Методические указания по выполнению заданий учебной практики

Задания учебной практики выполняются по неделям и оформляются в отчет за неделю. В отчете пишется:

- Название практической или лабораторной работы;
- Описание работы;
- Выводы и результаты.

Также работа может быть дополнена схемами, таблицами, рисунками и графиками. Если у студента нет возможности выполнять работы на реальном оборудовании, можно использовать виртуальную машину или выполнить работу в реферативном порядке.

Оформление отчета должно быть выполнено в любом текстовом редакторе с соблюдением правил нормоконтроля.

Первая неделя практики

Практическая работа № 1 Поддержка пользователей сети.

Задание:

1. С разрешения преподавателя включите компьютер, дождитесь завершения загрузки опе- рационной системы Windows (Windows XP, 7).

2. Найдите в вашей сети сетевой адаптер, концентратор (HUB или Switch), модем, воло- конноптический приёмопередатчик, Wi-Fi-роутер, интернет-сервер, файловый сервер, вы- деленный сервер, рабочую станцию (покажите преподавателю, что вы нашли).

3. Поместите на «Рабочий стол» значок «Сеть» (если его там нет), выполните двойной щелчок по этому значку и ознакомьтесь с содержимым вашей локальной компьютерной се- ти. Попробуйте определить, какая у вас локальная сеть (по способу взаимодействия компь- ютеров) – одноранговая или сеть с выделенным сервером?

− В одноранговой локальной сети все компьютеры равноправны. Общие устройства могут быть подключены к любому компьютеру в сети. Пользователи самостоятельно реша- ют, какие ресурсы своего компьютера (диски, папки, принтеры) сделать доступными для других пользователей сети. Подключенные к сети пользователи могут пользоваться ресурсами компьютера как своими собственными. Основным недостатком таких одно- ранговых сетей является слабая защищенность информации от несанкционированного доступа.

− Если к локальной сети подключено более 10 компьютеров, одноранговая сеть может оказаться недостаточно производительной.

− Для увеличения производительности, а также в целях обеспечения большей информаци- онной безопасности один из компьютеров локальной сети может быть выделен в каче- стве сервера, на котором хранится наиболее важная информация. Правила доступа к этой информации устанавливает один человек – администратор сети.

Сделайте **Screenshot** (копию экрана) окна «Сетевое окружение» и вставьте его в ваш отчёт.

4. Открывая в окне «Сетевое окружение» папки подключенных к сети ПК,

определите, ка- кие ресурсы они предоставляют в совместное использование. Сделайте **Screenshot** окон 2-х папок и вставьте их в ваш отчёт.

5. Выясните, куда входят компьютеры (рабочая группа, домен), определите название рабо- чей группы или домена, определите имя своего компьютера. Запишите результаты в отчёт. −*свойства папки «Мой компьютер» Имя компьютера.*

6. Определите, есть ли на вашем компьютере сетевые диски и сетевые принтеры.

− ***Сетевые диски*** *— это диски другого компьютера сети, которые данный компьютер воспринимает как своё дополнительное внешнее устройство.*

− ***Сетевые принтеры*** *— это принтеры другого компьютера сети, которые данный ком- пьютер воспринимает как свои дополнительные устройства печати.*

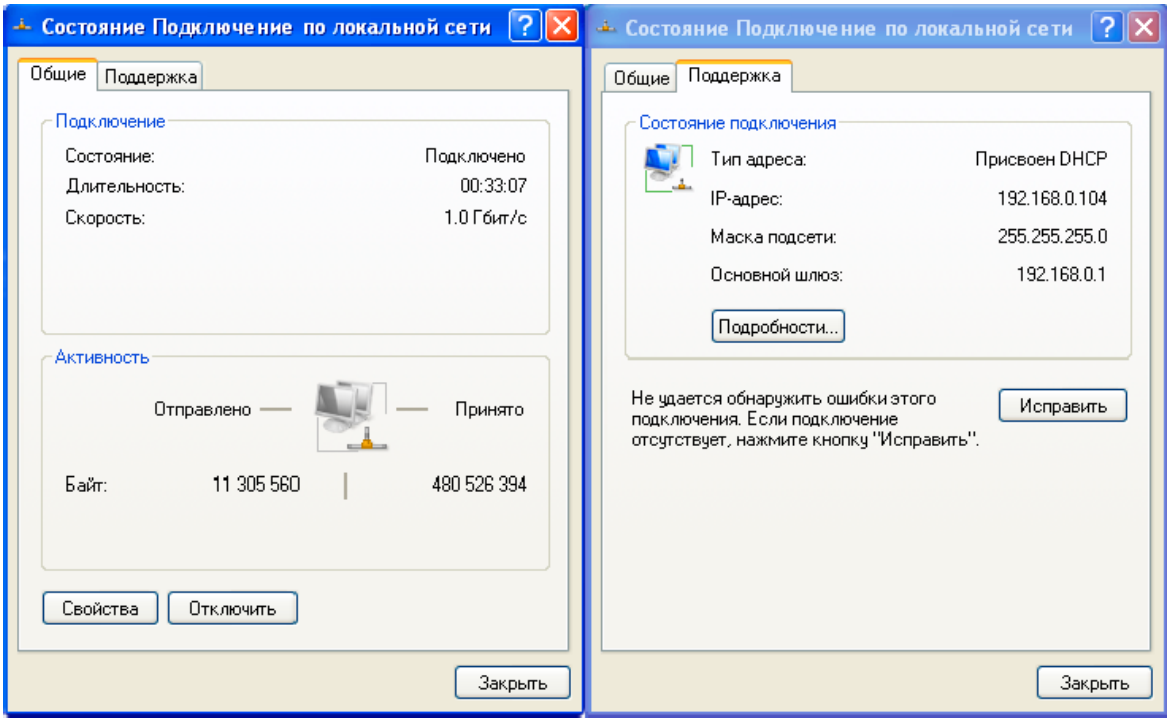
7. Подключите к своему компьютеру сетевой принтер. Какой вид имеет значок сетевого принтера?

− *Найдите в сетевом окружении компьютер преподавателя, выполните двойной щелчок мышью по нему, а затем по значку принтера. Принтер подключится автоматически.*

8. Создайте на сервере, в папке своей группы, которая находится в папке Students, новую папку и назовите её своей фамилией с инициалами, например, Чумак А.А и подключите её к своему компьютеру как сетевой диск. Какой вид имеет значок сетевого диска?

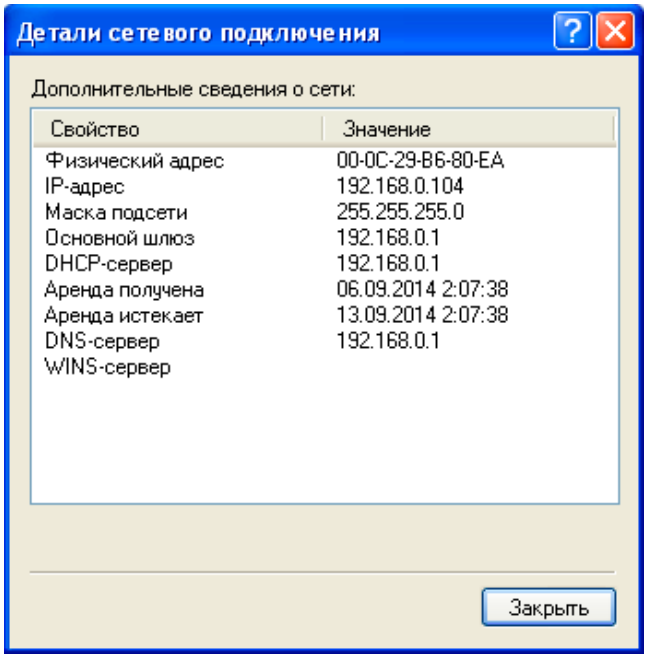
− *Удалить сетевые диски и принтеры можно, воспользовавшись контекстным меню вы- бранного объекта.*

9. Определите IP адрес вашего персонального компьютера. − *(см. свойства папки Сетевое окружение свойства параметра "Подключение по локальной сети" свойства пара- метра "Протокол TCP/IP"). Результаты запишите в отчёт. − Можно выполнить двойной щелчок по значку «Сеть» на панели индикации («системный трэй»):*

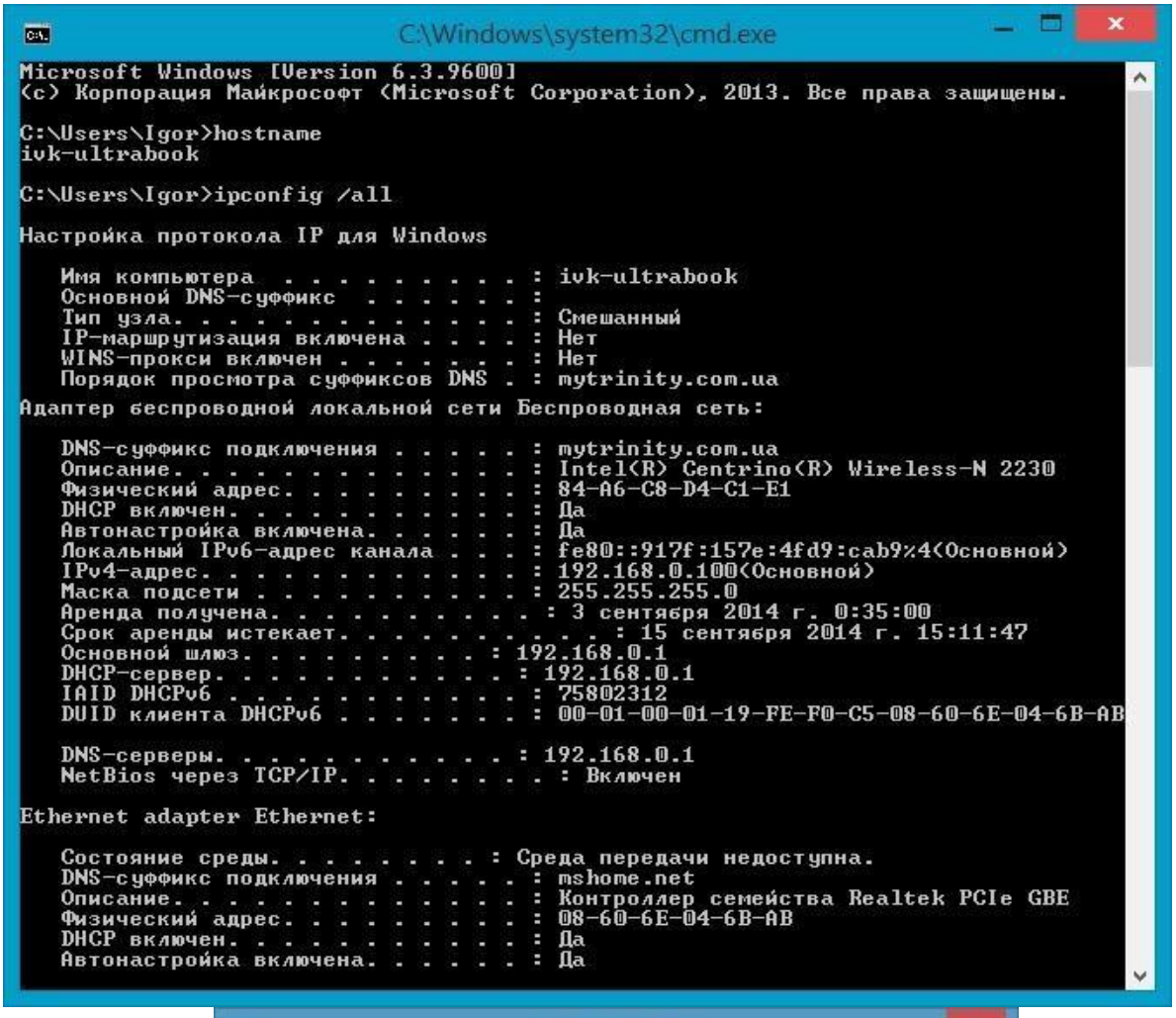


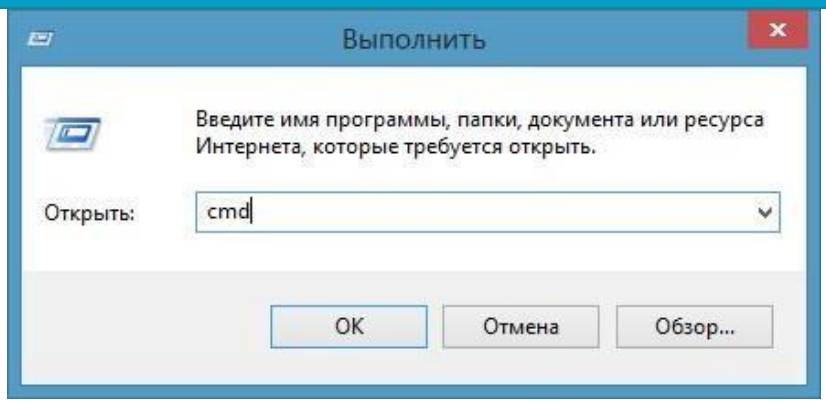
10. Определите физический адрес сетевой карты вашего компьютера

– *В окне «Состояние Подключение по локальной сети» нажмите кнопку «Подробности»:*



– ***Второй способ:*** *в «Главном меню» найдите команду «Выполнить», введите «cmd». От- кроется окно командного интерпретатора (режим «ДОС»). Введите в этом окне ко- манду «ipconfig /all» и нажмите «Enter».*


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.
C:\Users\Igor>hostname
ivk-ultrabook
C:\Users\Igor>ipconfig /all
Настройка протокола IP для Windows
Имя компьютера . . . . . : ivk-ultrabook
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Смешанный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . : mytrinity.com.ua
Адаптер беспроводной локальной сети Беспроводная сеть:
DNS-суффикс подключения . . . . . : mytrinity.com.ua
Описание. . . . . : Intel(R) Centrino(R) Wireless-N 2230
Физический адрес. . . . . : 84-A6-C8-D4-C1-E1
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::917f:157e:4fd9:cab9%4(Основной)
IPv4-адрес. . . . . : 192.168.0.100(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 3 сентября 2014 г. 0:35:00
Срок аренды истекает. . . . . : 15 сентября 2014 г. 15:11:47
Основной шлюз. . . . . : 192.168.0.1
DHCP-сервер. . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 75802312
DUID клиента DHCPv6 . . . . . : 00-01-00-01-19-FE-F0-C5-08-60-6E-04-6B-AB
DNS-серверы. . . . . : 192.168.0.1
NetBios через TCP/IP. . . . . : Включен
Ethernet adapter Ethernet:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . : mshome.net
Описание. . . . . : Контроллер семейства Realtek PCIe GBE
Физический адрес. . . . . : 08-60-6E-04-6B-AB
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

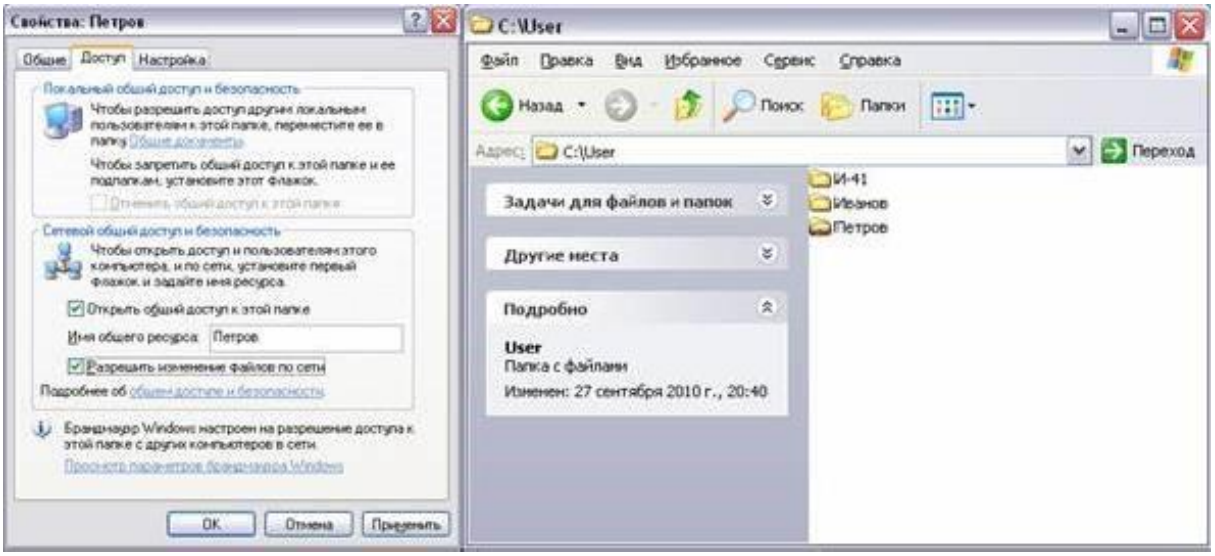

Выполнить
Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.
Открыть:
cmd
OK
Отмена
Обзор...

