Содержание

1. Типовой комплект учебного оборудования «Беспроводные компьютерные сети»

1.1. Описание комплекта

Комплект состоит из:

1. Центральной консоли, которая включает:
   - ✓ 2-а неуправляемых коммутатора Cisco SD205;
   - ✓ коммутатор-инжектор Cisco SRW208P, который является источником питания для оборудования доступа (используется технология Power over Ethernet, PoE);
   - ✓ коммутационную панель категории 5E на 24 порта RJ-45, которая позволяет коммутировать проводные и беспроводные устройства в зависимости от выполняемых задач и формировать необходимую топологию сети;
   - ✓ оборудование доступа, которое включает:
     - 2-е беспроводные точки доступа стандарта 802.11n Cisco WAP4410N;
     - 2-а беспроводных маршрутизатора стандарта 802.11b/g Cisco 881W;
2. 2-а ретранслятора сигнала Linksys WRE54G.
3. Оконечного клиентского оборудования, которое представляет собой 3 портативных компьютера.

На ноутбуках установлена операционная система Microsoft Windows XP Home Edition (лицензионный серийный номер смотрите на нижней стороне ноутбука) с дополнительным бесплатным пакетом программ для работы с сетями Wi-Fi. Также с комплектом поставляются флэш-диски, содержащие загрузочный образ операционной системы Arch Linux с дополнительным пакетом открытых программ для работы с сетями Wi-Fi. Процесс загрузки ОС Linux описан в разделе 1.2.

Все ноутбуки имеют два встроенных интерфейса: проводный Ethernet и беспроводный Wi-Fi. Дополнительно для каждого ноутбука поставляется внешний беспроводный USB-адаптер Linksys WUSB600N (IEEE 802.11n).

Оборудование доступа располагается на лицевой панели стенда и соединено кабелем с центральной консолью, которая содержит источник питания для беспроводных точек доступа. Также от точек доступа к центральной консоли идут проводные линии данных. Это необходимо, так как всё беспроводное оборудование содержит встроенные проводные Ethernet-интерфейсы, которые как минимум необходимы для настройки и управления данным оборудованием. Таким образом, в учебном комплекте и в реальной жизни нельзя достигнуть полной автономности оборудования Wi-Fi – как минимум необходима линия питания. Следовательно, сети Wi-Fi можно считать условно беспроводными.

Для регистрации на ноутбуках используйте следующую учетную запись:

пользователь: *root*
пароль: *qwerty*

Разводка портов коммутационной панели приведена на самой коммутационной панели.

Все узлы стенда включены в IP-подсети 192.168.0.0/24, 192.168.1.0/24. Распределение IP-адресов приведено в таблице 1.1.

Таблица 1.1 – Распределение IP-адресов

Узел		IP-адрес
Ноутбук 1	Интерфейс eth0	192.168.0.1
	Интерфейс wlan0	192.168.1.1
Ноутбук 2	Интерфейс eth0	192.168.0.2
	Интерфейс wlan0	192.168.1.2
Ноутбук 3	Интерфейс eth0	192.168.0.3
	Интерфейс wlan0	192.168.1.3

1.2. Загрузка операционной системы Arch Linux

Для загрузки операционной системы Arch Linux 2008 с флэш-диска необходимо выполнить следующие шаги:

1. Вставьте флэш-диск в любой USB-порт ноутбука.
2. Включите питание ноутбука.
3. Нажимайте клавишу F2 до тех пор, пока не загрузится BIOS.
4. Выберите закладку «Boot».
5. В поле «First Boot» выберите «USB: Kingston …».
6. Нажмите F10.
7. Подтвердите сохранение сделанных изменений и последующую перезагрузку.

1.3. Система восстановления операционных систем ноутбуков «U-Profi Rescue System»

Комплект поставляется вместе с системой восстановления операционной системы (ОС) Windows XP, установленной на всех ноутбуках. Данная система может оказаться полезной не только в случае отказа ОС, но также в тех случаях, когда после проведения ряда лабораторных работ необходимо быстро привести ОС к первоначальному виду.

Файловая система операционной системы Linux, установленной на флэш-дисках, при загрузке монтируется в режим «только чтение». Это означает, что все изменения настроек системы актуальны только на момент текущей работы, так как сохраняются только в ОЗУ. После перезагрузки все изменения удаляются.

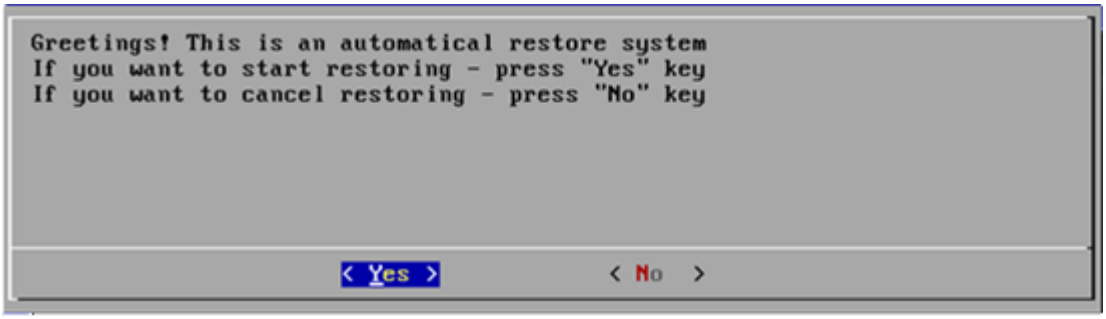
Далее приведена инструкция по работе с системой восстановления:

1. ВНИМАНИЕ! Восстановление уничтожит все данные на жёстком диске. Сделайте резервные копии важных данных.
2. Вставьте флэш-диск в USB-разъём (соблюдайте соответствие номера ноутбука и номера диска).
3. При загрузке нажмите клавишу F2 и выберите флэш-диск в качестве загрузочного устройства.
4. Подтвердите сохранение сделанных изменений и последующую перезагрузку.

5. Дождитесь появления следующего окна:

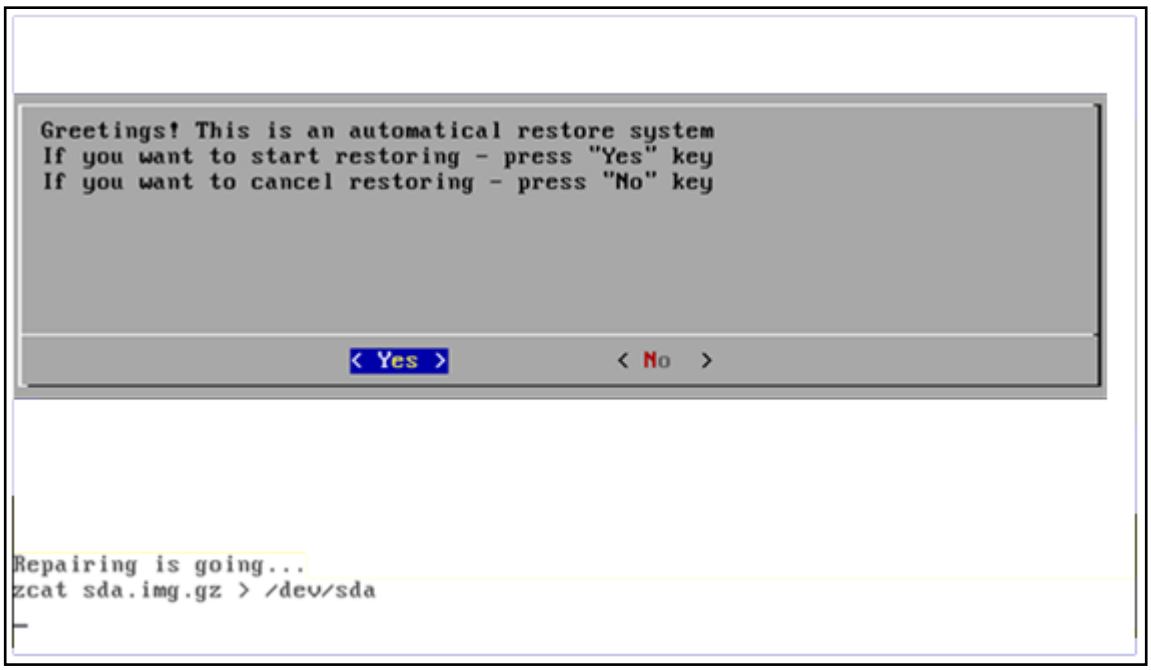
Для выхода из системы клавишей Tab выделите кнопку «Выход» и нажмите Enter. Это приведёт к перезагрузке компьютера. Иначе, для продолжения работы нажмите любую клавишу.

