МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Комплект контрольно-оценочных средств

междисциплинарного курса

МДК 01.05 Эксплуатация компьютерных сетей

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка - 2024

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1553, с учетом профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 536н, и с учетом профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 533н, и с учетом профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 525н.

Составитель:
Финошкин Д.Б., преподаватель ОГАПОУ «Алексеевский колледж»

1. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу МДК 01.05 Эксплуатация компьютерных сетей

КОС включают контрольные материалы для проведения промежуточной аттестации в форме дифференцированного зачета.

КОС разработан на основании рабочей программы МДК 01.05 Эксплуатация компьютерных сетей

1.2 Цели и задачи МДК – требования к результатам освоения МДК

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

иметь практический опыт:

О1 установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

О2 администрирование автоматизированных систем в защищенном исполнении

О3 эксплуатация компонентов систем защиты информации автоматизированных систем

О4 диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

уметь:

У1 осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем

У2 организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

У3 осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

У4 производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы

У5 настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

У6 обеспечивать работоспособность, обнаруживать и устранять неисправности

знать:

З1 состав и принципы работы автоматизированных систем, операционных систем и сред;

З2 принципы разработки алгоритмов программ, основных приемов программирования;

З3 модели баз данных;

З4 принципы построения, физические основы работы периферийных устройств

З5 теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации

З6 порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях

З7 принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н., «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н., которые актуализируются при изучении междисциплинарного курса:

1) способы защиты информации от утечки по техническим каналам;
2) основные методы управления защитой информации;
3) применять антивирусные средства защиты информации в операционных системах;
4) организационные меры по защите информации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении профессионального модуля:

1) знать и понимать: скорость изменения ИТ-сферы и области

информационной безопасности, а также важность соответствия современному уровню;

2) знать и понимать: подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;

3) знать и понимать: особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, MWare Workstation;

4) знать и понимать: типы угроз информационной безопасности, типы инцидентов;

5) знать и понимать: Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;

6) знать и понимать: структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;

знать и понимать: подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз

1.3. Планируемые личностные результаты освоения рабочей программы

ЛР 1. Осознающий себя гражданином и защитником великой страны.

ЛР 2. Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.

ЛР 3. Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 5. Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.

ЛР 6. Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях.

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

Результатом освоения МДК является овладение обучающимися видом деятельности - Эксплуатация автоматизированных (информационных) систем в защищенном исполнении в том числе профессиональными компетенциями (ПК):

Код	**Наименование результата обучения**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на

	государственном и иностранном языках
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.3 Результаты освоения междисциплинарного курса, подлежащие проверке

Наименование тем	Коды компетенций (ОК, ПК), личностных результатов (ЛР), умений (У), знаний (З), формированию которых способствует элемент программы	Средства контроля и оценки результатов обучения **в рамках текущей аттестации** (номер задания)	Средства контроля и оценки результатов обучения **в рамках промежуточной аттестации** (номер задания/контрольного вопроса/ экзаменационного билета)
Тема 1.1. Модели сетевого взаимодействия	О4 У5 У3 З6 ОК 02 ОК 07 ПК 1.1 ПК 1.4 ЛР 1 ЛР 5	ПЗ № 1	КВ № 1-31 ТЗ № 1
Тема 1.2. Физический уровень модели OSI	О1 У1 У3 З2 З3 ОК 01 ОК 03 ПК 1.1 ПК 1.2 ЛР 4 ЛР 7	ПЗ № 2	КВ № 1-31 ТЗ № 1
Тема 1.3. Топология компьютерных сетей	О2 У2 У3 З4 З7 ОК 05 ПК 1.1 ПК 1.4 ЛР 5 ЛР 9	ПЗ № 3	КВ № 1-31 ТЗ № 1

Тема 1.4. Технологии Ethernet	О1 У2 У4 З3 З7 ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 1 ЛР 6	ПЗ № 4	КВ № 1-31 ТЗ № 1
Тема 1.5. Технологии коммутации	О3 У1 У6 З2 З5 ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 1 ЛР 4	ПЗ № 5	КВ № 1-31 ТЗ № 1
Тема 1.6. Сетевой протокол IPv4	О1 У2 У4 З3 З7 ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 2 ЛР 3	ПЗ № 6	КВ № 1-31 ТЗ № 1
Тема 1.7. Скоростные и беспроводные сети	О3 У1 У6 З2 З5 ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 7	ПЗ № 7	КВ № 1-31 ТЗ № 1

Тема 2.1. Основы коммутации	О1 У2 У4 З3 З7 ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 4	ПЗ № 8	КВ № 1-31 ТЗ № 1
Тема 2.2. Начальная настройка коммутатора	О2 У2 У3 З4 З7 ОК 05 ПК 1.1 ПК 1.4 ЛР 9	ПЗ № 10	КВ № 1-31 ТЗ № 1
Тема 2.3. Виртуальные локальные сети (VLAN)	О3 У1 У6 З2 З5 ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 4	ПЗ № 11 ПЗ № 12	КВ № 1-31 ТЗ № 1
Тема 2.4. Функции повышения надежности и производительности	О2 У2 У3 З4 З7 ОК 05 ПК 1.1 ПК 1.4 ЛР 1 ЛР 2	ПЗ № 14	КВ № 1-31 ТЗ № 1
Тема 2.5. Адресация сетевого уровня и маршрутизация	О1 У1 У3 З2 З3 ОК 01 ОК 03 ПК 1.1 ПК 1.2 ЛР 1 ЛР 5	ПЗ № 15 ПЗ № 16	КВ № 1-31 ТЗ № 1

Тема 2.6. Качество обслуживания (QoS)	О3 У1 У6 З2 З5 ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 6 ЛР 7	ПЗ № 18	КВ № 1-31 ТЗ № 1
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	О1 У2 У4 З3 З7 ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 1	ПЗ № 19	КВ № 1-31 ТЗ № 1
Тема 2.8. Многоадресная рассылка	О2 У1 У5 З1 З3 ОК 03 ПК 1.2 ЛР 5 ЛР 7	ПЗ № 20	КВ № 1-31 ТЗ № 1
Тема 2.9. Функции управления коммутаторами	О2 У2 У3 З4 З7 ОК 05 ПК 1.1 ПК 1.4 ЛР 1 ЛР 7	ПЗ № 21	КВ № 1-31 ТЗ № 1
Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	О2 У1 У5 З1 З3 ОК 03 ПК 1.2 ЛР 4	ТЗ № 1	КВ № 1-31 ТЗ № 1

Тема 3.2. Межсетевые экраны	О4 У5 У3 З6 ОК 02 ОК 07 ПК 1.1 ПК 1.4 ЛР 1 ЛР 7	ПЗ № 22	КВ № 1-31 ТЗ № 1
Тема 3.3. Системы обнаружения и предотвращения проникновений	О2 У2 У3 З4 З7 ОК 05 ПК 1.1 ПК 1.4 ЛР 6	ПЗ № 23	КВ № 1-31 ТЗ № 1
Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	О1 У2 У4 З3 З7 ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 1 ЛР 5	ПЗ № 24	КВ № 1-31 ТЗ № 1

2. Комплект оценочных средств для текущей аттестации

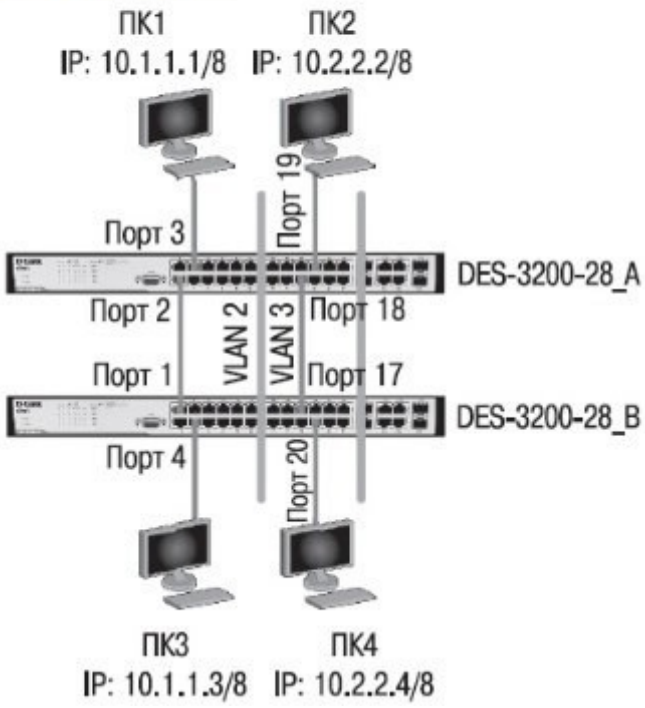
2.1. Практические задания (ПЗ)

ПЗ № 1

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.

ПЗ № 2

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.

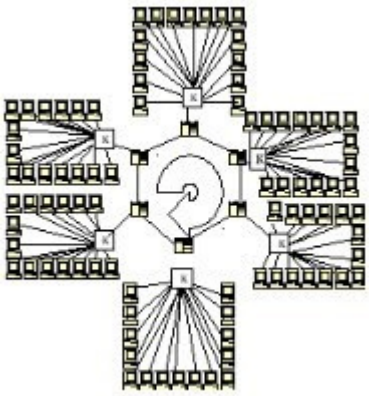
Задание 4. Проверьте кабель на работоспособность.

ПЗ № 3

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.

ПЗ № 4

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

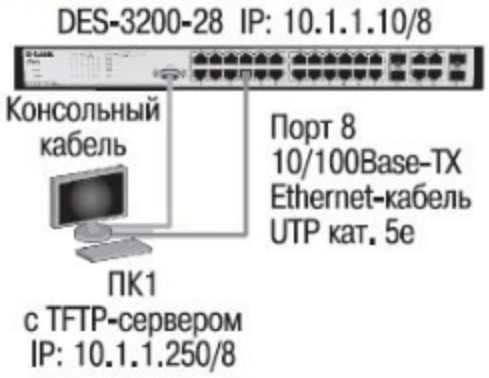
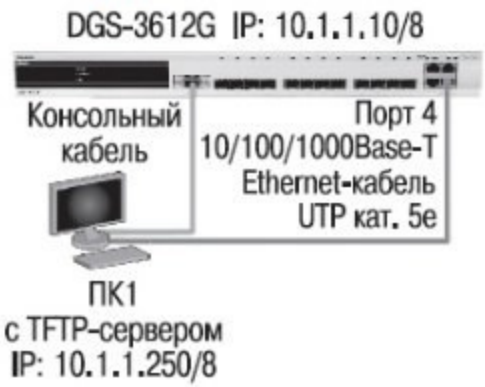


Схема 2



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 MACадресом (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.

ПЗ № 5

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.

ПЗ № 6

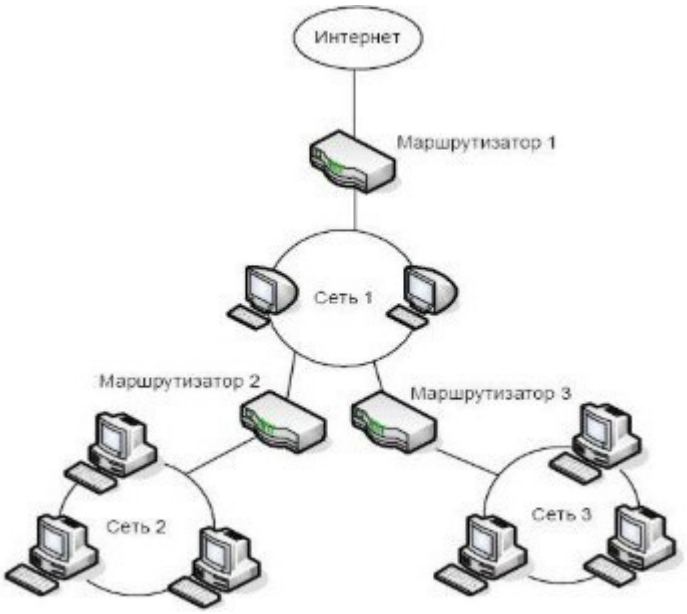
Задание 1. В работе даны 4 варианта задания (Табл. 1). Необходимо сделать все варианты. На приведенной схеме представлена составная локальная сеть. Отдельные локальные сети соединены маршрутизаторами. Для каждой локальной сети указано количество компьютеров. Провайдер, для вас выдал IP-сеть (данные о 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?

ПЗ № 7

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)
```

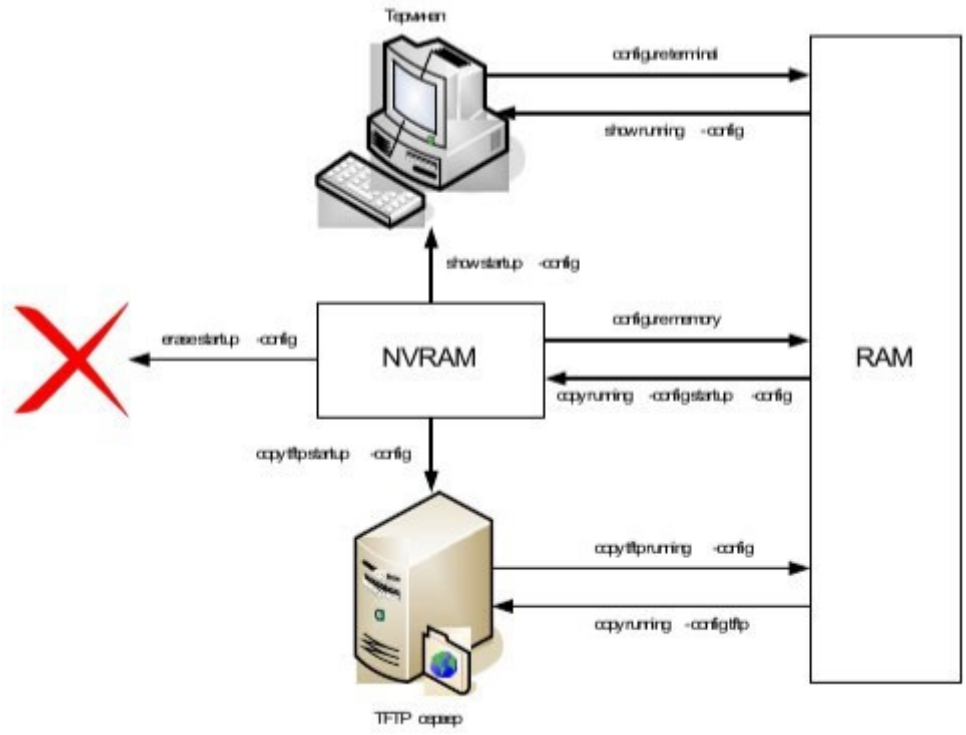
Задание 4. Опишите уровни доступа к командам маршрутизатора:

```
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.

ПЗ № 8

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.

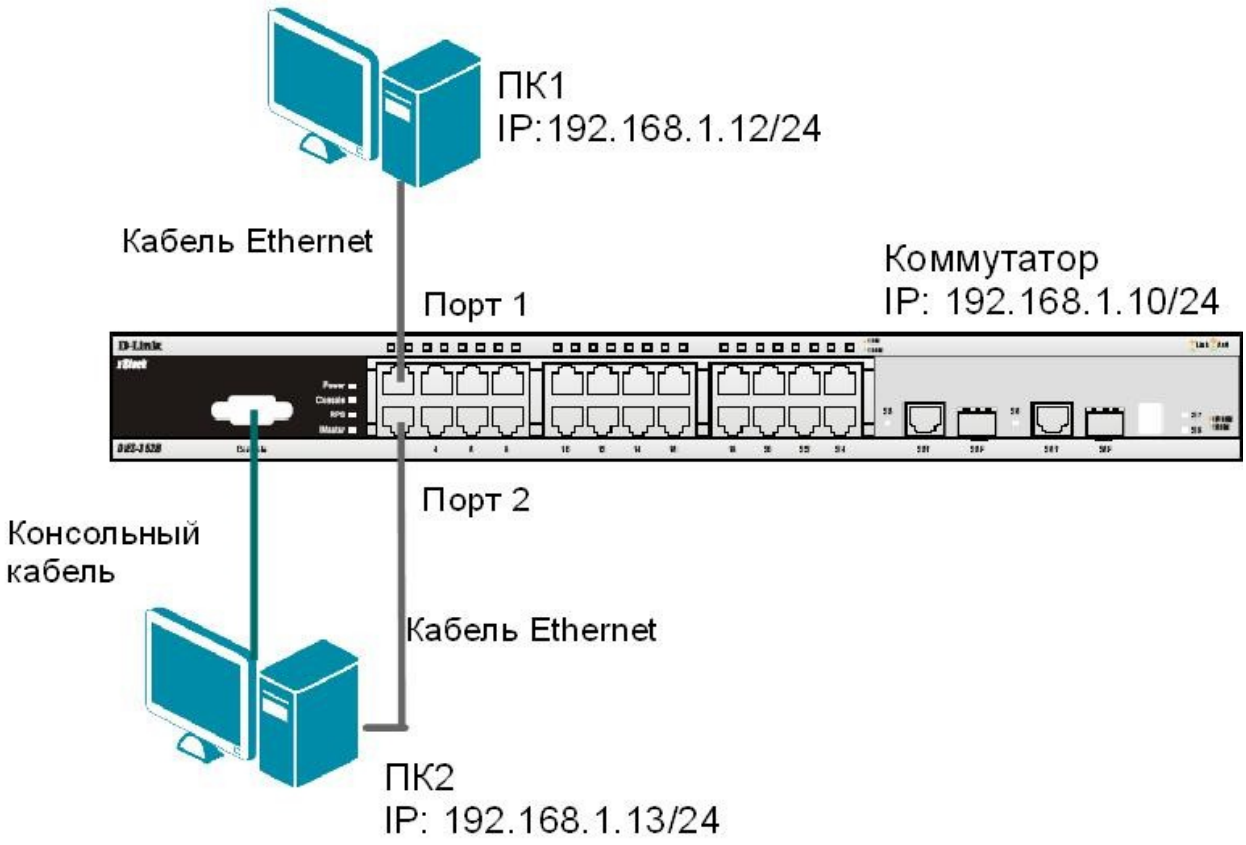
Задание 2. Опишите команды коммутатора:

- 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.

ПЗ № 10

Схема 3



3.1. Команды управления таблицей коммутации

Просмотрите содержимое таблицы MAC-адресов:
show fdb

Определите порт коммутатора, к которому подключено устройство с известным МАСадресом (в качестве МАС-адреса введите реальный МАС-адрес ПК1): show fdb mac_address 00-03-47-BD-3F-57
Посмотрите список МАС-адресов устройств, принадлежащих VLAN по умолчанию (default VLAN): show fdb vlan default
Посмотрите МАС-адреса устройств, изученные портом 2:
show fdb port 2
Просмотрите время нахождения записи в таблице МАС-адресов:
show fdb aging_time
Измените время нахождения МАС-адреса в таблице до 350 секунд:
config fdb aging_time 350
Удалите все динамически созданные записи из таблицы МАС-адресов:
clear fdb all
Создайте статическую запись в таблице МАС-адресов (в качестве МАС-адреса введите реальный МАС-адрес ПК2) на порте 2: create fdb default 00-03-47-BD-01-11 port 2
Просмотрите статические записи в таблице МАС-адресов:
show fdb static
Просмотрите статические записи таблицы МАС-адресов на порте 2:
show fdb static port 2
Удалите статическую запись из таблицы МАС-адресов:
delete fdb default 00-03-47-BD-01-11
Просмотрите содержимое таблицы МАС-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 МАС-адреса укажите МАС-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

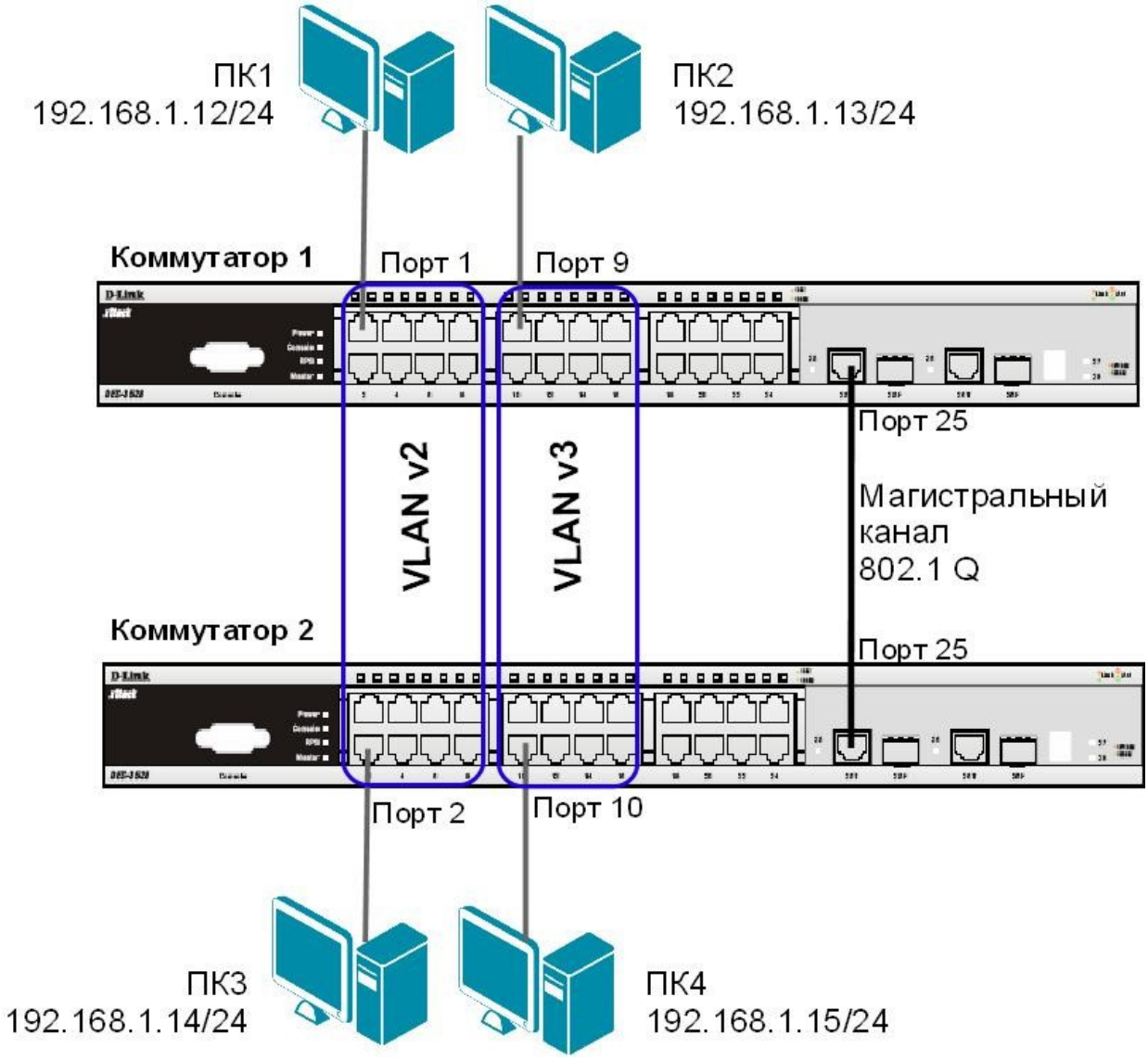
Проверьте, что запись удалена:
show arpentry static
Измените время нахождения записи в ARP-таблице до 30 минут (по умолчанию 20 минут): config arp_aging time 30
Проверьте выполненные настройки:
show arpentry