11. Предоставьте в совместное использование свои ресурсы - объявите свой каталог общим, выбрав команду «Доступ» в контекстном меню. − *В папке «Мои документы» создайте ка- талог с именем, совпадающим с Вашей фамилией.*

− *Задайте тип доступа Полный (команда «Разрешить изменение файлов по сети»).*

− *Обратите внимание на изменение вида значка каталога.*

Сделайте копию экрана и сохраните графический файл с этой копией в этой папке. Обме-няйтесь этими файлами с кем-нибудь по сети.



Практическая работа № 2

Эксплуатация технических средств сетевой инфраструктуры (принтеры, ком-пьютеры,серверы)

Порядок работы

1. Убедитесь в том, что компьютерная система обесточена (при необходимости, отклю- чите систему от сети).

2. Разверните системный блок задней стенкой к себе.

3. По наличию или отсутствию разъемов USB установите форм-фактор материнской платы (при наличии разъемов USB - форм-фактор ATX, при их отсутствии -AT). 4. Уста- новите местоположение и снимите характеристики следующих разъемов:

- питания системного блока;
- питания монитора;
- сигнального кабеля монитора;
- клавиатуры;
- последовательных портов; • параллельного порта (если есть);
- других разъемов.

5. Убедитесь в том, что все разъемы, выведенные на заднюю стенку системного блока, не взаимозаменяемы, то есть каждое базовое устройство подключается одним единственным способом.

6. Изучите способ подключения мыши.

7. Заполните таблицу:

Разъем	Тип разъема	Количество контактов	Примечания

8. Определить наличие основных устройств персонального компьютера.

9. Установите местоположение блока питания, выясните мощность блока питания (ука-зана на ярлыке).

10. Установите местоположение материнской платы.

11. Установите характер подключения материнской платы к блоку питания.

12. Установите местоположение жесткого диска.

Установите местоположение его разъема питания. Проследите направление шлейфа про-водников, связывающего жесткий диск с материнской платой.

13. Установите местоположение платы видеоадаптера.

14. При наличии прочих дополнительных устройств выявите их назначение, опишите характерные особенности данных устройств (типы разъемов, тип интерфейса и др.).

15. Заполните таблицу:

Устройство	Характерные особенности	Куда и при пом чегоподключается

Практическая работа № 3

Выполнение действий по устранению неисправностей

Классификация неисправностей АПС

Для выбора метода диагностики и определения первичных и вторичных симптомов отказа необходимо уметь классифицировать неисправность, т. к. первичный отказ часто вызывает целый спектр отказов вторичных, являющихся следствием первичного и затеняющих причину неисправности.

Предлагаемая классификация охватывает ошибки и отказы, вызванные электронными узлами *системной платы*, как наиболее сложной части PC, и может быть распространена на весь клон IBM PC.

С позиции аппаратных и программных средств, используемых в PC, неисправности подразделяются на аппаратные, программные и аппаратно-программные.

Аппаратные неисправности, т. е. неисправности аппаратных средств, в свою очередь, подразделяются на случайные, мягкие и жесткие ошибки.

К **случайным** ошибкам относят:

1) плавающие ошибки;
2) корректируемые отказы;
3) некорректируемые отказы (технические остановы).

Потенциально, любая неисправность, связанная со случайными ошибками, может привести к жесткой ошибке. Случайная ошибка, приобретшая фактор стабильности и делающая невозможной дальнейшую эксплуатацию системы классифицируется как жесткая, не корректируемая и требует анализа и диагностики неисправности АПС. Нередко, после коррекции условий эксплуатации ВС (температурно-климатические, вибрационные и т. д.), такие ошибки исчезают, но, по истечении некоторого времени, появляются снова. Таким образом, это – не метод устранения ошибок, и задача инженера или техника по ТО – наоборот, *ужесточить условия эксплуатации ВС на время диагностики,* с целью выявления ошибки и выделения отказавшего узла. Наиболее неприятны отказы, связанные с факторами нестабильности и неопределенности – плавающие ошибки.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом потеме занятия.

2. Запустить программу Everest на тестируемом компьютере и с помощью мастера отче-тов (меню «Отчёт») сформировать отчет об аппаратном обеспечении.

3. Заполнить табл. 1.

1. Результаты выполнения работы

№	Наименование компонента системного блока или характеристика	Найденное обозначение или характеристика
1	Тип ЦП, частота	
2	Тип системной платы, форм-фактор	
3	Чипсет системной платы	
4	Тип жесткого диска, объем	
5	Тип сетевого адаптера	
6	Тип видеоадаптера	
7	Тип звукового адаптера	
8	Разъемы ОЗУ	
9	Разъемы расширения системной платы	
10	Объем кэш-памяти процессора	

Практическая работа № 4

Выполнение мониторинга и анализа работы локальной сети с помощью программ***ныхсредств.***

Задание:

1. Проверка знакомства с процессом наблюдения за сетью

Опишите, в чём, по вашему мнению, заключается процесс мониторинга сети. Приведите примерего использования в производственной сети.

2: Изучение средств мониторинга сети

Проведите исследование и найдите три средства мониторинга сети. Перечислите эти три найденных средства.

Заполните следующую форму для выбранных средств мониторинга сети.

Поставщик	**Название продукта**	**Функциональные возможно-сти**

3: Выберите средство мониторинга сети

1: Выберите одно или несколько средств мониторинга из исследования.

Укажите одно или несколько средств из исследования, которые бы вы выбрали для мониторинга сети. Назовите эти средства и объясните свой выбор, перечислив конкретные функциональные возможности, которые по вашему мнению важны.

2: Изучите средство мониторинга сети PRTG.

Перейдите на веб-страницу www.paessler.com/prtg.

В следующих полях приведите примеры некоторых функций PRTG.

3. Какие выводы вы можете сделать на основании проведённого исследования в отношении про-граммного обеспечения для наблюдения за сетью?

Практическая работа № 5

Оформление технической документации, правила оформления документов

Полное наименование изделия на титульном листе, в основной надписи и при первом упомина-нии в тексте документа должно быть одинаковым с наименованием его в основном конструк- торском документе.

В последующем тексте порядок слов в наименовании должен быть прямой, т.е. на

первом месте должно быть определение (имя прилагательное), а затем - название изделия (имя существитель- ное); при этом допускается употреблять сокращенное наименование изделия.

Наименования, приводимые в тексте документа и на иллюстрациях, должны быть одинаковыми. Текст документа должен быть кратким, четким и не допускать различных толкований.

При изложении обязательных требований в тексте должны применяться слова "должен", "следу- ет", "необходимо", "требуется, чтобы", "разрешается только", "не допускается", "запрещается", "не следует". При изложении других положений следует применять слова - "могут быть", "как правило", "при необходимости", "может быть", "в случае" и т.д.

При этом допускается использовать повествовательную форму изложения текста документа,например "применяют", "указывают" и т.п.

В документах должны применяться научно-технические термины, обозначения и определения, установленные соответствующими стандартами, а при их отсутствии - общепринятые в научно-технической литературе.

Если в документе принята специфическая терминология, то в конце его (перед списком литера- туры) должен быть перечень принятых терминов с соответствующими разъяснениями. Переченьвключают в содержание документа.

В тексте документа не допускается:

- применять обороты разговорной речи, техницизмы, профессионализмы;
- применять для одного и того же понятия различные научно-технические термины, близ- кие по смыслу (синонимы), а также иностранные слова и термины при наличии равнозначных слов и терминов в русском языке;
- применять произвольные словообразования;
- применять сокращения слов, кроме установленных правилами русской орфографии, со- ответствующими государственными стандартами, а также в данном документе;
- сокращать обозначения единиц физических величин, если они употребляются без цифр, за исключением единиц физических величин в головках и боковиках таблиц, и в расшифровкахбуквенных обозначений, входящих в формулы и рисунки.

В тексте документа, за исключением формул, таблиц и рисунков, не допускается:

- применять математический знак минус (-) перед отрицательными значениями величин(следует писать слово "минус");

- применять знак "Ø" для обозначения диаметра (следует писать слово "диаметр"). При указании размера или предельных отклонений диаметра на чертежах, помещенных в тексте до-кумента, перед размерным числом следует писать знак "Ø";

- применять без числовых значений математические знаки, например > (больше), <(мень- ше), =(равно), ≥(больше или равно), ≤(меньше или равно), ≠(не равно), а также знаки № (номер),

% (процент);

- применять индексы стандартов, технических условий и других документов без регистра-ционного номера.

Если в документе приводятся поясняющие надписи, наносимые непосредственно на изготовля-емое изделие (например на планки, таблички к элементам управления и

т.п.), их выделяют шрифтом (без кавычек), например ВКЛ., ОТКЛ., или кавычками - еслинадпись состоит из цифр и (или) знаков.

Наименования команд, режимов, сигналов и т.п. в тексте следует выделять кавычками, напри-мер, "Сигнал +27 включено".

Перечень допускаемых сокращений слов установлен в ГОСТ 2.316.

Если в документе принята особая система сокращения слов или наименований, то в нем должен быть приведен перечень принятых сокращений, который помещают в конце документа перед перечнем терминов.

Условные буквенные обозначения, изображения или знаки должны соответствовать принятым в действующем законодательстве и государственных стандартах. В тексте документа перед обо- значением параметра дают его пояснение, например "Временное сопротивление разрыву $\sigma_в$".

При необходимости применения условных обозначений, изображений или знаков, не установ- ленных действующими стандартами, их следует пояснять в тексте или в перечне обозначений. В документе следует применять стандартизованные единицы физических величин, их наимено-вания и обозначения в соответствии с ГОСТ 8.417.

Наряду с единицами СИ, при необходимости, в скобках указывают единицы ранее применяв- шихся систем, разрешенных к применению. Применение в одном документе разных систем обо-значения физических величин не допускается.

В тексте документа числовые значения величин с обозначением единиц физических величин иединиц счета следует писать цифрами, а числа без обозначения единиц физических величин и единиц счета от единицы до девяти - словами. Примеры

1 Провести испытания пяти труб, каждая длиной 5 м.

2 Отобрать 15 труб для испытаний на давление.

Единица физической величины одного и того же параметра в пределах одного документа долж- на быть постоянной. Если в тексте приводится ряд числовых значений, выраженных в одной и той же единице физической величины, то ее указывают только после последнего числового зна-чения, например 1,50; 1,75; 2,00 м.

Если в тексте документа приводят диапазон числовых значений физической величины, выра- женных в одной и той же единице физической величины, то обозначение единицы физической величины указывается после последнего числового значения диапазона. Примеры:

1. От 1 до 5 мм.
2. От 10 до 100 кг.
3. От плюс 10 до минус 40°С.
4. От плюс 10 до плюс 40°С.

Недопустимо отделять единицу физической величины от числового значения (переносить их на разные строки или страницы), кроме единиц физических величин, помещаемых в таблицах, вы-полненных машинописным способом.

Приводя наибольшие или наименьшие значения величин, следует применять словосочетание"должно быть не более (не менее)".

Приводя допустимые значения отклонений от указанных норм, требований, следует применятьсловосочетание "не должно быть более (менее)".

Например, массовая доля углекислового натрия в технической кальцинированной соде должнабыть не менее 99,4 %.

Числовые значения величин в тексте следует указывать со степенью точности, которая необхо- дима для обеспечения требуемых свойств изделия, при этом в ряду величин осуществляется вы-равнивание числа знаков после запятой.

Округление числовых значений величин до первого, второго, третьего и т.д. десятичного знака для различных типоразмеров, марок и т.п. изделий одного наименования должно быть одинако-вым. Например, если градация толщины стальной горячекатаной ленты

0,25 мм, то весь ряд толщин ленты должен быть указан с таким же количеством десятичных знаков, например 1,50; 1,75; 2,00.

Дробные числа необходимо приводить в виде десятичных дробей, за исключением размеров в дюймах, которые следует записывать $\frac{1''}{4}$ $\frac{1''}{2}$ $^1/_4''$; $^1/_2''$

При невозможности выразить числовое значение в виде десятичной дроби, допускается записы-вать в виде простой дроби в одну строчку через косую черту, например, 5/32; (50A- 4C)/(40B+20).

В формулах в качестве символов следует применять обозначения, установленные соответству- ющими государственными стандартами. Пояснения символов и числовых коэффициентов, вхо- дящих в формулу, если они не пояснены ранее в тексте, должны быть приведены непосред- ственно под формулой. Пояснения каждого символа следует давать с новой строки в той после- довательности, в которой символы приведены в формуле. Первая строка пояснения должна начинаться со слова "где" без двоеточия после него.

Пример - Плотность каждого образца, Pкг/м^3, вычисляют по формуле

$$\rho = \frac{m}{V}$$

,где m - масса образца, кг; V- объем образца, м^3.

Формулы, следующие одна за другой и не разделенные текстом, разделяют запятой. Переносить формулы на следующую строку допускается только на знаках выполняемых опера- ций, причем знак в начале следующей строки повторяют. При переносе формулы на знаке умножения применяют знак "×".

В документах, издаваемых нетипографским способом, формулы могут быть выполнены маши- нописным, машинным способами или чертежным шрифтом высотой не менее 2,5 мм. Примене- ние машинописных и рукописных символов в одной формуле не допускается.

Формулы, за исключением формул, помещаемых в приложении, должны нумероваться сквозной нумерацией арабскими цифрами, которые записывают на уровне формулы справа в круглых скобках. Одну формулу обозначают - (1).

Ссылки в тексте на порядковые номера формул дают в скобках, например, ... в формуле (1). Формулы, помещаемые в приложениях, должны нумероваться отдельной

нумерацией арабски- ми цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначенияприложения, например формула (В.1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой, например (3.1).

Порядок изложения в документах математических уравнений такой же, как и формул. Примечания приводят в документах, если необходимы пояснения или справочные данные к со-держанию текста, таблиц или графического материала.

Примечания не должны содержать требований.

