс:

`Interfaces → Interface Group → Add`



Командная строка:

```
add Interface InterfaceGroup dns_relay_int Members=lan,dmz
```

Правила фильтрования

Создать Правила, перенаправляющие DNS-трафик из локальных сетей к DNS-серверу в интернете. Это можно сделать несколькими способами:

1. Создать правила **SAT** и **NAT** для каждого интерфейса, соединенному с сетями, которым необходим сервис DNS. В качестве сети источника следует указать сеть (группу сетей), которой требуется сервис DNS. В качестве сети назначения следует указать IP-адрес интерфейса.

Правило **SAT** заменяет IP-адрес получателя на IP-адрес, указанный на вкладке **SAT**.

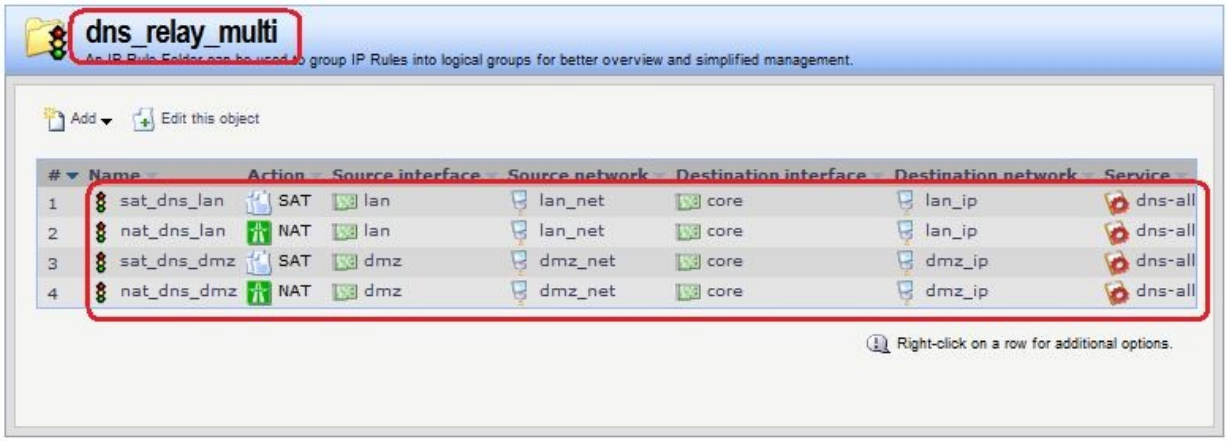
На вкладке **SAT** в качестве адреса назначения следует указать IP-адрес DNS-сервера.

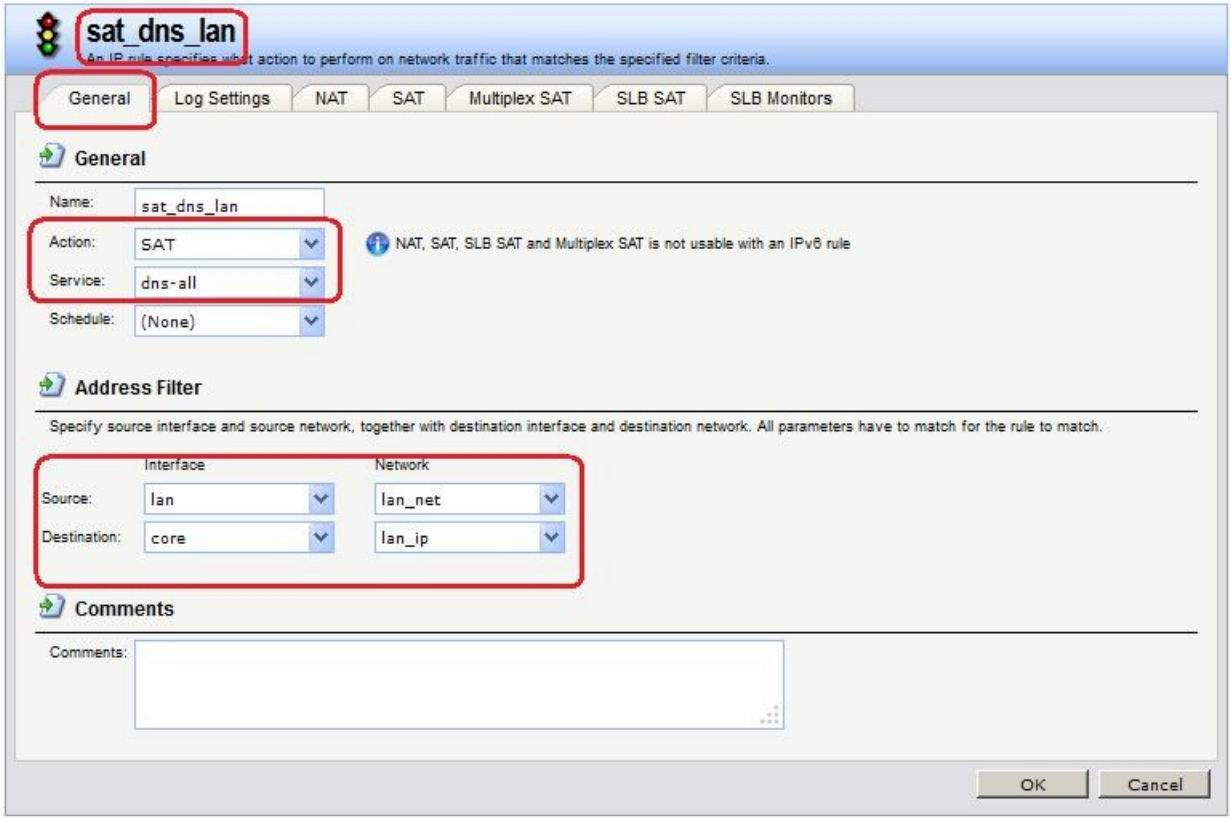
Веб-интерфейс:

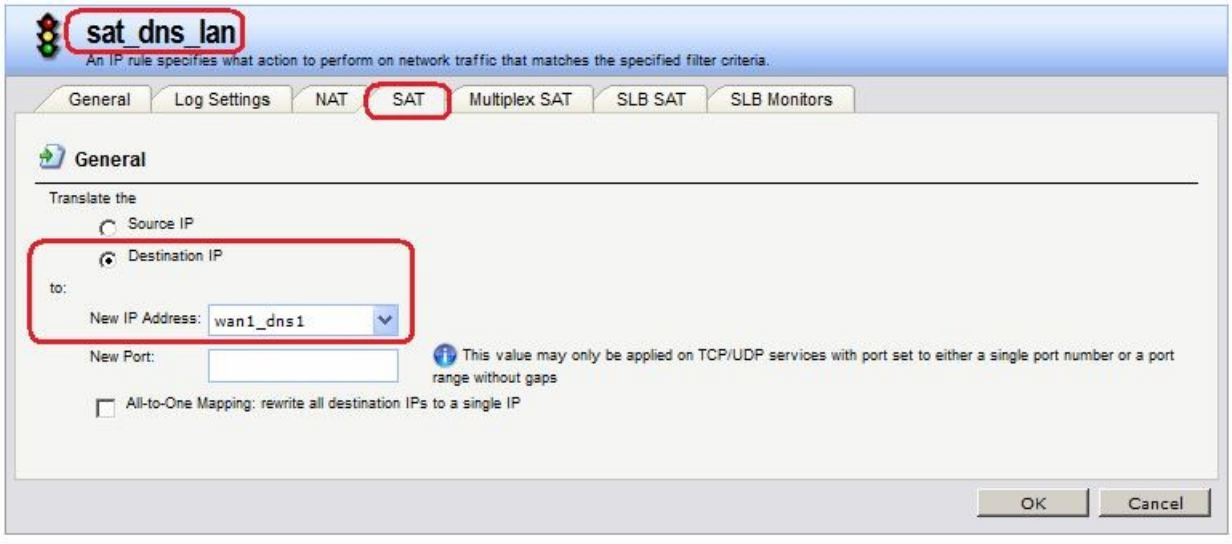
Rules → IP Rules → Add → IP Rule Folder

Name: dns_relay_multi

Rules → IP Rules → dns_relay_multi


dns_relay_multi
group IP Rules into logical groups for better overview and simplified management.
Add
Edit this object
Name Action Source interface Source network Destination interface Destination network Service
1 sat_dns_lan SAT lan lan_net core lan_ip dns-all
2 nat_dns_lan NAT lan lan_net core lan_ip dns-all
3 sat_dns_dmz SAT dmz dmz_net core dmz_ip dns-all
4 nat_dns_dmz NAT dmz dmz_net core dmz_ip dns-all
Right-click on a row for additional options.


sat_dns_lan
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.
General
Log Settings
NAT
SAT
Multiplex SAT
SLB SAT
SLB Monitors
General
Name: sat_dns_lan
Action: SAT
Service: dns-all
Schedule: (None)
NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule
Address Filter
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.
Interface
Network
Source: lan lan_net
Destination: core lan_ip
Comments
Comments:
OK
Cancel


sat_dns_lan
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.
General
Log Settings
NAT
SAT
Multiplex SAT
SLB SAT
SLB Monitors
General
Translate the
Source IP
Destination IP
to:
New IP Address: wan1_dns1
New Port:
This value may only be applied on TCP/UDP services with port set to either a single port number or a port range without gaps
All-to-One Mapping: rewrite all destination IPs to a single IP
OK
Cancel

Командная строка:

```
add IPRuleFolder Name=dns_relay_multi

cc IPRuleFolder <N folder>

add IPRule Action=SAT SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=core DestinationNetwork=lan/lan_ip Service=dns-all
SATTranslateToIP=wan1/wan1_dns1 Name=sat_dns_lan

add IPRule Action=NAT SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=core DestinationNetwork=lan/lan_ip Service=dns-all
Name=nat_dns_lan

add IPRule Action=SAT SourceInterface=dmz SourceNetwork=dmz/dmz_net
DestinationInterface=core DestinationNetwork=dmz/dmz_ip Service=dns-all
SATTranslateToIP=wan1/wan1_dns1 Name=sat_dns_dmz

add IPRule Action=NAT SourceInterface=dmz SourceNetwork=dmz/dmz_net
DestinationInterface=core DestinationNetwork=dmz/dmz_ip Service=dns-all
Name=nat_dns_dmz
```

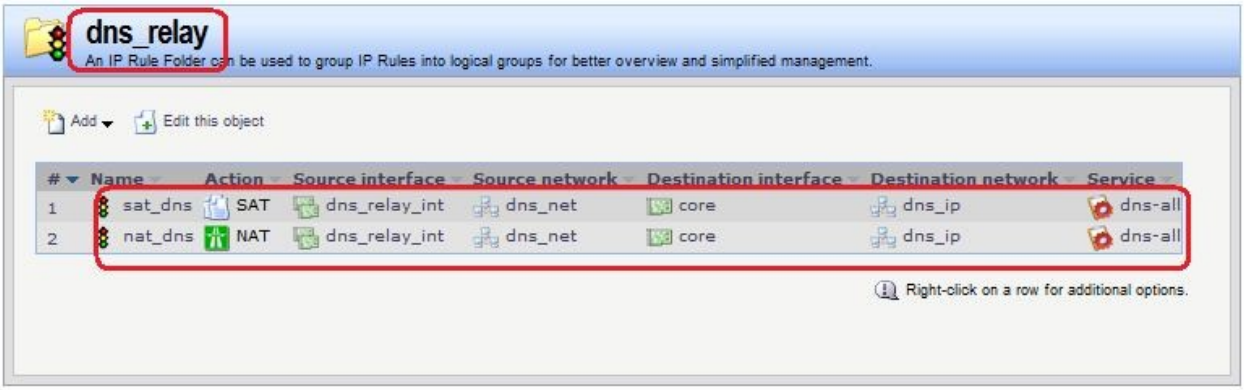
2. Использовать созданные группы IP-сетей, IP-адресов и интерфейсов, для сетей которых необходим сервис DNS. В этом случае будет достаточно одной пары правил SAT-NAT.

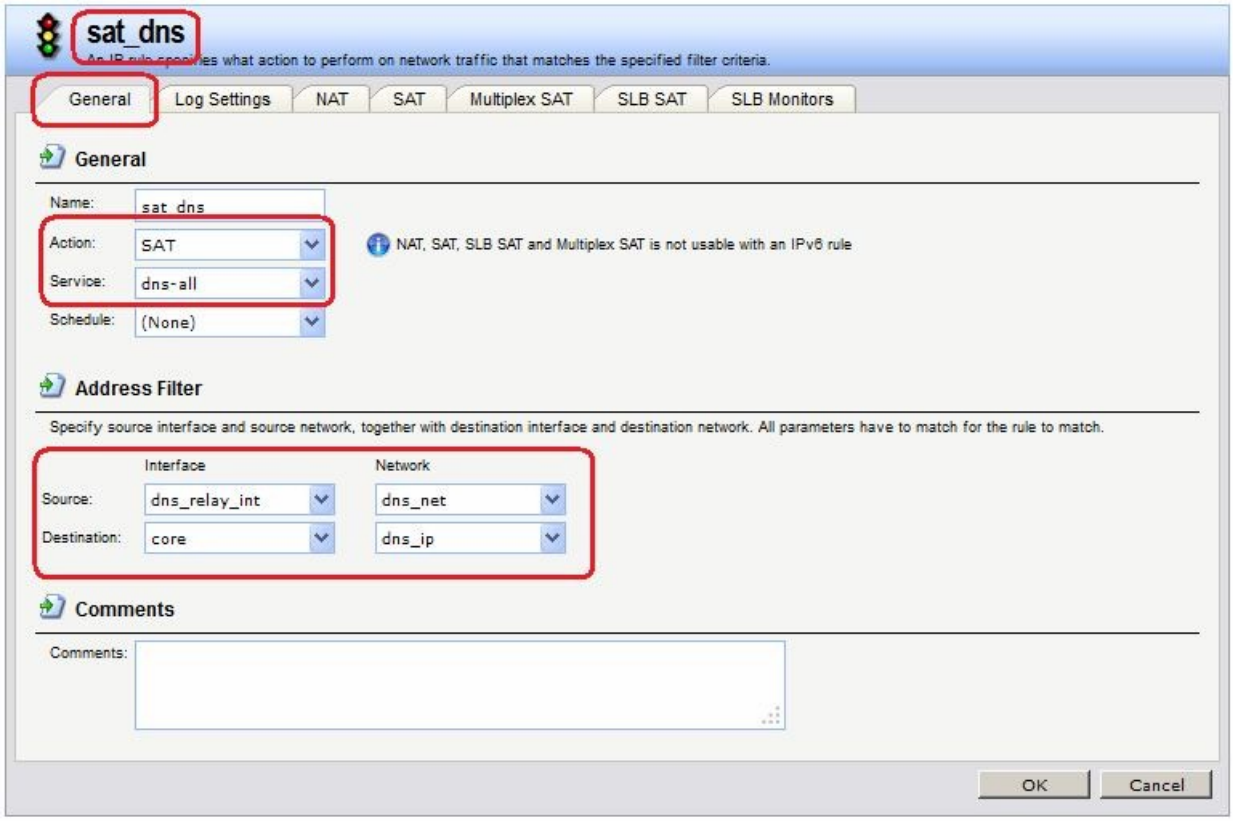
Веб-интерфейс:

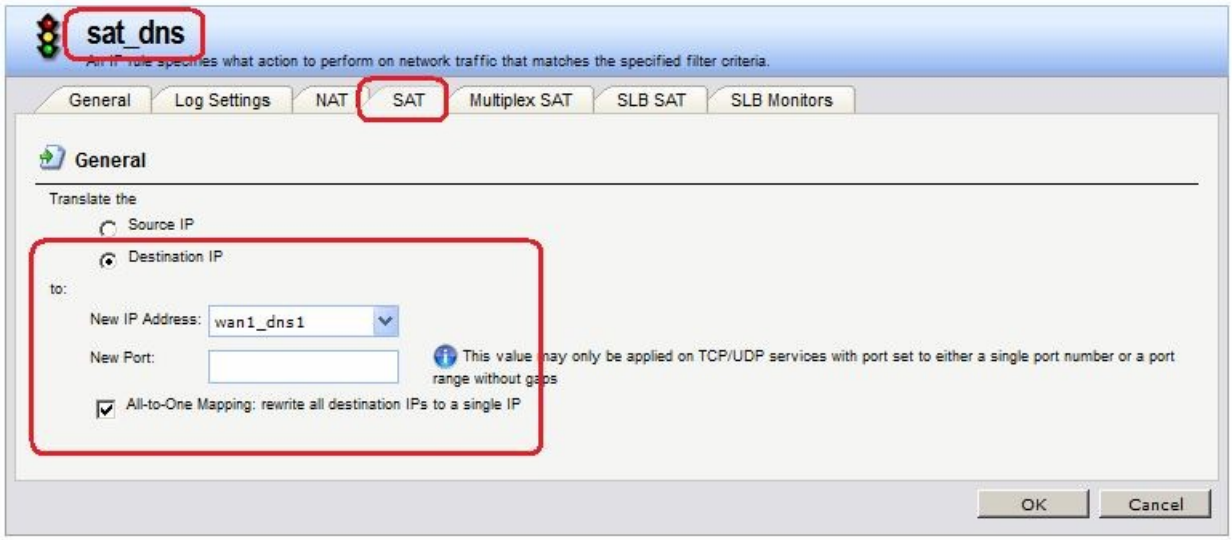
Rules → IP Rules → Add → IP Rule Folder

Name: dns_relay

Rules → IP Rules → dns_relay → Add







Второе Правило зависит от требований провайдера. На МЭ 1 указано правило **NAT**. В этом случае провайдер видит только IP-адрес интерфейса **wan1** МЭ1.

Командная строка:

```
add IPRuleFolder Name=dns_relay
```

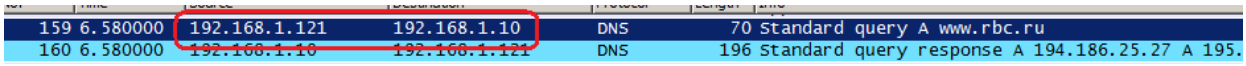
```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=SAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_relay_net DestinationInterface=core
DestinationNetwork=dns_relay/dns_ip Service=dns-all SATAllToOne=Yes
SATTranslateToIP=wan1/wan1_dns1 Name=sat_dns
```

```
add IPRule Action=NAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_relay_net DestinationInterface=core
DestinationNetwork=dns_relay/dns_ip Service=dns-all Name=nat_dns
```

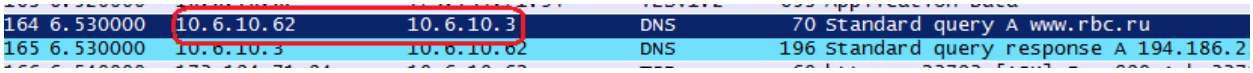
Результирующий трафик следующий.

На интерфейс **lan** приходит трафик:



159 6.580000	192.168.1.121	192.168.1.10	DNS	70 Standard query A www.rbc.ru
160 6.580000	192.168.1.10	192.168.1.121	DNS	196 Standard query response A 194.186.25.27 A 195.

С интерфейса **wan1** уходит трафик:

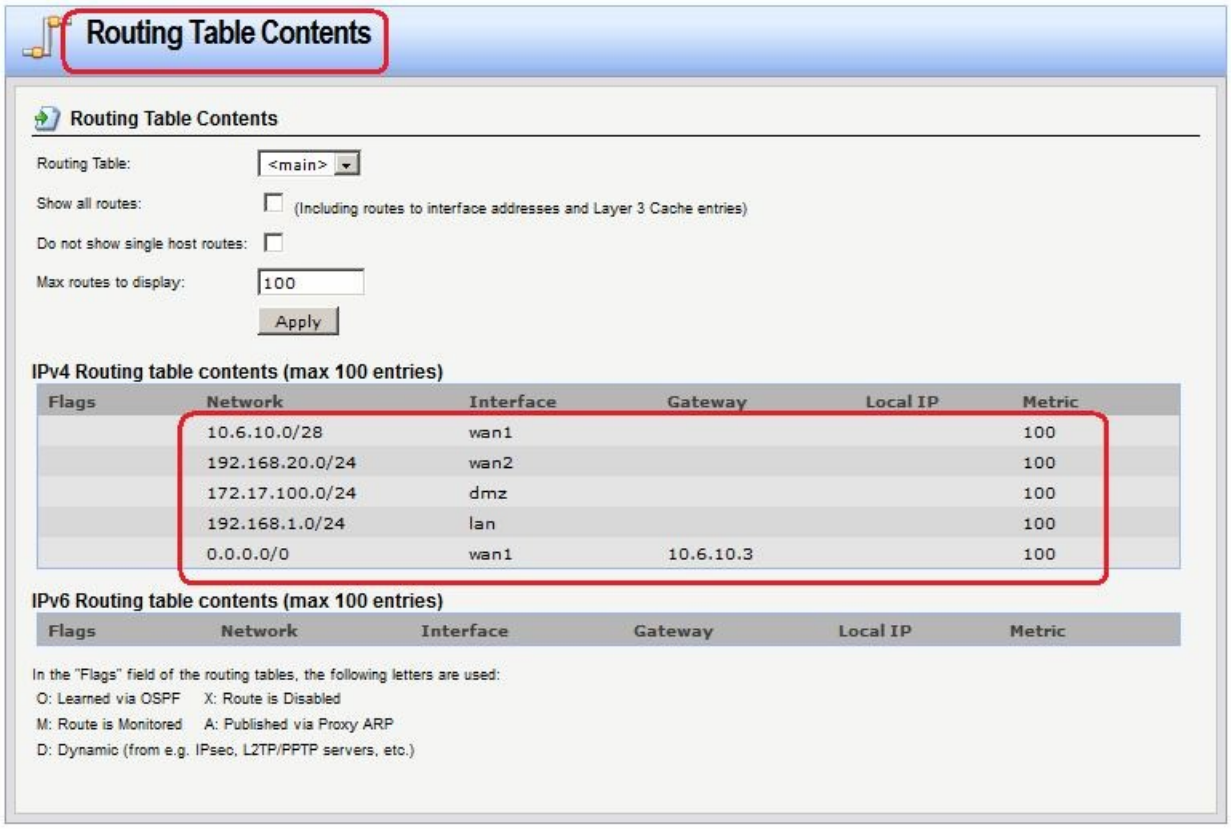


164 6.530000	10.6.10.62	10.6.10.3	DNS	70 Standard query A www.rbc.ru
165 6.530000	10.6.10.3	10.6.10.62	DNS	196 Standard query response A 194.186.2

1. Адрес получателя тот, который указан на вкладке **SAT** правила **SAT**.
2. Адрес отправителя соответствует правилу **NAT**.

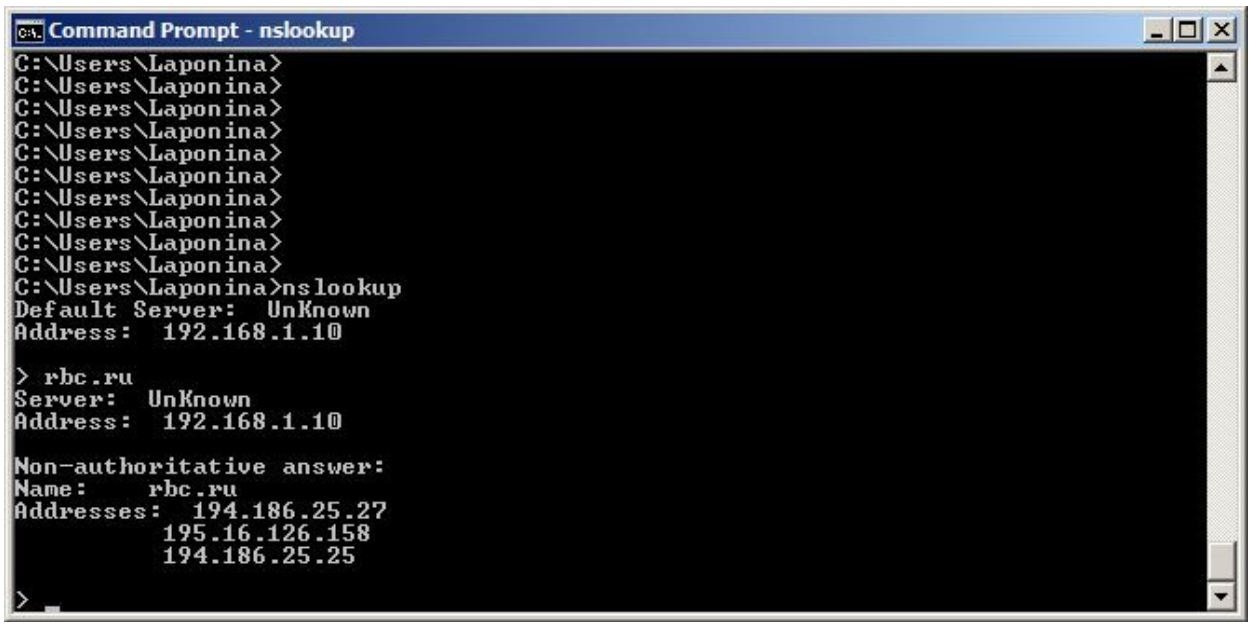
Статическая маршрутизация

В таблице маршрутизации уже существуют маршруты ко всем сетям, которые непосредственно доступны с интерфейсов. В результате таблица маршрутизации на МЭ1 выглядит следующим образом:

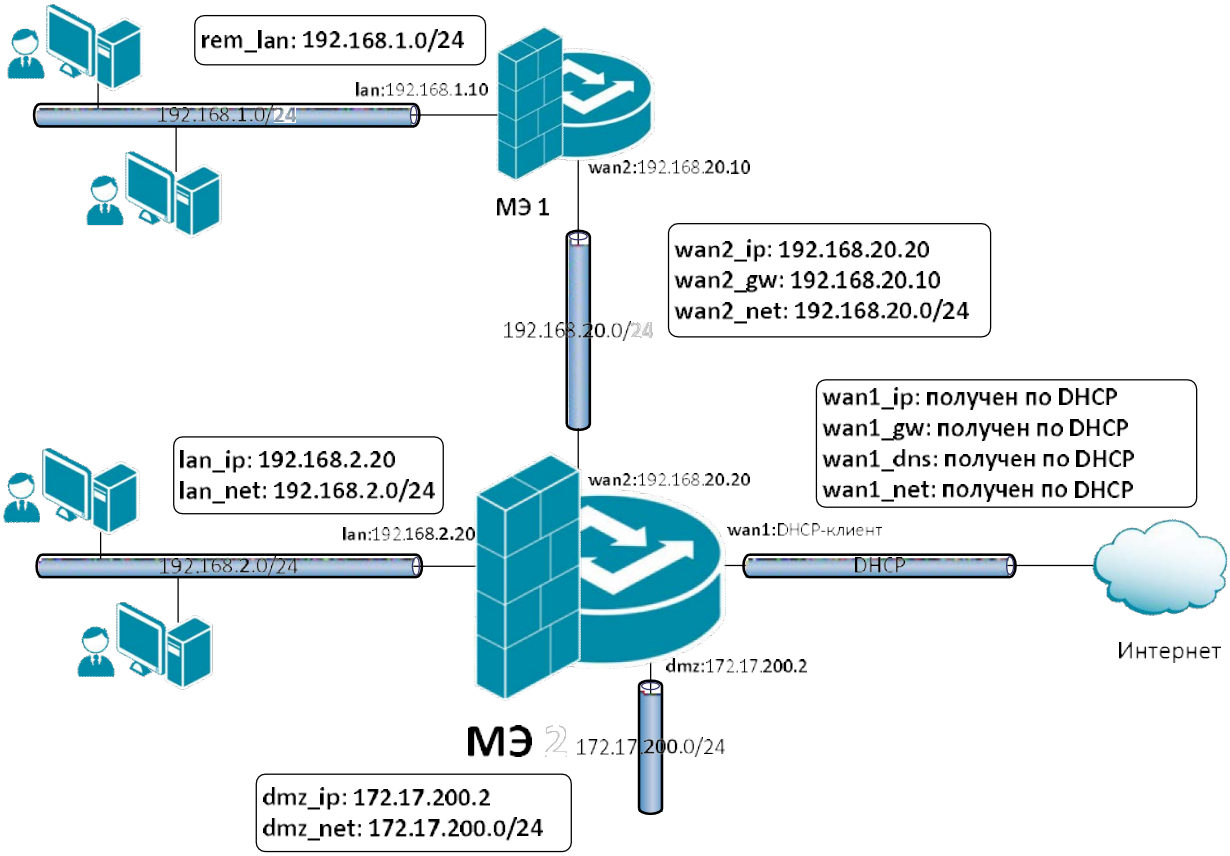


Проверка доступности DNS-сервисов из локальной сети

Проверить из командной строки на рабочей станции, расположенной в локальной сети, возможность обрабатывать DNS-запросы с помощью команды **nslookup**:



Межсетевой Экран 2



На Межсетевом Экране 2 следует выполнить аналогичные настройки.

1. В Адресной Книге создать необходимые объекты.
2. Для удобства конфигурирования объединить в одну группу интерфейсы, которые требуют одинаковых правил фильтрования.
3. Создать правила, перенаправляющие DNS-трафик из локальной сети и dmz-сети к DNS-серверу.
4. При необходимости в таблицу маршрутизации добавить маршруты.

Объекты Адресной Книги

В Адресной Книге создать необходимые объекты.