ПЗ № 11

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>

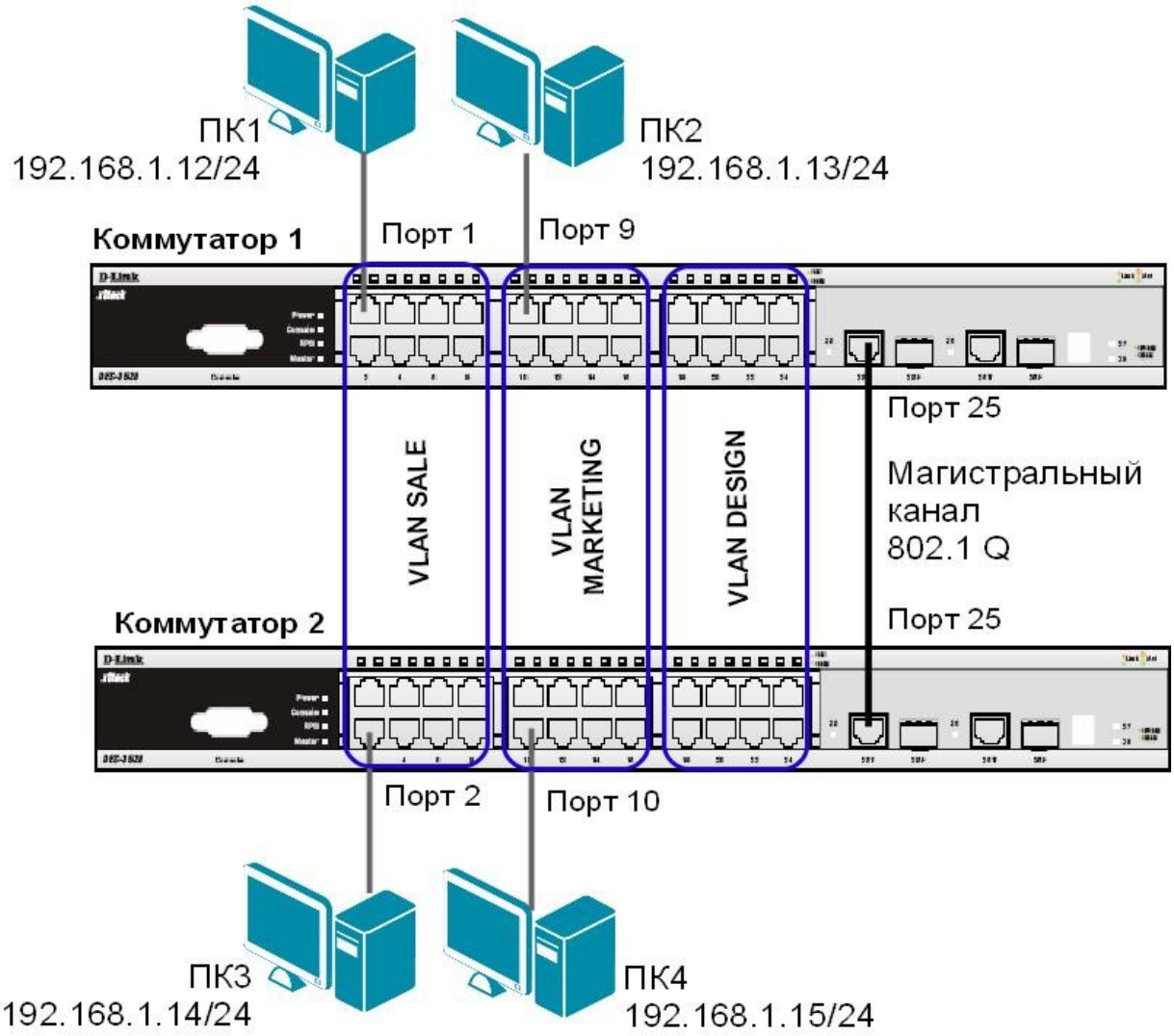
- от ПК1 к ПК 2 _____
- от ПК1 к ПК4 _____

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

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.

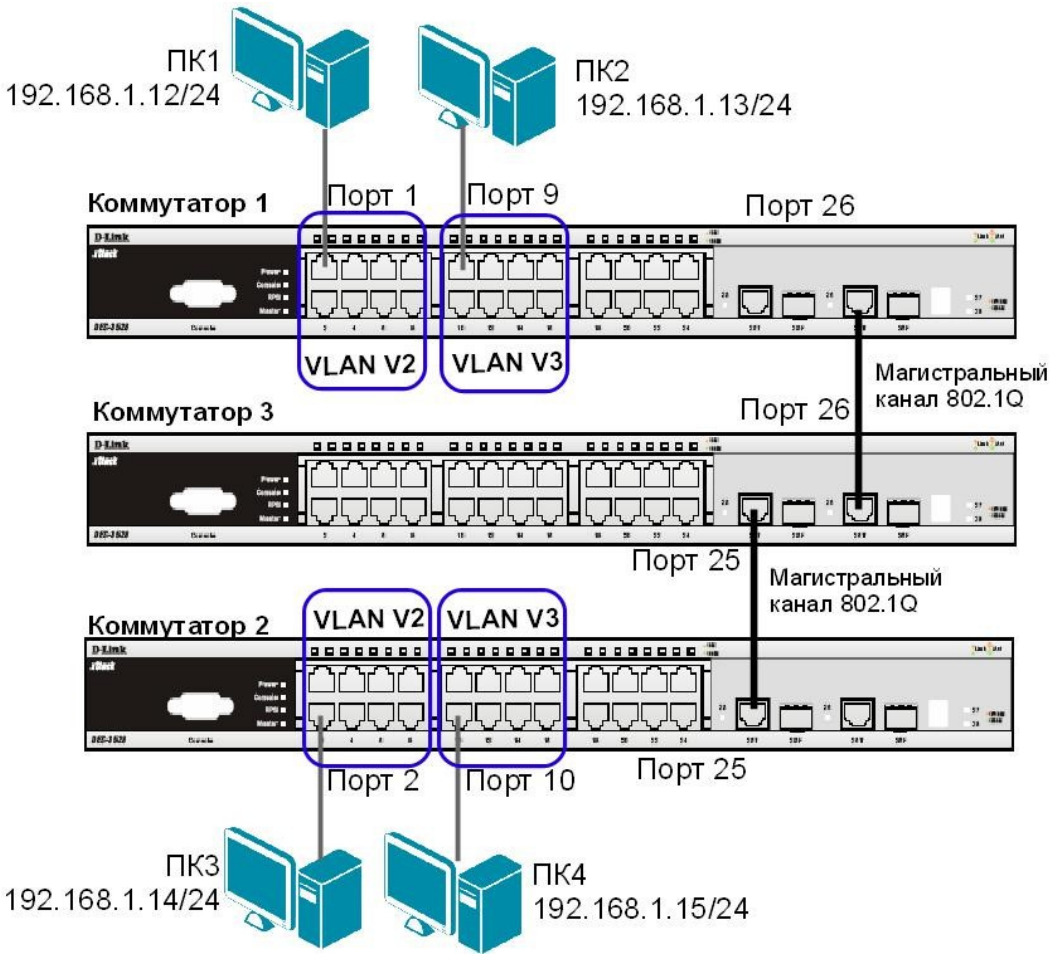
Проверьте доступность соединения между рабочими станциями командой ping:
ping <IP-address>

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

Отключите магистральные каналы на обоих коммутаторах:
disable vlan_trunk

ПЗ № 12

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 _____

ПЗ № 14

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

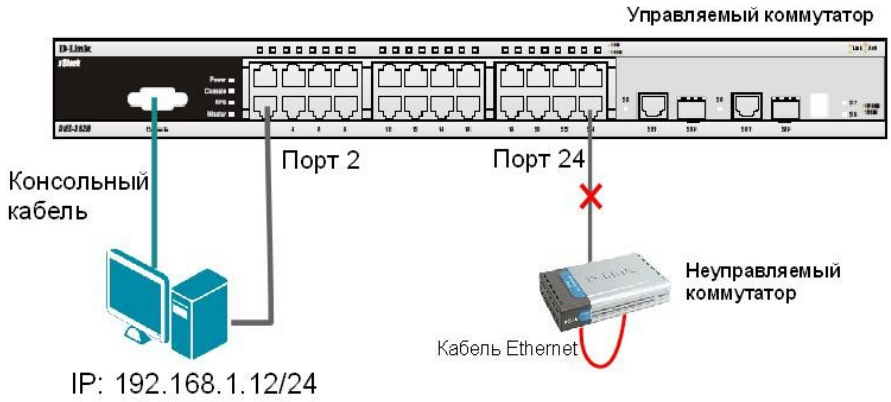
В данном задании рассматривается блокирование порта управляемого коммутатора при обнаружении петли в подключённом сегменте.

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 all
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.

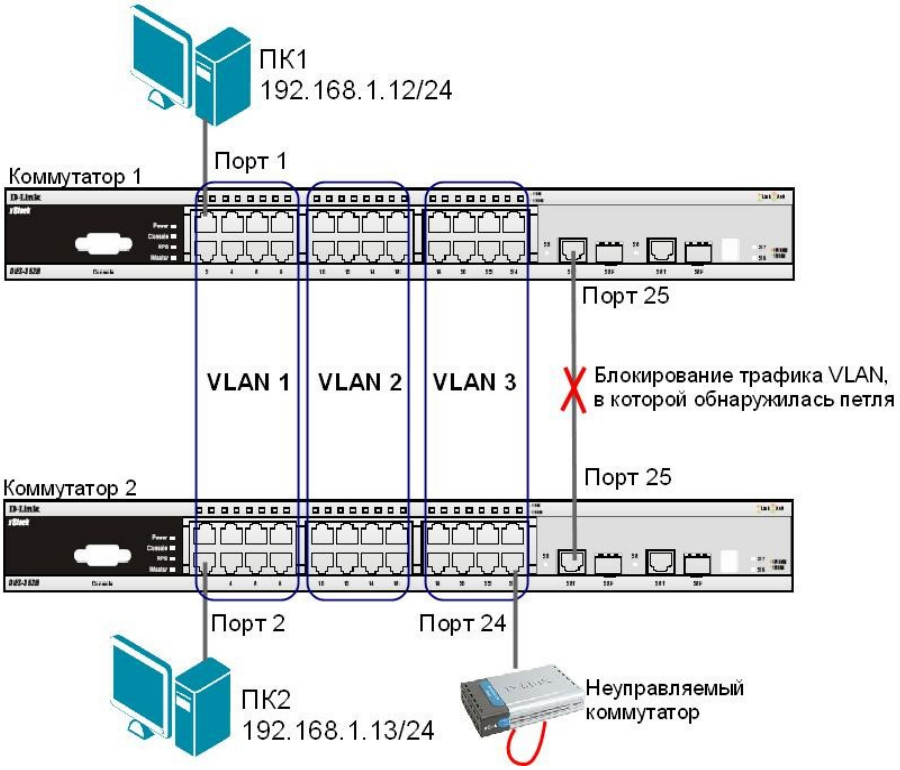
_____
_____

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 all
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.

ПЗ № 15

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
Шлюз_ФАМИЛИЯ	G0/1	192.168.1.254	255.255.255.0
	S0/0/1	209.165.200.226	255.255.255.252
Поставщик услуг Интернета	S0/0/1 (DCE)	209.165.200.225	255.255.255.252

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Обнаружение сетевых ресурсов с помощью протокола CDP

Часть 3. Обнаружение сетевых ресурсов с помощью протокола LLDP

Необходимые ресурсы

- 2 маршрутизатора Cisco
- 3 коммутатора Cisco
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией

Часть 1: Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры для маршрутизатора и коммутаторов.

Шаг 1: Создайте сеть согласно топологии.

В топологии не указаны Ethernet-порты, используемые на коммутаторах. Можно воспользоваться любыми Ethernet-портами для подключения коммутаторов с помощью сетевого кабеля, как указано на диаграмме топологии.

Шаг 2: При необходимости инициализируйте и перезагрузите сетевые устройства.

Шаг 3: Настройте основные параметры коммутаторов.

a. Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режим EXEC.
b. Войдите в режим конфигурации.
c. Отключите поиск DNS, чтобы предотвратить попытки коммутатора неверно преобразовывать введенные команды таким образом, будто они являются именами хостов.
d. Укажите имя хоста в соответствии с топологией.
e. Убедитесь, что порты коммутаторов, к которым подключены кабели Ethernet, включены.
f. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте основные параметры маршрутизаторов.

a. Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режим EXEC.
b. Войдите в режим конфигурации.
c. Скопируйте и вставьте следующие конфигурации для маршрутизаторов. Не забудьте указать вашу фамилию на английском языке при использовании команды hostname.

ISP:

hostname ISP no
ip domain lookup
interface
Serial0/0/1
ip address 209.165.200.225 255.255.255.252
no shutdown **Шлюз:**

hostname Gateway_ФАМИЛИЯ no ip
domain lookup interface
GigabitEthernet0/1 ip address
192.168.1.254 255.255.255.0 ip nat
inside no shutdown interface Serial0/0/1
ip address 209.165.200.226 255.255.255.252
ip nat
outside no
shutdown
ip nat inside source list 1 interface Serial0/0/1 overload access-list 1 permit
192.168.1.0 0.0.0.255

d. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Часть 2: Обнаружение сетевых ресурсов с помощью протокола CDP

На устройствах Cisco протокол CDP включен по умолчанию. Воспользуйтесь CDP, чтобы обнаружить порты, к которым подключены кабели.

a. На маршрутизаторе Gateway_ФАМИЛИЯ введите команду для отображения сведений, полученный в ходе работы протокола CDP, чтобы убедиться в том, что на маршрутизаторе включен протокол CDP.
С какой периодичностью отправляются пакеты CDP?

_____
_____

Если на маршрутизаторе Gateway_ФАМИЛИЯ отключен протокол CDP, включите его в режиме глобальной конфигурации.
Выполните команду для отображения списка интерфейсов, участвующих в объявлениях CDP.
Сколько интерфейсов участвует в объявлениях CDP? Какие из них активны?

_____
_____

b. Выполните команду для определения соседей CDP.
c. Чтобы отобразить более подробные сведения о соседях CDP, выполните команду из пункта b с ключом **detail**.
d. Какую информацию можно узнать об ISP и S3 в результате выполнения команды из предыдущего пункта?

_____
_____
_____
_____

e. Настройте интерфейс SVI на S3 (можно использовать VLAN 1). Укажите доступный IP-адрес в пределах сети 192.168.1.0/24. В качестве шлюза по умолчанию укажите 192.168.1.254.
f. Выполните команду для отображения детальной информации о соседях CDP на маршрутизаторе Gateway_ФАМИЛИЯ. Какие дополнительные сведения доступны теперь?

_____
_____

g. Из соображений безопасности рекомендуется отключить протокол CDP на интерфейсах, которые используются для подключения к внешним сетям.
Отключите протокол CDP в режиме конфигурации интерфейса S0/0/1 на маршрутизаторе Gateway_ФАМИЛИЯ.
Проверьте, отключен ли протокол CDP для интерфейса S0/0/1. Возможно, потребуется подождать, пока истечет время удержания. Время удержания — это

время, в течение которого сетевые устройства хранят пакеты CDP, пока эти пакеты не будут отклонены устройствами.
Интерфейс S0/0/1 маршрутизатора Gateway_ФАМИЛИЯ больше не связан с маршрутизатором ISP посредством отношений смежности (adjacency) CDP. Однако у этого интерфейса по-прежнему имеются отношения смежности с другими интерфейсами. В этом можно убедиться с помощью определенной команды, которая уже использовалась в пункте «a».

h. Отключите протокол CDP в режиме глобальной конфигурации.
Какие команды необходимо выполнить, чтобы убедиться в том, что протокол CDP отключен?

_____

_____

i. Включите протокол CDP глобально на маршрутизаторе Gateway_ФАМИЛИЯ. На скольких интерфейсах включен протокол CDP? На каких интерфейсах этот протокол отключен?

_____

_____

j. Подключитесь ко всем коммутаторам через консоль и выполните необходимые команды CDP, чтобы определить Ethernet-порты, которые используются для подключения к другим устройствам. Например, можно посмотреть информацию о соседях CDP.

Часть 3: Обнаружение сетевых ресурсов с помощью протокола LLDP

На устройствах Cisco протокол LLDP может быть включен по умолчанию.
Воспользуйтесь LLDP, чтобы обнаружить порты, к которым подключены кабели.

a. На маршрутизаторе Gateway_ФАМИЛИЯ выполните команду **show lldp** в привилегированном режиме EXEC. Включен ли протокол LLDP?
Если на маршрутизаторе Gateway_ФАМИЛИЯ отключен протокол LLDP, включите его.

b. На маршрутизаторе Gateway_ФАМИЛИЯ введите снова введите команду, чтобы убедиться в том, что на маршрутизаторе включен протокол LLDP.
Выполните определенную команду для просмотра того, какие устройства имеются по соседству с маршрутизатором Gateway_ФАМИЛИЯ?

_____

_____

c. Если у маршрутизатора Gateway_ФАМИЛИЯ нет соседей LLDP, включите протокол LLDP на коммутаторах в режиме глобальной конфигурации.

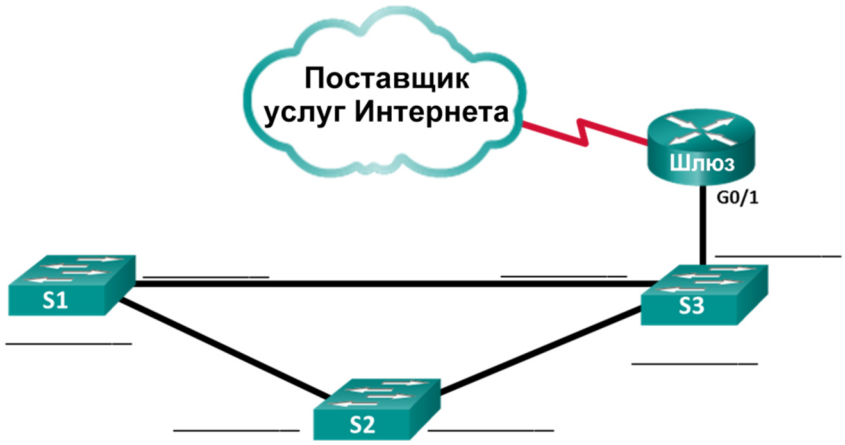
d. Выполните команду для отображения информации о соседях LLDP на коммутаторах и маршрутизаторе, чтобы отобразить список портов, на которых включен LLDP.

e. На маршрутизаторе Gateway_ФАМИЛИЯ выполните команду из предыдущего пункта с ключом **detail**.
Какой порт используется на S3 для подключения к маршрутизатору шлюза?

_____

_____

f. Используйте результаты выполнения команды **show** для протоколов CDP и LLDP, чтобы указать подключенные порты в топологии сети.