Примечания следует помещать непосредственно после текстового, графического материала или в таблице, к которым относятся эти примечания, и печатать с прописной буквы с абзаца. Если примечание одно, то после слова "Примечание" ставится тире и примечание печатается тоже с прописной буквы. Одно примечание не нумеруют. Несколько примечаний нумеруют по порядку арабскими цифрами. Примечание к таблице помещают в конце таблицы над линией, обознача- ющей окончание таблицы. Примеры:

В текстовом документе допускаются ссылки на данный документ, стандарты, технические усло- вия и другие документы при условии, что они полностью и однозначно определяют соответ- ствующие требования и не вызывают затруднений в пользовании документом.

Ссылки на стандарты предприятий (СТП) и другую техническую документацию должны бытьоговорены в договоре на разработку изделия.

Ссылаться следует на документ в целом или его разделы и приложения. Ссылки на подразделы, пункты, таблицы и иллюстрации не допускаются, за исключением подразделов, пунктов, таблици иллюстраций данного документа.

При ссылках на стандарты и технические условия указывают только их обозначение, при этом допускается не указывать год их утверждения при условии записи обозначения с годом утвер-ждения в конце текстового документа под рубрикой ’’ССЫЛОЧНЫЕ НОРМАТИВНЫЕ ДО-КУМЕНТЫ" по форме:

Обозначение документа, на которыйдана ссылка	Номер раздела, подраздела, пункта, подпункта, перечисления, приложения, разрабатываемого до-кумента, в котором дана ссылка

При ссылках на другие документы в графе "Обозначение документа" указывают также

и наиме-нование документа. При ссылках на раздел или приложение указывают его номер.

Задание:

1. Оформить текст используя правила стандартов ЕСКД:

Вторая неделя практики

Практическая работа № 1Протокол управления SNMP

Для успешного администрирования сети необходимо знать состояние каждого ее элемента с возможностью изменять параметры его функционирования. Обычно сеть состоит из устройств различных производителей и управлять ею было бы нелегкой задачей, если бы каждое из сете- вых устройств понимало только свою систему команд. Поэтому возникла необходимость в со- здании единого языка управления сетевыми ресурсами, который бы понимали все устройства, и который, в силу этого, использовался бы всеми пакетами управления сетью для взаимодействия с конкретными устройствами.

Подобным языком стал SNMP - Simple Network Management Protocol. Разработанный для систем, ориентированных под операционную систему UNIX, он стал фактически общепринятым стандартом сетевых систем управления и поддерживается подавляющим большинством произ- водителей сетевого оборудования в своих продуктах.

В силу своего названия - Простой Протокол Сетевого Управления - основной задачей при его разработке было добиться максимальной простоты его реализации. В результате возник про- токол, включающий минимальный набор команд, однако позволяющий выполнять практически весь спектр задач управления сетевыми устройствами - от получения информации о местона- хождении конкретного устройства, до возможности производить его тестирование.

Протокол SNMP дает возможность администраторам управлять узлами, такими как серве- ры, рабочие станции, маршрутизаторы, коммутаторы и устройства безопасности в сети IP. Он позволяет сетевым администраторам контролировать работу сети, выполнять поиск и разреше- ние сетевых проблем, а также планировать рост сети.

Сегодня SNMP является самым популярным протоколом управления различными коммер-ческими, университетскими и исследовательскими объединенными сетями.

Применяют SNMP для:

– Получение информации о состоянии сетевого оборудования Локализация неполадок в сети
– Удаленное управление узлами сети

- Сбор статистической информации о состоянии сети
- Возможно применение протокола SNMP в областях, не связанных с сетевыми технологиями:
    - Проекты по использованию SNMP в системах управления светофорами
    - Производства, имеющие сеть измерительных приборов, разбросанных географически, нуждающиеся в мониторинге состояния и показаний этих приборов

Основные преимущества протокола SNMP:

- простота;
- доступность;
- независимость от производителей.

Основной концепцией протокола является то, что вся необходимая для управления устрой- ством информация хранится на самом устройстве - будь то сервер, модем или маршрутизатор - в так называемой Административной Информационной Базе (MIB - Management Information Base

- RFC 1213).

Применяются базы управляющей информации (MIB) для упрощения. запоминания адреса объектов устройств, определяемых в цифровом формате. Базы MIB описывают структуру управляемых данных на подсистеме устройства; они используют иерархическое пространство имен, содержащее идентификаторы объектов (OID-ы). Каждый OID состоит из двух частей: тек- стового имени и SNMP адреса в цифровом виде. Базы MIB являются необязательными и выпол- няют вспомогательную роль по переводу имени объекта из человеческого формата (словесного) в формат SNMP (цифровой). Так как структура объектов на устройствах разных производителей не совпадает, без базы MIB практически невозможно определить цифровые SNMP адреса нуж- ных объектов.

MIB представляет собой набор переменных, характеризующих состояние объекта управле- ния. Эти переменные могут отражать такие параметры, как количество пакетов, обработанных устройством, состояние его интерфейсов, время функционирования устройства и т.п.

Для того, чтобы проконтролировать работу некоторого устройства сети, необходимо просто получить доступ к его MIB, которая постоянно обновляется самим устройством, и проанализи- ровать значения некоторых переменных.

Модель SNMP состоит из четырех компонентов:

- управляемых узлов;
- станций управления (менеджеров);
- управляющей информации;
- протокола управления.

Агентами в SNMP являются программные модули, которые работают в управляемых устройствах. Агенты собирают информацию об управляемых устройствах, в которых они работают, и делают эту информацию доступной для систем управления сетями (network management systems - NMS) с помощью протокола SNMP.

Управляемое устройство может быть узлом любого типа, находящимся в какой-нибудь сети: это хосты, служебные устройства связи, принтеры, роутеры, мосты и концентраторы, коммутаторы.

При использовании SNMP один или более административных компьютеров (где функционируют программные средства, называемые менеджерами) выполняют отслеживание или управление группой хостов или устройств в компьютерной сети. На каждой управляемой систе- ме есть постоянно запущенная программа, называемая агент, которая через SNMP передаёт ин- формацию менеджеру.

Менеджеры SNMP обрабатывают данные о конфигурации и функционировании управляе- мых систем и преобразуют их во внутренний формат, удобный для поддержания протокола SNMP. Протокол также разрешает активные задачи управления, например, изменение и приме- нение новой конфигурации через удаленное изменение этих переменных. Доступные через SNMP переменные организованы в иерархии. Эти иерархии, как и другие метаданные (напри- мер, тип и описание переменной), описываются базами управляющей информации (базы MIB, от англ. Management information base).

Управляемые протоколом SNMP сети состоят из трех ключевых компонентов:

– Управляемое устройство;

– Агент — программное обеспечение, запускаемое на управляемом устрой- стве, либо на устройстве, подключенном к интерфейсу управления управляемого устрой- ства;

– Система сетевого управления (Network Management System, NMS) — про- граммное обеспечение, взаимодействующее с менеджерами для поддержки комплексной структуры данных, отражающей состояние сети.

Управляемое устройство — элемент сети (оборудование или программное средство),

реали- зующий интерфейс управления (не обязательно SNMP), который разрешает однонаправленный (только для чтения) или двунаправленный доступ к конкретной информации об элементе. Управляемые устройства обмениваются этой информацией с менеджером. Управляемые устройства могут относиться к любому виду устройств: маршрутизаторы, серверы доступа, коммутаторы, мосты, концентраторы, IP-телефоны, IP-видеокамеры, компьютеры-хосты, прин- теры и т. п.

Агентом называется программный модуль сетевого управления, располагающийся на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управля-емого устройства. Агент обладает локальным знанием управляющей информации и переводит эту информацию в специфичную для SNMP форму или из неё (медиация данных).

В состав системы сетевого управления (*NMS*) входит приложение, отслеживающее и кон- тролирующее управляемые устройства. NMS обеспечивают основную часть обработки данных, необходимых для сетевого управления. В любой управляемой сети может быть одна и более NMS.

Детали протокола

SNMP работает на прикладном уровне TCP/IP (седьмой уровень модели OSI). Агент SNMP получает запросы по UDP-порту 161. Менеджер может посылать запросы с любого доступного порта источника на порт агента. Ответ агента будет отправлен назад на порт источника на мене-джере. Менеджер получает уведомления (Traps и InformRequests) по порту 162. Агент может генерировать уведомления с любого доступного порта. При использова- нии TLS или DTLS запросы получаются по порту 10161, а ловушки отправляются на порт 10162.

В SNMPv1 указано пять основных протокольных единиц обмена (protocol data units — PDU). Еще две PDU, GetBulkRequest и InformRequest, были введены в SNMPv2 и перенесены в SNMPv3.

Все PDU протокола SNMP построены следующим образом:

IP header (IP-заголо-вок)	UDP header (UDP-заголо-вок)	version (вер-сия)	communit y (пароль)	PDU-type (PDU -тип)	request-id (id запро-са)	error-status (статус ошиб-ки)	error-index (индекс ошиб-ки)	variable bindings (связанные перемен-ные)

Существует семь протокольных единиц обмена SNMP, из которых два основных: GetRequest

Запрос от менеджера к объекту для получения значения переменной или списка перемен- ных. Требуемые переменные указываются в поле variable bindings (раздел поля values при этом не используется). Получение значений указанной переменной должно быть выполнено агентом как *Атомарная операция* (операции, выполняющиеся как единое целое, либо не выполняющие- ся вовсе.). Менеджеру будет возвращен Response (ответ) с текущими значениями.

SetReques

Запрос от менеджера к объекту для изменения переменной или списка переменных. Связан- ные переменные указываются в теле запроса. Изменения всех указанных переменных должны быть выполнены агентом как атомарная операция. Менеджеру будет возвращен Response с (те- кущими) новыми значениями переменных.

Ловушки агента SNMP

NMS периодически проводит опрос агентов SNMP, размещенных на управляемых устрой- ствах, запрашивая данные у устройства с помощью запроса get. С помощью этого процесса при- ложение для управления сетями может собирать информацию для мониторинга транспортной нагрузки и проверять настройки управляемых устройств. Информация может отображаться че- рез графический интерфейс пользователя в системе NMS. Можно вычислить минимальные, средние и максимальные значения, создать графическое представление данных или установить пороговые значения, при превышении которых будут отправляться соответствующие уведомле- ния. Например, система NMS может контролировать использование центрального процессора маршрутизатора Cisco. Диспетчер SNMP осуществляет периодическую выборку значений и представляет эту информацию в графическом виде, чтобы сетевой администратор могу исполь- зовать её для вычисления базовых показателей.

Периодический опрос SNMP имеет свои недостатки. Во-первых, существует задержка меж- ду временем обнаружения события и временем отправки соответствующего уведомления (путём опроса) системой NMS. Во-вторых, существует компромисс между частотой опроса и использо-ванием пропускной способности.

Чтобы смягчить воздействие этих недостатков, агенты SNMP могут создавать и отправлять ловушки, сообщая системе NMS о некоторых событиях немедленно. Ловушки — это незапра- шиваемые сообщения, предупреждающие диспетчера SNMP о каком-либо

условии или событии в сети. Примерами условий ловушек, помимо прочего, являются следующие: неправильная аутентификация пользователей, перезапуски, изменение состояния канала (на активное или не- активное), отслеживание MAC-адресов, закрытие подключения TCP, потеря подключения к со- седнему узлу или другие важные события. Уведомления, направленные на ловушки, помогают сократить использование ресурсов сети и агентов, устраняя необходимость в некоторых запро- сах на опрос SNMP.

Версии SNMP

Существует несколько версий SNMP, включая следующие:

SNMPv1 — простой протокол управления сетями, полноценный стандарт Интернета, опи- санный в документе RFC 1157.

SNMPv2c — описан в серии документов RFC 1901—1908; использует среду администриро- вания на базе строки сообщества.

SNMPv3 — обеспечивающий взаимодействие протокол на основе стандартов, первоначаль- но определённый в серии документов RFC 2273—2275; обеспечивает защищённый доступ к устройствам с помощью аутентификации и шифрования пакетов в сети. Данная версия протоко- ла включает следующие функции обеспечения безопасности: контроль целостности сообщений для защиты пакетов от искажения при пересылке; аутентификация для подтверждения досто- верности источника сообщения и шифрование для предотвращения прочтения содержимого со- общения несанкционированным источником.

В SNMPv1 и SNMPv2c используется модель безопасности на основе сообществ (community). Сообщество диспетчеров, имеющих доступ к базе MIB агента, определяется спис- ком контроля доступа и паролем.

В отличие от SNMPv1, версия SNMPv2c предусматривает механизм массового извлечения записей и более подробное информирование станций управления об ошибках. Механизм массо- вого извлечения получает таблицы и большие объёмы информации, сводя к минимуму затраты времени на двустороннее согласование. Усовершенствованная обработка ошибок в SNMPv2c

предусматривает расширенные коды ошибок для различных условий возникновения ошибок. Эти условия обозначаются одним кодом ошибки в SNMPv1. Коды возврата по ошибке в SNMPv2c включают тип ошибки.

Примечание. SNMPv1 и SNMPv2c включают минимальный набор средств обеспечения без- опасности. В частности, SNMPv1 и SNMPv2c не обеспечивают ни аутентификацию источника сообщения управления, ни шифрование. Наиболее обновлённое

описание версии SNMPv3 со- держится в серии документов RFC 3410—3415. В эту версию протокола добавлены методы обеспечения безопасной передачи наиболее важных данных между управляемыми устройства- ми.

SNMPv3 предусматривает как модели безопасности, так и уровни безопасности. Модель безопасности — это стратегия аутентификации, настроенная для пользователя и группы, в кото- рой данный пользователь находится. Уровень безопасности характеризует допустимую степень безопасности в модели. Сочетание уровня безопасности и модели безопасности определяет, ка- кой механизм безопасности будет использоваться при обработке пакета SNMP. Доступные мо- дели безопасности — SNMPv1, SNMPv2c и SNMPv3.

Сетевой администратор должен настроить агент SNMP для использования версии SNMP, поддерживаемой станцией управления. Поскольку агент может взаимодействовать с нескольки- ми диспетчерами SNMP, можно настраивать программное обеспечение для поддержки связи с помощью SNMPv1, SNMPv2c или SNMPv3.

6. Порядок выполнения работы

6.1 Собрать схему в соответствии с физической топологией, показанной на рис. 1.

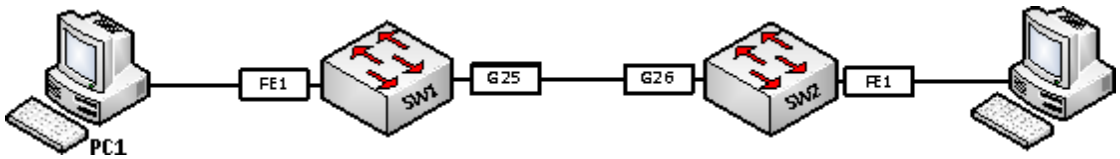


Рисунок 1. (FE1 – Порт Fast Ethernet 1, G25 – Порт Gigabit Ethernet 25).

6.2 Настроить адресацию сети в соответствии с диаграммой сетевого уровня, показанной нарис. 2. Коммутаторы предварительно настроены.