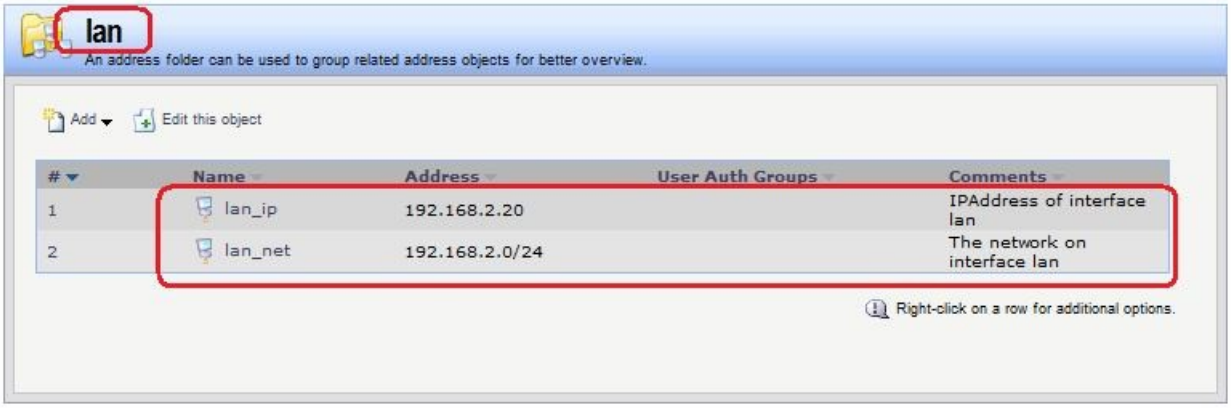
1. Объекты интерфейса **lan**.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: lan

Object → Address Book → lan



Командная строка:

```
add Address AddressFolder lan
cc Address AddressFolder lan
add IP4Address lan_ip Address=192.168.2.20 Comments='IPAddress of interface lan'
add IP4Address lan_net Address=192.168.2.0/24 Comments='The network on interface lan'
```

2. Объекты интерфейса **dmz**.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: dmz

Object → Address Book → dmz

Командная строка:

```
add Address AddressFolder dmz
cc Address AddressFolder dmz
```

```
add IP4Address dmz_ip Address=172.17.200.20 Comments='IPAddress of interface dmz'
add IP4Address dmz_net Address=172.17.200.0/24 Comments='The network on interface dmz'
```

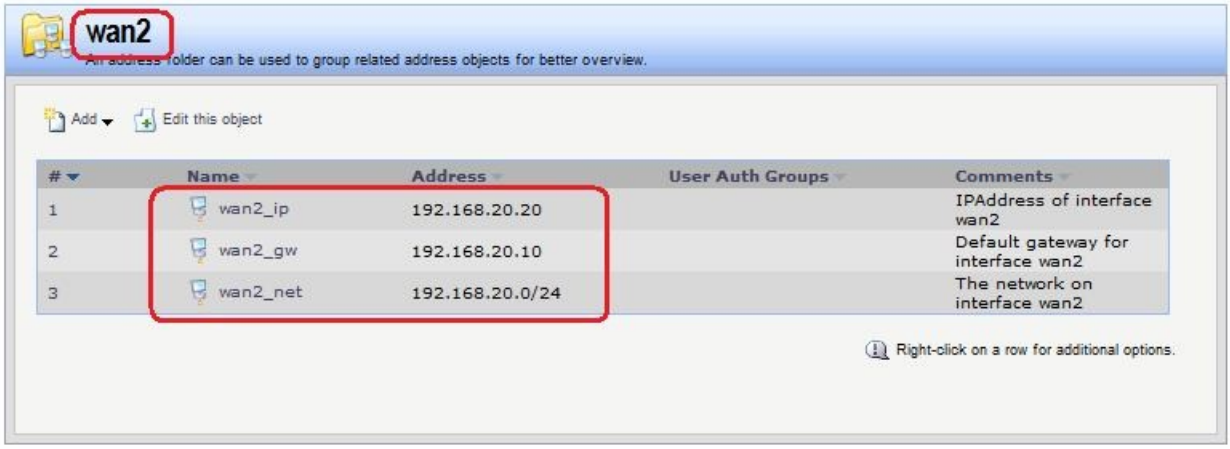
3. Объекты интерфейса **wan2.**

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: wan2

Object → Address Book → wan2



Командная строка:

```
add Address AddressFolder wan2
cc Address AddressFolder wan2
add IP4Address wan2_ip Address=192.168.20.20 Comments='IPAddress of interface wan2'
add IP4Address wan2_gw Address=192.168.20.10 Comments='Default gateway for interface wan2'
add IP4Address wan2_net Address=192.168.20.0/24 Comments='The network on interface wan2'
```

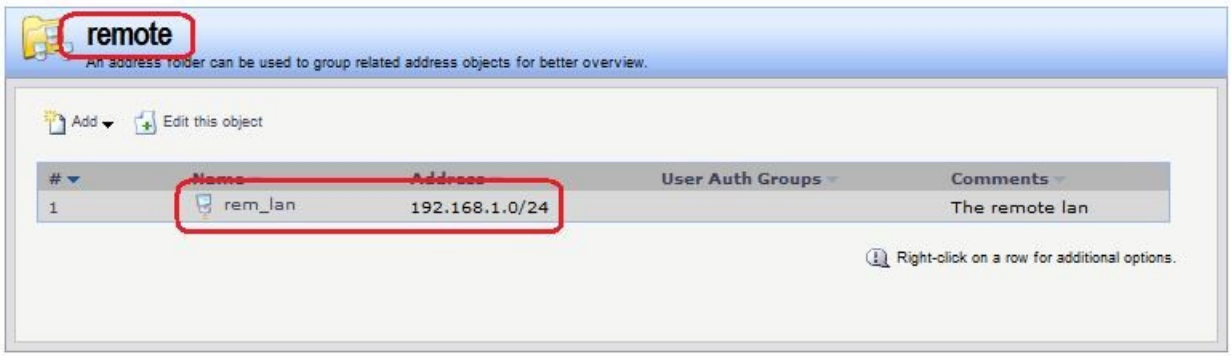
4. Объекты, описывающие сети, расположенные за МЭ 1.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: remote

Object → Address Book → remote



Командная строка:

```
add Address AddressFolder remote Comments='The remote objects'
cc Address AddressFolder remote
add IP4Address rem_lan Address=192.168.1.0/24 Comments='The remote lan'
```

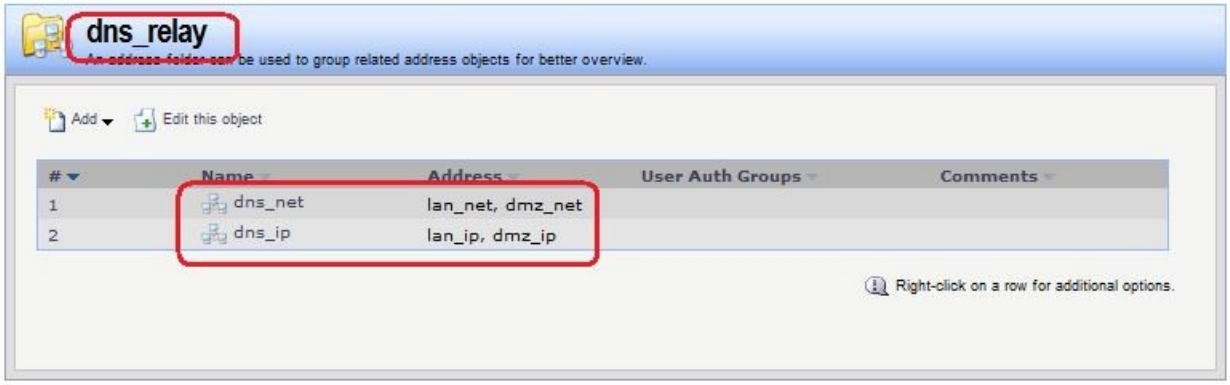
5. Дополнительные объекты, необходимые для удобства администрирования и объединяющие в одну группу сети и IP-адреса, которые необходимы одинаковые сервисы DNS.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: dns_relay

Object → Address Book → dns_relay



Командная строка:

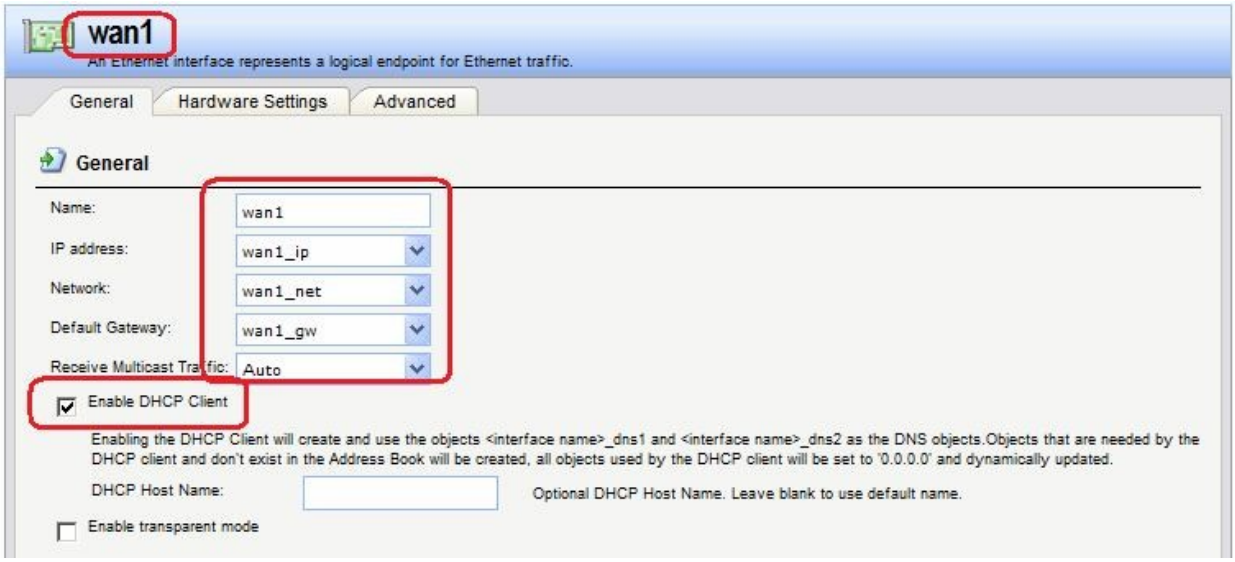
```
add Address AddressFolder dns_relay Comments='DNS services'
cc Address AddressFolder dns_relay
add IP4Group dns_net Members =lan/lan_net, dmz/dmz_net
add IP4Group dns_ip Members = lan/lan_ip, dmz/dmz_ip
```

Привязка созданных объектов Адресной Книги к интерфейсам

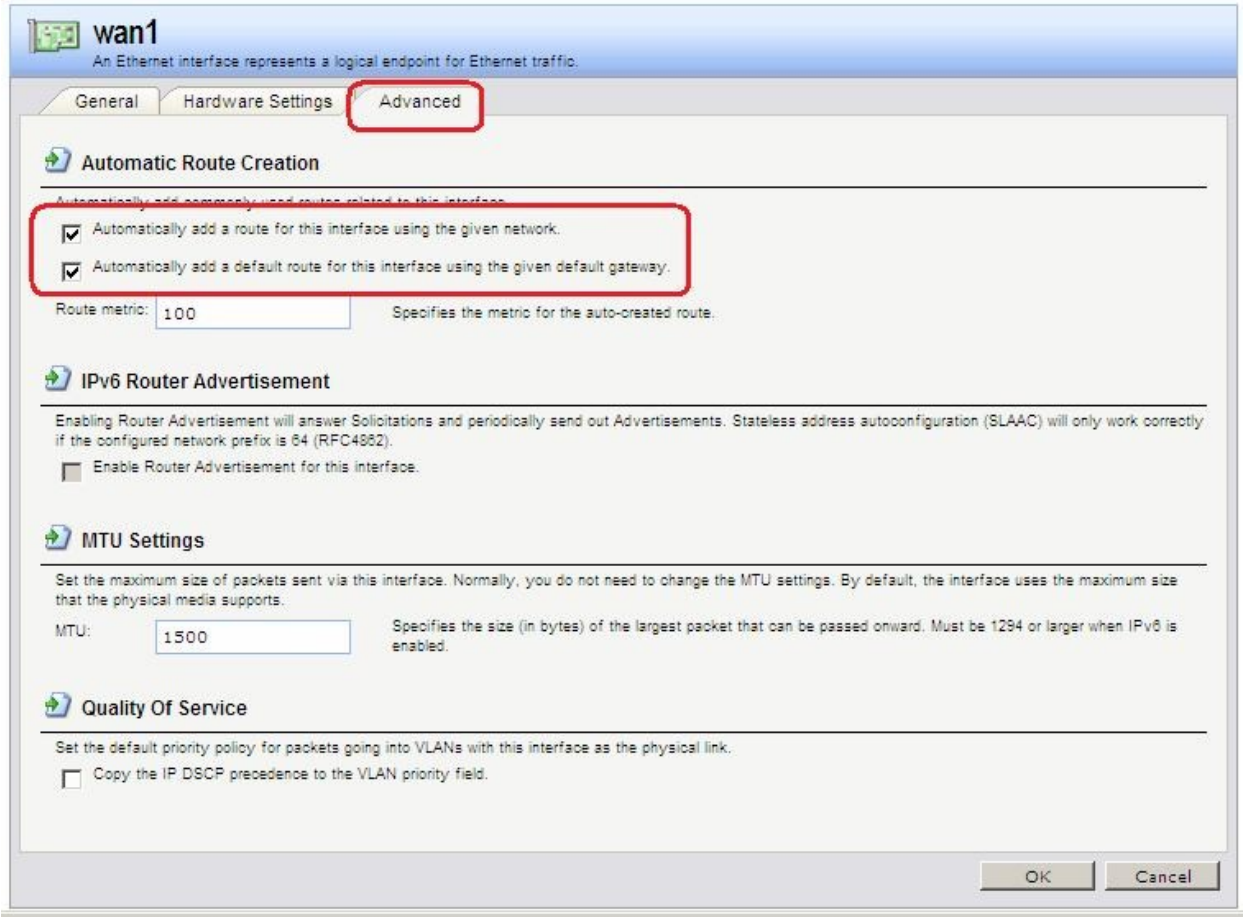
Объекты, созданные в пунктах 1, 2 и 3, должны быть привязаны к соответствующим Ethernet-интерфейсам.

Веб-интерфейс:

Interfaces → Ethernet → wan1



Если IP-адрес данного интерфейса должен быть получен по протоколу DHCP, то следует установить соответствующий флаг «**Enable DHCP Client**».



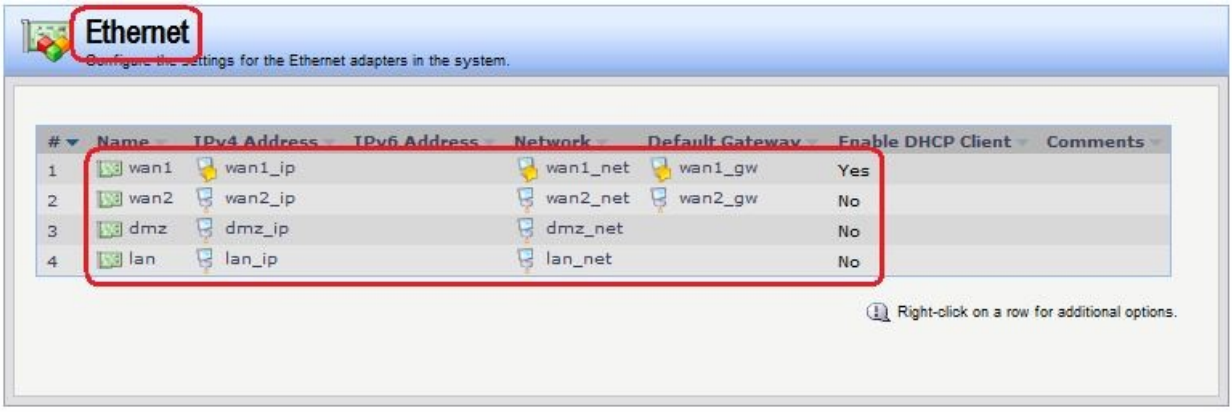
На вкладке **Advanced** рекомендуется добавить флаг автоматического добавления маршрута к указанной сети, используя данный интерфейс. Для интерфейса **wan1** следует также установить флаг добавления маршрута по умолчанию к указанному шлюзу через данный интерфейс.

Аналогично привязать созданные объекты к другим интерфейсам.

Командная строка:

```
set Interface Ethernet lan IP=lan/lan_ip Network=lan/lan_net Name=lan AutoInterfaceNetworkRoute=yes

set Interface Ethernet dmz IP=dmz/dmz_ip Network=dmz/dmz_net Name=dmz AutoInterfaceNetworkRoute=yes

set Interface Ethernet wan1 IP=wan1/wan1_ip Network=wan1/wan1_net DefaultGateway=wan1/wan1_gw Name=wan1 AutoInterfaceNetworkRoute=yes DefaultGateway= wan1/wan1_gw DHCPEnabled=Yes

set Interface Ethernet wan2 IP=wan2/wan2_ip Network=wan2/wan2_net Name=wan2 AutoInterfaceNetworkRoute=yes
```

В результате заданы следующие параметры интерфейсов:

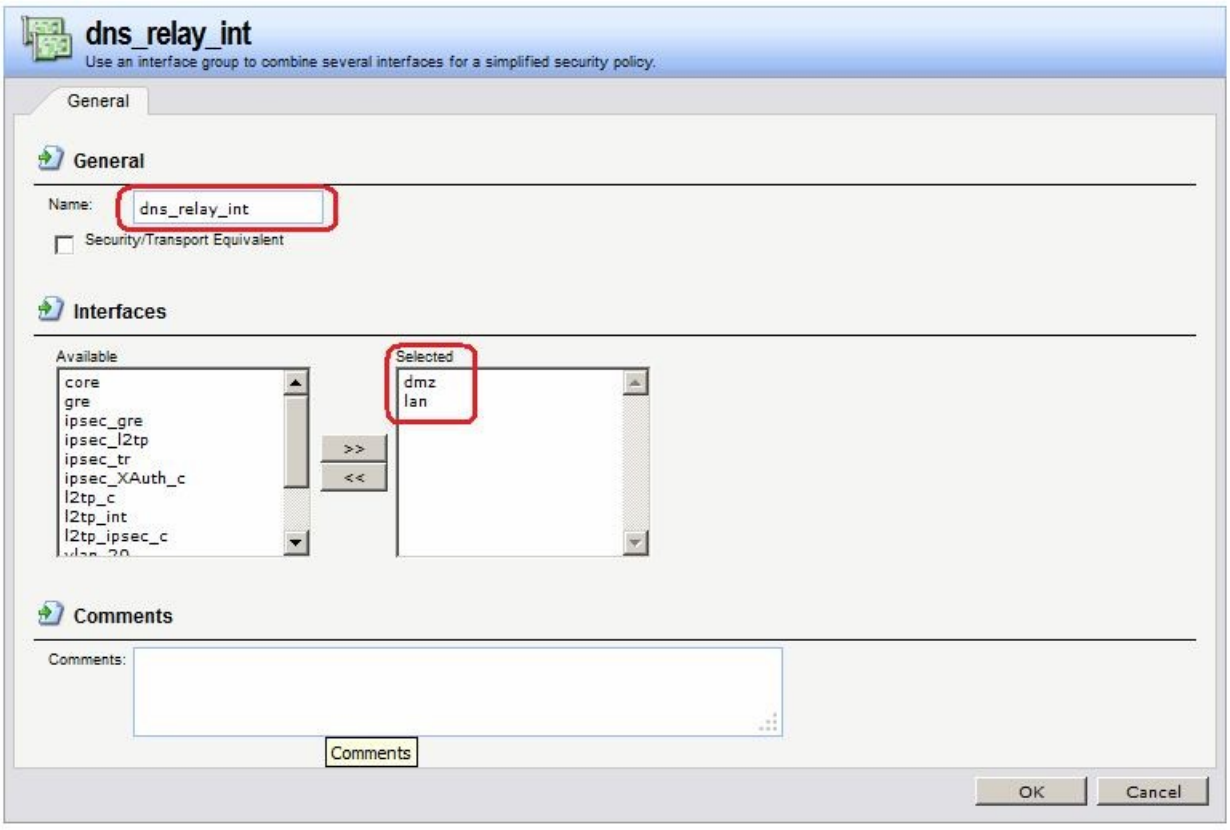


Группа интерфейсов

Для удобства можно создать группу интерфейсов, в которой перечислены интерфейсы, трафик с которых можно объединить в одно Правило фильтрования. В нашем случае это интерфейсы **dmz** и **lan**.

Веб-интерфейс:

Interfaces → Interface Groups → Add → Interface Group



Командная строка:

add Interface InterfaceGroup dns_relay_int Members=lan,dmz

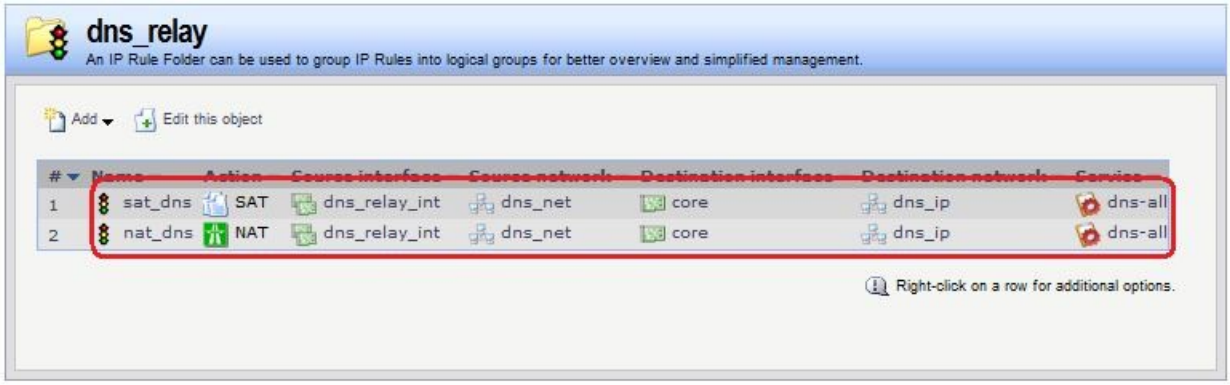
Правила фильтрования

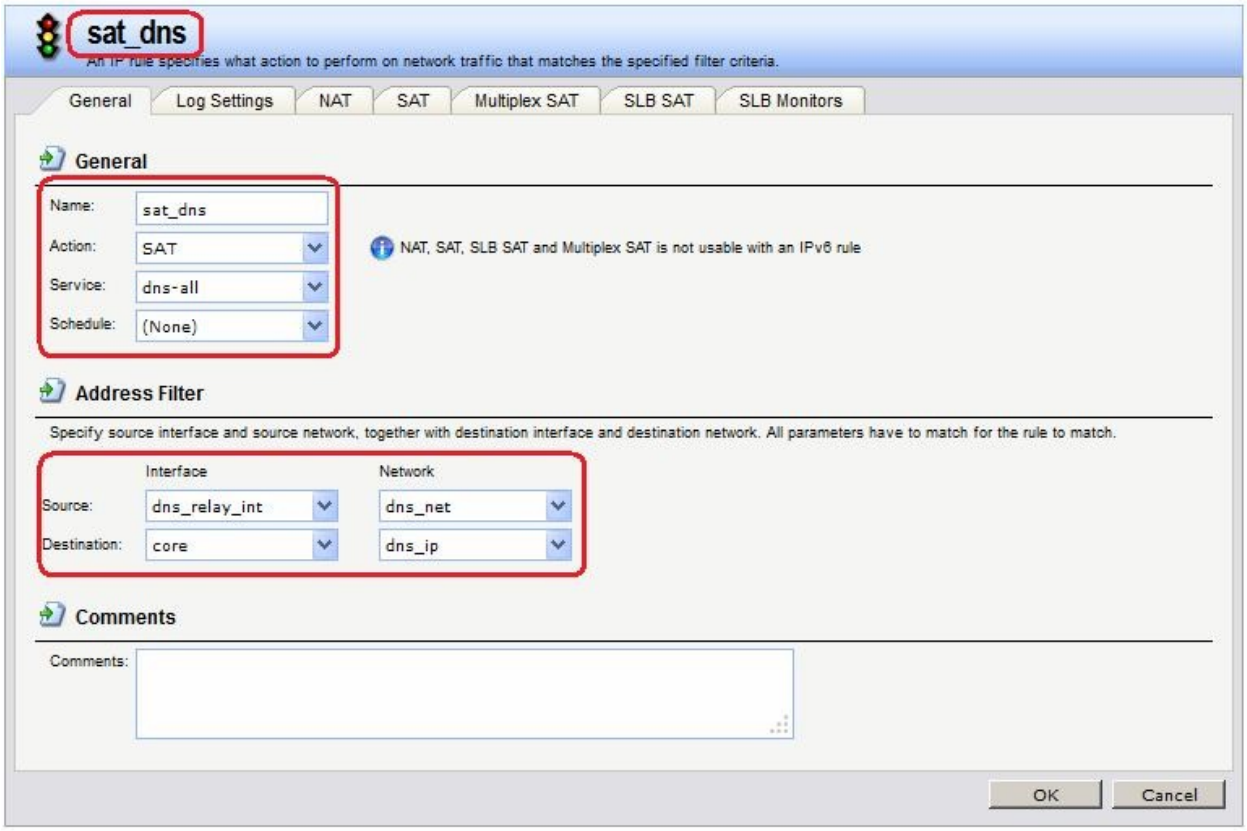
Веб-интерфейс:

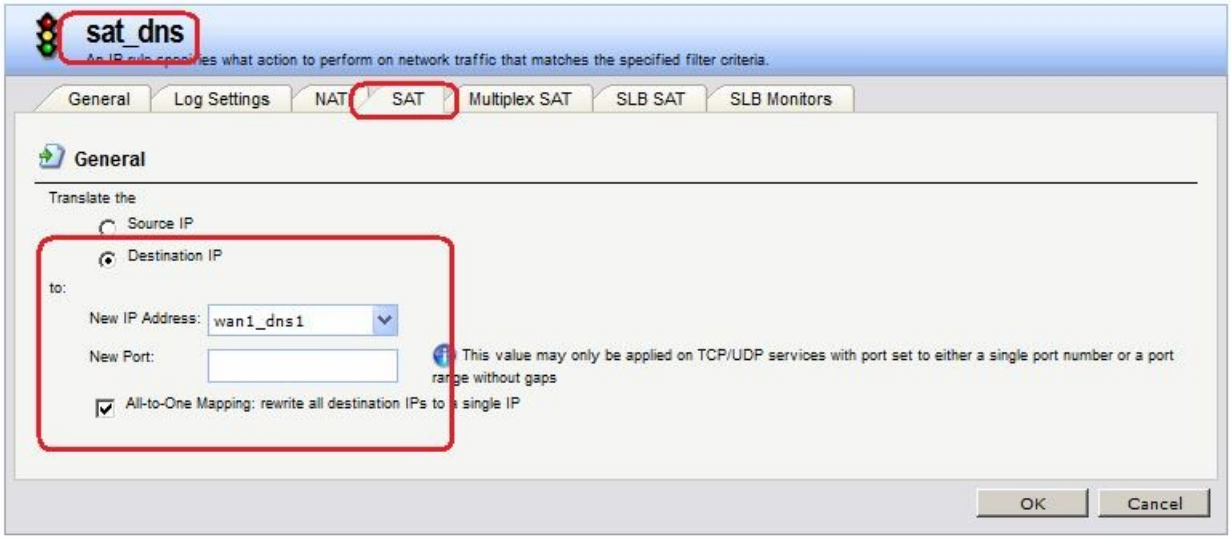
Rules → IP Rules → Add → IP Rule Folder

Name: dns_relay

Rules → IP Rules → dns_relay







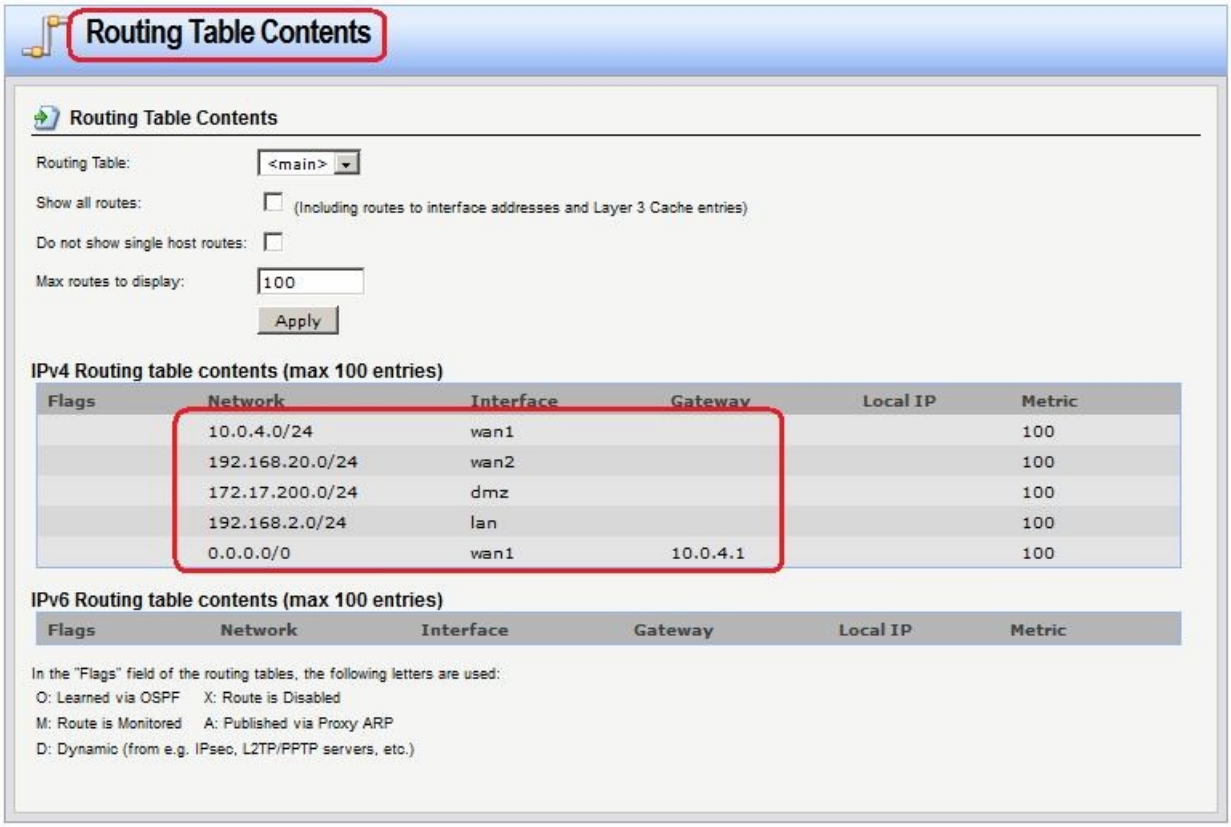
Вторым правилом на МЭ2 является правило **NAT**.