ПЗ № 16

Роутер1:

%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to up
%LINK-3-UPDOWN: Interface Bri0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Bri0, changed state to up
router1(config-line)#
router1(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console

На Маршрутизаторе 1 запускаем команду показа порта Serial0.

router1#show interfaces serial0
Serial0 is up, line protocol is up
Hardware is HD64570
Description: Serial Link to Router3
Internet address is 175.10.1.1/24
MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of show interface counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

На маршрутизаторе 1 конфигурируем PPP формирование пакета для интерфейса S0.

router1(config)#interface serial0
router1(config-if)#encapsulation ppp

%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
router1(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
На маршрутизаторах 1 3 выводим показ интерфейса Serial0, чтобы проверить, сконфигурирован ли PPP. прозваниваем от Маршрутизатора 1 Маршрутизатор 3, это должно показать, что связь операционная.
router1#show interfaces serial0
Serial0 is up, line protocol is down
Hardware is HD64570
Description: Serial Link to Router3
Internet address is 175.10.1.1/24
MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP ACKRCVD
Closed: IPCP , CDPCP
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of show interface counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
router1#ping 175.10.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 175.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Конфигурируем PPP идентификацию для S0 через связь между маршрутизатором 1 и 3. Используем пароль cisco.
router1(config)#username router3 password cisco
router1(config)#interface serial0
router1(config-if)#ppp authentication chap
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
router1(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

Для того, чтобы убедиться в правильности работы данных команд, запускаем показ интерфейса serial0, а так же пингуем связь между 1 и 3 маршрутизаторами.

```
router1#show interface serial0
Serial0 is up, line protocol is up
Hardware is HD64570
Description: Serial Link to Router3
Internet address is 175.10.1.1/24
MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of show interface counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
router1#ping 175.10.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 175.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Аналогично роутер 3:

```
%LINK-3-UPDOWN: Interface Serial1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to up
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to up
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
router3(config-router)#
router3(config-router)#exit
router3(config)#interface serial0
router3(config-if)#encapsulation ppp
router3(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
router3#show interfaces serial0
Serial0 is up, line protocol is up
Hardware is HD64570
Internet address is 175.10.1.2/24
```

MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of show interface counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
router3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router3(config)#username router1 password cisco
router3(config)#interface serial0
router3(config-if)#ppp authentication chap
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
router3(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
router3#show interfaces serial0
Serial0 is up, line protocol is up
Hardware is HD64570
Internet address is 175.10.1.2/24
MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of show interface counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier

+0 output buffer failures, 0 output buffers swapped out

ПЗ № 18

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

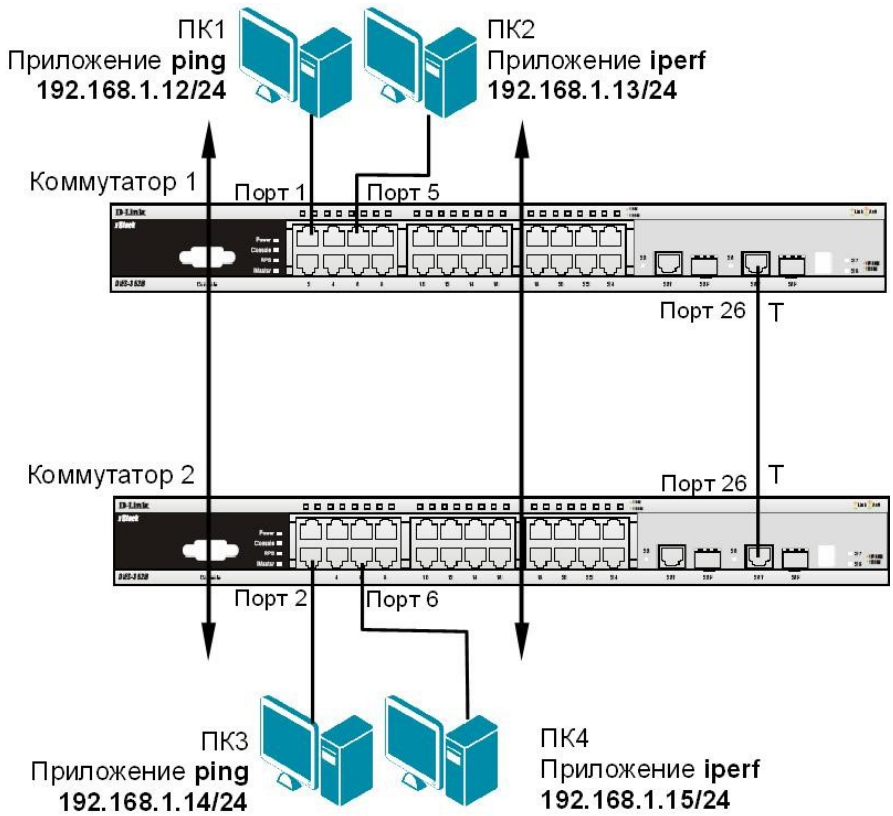
Настройка коммутатора 1

Для создания «узкого» места, настройте на порте 26 функцию bandwidth_control, ограничивающую приём и передачу данных скоростью 64 Кбит/с: config bandwidth_control 26 rx_rate 64 tx_rate 64

Настройка коммутатора 2

Для создания «узкого» места, настройте на порте 26 функцию bandwidth_control, ограничивающую приём и передачу данных скоростью 64 Кбит/с: config bandwidth_control 26 rx_rate 64 tx_rate 64

Схема 1_1



ЗАДАНИЕ 1

Назначьте на всех ПК IP-адреса из одной подсети. Запустите продолжительный тест ping между ПК1 и ПК3, а так же между ПК2 и ПК4.

Собрав в течение 20-30 секунд статистику, запишите примерное среднее время откликов и количество потерь (запросов без ответов), если они существуют:

между ПК1 и ПК3 _____

между ПК2 и ПК4 _____

ЗАДАНИЕ 2 Запустите продолжительный тест ping между ПК1 и ПК3, а так же между ПК2 и ПК4.

Для создания нагрузки на линию связи между коммутаторами, запустите программу iperf:

- на ПК2 с ключом «-s» (в роли сервера): iperf –s -u
- на ПК4 с ключами «-c ip-сервера -i 1 -t 10000 -r -u -b10M -P5» (в роли клиента):

iperf -c 192.168.1.13 -i 1 -t 10000 -r -u -b10M -P5

НЕ ОСТАНАВЛИВАЙТЕ запущенные программы ping и iperf. Собранная с помощью них статистика понадобится для выполнения следующего задания.
Собрав в течение 20-30 секунд статистику, запишите примерную среднюю скорость, выводимую программой iperf:

- ПК2 _____
- ПК4 _____

Посмотрите на ПК1 и ПК3, ПК2 и ПК4 информацию и запишите примерное среднее время откликов и количество потерь (запросов без ответов), если они есть:
от ПК1 к ПК3
_____ от ПК3 и ПК1 _____ от ПК2 и ПК4
_____ от ПК4 и ПК2 _____
Запишите ваши наблюдения, сравните их с результатами задания 1:

_____
_____
_____

ЗАДАНИЕ 3

Настройте приоритизацию. Для этого поменяйте на порте 1, к которому подключена рабочая станция ПК1, значение приоритета по умолчанию на 7: config 802.1p default_priority 1 7
Примечание: пользовательский приоритет и метод обработки остаются по умолчанию.
Поменяйте на порте 2, к которому подключена рабочая станция ПК3, значение приоритета по умолчанию на 7:
config 802.1p default_priority 2 7
Примечание: благодаря изменению значения приоритета портов, к которым подключены компьютеры с приоритетным трафиком на 7, все кадры, передаваемые ими, получат наивысший приоритет по сравнению с кадрами, поступающими от других компьютеров на остальные не приоритизированные порты обоих коммутаторов.
Посмотрите текущие настройки приоритета по умолчанию на портах коммутаторов 1 и 2: show 802.1p default_priority
Какой приоритет назначен по умолчанию порту 3?

_____
Посмотрите карту привязки пользовательских приоритетов 802.1p к очередям класса обслуживания: show 802.1p user_priority

Запишите, что вы наблюдаете. Какому классу обслуживания соответствует приоритет по умолчанию = 0?

_____

При включении приоритизации посмотрите, как изменились условия прохождения трафика. Изменились ли они, и насколько? Сравните результаты с заданием 2.

_____
_____
_____

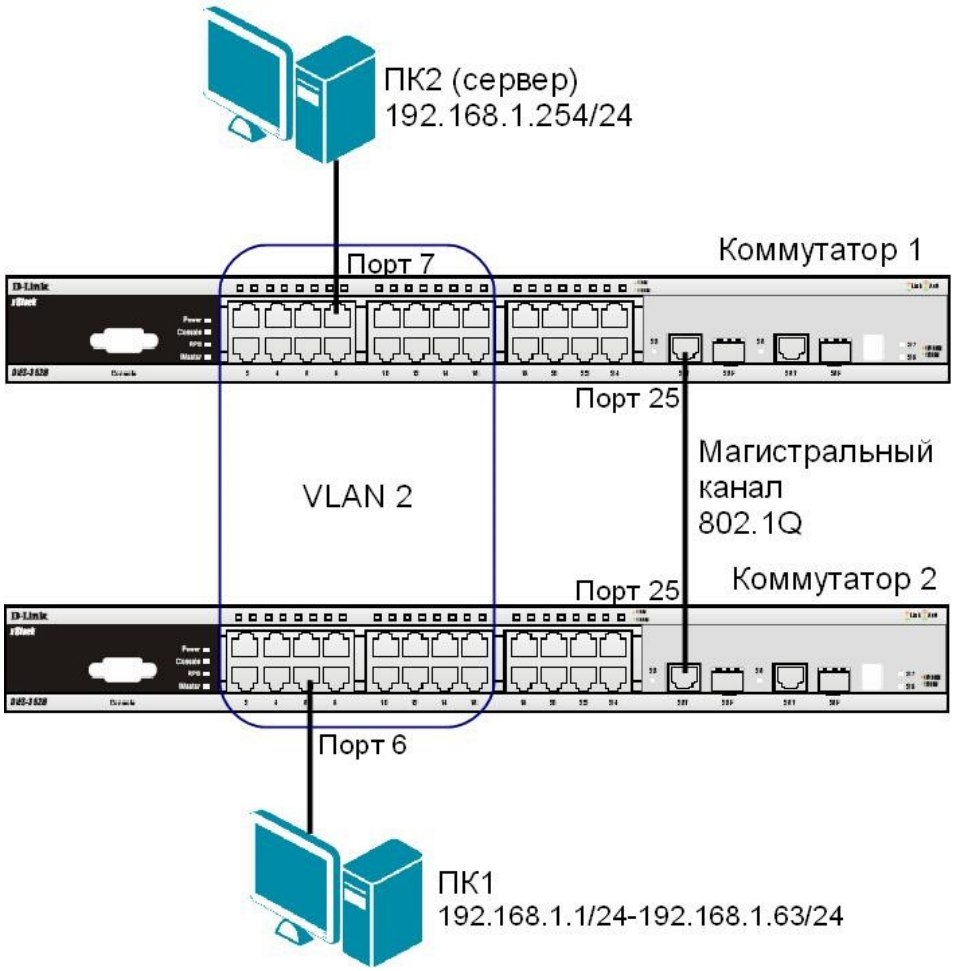
Сравните результаты с заданием 1. Удалось ли достичь в нагруженном канале с включённой приоритизацией таких же параметров, что и в не нагруженном канале для трафика между ПК 1 и ПК3? Объясните почему?

_____
_____

ПЗ № 19

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.

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

Правило 1.
Создайте профиль доступа с номером 5, разрешающий доступ для подсети 192.168.1.0/26 (узлам с 1 по 63):
create access_profile profile_id 5 profile_name 5 ip source_ip_mask 255.255.255.192
Создайте правило для профиля доступа 5:
config access_profile profile_id 5 add access_id 1 ip source_ip 192.168.1.0 port 25 permit
Примечание: созданное правило разрешает прохождение трафика IP-подсети 192.168.1.0/26 через 25 порт.

Правило 2
Создайте профиль доступа с номером 15, запрещающий остальным станциям доступ к серверу:
create access_profile profile_id 15 profile_name 15 ip source_ip_mask 255.255.255.0
Создайте правило для профиля доступа 15:
config access_profile profile_id 15 add access_id 1 ip source_ip 192.168.1.0 port 25 deny
Примечание: созданное правило запрещает прохождение через 25 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 192.168.1.64192.168.1.254/24)

Протестируйте командой ping соединение с сервером 192.168.1.254/24.
Что вы наблюдаете? Запишите.

_____

_____

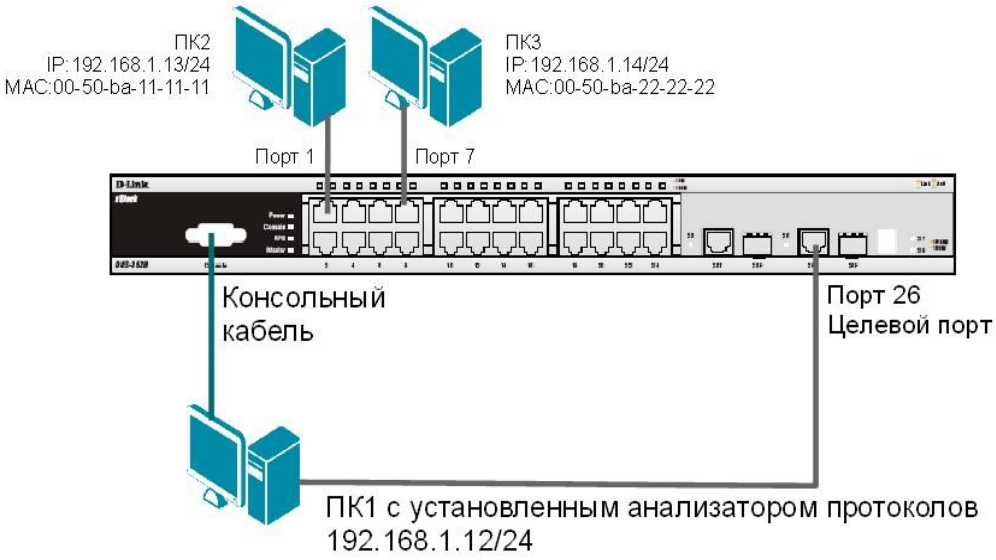
Удалите профиль ACL (например, профиль 15).
delete access_profile profile_id 15
Проверьте соединение с сервером командой ping:
ping 192.168.1.254
Что вы наблюдаете? Запишите.

_____

_____

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 MACадреса рабочих станций.

Создайте профиль доступа 5:

create access_profile profile_id 5 profile_name 5 ethernet source_mac FF-FF-FF-FF-FF-FF

Создайте правило для профиля доступа 5, в результате выполнения которого кадры, принимаемые на любой порт коммутатора с ПК3 будут зеркалироваться на целевой порт: config access_profile profile_id 5 add access_id 1 ethernet source_mac 00-50-ba-22-22-22 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

ПЗ № 20

1. Сделать выполнение приема и отправки данных параллельными

Необходимо реализовать программу, ведующую прием сообщений непрерывно, и при этом позволяющую пользователю ввести и отправить сообщение в любой момент.
Программа:

1.1. Создает дейтаграммный сокет для работы в сетях IPv4 по протоколу UDP.
1.2. Запрашивает у пользователя адрес и порт для указания как собственных и выполняет привязку сокета.
1.3. Запрашивает у пользователя адрес и порт для отправки на них сообщений и сохраняет эти данные в переменной-структуре sockaddr_in.
1.4. Создает поток для приема сообщений, который в бесконечном цикле принимает сообщение и отображает его на экране по прибытии вместе с адресом и портом отправителя.
1.5. В бесконечном цикле (в основном потоке):
1.5.1. Запрашивает у пользователя текст сообщения.
1.5.2. Если введенный текст — /quit, прерывает цикл.
1.5.3. Иначе отправляет сообщение на заданный в п. 1.3 адрес и порт.
1.6. Закрывает ранее созданный сокет.

2. Изменить программу, задействовав вместо одноадресной рассылки (unicast) многоадресную (multicast) с использованием фиксированной группы multicast.

2.1. Необходимые заголовочные файлы: <winsock2.h> вместо
<winsock.h>, <ws2tcpip.h> для многоадресной рассылки.
2.2. В пункте 1.3 требуется отныне и впредь вводить адреса класса D.
2.3. До начала передачи данных (перед пунктом 1.4) выполнять настройку сокета функцией setsockopt():
2.3.1. Отключить доставку пакетов multicast обратно источнику, если он находится в той же группе multicast, куда отправлен пакет (уровень IPPROTO_IP, параметр IP_MULTICAST_LOOP).
2.3.2. Указать отправлять пакеты multicast через сетевой интерфейс, которому принадлежит адрес, указанный в пункте 1.2 (уровень IPPROTO_IP, параметр IP_MULTICAST_IF).
2.3.3. Присоединиться к группе multicast, адрес которой указан в п. 1.3
(уровень IPPROTO_IP, параметр IP_ADD_MEMBERSHIP).

2.4. Вместе с пунктом 1.6 необходимо покидать группу многоадесной рассылки
(параметр IP_DROP_MEMBERSHIP уровня IPPROTO_IP).

2.5. Проверить правильность работы многоадресной рассылки.

2.5.1. **В случае, если доступны две машины,** программам на них следует присоединиться к одной группе multicast (с указанием одинакового номера порта) и отправить по сообщению. Каждая программа должна получать сообщения, отправленные другой, и не получать своих. **Внимание:** машины должны быть в одной сети!

2.5.2. **В случае, если доступна только одна машина,** тестирование можно осуществить так:

- оба экземпляра программы должны присоединяться к общей группе multicast (например, 226.0.0.1);
- первый экземпляр должен получать сообщения на порт *N*, а отправлять на порт *(N+1)*, второй — наоборот.

Нескольким экземплярам программы следует присоединиться к одной группе multicast (с указанием одинакового номера порта) и отправить по сообщению. Каждая программа должна получать все сообщения, включая собственные.

3. Обеспечить поддержку псевдонимов пользователей

Необходимо добавить возможность пользователям устанавливать псевдонимы, которыми будут подписываться их сообщения вместо адресов и портов, специальным сообщением-командой.

3.1. Перед пунктом 1.4 требуется запросить у пользователя желаемый псевдоним name и отправить сообщение вида **/nick** name, а затем некоторое время (например, 1 с) дожидаться возможного сообщения о том, что данный псевдоним уже используется.