6. Дождитесь появления следующего окна:



Чтобы начать восстановление, нажмите «Yes», иначе нажмите «No» или просто перезагрузите компьютер. В связи с техническими ограничениями на данный момент при нажатии клавиш навигации перерисовка экрана с диалогом пользователя не происходит. Однако сами нажатия учитываются.

7. Когда восстановление начнётся, вы увидите следующее окно:



В системе не реализован прогресс-индикатор (индикатор объёма выполненной работы). Признаком того, что система не зависла, является индикатор обращения к жесткому диску компьютера на его системном блоке. Процесс восстановления в среднем занимает около 1 часа.

8. Когда восстановление будет закончено, появится следующее окно:

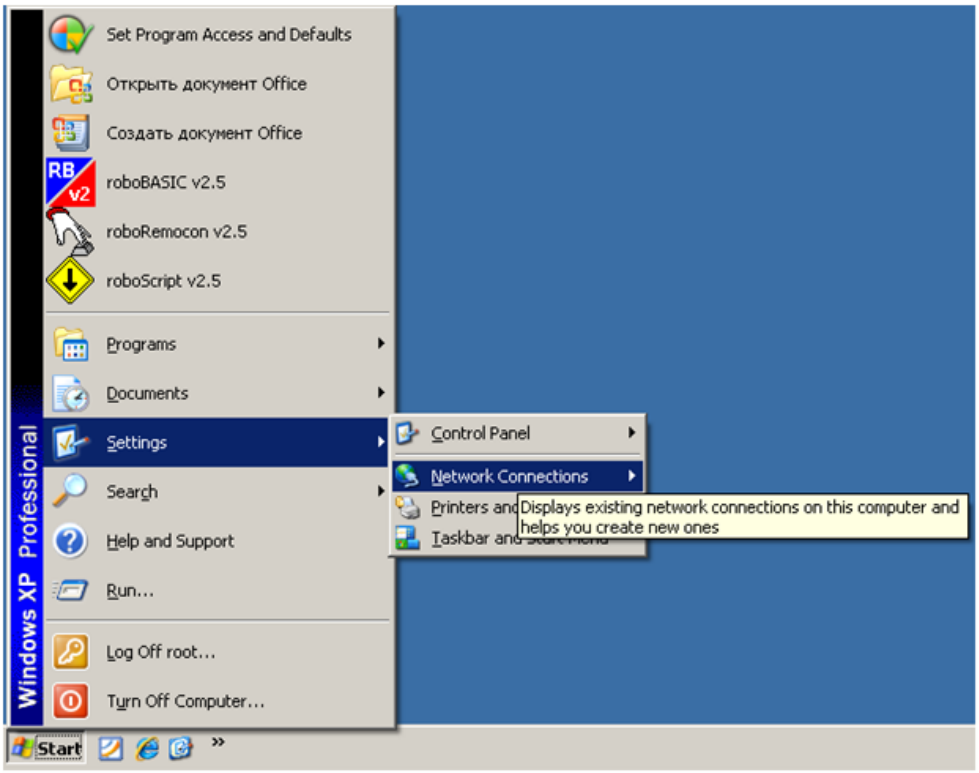
9. Нажмите «ОК». Произойдёт перезагрузка. Не забудьте извлечь диск из привода.