Командная строка:

```
add IPRuleFolder Name=dns_relay
cc IPRuleFolder <N folder>
add IPRule Action=SAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_net DestinationInterface=core
DestinationNetwork=dns_relay/dns_ip SATAllToOne=Yes
SATTranslateToIP=wan1/wan1_dns1 Service=dns-all Name=sat_dns
add IPRule Action=NAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_net DestinationInterface=core
DestinationNetwork=dns_relay/dns_ip Service=dns-all Name=nat_dns
```

Статическая маршрутизация

В таблице маршрутизации уже созданы все необходимые маршруты.



Доступ в интернет

Межсетевой Экран 1

На МЭ 1 все необходимые объекты в Адресной Книге уже созданы и маршруты определены. Осталось добавить Правила фильтрования, разрешающие доступ в интернет.

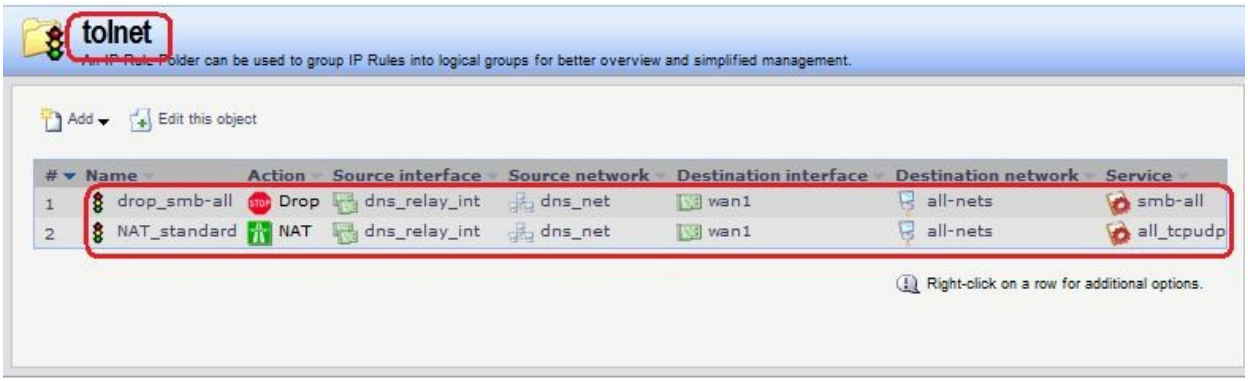
Правила фильтрования

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: toInet

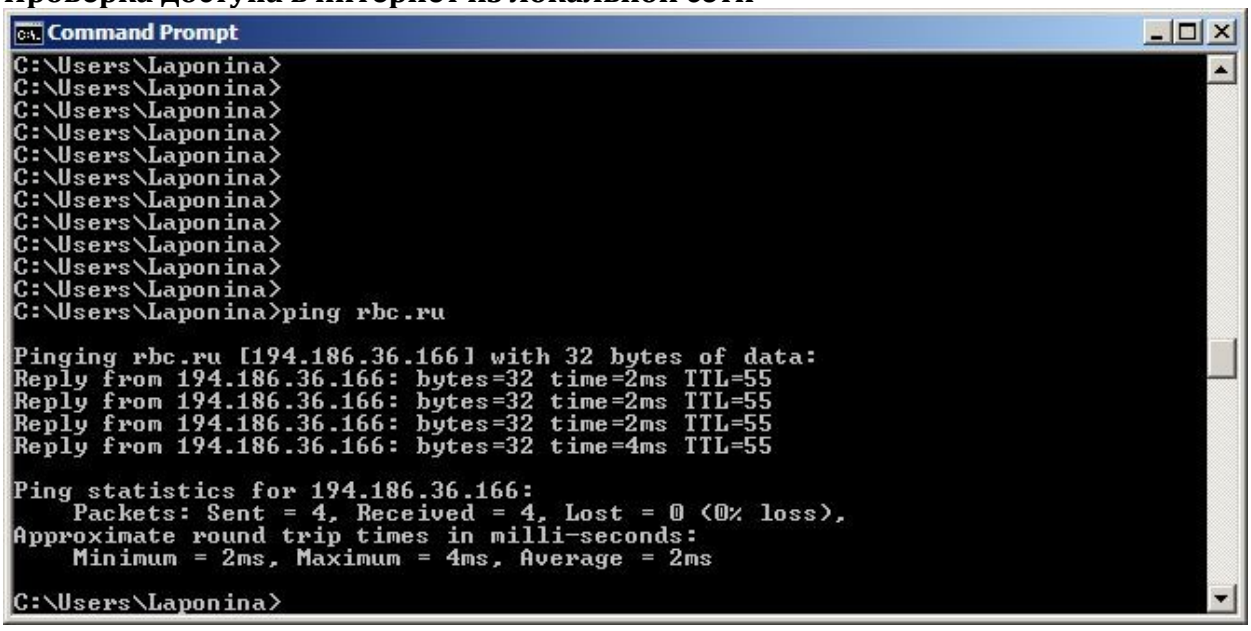
Rules → IP Rules → toInet



Командная строка:

```
add IPRuleFolder Name=toInet

cc IPRuleFolder <N folder>

add IPRule Action=Drop SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_relay_net DestinationInterface=wan2
DestinationNetwork=all-nets Service=smb_all Name=drop_smb-all

add IPRule Action=NAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_relay_net DestinationInterface=wan2
DestinationNetwork=all-nets Service=all_tcpudp Name=NAT_standard
```

Проверка доступа в интернет из локальной сети



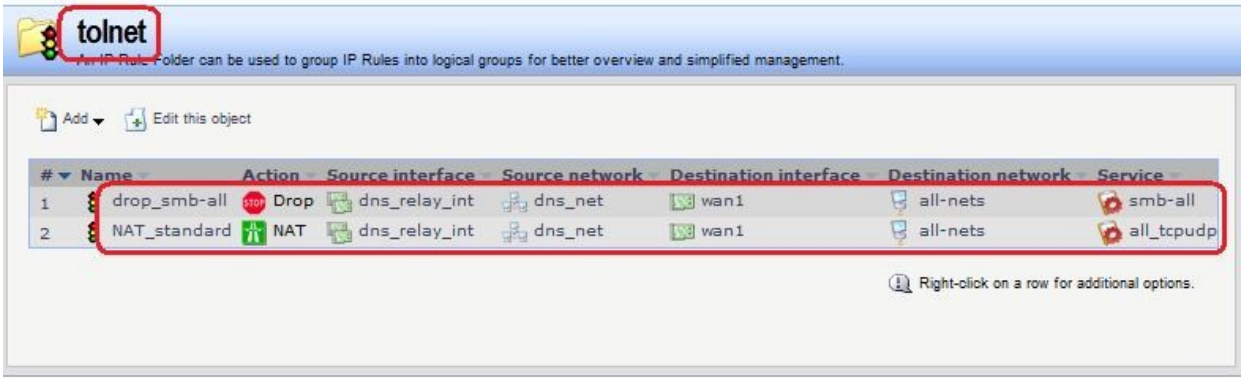
Межсетевой Экран 2

На МЭ1 все необходимые объекты в Адресной Книге уже созданы и маршруты определены. Осталось добавить Правила фильтрования, разрешающие доступ в интернет. Для удобства конфигурирования Правил фильтрования был создан объект в Адресной Книге, который объединяет все сети, из которых необходим доступ в интернет.

Правила фильтрования

Веб-интерфейс:

```
Rules → IP Rules → Add → IP Rule Folder
      Name: toInet
Rules → IP Rules → toInet
```



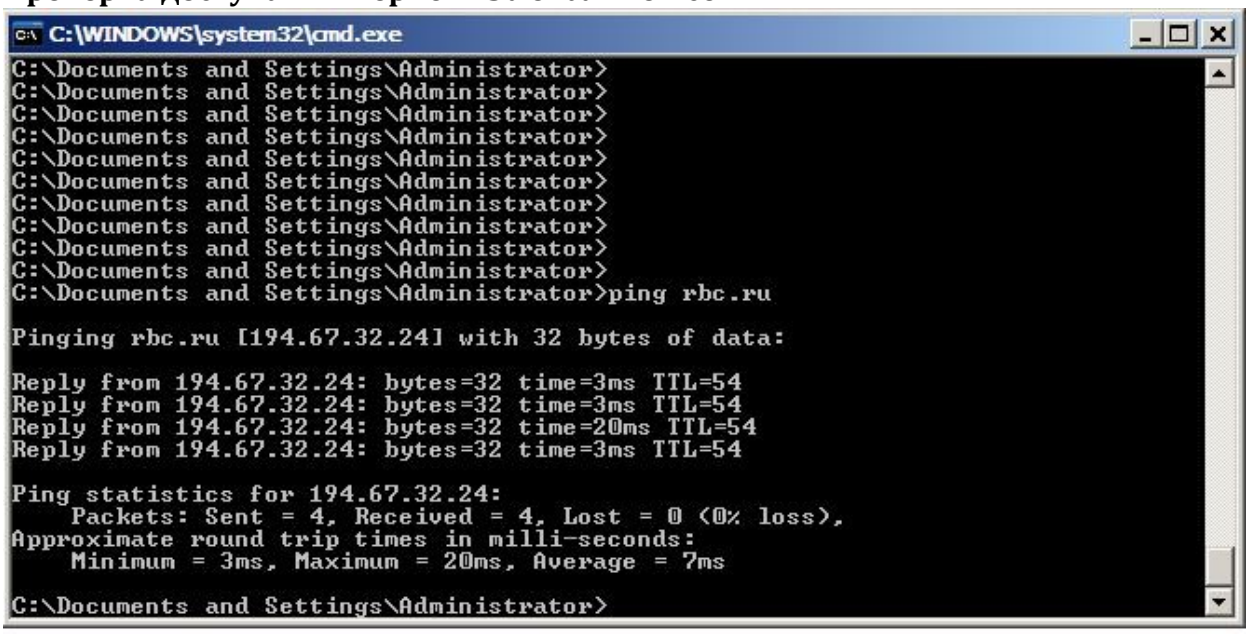
Командная строка:

```
add IPRuleFolder Name=toInet
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=NAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_net DestinationInterface=wan1
DestinationNetwork=all-nets Service=all_tcpudp Name=NAT_standard
```

Проверка доступа в интернет из локальной сети



Доступ из локальных сетей к каждому межсетевому экрану

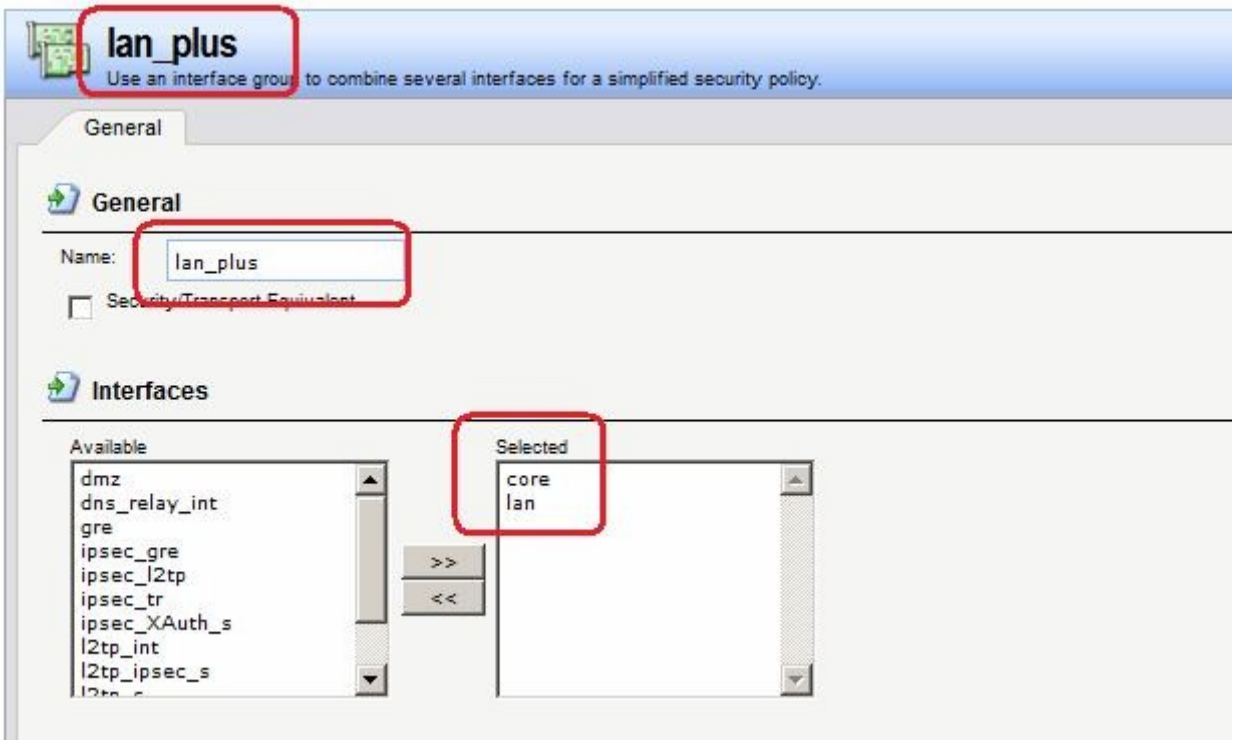
Межсетевой Экран 1

Группа интерфейсов

Объединить интерфейсы **lan** и **core** в одну группу, чтобы разрешить доступ как к рабочим станциям в локальной сети, так и к lan-интерфейсу межсетевого экрана.

Веб-интерфейс:

Interfaces → Interface Groups → Add → Interface Group



Командная строка:

```
add Interface InterfaceGroup lan_plus Members=core,lan
```

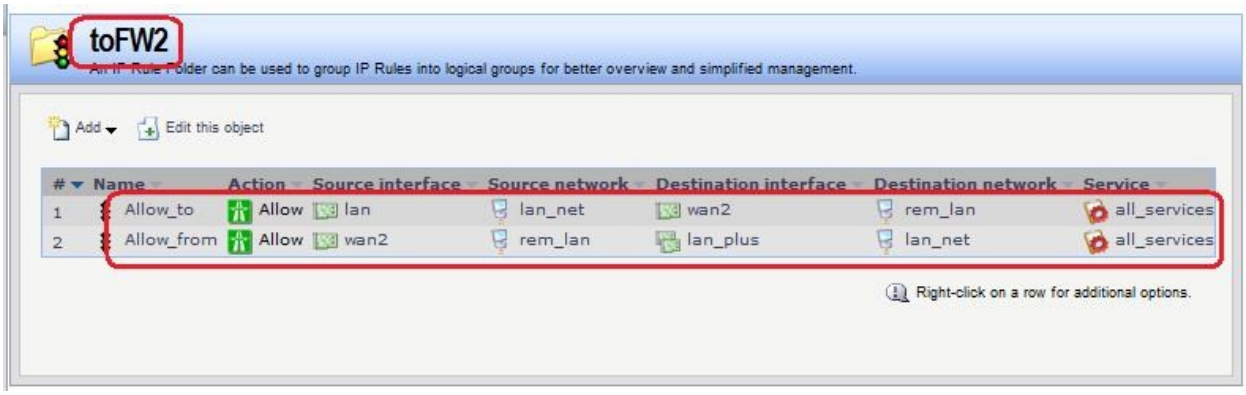
Правила фильтрования

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: toFW2

Rules → IP Rules → toFW2



Командная строка:

```
add IPRuleFolder Name=toFW2
```

```
cc IPRuleFolder <N folder>
```

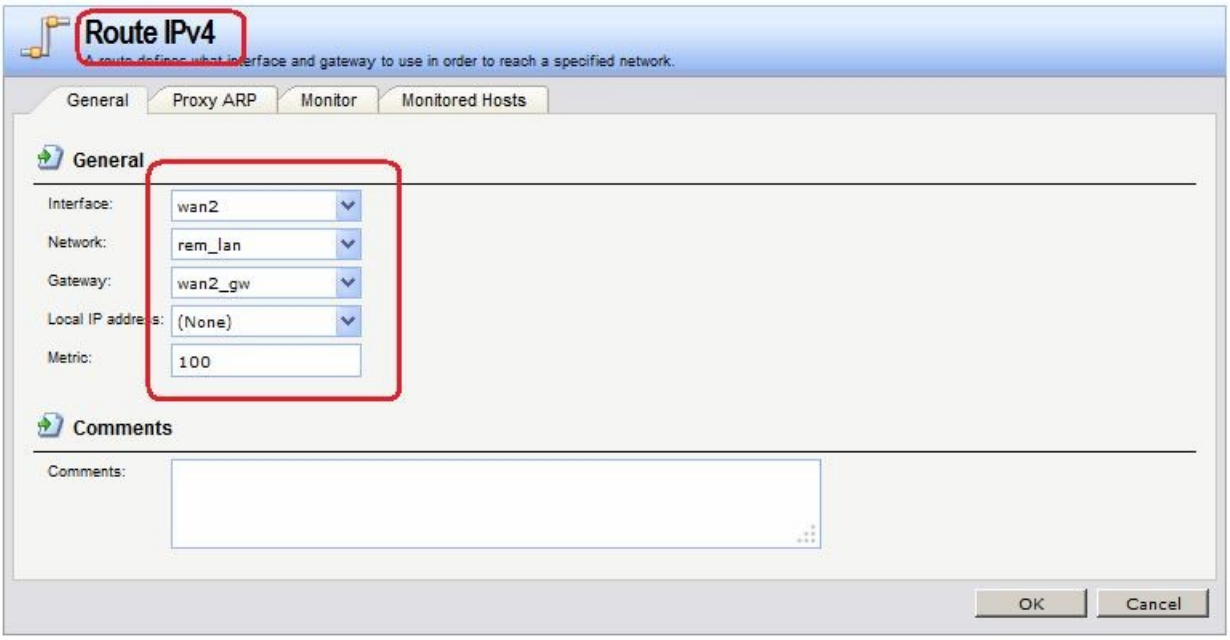
```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan2 DestinationNetwork=remote/rem_lan
Service=all_services Name=Allow_to
```

```
add IPRule Action=Allow SourceInterface=wan2 SourceNetwork=remote/rem_lan
DestinationInterface=lan_plus DestinationNetwork=lan/lan_net
Service=all_services Name=Allow_from
```

Статическая маршрутизация

Веб-интерфейс:

`Routing → Routing Tables → main → Add → Route IPv4`



Командная строка:

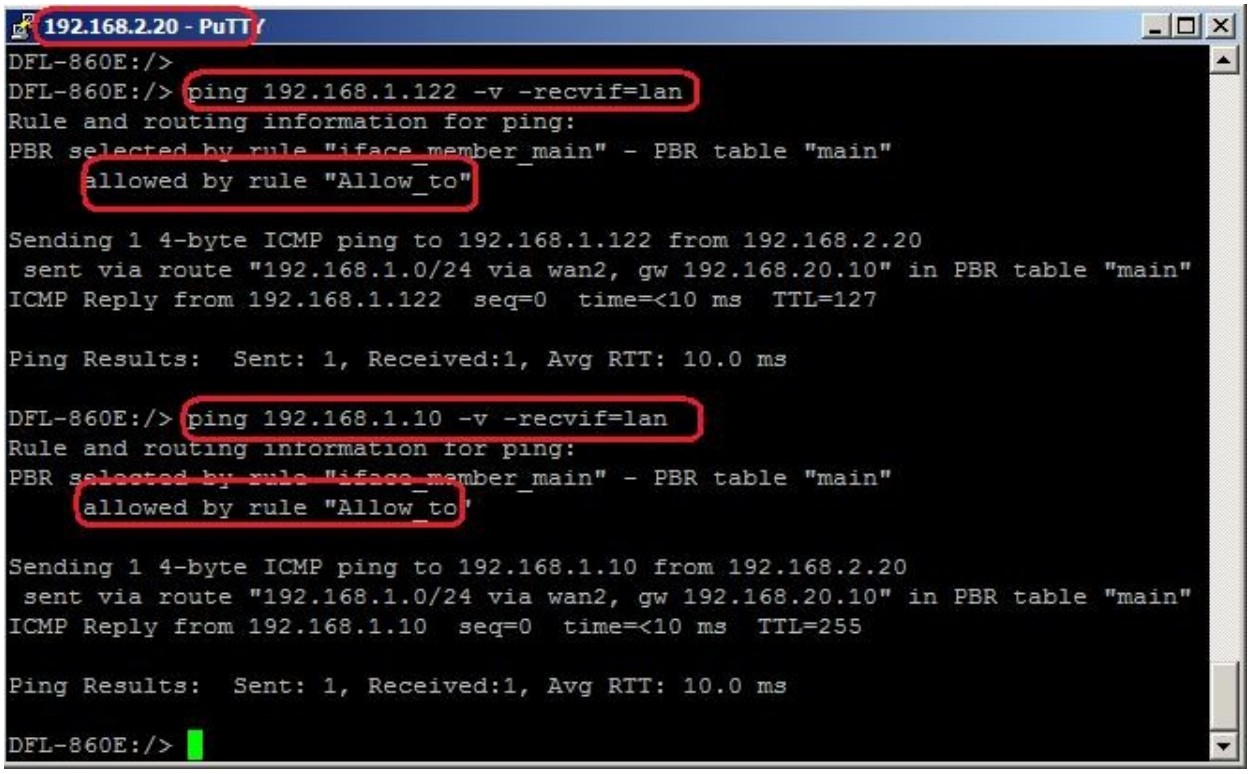
```
cc RoutingTable main
add Route Interface=wan2 Network=remote/rem_lan Gateway=wan2/wan2 Metric=100
```

Межсетевой Экран 2

Следует выполнить настройки, аналогичные настройкам, сделанным на Межсетевом Экране 1.

Проверка конфигурации

Проверяем доступ (команда **`ping`**) с lan-интерфейса межсетевого экрана 1 к рабочей станции в локальной сети (IP-адрес 192.168.1.122) и к lan-интерфейсу межсетевого экрана 1.

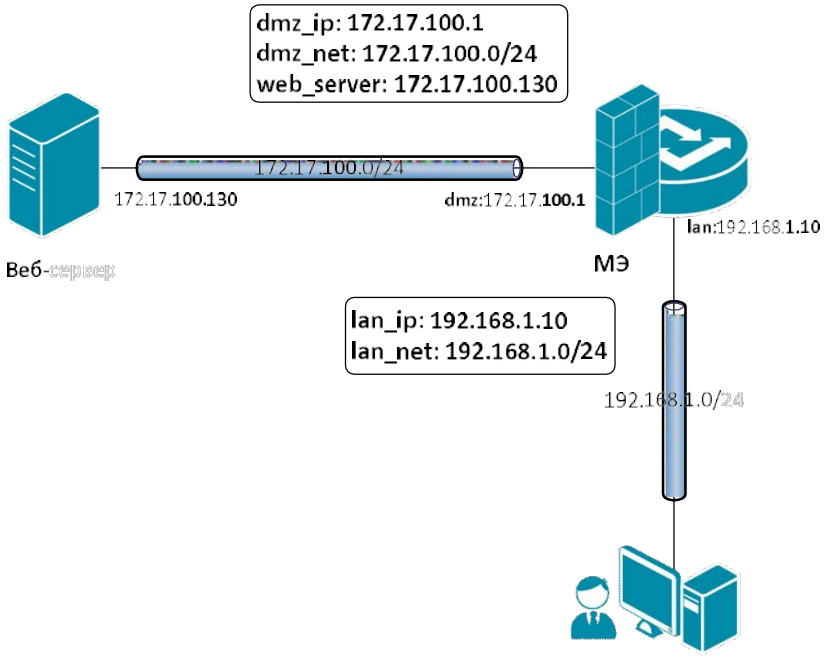


Практическая работа №39
Создание политики без проверки состояния

Цель

Создать политику без проверки состояния, которая должна разрешать http-трафик из локальной сети 192.168.1.0/24 к веб-серверу, расположенному в DMZ и имеющему IP-адрес 172.17.100.130.

Топология сети



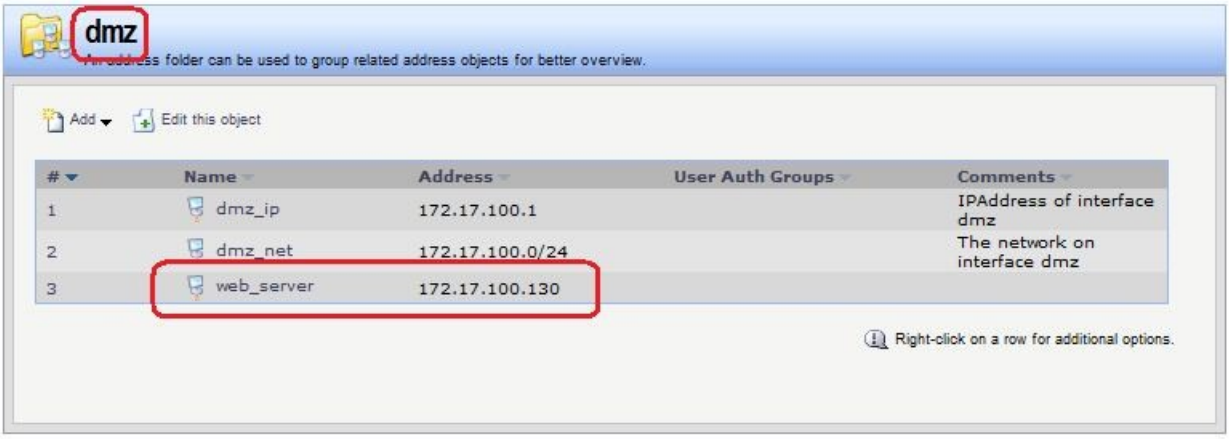
Описание практической работы

Объекты Адресной Книги

В адресную книгу следует добавить объект, указывающий IP-адрес веб-сервера.

Веб-интерфейс:

`Object → Address Book → dmz`



Командная строка:

```
cc Address AddressFolder dmz
add IP4Address web_server Address=172.17.100.130
```

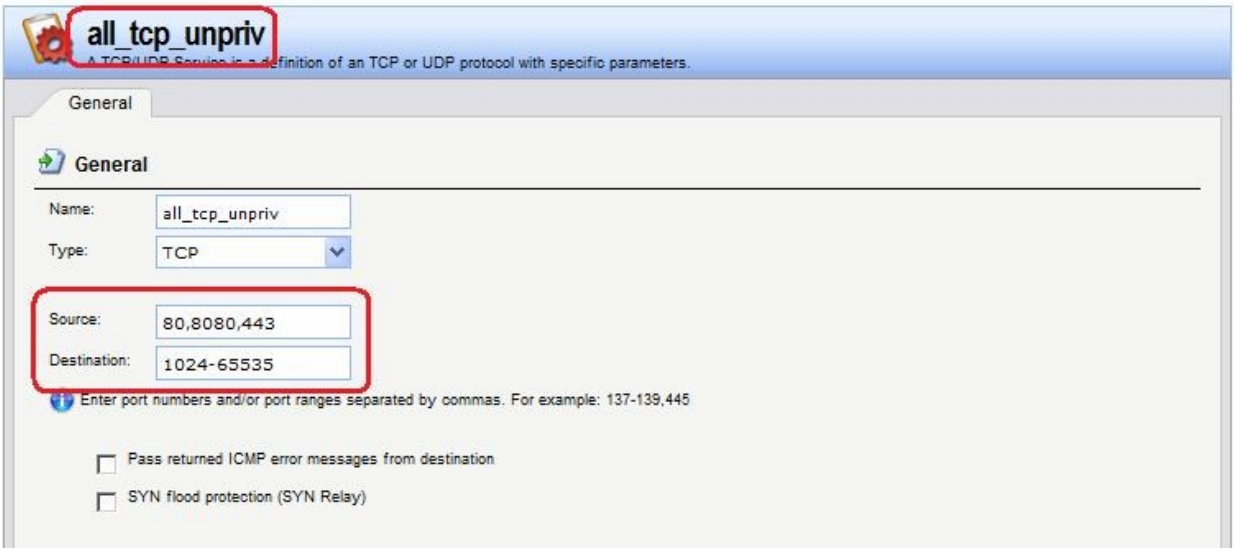
Правила фильтрования

Правила без проверки состояния будем создавать на межсетевом экране 1 (МЭ 1).

1. Создаем сервис, в котором в качестве портов отправителя указаны все необходимые порты HTTP, а в качестве портов получателя указаны все непривилегированные порты (так называемые порты с «большими» номерами).