3.2. Если за время ожидания было получено сообщение **/taken** name , где name — тот же псевдоним, который хотел занять пользователь, следует напечатать сообщение об этом и вернуться к пункту 3.1. В противном случае (сообщение не получено) следует отправить сообщение **/taken** name и начать обмен сообщениями (пункт 1.4 и далее).

3.3. Всем программам в любой момент, кроме времени ожидания в пункте 3.1:

3.3.1. При получении сообщения **/nick** name, если name совпадает с псевдонимом, который удалось занять в пункте 3.2, необходимо отправить сообщение **/taken** name источнику сообщения **/nick** name.

3.3.2. При получении сообщения **/taken** name необходимо сохранить информацию, что псевдоним name соответствует аресу и порту отправителя пакета.

3.4. При печати сообщений вместо адреса и порта отправителя требуется печатать псевдоним отправителя, если он известен из пункта 3.3.2.

Произвольная программа (необязательная)

4. Добавить возможность читать сообщения нескольких групп multicast

Сокет может одновременно входить в несколько групп многоадресной рассылки. Процедуры отправки и приема сообщений никак не изменятся, однако, получены будут сообщения, адресованные любой из групп, в которые входит сокет. Отправка данных по-прежнему выполняется на конкретный адрес и порт (в одну группу, куда клиент входил изначально).

Необходимо дать пользователю возможность входить в группу multicast командой **/join** *address*, например, **/join** *226.0.0.10*, и покидать группу командой **/leave** *address*, например, **/leave** *226.0.0.10*.

5. **Добавить возможность отправки личных сообщений**

Требуется добавить в режиме групповой переписки возможность адресной отправки сообщений. При вводе пользователем сообщения специального вида **/to** *host port* private message text, например,

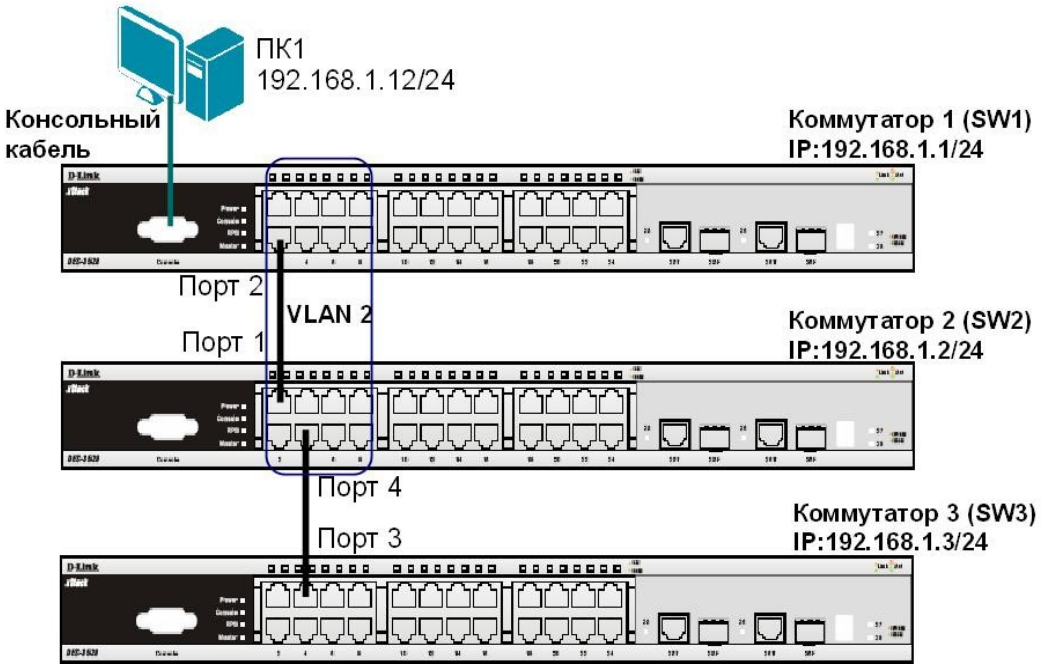
/to *10.100.0.42 1234* Грузите апельсины бочками., сообщение требуется отправлять не в группу multicast, а по указанному адресу и на заданный порт. Вместо адреса и порта следует также предусмотреть указание и псевдонима: **/to** *корейко* Грузите апельсины бочками.

6. **Добавить команду для определения участников переписки**

При получении сообщения **/who** следует не отображать его, как остальные, но автоматически ответить отправителю сообщением **/taken** *name* , где *name* — псевдоним пользователя, который получил команду **/who**.

ПЗ № 21

Схема 16



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

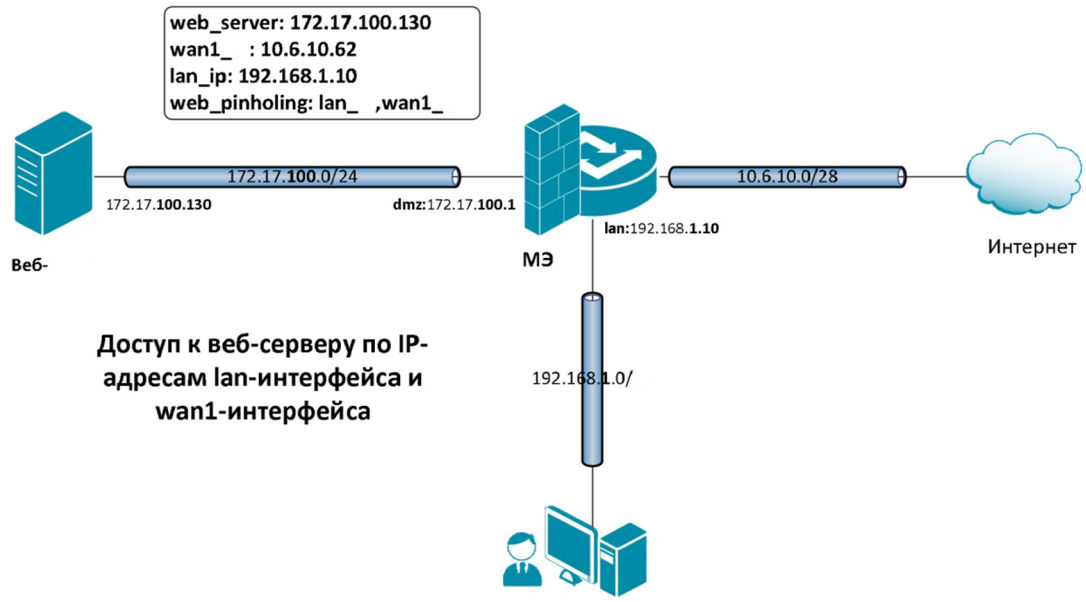
Настройка коммутатора 1 (SW1)

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 LLDPсообщений 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

ПЗ № 22

Топология сети



Описание практической работы

Проверка отсутствия конфликта по портам

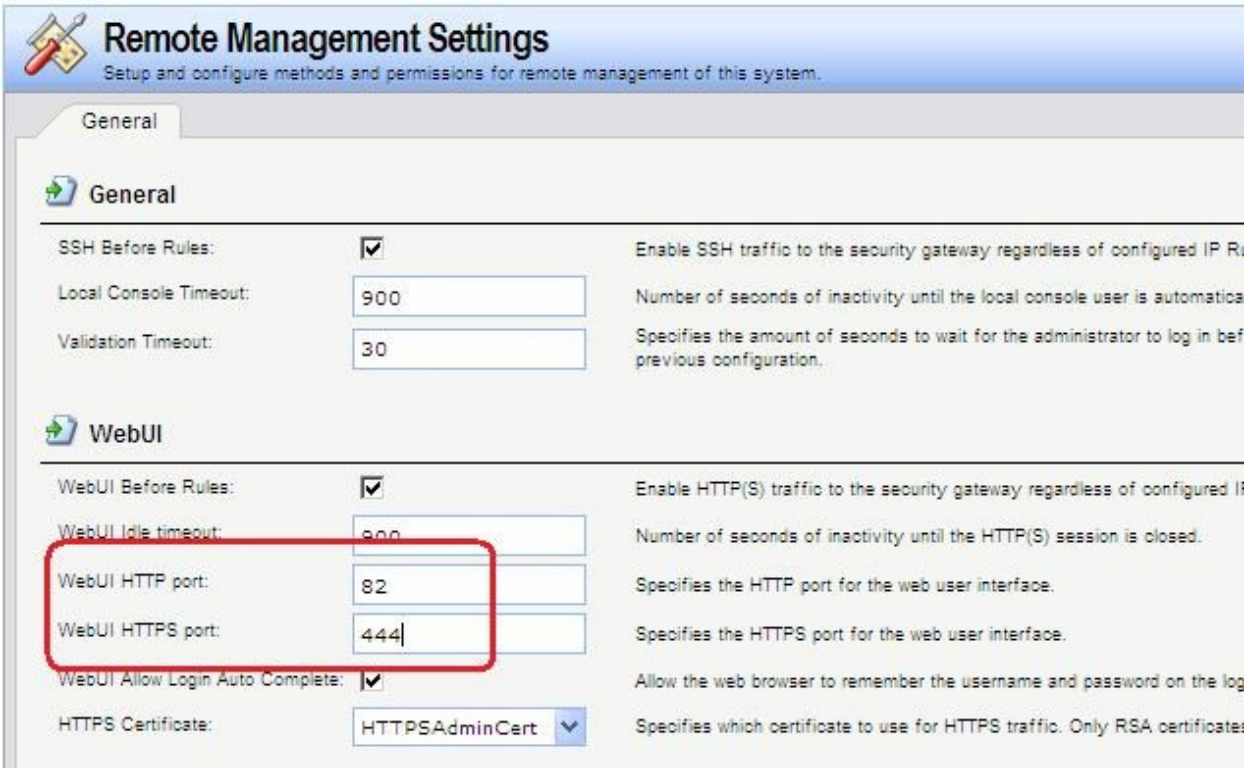
Метод pinholing некоторые производители называют SAT.

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:

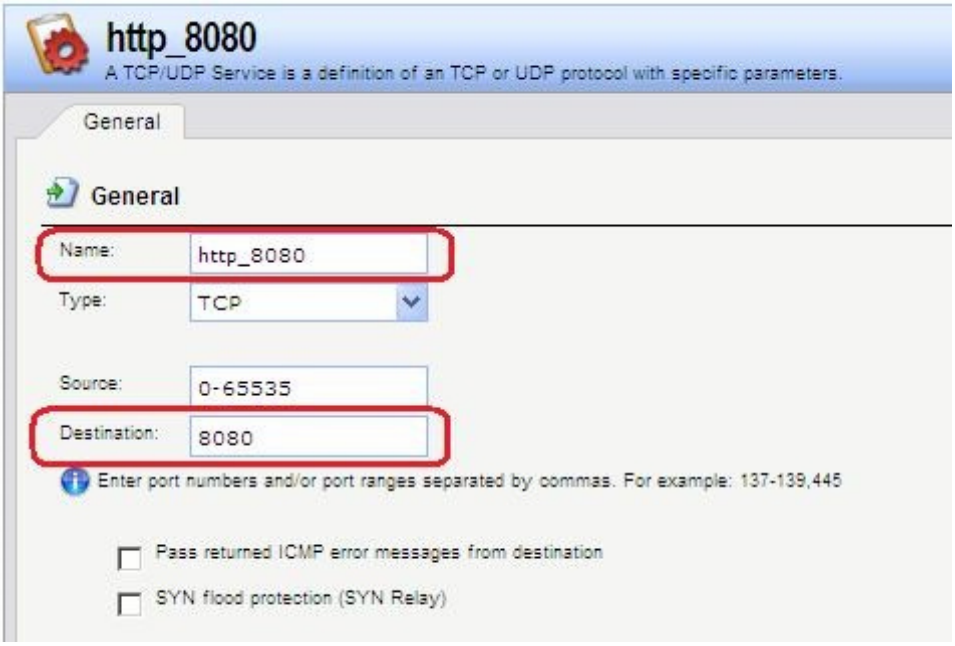
set Settings RemoteMgmtSettings WWWSrv_HTTPPort=82 WWWSrv_HTTPSPort=444

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



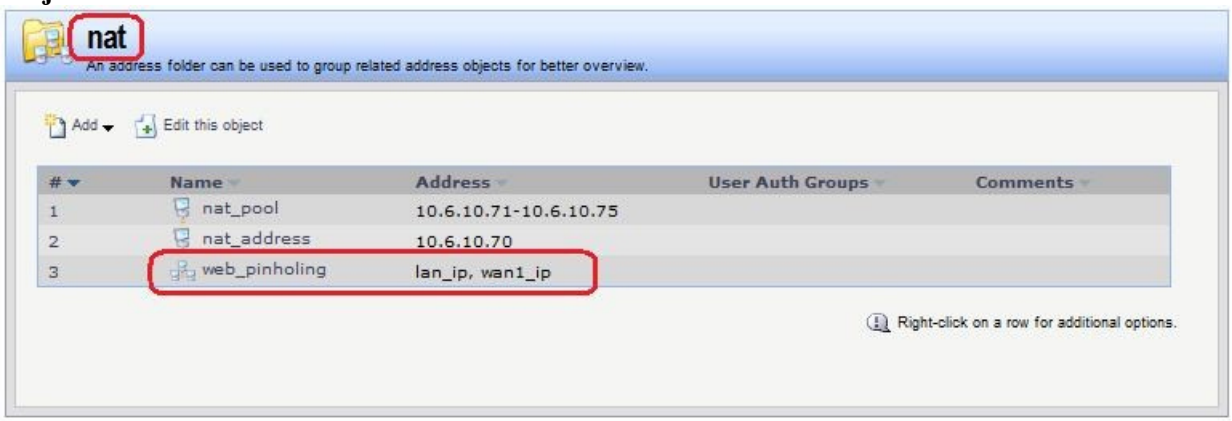
Командная строка: add Service ServiceTCPUDP http_8080 DestinationPorts=8080 SourcePorts=0-65535

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

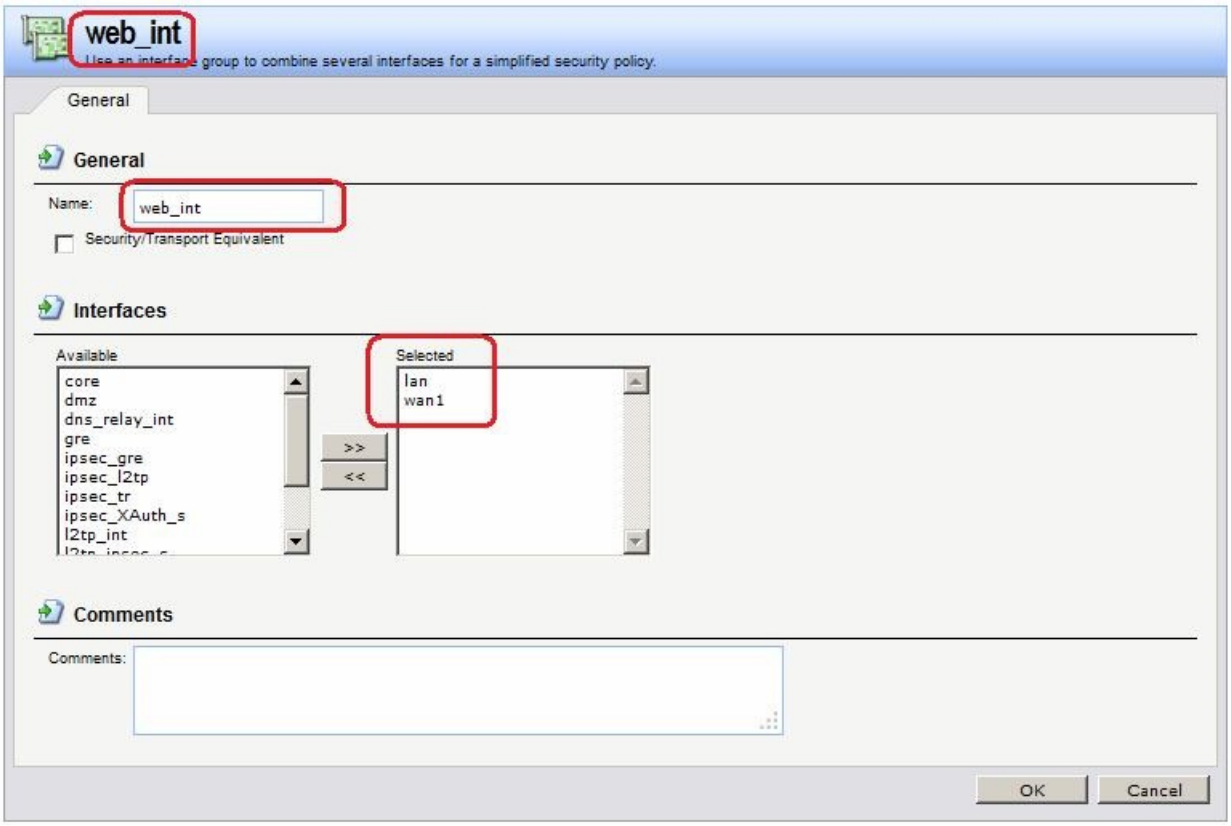


Командная строка: cc Address
AddressFolder nat
add IP4Group web_pinholing Members =lan/lan_ip, wan1/wan1_ip

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 вебсервера. В нашем случае это группа интерфейсов web_int.

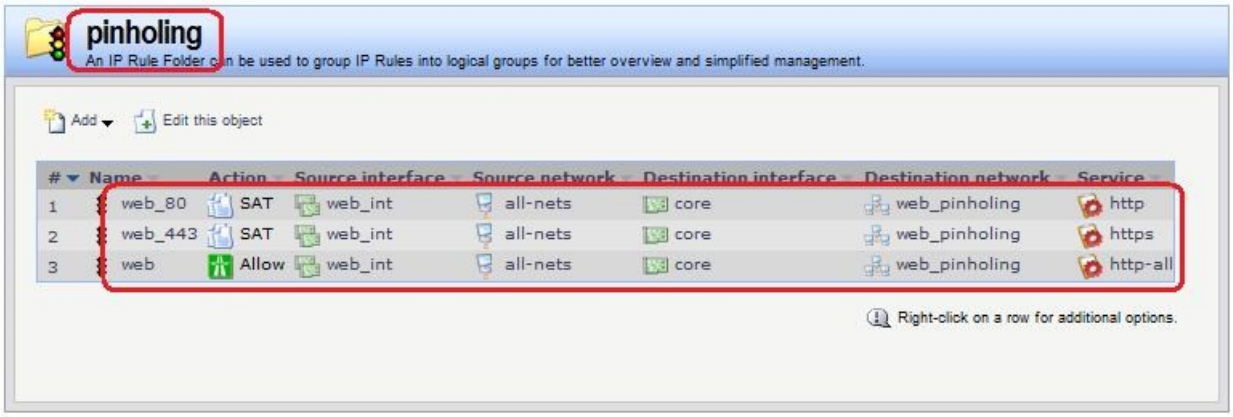
Создать правило фильтрования с действием **Allow**.

Веб-интерфейс:

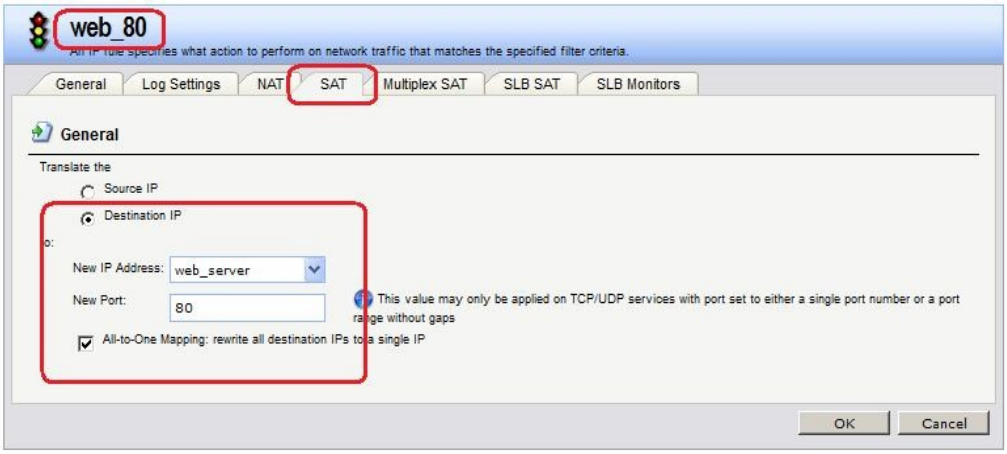
Rules □ IP Rules □ Add □ IP Rule Folder

Name: pinholing

Rules □ IP Rules □ pinholing □ Add



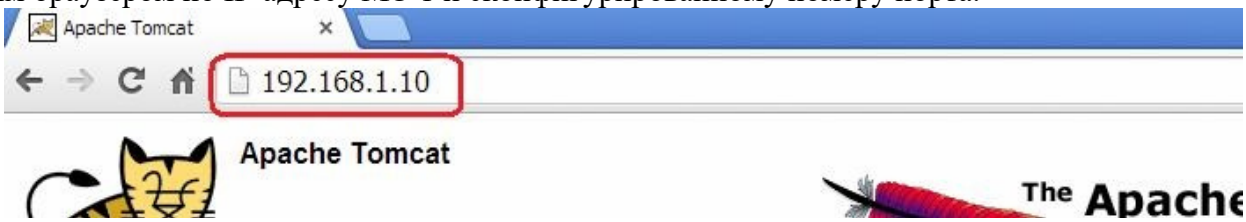
На вкладке **SAT** указать адрес веб-сервера и порт, который он слушает. Если необходимо, чтобы веб-сервер слушал несколько портов, например, 80 (http) и 443 (https), то требуется два правила **SAT**.



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=httpall Name=web

Проверка конфигурации

Заходим браузером по IP-адресу МЭ 1 и сконфигурированному номеру порта.



ПЗ № 23

Использование шлюза прикладного уровня (ALG) для активизация антивирусного сканирования

1. **Реакция на невозможность выполнения проверки на наличие вирусов**

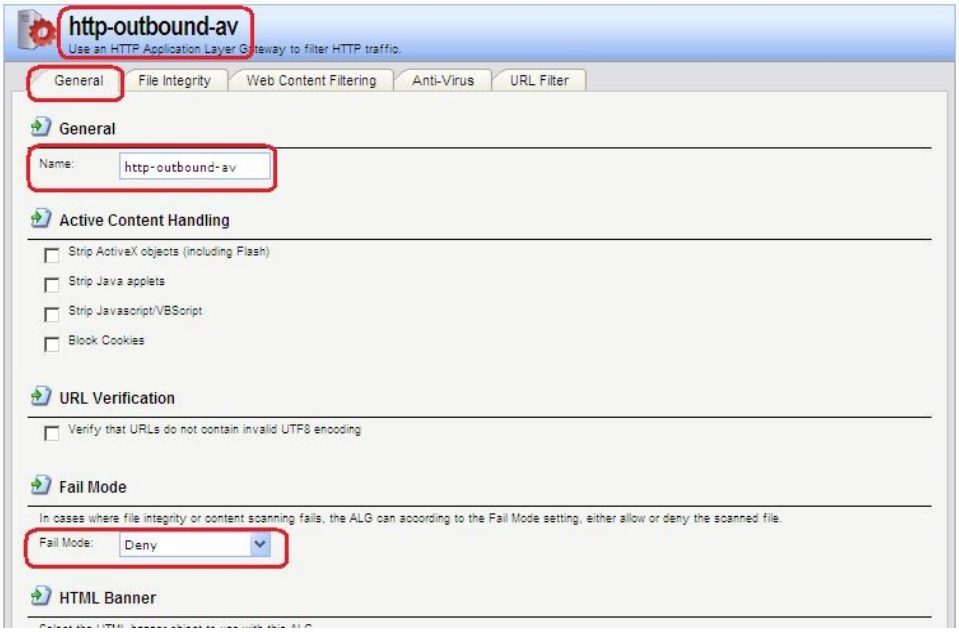
Антивирус NetDefendOS активизируется с помощью шлюза прикладного уровня (ALG), который связан с соответствующим протоколом. Активизация доступна для загружаемых файлов, связанных со следующими ALG и включается непосредственно в самом ALG:

- **HTTP ALG**
- **FTP ALG**
- **POP3 ALG**
- **SMTP ALG**

Если по какой-либо по причине не удается выполнить проверку на наличие вирусов, то при режиме **Deny** дальнейшая передача данных прекращается, при этом данное событие регистрируется в логах. Если установлен режим **Allow**, то ситуация, когда антивирусные базы не доступны или текущая лицензия не действительна, не приведет к запрещению пересылки. В этом случае пересылка файлов будет разрешена, и будет сгенерировано сообщение в логах, указывающее на то, что произошел сбой.

Веб-интерфейс:

Object □ ALG with AV/WCF □ Add □ HTTP ALG



2. **Режим сканирования**

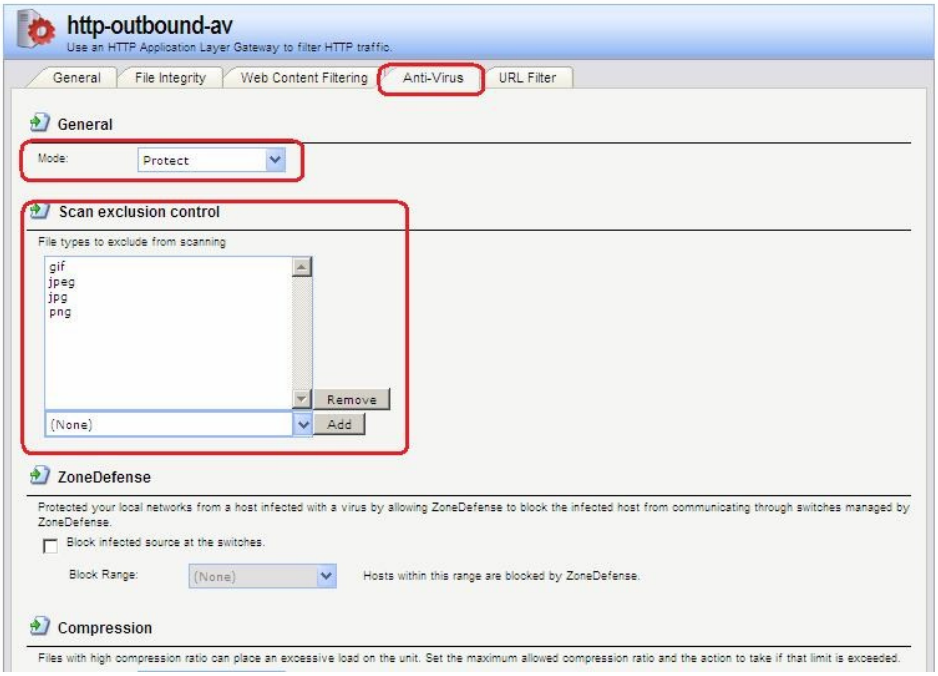
Режим сканирования может быть следующим:

- **Disabled** – Функция Антивирус выключена.
- **Audit** – Сканирование активизировано, но единственным действием является ведение логов.
- **Protect** – Функция Антивируса активизирована. Подозрительные файлы будут удалены, информация об этом будет записана в логи.

3. **Исключение из сканирования**

При необходимости можно явно отменить сканирование файлов с определенным расширением. Данное действие может увеличить общую пропускную способность, если загрузка файлов с данным расширением часто используется в каком-либо протоколе, например, HTTP.

NetDefendOS выполняет проверку всех MIME-расширений файлов, чтобы установить, что расширение файла корректно и затем посмотреть, не находится ли это расширение в списке исключенных.



4. Ограничение степени сжатия

При сканировании сжатых файлов файл сначала распаковывается. В некоторых случаях распакованный файл намного больше сжатого. Это означает, что сравнительно небольшое вложение сжатого файла может значительно израсходовать ресурсы межсетевого экрана и заметно снизить пропускную способность.

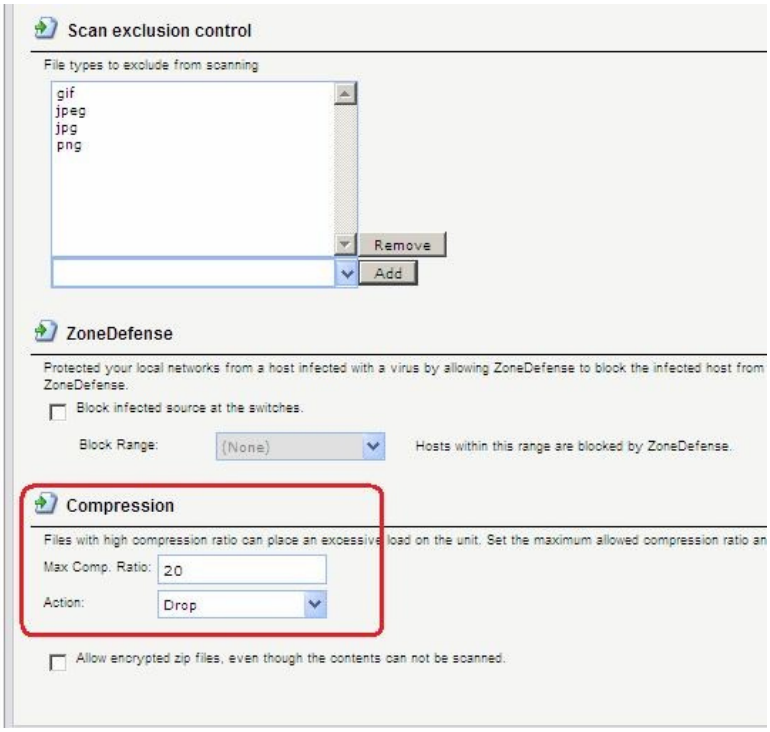
Для предотвращения подобной ситуации, следует указать предел степени сжатия (**Compression Ratio**). Если предел степени сжатия указан 20, то это будет означать, что, если несжатый файл в 20 раз больше, чем сжатый, то следует выполнить одно из следующих действий:

Allow – Разрешить передачу файла без проверки на наличие вирусов

Scan – Сканировать файл на наличие вирусов

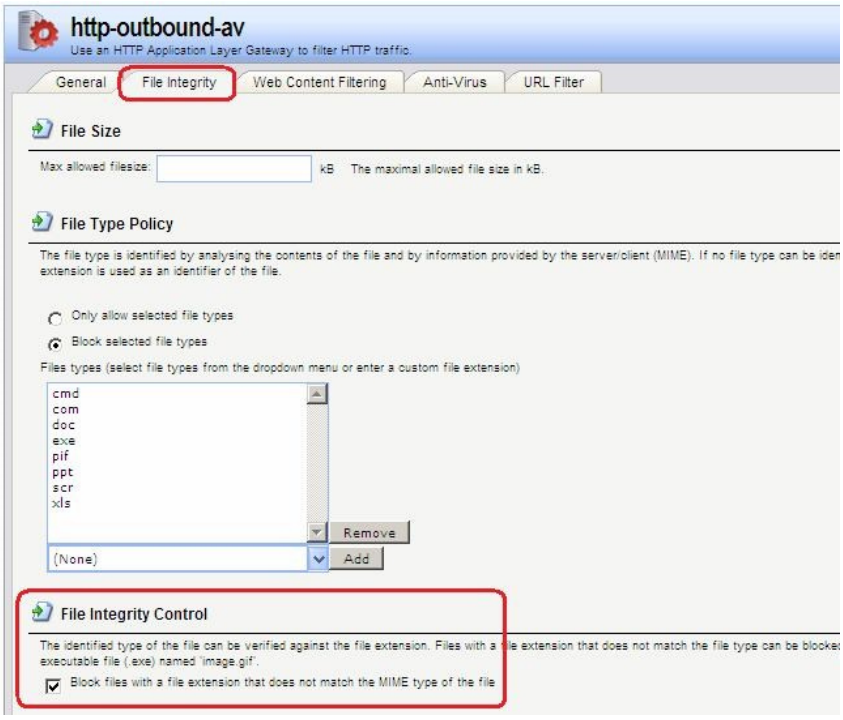
Drop – Отбросить файл

В любом случае данное событие заносится в логи.

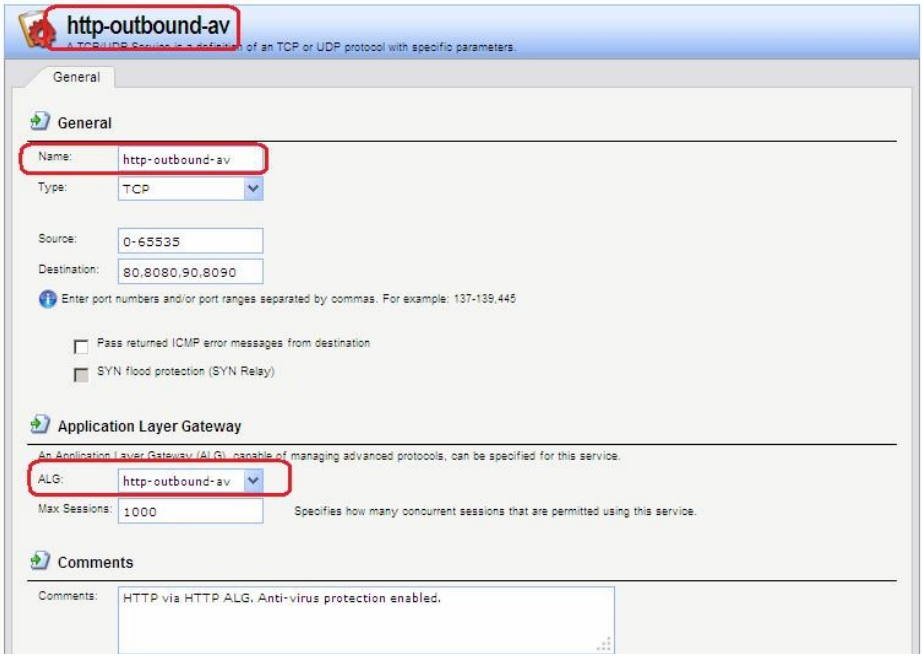


5. Проверка файлов на соответствие типам MIME

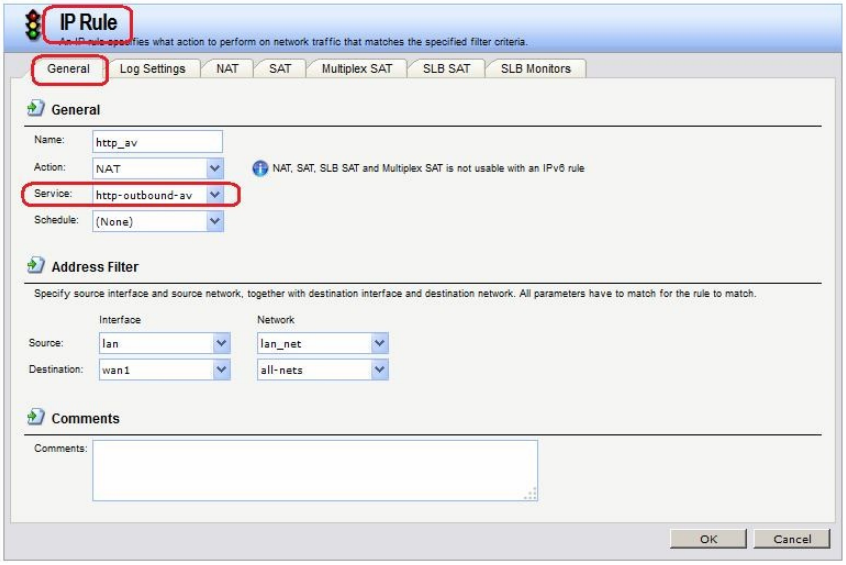
Параметр ALG **File Integrity** могут быть использован совместно с антивирусным сканированием для того, чтобы проверить, соответствует ли содержание файла типу MIME.
MIME-тип определяет тип файла. Например, файл может быть определен как **.gif** и, следовательно, должен содержать данные этого типа. Некоторые вирусы могут пытаться скрыться внутри файлов, используя ложное расширение. Файл может быть указан как **.gif**, но содержимое файла не будет соответствовать данным этого типа, так как он заражен вирусом.
Включение этой функции рекомендуется для того, чтобы предотвратить прохождение вируса.



Командная строка: set ALG ALG_HTTP http-outbound-av Antivirus=Protect
Создание сервиса с ALG с установленной антивирусной защитой **Веб-интерфейс: Object □ Services □ Add □ TCP/UDP Services**



Командная строка:
add Service ServiceTCPUDP http-outbound-av DestinationPorts=80,8080,90.8090 SourcePorts=0-65535 ALG=http-outbound-av
Определение правила фильтрования с созданным сервисом **Веб-интерфейс:**
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=http-outboundav Name=http_av

Лабораторная работа 9. 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 HTTPсоединения 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 FTPсервера 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.

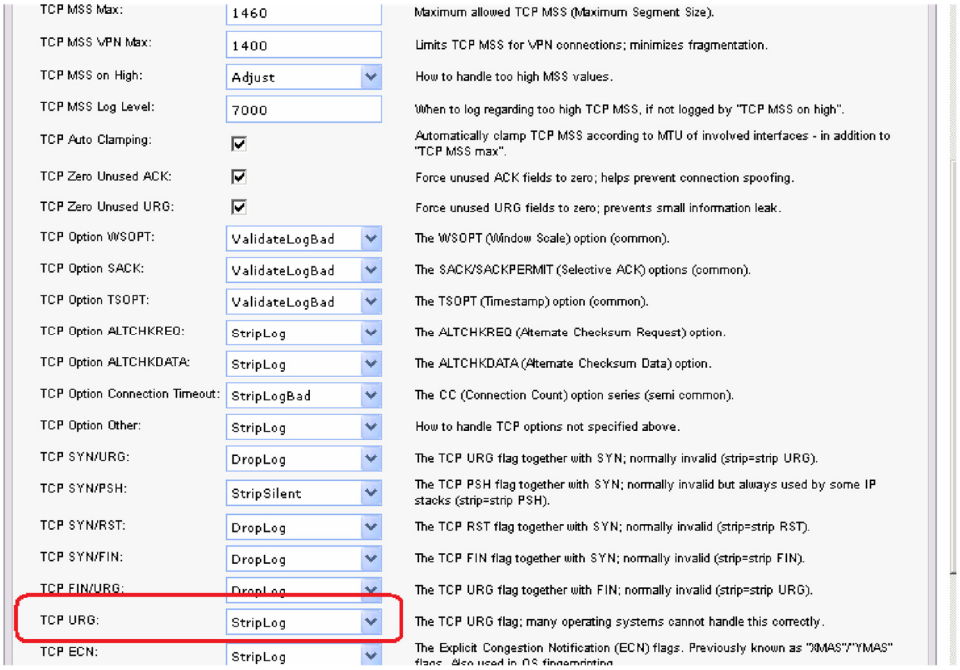
Атаки Land и LaTierra регистрируются в логах NetDefendOS как отброшенные пакеты с указанием на правило по умолчанию **AutoAccess**, или, если определены другие правила доступа, указано правило правило доступа, в результате которого отброшен пакет. В данном случае IP-адрес отправителя не представляет интереса, так как он совпадает с IPадресом 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-ofband».

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 сеtb 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.

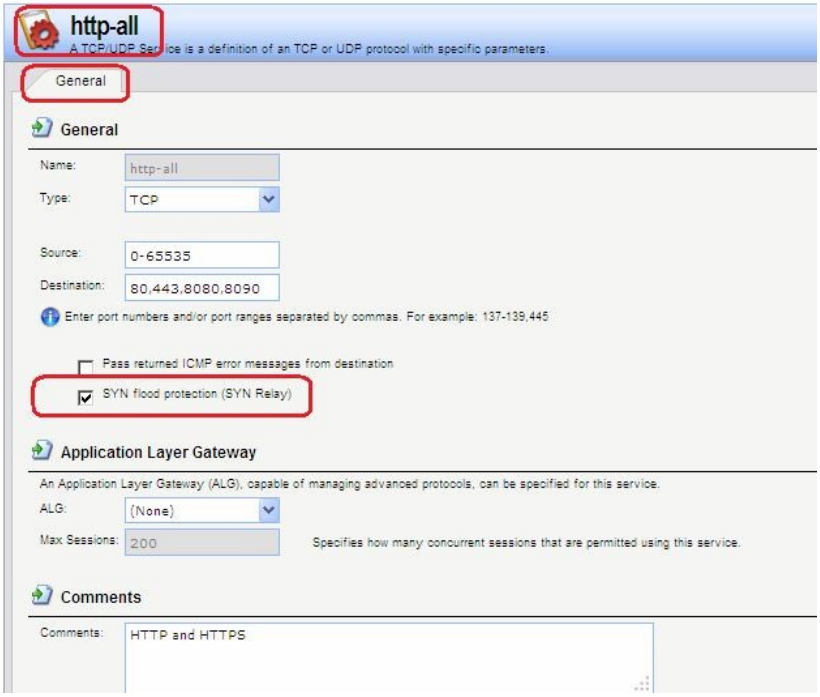
- Типы flood-атак Smurf и Papasmurf на стороне жертвы выглядят как ответы ICMP **Echo Response**. Если не используются правила **FwdFast**, таким пакетам не будет разрешено инициировать новые соединения независимо от того, существуют ли правила, разрешающие прохождение пакетов.
- Пакеты Fraggle могут 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)

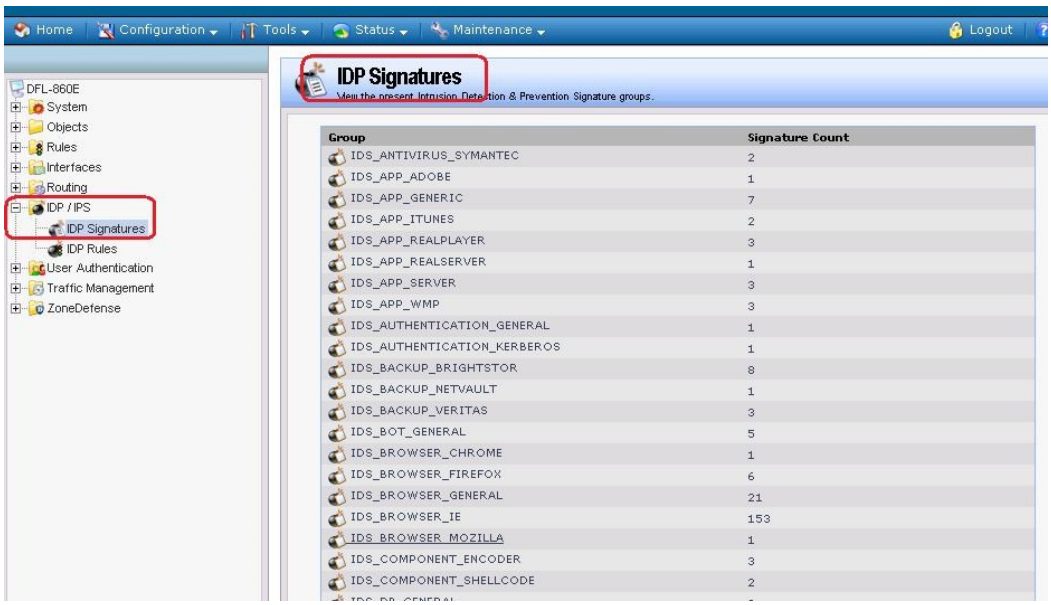
Наиболее сложной DoS-атакой является атака *Distributed Denial of Service*. Хакеры используют сотни или тысячи компьютеров по всей сети интернет, устанавливая на них программное обеспечение для выполнения DDoS-атак и управляя всеми этими компьютерами для осуществления скоординированных атак на сайты 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.