2. Операционная система MS Windows XP

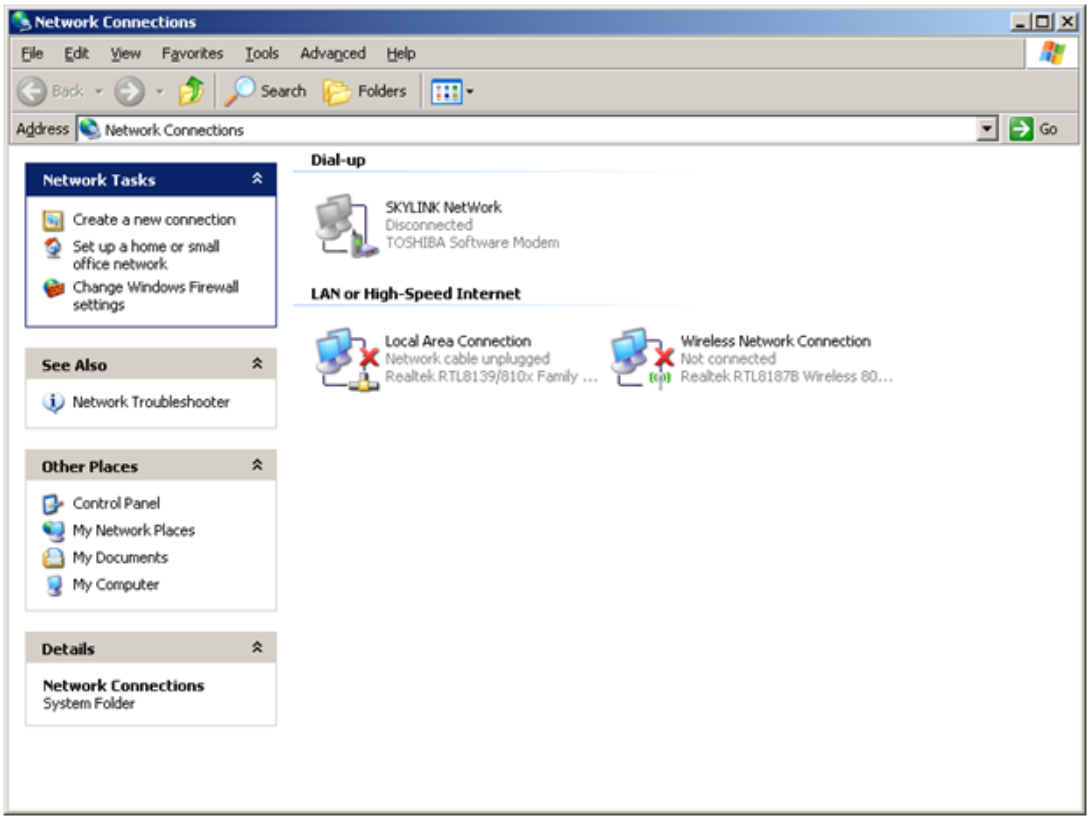
2.1. Настройка сетевых параметров

Настройка проводного интерфейса

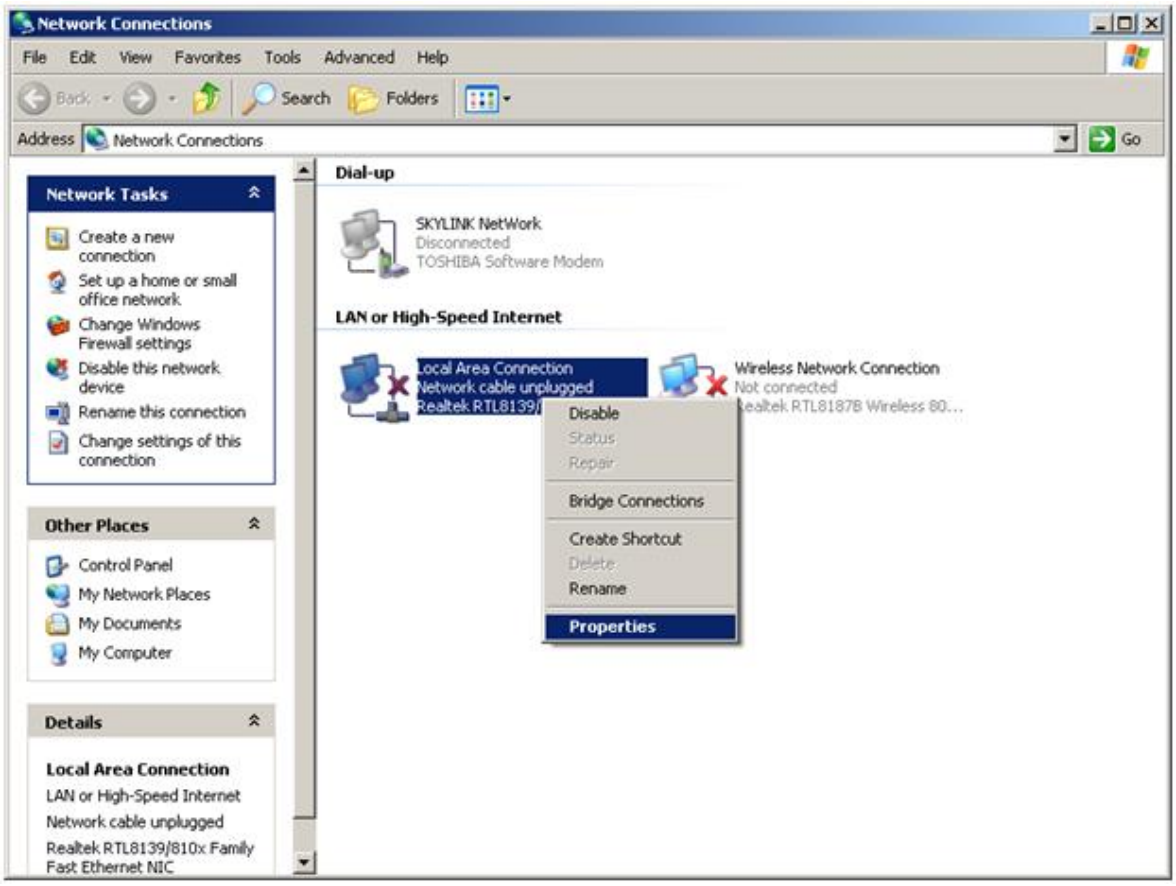
1. Откройте меню Пуск → Настройка → Сетевые подключения



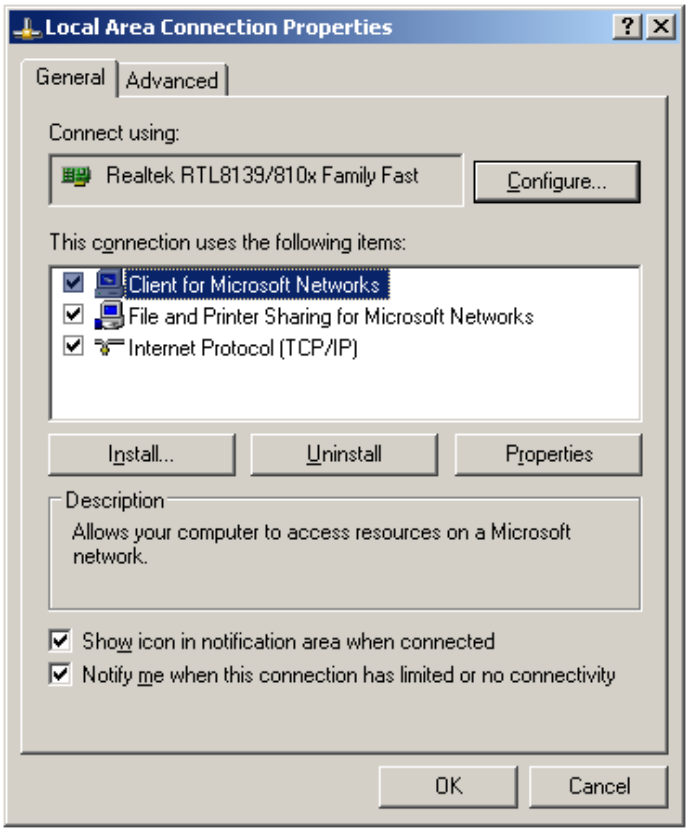
2. Вы увидите следующее окно



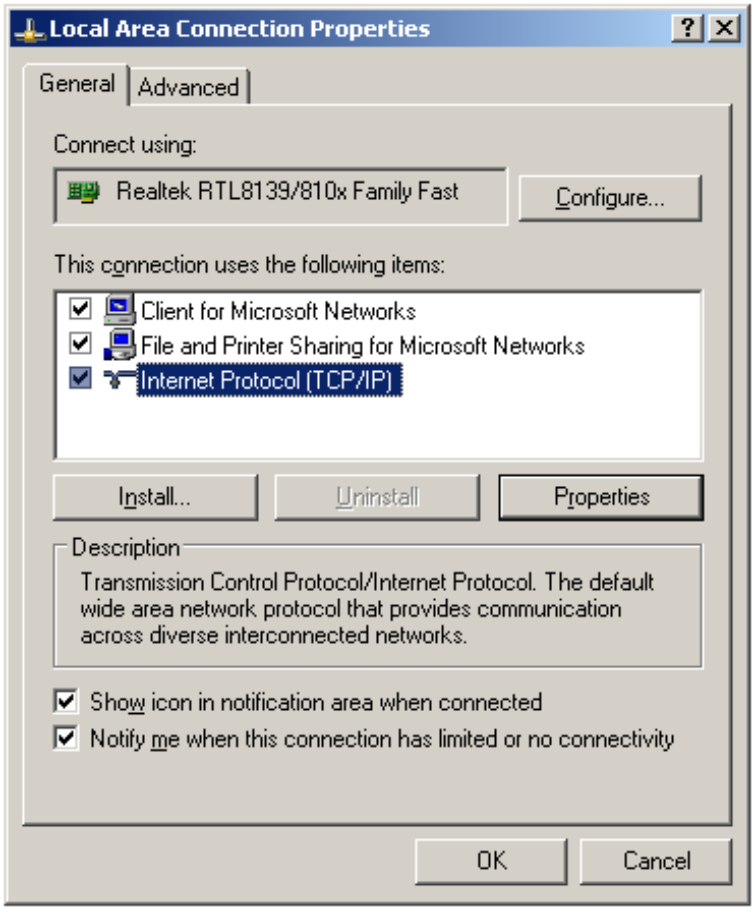
3. Выберите проводной интерфейс (Local Area Connection, Подключение к локальной сети), нажмите правую кнопку и выберите пункт меню «Свойства».