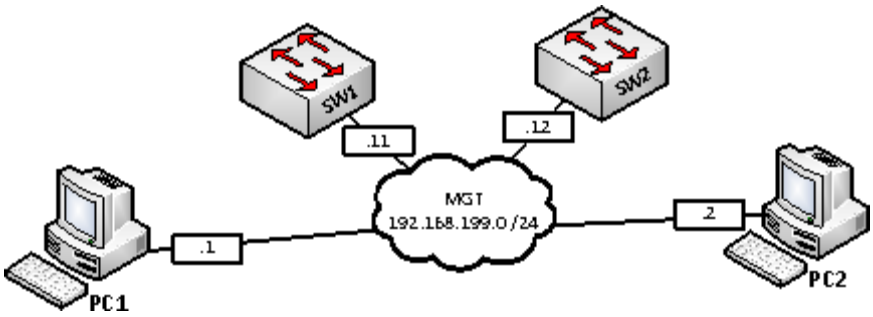


Рисунок 2. Сетевой уровень.

Все устройства в сети должны быть доступны, проверить командой «ping», например с

PC1 проверить связь до SW1 командой «ping 192.168.199.11», до SW2 командой «ping 192.168.199.12», до PC2 командой «ping 192.168.199.2», как показано на рис. 3.

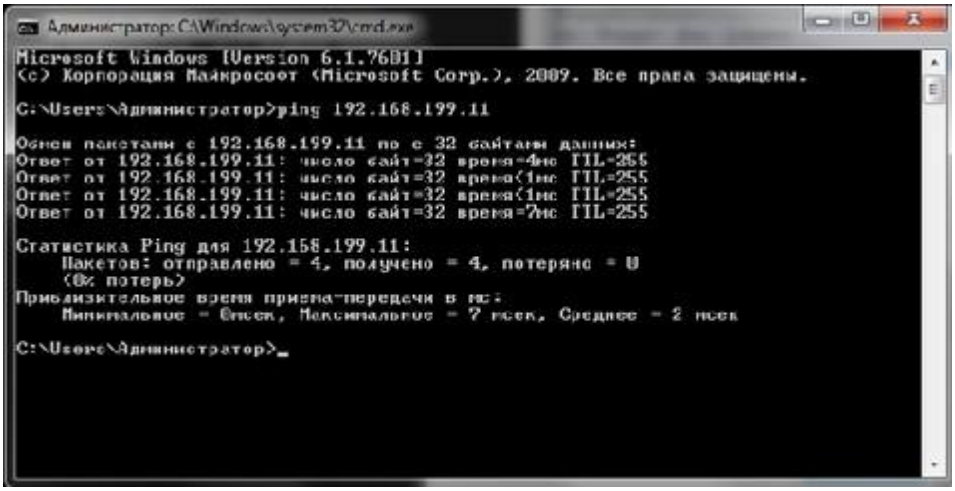
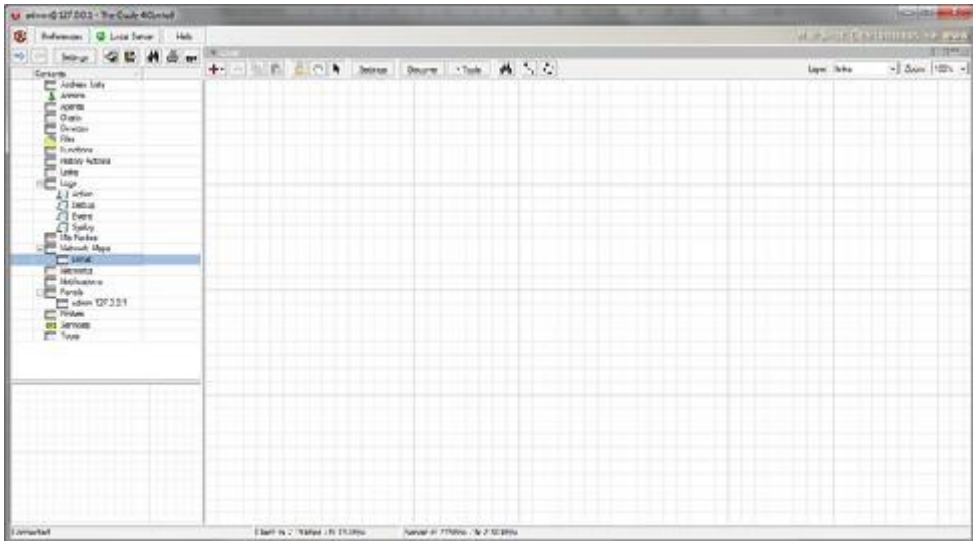
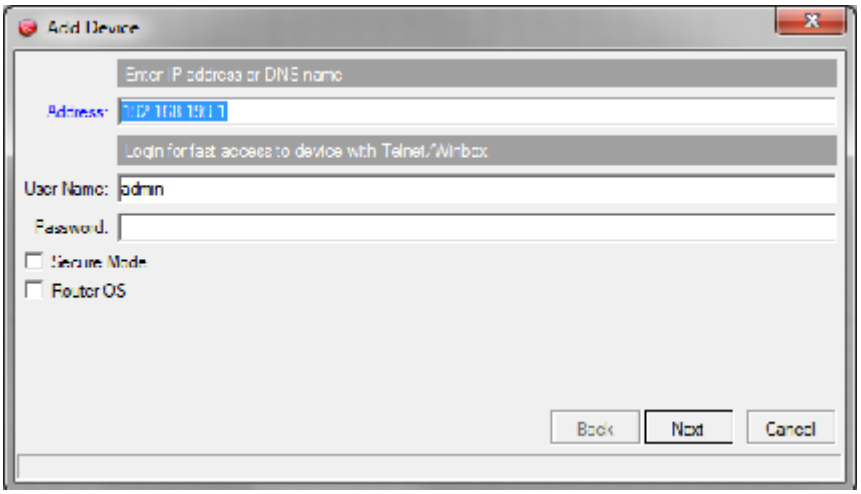


Рисунок 3. Результат проверки связи до SW1.

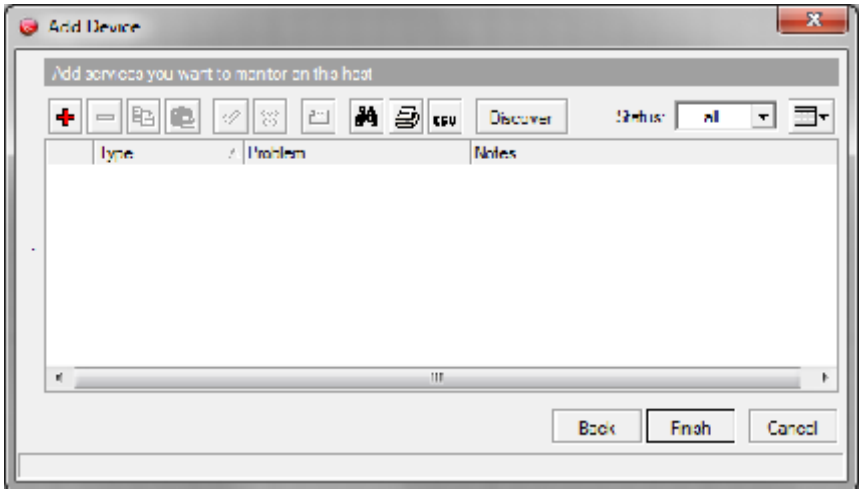
6.3. Произвести настройку SNMP сервера установленного на компьютере, для чего открытьпрограмму «The Dude», в слева в меню выбрать карту сети (Network Maps > Local).



Добавить устройства в соответствии с L1 диаграммой, изображенной на рис. 1. Для этого на панели инструментов нужно нажать красный плюс и выбрать пункт «Device», в открывшемся диалоговом окне ввести IP-адрес нужного устройства и нажать «Next».

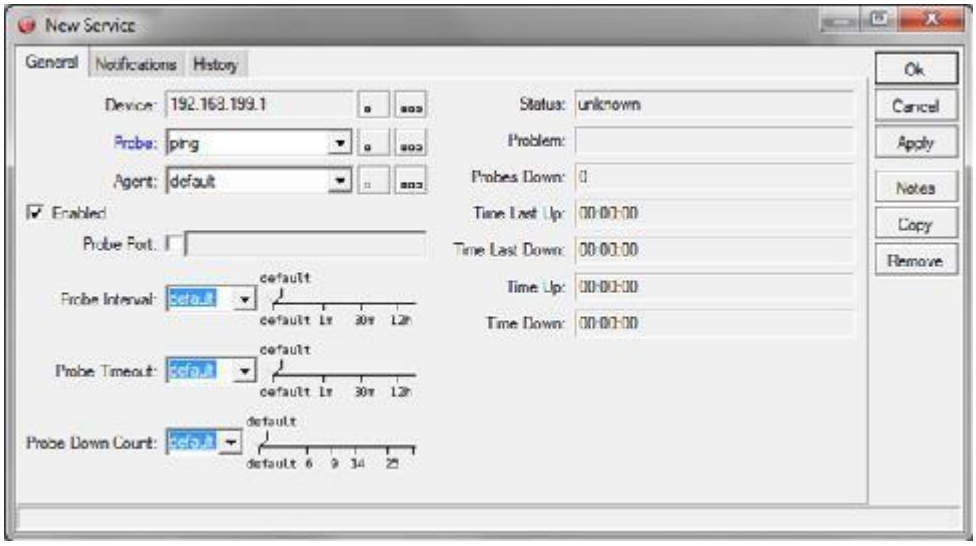


В открывшемся окне выбрать метод проверки работоспособности устройства, для этого нажать красный плюс.

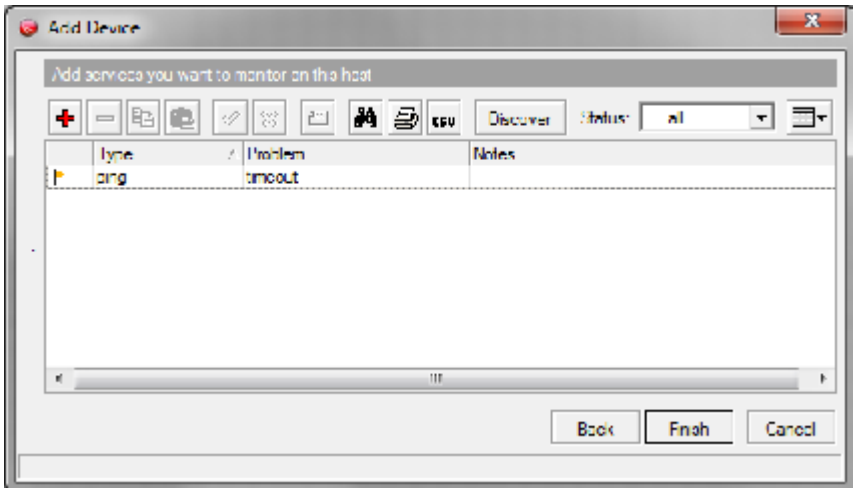


OK.

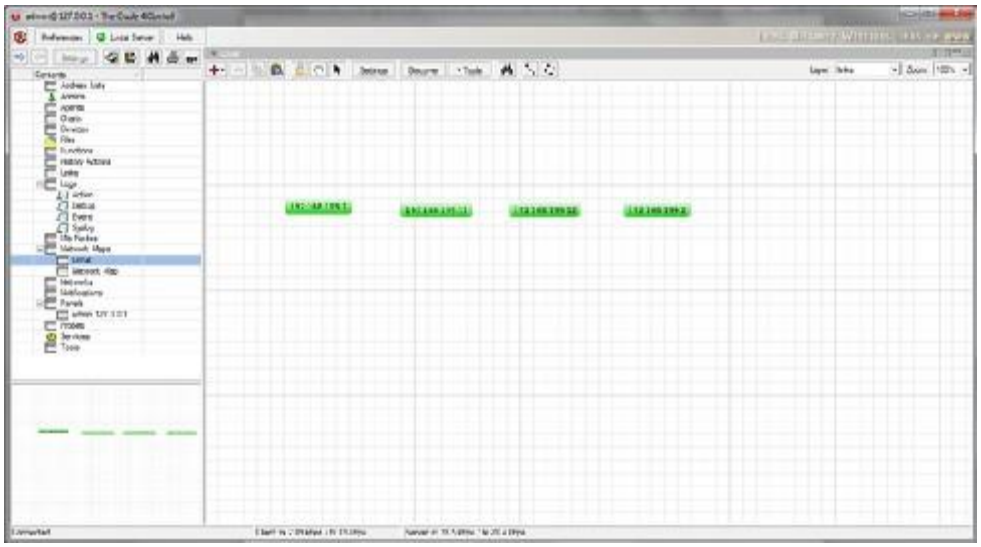
В открывшемся окне из выпадающего списка «Probe» выбрать тип «Ping» и нажать кнопку



Затем нажать кнопку «Finish».

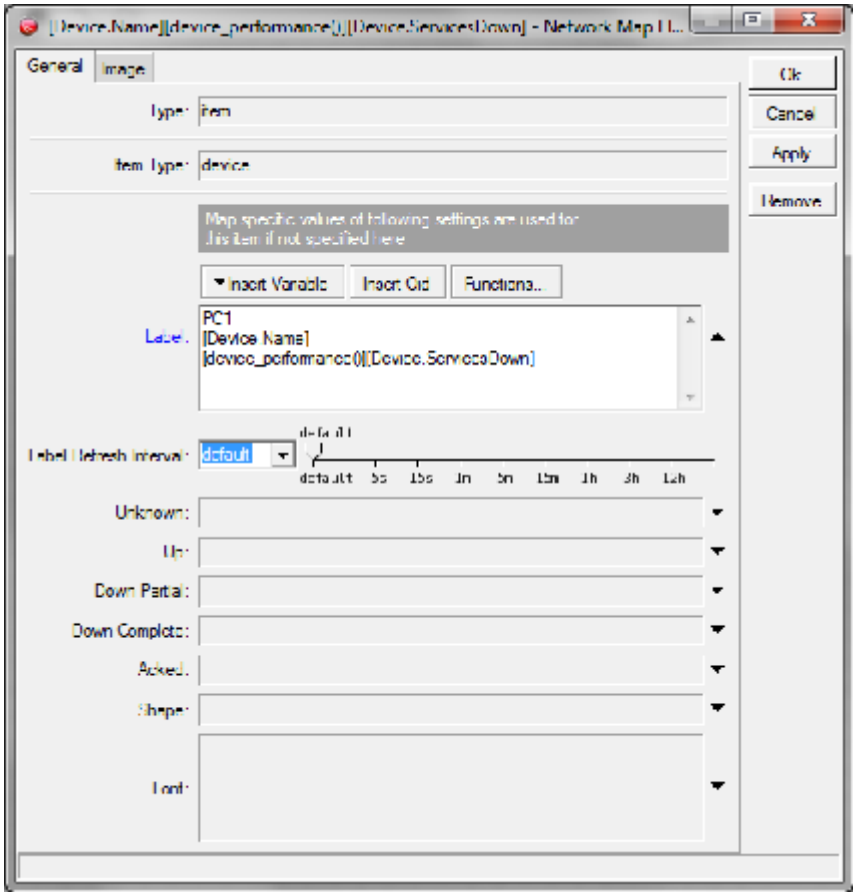


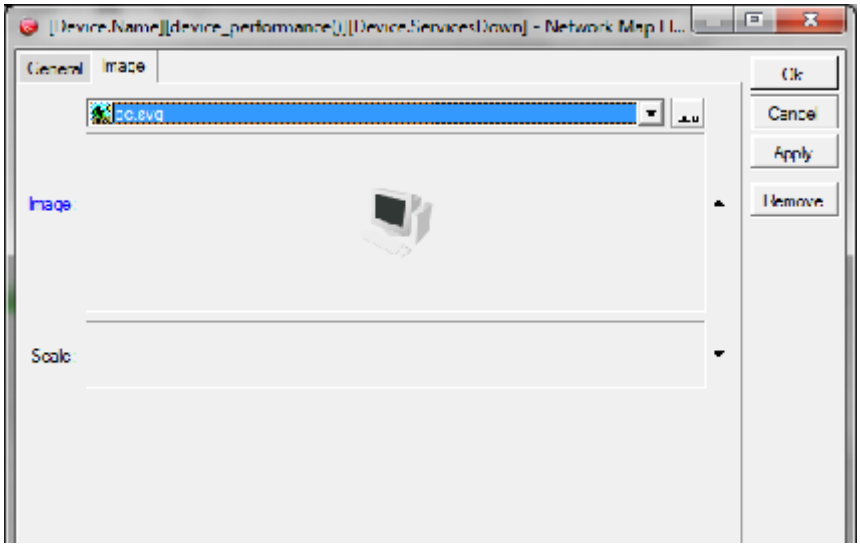
Аналогично добавить коммутаторы SW1, SW2 и PC2.