Веб-интерфейс:

Object → Services → Add



Командная строка:

```
add Service ServiceTCPUDP all_tcp_unpriv DestinationPorts=1024-65535
SourcePorts=80,8080,443
```

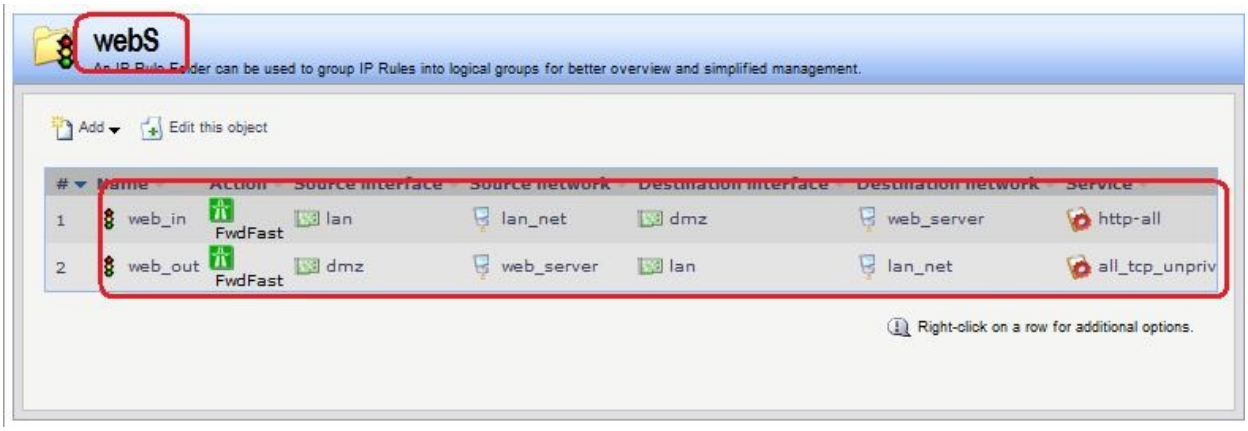
2. Создаем два правила фильтрования с действием **FwdFast**. В первом правиле в качестве сервиса указываем стандартный сервис **http-all**, в котором в качестве портов отправителя указаны все порты с непривилегированными («большими») номерами, а в качестве портов получателя указаны порты, необходимые веб-серверу. Во втором правиле в качестве сервиса указываем созданный в п.1 сервис. Для входящего трафика (**web_in**) открыты только порты, необходимые для протокола http. Для исходящего трафика (**web_out**) открыты все непривилегированные порты, так как на стороне клиента порт может быть любой.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: webS

Rules → IP Rules → webS → Add



Командная строка:

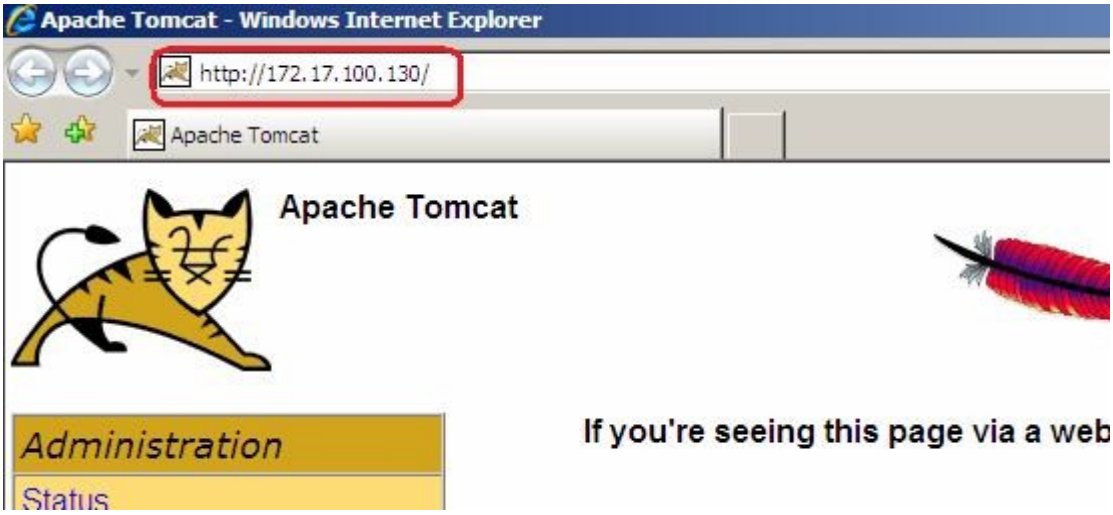
```
add IPRuleFolder Name=webS
cc IPRuleFolder <N folder>
add IPRule Action=FwdFast SourceInterface=lan SourceNetwork= lan/lan_net
DestinationInterface=dmz DestinationNetwork= dmz/web_server Service=http-all
Name=web_in
add IPRule Action=FwdFast SourceInterface=dmz SourceNetwork=dmz/web_server
DestinationInterface=lan DestinationNetwork=lan/lan_net
Service=all_tcp_unpriv Name=web_out
```

Статическая маршрутизация

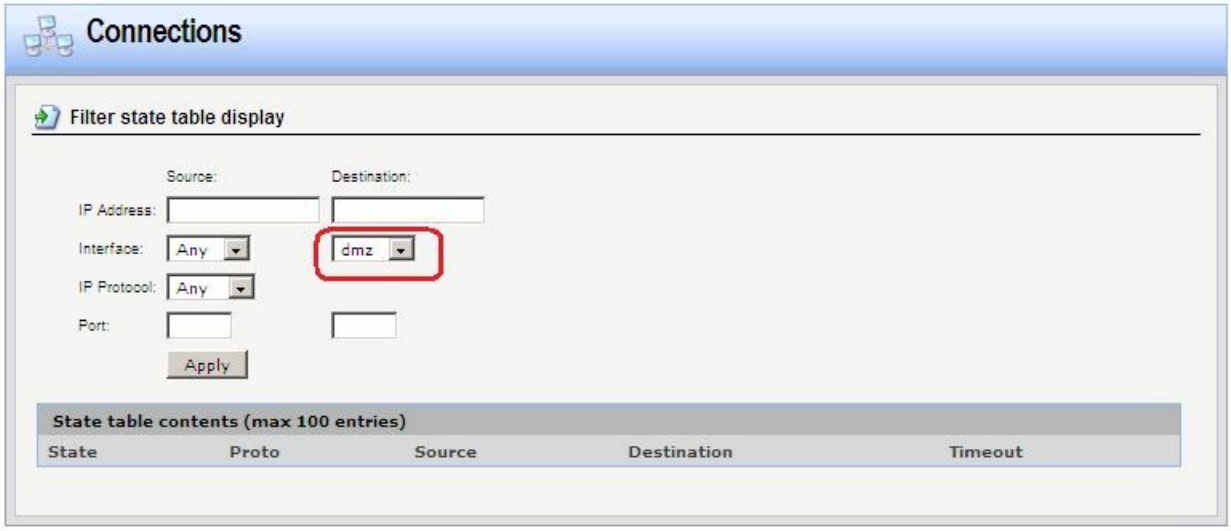
Правила маршрутизации созданы автоматически при определении параметров Ethernet-интерфейсов.

Проверка конфигурации

Лабораторная работа 5. Используем браузер, в качестве адреса указываем IP-адрес.



Лабораторная работа 6. Проверяем, что таблица состояний для интерфейса **dmz** пустая.



Практическая работа №40

Создание политик для традиционного (илиисходящего) NAT

Цель

Создать политики для доступа пользователей, расположенных за NAT, во внешнюю сеть.

Топология сети

Описание практической работы

Статическая маршрутизация

Правила маршрутизации созданы автоматически при определении параметров Ethernet-интерфейсов.

Правила фильтрования

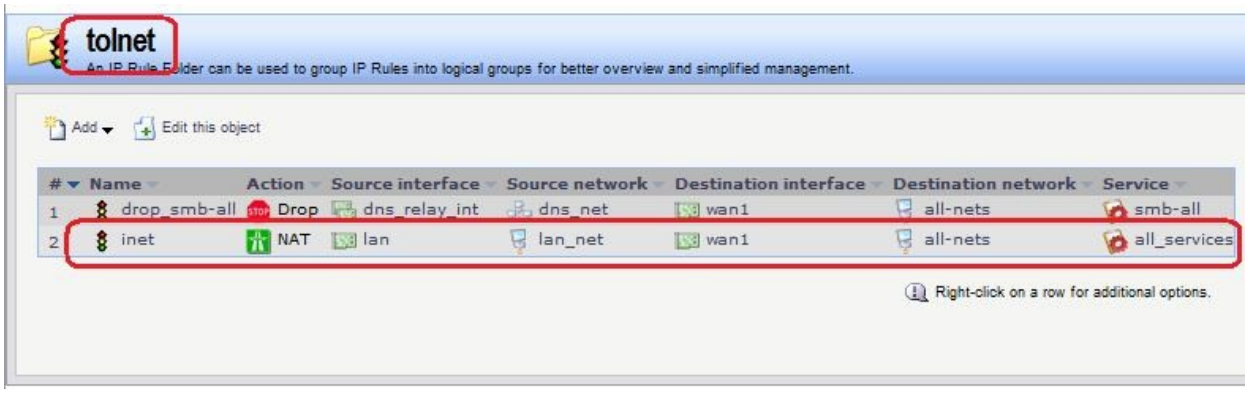
Создаем правило с действием **NAT**.

Веб-интерфейс:

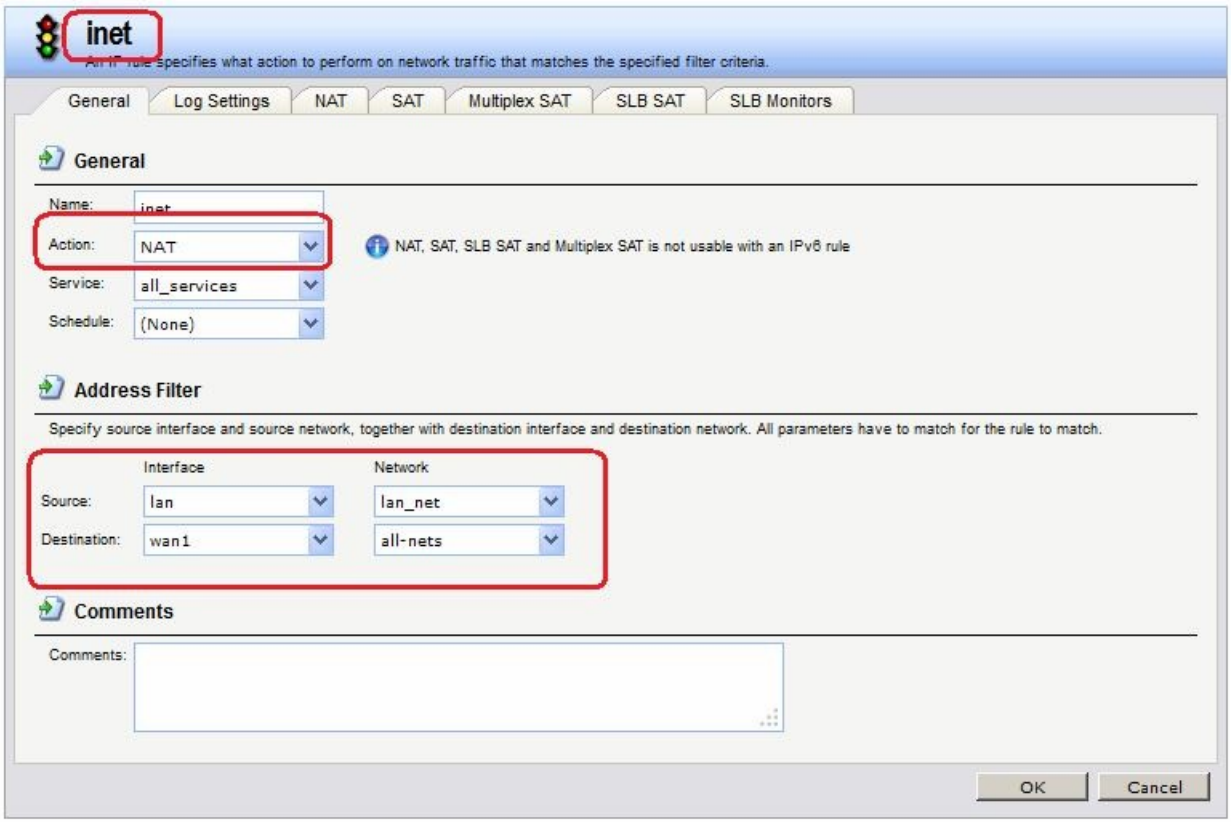
Rules → IP Rules → Add → IP Rule Folder

Name: toInet

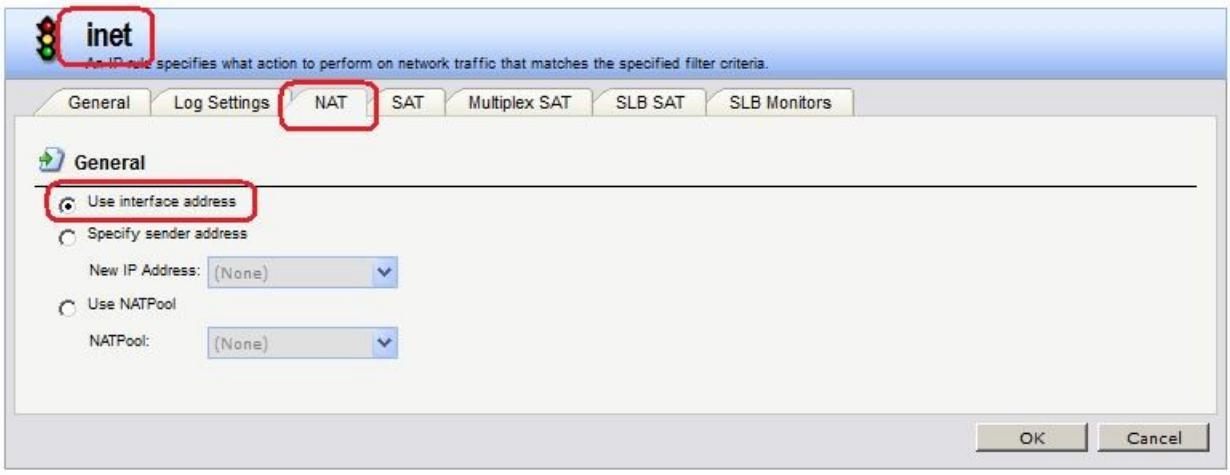
Rules → IP Rules → Add → toInet



На вкладке **`General`** указано действие **`NAT`** и интерфейсы и сети источника и получателя:



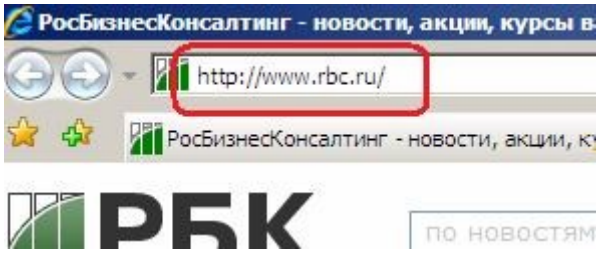
1. На вкладке **`NAT`** указано использование адреса интерфейса в качестве адреса источника:



Командная строка:

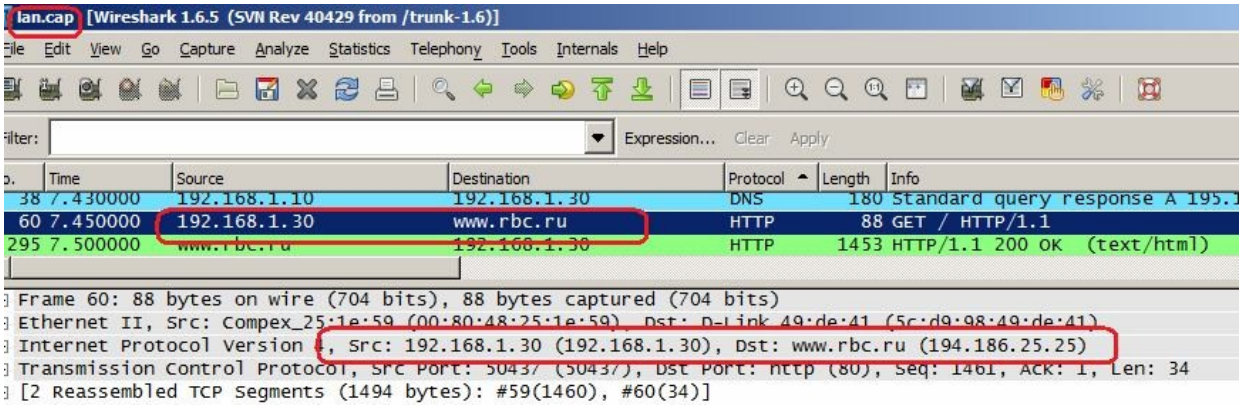
```
add IPRuleFolder Name=toInet
cc IPRuleFolder <N folder>
add IPRule Action=NAT SourceInterface=lan SourceNetwork= lan/lan_net
DestinationInterface=wan1 DestinationNetwork= all-nets Service=all_services
Name=inet
```

Проверяем возможность выхода в интернет.

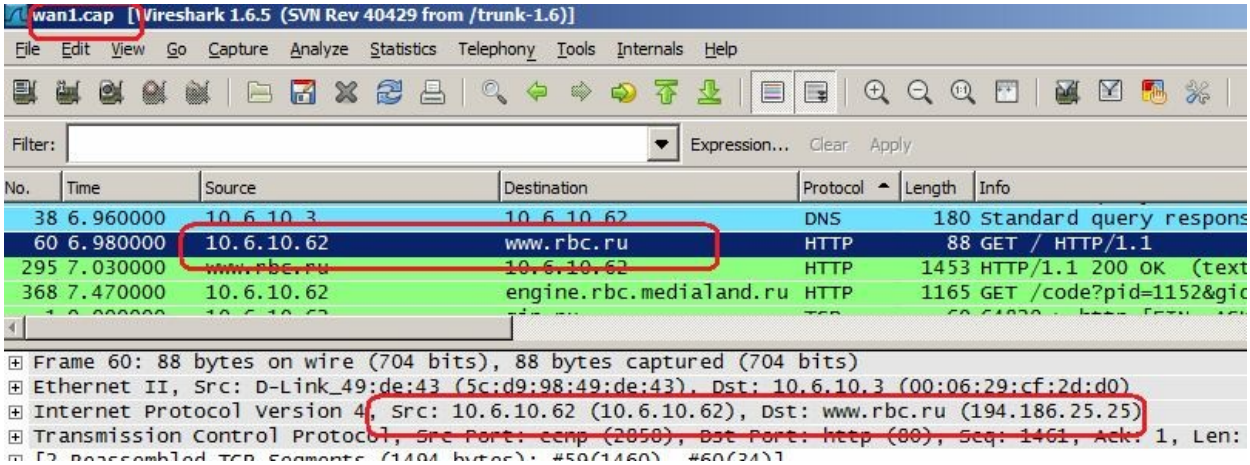


Проверяем выполнение преобразования NAT.

До преобразования NAT:



После преобразования NAT:



2. На вкладке **NAT** указан IP-адрес, который будет использоваться в качестве IP-адреса источника. Данный IP-адрес должен быть предварительно создан в Адресной Книге.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

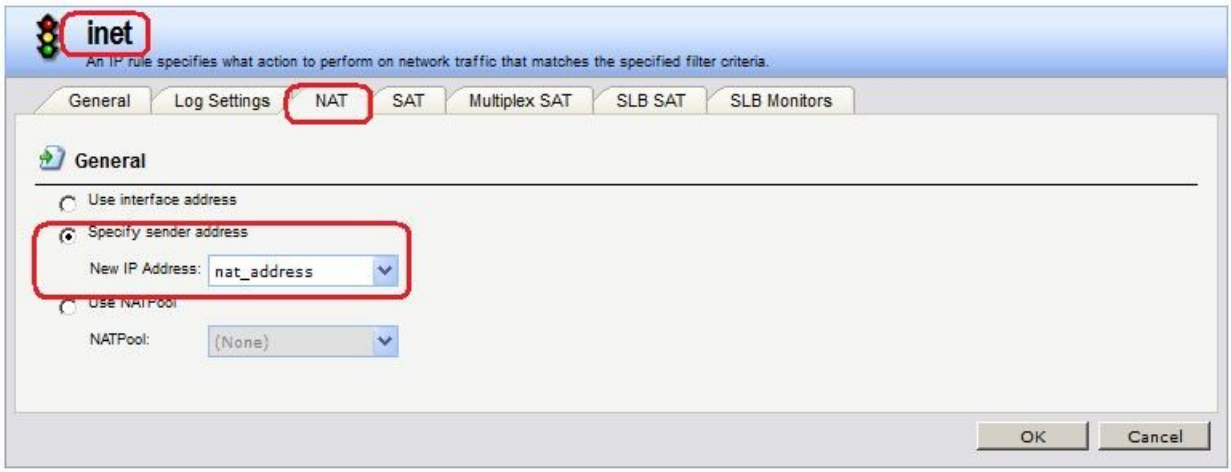
Name: nat

Object → Address Book → nat

Командная строка:

```
add Address AddressFolder nat
cc Address AddressFolder nat
add IP4Address nat_address Address=10.6.10.70
```

Веб-интерфейс:

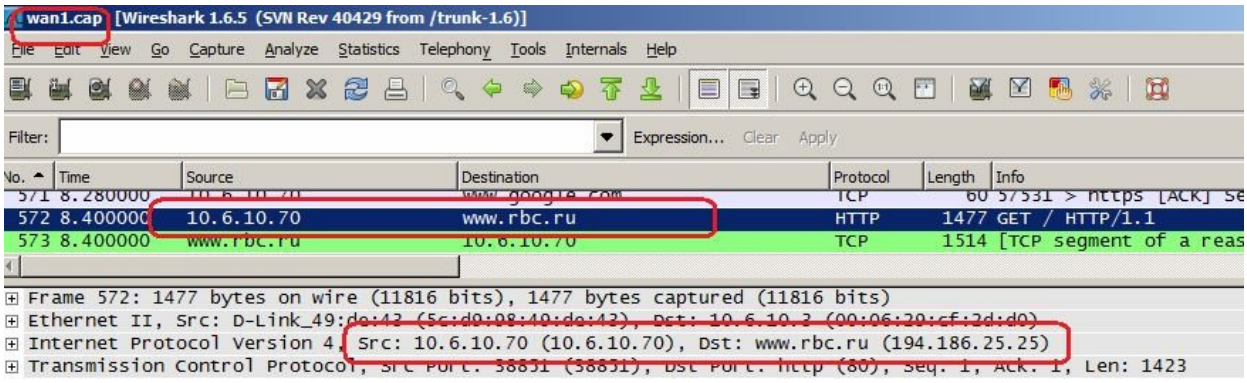


Командная строка:

```
cc IPRuleFolder <N folder>
set IPRule <N rule> NATAction=SpecifySenderAddress
NATSenderAddress=nat/nat_address
```

Проверяем выполнение преобразования NAT.

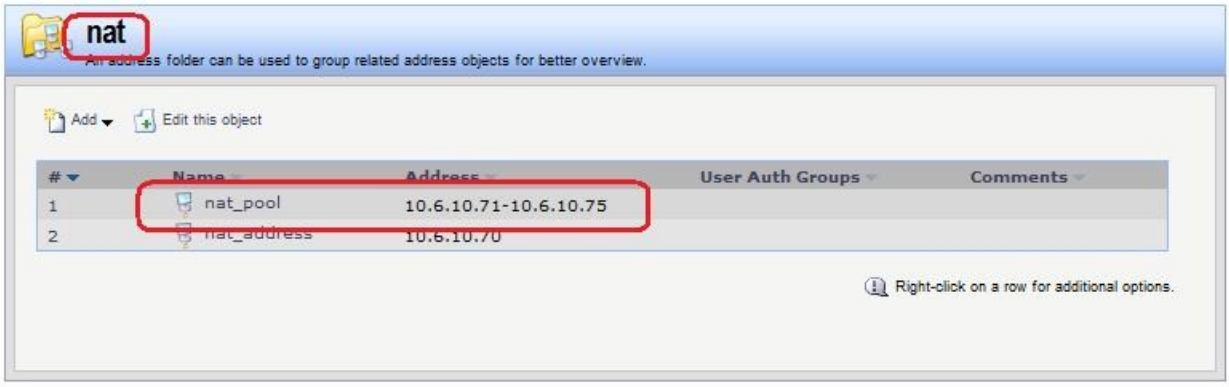
После преобразования NAT:



Лабораторная работа 7. На вкладке **NAT** указано использование NAT-пула, IP-адреса из которого будут использоваться в качестве IP-адреса источника. Данный NAT-пул должен быть предварительно создан.

Веб-интерфейс:

Object → Address Book → nat

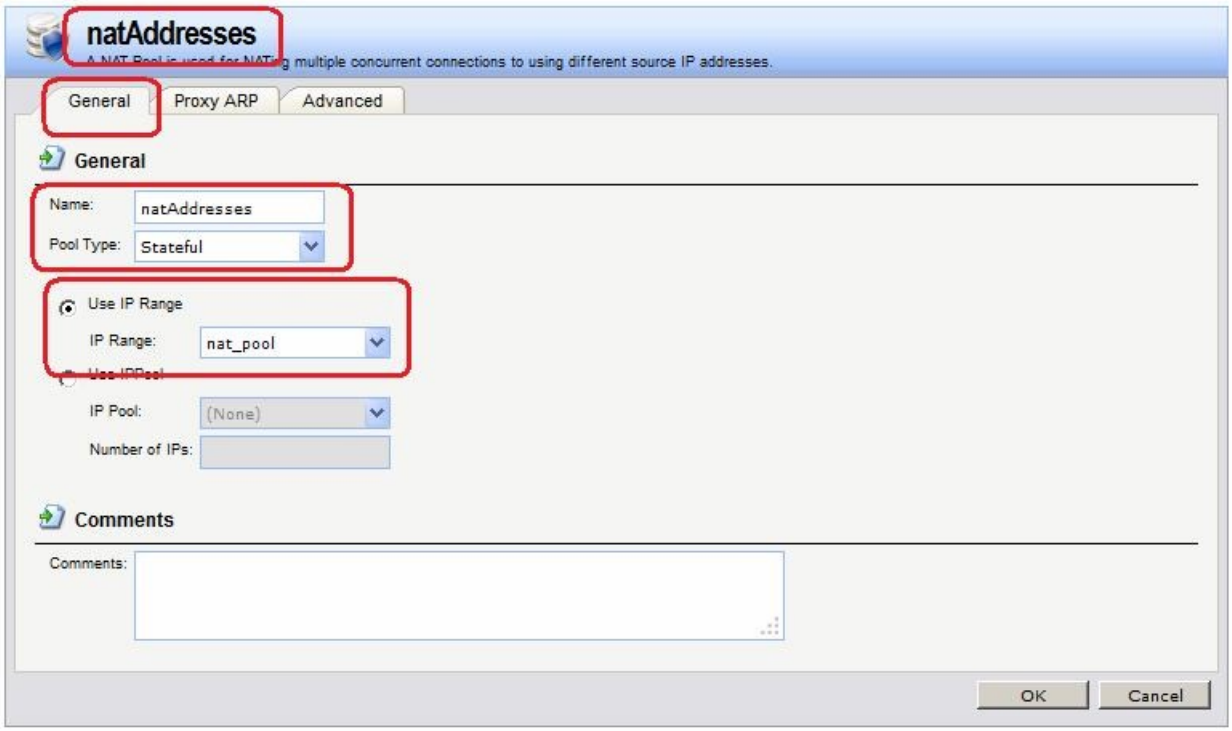


Командная строка:

```
cc Address AddressFolder nat
add IP4Address nat_pool Address=10.6.10.71-10.6.10.75
```

Веб-интерфейс:

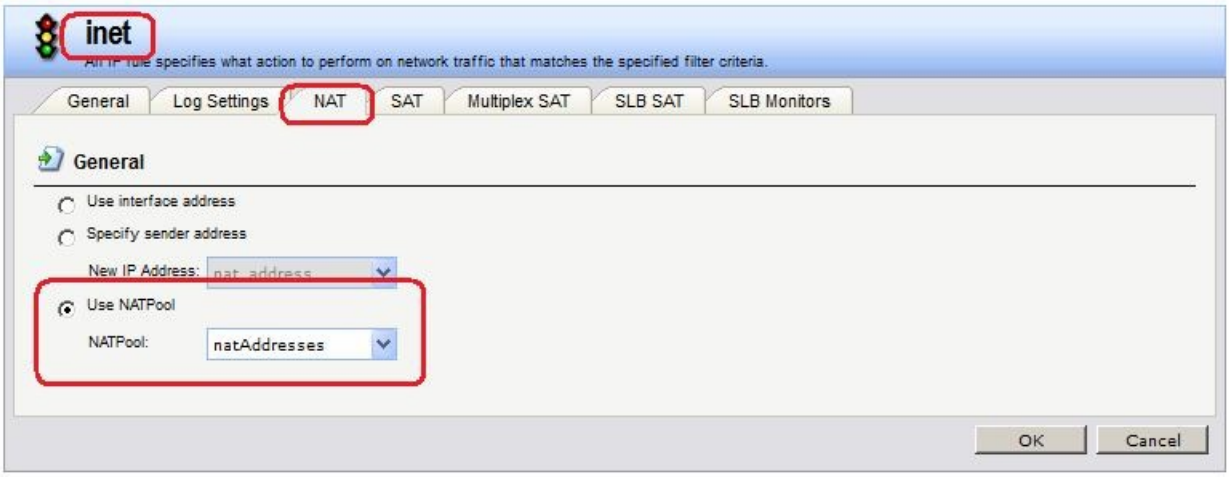
Object → NAT Pools → Add



Командная строка:

```
add NATPool natAddresses IPRange=nat/nat_pool
```

Веб-интерфейс:

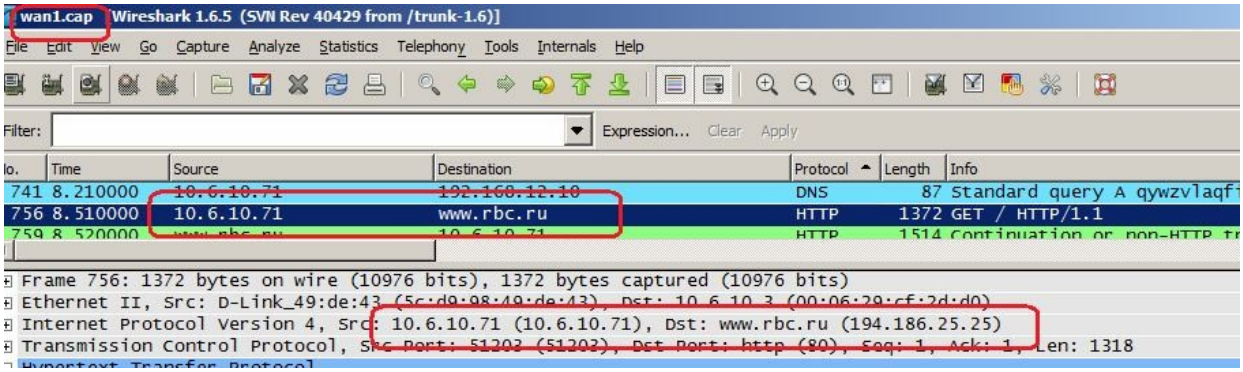


Командная строка:

```
cc IPRuleFolder <N folder>
set IPRule <N rule> NATAction=UseNATPool NATPool=natAddresses
```

Проверяем выполнение преобразования NAT.