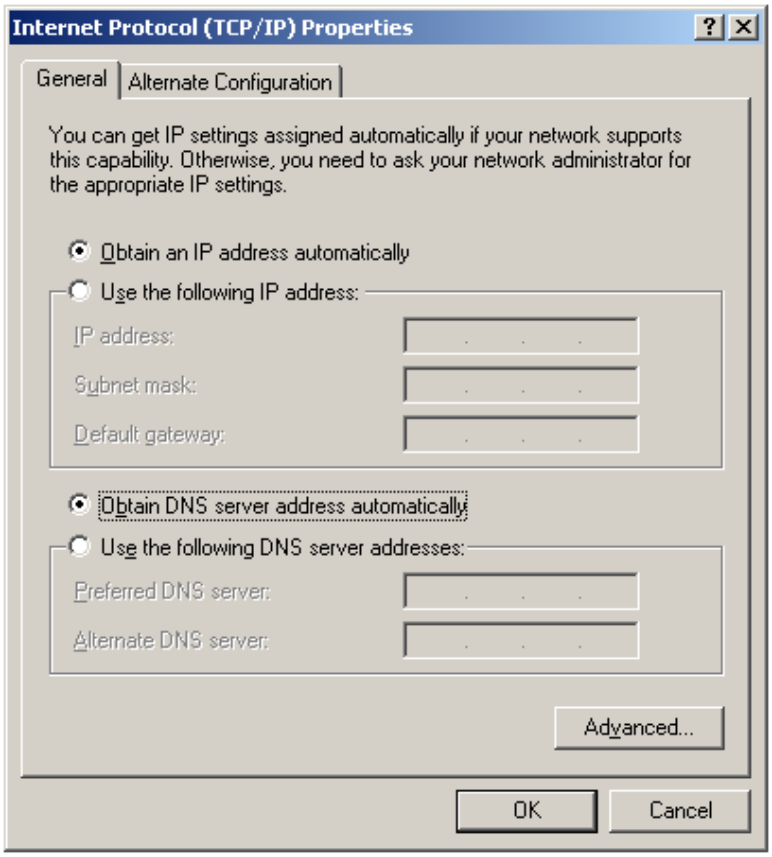
4. Вы увидите следующее окно



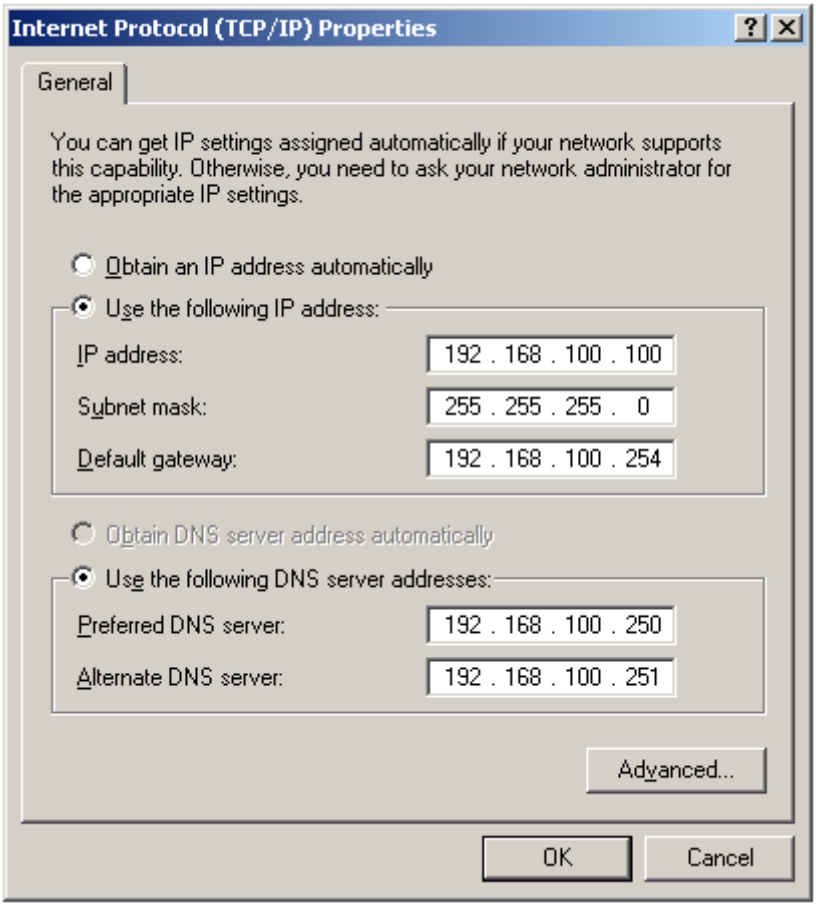
5. Выберите элемент «Протокол TCP/IP» («Internet Protocol») и нажмите на кнопку «Свойства»



6. Откроется следующее окно



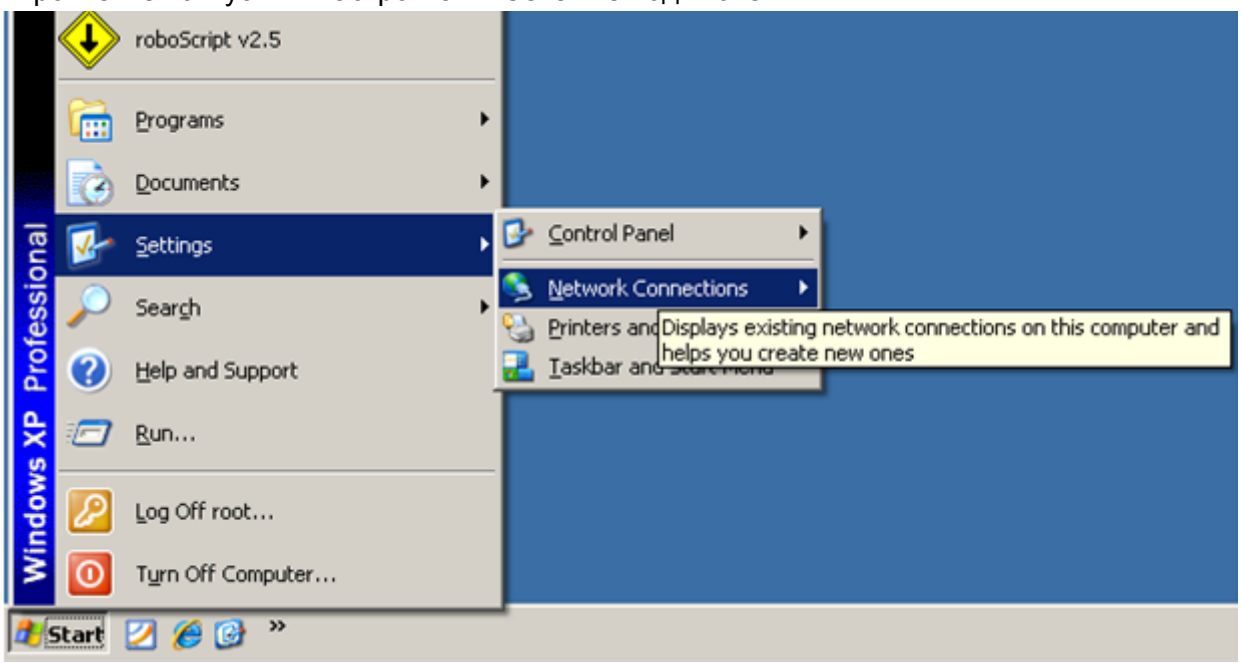
7. Если в сети используется DHCP-сервер — оставьте все настройки без изменений. В противном случае укажите IP-адрес компьютера, маску сети, шлюз (если требуется), DNS-серверы (если требуются).