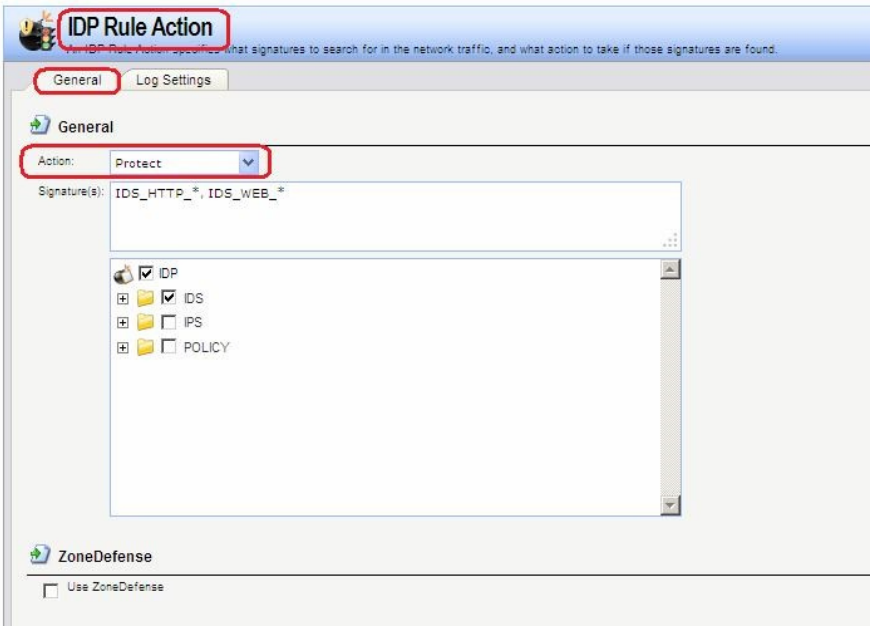
Веб-интерфейс:

IDP / IPS □ IDP Rules □Add □ IDP Rule

Действия IDP

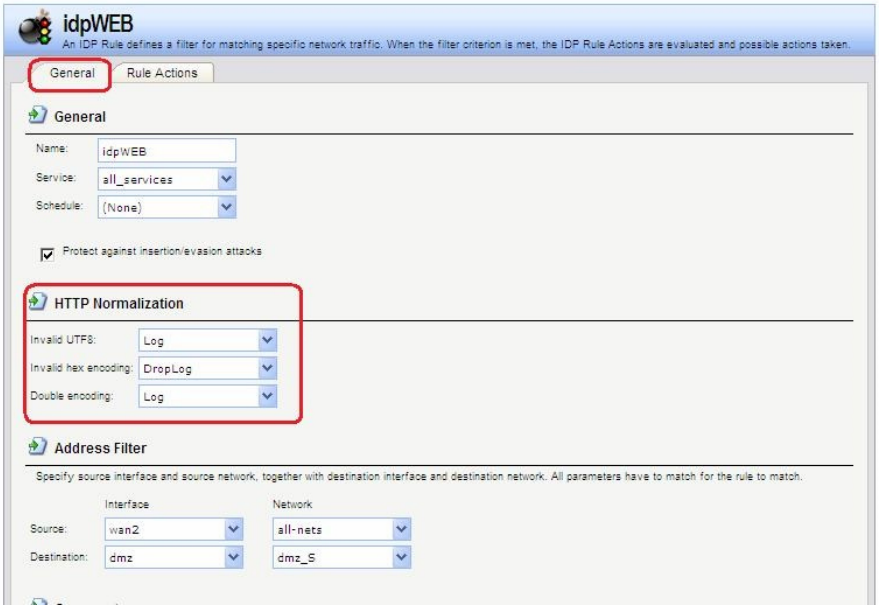
При выявлении вторжения будет выполнено действие, указанное в правиле IDP. Может быть указано одно из трех действий:

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

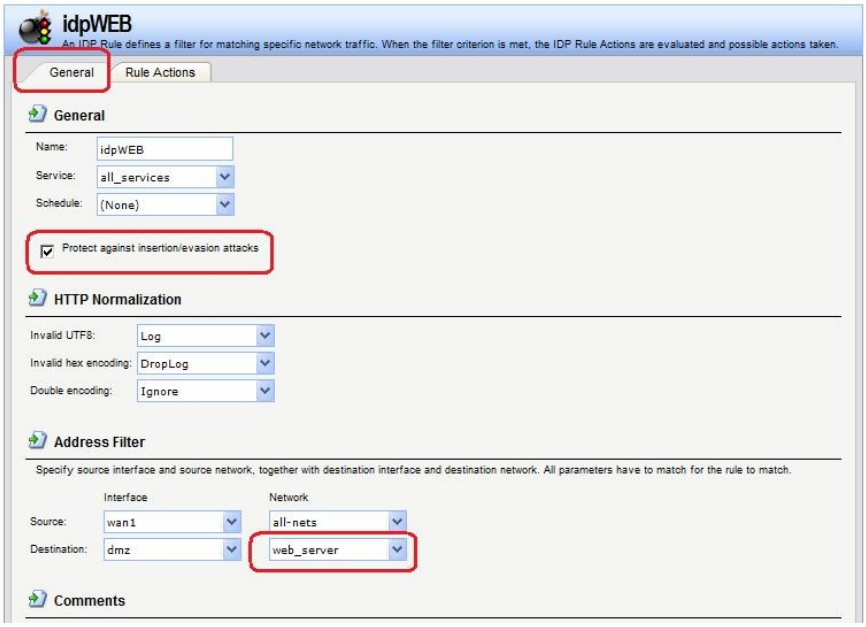
злоумышленника состоит в том, чтобы отправить два фрагмента **p2'** и **p3'** системе IDP и два других фрагмента **p2** и **p3** приложению. В результате получаются различные потоки данных, который получены системой IDP и приложением.

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:

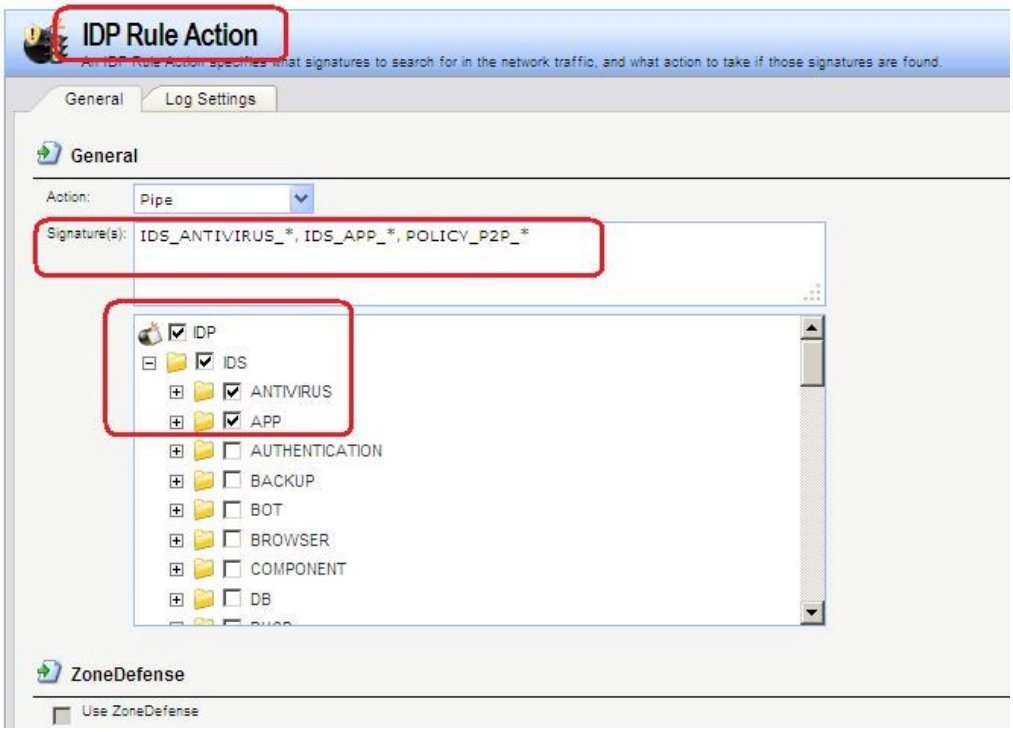
- Сообщение **Attack Detected**, указывающее на то, что атака была обнаружена и предотвращена.
- Сообщение **Unable to Detect,** уведомляющее о том, что система NetDefendOS не смогла выявить возможную атаку при сборке потока TCP/IP, хотя подобная атака могла присутствовать. Эта ситуация возможна при 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:

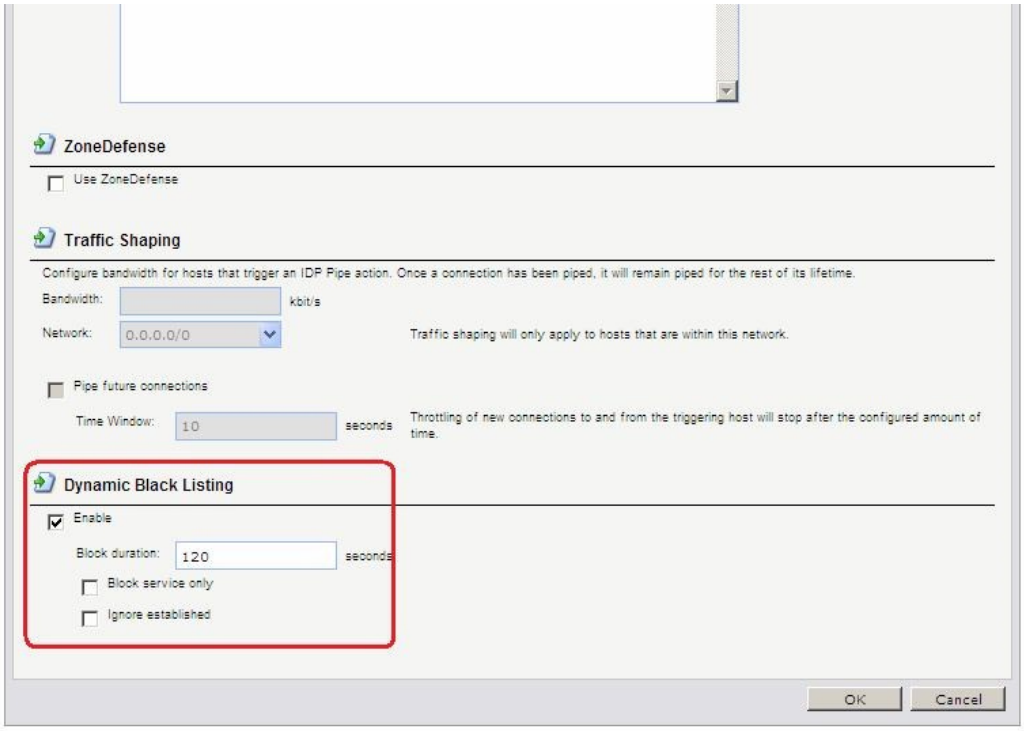
Использование подстановки символов (Wildcarding) в сигнатурах IDP

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 in Seconds Хост или сеть, которые являются источником трафика, 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**.

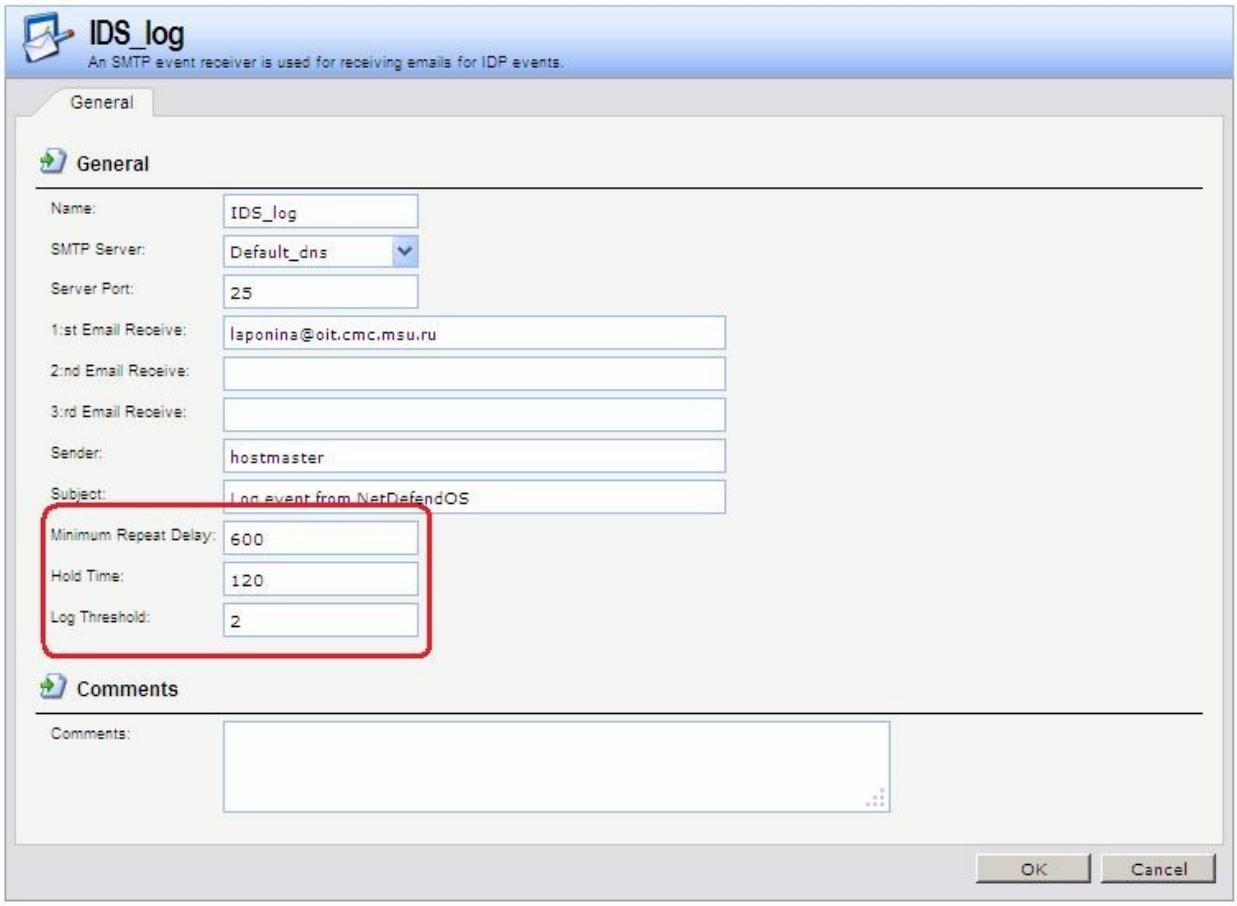
Командная строка:

add IDPRule Service=http-all SourceInterface=wan2 SourceNetwork=all-nets DestinationInterface=dmz DestinationNetwork=dmz/dmz_net Name=idpWEB

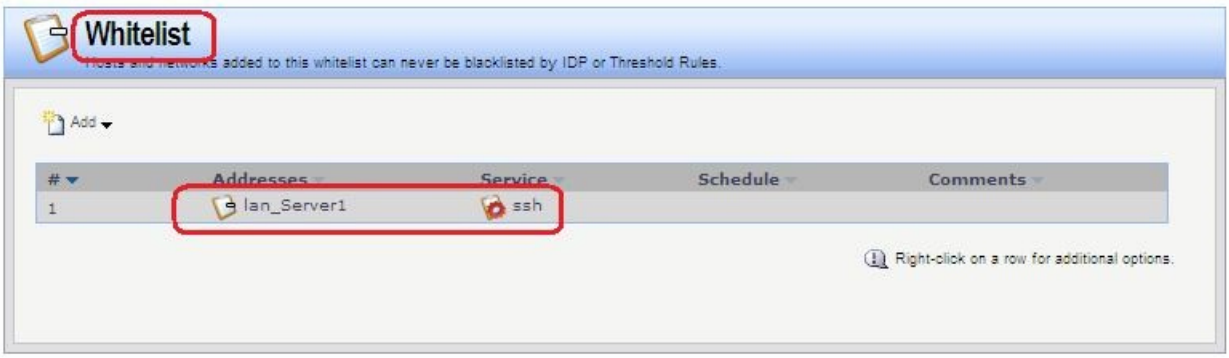
Получение по e-mail сообщений о событиях IDP

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 SMTPсервера, 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

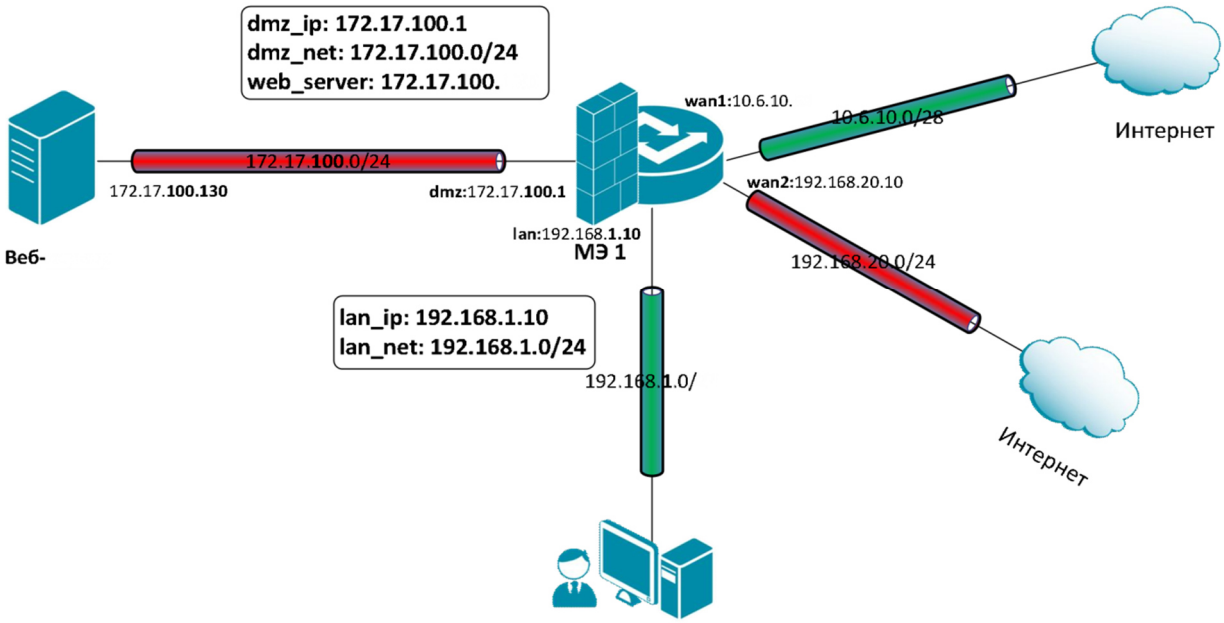


Командная строка: add BlacklistWhiteHost Addresses=lan/lan_Server1 Service=ssh

ПЗ № 24

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.

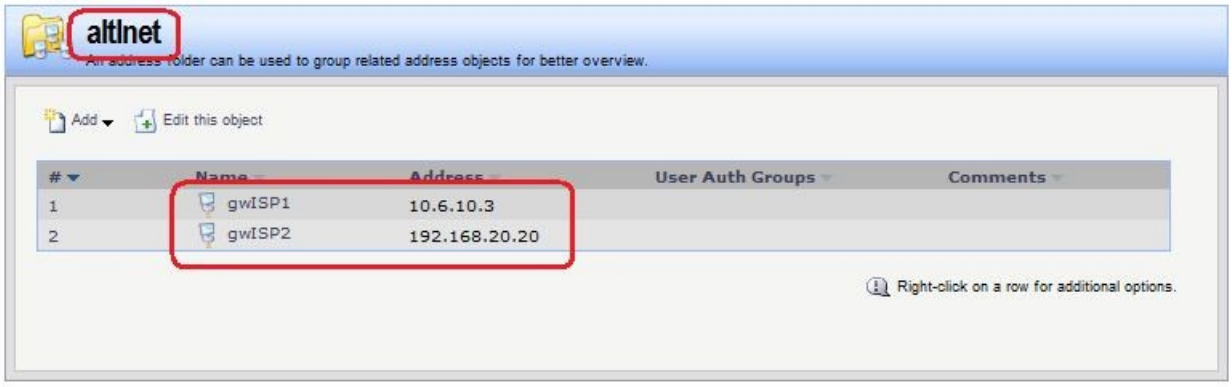
Описание практической работы

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 интернетпровайдеров.



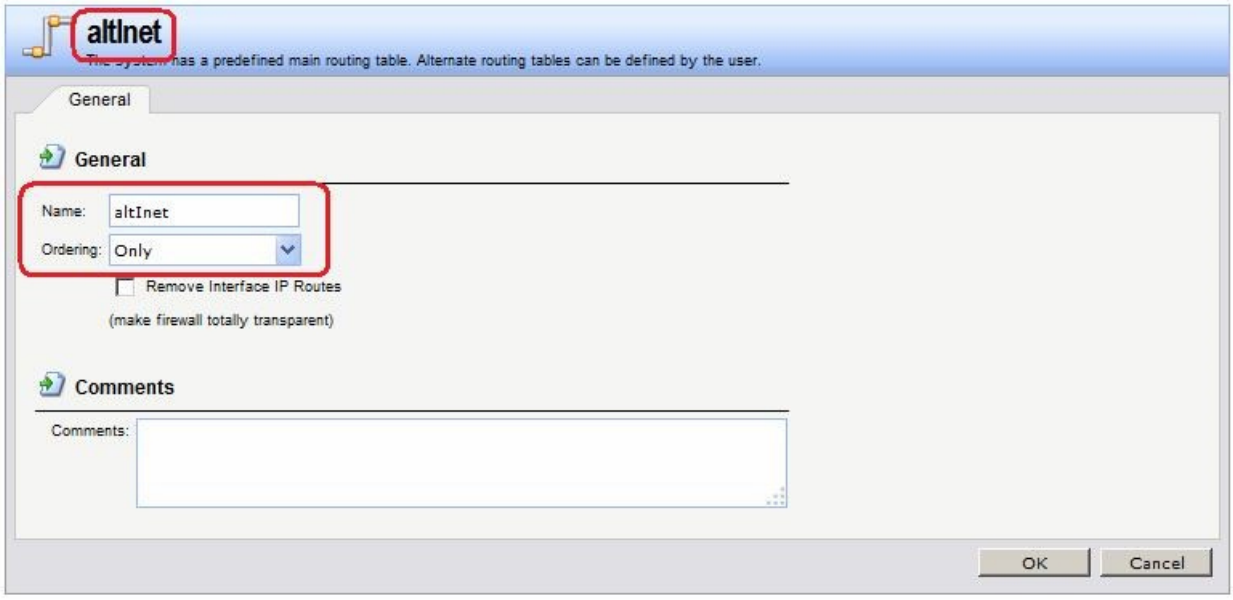
Альтернативная таблица маршрутизации Создать альтернативную таблицу маршрутизации.

Веб-интерфейс:

Routing □ Routing Tables □ Add □ Routing Table

Name: altInet

Ordering: Only

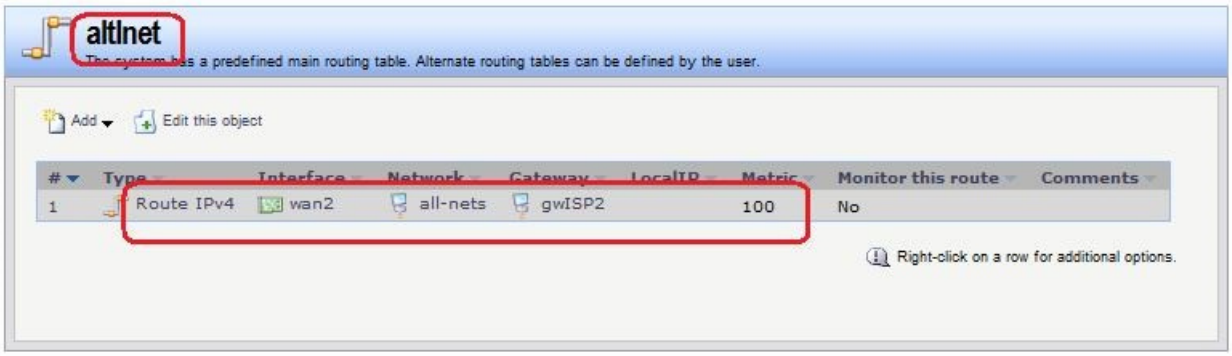


Командная строка: add RoutingTable altInet Ordering=Only

В созданной таблице создать маршрут по умолчанию к ISP2 через интерфейс **wan2**.

Веб-интерфейс:

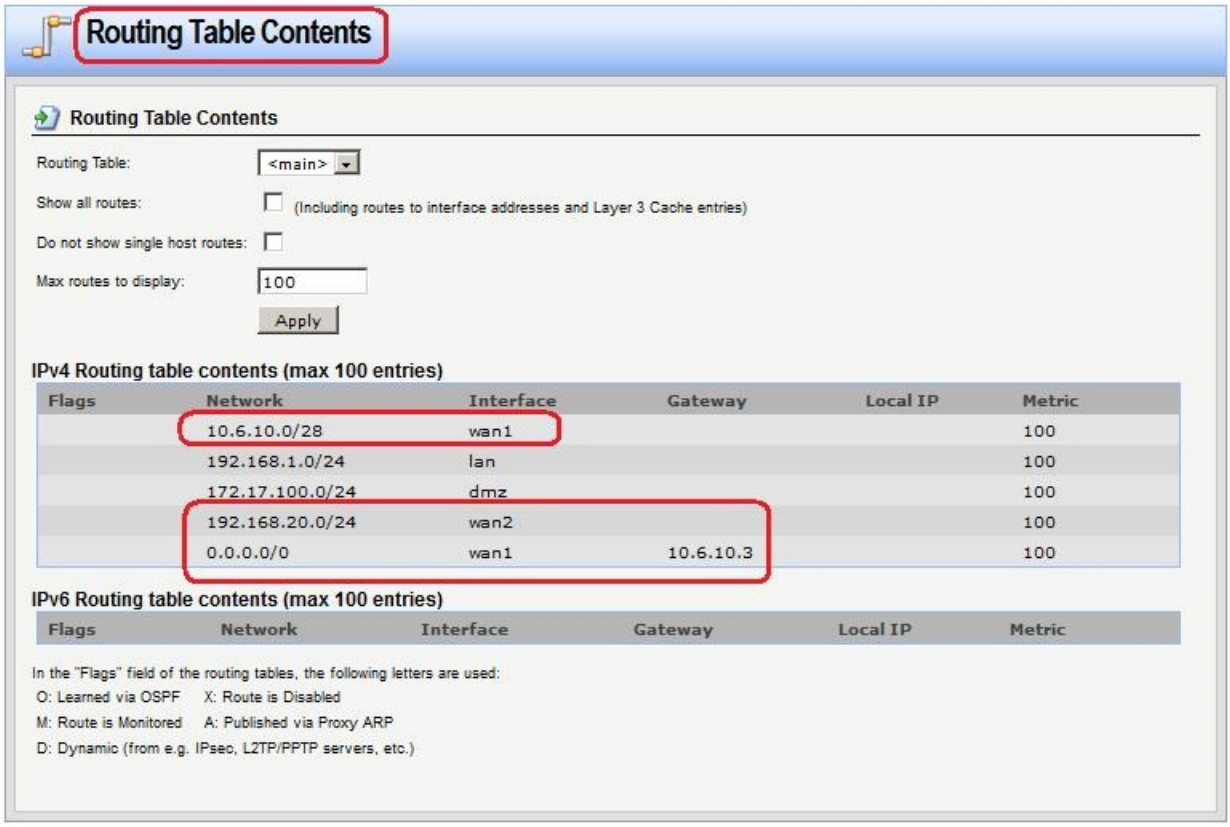
Routing □ Routing Tables □ altInet □ Add



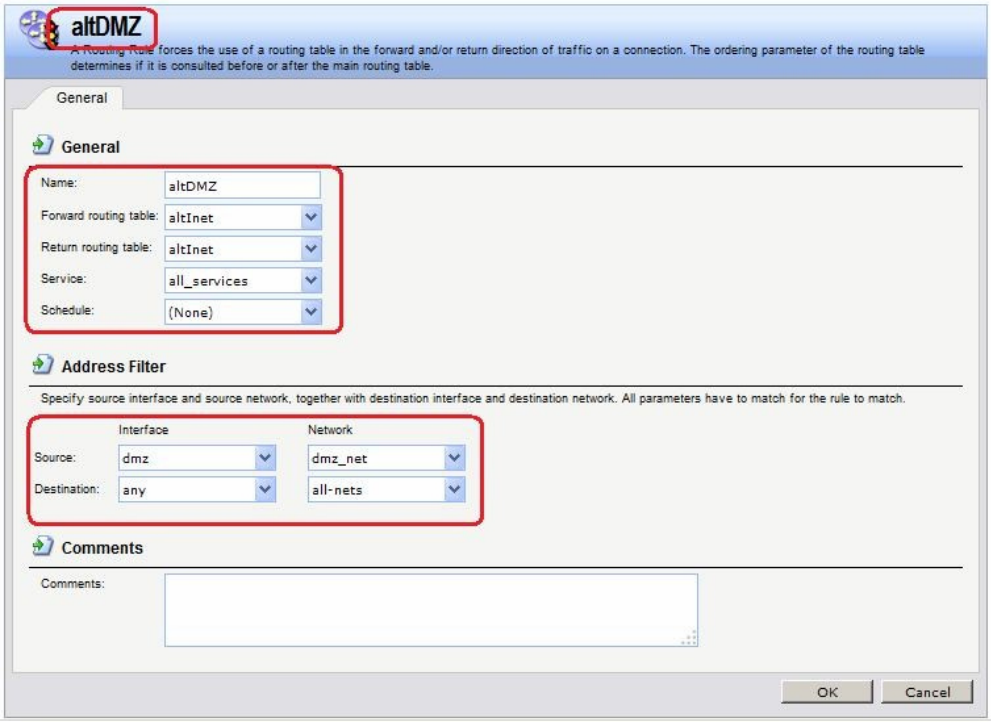
Командная строка: cc RoutingTable altInet add Route Interface=wan2 Network=all-nets Gateway=altInet/gwISP2 Metric=100

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:

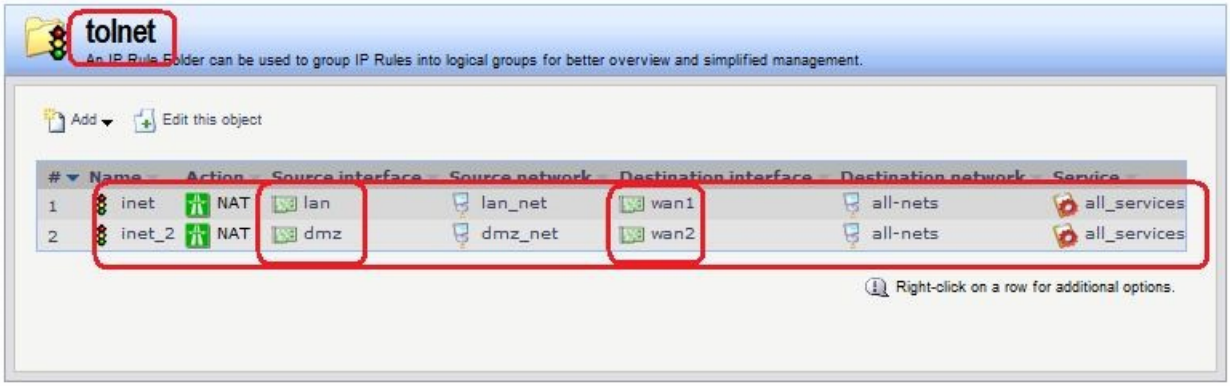
add RoutingRule ForwardRoutingTable=altDMZ ReturnRoutingTable=altDMZ SourceInterface=dmz SourceNetwork= dmz/dmz_net DestinationInterface=any DestinationNetwork=all-nets Service=all_services Name=altDMZ

Правила фильтрования **Веб-интерфейс:**

Rules □ IP Rules □ Add □ IP Rule Folder

Name: toInet

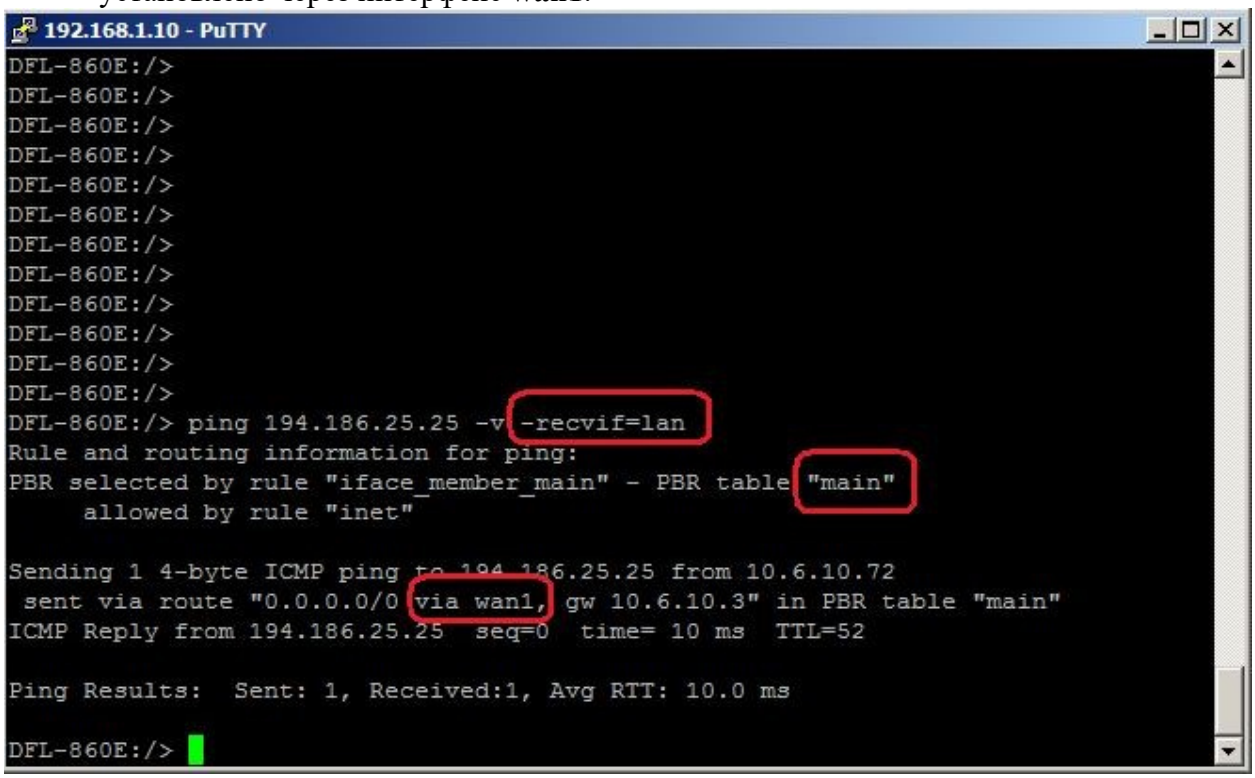
Rules □ IP Rules □ toInet □ Add □ IP Rule



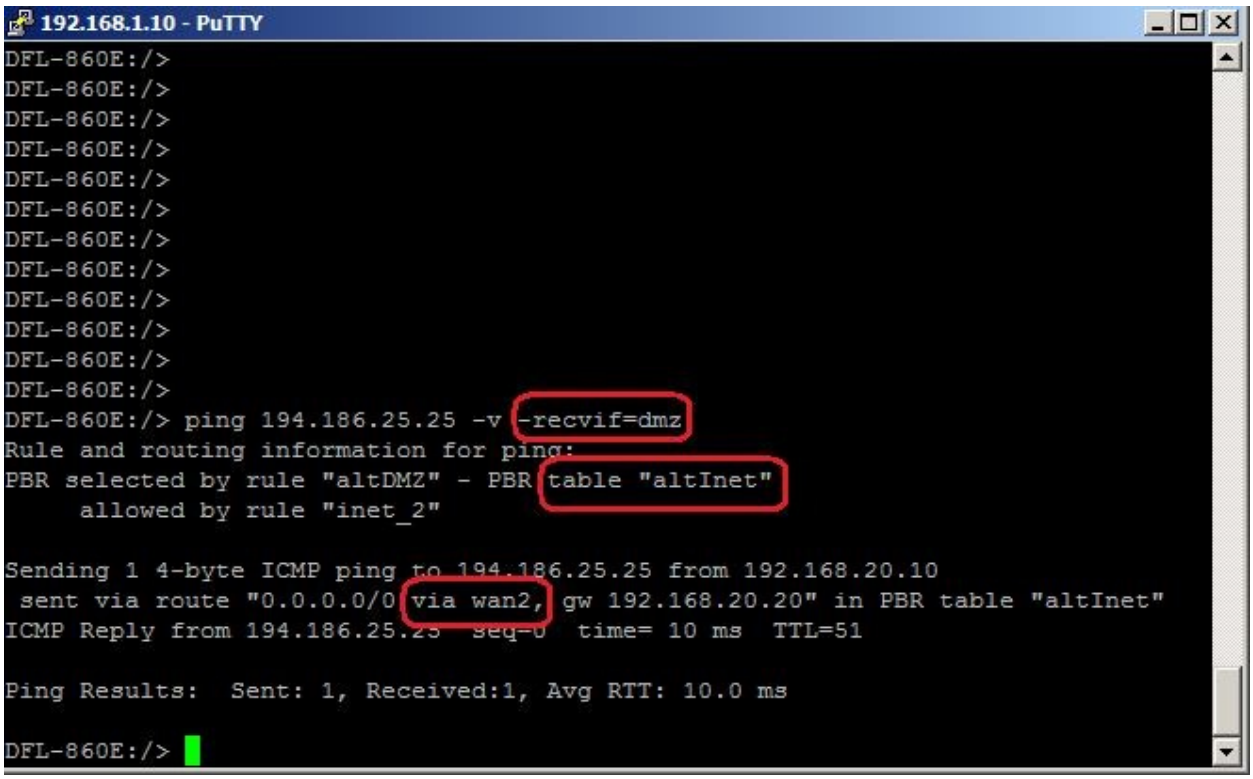
Командная строка: add IPRuleFolder Name=toInet cc IPRuleFolder <N folder>
add IPRule Action=NAT SourceInterface=lan SourceNetwork= lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services Name=inet
add IPRule Action=NAT SourceInterface=dmz SourceNetwork=dmz/dmz_net
DestinationInterface=wan2 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**.



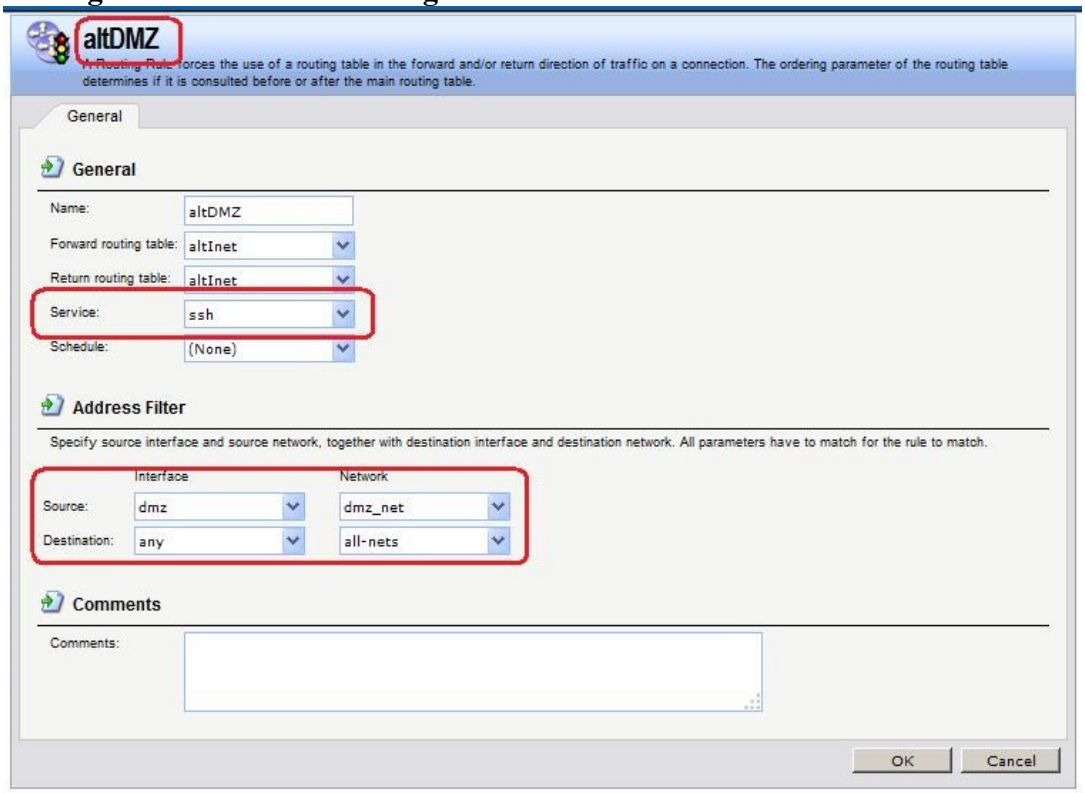
Маршрутизация на основе сервиса

Альтернативная таблица маршрутизации

Альтернативная таблица маршрутизации создается аналогично маршрутизации на основе адреса источника.

Правило выбора таблицы маршрутизации PBR **Веб-интерфейс:**

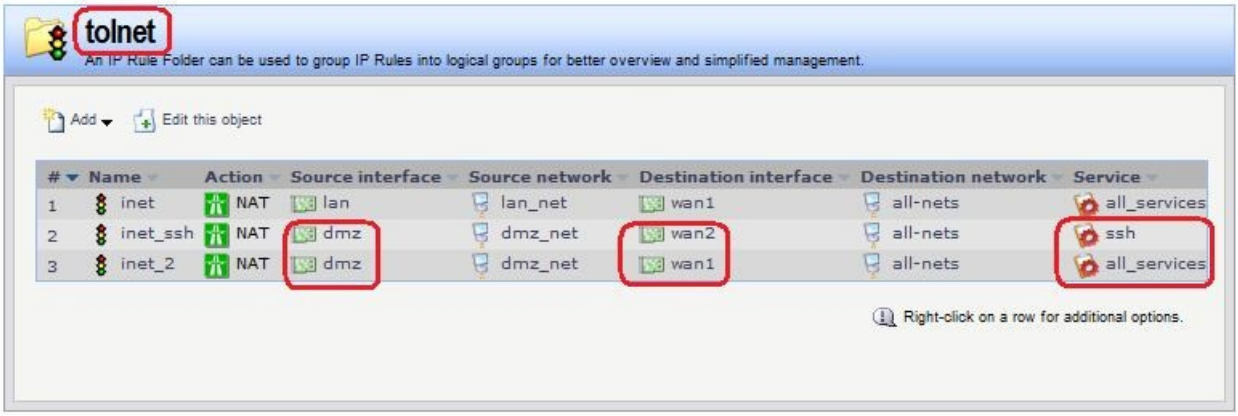
Routing □ Routing Rules □ Add □ Routing Rule



Командная строка:

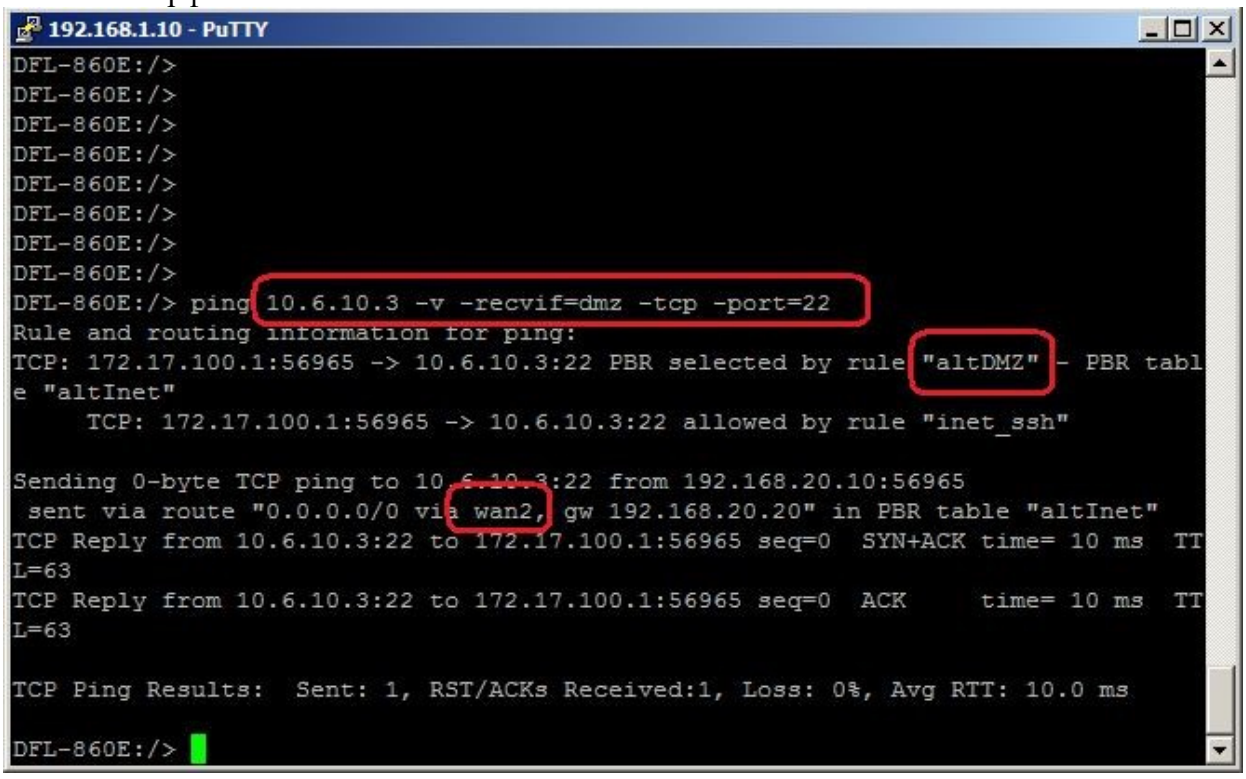
add RoutingRule ForwardRoutingTable=altInet ReturnRoutingTable=altInet SourceInterface=dmz SourceNetwork=dmz/dmz_net DestinationInterface=any DestinationNetwork=all-nets Service=ssh Name=altDMZ

Правила фильтрования **Веб-интерфейс:**
Rules □ IP Rules □ Add □ IP Rule Folder
Name: toInet
Rules □ IP Rules □ toInet □ Add □ IP Rule

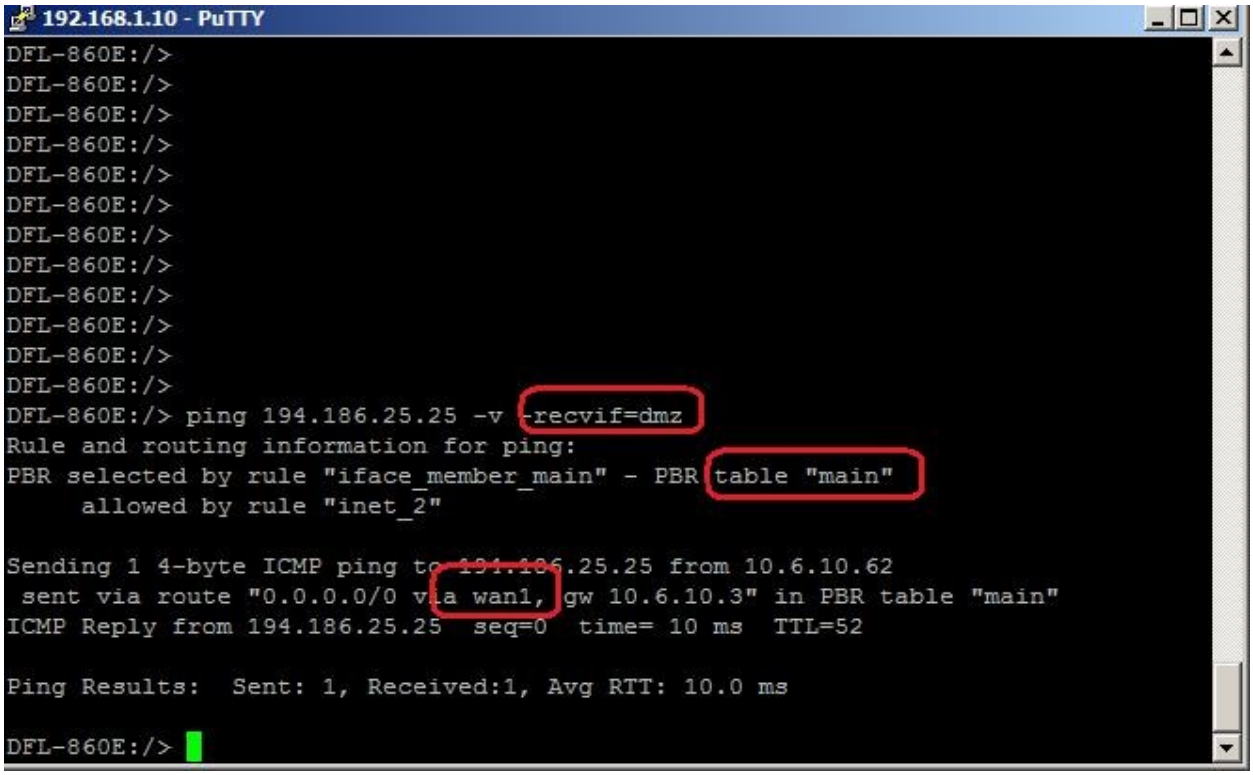


Командная строка: add
IPRuleFolder Name=toInet cc
IPRuleFolder <N folder>
add IPRule Action=NAT SourceInterface=lan SourceNetwork= lan/lan_net DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services Name=inet
add IPRule Action=NAT SourceInterface=dmz SourceNetwork= dmz/dmz_net DestinationInterface=wan2 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 dmzинтерфейса.



Лабораторная работа 11. Выполняем выход в интернет по протоколу ICMP с dmzинтерфейса.



2.2. Тестовые задания (ТЗ)

ТЗ № 1

Задание # 1

Вопрос:

Составление списка объектов, которые будут подлежать защите, и субъектов, которые задействованы в данном информационном пространстве, и будут влиять на информационную защиту системы, - это ...

Запишите ответ:

_____

Задание # 2

Вопрос:

... - злоумышленник, использующий в собственных интересах уязвимости в телефонных системах.

Выберите один из 5 вариантов ответа:

1) Хакер
2) Кракер
3) Фрикер
4) Джокер
5) Анонимайзер

Задание # 3

Вопрос:

... - это набор мероприятий по сбору сведений об информационной системе, напрямую не связанный с техническими подробностями реализации системы, основанный на человеческом факторе.

Запишите ответ:

_____

Задание # 4

Вопрос:

... в аппаратном обеспечении -это устройство, которое выполняет некоторые недокументированные функции, обычно в ущерб пользователю данной информационной системы.

Запишите ответ:

_____

Задание # 5

Вопрос:

... - это устройство, хранящее некий уникальный параметр, на основе которого выдается корректный ответ на запрос системы об аутентификации.

Выберите один из 4 вариантов ответа:

1) Токен
2) Пароль
3) Биометрические параметры
4) Мастер-ключ

Задание # 6

Вопрос:

Аутентификация основывается на одном из следующих параметров или их комбинации:

Выберите несколько из 4 вариантов ответа:

1) Токен
2) Пароль
3) Биометрические параметры
4) Мастер-ключ

Задание # 7

Вопрос:

Выполнение пользователем, получившим дюступ в систему, различных несанкционированных действий, называется атакой на ...

Запишите ответ:

_____

Задание # 8

Вопрос:

... - это программа, перехватывающая пакеты, поступающие к данной станции, в том числе и те, котрое станция при нормальной работе должна проигнорировать.

Запишите ответ:

_____

Задание # 9

Вопрос:

Какие из атак являются удаленнами атаками.

Выберите несколько из 5 вариантов ответа:
1) Вирусы и троянские программы
2) Отказ в обслуживании
3) Маскировка
4) Атаки на средства аутентификации
5) Перехват сессии

Задание # 10
Вопрос:
Какие из атак являются локальными атаками.

Выберите несколько из 5 вариантов ответа:
1) Вирусы и троянские программы
2) Социальная инженериерия
3) Маскировка
4) Атаки на средства аутентификации
5) Перехват сессии

Задание # 11
Вопрос:
Какие из атак являются атаками на поток данных.

Выберите несколько из 5 вариантов ответа:
1) Атака повтором
2) Социальная инженериерия
3) Маскировка
4) Прослушивание сетей
5) Перехват сессии

Задание # 12
Вопрос:
Какие из атак являются удаленнами атаками.

Выберите несколько из 5 вариантов ответа:
1) Закладки в аппаратном обеспечении
2) Переполнение буфера
3) Атака потоком Syn запросов
4) Атаки на средства аутентификации
5) Перехват сессии

Задание # 13
Вопрос:
Какие из атак являются локальными атаками.

Выберите несколько из 5 вариантов ответа:
1) Атаки класса "повышение привелегий"
2) Закладки в аппаратном обеспечении
3) Маскировка
4) Атака на маршрутизацию
5) Перехват сессии

Задание # 14
Вопрос:
Маскировка по другим название это ...

Выберите один из 5 вариантов ответа:
1) spoofing
2) sharing
3) sniffer
4) ids
5) firewall

Задание # 15
Вопрос:
... - программа, перехватывающая пакеты, поступающие к данной станции, в том числе и те, которые станция при нормальной работе должна проигнорировать.

Выберите один из 5 вариантов ответа:
1) Sniffer
2) Программа повышения прав
3) Spoofing
4) Sharing
5) Ids

Задание # 16
Вопрос:
Системы обнаружения атак другими словами это ...

Выберите один из 5 вариантов ответа:
1) Sniffer
2) Программа повышения прав
3) Spoofing
4) Sharing
5) Ids

Задание # 17
Вопрос:
... позволяют провести анализ и пошаговое выполнение программного обеспечения с тем, чтобы понять его внутреннюю логику и уязвимость или вызвать в его работе сбой с предсказуемым результатом, либо изменить ход работы программы в свою пользу.

Выберите один из 5 вариантов ответа:
1) Дизассемблеры
2) Программа повышения прав
3) Атаки на переполнение буфера
4) Sharing
5) Программы подбора паролей

Задание # 18
Вопрос:
... когда поступающие в программу данные вызывают сбой либо проблемы с выдачей программой информации, которая должна быть скрыта, либо с выполнением ряда действий иначе, чем это было запланировано разработчиком программы.

Выберите один из 5 вариантов ответа:
1) Дизассемблеры
2) Программа повышения прав

3) Атаки на переполнение буфера
4) Sharing
5) Программы подбора паролей

Задание # 19

Вопрос:

Перечислите классы атак на отказ в обслуживании.

Выберите несколько из 5 вариантов ответа:

1) Перегрузка пропускной способности сети.
2) Перегрузка системного процессора
3) Занятие возможных портов.
4) Перерасход системных ресурсов.
5) Вирусы и троянские программы

Задание # 20

Вопрос:

Перечислите примеры атак на отказ в обслуживании.

Выберите несколько из 5 вариантов ответа:

1) Атака Ping смерти.
2) Атака потоком Syn запросов.