После преобразования NAT:



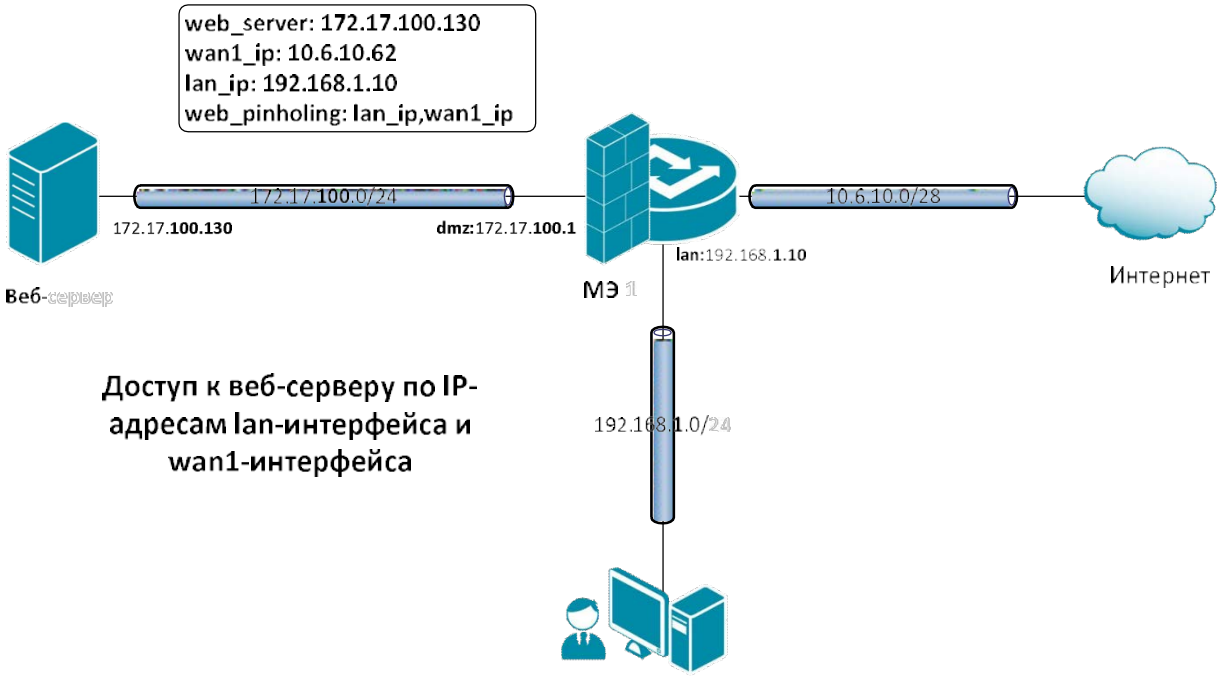
Практическая работа №41

Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing

Цель

Создать политики для доступа к серверу, расположенному за NAT, используя метод pinholing, т.е. используя IP-адрес межсетевого экрана.

Топология сети



Описание практической работы

Проверка отсутствия конфликта по портам

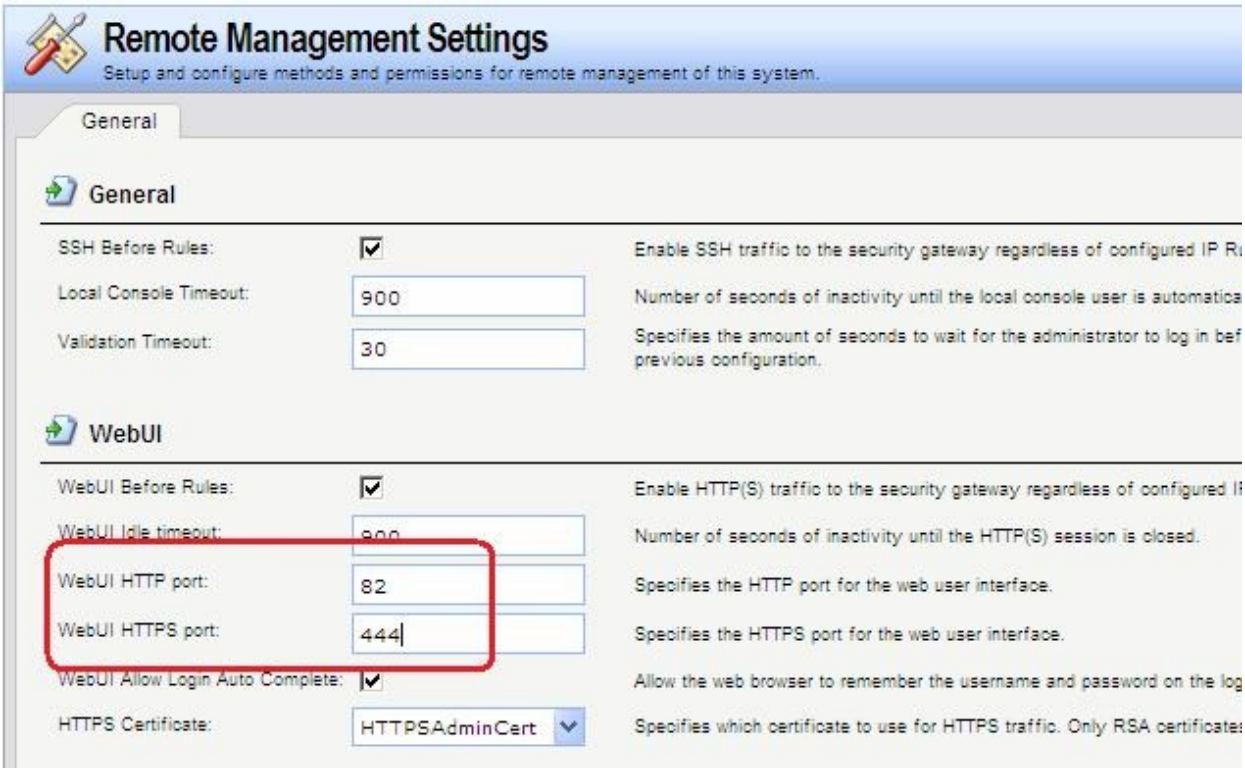
Метод pinholing некоторые производители называют SAT.

К веб-серверу будут обращаться по IP-адресу МЭ 1, поэтому следует гарантировать отсутствие конфликта по портам с удаленным администрированием МЭ 1. Это можно сделать несколькими способами.

1. Указать номер порта для удаленного администрирования, отличный от номера порта веб-сервера.

Веб-интерфейс:

`System → Remote Management → Advanced Settings`



Командная строка:

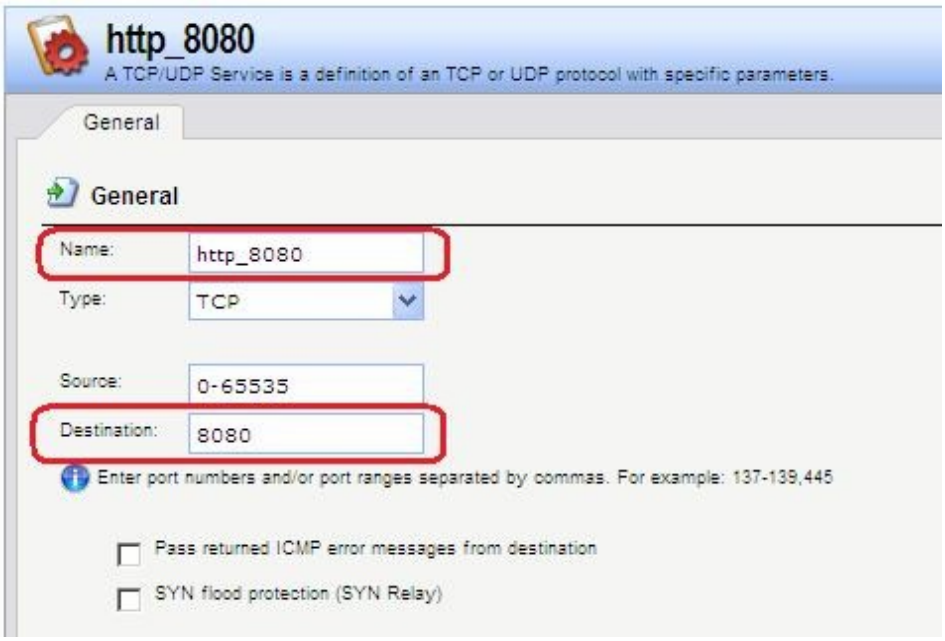
```
set Settings RemoteMgmtSettings WWWSrv_HTTPPort=82 WWWSrv_HTTPSPort=444
```

2. Указать номер порта для доступа к веб-серверу, отличный от номера порта для удаленного администрирования. При этом номер порта на самом веб-сервере можно не изменять, достаточно создать новый http-сервис с номером порта, отличным от порта удаленного администрирования. Будем предполагать, что используется второй способ.

Веб-интерфейс:

Object → Services → Add

Name: http_8080



Командная строка:

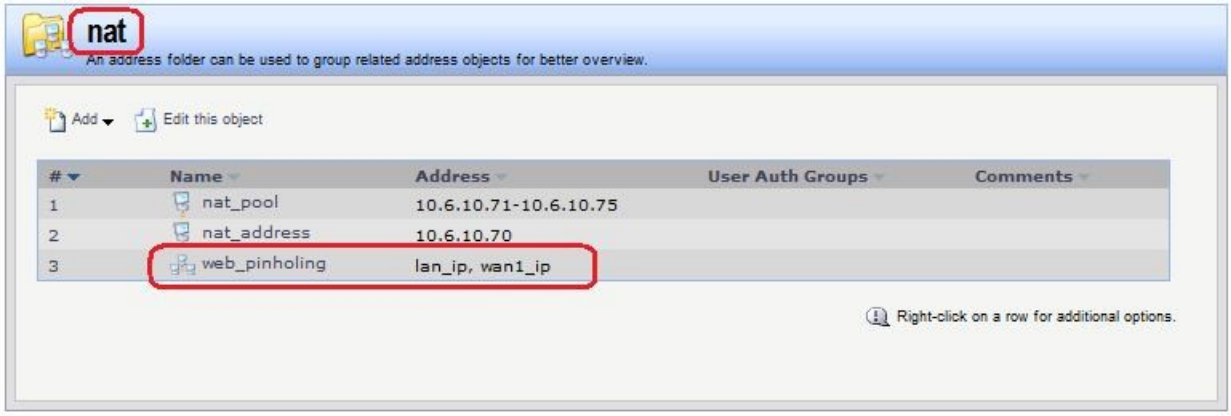
```
add Service ServiceTCPUDP http_8080 DestinationPorts=8080 SourcePorts=0-65535
```

Объекты Адресной Книги

Чтобы иметь возможность использовать в качестве адреса веб-сервера IP-адреса интерфейсов, к которым подсоединены сети, а также для того, чтобы в правилах фильтрования доступ к веб-серверу описать с помощью единственного правила, создадим дополнительные объекты в Адресной Книге.

Веб-интерфейс:

Object → Address Book → nat



Командная строка:

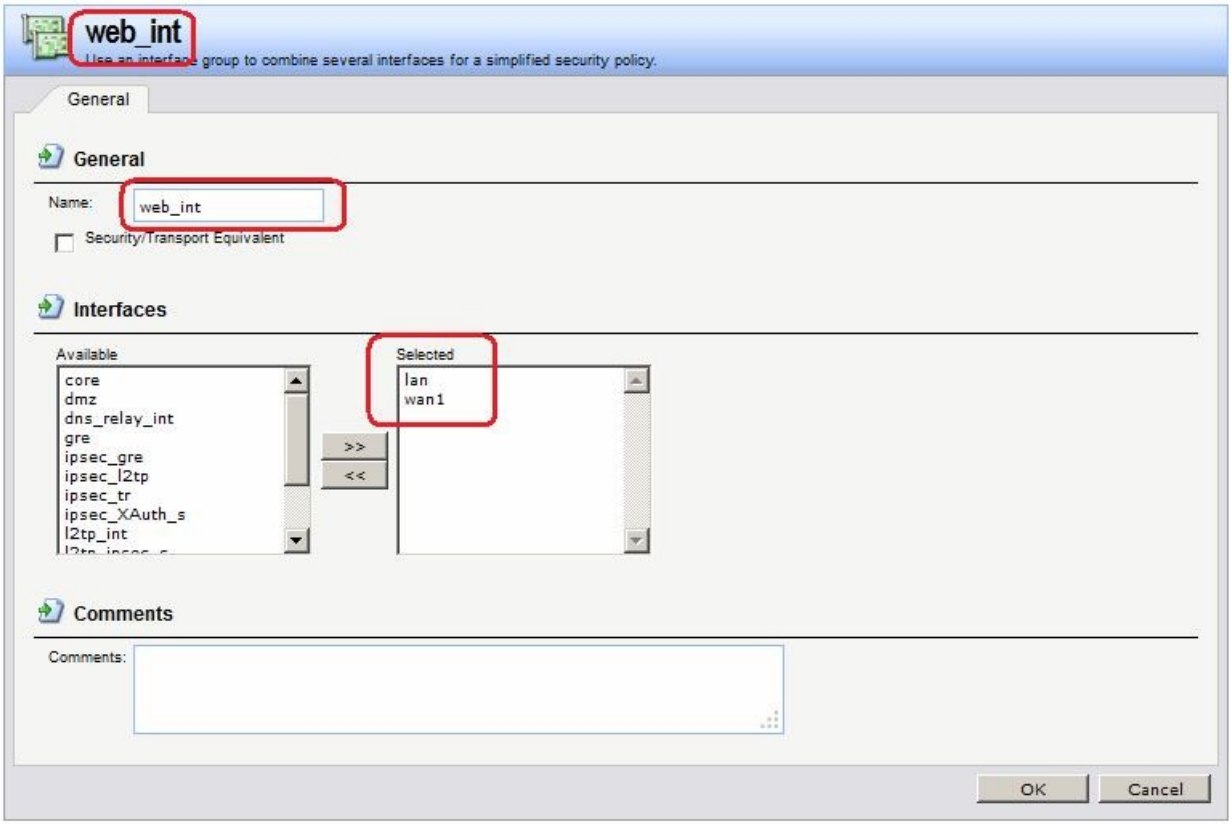
```
cc Address AddressFolder nat
add IP4Group web_pinholing Members =lan/lan_ip, wan1/wan1_ip
```

Группа интерфейсов

Объединить интерфейсы в Группу, чтобы несколько интерфейсов можно было указывать одним параметром в Правилах фильтрования.

Веб-интерфейс:

Interfaces → Interface Group → Add



Командная строка:

```
add Interface InterfaceGroup web_int Members=lan,wan1
```

Правила фильтрования

Создать два правила фильтрования с действием **SAT**. В первом правиле качестве сервиса указать http, во втором правиле - https. Интерфейсом получателя должен быть core. Адрес получателя – IP-адреса интерфейсов, которые будут указываться клиентом в качестве веб-сервера. В нашем случае это группа интерфейсов web_int.

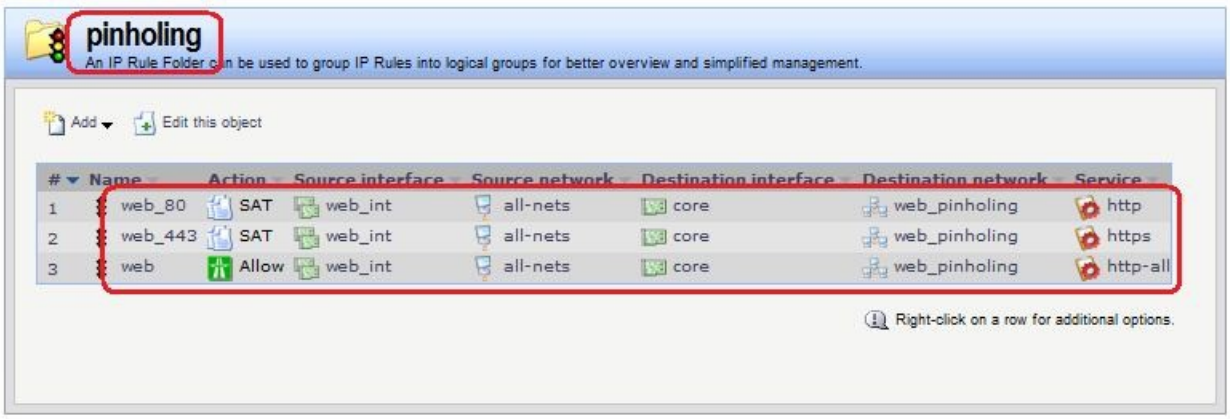
Создать правило фильтрования с действием **Allow**.

Веб-интерфейс:

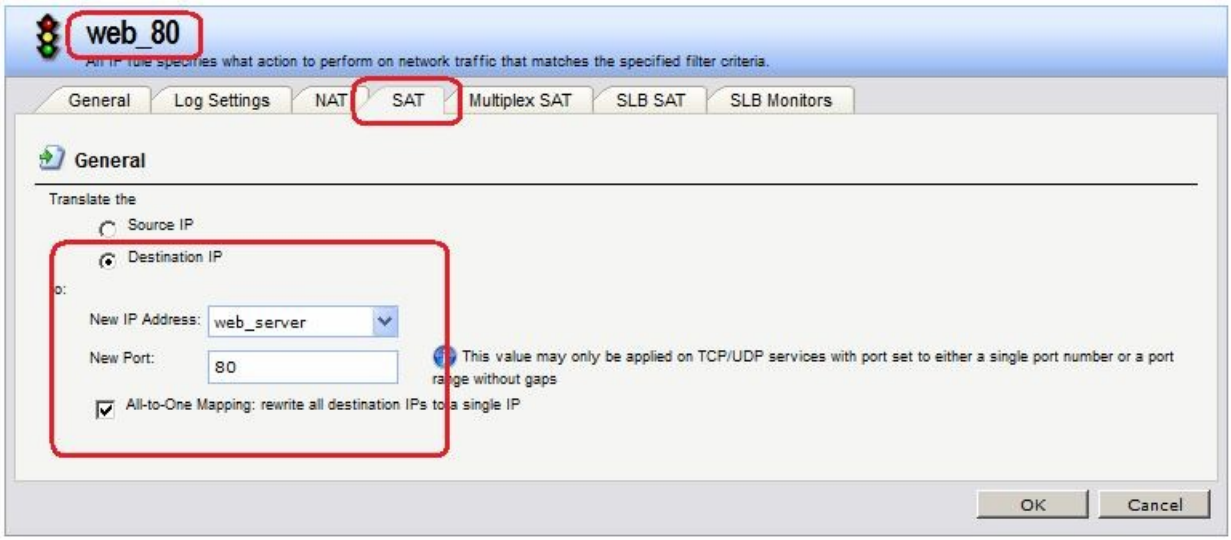
Rules → IP Rules → Add → IP Rule Folder

Name: pinholing

Rules → IP Rules → pinholing → Add



На вкладке **SAT** указать адрес веб-сервера и порт, который он слушает. Если необходимо, чтобы веб-сервер слушал несколько портов, например, 80 (http) и 443 (https), то требуется два правила **SAT**.



Командная строка:

```
cc IPRuleFolder <N Folder>
```

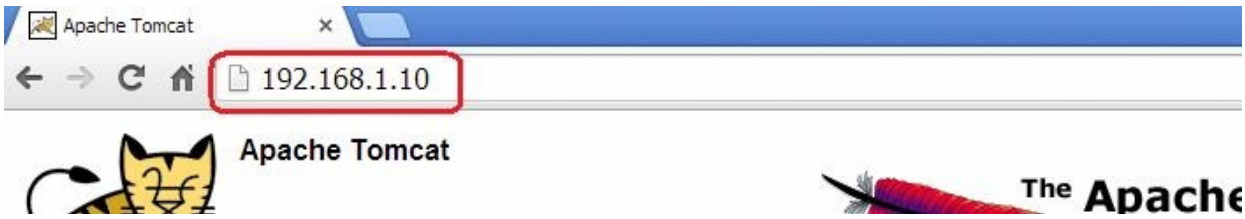
```
add IPRule Action=SAT SourceInterface=web_int SourceNetwork=all-nets
DestinationInterface=core DestinationNetwork=nat/web_pinholing Service=http
SATTranslateToIP=dmz/web_server SATAllToOne=Yes SATTranslateToPort=80
Name=web_80
```

```
add IPRule Action=SAT SourceInterface=web_int SourceNetwork=all-nets
DestinationInterface=core DestinationNetwork=nat/web_pinholing Service=https
SATTranslateToIP=dmz/web_server SATAllToOne=Yes SATTranslateToPort=443
Name=web_443
```

```
add IPRule Action=Allow SourceInterface=web_int SourceNetwork=all-nets
DestinationInterface=core DestinationNetwork=nat/web_pinholing Service=http-
all Name=web
```

Проверка конфигурации

Заходим браузером по IP-адресу МЭ 1 и сконфигурированному номеру порта.


Apache Tomcat
192.168.1.10
Apache Tomcat
The Apache

Практическая работа №42

Обнаружение и предотвращение вторжений

Принципы использования IDS

Обнаружение и предотвращение вторжений (IDP) является подсистемой NetDefendOS, которая предназначена для защиты от попыток вторжения. Система просматривает сетевой трафик, проходящий через межсетевой экран, и ищет трафик, соответствующий шаблонам. Обнаружение такого трафика указывает на попытку вторжения. После обнаружения подобного трафика IDP выполняет шаги по нейтрализации как вторжения, так и его источника.

Для обнаружения и предотвращения вторжения, необходимо указать следующую информацию:

1. Какой трафик следует анализировать.
2. Что следует искать в анализируемом трафике.
3. Какое действие необходимо предпринять при обнаружении вторжения.

Эта информация указывается в **IDP-правилах**.

Maintenance и Advanced IDP

Компания D-Link предоставляет два типа IDP:

1. **Maintenance IDP**

Maintenance IDP является основой системы IDP и включено в стандартную комплектацию NetDefend DFL-210, 800, 1600 и 2500.

Maintenance IDP является упрощенной IDP, что обеспечивает базовую защиту от атак, и имеет возможность расширения до более комплексной *Advanced IDP*.

IDP не входит в стандартную комплектацию DFL-260, 860, 1660, 2560 и 2560G; для этих моделей межсетевых экранов необходимо приобрести подписку на *Advanced IDP*.

2. **Advanced IDP**

Advanced IDP является расширенной системой IDP с более широким диапазоном баз данных сигнатур и предъявляет более высокие требования к оборудованию. Стандартной является подписка сроком на 12 месяцев, обеспечивающая автоматическое обновление базы данных сигнатур IDP.

Эта опция IDP доступна для всех моделей D-Link NetDefend, включая те, в стандартную комплектацию которых не входит *Maintenance IDP*.

Maintenance IDP можно рассматривать, как ограниченное подмножество *Advanced IDP*. Рассмотрим функционирование *Advanced IDP*.

Advanced IDP приобретается как дополнительный компонент к базовой лицензии NetDefendOS. Подписка означает, что база данных сигнатур IDP может быть загружена на NetDefendOS, а также, что база данных регулярно обновляется по мере появления новых угроз.

Обновления базы данных сигнатур автоматически загружаются системой NetDefendOS через сконфигурированный интервал времени. Это выполняется с помощью HTTP-соединения с сервером сети D-Link, который предоставляет последние обновления базы данных сигнатур. Если на сервере существует новая версия базы данных сигнатур, она будет загружена, заменив старую версию.

Термины Intrusion Detection and Prevention (IDP), Intrusion Prevention System (IDP) и Intrusion Detection System (IDS) взаимозаменяют друг друга. Все они относятся к функции IDP.

Последовательность обработка пакетов

Последовательность обработки пакетов при использовании IDP является следующей:

1. Пакет приходит на межсетевой экран. Если пакет является частью нового соединения, то первым делом ищется соответствующее IP-правило фильтрования. Если пакет является частью существующего соединения, он сразу же попадает в модуль IDP. Если пакет не является частью существующего соединения или отбрасывается IP-правилом, то дальнейшей обработки данного пакета не происходит.
2. Адреса источника и назначения пакета сравниваются с набором правил IDP. Если найдено подходящее правило, то пакет передается на обработку системе IDP, в которой ищется совпадение содержимого пакета с одним из шаблонов. Если совпадения не обнаружено, то пакет пропускается системой IDP. Могут быть определены дальнейшие действия в IP-правилах фильтрования, такие как NAT и создание логов.

Поиск на соответствие шаблону

Сигнатуры

Для корректного определения атак система IDP использует *шаблоны*, связанные с различными типами атак. Эти предварительно определенные шаблоны, также называемые *сигнатурами*, хранятся в локальной базе данных и используются системой IDP для анализа трафика. Каждая сигнатура имеет уникальный номер.

Рассмотрим пример простой атаки, состоящий в обращении к FTP-серверу. Неавторизованный пользователь может попытаться получить файл паролей **`passwd`** с FTP-сервера с помощью команды FTP **`RETR passwd`**. Сигнатура, содержащая текстовые строки ASCII **`RETR`** и **`passwd`**, обнаружит соответствие, указывающее на возможную атаку. В данном примере шаблон задан в виде текста ASCII, но поиск на соответствие шаблону выполняется аналогично и для двоичных данных.

Распознавание неизвестных угроз

Злоумышленники, разрабатывающие новые атаки, часто просто модифицируют старый код. Это означает, что новые атаки могут появиться очень быстро как расширение и обобщение старых. Чтобы противостоять этому, D-Link IDP использует подход, при котором модуль выполняет сканирование, учитывая возможное многократное использование компонент, выявляя соответствие шаблону общих блоков, а не конкретного кода. Этим достигается защита как от известных, так и от новых, недавно разработанных, неизвестных угроз, созданных модификацией программного кода атаки.

Описания сигнатур

Каждая сигнатур имеет пояснительное текстовое описание. Прочитав текстовое описание сигнатуры, можно понять, какую атаку или вирус поможет обнаружить данная сигнатура. В связи с изменением характера базы данных сигнатур, текстовые описания не содержатся в документации D-Link, но доступны на Web-сайте D-Link: http://security.dlink.com.tw

Типы сигнатур IDP

В IDP имеется три типа сигнатур, которые предоставляют различные уровни достоверности в определении угроз:

- **Intrusion Protection Signatures (IPS)** – Данный тип сигнатур обладает высокой точностью, и соответствие трафика данному шаблону в большинстве случаев означает атаку. Для данных угроз рекомендуется указывать действие **`Protect`**. Эти сигнатуры могут обнаружить действия, направленные на получение прав администратора, и сканеры безопасности.
- **Intrusion Detection Signatures (IDS)** – У данного типа сигнатур меньше точности, чем у IPS, и они могут дать иметь ложные срабатывания, таким образом, поэтому перед тем как указывать действие **`Protect`** рекомендуется использовать действие **`Audit`**.
- **Policy Signatures** - Этот тип сигнатур обнаруживает различные типы прикладного трафика. Эти сигнатуры могут использоваться для блокировки некоторых приложений, предназначенных для совместного использования приложений и мгновенного обмена сообщениями.

Предотвращение атак Denial-of-Service

Механизмы DoS-атак

DoS-атаки могут выполняться самыми разными способами, но все они могут быть разделены на три основных типа:

- Исчерпание вычислительных ресурсов, таких как полоса пропускания, дисковое пространство, время ЦП.
- Изменение конфигурационной информации, такой как информация маршрутизации.
- Порча физических компонентов сети.

Одним из наиболее часто используемых методов является исчерпание вычислительных ресурсов, т.е. невозможность нормального функционирования сети из-за большого количества запросов, часто неправильно сформатированных, и расходования ресурсов, используемых для запуска критически важных приложений. Могут также использоваться уязвимые места в операционных системах Unix и Windows для преднамеренного разрушения системы.

Перечислим некоторые из наиболее часто используемых DoS-атак:

- Ping of Death / атаки Jolt
- Перекрытие фрагментов: Teardrop / Bonk / Boink / Nestea
- Land и LaTierra атаки
- WinNuke атака
- Атаки с эффектом усиления: Smurf, Papasmurf, Fraggle
- TCP SYN Flood
- Jolt2

Атаки Ping of Death и Jolt

«Ping of Death» является одной из самых ранних атак, которая выполняется на 3 и 4 уровнях стека протоколов. Один из простейших способов выполнить эту атаку - запустить **`ping -l 65510 1.2.3.4`** на Windows 95, где 1.2.3.4 - это IP-адрес компьютера-жертвы. «Jolt» – это специально написанная программа для создания пакетов в операционной системе, в которой команда **`ping`** не может создавать пакеты, размеры которых превышают стандартные нормы.

Смысл атаки состоит в том, что общий размер пакета превышает 65535 байт, что является максимальным значением, которое может быть представлено 16-битным целым числом. Если размер больше, то происходит переполнение.

Защита состоит в том, чтобы не допустить фрагментацию, приводящую к тому, что общий размер пакета превышает 65535 байт. Помимо этого, можно настроить ограничения на длину IP-пакета.

Атаки Ping of Death и Jolt регистрируются в логах как отброшенные пакеты с указанием на правило «LogOversizedPackets». Следует помнить, что в этом случае IP-адрес отправителя может быть подделан.

Атаки, связанные с перекрытием фрагментов: Teardrop, Bonk, Boink и Nestea

Teardrop - это атака, связанная с перекрытием фрагментов. Многие реализации стека протоколов плохо обрабатывают пакеты, при получении которых имеются

перекрывающиеся фрагменты. В этом случае возможно как исчерпание ресурсов, так и сбой.