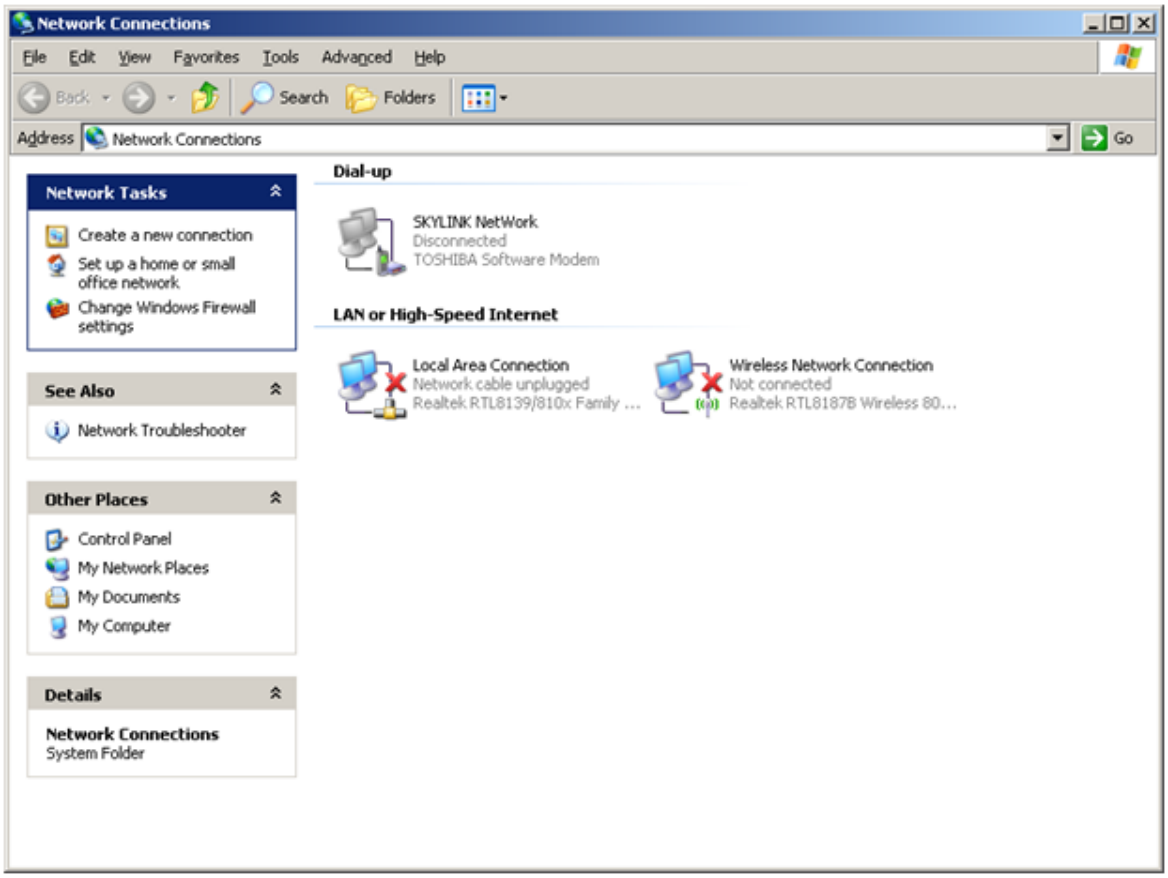
8. Нажмите ОК, а затем нажмите ОК вы всех предыдущих окнах.

Настройка беспроводного интерфейса

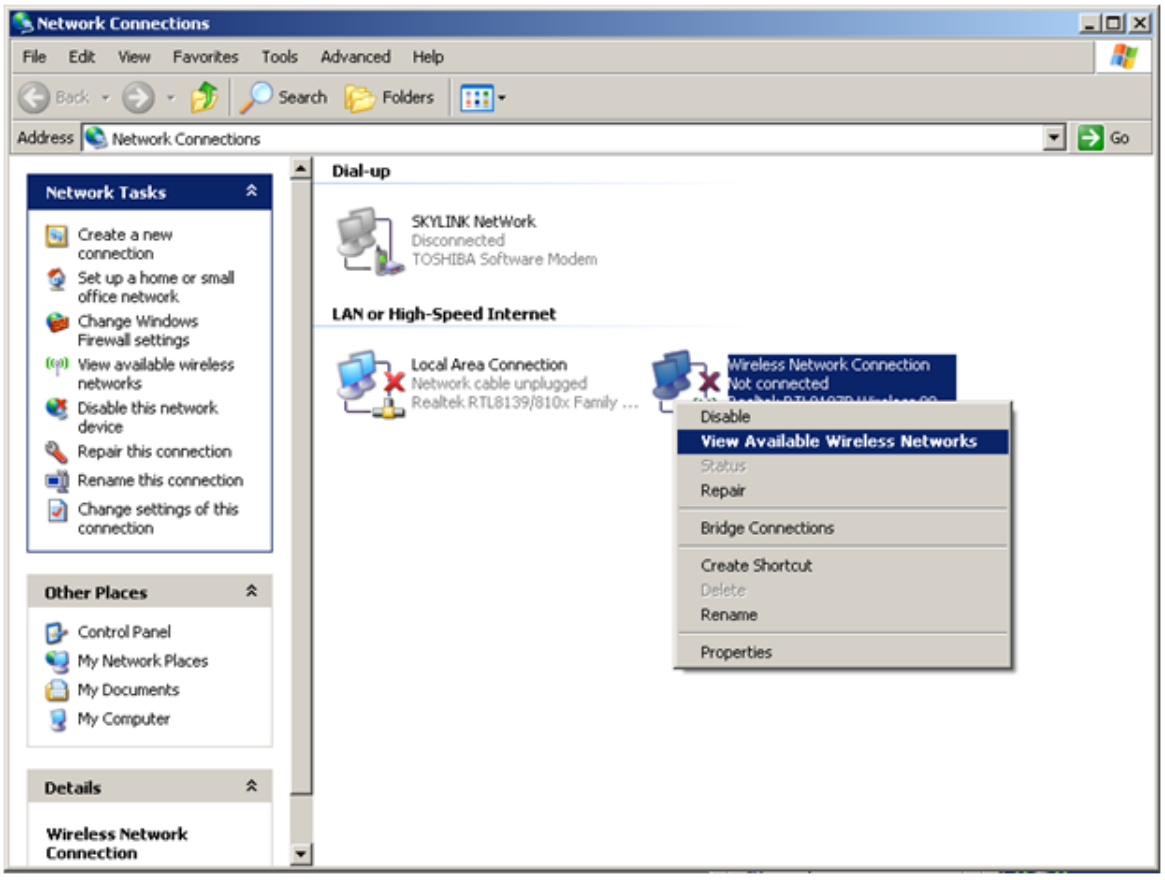
1. Откройте меню Пуск → Настройка → Сетевые подключения