Производим настройку компьютеров, нажимаем правой кнопкой на PC1 из

контекстного меню выбираем «Appearance», в открывшемся окне во кладке «General», в поле «Lable» доба- вить имя PC1, а на вкладке «Image» из выпадающего списка выбрать «pc.svg» и нажать Ок.





Аналогично выполнить для PC2.

Произвести настройку коммутаторов, для этого на коммутаторе нажать правой кнопкой и выбрать пункт «Appearance», в открывшемся окне во вкладке «Image» из

выпадающего списка выбрать «switch.svg». Во вкладке «General» в поле «Lable», ввести параметры за которыми будет производится мониторинг по протоколу SNMP. Для примера следующие OID:

А. 1.3.6.1.2.1.1.1.0 – Запрос по протоколу SNMP на наименование модели устройства.

Б. 1.3.6.1.2.1.1.3.0 – Запрос времени работы устройства с момента последнего включенияили сбоя.

В. 1.3.6.1.4.1.171.12.1.1.6.1.0 – Запрос загрузки CPU коммутатора в процентах.

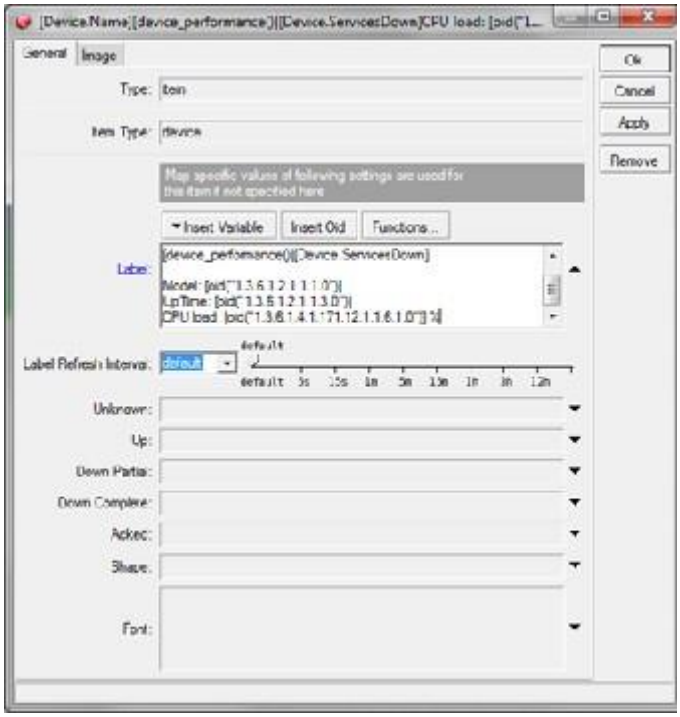
Пример формирования запроса: запрос к конкретному OID осуществляется строкой

«[oid("1.3.6.1.4.1.171.12.1.1.6.1.0")]», которая будет выводить значение загрузки CPU одним числом. Для того чтобы данный параметр был интуитивно понятен на создаваемой схеме можнонаписать следующую строку: «CPU load: [oid("1.3.6.1.4.1.171.12.1.1.6.1.0")] %».

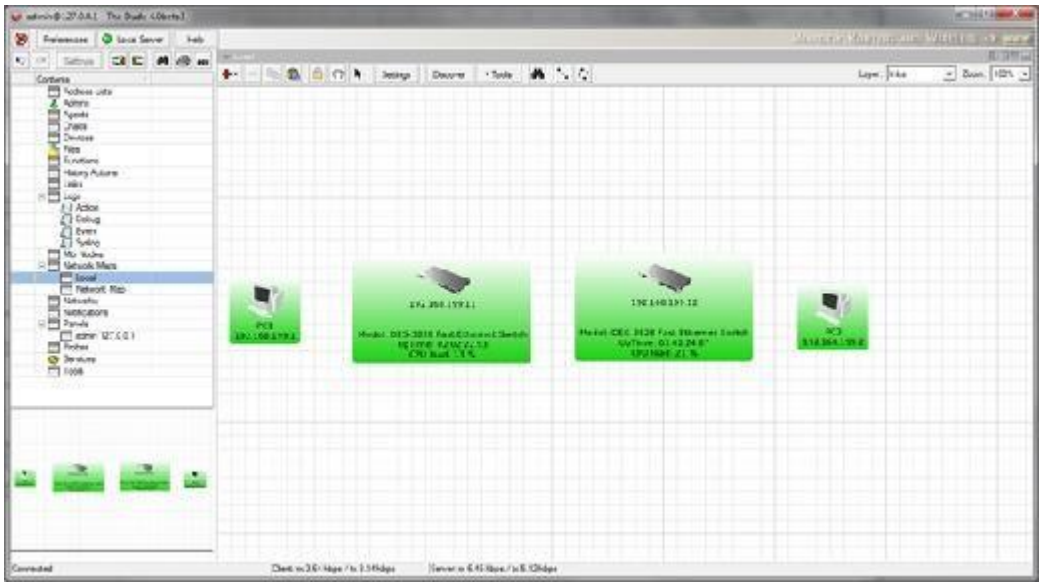
Все запросы могут выглядеть так:Model: [oid("1.3.6.1.2.1.1.1.0")]

UpTime: [oid("1.3.6.1.2.1.1.3.0")]

CPU load: [oid("1.3.6.1.4.1.171.12.1.1.6.1.0")] %



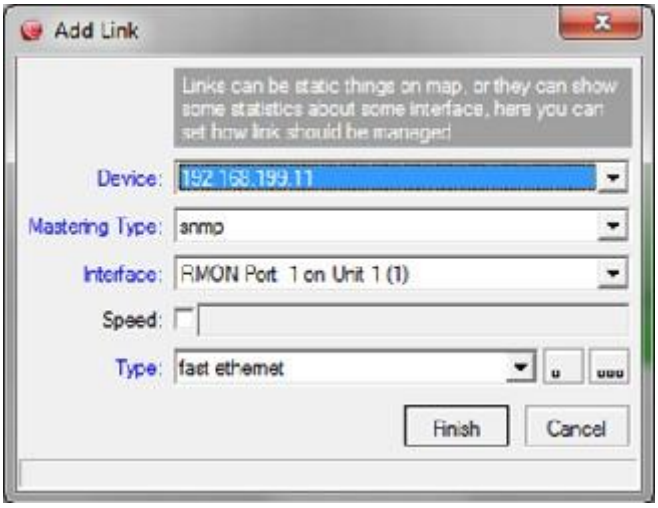
Затем нажать кнопку ОК и сделать аналогичное для коммутатора SW2.

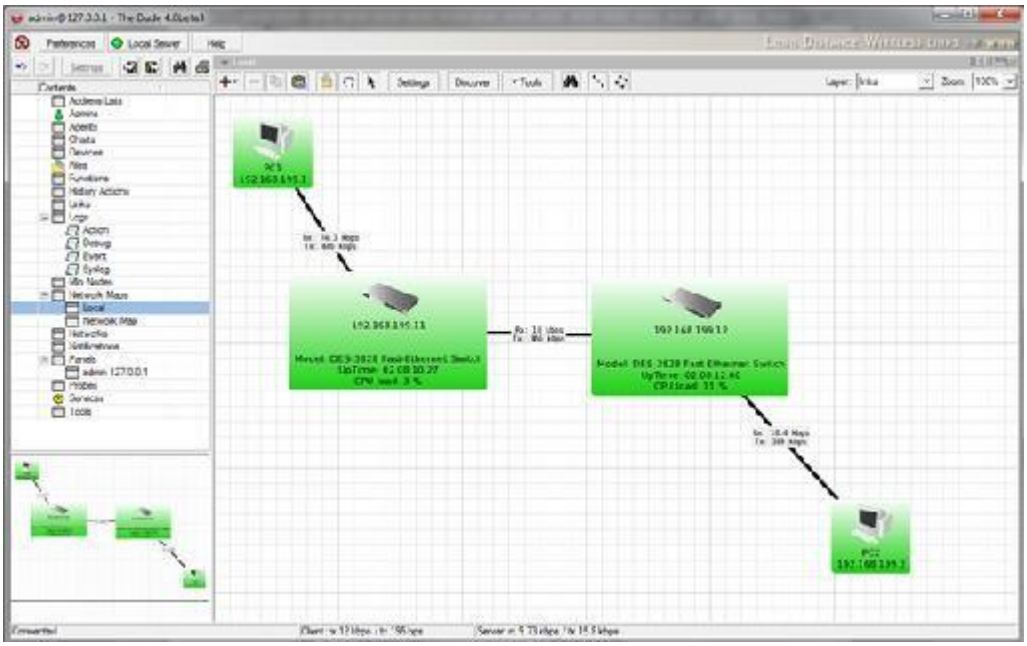


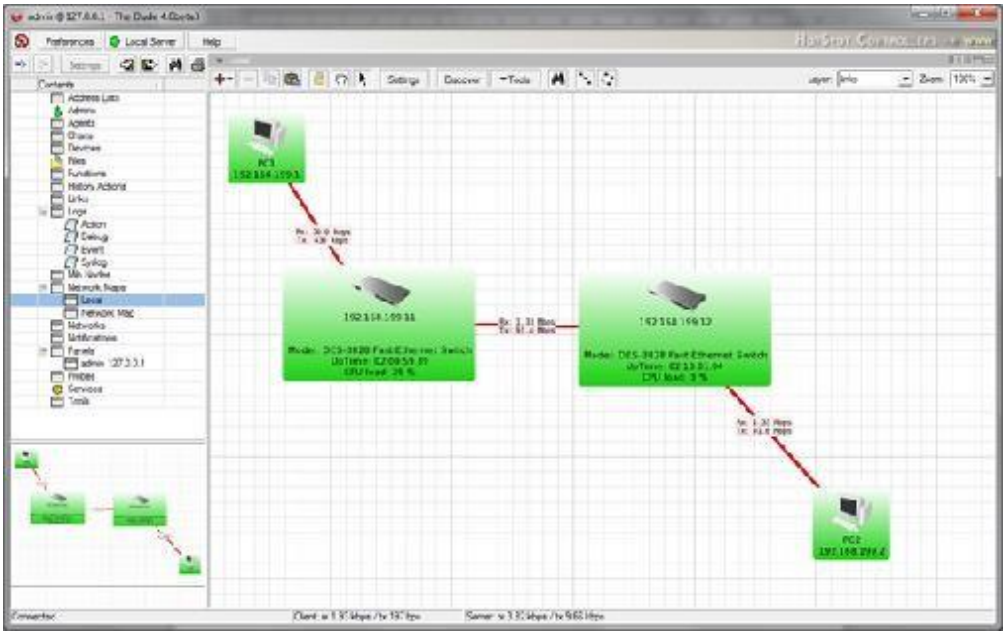
Настройка связей между устройствами. Для добавления связи необходимо нажать на крас- ный плюс, выбрать «Link» и провести между устройствами в открывшемся окне линию, выбрать параметры в соответствии с тем между какими устройствами настраивается связь. Например, если это связь между PC1 и SW, то необходимо выбрать Device – 192.168.199.11, Mastering Type

– snmp, Interface – RMON Port 1 on Unit 1 (1) , Type – Fast Ethernet, затем нажать кнопку

«Finish», аналогично добавить связи между SW1-SW2 и SW2-PC2.


Add Link
Links can be static things on map, or they can show some statistics about some interface, here you can set how link should be managed
Device:
192.168.199.11
Mastering Type:
snmp
Interface:
RMON Port 1 on Unit 1 (1)
Speed:
Type:
fast ethernet
Finish
Cancel



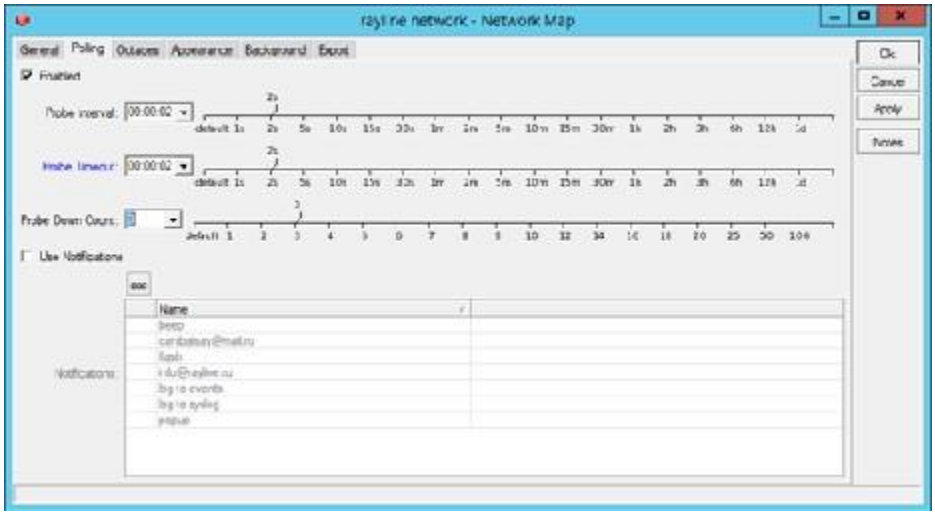


6.4 Проверка выполненной лабораторной работы**.**

1. За всеми устройствами, включенными в сеть, должен выполняться мониторинг, об этомдолжен свидетельствовать зеленый цвет устройств на карте сети.

2. Мониторинг вышедшего из строя оборудования – для проверки необходимо отключать кабель в разных участках сети и наблюдайте за картой сети, устройства до которых была потеряна связь будут отмечены красным, при возобновлении связи устройства станут опять зелеными. Если устройства не меняют свой цвет, то необходимо уменьшить время опроса оборудования, для этого зайдите в настройки (settings), затем на вкладке Polling выставите время опроса 2 секунды, как показано на рисунке. И затем повторно выполни- те проверку пункта

3. Между всеми устройствами должен осуществляться мониторинг пропускной способно- сти в реальном времени – об этом свидетельствуют цифры в килобит/с или мегабит/с на связях между устройствами. Для проверки работы запустите тест проверки скорости с компьютеров и наблюдайте за показаниями реальной скорости в системе мониторинга. При проверке скорости между PC1 и PC2 можно видеть изменение скорости в реальном времени, а также наблюдать изменение нагрузки на CPU коммутаторов.