NetDefendOS обеспечивает защиту от атак перекрытия фрагментов. Перекрывающимся фрагментам не разрешено проходить через систему.

Teardrop и похожие атаки регистрируются в логах NetDefendOS как отброшенные пакеты с указанием на правило «IllegalFrags». Следует помнить, что в этом случае IP-адрес отправителя может быть подделан.

Атаки Land и LaTierra

Атаки Land и LaTierra состоят в посылке такого пакета компьютеру-жертве, который заставляет его отвечать самому себе, что, в свою очередь, генерирует еще один ответ самому себе, и т.д. Это вызовет либо полную остановку работы компьютера, либо крах какой-либо из его подсистем

Атака состоит в использовании IP-адреса компьютера-жертвы в полях **`Source`** и **`Destination`**.

NetDefendOS обеспечивает защиту от атаки Land, используя защиту от IP-спуфинга ко всем пакетам. При использовании настроек по умолчанию все входящие пакеты сравниваются с содержанием таблицы маршрутизации; если пакет приходит на интерфейс, с которого невозможно достигнуть IP-адреса источника, то пакет будет отброшен.

Атаки Land и LaTierra регистрируются в логах NetDefendOS как отброшенные пакеты с указанием на правило по умолчанию **`AutoAccess`**, или, если определены другие правила доступа, указано правило правило доступа, в результате которого отброшен пакет. В данном случае IP-адрес отправителя не представляет интереса, так как он совпадает с IP-адресом получателя.

Атака WinNuke

Принцип действия атаки WinNuke заключается в подключении к TCP-сервису, который не умеет обрабатывать «out-of-band» данные (TCP-пакеты с установленным битом **`URG`**), но все же принимает их. Это обычно приводит к зацикливанию сервиса и потреблению всех ресурсов процессора.

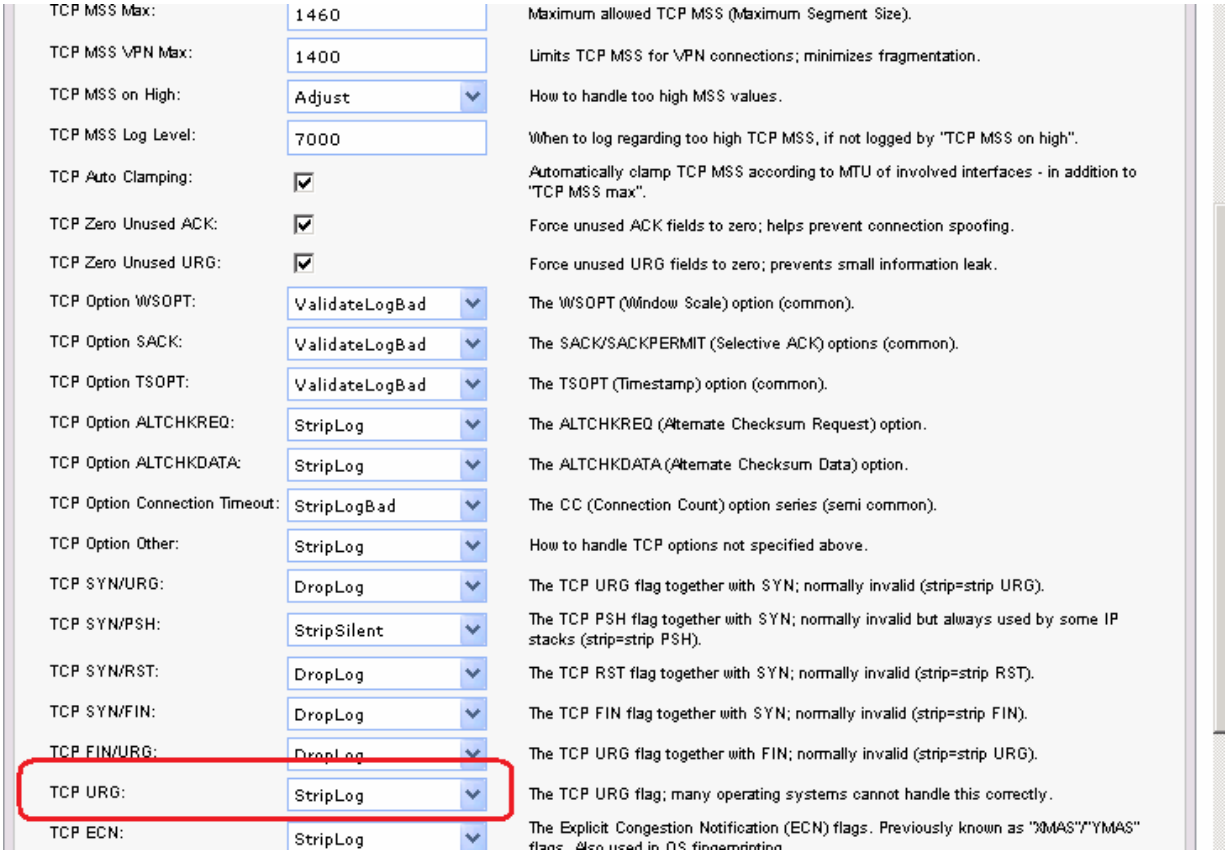
Одним из таких сервисов был NetBIOS через TCP/IP на WINDOWS-машинах, которая и дала имя данной сетевой атаке.

NetDefendOS обеспечивает защиту двумя способами:

- Политики для входящего трафика как правило разработаны достаточно тщательно, поэтому количество успешных атак незначительно. Извне доступны только публичные сервисы, доступ к которым открыт. Только они могут стать жертвами атак.
- Удаление бита **`URG`** из всех TCP-пакетов.

Веб-интерфейс

`Advanced Settings → TCP → TCPUrg`



Как правило, атаки WinNuke регистрируются в логах как отброшенные пакеты с указанием на правило, запретившего попытку соединения. Для разрешенных соединений появляется запись категории «TCP» или «DROP» (в зависимости от настройки TCPUrg), с именем правила «TCPUrg». IP-адрес отправителя может быть не поддельным, так как соединение должно быть полностью установлено к моменту отправки пакетов «out-of-band».

Атаки, приводящие к увеличению трафика: Smurf, Papasmurf, Fraggle

Эта категория атак использует некорректно настроенные сети, которые позволяют увеличивать поток трафика и направлять его целевой системе. Целью является интенсивное использование полосы пропускания жертвы. Атакующий с широкой полосой пропускания может не использовать эффект усиления, позволяющий полностью загрузить всю полосу пропускания жертвы. Эти атаки позволяют атакующим с меньшей полосой пропускания, чем у жертвы, использовать усиление, чтобы занять полосу пропускания жертвы.

- «Smurf» и «Papasmurf» отправляют эхо-пакеты ICMP по широковещательному адресу, указывая в качестве IP-адреса источника IP-адрес жертвы. После этого все компьютеры посылают ответные пакеты жертве.
- «Fraggle» базируется на «Smurf», но использует эхо-пакеты UDP и отправляет их на порт 7. В основном, атака «Fraggle» имеет более слабое усиление, так как служба echo активирована у небольшого количества хостов.

Атаки Smurf регистрируются в логах NetDefendOS как большое число отброшенных пакетов ICMP **`Echo Reply`**. Для подобной перегрузки сети может использоваться поддельный IP-адрес. Атаки Fraggle также отображаются в логах NetDefendOS как большое количество отброшенных пакетов. Для перегрузки сеть используется поддельный IP-адрес.

При использовании настроек по умолчанию пакеты, отправленные по адресу широковещательной рассылки, отбрасываются.

Веб-интерфейс

`Advanced Settings → IP → DirectedBroadcasts`

В политиках для входящего трафика следует учитывать, что любая незащищенная сеть может также стать источником подобных атак усиления.

Защита на стороне компьютера-жертвы

Smurf и похожие атаки являются атаками, расходующими ресурсы соединения. В общем случае межсетевой экран является узким местом в сети и не может обеспечить достаточную защиту против этого типа атак. Когда пакеты доходят до межсетевого экрана, ущерб уже нанесен.

Тем не менее система NetDefendOS может уменьшить нагрузку на внутренние сервера, делая их сервисы доступными изнутри или через альтернативное соединение, которое не стало целью атаки.

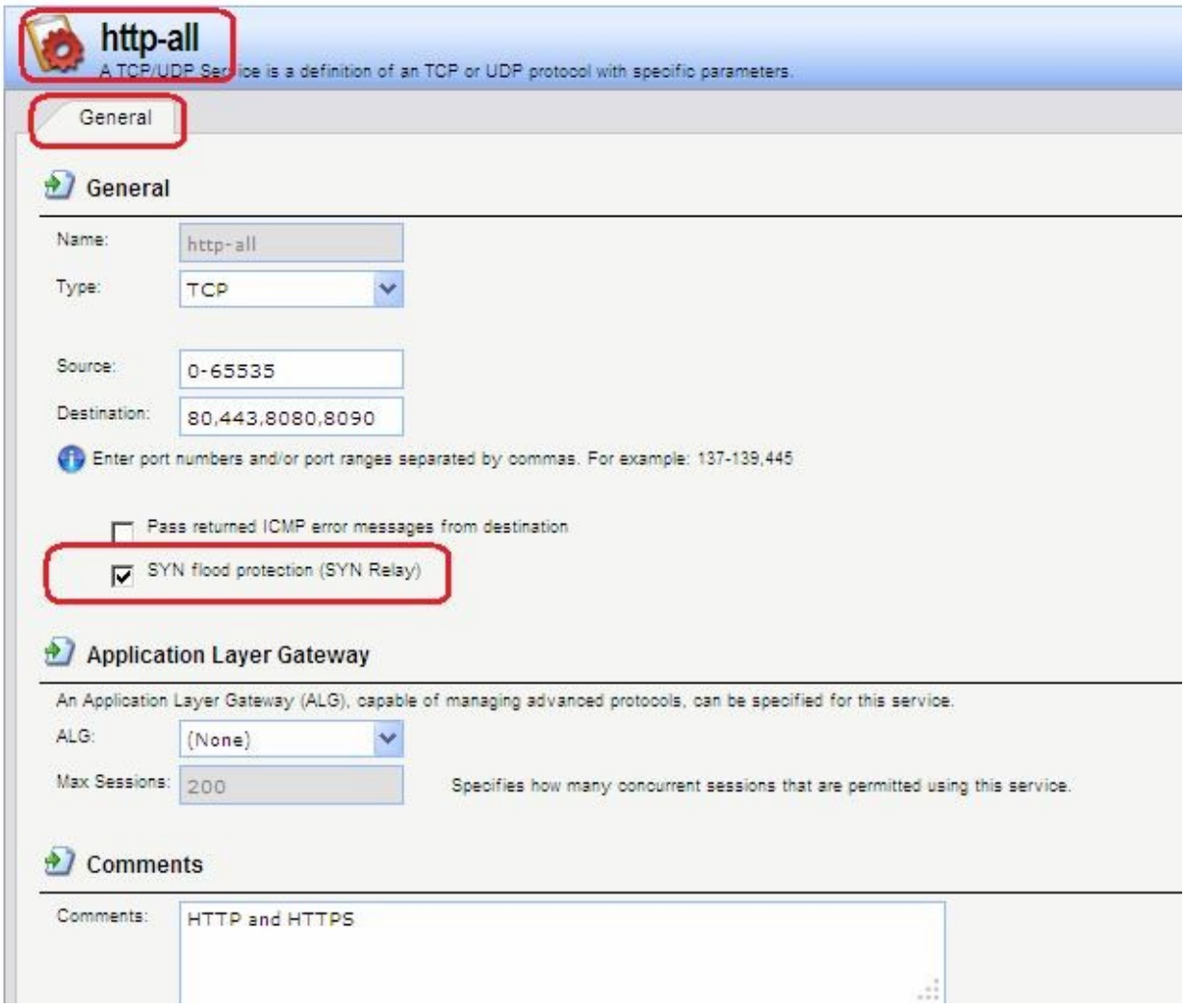
- Типы flood-атак Smurf и Papasmurf на стороне жертвы выглядят как ответы ICMP **`Echo Response`**. Если не используются правила **`FwdFast`**, таким пакетам не будет разрешено инициировать новые соединения независимо от того, существуют ли правила, разрешающие прохождение пакетов.
- Пакеты Fraggle могут прийти на любой UDP-порт назначения, который является мишенью атакующего. В этой ситуации может помочь увеличение ограничений в наборе правил.

Шейпинг трафика также помогает предотвращать некоторые flood-атаки на защищаемые сервера.

Атаки TCP SYN Flood

Принцип атак *TCP SYN Flood* заключается в отправке большого количества TCP-пакетов с установленным флагом **`SYN`** на определенный порт и в игнорировании отправленных в ответ пакетов с установленными флагами **`SYN ACK`**. Это позволяет исчерпать ресурсы стека протоколов на сервере жертвы, в результате чего он не сможет устанавливать новые соединения, пока не истечет таймаут существования полуоткрытых соединений.

Система NetDefendOS обеспечивает защиту от flood-атак TCP SYN, если установлена опция **`SYN Flood Protection`** в соответствующем сервисе, который указан в IP-правиле фильтрования. Иногда опция может обозначаться как **`SYN Relay`**.



Защита от flood-атак включена по умолчанию в таких сервисах, как **`http-in`**, **`https-in`**, **`smtp-in`** и **`ssh-in`**.

Механизм защиты от атак SYN Flood

Защиты от атак SYN Flood выполняется в течение трехкратного рукопожатия, которое происходит при установлении соединения с клиентом. В системе NetDefendOS как правило не происходит исчерпание ресурсов, так как выполняется более оптимальное управление ресурсами и отсутствуют ограничения, имеющие место в других операционных системах. В операционных системах могут возникнуть проблемы уже с 5 полуоткрытыми соединениями, не получившими подтверждение от клиента, NetDefendOS может заполнить всю таблицу состояний, прежде чем будут исчерпаны какие-либо ресурсы. Когда таблица состояний заполнена, старые неподтвержденные соединения отбрасываются, чтобы освободить место для новых соединений.

Обнаружение SYN Floods

Атаки TCP SYN flood регистрируются в логах NetDefendOS как большое количество новых соединений (или отброшенных пакетов, если атака направлена на закрытый порт). Следует помнить, что в этом случае IP-адрес отправителя может быть подделан.

ALG автоматически обеспечивает защиту от flood-атак

Следует отметить, что нет необходимости включать функцию защиты от атак SYN Flood для сервиса, для которого указан ALG. ALG автоматически обеспечивает защиту от атак SYN flood.

Атака Jolt2

Принцип выполнения атаки Jolt2 заключается в отправке непрерывного потока одинаковых фрагментов компьютеру-жертве. Поток из нескольких сотен пакетов в секунду останавливает работу уязвимых компьютеров до полного прекращения потока.

NetDefendOS обеспечивает полную защиту от данной атаки. Первый полученный фрагмент ставится в очередь до тех пор, пока не придут предыдущие по порядку фрагменты, чтобы все фрагменты могли быть переданы в нужном порядке. В случае наличия атаки ни один фрагмент не будет передан целевому приложению. Последующие фрагменты будут отброшены, так как они идентичны первому полученному фрагменту.

Если выбранное злоумышленником значение смещения фрагмента больше, чем ограничения, указанные в настройках **`Advanced Settings → Length Limit Settings`** в NetDefendOS, пакеты будут немедленно отброшены. Атаки Jolt2 могут быть зарегистрированы в логах. Если злоумышленник выбирает слишком большое значение смещения фрагмента для атаки, это будет зарегистрировано в логах как отброшенные пакеты с указанием на правило **`LogOversizedPackets`**. Если значение смещения фрагмента достаточно маленькое, регистрации в логах не будет. IP-адрес отправителя может быть подделан.

Атаки Distributed DoS (DDoS)

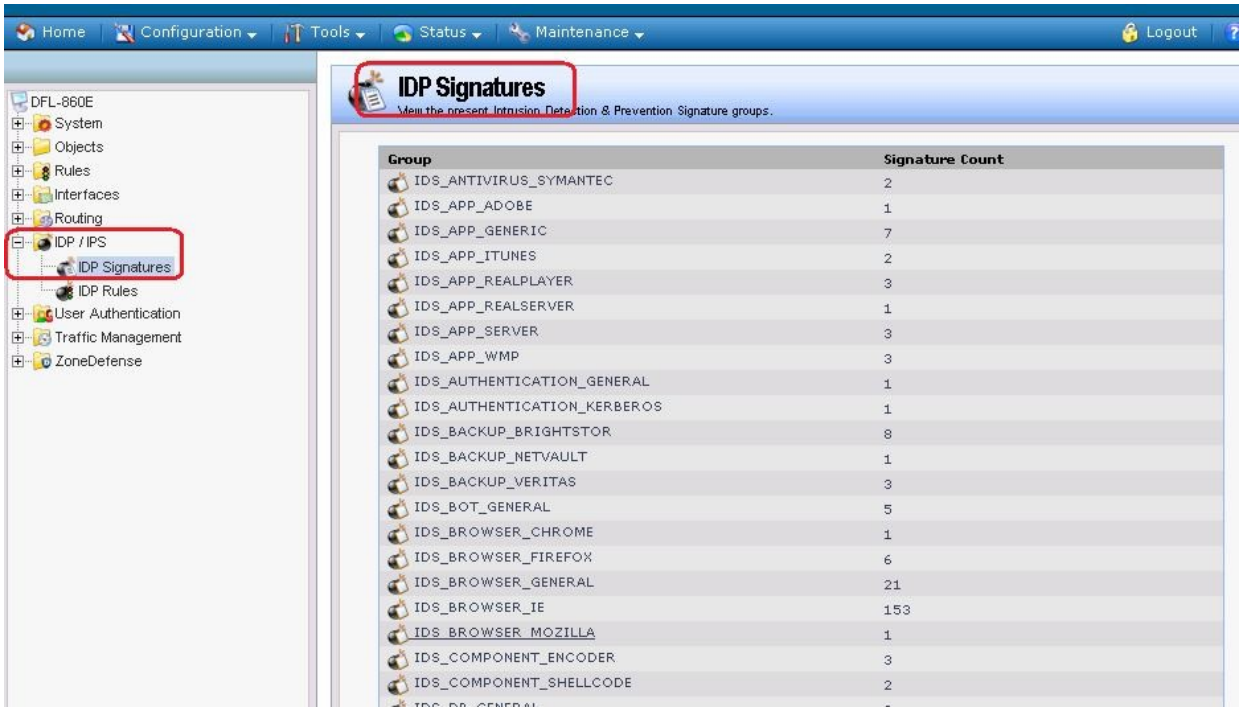
Наиболее сложной DoS-атакой является атака *Distributed Denial of Service*. Хакеры используют сотни или тысячи компьютеров по всей сети интернет, устанавливая на них программное обеспечение для выполнения DDoS-атак и управляя всеми этими компьютерами для осуществления скоординированных атак на сайты жертвы. Как правило эти атаки расходуют полосу пропускания, вычислительные мощности маршрутизатора или ресурсы для обработки стека протоколов, в результате чего сетевые соединения с жертвой не могут быть установлены.

Хотя последние DDoS-атаки были запущены как из частных, так и из публичных сетей, хакеры, как правило, часто предпочитают корпоративные сети из-за их открытого и распределенного характера. Инструменты, используемые для запуска DDoS-атак, включают Trin00, TribeFlood Network (TFN), TFN2K и Stacheldraht.

Описание практической работы

Общий список сигнатур

В веб-интерфейсе все сигнатуры перечислены в разделе **`IDP/IPS →IDP Signatures`**.



IDP-правила

Правило IDP определяет, какой тип трафика необходимо анализировать. Правила IDP создаются аналогично другим правилам, например, IP-правилам фильтрования. В правиле IDP указывается комбинация адреса/интерфейса источника/назначения, сервиса, определяющего какие протоколы будут сканироваться. Главное отличие от правил фильтрования в том, что правило IDP определяет **Действие**, которое следует предпринять при обнаружении вторжения.

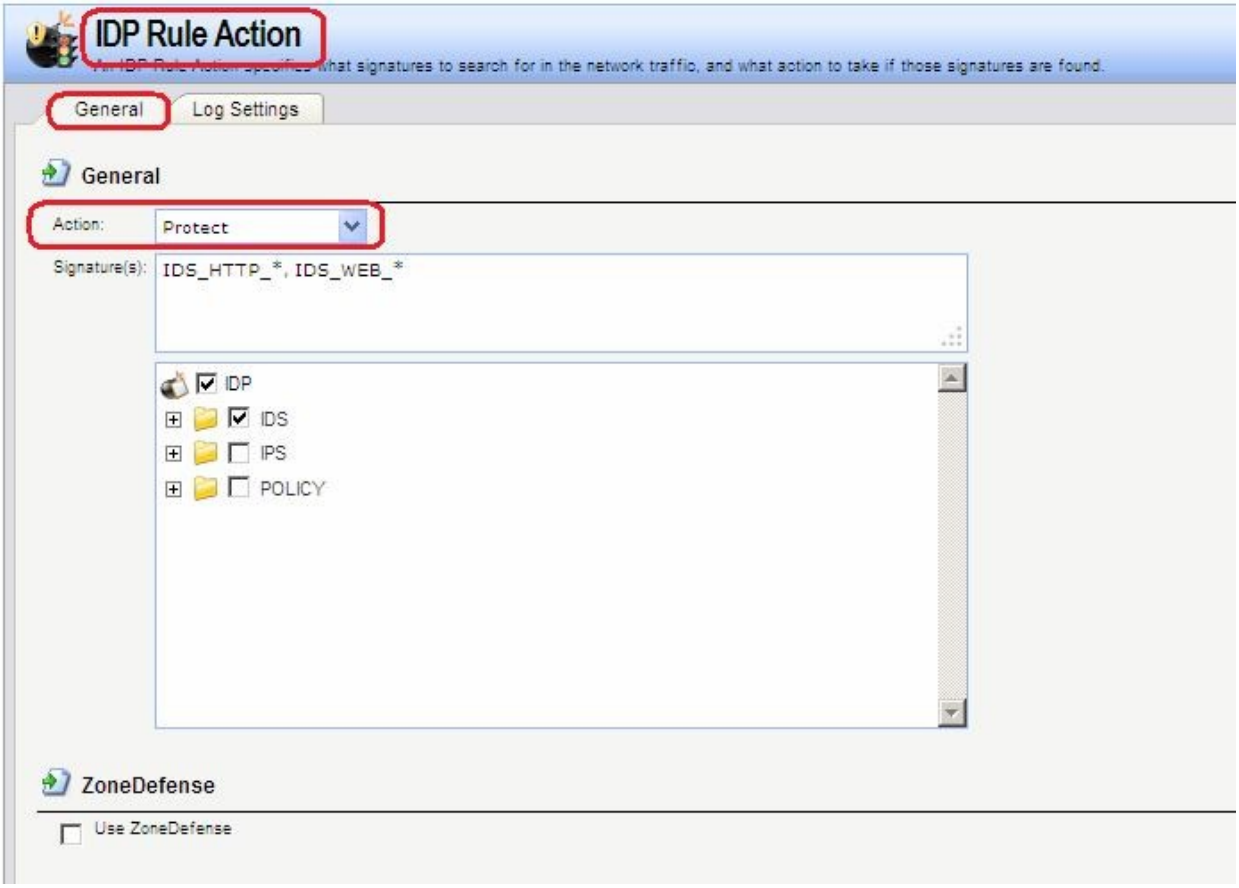
Веб-интерфейс:

`IDP / IPS → IDP Rules →Add → IDP Rule`

Действия IDP

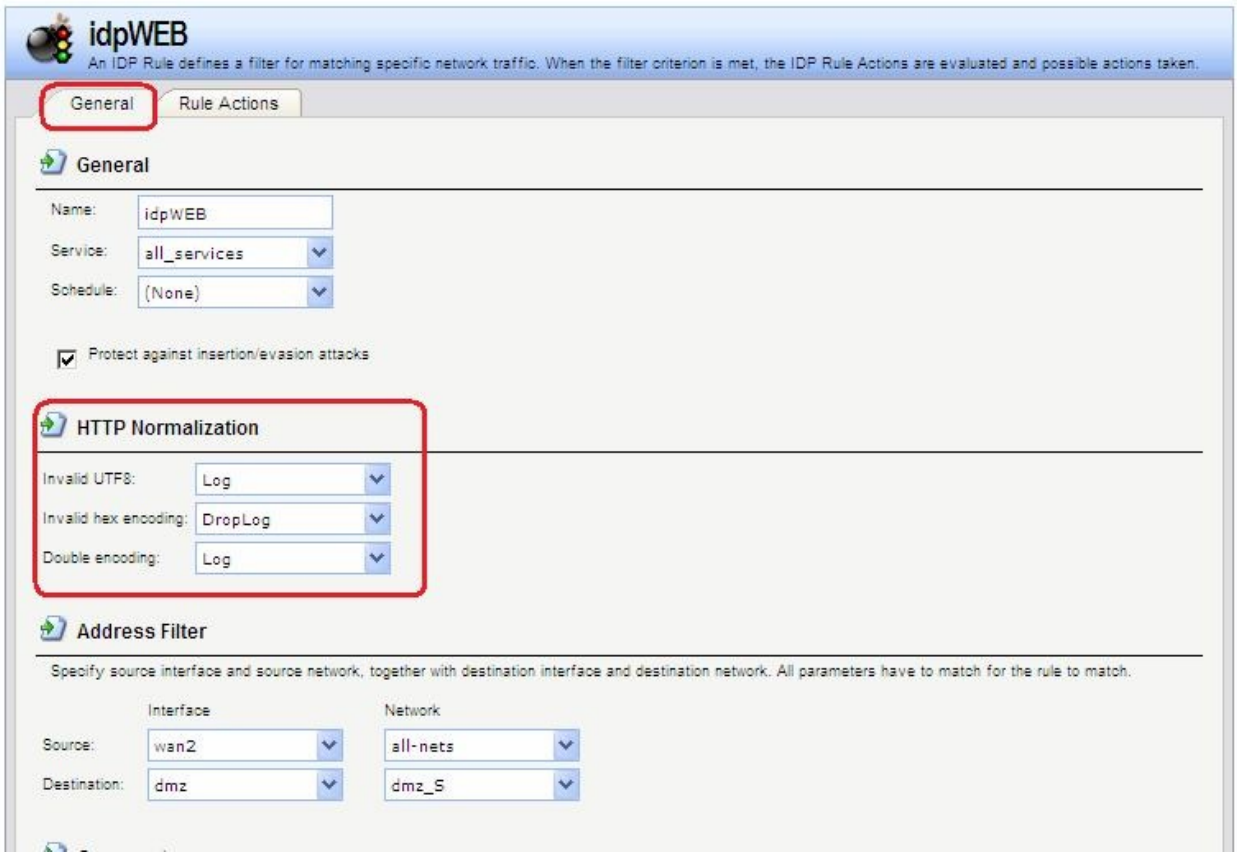
При выявлении вторжения будет выполнено действие, указанное в правиле IDP. Может быть указано одно из трех действий:

1. **`Ignore`** – Если обнаружено вторжение, не выполнять никаких действий и оставить соединение открытым.
2. **`Audit`** – Оставить соединение открытым, но зарегистрировать событие.
3. **`Protect`** – Сбросить соединение и зарегистрировать событие. Возможно использовать дополнительную опцию занесения в «черный список» источник соединения.



Нормализация HTTP

IDP выполняет *нормализацию HTTP*, т.е. проверяет корректность URI в HTTP-запросах. В IDP-правиле можно указать действие, которое должно быть выполнено при обнаружении некорректного URI.



IDP может определить следующие некорректные URI:

Некорректная кодировка UTF8

Выполняется поиск любых недействительных символов UTF8 в URI.

Некорректный шестнадцатеричный код

Корректной является шестнадцатеричная последовательность, где присутствует знак процента, за которым следуют два шестнадцатеричных значения, являющихся кодом одного байта. Некорректная шестнадцатеричная последовательность – это последовательность, в которой присутствует знак процента, за которым не следуют шестнадцатеричные значения, являющиеся кодом какого-либо байта.

Двойное кодирование

Выполняется поиск любой шестнадцатеричной последовательности, которая сама является закодированной с использованием других управляющих шестнадцатеричных последовательностей. Примером может быть последовательность **%2526**, при этом **%25** может быть интерпретировано HTTP-сервером как **%**, в результате получится последовательность **%26**, которая будет интерпретирована как **&**.

Предотвращение атак, связанных со вставкой символов или обходом механизмов IDP
В IDP-правиле можно установить опцию **Protect against Insertion/Evasion attack**. Это защита от атак, направленных на обход механизмов IDP. Данные атаки используются тот факт, что в протоколах TCP/IP пакет может быть фрагментирован, и отдельные пакеты могут приходить в произвольном порядке. Атаки, связанные со вставкой символов и обходом механизмов IDP, как правило используют фрагментацию пакетов и проявляются в процессе сборки пакетов.

Атаки вставки

Атаки вставки состоят в такой модификации потока данных, чтобы система IDP пропускала полученную в результате последовательность пакетов, но данная последовательность будет являться атакой для целевого приложения. Данная атака может быть реализована созданием двух различных потоков данных.