3) Амплификация.
4) Неверно сформированные пакеты.
5) Атака Smurf.

Задание # 21

Вопрос:

Перечислите методики оценки рисков.

Выберите несколько из 5 вариантов ответа:

1) Модель качественной оценки.
2) Количественная модель.
3) Модель обобщенного стоимостного результата Миоры.
4) Оранжевая книга.
5) Среднестатистическая модель.

Задание # 22

Вопрос:

Имеется здание с внутренней инфраструктурой общей стоимостью 20 000 000 долларов. Пожар может нанести ущерб с фактором воздействия 65%. Пожар может случится раз в 5 лет. Оцените эффективную трату на предотвращение риска.

Запишите число:

_____

Задание # 23

Вопрос:

... - это наука о методах и средствах преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею.

Выберите один из 3 вариантов ответа:

1) Криптография
2) Криптоанализ

3) Хэш-функции

Задание # 24

Вопрос:

Первым документально зафиксированным в письменности шифром является ...

Выберите один из 5 вариантов ответа:

1) шифр Цезаря.
2) квадрат Полибия.
3) шифр Кордано.
4) таблица Вижнера.
5) шифр Вернама.

Задание # 25

Вопрос:

Данный метод шифрования был удобен для передачи на большие расстояния визуально (костры, ...) либо звуками (выстрелы, перестукивания, ...).

Выберите один из 5 вариантов ответа:

1) шифр Цезаря.
2) квадрат Полибия.
3) шифр Кордано.
4) таблица Вижнера.
5) шифр Вернама.

Задание # 26

Вопрос:

В данном методе шифрования использовался квадрат с прорезанными в нем несколькими ячейками.

Выберите один из 5 вариантов ответа:

1) шифр Цезаря.
2) квадрат Полибия.
3) шифр Кордано.
4) таблица Вижнера.
5) шифр Вернама.

Задание # 27

Вопрос:

Какой шифр становится абсолютно стойким при ключе, равеным длине сообщения.

Выберите один из 5 вариантов ответа:

1) шифр Цезаря.
2) квадрат Полибия.
3) шифр Кордано.
4) таблица Вижнера.
5) шифрование методом однократного гаммирования

Задание # 28

Вопрос:

Данный вид шифрования еще называют тюремной азбукой.

Выберите один из 5 вариантов ответа:

1) шифр Цезаря.

2) квадрат Полибия.
3) шифр Кордано.
4) таблица Вижнера.
5) шифр Вернама.

Задание # 29

Вопрос:

В данном методе шифрования символ заменялся парой чисел.

Выберите один из 5 вариантов ответа:

1) шифр Цезаря.
2) квадрат Полибия.
3) шифр Кордано.
4) таблица Вижнера.
5) шифр Вернама.

Задание # 30

Вопрос:

В данном методе шифрования алфавит сдвигался на n позиций, а при дешифровании - на те же n позиций, только в обратную сторону.

Выберите один из 5 вариантов ответа:

1) шифр Цезаря.
2) квадрат Полибия.
3) шифр Кордано.
4) таблица Вижнера.
5) шифр Вернама.

Задание # 31

Вопрос:

Какой метод шифрования неустойчив к частотному анализу.

Выберите один из 5 вариантов ответа:

1) шифр Цезаря.
2) квадрат Полибия.
3) шифр Кордано.
4) таблица Вижнера.
5) шифр Вернама.

Задание # 32

Вопрос:

Какое количество ключей используется при симметричном шифровании.

Выберите один из 4 вариантов ответа:

1) 1
2) 2
3) 3
4) 4

Задание # 33

Вопрос:

Какое количество ключей используется при асимметричном шифровании.

Выберите один из 4 вариантов ответа:

1) 1
2) 2
3) 3
4) 4

Задание # 34

Вопрос:

Как еще называют системы обнаружения атак.

Выберите один из 5 вариантов ответа:

1) Ids
2) Firewall
3) DMZ
4) DHCP
5) UDP

Ответы:

1) Верный ответ (2 б.): "инвентаризация".
2) Верный ответ : 3;
3) Верный ответ : "Социальная инженерия".
4) Верный ответ : "Закладка".
5) Верный ответ : 1;
6) Верные ответы : 1; 2; 3;
7) Верный ответ : "повышение привилегий".
8) Верный ответ : "Сниффер".
9) Верные ответы : 1; 2; 3;
10) Верные ответы : 2; 4;
11) Верные ответы : 1; 4; 5;
12) Верные ответы : 2; 3;
13) Верные ответы : 1; 2;
14) Верный ответ : 1;
15) Верный ответ : 1;
16) Верный ответ : 5;
17) Верный ответ : 1;
18) Верный ответ : 3;
19) Верные ответы : 1; 2; 3; 4;
20) Верные ответы : 1; 2; 3; 4; 5;
21) Верные ответы : 1; 2; 3;
22) Верный ответ : 2600000.
23) Верный ответ : 1;
24) Верный ответ : 1;
25) Верный ответ : 2;
26) Верный ответ : 3;
27) Верный ответ : 5;
28) Верный ответ : 2;
29) Верный ответ : 2;
30) Верный ответ : 1;
31) Верный ответ : 1;
32) Верный ответ : 1;
33) Верный ответ : 2;
34) Верный ответ: 1;

3. Комплект оценочных средств для промежуточной аттестации

3.1. Контрольные вопросы (КВ)

КВ №1. Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.

КВ №2. Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.

КВ №3. Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.

КВ №4. Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.

КВ №5. Оптоволоконные линии связи

КВ №6. Стандарты кабелей. Электрическая проводка.

КВ №7. Беспроводная среда передачи.

КВ №8. Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий

КВ №9. Обзор технологий построения локальных сетей.

КВ №10. Технология Ethernet. Физический уровень.

КВ №11. Технология Ethernet. Канальный уровень

КВ №12. Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI.

КВ №13. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.

КВ №14. Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети

КВ №15. Технология PoweroverEthernet
Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.

КВ №16. Маршрутизация пакетов IPv4

КВ №17. Протоколы динамической маршрутизации

КВ №18. Сеть FDDI. Сеть 100VG-AnyLAN

КВ №19. Сверхвысокоскоростные сети

КВ №20. Беспроводные сети

КВ №21. Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.

КВ №22. Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.

КВ №23. Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.

КВ №24. Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.

КВ №25. Управление множеством коммутаторов. Протокол SNMP.

КВ №26. RMON (Remote Monitoring). Функция Port Mirroring.

КВ №27. Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.

КВ №28. Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.

КВ №29. Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.

КВ №30. Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.

КВ №31. Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.

3.2. Тестовые задания (ТЗ)

ТЗ № 1

Вопрос 1
Как называлась первая компьютерная сеть?
Варианты ответов
- Relcom
- +Arpanet
- Nercnet

Вопрос 2
Первое слово, которым обменялись по сети...
Варианты ответов
- Login
- +Password
- Hello Wolld

Вопрос 3
Линии связи - это...
Варианты ответов
- передающая среда
- станции
- +абоненты сети

Вопрос 4
Тип кабеля, обеспечивающий самую высокую скорость передачи информации...
Варианты ответов

- витая пара
- +оптоволоконный
- коаксиальный

Вопрос 5

Конфигурация (топология) локальной компьютерной сети, в которой все рабочие станции соединены с сервером, называется:

Варианты ответов

- кольцо
- звезда
- +шина
- полносвязная звезда

Вопрос 6

Компьютер, предоставляющий свои ресурсы другим компьютерам при совместной работе, называется:

Варианты ответов

- адаптером
- коммутатором
- рабочей станцией
- +сервером

Вопрос 7

Такие угрозы в сети могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия, например, нарушение целостности и доступности информации:

Варианты ответов

- +умышленные
- не умышленные
- спланированные

Вопрос 8

Какие сети появились раньше?

Варианты ответов

- Глобальные
- Локальные
- +Персональные

Вопрос 9

Укажите все характеристики компьютерной сети.

Варианты ответов

- Компьютерная сеть - несколько компьютеров, используемых для схожих операций
- Компьютерная сеть - группа компьютеров, соединенных с помощью специальной аппаратуры
- Обязательное наличие сервера
- +В сети возможен обмен данными между любыми компьютерами
- Компьютеры должны соединяться непосредственно друг с другом

Вопрос 10

Удаленные соединения типа «терминал - компьютер» появились с созданием чего?

Варианты ответов

- Систем пакетной обработки
- Первых локальных сетей
- Глобальных сетей
- Стандартных технологий локальных сетей
- +Многотерминальных систем

Вопрос 11

К созданию чего привело появление персональных компьютеров?

Варианты ответов

- +Систем пакетной обработки
- Первых локальных сетей
- Глобальных сетей
- Стандартных технологий локальных сетей
- Многотерминальных систем

Вопрос 12

Компьютерное сетью называется:

Варианты ответов

- Совокупность компьютеров, находящихся в одном помещении
- +Совокупность компьютеров, соединенных линиями связи
- Совокупность всего коммуникационного оборудования, находящегося в одном помещении

Вопрос 13

Небольшая организация (5 сотрудников) собирается построить сеть. Какой тип сети является для нее наиболее приемлемым?

Варианты ответов

- Одноранговая сеть
- +Сеть с выделенным сервером
- персональная сеть

Вопрос 14

В каком типе сетей безопасность находится на более высоком уровне?

Варианты ответов

- В одноранговых сетях
- +В сетях на основе сервера

Вопрос 15

Коаксиальный кабель имеет жилу, изготовленную из:

Варианты ответов

- Меди
- Стекла
- +Пластика
- Стали

Вопрос 16

Какого типа коаксиального кабеля не существует?

Варианты ответов

- Тонкий
- +Средний
- Толстый

Вопрос 17

Установите соответствие между типом сетевого кабеля и его описанием:

Варианты ответов

- Состоит из тонкой стеклянной жилы, покрытой слоем стекла с иным, чем у жилы, коэффициентом преломления
- +Состоит из медной жилы, окружающей ее изоляции, экрана в виде металлической оплетки и внешней оболочки
- Состоит из нескольких перевитых друг вокруг друга изолированных медных проводов

Вопрос 18

Для подключения витой пары к компьютеру используется вилка и гнездо:

Варианты ответов

- RG-44
- RG-45

- +RG-54
- RG-55

Вопрос 19

Кабель, способный передавать большие объемы данных на большие расстояния, - это:

Варианты ответов

- +Коаксиальный кабель
- Витая пара
- Оптоволоконный кабель

Вопрос 20

Для работы технологии Bluetooth наличие прямой видимости:

Варианты ответов

- Обязательно
- Необязательно
- +Желательно

Вопрос 21

Кто автор идеи связать несколько компьютеров в одну сеть?

Варианты ответов

- Пол Бэрэн
- +Роберт Тейлор