4. Проверка времени работы с момента последнего запуска или сбоя (Uptime)– показывает сколько времени назад было включено устройство. Для проверки, запомните время Up- time на одном из устройств, затем перезагрузите устройство (отключите и подключите питание к коммутатору), после загрузки устройства убедитесь, что счетчик Uptime обну- лился и начался новый отсчет времени.

Практическая работа № 2

Основные характеристики протокола SNMP

Топология

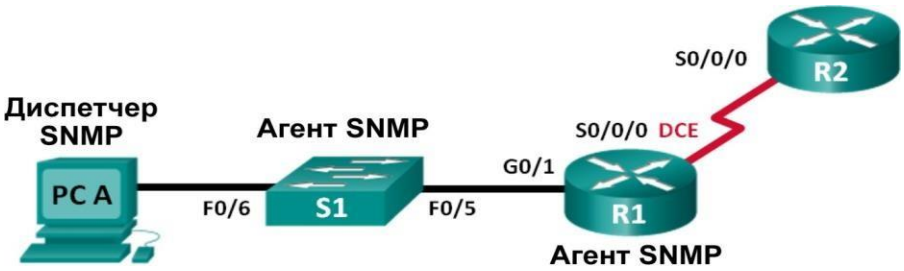


Таблица адресации

Устройство	**Интерфейс**	**IP-адрес**	**Маска подсе-ти**	**Шлюз по умолчанию**
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0	192.168.2.1	255.255.255.252	Недоступно
R2	S0/0/0	192.168.2.2	255.255.255.252	Недоступно
S1	VLAN 1	192.168.1.2	255.255.255.0	Недоступно
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

1. **Создание сети и настройка базовых параметров устройств**
2. **Настройка диспетчера и агентов SNMP**
3. **Преобразование кодов OID с использованием Cisco SNMP Object Navigator**

Исходные данные/сценарий

Протокол SNMP (Simple Network Management Protocol — простой протокол управления сетями)

— это протокол управления сетью и стандарт IETF, который может использоваться как для мо- ниторинга сети, так и для контроля клиентов в ней. SNMP может использоваться для получения и настройки переменных, связанных с состоянием и настройкой сетевых машин, таких как маршрутизаторы и коммутаторы, а также клиентские компьютеры сети. Диспетчер SNMP мо- жет опрашивать агенты SNMP для получения данных, либо данные могут автоматически от- правляться на диспетчер SNMP путём настройки ловушек на агентах SNMP.

В этой лабораторной работе вы будете должны загрузить, установить и настроить

программное обеспечение для управления SNMP с на компьютере ПК A. Вы также настроите маршрутизатор Cisco и коммутатор Cisco в качестве агентов SNMP. После получения сообщений с уведомлени-ем SNMP от агента SNMP вы должны будете преобразовать коды MIB/ID объекта (OID), чтобы получить подробную информацию данных сообщений с помощью Cisco SNMP Object Navigator. **Примечание**. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, а также других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интер- фейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной рабо-ты.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удале- ны и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору. **Примечание**. Применение команд **snmp-server** в этой лабораторной работе приведёт к тому, что коммутатор Cisco 2960 сгенерирует сообщение с предупреждением при сохранении файла настройки в NVRAM. Чтобы избежать этого сообщения с предупреждением, убедитесь, что коммутатор использует шаблон **lanbase-routing**. Шаблон IOS контролируется диспетчером базы данных коммутатора (SDM). При изменении предпочтительного шаблона новый шаблон будет использоваться после перезагрузки, даже если настройка не сохраняется.

S1# **show sdm prefer**

Используйте следующие команды для назначения шаблона **lanbase-routing** в качестве шаблонаSDM по умолчанию.

S1# **configure terminal**

S1(config)# **sdm prefer lanbase-routing** S1(config)# **end** S1# **reload Необходимые ресурсы:**

2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) илианалогичная модель);

1 коммутатор (Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образlanbasek9 или аналогичный);

1 ПК (с Windows 7, Vista или XP с программой эмуляции терминала, например Tera

Term);1 ПК (с Windows 7, Vista или XP с доступом к Интернету);

консольные кабели для настройки устройств Cisco IOS через порты консоли; кабели Ethernet и последовательные кабели в соответствии с топологией.

ПО для управления протоколом SNMP (PowerSNMP Free Manager компании Dart Communications или сервер Syslog SolarWinds Kiwi, ознакомительная версия с испытательнымпериодом 30 дней)

Часть 1: Построение сети и базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и сделать базовую настройку устройств.

Шаг 1: Подключите кабели в сети в соответствии с топологией.Шаг 2: Настройте компьютер.

Шаг 3: Инициализируйте и перезагрузите коммутатор и маршрутизаторы при необходи-мости.

Шаг 4: Произведите базовую настройку маршрутизаторов и коммутатора. a. Отключитепоиск DNS.

Настройте имена устройств в соответствии с топологией. Настройте IP-адреса в соответствии с таблицей адресации

Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйтеучётную запись.

Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд. Проверьте подключения между устройствами локальной сети с помощью команды ping.

Скопируйте текущую конфигурацию в файл загрузочной конфигурации. Часть 2: Настройка диспетчера и агентов SNMP

В части 2 вы должны будете установить ПО для управления SNMP и настроить его на ПК A, атакже настроить R1 и S1 в качестве агентов SNMP.

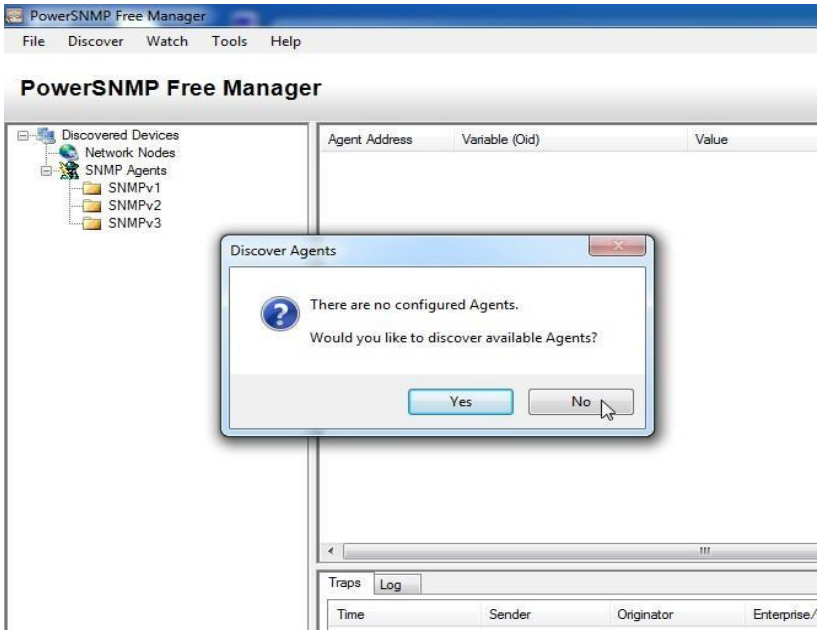
Шаг 1: Установите программу управления SNMP.

Загрузите и установите бесплатное приложение PowerSNMP Free Manager от компании Dart Communications, перейдя по следующему URL-адресу: http://www.dart.com/snmp-free- manager.aspx.

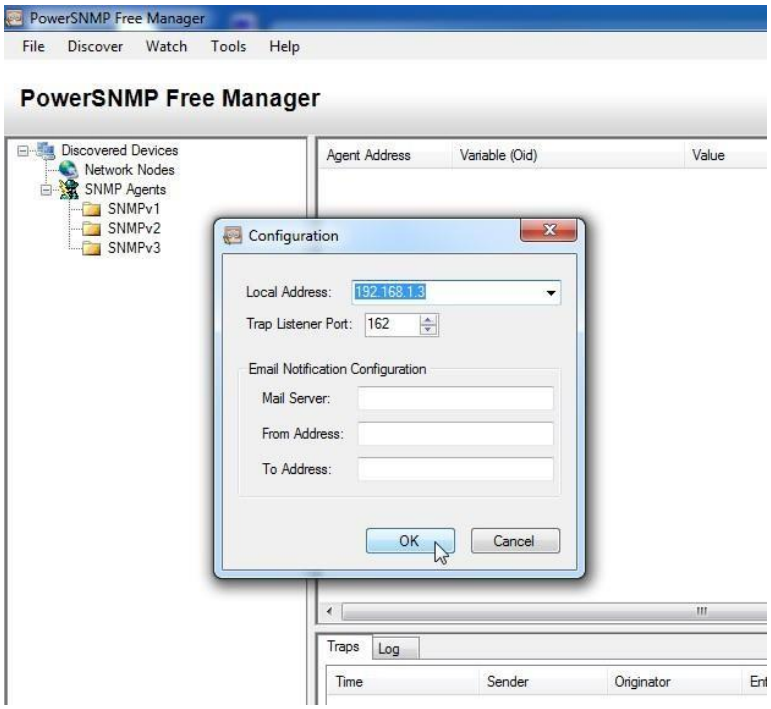
Запустите программу PowerSNMP Free Manager.

При отображении запроса на поиск доступных агентов SNMP нажмите кнопку **No**

(Нет). Поиск агентов SNMP осуществляется после настройки SNMP на маршрутизаторе R1. PowerSNMP Free Manager поддерживает SNMP версии 1, 2, и 3. В данной лабораторной работе используется SNMPv2.



Во всплывающем окне настройки (если всплывающее окно не отображается, перейдите во вкладку Tools > Configuration (Инструменты > Настройка)) назначьте локальный IP-адрес дляпрослушивания на 192.168.1.3 и нажмите **OK**.



Примечание. При отображении запроса на поиск доступных агентов SNMP нажмите кнопку **No**

и перейдите к следующему части данной лабораторной работы.

Шаг 2: Настройте агент SNMP.

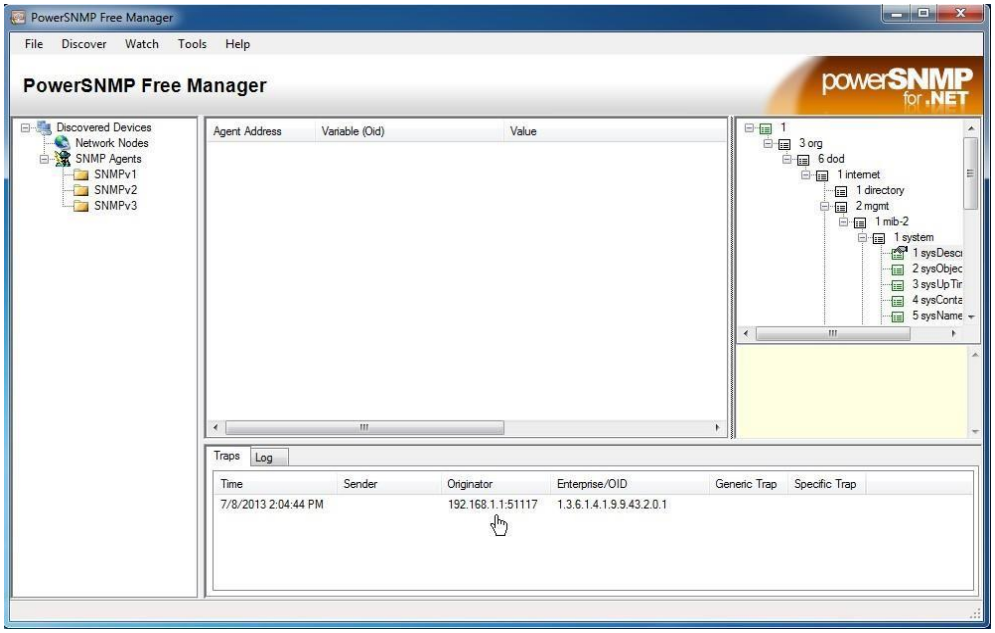
На маршрутизаторе R1 введите следующие команды в режиме глобальной конфигурации, чтобы настроить его в качестве агента SNMP. В строке 1 ниже строкой сообщества SNMP является **ciscolab** с правами только для чтения, а именованный список доступа SNMP_ACL определяет, какие узлы могут получать данные SNMP от маршрутизатора R1. В строках 2 и 3 команды ме- стоположения и контактной информации агента SNMP предоставляют описательную контакт- ную информацию. В строке 4 указаны IP-адрес узла, который будет получать уведомления SNMP, версия SNMP и строка сообщества. Строка 5 включает все ловушки SNMP по умолча- нию; строки 6 и 7 создают именованный список контроля доступа, определяющий, каким узлам разрешено получение информации SNMP от маршрутизатора.

R1(config)# **snmp-server community ciscolab ro SNMP_ACL** R1(config)# **snmp-server location snmp_manager** R1(config)# **snmp-server contact ciscolab_admin**

R1(config)# **snmp-server host 192.168.1.3 version 2c ciscolab**

R1(config)# **snmp-server enable traps** R1(config)# **ip access-list standard SNMP_ACL**R1(config-std-nacl)# **permit 192.168.1.3**

На этом этапе можно заметить, что PowerSNMP Free Manager получает уведомления от маршру- тизатора R1. Если уведомления не приходят, вы можете попытаться принудительно установить отправку уведомления SNMP, введя команду **copy run start** на маршрутизаторе R1. Если вам не удаётся это сделать, перейдите к следующему шагу.

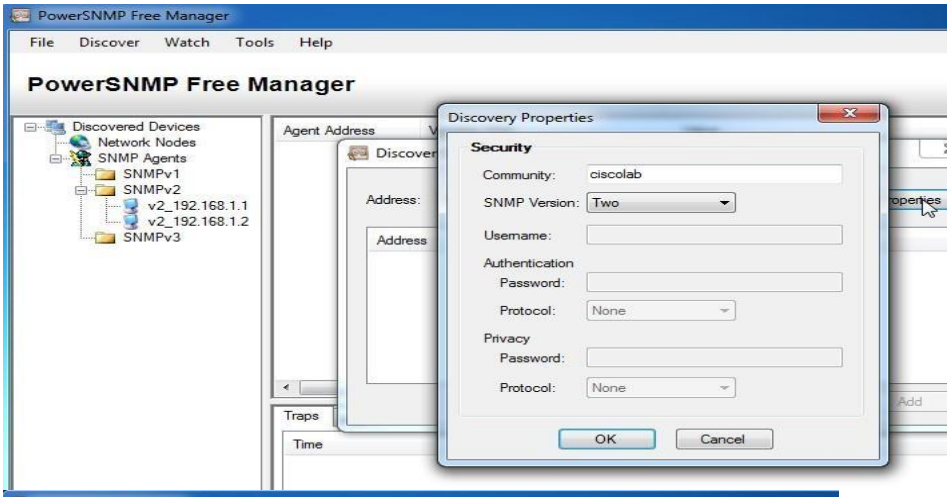


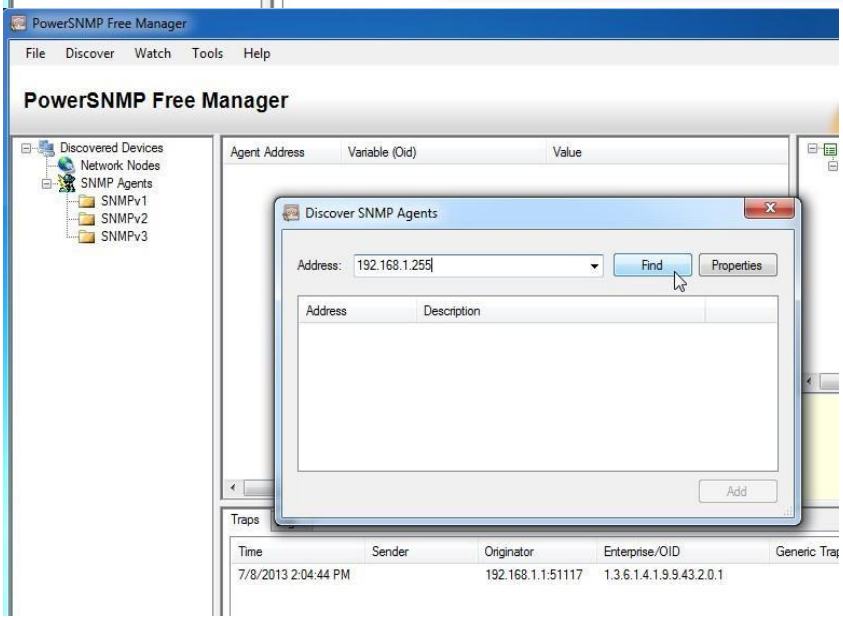
Шаг 3: Выполните обнаружение агентов SNMP.