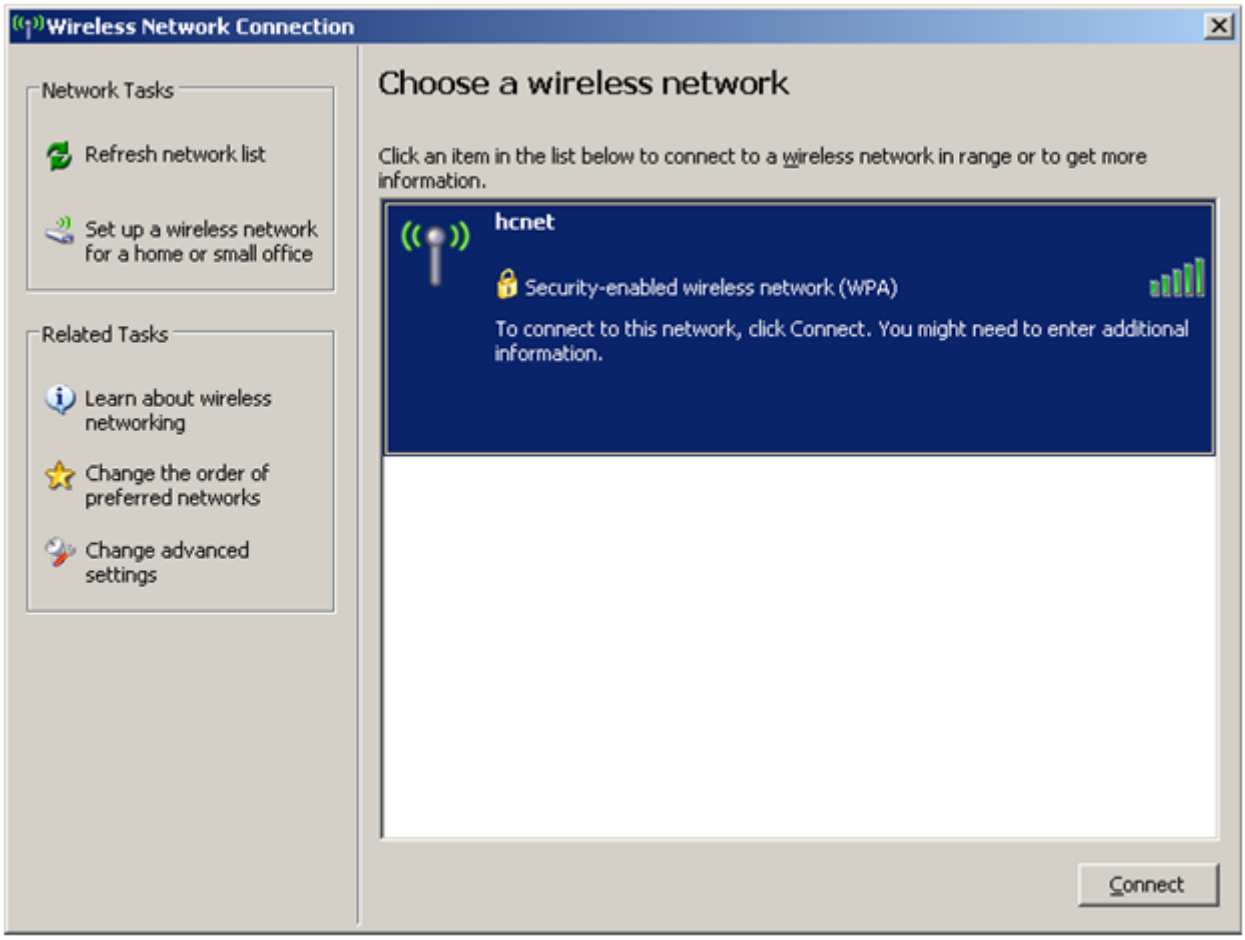
2. Вы увидите следующее окно



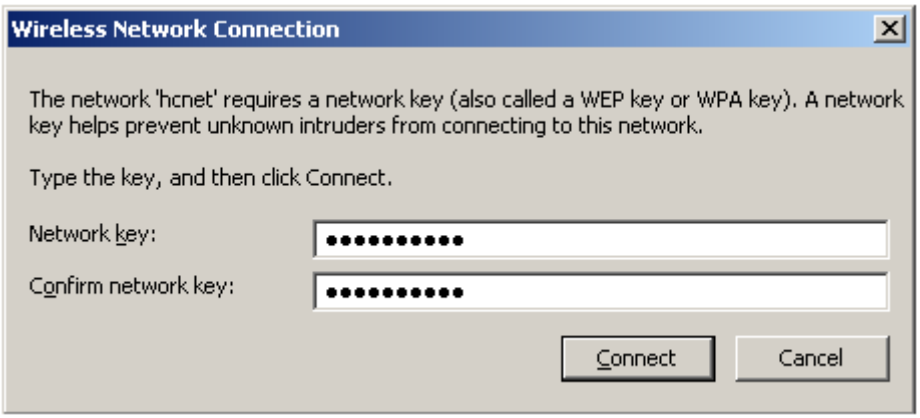
3. Если беспроводная сеть является видимой — выберите беспроводной интерфейс (Wireless Connection Network, Подключение к беспроводной сети), нажмите правую кнопку и выберите пункт меню «Показать доступные беспроводные сети»



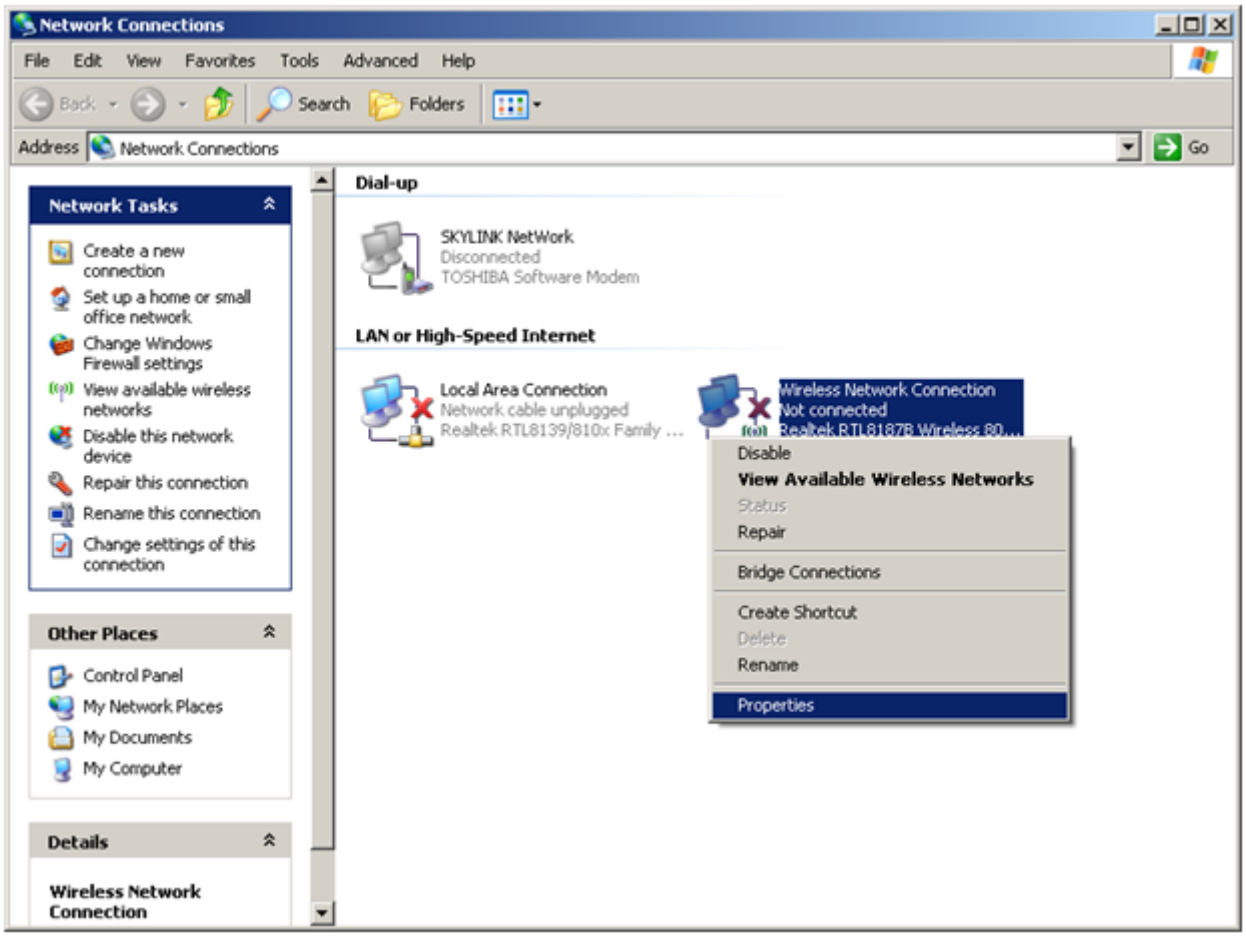
4. Появится следующее окно, в котором отразятся обнаруженные беспроводные сети