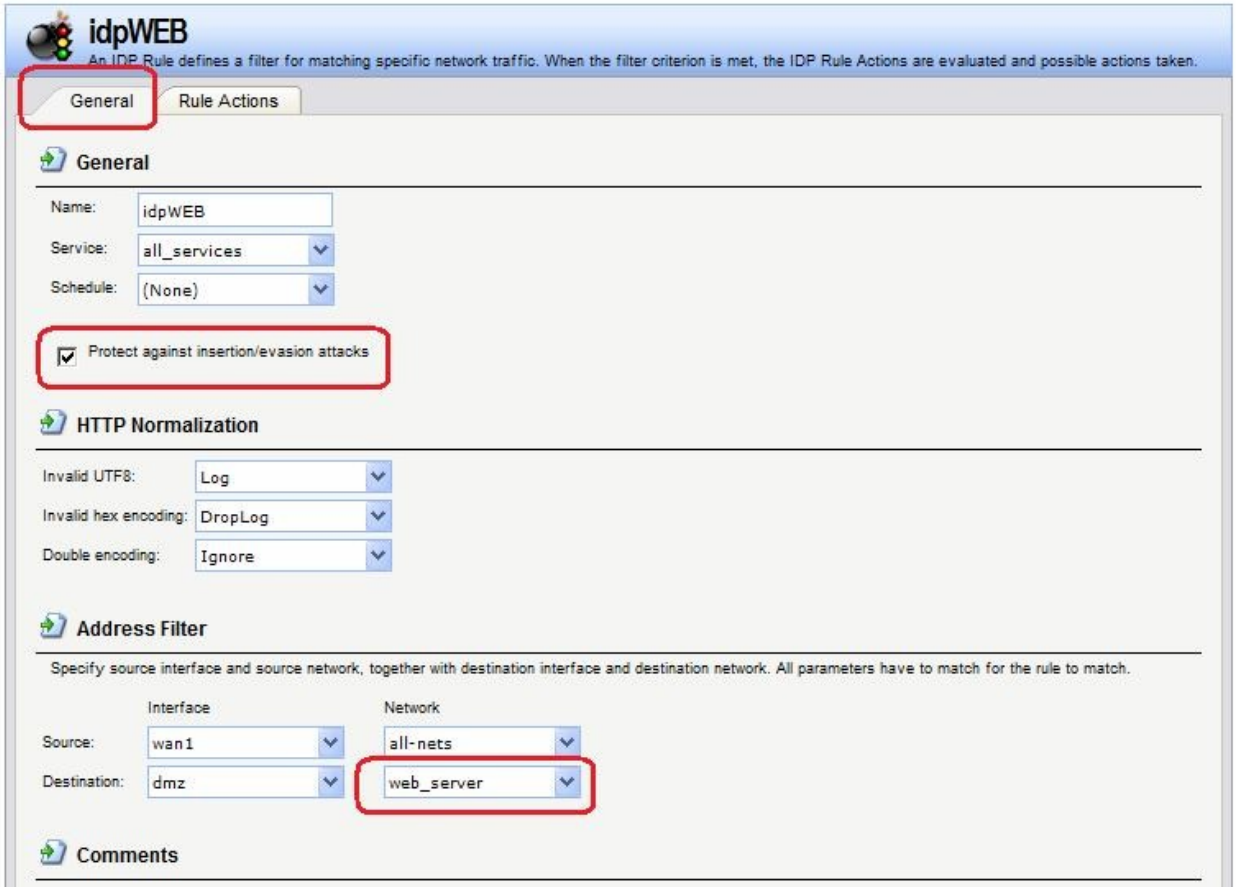
В качестве примера предположим, что поток данных состоит из 4 фрагментов пакетов: **p1**, **p2**, **p3** и **p4**. Злоумышленник может сначала отправить фрагменты пакетов **p1** и **p4** целевому приложению. Они будут удерживаться и системой IDP, и приложением до прихода фрагментов **p2** и **p3**, после чего будет выполнена сборка. Задача злоумышленника состоит в том, чтобы отправить два фрагмента **p2'** и **p3'** системе IDP и два других фрагмента **p2** и **p3** приложению. В результате получаются различные потоки данных, который получены системой IDP и приложением.

Атаки обхода

У атак обхода такой же конечный результат, что и у атак вставки, также образуются два различных потока данных: один видит система IDP, другой видит целевое приложение, но в данном случае результат достигается противоположным способом, который заключается в отправке фрагментов пакетов, которые будут отклонены системой IDP, но приняты целевым приложением.

Обнаружение подобных атак

Если включена опция **Insertion/Evasion Protect attacts**, и атака вставки или обхода обнаружена, межсетевой экран автоматически корректирует поток данных, удаляя данные, связанные с атакой.



Запись в лог событий, связанных с атаками вставки и обхода

Подсистема, предотвращающая атаки вставки и обхода, может создавать два типа сообщений в логах:

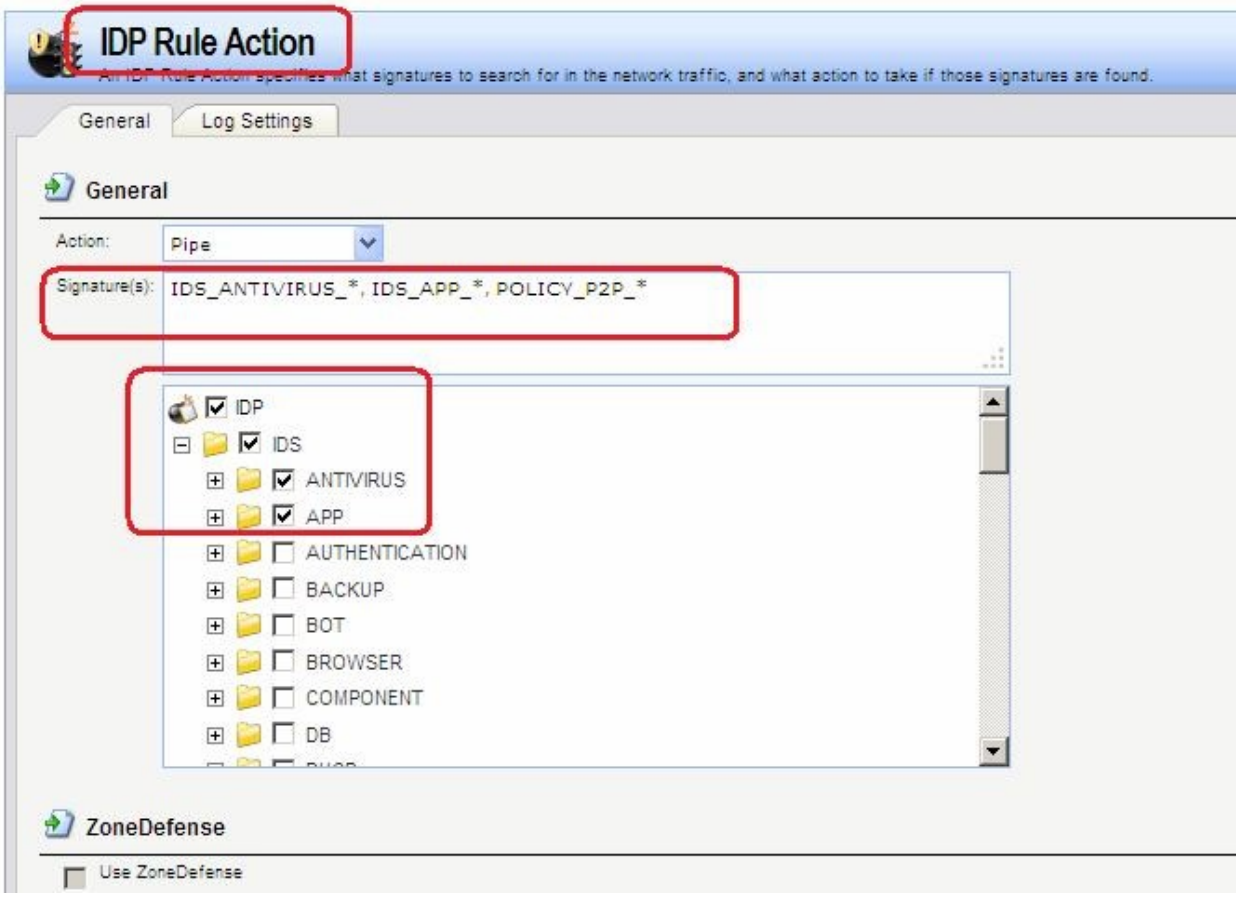
- Сообщение **`Attack Detected`**, указывающее на то, что атака была обнаружена и предотвращена.
- Сообщение **`Unable to Detect`,** уведомляющее о том, что система NetDefendOS не смогла выявить возможную атаку при сборке потока TCP/IP, хотя подобная атака могла присутствовать. Эта ситуация возможна при редких и сложных шаблонах данных.

Рекомендуемые настройки

По умолчанию, защита от атак вставки и обхода включена для всех IDP-правил, и это рекомендуемая настройка для большинства конфигураций. Существует две причины для отключения опции:

- **Требуется увеличение пропускной способности.** Если необходима высокая пропускная способность, следует выключить функцию, так как это обеспечит небольшое увеличение скорости обработки.
- **Чрезмерное количество ложных срабатываний.** Если наблюдается большое количество ложных срабатываний при обнаружении атак вставки и обхода, то целесообразно выключить данную опцию до выяснения причин этих ложных срабатываний.

Группы сигнатур IDP



Как правило, для каждого протокола существует несколько типов атак, и наилучшим подходом во время анализа сетевого трафика является обнаружение всех атак. Для простоты указания всех типов атак сигнатуры, описывающие атаки на определенный протокол, сгруппированы вместе. Например, образуют группу все сигнатуры, которые относятся к FTP-протоколу. При создании правил удобнее указывать группу, которая относится к определенному протоколу, чем перечислять отдельные сигнатуры. При

необходимости повышения производительности поиск следует выполнять для минимального количества сигнатур.

Группы сигнатур IDP имеют три уровня иерархии. На верхнем уровне указывается тип группы сигнатур, на втором указывается тип приложения или протокола и на третьем указывается отдельное приложение или протокол. Примером является **IDS_AUTHENTICATION_KERBEROS**, где **IDS** означает тип сигнатуры, **AUTHENTICATION** – тип протокола и **KERBEROS** – конкретный протокол. Определены следующие типы групп сигнатур и приложений:

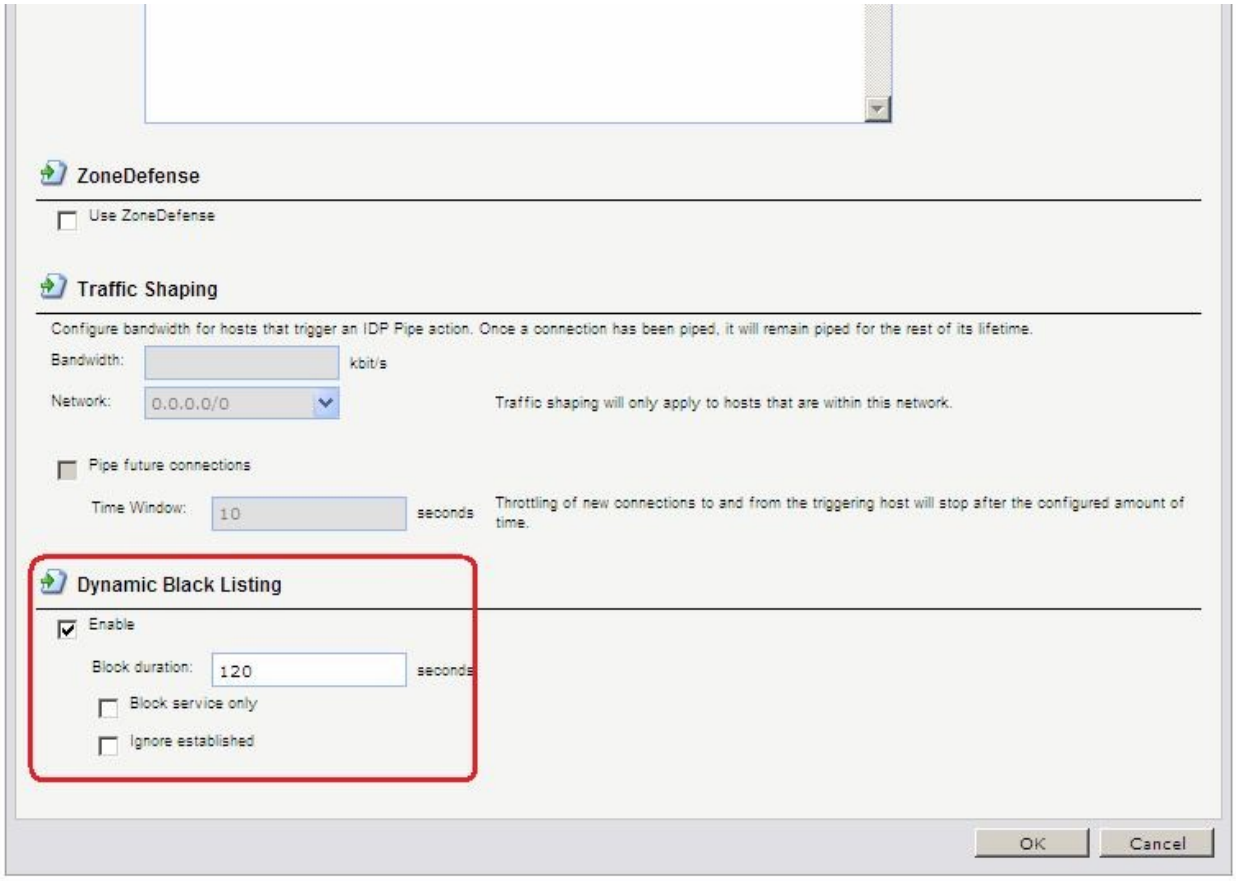
Использование подстановки символов (Wildcarding) в сигнатурах IDP

Для выбора более одной группы сигнатур IDP можно использовать метод подстановки (Wildcarding). Символ «?» используется для подстановки единственного знака в имени группы. Символ «*» используется для замены любого количества символов.

Для увеличения производительности следует использовать минимальное количество сигнатур. Например, использование **IDS_WEB***, **IPS_WEB***, **IDS_HTTP*** и **IPS_HTTP*** будет достаточным для защиты HTTP-сервера.

«Черный список» хостов и сетей

Если указано действие **Protect,** можно добавлять в «черный список» отдельные хосты или сети, на которых сработало данное правило. В этом случае весь последующий трафик, идущий с источника, который находится в «черном списке», будет автоматически отклонен.



Можно включить функцию автоматического занесения в «черный список» хоста или сети в IDP и в правилах порога, указав действие **Protect** в правиле. Существуют три параметра «черного списка»:

Time to Block Хост или сеть, которые являются источником трафика,

Host/Network in Seconds	остаются в «черном списке» в течение указанного времени, а затем удаляются. Если тот же источник содержится в другой записи в «черном списке», то в таком случае будет восстановлено первоначальное время блокировки, т.е. суммирования не происходит.
Block only this Service	По умолчанию «черный список» блокирует все сервисы с данного хоста.
Exempt already established connections from Blacklisting	Если существуют установленные соединения с тем же источником, что и новая запись в «черном списке», то они не будут удалены, если установлена данная опция.

IP-адреса или сети добавляются в список, после этого трафик с этих источников блокируется на указанный период времени. При перезапуске межсетевого экрана «черный список» не уничтожается.

Для просмотра, а также для управления содержимым «черного» и «белого списков» используется команда **blacklist**.

Командная строка:

```
add IDPRule Service=http-all SourceInterface=wan2 SourceNetwork=all-nets
DestinationInterface=dmz DestinationNetwork=dmz/dmz_net Name=idpWEB
```

Получение по e-mail сообщений о событиях IDP

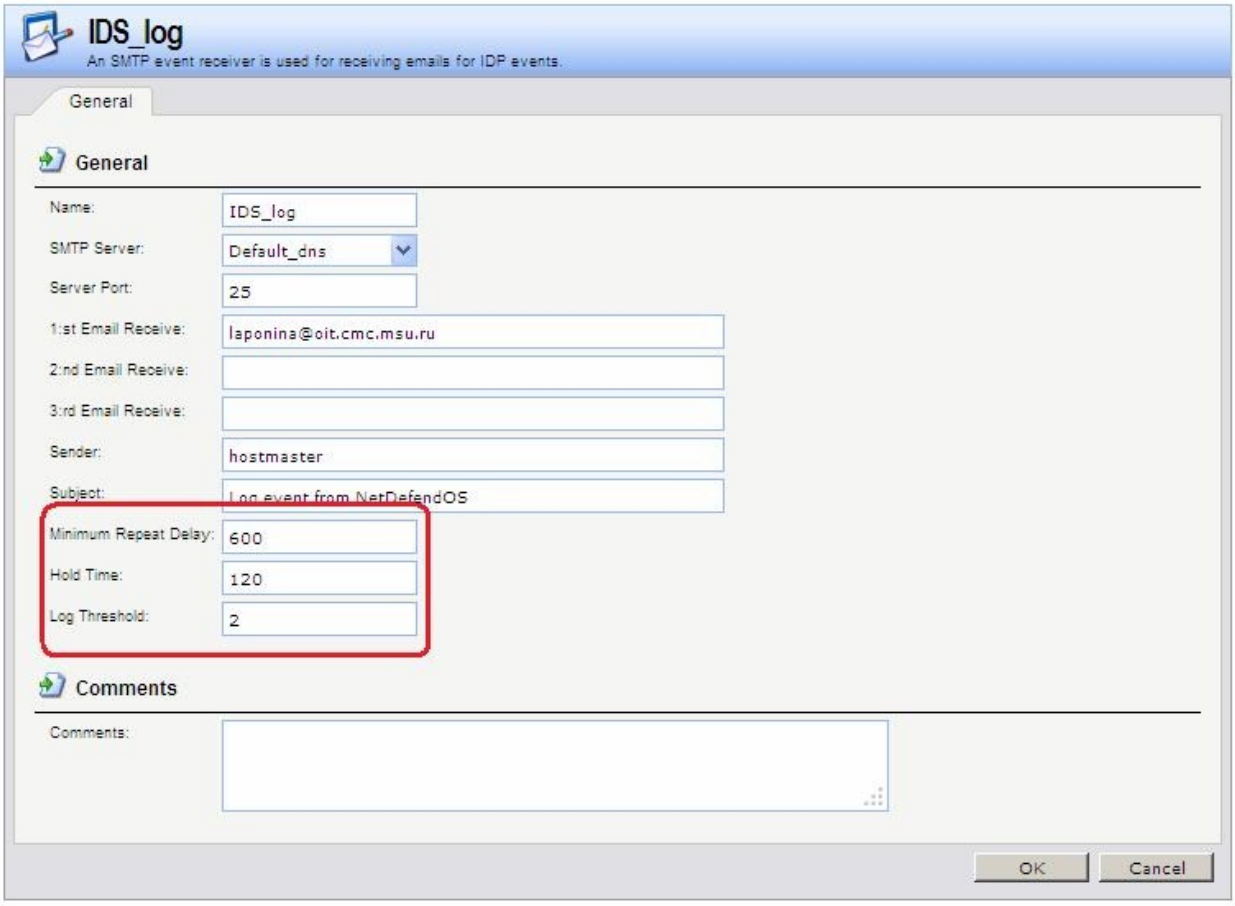
Для того чтобы получать уведомления по электронной почте о событиях IDP, необходимо настроить **SMTP Log receiver**. Получаемое сообщение электронной почты будет содержать краткое описание событий IDP, которые произошли за установленный период времени.

После того, как произошло событие IDP, NetDefendOS ожидает несколько секунд (определяется параметром **Hold Time)** прежде, чем отправить уведомление по электронной почте. При этом сообщение будет отправлено только в том случае, если число событий, произошедших в этот период времени, больше или равно, чем значение **Log Threshold**. После отправки уведомления NetDefendOS ожидает несколько секунд (**Minimum Repeat Time)** прежде, чем отправить новое сообщение.

Для указания получения логов по протоколу SMTP, необходимо указать IP-адрес SMTP-сервера, доменное имя в данном случае использоваться не может.

Веб-интерфейс:

System → Log and Event Receivers → Add → SMTP Event Receiver



Командная строка:

```
add LogReceiver LogReceiverSMTP IDS_log1
IPAddress=InterfaceAddresses/Default_dns Receiver1=admin@oit.cmc.msu.ru
```

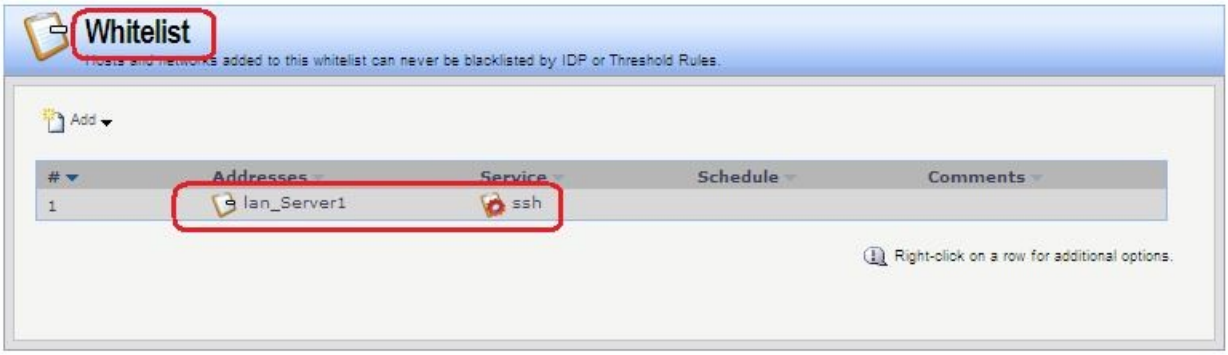
«Белый список» хостов и сетей

Для того чтобы трафик, поступающий из надежных источников, таких как рабочие станции управления, не попал в «черный список» ни при каких обстоятельствах, система NetDefendOS также поддерживает «*белый список*». Любой IP-адрес объекта может быть добавлен в этот «белый список».

Важно помнить, что хотя использование «белого списка» предотвращает занесение в «черный список» определенных IP-адресов источников, это не мешает механизмам NetDefendOS отбрасывать соединения с этого источника. «Белый список» предотвращает только добавление источника в «черный список», если это может произойти в результате срабатывания правила.

Веб-интерфейс:

System → Whitelist → Add → Whitelist Host



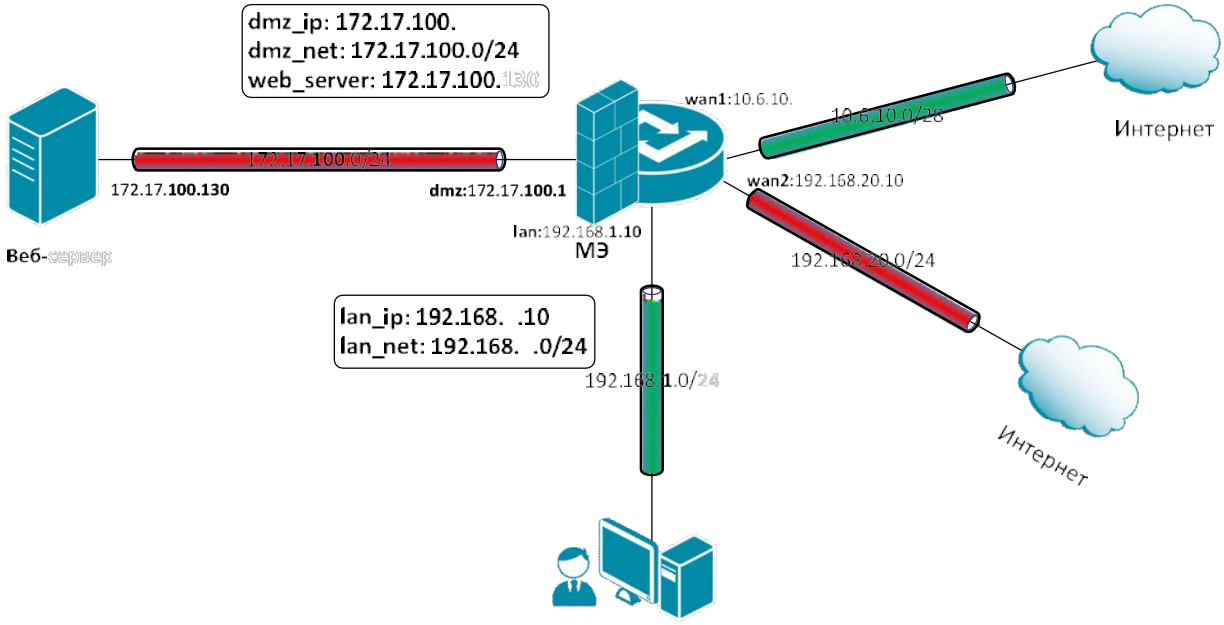
Командная строка:

```
add BlacklistWhiteHost Addresses=lan/lan_Server1 Service=ssh
```

Практическая работа №43
Создание альтернативных маршрутов с использованием статической маршрутизации

Цель
Использовать два выхода в интернет: один канал использовать для доступа в интернет из локальной сети, в другой для доступа из DMZ-сети.

Топология сети

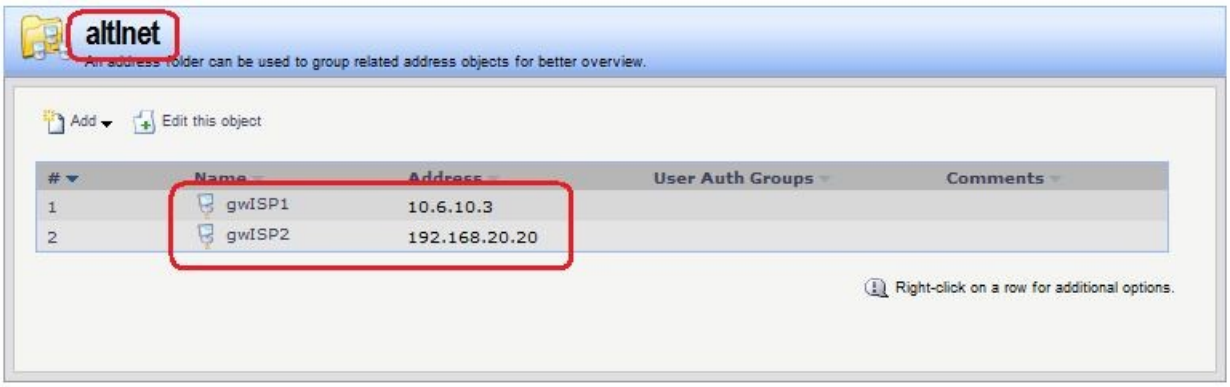


Следует использовать статическую маршрутизацию на основе правил (Policy-Based Routing - PBR) для создания сети с двумя выходами в интернет.

Описание практической работы
Создать статическую маршрутизацию и политики доступа, которые обеспечивают доступ в интернет компьютеров из локальной сети LAN через канал, подключенный к **`wan1`**-интерфейсу маршрутизатора и доступ в интернет из DMZ-сети через канал, подключенный к **`wan2`**-интерфейсу маршрутизатора. Для этого следует использовать статическую маршрутизацию на основе правил.

Маршрутизация на основе адреса источника

Объекты Адресной Книги
В Адресной Книге создать объекты, описывающие альтернативные шлюзы интернет-провайдеров.



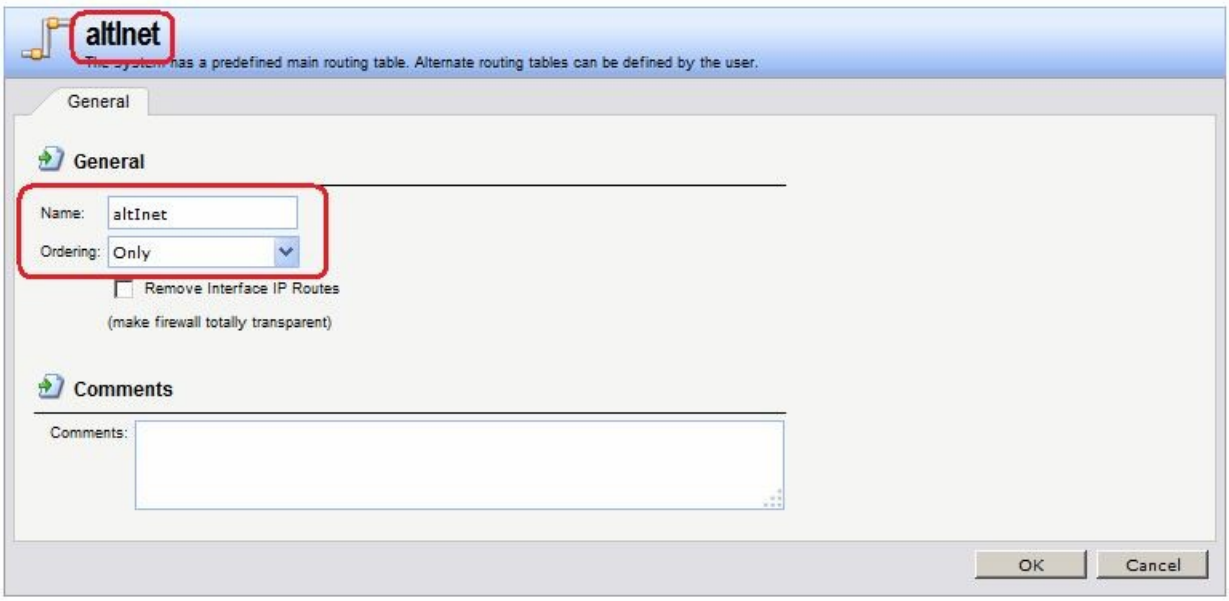
Альтернативная таблица маршрутизации
Создать альтернативную таблицу маршрутизации.

Веб-интерфейс:

`Routing → Routing Tables → Add → Routing Table`

`Name: altInet`

`Ordering: Only`



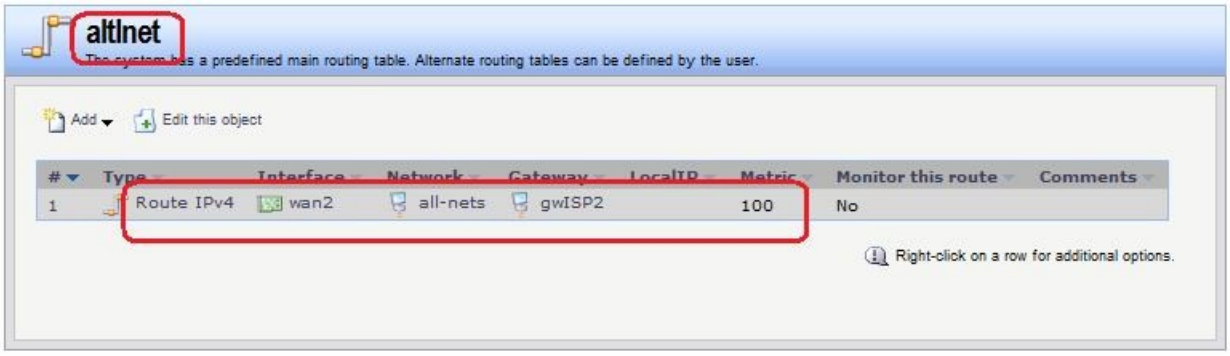
Командная строка:

`add RoutingTable altInet Ordering=Only`

В созданной таблице создать маршрут по умолчанию к ISP2 через интерфейс **`wan2`**.