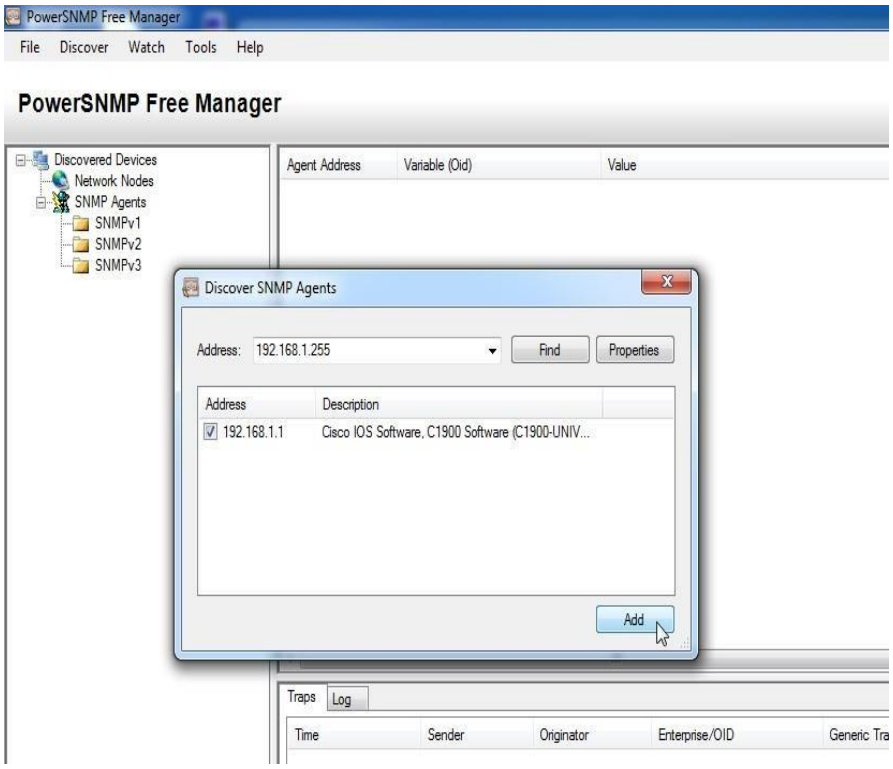
В программе PowerSNMP Free Manager на компьютере ПК A откройте окно **Discover > SNMP Agents** (Обнаружение > Агенты SNMP). Введите IP-адрес **192.168.1.255**. В том же окне щёлкни-те

Properties (Свойства) и выберите в поле «Community» (Сообщество) параметр **ciscolab**, а в поле

«SNMP Version» параметр **Two** (2), затем щёлкните **OK**. Теперь можете нажать **Find** (Найти) для обнаружения всех агентов SNMP в сети 192.168.1.0. Программа PowerSNMP Free Manager должна обнаружить маршрутизатор R1 по адресу 192.168.1.1. Установите флажок и щёлкните **Add** (Добавить), чтобы добавить маршрутизатор R1 в качестве агента SNMP.

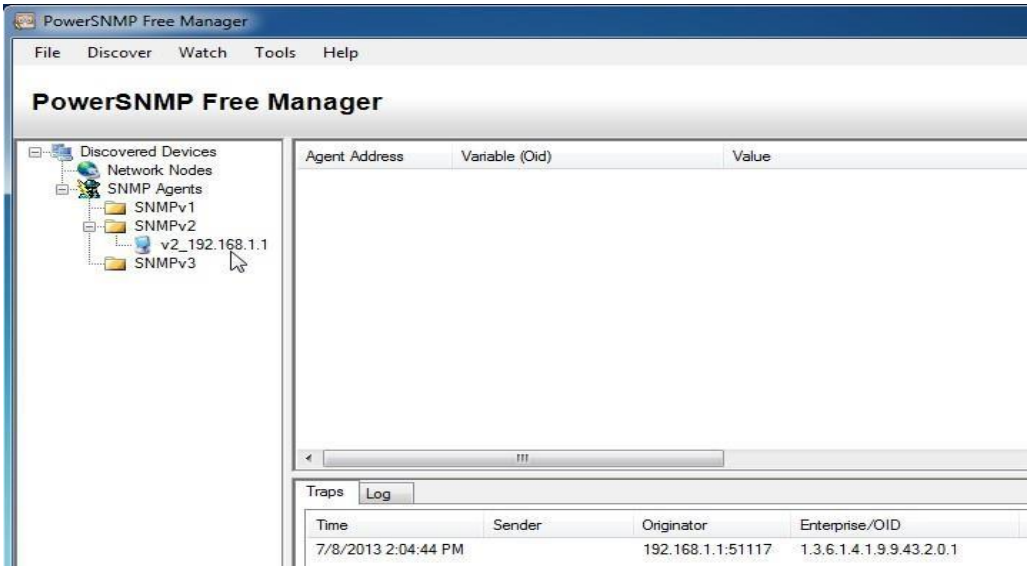






В программе PowerSNMP Free Manager маршрутизатор R1 добавляется в список

доступныхагентов SNMPv2.



Настройте коммутатор S1 в качестве агента SNMP. Вы можете использовать те же команды

snmpserver, которые вы использовали для настройки R1.

После завершения настройки коммутатора S1 уведомления SNMP с адреса 192.168.1.2 отобра- жаются в окне «Traps» (Прерывания) программы PowerSNMP Free Manager. В программе PowerSNMP Free Manager добавьте коммутатор S1 в качестве агента SNMP с помощью тех жедействий, которые вы выполнили для обнаружения R1.

Часть 3: Преобразование кодов OID с использованием Cisco SNMP Object Navigator

В части 3 принудительно установите отправку уведомлений SNMP на диспетчер SNMP, разме-щенный на компьютере ПК A. После этого вы должны будете преобразовать полученные коды

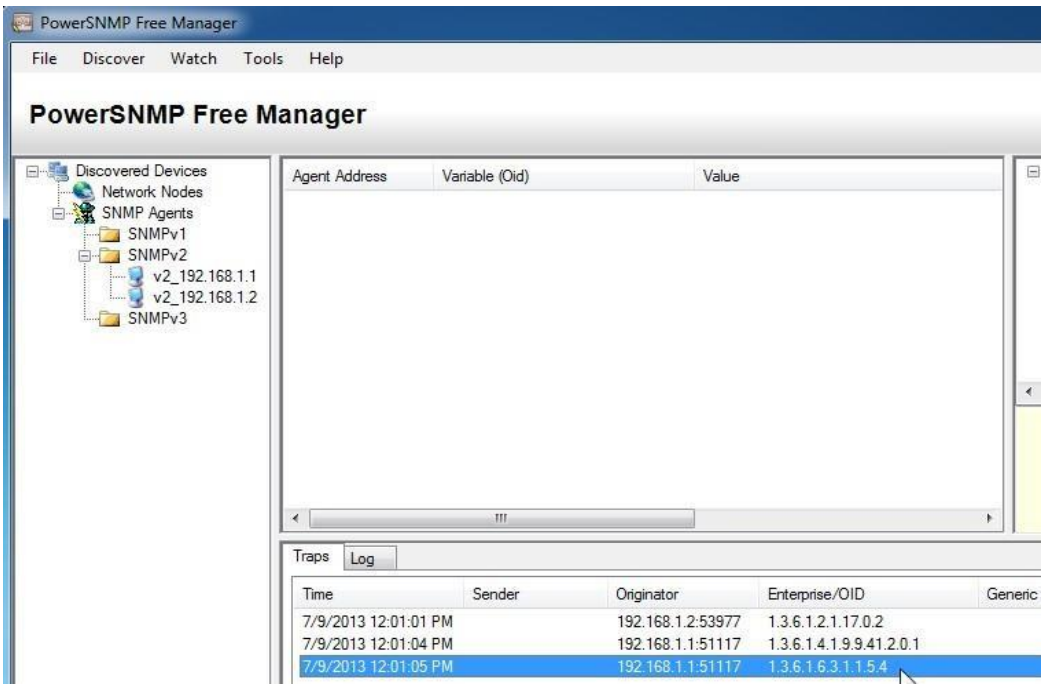
OID в имена, чтобы прочитать сообщения. Коды MIB/OID можно легко преобразовать с помо- щью средства Cisco SNMP Object Navigator на веб-сайте http://www.cisco.com.

Шаг 1: Удалите текущие сообщения SNMP.

В программе PowerSNMP Free Manager щёлкните правой кнопкой мыши окно **Traps** (Ловушки)и выберите **Clear** (Очистить) для удаления сообщений SNMP.

Шаг 2: Создайте ловушку и уведомление SNMP.

На маршрутизаторе R1 настройте интерфейс S0/0/0 согласно таблице адресации в начале данной лабораторной работы. Перейдите в режим глобальной конфигурации и разрешите интерфейсу отправлять уведомления, создаваемые в случае ловушки SNMP, на диспетчер SNMP на компью-тере ПК A. Запомните коды организации/OID, отображаемые в окне ловушек.

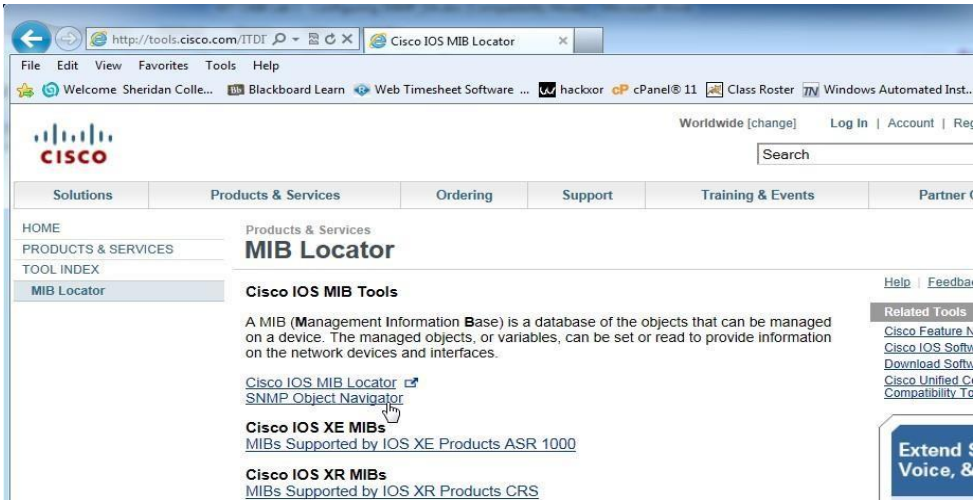


Шаг 3: Декодируйте сообщения MIB/OID SNMP.

На компьютере с доступом к Интернету откройте веб-браузер и перейдите на веб-сайтhttp://www.cisco.com.

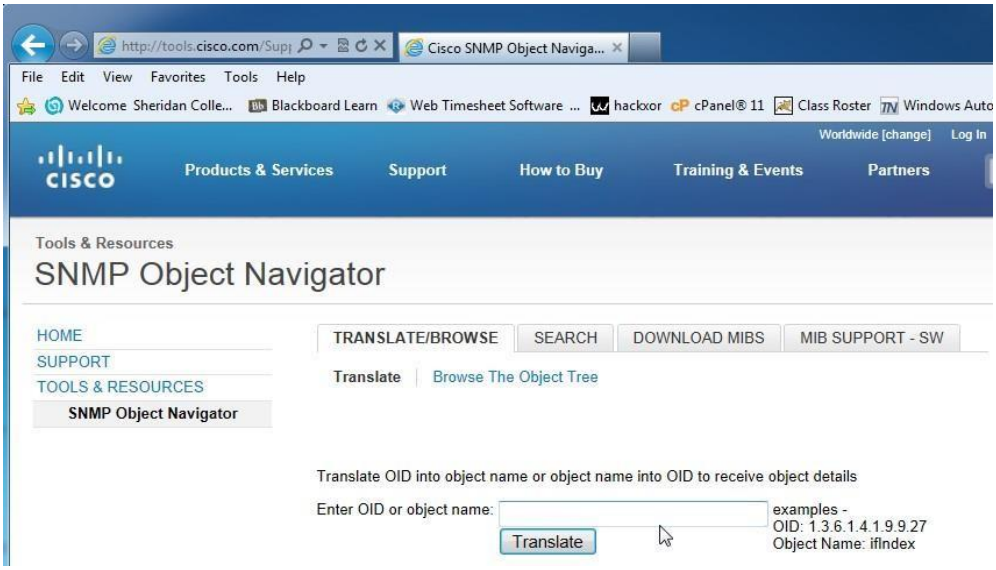
С помощью средства поиска в верхней части окна выполните поиск **SNMP Object Navigator**. Выберите в результатах **SNMP Object Navigator MIB Download MIBs OID OIDs**.

Перейдите на страницу **MIB Locator**. Выберите **SNMP Object Navigator**.



На странице **SNMP Object Navigator** выполните декодирование кода OID из программы

PowerSNMP Free Manager, который был создан в действии 2 части 3 данной лабораторной рабо-ты. Введите код OID и выберите **Translate** (Преобразовать).



Запишите коды OID и соответствующие им сообщения, полученные в результате преоб-разования, ниже.

Вопросы на закрепление

Перечислите несколько потенциальных преимуществ наблюдения за сетью с помощьюпротокола SNMP.

Почему при работе с SNMPv2 предпочтительно использовать исключительно доступ справами только для чтения?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель марш-рутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфей-сы с целью определения типа маршрутизатора и количества имеющихся на нём интер- фейсов. Эффективного способа перечисления всех сочетаний настроек для каждого клас- са маршрутизаторов не существует.

В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последо-вательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В ка-честве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления ин терфейса

Третья неделя практики

Практическая работа № 1

Задачи управления: анализ производительности сети

Задание 1. Получение справочной информации по командам.

Выведите на экран справочную информацию по всем рассмотренным утилитам.

Для этого в командной строке введите имя утилиты без параметров и дополните **/?**.

Сохраните справочную информацию в отдельном файле. Изучите ключи, используемые при запуске утилит.

Задание 2. Получение имени хоста.

Выведите на экран имя локального хоста с помощью команды hostname.

Сохраните результат в отдельном файле.

Задание 3. Изучение утилиты ipconfig.

Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполнитетаблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

Задание 4. Тестирование связи с помощью утилиты ping.

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.

2. Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.