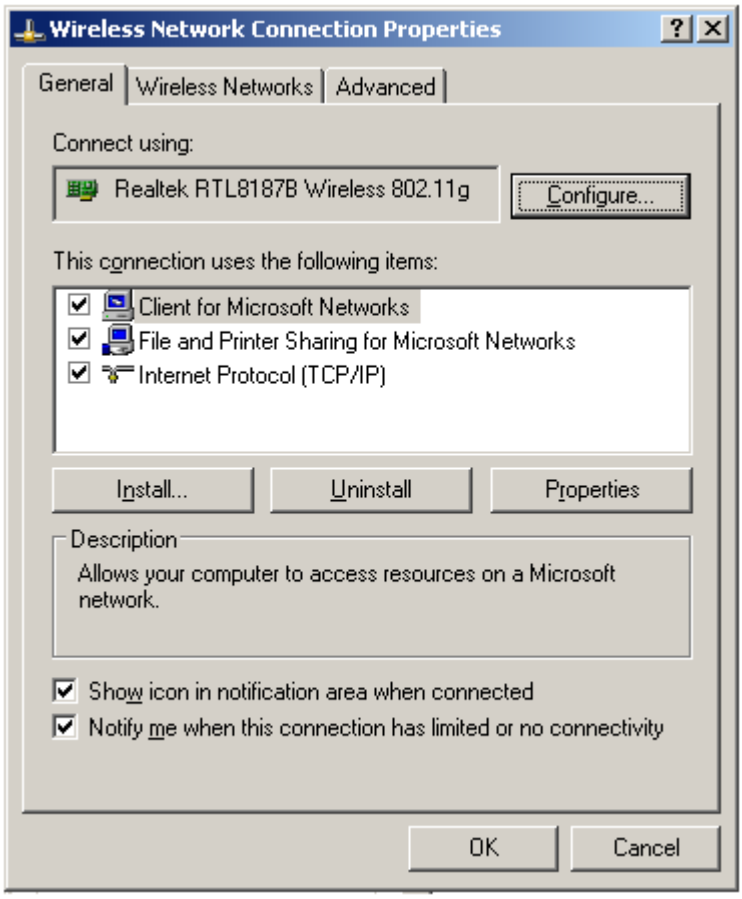
5. Выберите нужную сеть и нажмите кнопку «Подключиться» («Connect»). Если сеть использует WEP- или WPA-шифрование, появится запрос на ввод ключа.



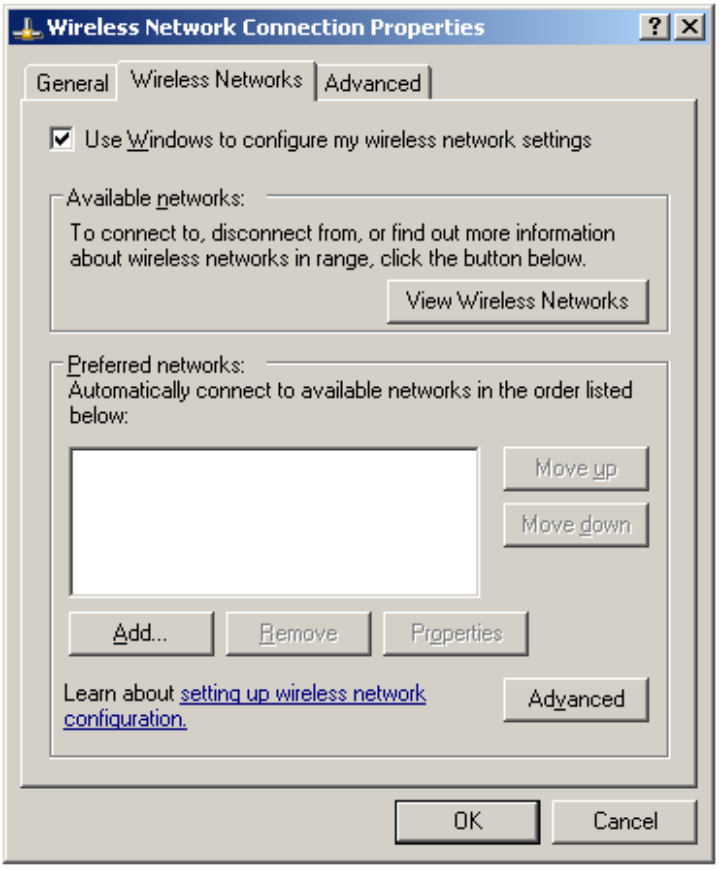
6. Введите правильный ключ в оба поля и нажмите кнопку «Подключиться» («Connect»).
7. Если нужная сеть является скрытой, то на шаге 3 выберите беспроводной интерфейс, нажмите правую кнопку мыши и выберите пункт меню «Свойства».



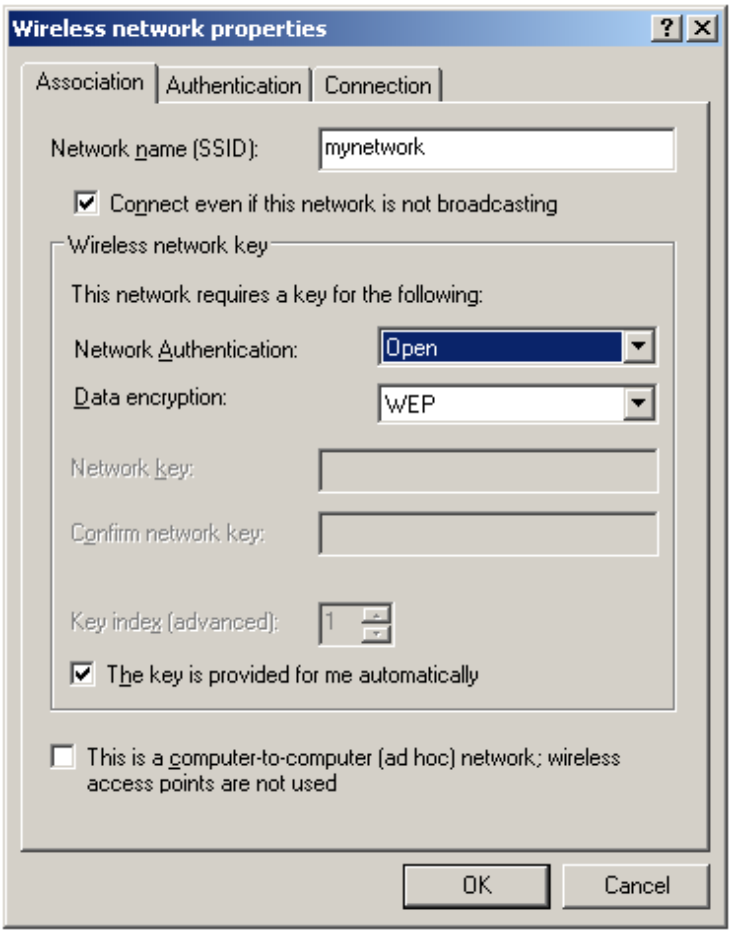
8. Откроется следующее окно



9. Откройте вкладку «Беспроводные сети» («Wireless Networks»).