Веб-интерфейс:

`Routing → Routing Tables → altInet → Add`



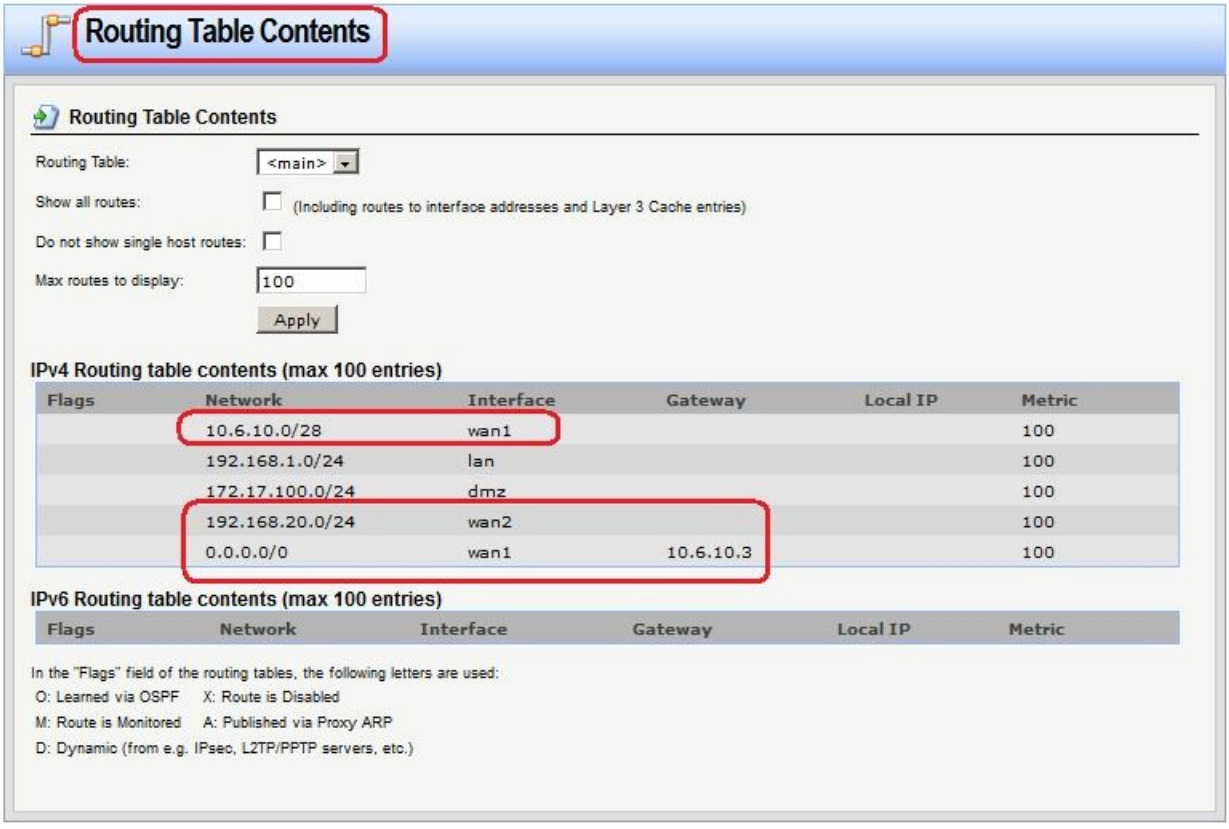
Командная строка:

```
cc RoutingTable altInet
add Route Interface=wan2 Network=all-nets Gateway=altInet/gwISP2 Metric=100
```

В таблице маршрутизации **`main`** проверить наличие маршрутов по умолчанию к ISP2 через интерфейс **`wan2`**, а также остальных необходимых маршрутов.

Веб-интерфейс:

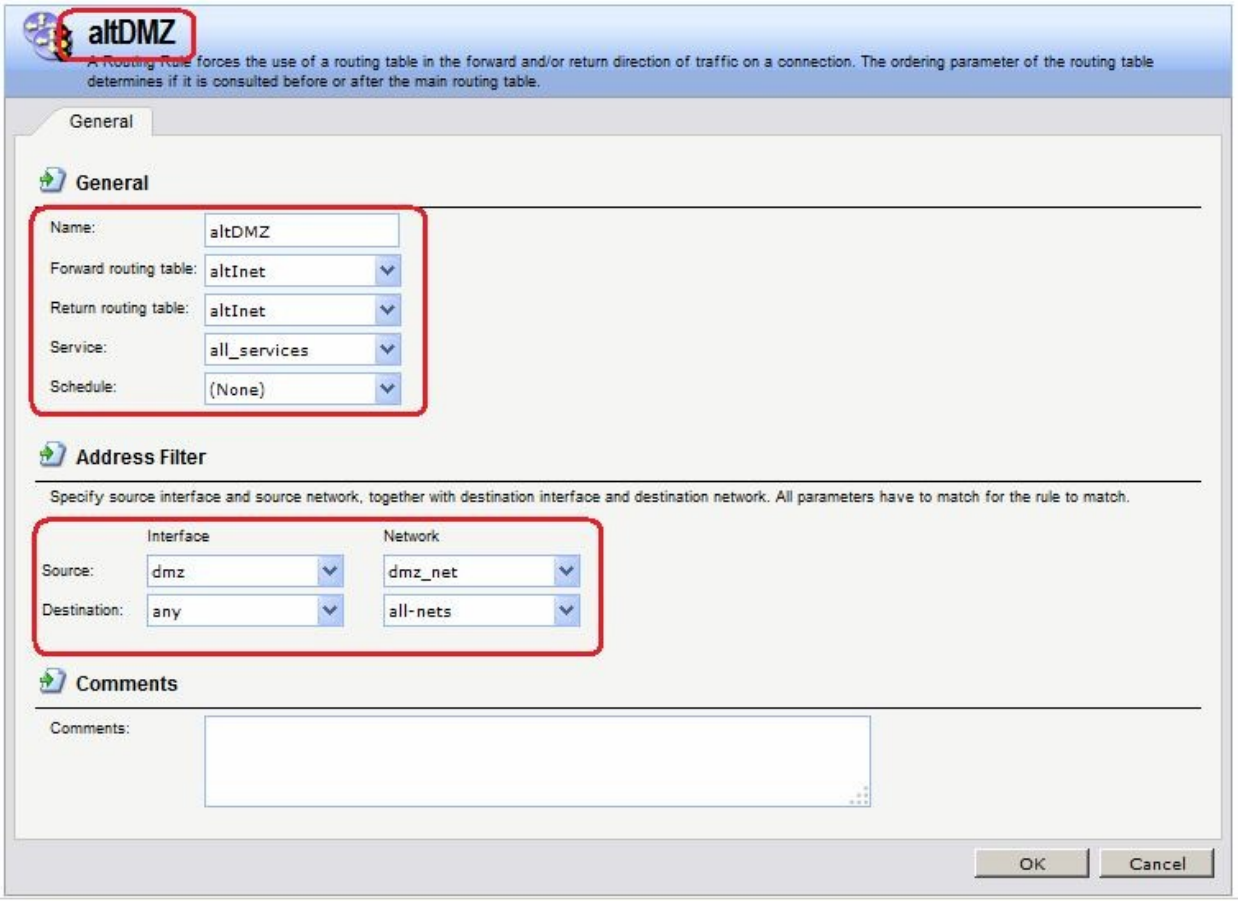
`Routing → Routing Tables → main → Add`



Правило выбора таблицы маршрутизации PBR

Веб-интерфейс:

`Routing → Routing Rules → Add → Routing Rule`



Командная строка:

```
add RoutingRule ForwardRoutingTable=altDMZ ReturnRoutingTable=altDMZ
SourceInterface=dmz SourceNetwork= dmz/dmz_net DestinationInterface=any
DestinationNetwork=all-nets Service=all_services Name=altDMZ
```

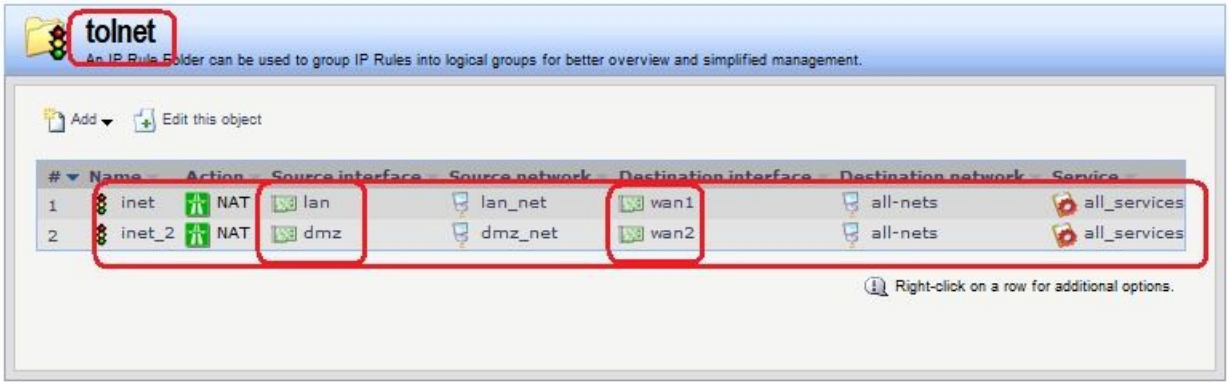
Правила фильтрования

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: toInet

Rules → IP Rules → toInet → Add → IP Rule



Командная строка:

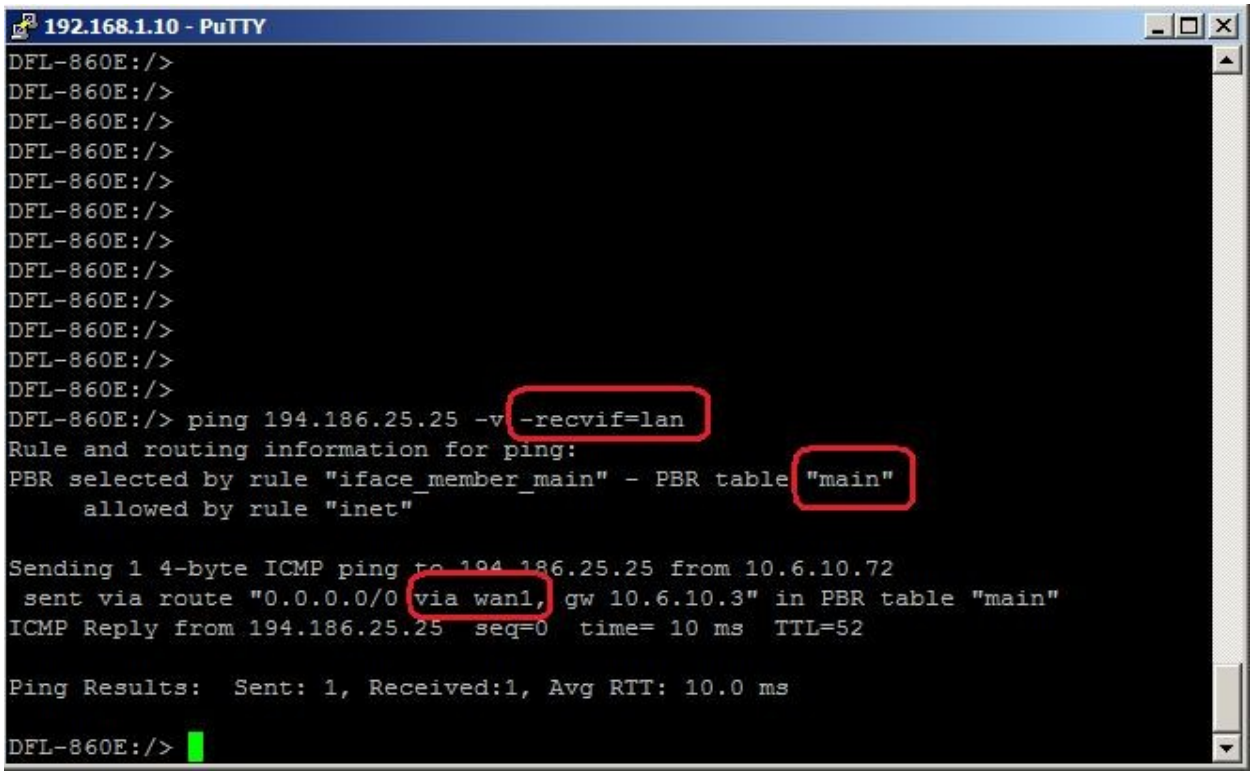
```
add IPRuleFolder Name=toInet
```

```
cc IPRuleFolder <N folder>
```

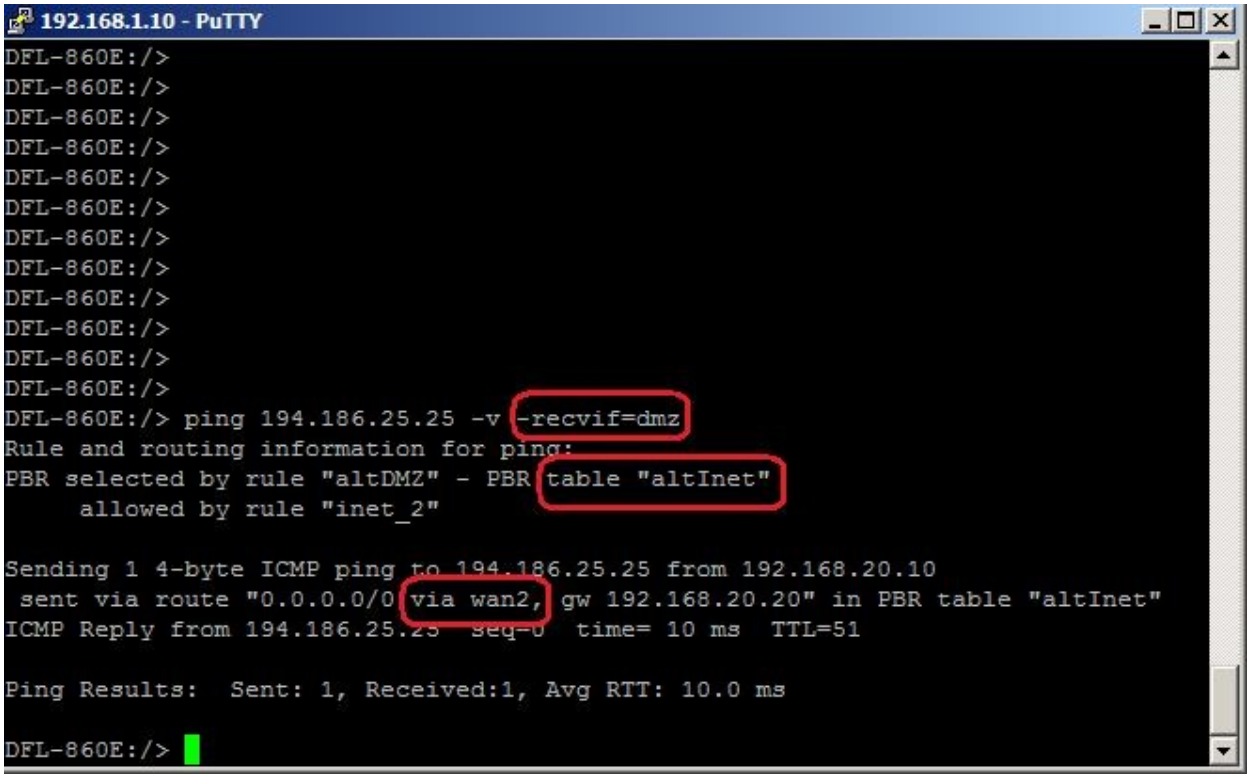
```
add IPRule Action=NAT SourceInterface=lan SourceNetwork= lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
Name=inet

add IPRule Action=NAT SourceInterface=dmz SourceNetwork=dmz/dmz_net
DestinationInterface=wan2 DestinationNetwork=all-nets Service=all_services
Name=inet_2
```

Проверка конфигурации

1. Выполняем выход в интернет с интерфейса **lan** и проверяем, что соединение установлено через интерфейс **wan1**.



2. Выполняем выход в интернет с интерфейса **dmz** и проверяем, что соединение установлено через интерфейс **wan1**.

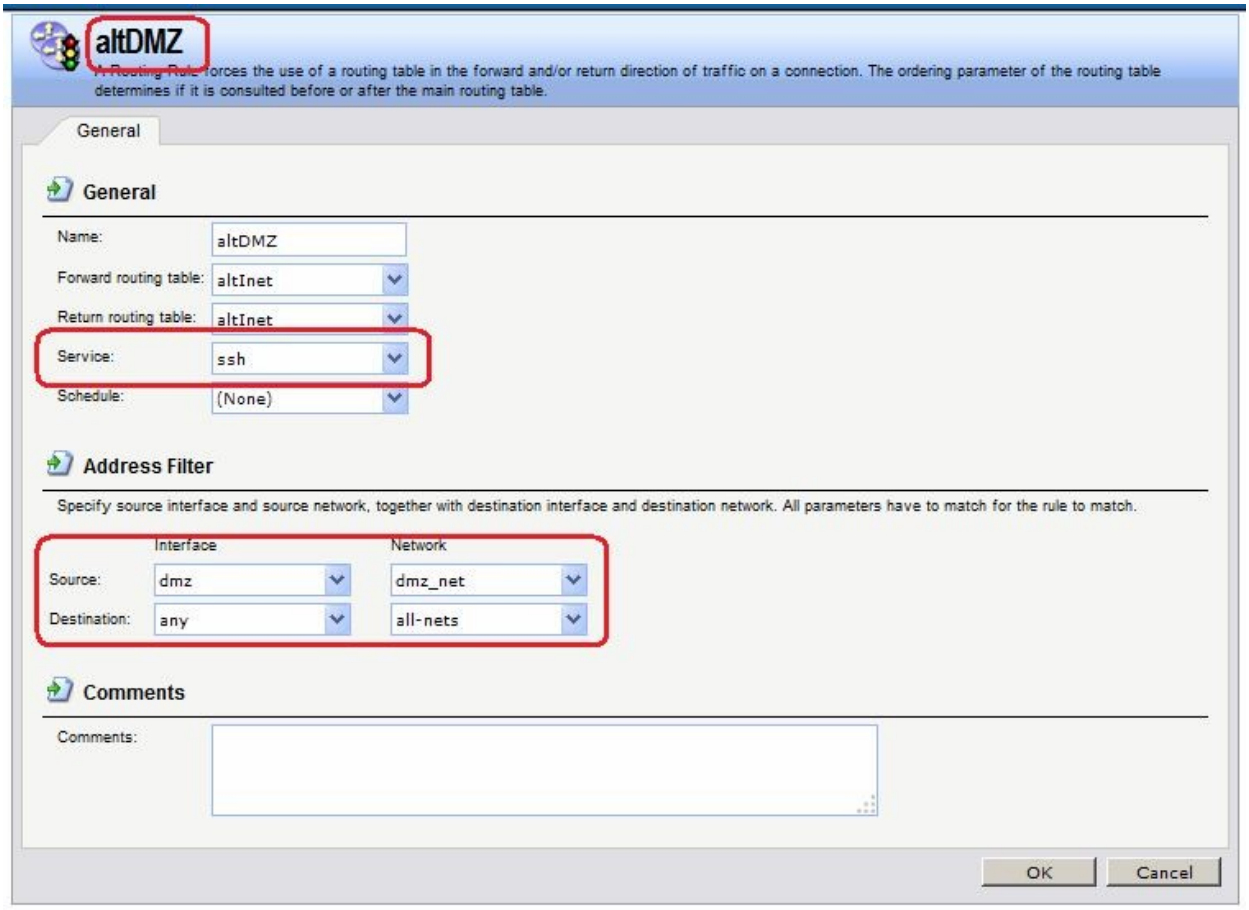


Маршрутизация на основе сервиса

Альтернативная таблица маршрутизации
Альтернативная таблица маршрутизации создается аналогично маршрутизации на основе адреса источника.

Правило выбора таблицы маршрутизации PBR
Веб-интерфейс:

`Routing → Routing Rules → Add → Routing Rule`



Командная строка:

```
add RoutingRule ForwardRoutingTable=altInet ReturnRoutingTable=altInet SourceInterface=dmz SourceNetwork=dmz/dmz_net DestinationInterface=any DestinationNetwork=all-nets Service=ssh Name=altDMZ
```

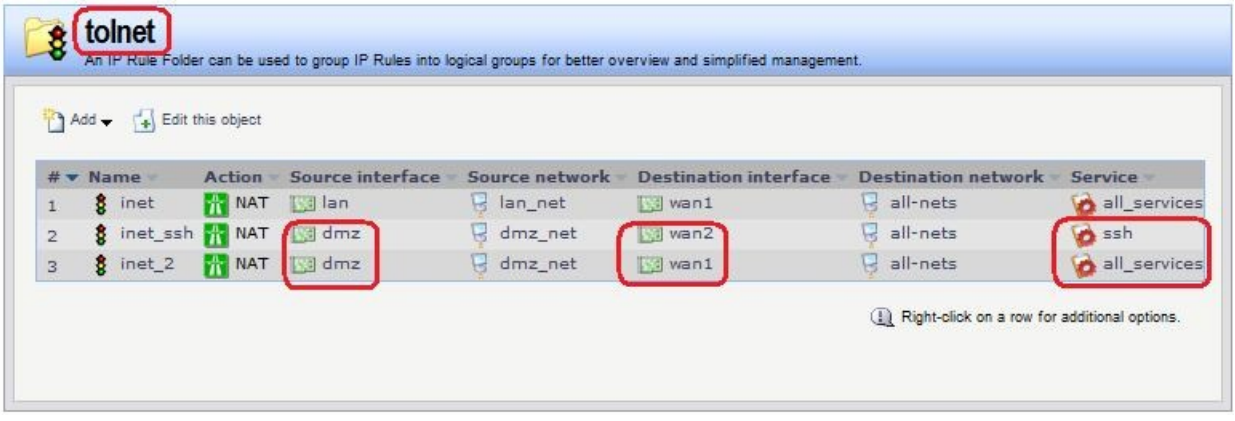
Правила фильтрования

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: toInet

Rules → IP Rules → toInet → Add → IP Rule



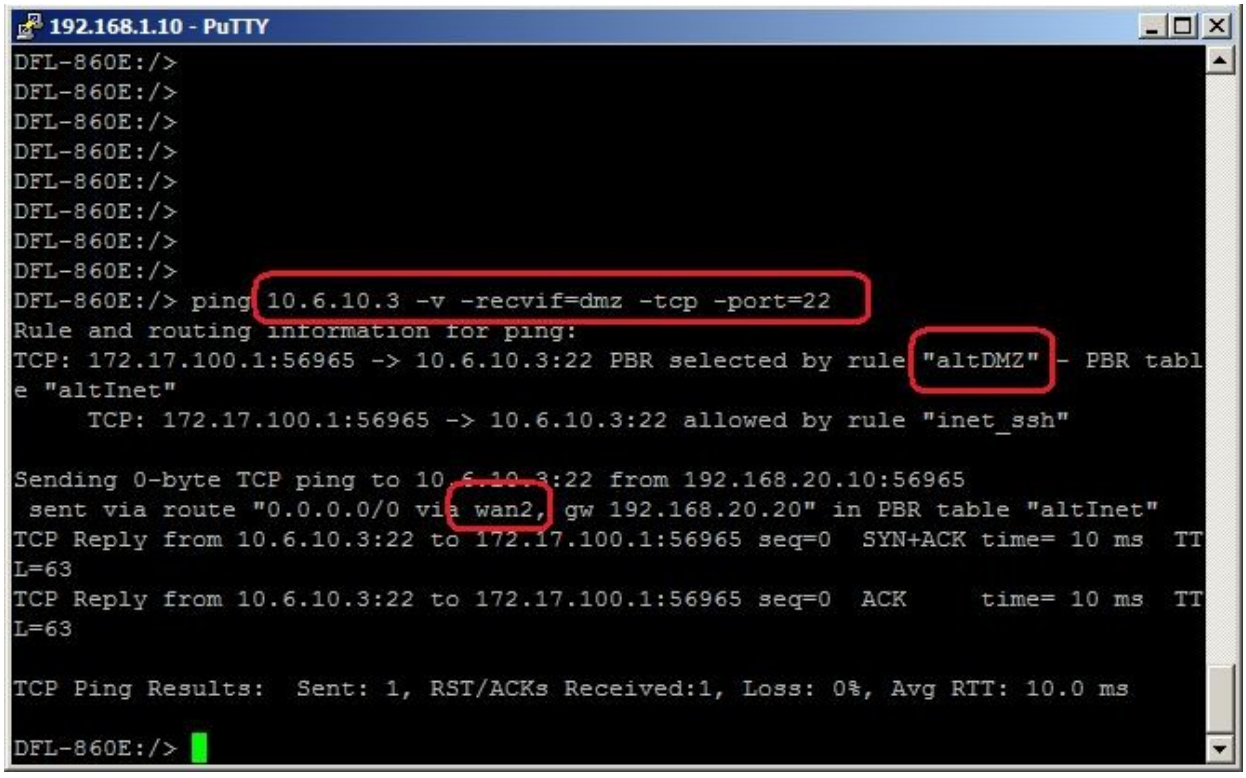
Командная строка:

```
add IPRuleFolder Name=toInet
```

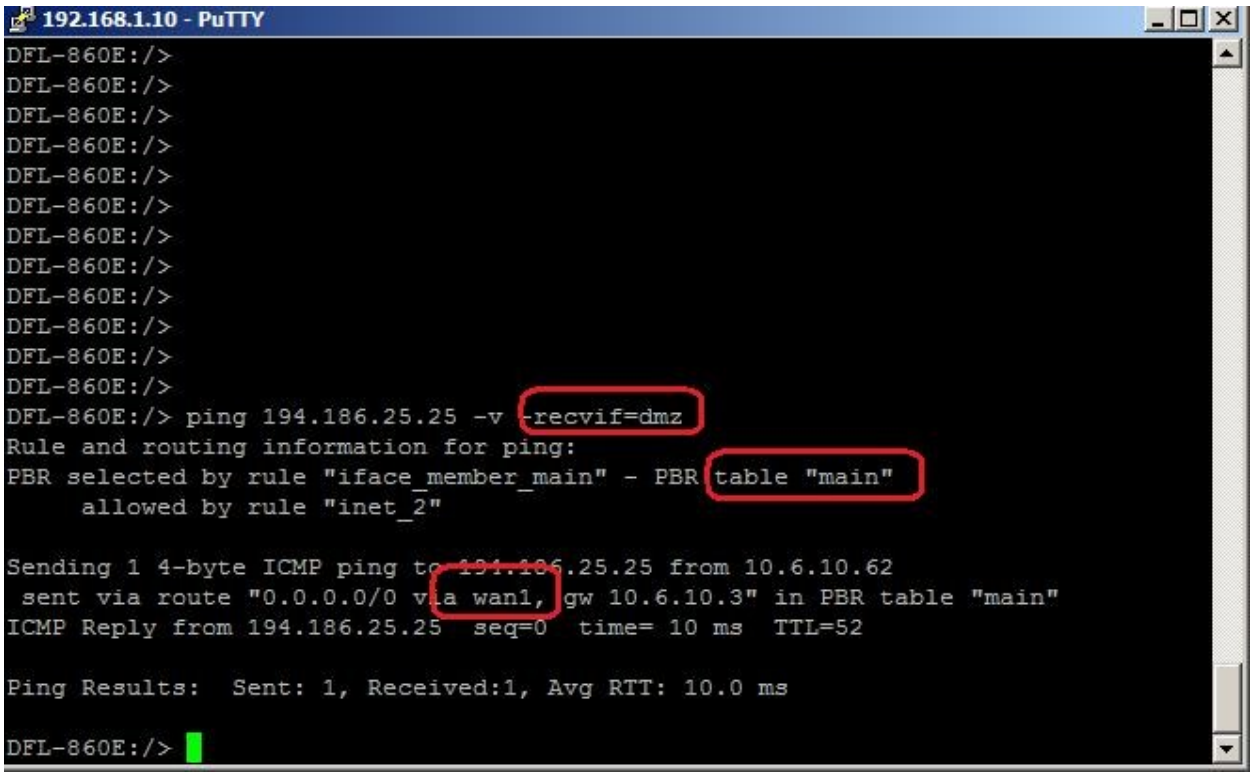
```
cc IPRuleFolder <N folder>

add IPRule Action=NAT SourceInterface=lan SourceNetwork= lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
Name=inet

add IPRule Action=NAT SourceInterface=dmz SourceNetwork= dmz/dmz_net
DestinationInterface=wan2 DestinationNetwork=all-nets Service=ssh
Name=inet_ssh

add IPRule Action=NAT SourceInterface=dmz SourceNetwork= dmz/dmz_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
Name=inet_2
```

Проверка конфигурации

Лабораторная работа 10. Выполняем выход в интернет по протоколу ssh с dmz-интерфейса.



Лабораторная работа 11. Выполняем выход в интернет по протоколу ICMP с dmz-интерфейса.



Критерии оценки

Процент результативности (правильных ответов)	**Качественная оценка индивидуальных образовательных достижений**	
	балл (отметка)	**вербальный аналог**
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	не удовлетворительно

Составитель: Е.А.Романцова