- Рей Томлинсон

Вопрос 22

Программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами называют:

Варианты ответов

- Трафик
- +Webserver
- Firewall
- Провайдер

Вопрос 23

К морально-этическим средствам защиты компьютерных сетей можно отнести:

Варианты ответов

- Законы, постановления правительства и указы президента, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации ограниченного доступа
- Всевозможные нормы, которые сложились по мере распространения вычислительных средств в той или иной стране
- Действия, предпринимаемые руководством предприятия или организации для обеспечения информационной безопасности
- +Экранирование помещений для защиты от излучения, проверка поставляемой аппаратуры на соответствие ее спецификациям и отсутствие аппаратных «жучков», средства наружного наблюдения, устройства, блокирующие физический доступ к отдельным блокам компьютера

Вопрос 24

Предоставление каждому сотруднику предприятия того минимально уровня привилегий на доступ к данным, который необходим ему для выполнения его должностных обязанностей является принципом:

Варианты ответов

- Политики безопасности
- Морально-этических норм в сети
- +Административной ответственности

Вопрос 25

Весь входящий во внутреннюю сеть и выходящий во внешнюю сеть трафик должен проходить через единственный узел сети, например, через межсетевой экран (firewall) – это принцип политики безопасности:

Варианты ответов

- +принцип единого контрольно-пропускного пункта
- использование комплексного подхода к обеспечению безопасности
- использование средств, которые при отказе переходят в состояние максимальной защиты

Вопрос 26

Электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности относят к:

Варианты ответов

- программным средствам защиты
- +аппаратным средствам защиты
- антивирусным средствам защиты

Вопрос 27

К основным аппаратным средствам защиты информации относятся:

Варианты ответов

- устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.)
- устройства для шифрования информации
- +устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы)
- программные средства блокировки несанкционированного доступа

Вопрос 28

К основным программным средствам защиты информации относятся:

Варианты ответов

- программы идентификации и аутентификации пользователей КС
- программы разграничения доступа пользователей к ресурсам КС
- +программы шифрования информации
- программы архивации данных

Вопрос 29

Подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта) называют:

Варианты ответов

- Аккредитация
- +Идентификация
- Аутентификация

Вопрос 30

Процедура анализа накопленной в результате протоколирования информации. Этот анализ может осуществляться оперативно в реальном времени или периодически, процедура называется:

Варианты ответов

- Средство управления доступом
- +Аудит
- Протоколирование
- Аутентификация

Вопрос 31

Исторически первые сети технологии Ethernet были созданы на кабеле:

Варианты ответов

- тонком коаксиале

- +витой паре
- оптоволоконном
- толстом коаксиале

Вопрос 32

Выберите обозначение кабеля на основе неэкранированной витой пары:

Варианты ответов

- +10Base-F
- 10Base-T
- 10Base-2
- 10Base-FL

Вопрос 33

Какое устройство принимает сигналы из одного сегмента кабеля и побитно синхронно повторяет их в другом сегменте, улучшая форму и мощность импульсов, а также синхронизируя импульсы?

Варианты ответов

- Концентратор
- Повторитель
- +Шлюз
- Мост

Вопрос 34

Он использует в качестве среды передачи данных коаксиальный кабель с волновым сопротивлением 50 Ом, диаметром центрального медного провода 2,17 мм и внешним диаметром около 10 мм

Варианты ответов

- 10Base-F
- +10Base-T
- 10Base-2
- 10Base-5

Вопрос 35

Петлевидное соединение концентраторов в стандарте _____запрещено, так как оно приводит к некорректной работе сети.

Варианты ответов

- 10Base-F
- +10Base-T
- 10Base-2
- 10Base-5

Вопрос 36

Гарантирует длину связи между повторителями до 1 км при общей длине сети не более 2500 м. Максимальное число повторителей между любыми узлами сети - 4

Варианты ответов

- 10Base-F
- 10Base-T
- +10Base-2
- 10Base-5

Вопрос 37

Укажите правильную аббревиатуру экранированной витой пары:

Варианты ответов

- FTP
- +UTP
- STP
- UDP

Вопрос 38

Такая подсистема состоит из внутренних горизонтальных кабелей между кроссовой этажа и информационными розетками рабочих мест:

Варианты ответов

- внешних магистралей
- +внутренних магистралей
- горизонтальная

Вопрос 39

Последовательность работ по монтажу СКС:

Варианты ответов

- 6установку кабельных каналов (в коробах, лотках, гофротрубе, трубах и т.п.);
- 2пробивку отверстий в стенах
- 5прокладку кабеля в кабельных каналах
- 1установку розеток и заделку кабеля модули розетки
- 3сборку и установку монтажного шкафа
- 4установку и набивку патч-панелей и органайзеров

Вопрос 40

Обычно состоит из разъема для сетевого проводника (обычно, витой пары) и микропроцессора, который кодирует/декодирует сетевые пакеты.

Варианты ответов

- Сетевой мост
- Маршрутизатор
- +Сетевая карта
- Терминатор

Вопрос 41

Оборудование, которое способно обрабатывать или преобразовывать передаваемую по сети информацию называют:

Варианты ответов

- активным сетевым оборудованием
- +пассивным сетевым оборудованием
- интерактивным сетевым оборудованием

Вопрос 42

Какое сетевое устройство принимает сигнал от одного компьютера и рассылает его сразу на все свои порты, то есть всем компьютерам в сети?

Варианты ответов

- Сетевой мост
- Маршрутизатор
- +Сетевая карта
- Повторитель
- Концентратор

Вопрос 43

Wreless fidelity расшифровывается как:

Варианты ответов

- +Сетевая активность
- Проводная связь
- Шифрование данных
- Беспроводная связь

Вопрос 44

Различают три типа беспроводных сетей, выберите:

Варианты ответов

- +WAN
- +WPAN
- BWA

- +WLAN

Вопрос 45

Беспроводные локальные сети создаются на основе какого семейства стандартов?

Варианты ответов

- +IEEE 802.11
- IEEE 802.4
- IEEE 802.9
- IEEE 802.3

Вопрос 46

Существует три основных группы стандартов **Internet,** укажите

Варианты ответов

- +Международные
- Европейские
- Американские
- Отраслевые

Вопрос 47

Проектирование СКС разделяют на две основные стадии: телекоммуникационную и:

Варианты ответов

- структурную
- +архитектурную
- подготовительную

Вопрос 48

Включает требования заказчика по числу рабочих мест, их расположению, категории или классу системы. Этажные планы здания позволяют наглядно отобразить расположение различных элементов систем, оценить их параметры

Варианты ответов

- Технический проект
- +Техническое задание
- Техническая документация

Вопрос 49

Возможность радиоустройства перемещаться за пределы действия базовой станции и, находясь в зоне действия "гостевой" станции, иметь доступ к "домашней" сети называется:

Варианты ответов

- Роуминг
- +Фишинг
- Адаптируемость

Вопрос 50

Всегда маскируется под какую-нибудь полезную утилиту или игру, а производит действия, разрушающие систему:

Варианты ответов

- Червь
- Троянский конь
- +Рукит
- Шпион

Вопрос 51

Какой уровень сетевой коммуникации (OSI), включает сетевое оборудование - сетевые кабели, разъемы, концентраторы и т.д.?

Варианты ответов

- физический
- сетевой
- +канальный

Вопрос 52
Какой протокол предназначен для автоматизации назначения ip-адресов в локальных сетях?
Варианты ответов

- +DHCP
- TCP/IP
- PPP
- RIP

Шкала оценки тестирования

Процент результативности (правильных ответов)	Оценка уровня подготовки	
	балл (отметка)	вербальный аналог
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	неудовлетворительно

Критерии оценивания

«5» «отлично» или «зачтено» – студент показывает глубокое и полное овладение содержанием программного материала по МДК, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо» или «зачтено» – студент в полном объеме освоил программный материал по МДК, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно» или «зачтено» – студент обнаруживает знание и понимание основных положений программного материала по МДК но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и

профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» или «не зачтено» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по МДК, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

3. Информационное обеспечение

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Компьютерные сети: учебное пособие/ Кузин А.В. – 4-е изд. – М.: ФОРУМ, 2023. – 190 с.
2. Организация, принципы построения и функционирования компьютерных сетей: учебник/И.А.Ушаков-М.:Академия,2019-240 с.
3. Костров Б. В. Сети и системы передачи информации – М.: Издательский центр «Академия», 2019 -224 с.

Дополнительные источники:

1. Компьютерные сети 5-е изд., учебное пособие /Новожилов Е.О. – М.:ИЦ Академия,2017 г.
2. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2015.
3. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2013.
4. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
5. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2013.

Электронные издания (электронные ресурсы):

Цифровая образовательная среда СПО PROFобразование:

- Демидов, Л. Н. Основы эксплуатации компьютерных сетей : учебник для бакалавриата / Л. Н. Демидов. — Москва : Прометей, 2019. — 798 c. — ISBN 978-5-907100-01-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/94481 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. Пользователей

- Оливер, Ибе Компьютерные сети и службы удаленного доступа / Ибе Оливер ; перевод И. В. Синицын. — 2-е изд. — Саратов : Профобразование, 2019. — 335 c. — ISBN 978-5-4488-0054-2. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87999 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:

IPR BOOKS - https://www.iprbookshop.ru/89416.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/

«Алексеевский колледж» http://moodle.alcollege.ru/