3. Проверьте возможность установления соединения с удаленным хостом.

4. С помощью команды ping проверьте адреса (взять из списка локальных ресурсов на сайте aspu.ru) и для каждого из них отметьте время отклика. Попробуйте изменить

параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

Задание 5. Определение пути IP-пакета.

С помощью команды tracert проверьте для перечисленных ниже адресов, черезкакие промежуточные узлы идет сигнал. Изучите ключи команды.

a) aspu.ru

b) mathmod.aspu.ru

c) yarus.aspu.ru

Задание 6: Просмотр ARP-кэша.

С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.Внести в кэш локального компьютера любую статическую запись.

Задание 7: Просмотр локальной таблицы маршрутизации.

С помощью утилиты route просмотрите локальную таблицу маршрутизации.

Задание 8. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы:

1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут, маска сети, авторитетный/неавторитетный (компетентный) DNS-сервер, порт TCP, петля обратной связи, время отклика.
2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
3. Каким образом команда ping проверяет соединение с удаленным хостом?
4. Каково назначение протокола ARP?
5. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
6. Какие могут быть причины неудачного завершения ping и tracert? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни при передаче пакета).
7. Всегда ли можно узнать символьное имя узла по его ip-адресу?
8. Какой тип записи запрашивает у DNS-сервера простейшая форма nslookup?

Практическая работа № 2

Задачи управления: анализ надежности сети

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсе-ти	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка базовых мер безопасности на маршрутизаторе Часть 3. Настройка базовых мер безопасности на коммутаторе Общие сведения/сценарий

Все сетевые устройства рекомендуется настраивать с использованием хотя бы мини- мального набора эффективных команд обеспечения безопасности. Это относится к устройствам конечных пользователей, серверам и сетевым устройствам, таким как маршрутизаторы и коммутаторы.

В ходе лабораторной работы вы должны будете настроить сетевые устройства в тополо- гии таким образом, чтобы разрешать SSH-соединения для удаленного управления. Кроме того, вы должны будете настроить основные эффективные меры обеспечения безопасно- сти через интерфейс командной строки операционной системы Cisco IOS. Затем вам необходимо будет протестировать меры обеспечения безопасности и убедиться в том, что они правильно внедрены и работают без ошибок.

Примечание. В практических лабораторных работах CCNA используются маршрутиза- торы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные

идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лаборатор- ной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удаленаначальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

1 маршрутизатор (Cisco 1941 с ПО Cisco IOS версии 15.2(4)M3 с универсальным образомили аналогичная модель)

1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или анало-гичная модель)

1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например,Tera Term)

Консольные кабели для настройки устройств Cisco IOS через консольные порты Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров устройств

В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на устройствах.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, показанные в топологии, и кабели соответствующим образом. **Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.Шаг 3: Выполните настройку маршрутизатора и коммутатора.**

Подключитесь к устройству с помощью консольного подключения и активируйте при-вилегированный режим EXEC.

Назначьте устройству имя в соответствии с таблицей адресации.

Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобра- зовывать введенные команды таким образом, как будто они являются именами узлов.

Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.

Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.

Создайте баннер с предупреждением о запрете несанкционированного доступа к устрой-ству.

Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию,приведенную в таблице адресации.

Задайте для используемого по умолчанию интерфейса SVI сведения об IP-адресе соглас-но таблице адресации.

Сохраните текущую конфигурацию в файл загрузочной конфигурации. Часть 2: Настройка базовых мер безопасности на маршрутизаторе **Шаг 1: Зашифруйте открытые пароли.**

R1(config)# **service password-encryption**

Шаг 2: Установите более надежные пароли.

Администратор должен следить за тем, чтобы пароли отвечали стандартным рекоменда- циям по созданию надежных паролей. В рекомендациях должны быть определены соче-тания в пароле букв, цифр и специальных символов и его минимальная длина.

Примечание. Согласно данным рекомендациям по лучшим практическим методикам надежные пароли, примеры которых приведены в этой лабораторной работе, необходимо всегда использовать в реальной работе. Однако для упрощения выполнения работы в остальных лабораторных работах данного курса используются пароли cisco и class.

Измените зашифрованный пароль привилегированного режима EXEC в соответствии срекомендациями.

R1(config)# **enable secret Enablep@55**

Установите минимальную длину 10 символов для всех паролей. R1(config)# **securitypasswords min-length 10**

Шаг 3: Разрешите подключения по протоколу SSH.

В качестве имени домена укажите **CCNA-lab.com**. R1(config)# **ip domain-name CCNA-lab.com**

Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к маршрутизатору через SSH. Пароль должен соответствовать стан- дартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий не задан в команде, то пользователь по умолчанию будет иметь пра-ва доступа EXEC (уровень 15).

R1(config)# **username SSHadmin privilege 15 secret Admin1p@55**

Настройте транспортный вход для линий VTY таким образом, чтобы они могли разре-шать подключения по протоколу SSH, но не разрешали подключения по протоколу Telnet.

R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh**

Аутентификация на линиях VTY должна выполняться с использованием базы данныхлокальных пользователей.

R1(config-line)# **login local**

R1(config-line)# **exit**

Создайте ключ шифрования RSA с длиной 1024 бит. R1(config)# **crypto key generate rsa modulus 1024 Шаг 4: Обеспечьте защиту консоли и линий VTY.**

Маршрутизатор можно настроить таким образом, чтобы он завершал сеанс подключения в случае отсутствия активности в течение заданного времени. Если сетевой администра- тор вошел в систему сетевого устройства, а потом был внезапно вынужден покинуть ра- бочее место, то по истечении установленного времени эта команда автоматически за- вершит сеанс подключения. Приведенные ниже команды обеспечивают закрытие сеанса линии связи через пять минут отсутствия активности.

R1(config)# **line console 0**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **line vty 0 4**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **exit**

R1(config)#

Команда, приведенная ниже, не разрешает вход в систему с использованием метода пол- ного перебора. Маршрутизатор блокирует попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введен неверный пароль. Низкое значение этого тай- мера установлено специально для данной лабораторной работы.

R1(config)# **login block-for 30 attempts 2 within 120** Что означает **2 within 120** в приве-денной выше команде?

_ неудачные попытки в течение 120 секунд

Что означает **block-for 30** в приведенной выше команде? заблокировать на 30 секунд

Шаг 5: Убедитесь, что все неиспользуемые порты отключены.

Порты маршрутизатора отключены по умолчанию, однако рекомендуется лишний раз убедиться, что все неиспользуемые порты отключены администратором. Для этого мож-но воспользоваться командой **show ip interface brief**. Все неиспользуемые порты, не от-ключенные администратором, необходимо отключить с помощью команды **shutdown** в режиме конфигурации интерфейса.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES NVRAM administratively down downGigabitEthernet0/0 unassigned YES NVRAM

administratively down down GigabitEthernet0/1 192.168.1.1 YES manual up up

Serial0/0/0 unassigned YES NVRAM administratively down down Serial0/0/1unassigned YES NVRAM administratively down down R1#

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколуTelnet.

Разрешает ли R1 подключение по протоколу Telnet? Дайте пояснение.Нет, Telnet не был активирован во время настройки маршрутизатора.

С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколуSSH.

Разрешает ли R1 подключение по протоколу SSH?_____Да.

Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли за-блокирован доступ к системе после двух неудачных попыток.

Что произошло после ввода неправильных данных для входа в систему во второй раз?Маршрутизатор отклоняет входящие соединения по протоколу SSH.

Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду **show login**, чтобы проверить состояние входа в систему. В приведенном ниже примере коман-да **show login** была введена в течение 30-секундной блокировки доступа к системе и по- казывает, что маршрутизатор находится в режиме Quiet. Маршрутизатор не будет раз- решать попытки входа в систему в течение еще 14 секунд.

R1# **show login**

A default login delay of 1 second is applied.

No Quiet-Mode access list has been configured. Router enabled to watch for login Attacks.

If more than 2 login failures occur in 120 seconds or less, logins will be disabled for 30 seconds.

Router presently in Quiet-Mode.

Will remain in Quiet-Mode for 14 seconds.Denying logins from all sources.

R1#

По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и вой-дите в систему, используя имя **SSHadmin** и пароль **Admin1p@55**.

Что отобразилось после успешного входа в систему? Баннер MOTD и интерпретатор

Войдите в привилегированный режим EXEC и введите в качестве пароля

Enablep@55.Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачныхпопыток в течение 120 секунд? Дайте пояснение.

Нет, так как login block-for защищает вход в консоль, а не в _ привилегированный режимEXEC.

Введите команду **show running-config** в строке приглашения привилегированного режи-ма EXEC для просмотра установленных параметров безопасности.

Часть 3: Настройка базовых мер безопасности на коммутаторе

Шаг 1: Зашифруйте открытые пароли.

S1(config)# **service password-encryption**

Шаг 2: Установите более надежные пароли на коммутаторе.

Измените зашифрованный пароль привилегированного режима EXEC в соответствии срекомендациями по установке надежного пароля.

S1(config)# **enable secret Enablep@55**

Примечание. Команда безопасности **password min-length** на коммутаторах модели 2960недоступна.

Шаг 3: Разрешите подключения по протоколу SSH.

В качестве имени домена укажите **CCNA-lab.com**. S1(config)# **ip domain-name CCNA-lab.com**

Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к коммутатору через SSH. Пароль должен соответствовать стандартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий не задан в команде, то пользователь по умолчанию будет иметь права досту-па EXEC (уровень 1).

S1(config)# **username SSHadmin privilege 1 secret Admin1p@55**

Настройте транспортный вход для линий VTY таким образом, чтобы они могли разре-шать подключения по протоколу SSH, но не разрешали подключения по протоколу Telnet.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh**

Аутентификация на линиях VTY должна выполняться с использованием базы данныхлокальных пользователей.

S1(config-line)# **login local**

S1(config-line)# **exit**

Создайте ключ шифрования RSA с длиной 1024 бит. S1(config)# **crypto key generate rsa modulus 1024 Шаг 4: Обеспечьте защиту консоли и линий VTY.**

Настройте коммутатор таким образом, чтобы он закрывал линию через десять минут от-сутствия активности.

S1(config)# **line console 0**

S1(config-line)# **exec-timeout 10 0** S1(config-line)# **line vty 0 15**

S1(config-line)# **exec-timeout 10 0**

S1(config-line)# **exit**

S1(config)#

Чтобы помешать попыткам входа в систему с использованием метода полного перебора,настройте коммутатор таким образом, чтобы он блокировал доступ к системе на 30 се- кунд после двух неудачных попыток входа в течение 120 секунд. Низкое значение этоготаймера установлено специально для данной лабораторной работы.

S1(config)# **login block-for 30 attempts 2 within 120** S1(config)# **end Шаг 5: Убедитесь, что все неиспользуемые порты отключены.**

По умолчанию порты коммутатора включены. Отключите на коммутаторе все неисполь-зуемые порты. a. Состояние портов коммутатора можно проверить с помощью команды **show ip interface brief**.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down

FastEthernet0/16 unassigned YES unset down down

FastEthernet0/17 unassigned YES unset down down

FastEthernet0/18 unassigned YES unset down down

FastEthernet0/19 unassigned YES unset down down FastEthernet0/20 unassigned YES unset down down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

GigabitEthernet0/1 unassigned YES unset down down GigabitEthernet0/2 unassigned YES unset down downS1#

Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой **interfacerange**.

S1(config)# **interface range f0/1–4 , f0/7-24 , g0/1-2**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **end**

S1#

Убедитесь, что все неактивные интерфейсы отключены администратором.S1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.11 YES manual up up FastEthernet0/1 unassigned YES unset administratively down down FastEthernet0/2 unassigned YES unset administratively down down FastEthernet0/3 unassigned YES unset administratively down down FastEthernet0/4 unassigned YES unset administratively down down FastEthernet0/5 unassigned YES unset up up FastEthernet0/6 unassigned YES unset up up FastEthernet0/7 unassigned YES unset administratively down down FastEthernet0/8 unassigned YES unset administratively down down FastEthernet0/9 unassigned YES unset administratively down down FastEthernet0/10 unassigned YES unset administratively down down FastEthernet0/11 unassigned YES unset administratively down down FastEthernet0/12 unassigned YES unset administratively down down FastEthernet0/13 unassigned YES unset administratively down down FastEthernet0/14 unassigned YES unset administratively down down

FastEthernet0/15 unassigned YES unset administratively down down
FastEthernet0/16 unassigned YES unset administratively down down
FastEthernet0/17 unassigned YES unset administratively down down
FastEthernet0/18 unassigned YES unset administratively down down
FastEthernet0/19 unassigned YES unset administratively down down
FastEthernet0/20 unassigned YES unset administratively down down
FastEthernet0/21 unassigned YES unset administratively down down
FastEthernet0/22 unassigned YES unset administratively down down
FastEthernet0/23 unassigned YES unset administratively down down
FastEthernet0/24 unassigned YES unset administratively down down

GigabitEthernet0/1 unassigned YES unset administratively down down GigabitEthernet0/2 unassigned YES unset administratively down down S1#

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

Убедитесь, что протокол Telnet на коммутаторе отключен.

Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имяпользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.

По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и вой-дите в систему, используя имя пользователя **SSHadmin** и пароль **Admin1p@55**.

Появился ли баннер после успешного входа в систему? _____

Войдите в привилегированный режим EXEC, используя **Enablep@55** в качестве пароля. Введите команду **show running-config** в строке приглашения привилегированного режи-ма EXEC для просмотра установленных параметров безопасности.

Вопросы для повторения

В части 1 для консоли и линий VTY в вашей базовой конфигурации была введена ко- манда **password cisco**. Когда используется этот пароль после применения наиболее эффективных мер обеспечения безопасности?

При подключении через консольный порт будет запрошен именно этот пароль "cisco".

Распространяется ли команда **security passwords min-length 10** на настроенные ранеепароли, содержащие меньше десяти символов?

Нет.

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель марш-рутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс № 1**	Последовательный интерфейс №2
1800	Fast Ethernet 0/0(F0/0)	Fast Ethernet 0/1(F0/1)	Serial 0/0/0 (S0/0/0)	**Serial 0/0/1 (S0/0/1)**
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	**Serial 0/0/1 (S0/0/1)**
2801	Fast Ethernet 0/0(F0/0)	Fast Ethernet 0/1(F0/1)	Serial 0/1/0 (S0/0/0)	**Serial 0/1/1 (S0/0/1)**
2811	**Fast Ethernet 0/0(F0/0)**	**Fast Ethernet 0/1(F0/1)**	**Serial 0/0/0 (S0/0/0)**	**Serial 0/0/1 (S0/0/1)**
2900	Gigabit Ethernet 0/0(G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечис-лить все комбинации

конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокраще- ние, которое можно использовать в командах Cisco IOS для обозначения интерфейса.

На экране Dynamic Update (динамические обновления), выберем один из трех возможных вариантов динамического обновления.

Разрешить только безопасные динамические обновления (Allow Only Secure

Dynamic Updates). Это опция доступна, только если зона интегрирована в Active Directory.

Разрешить любые, безопасные и не безопасные динамические обновления (Allow Both Nonsecure And Secure Dynamic Updates). Данный переключатель, позволяет любому клиенту обновлять его записи ресурса в DNS при наличии изменений.

Запретить динамические обновления (Do Not Allow Dynamic Updates). Это опция отключает динамические обновления DNS. Ее следует использовать только при отсутствии интеграции зоны с Active Directory.