10. Нажмите кнопку «Add». Появится следующее окно.



11. Введите имя сети (Network name, SSID). Если требуется — выберите тип шифрования и введите ключ. Для завершения настройки нажмите кнопку ОК. Через некоторое время (если сеть будет найдена в зоне действия интерфейса и все настройки сделаны верно) вы будете подключены к выбранной беспроводной сети. Если в сети нет DHCP-сервера, то можно указать IP-адрес и прочие параметры на шаге 8 аналогично шагам 4-8 руководства по настройке проводного интерфейса.

Утилиты для работы с сетями Wi-Fi

2.2. NetStumbler

NetStumbler является сниффером сетей Wi-Fi. После запуска NetStumbler отображается основной экран (рисунок 5.1).

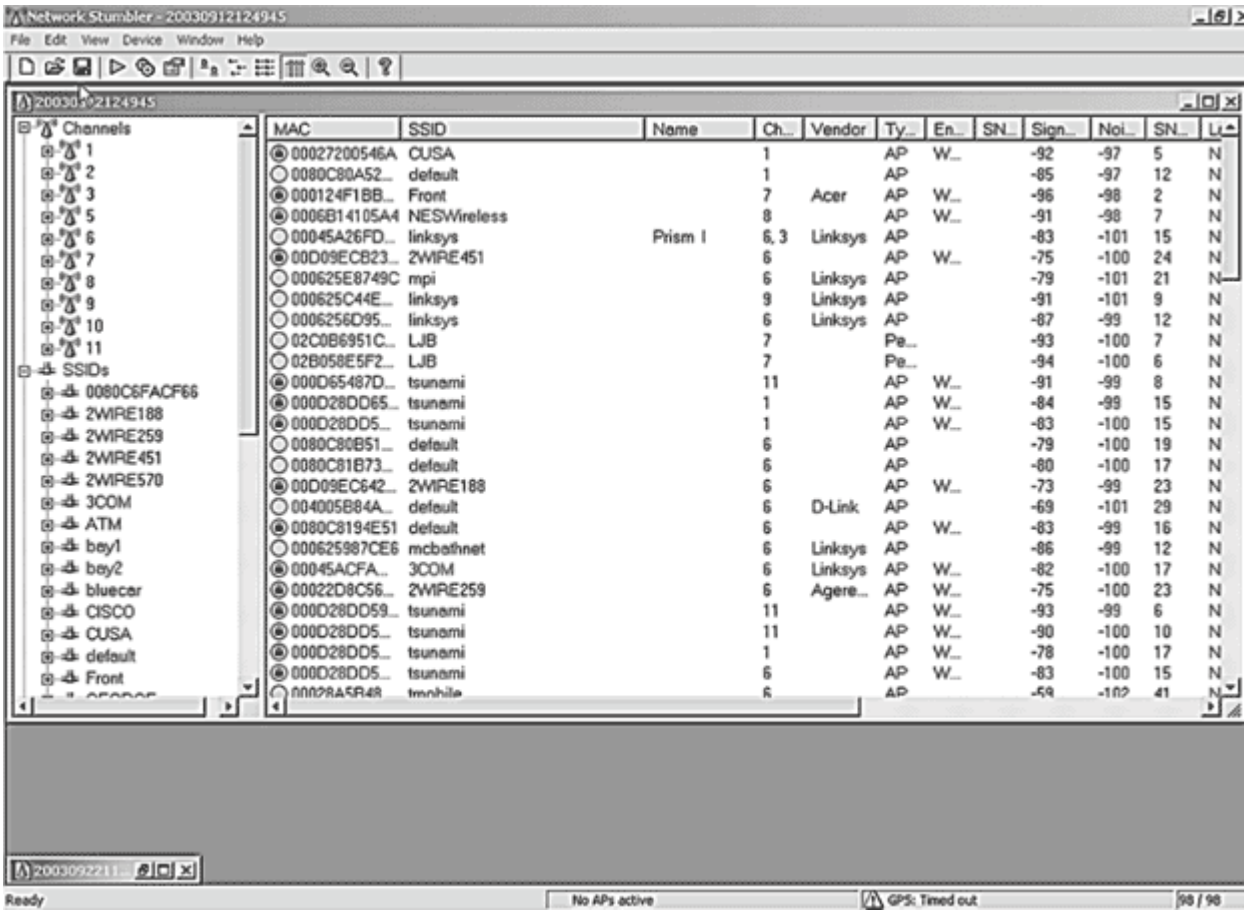


Рисунок 5.1. Основной экран NetStumbler.

В столбце MAC можно видеть список точек доступа, обнаруженных NetStumbler. Иконки сетей слева от MAC-адреса окрашены в зеленый цвет, если они в настоящее время в зоне досягаемости. По мере удаления от сети иконки становятся сначала желтыми, а затем красными. Иконки неактивных сетей будут серыми. Если в сети применяется шифрование, то отобразится замочек в кружке. Это позволяет быстро понять, в каких сетях используется WEP. NetStumbler собирает дополнительные данные о любой обнаруживаемой точке.

Поля данных NetStumbler

MAC – BSSID или MAC-адрес базовой станции. Это уникальный идентификатор, присвоенный производителем. Он полезен, когда у вас много станций с одним и тем же подразумеваемым SSID производителя, таким как linksys.

SSID – Идентификатор набора сервисов, с которым настраивается каждая точка доступа. Он определяет беспроводную сеть и необходим для входа в нее. NetStumbler охотно извлечет его для вас из сигналов радиомаяка. Как отмечено в описании поля MAC, это не обязательно уникальный идентификатор, так как другие базовые станции могут иметь такое же значение SSID. Возможны проблемы, если две организации в одном здании используют одинаковые подразумеваемые значения SSID. В таком случае

может статься, что служащие используют сеть или выход в Интернет другой организации

Name – Необязательное описательное имя точки доступа. Иногда производитель задает его. Владелец сети может его редактировать; например, Acme Corp Wireless Network. Иногда лучше оставить это поле пустым, если вы не хотите, чтобы посторонние, исследующие сетевой радиоэфир, узнали, что эта точка доступа принадлежит вам

Channel – Канал, в котором оперирует базовая станция. Если вы столкнулись с помехами, изменение этого значения у точки доступа может их устранить. Большинство производителей используют подразумеваемый канал. Например, для точек доступа Linksys подразумеваемым служит шестой канал

Vendor – NetStumbler с помощью BSSID пытается идентифицировать производителя и модель выявленного беспроводного оборудования

Type – Указывает, была ли найдена точка доступа, узел сети или устройство какого-то другого типа. Обычно будут находиться точки доступа, которые обозначаются AP. Беспроводные узлы показываются как Peer. Именно поэтому, даже без настроенной беспроводной сети, наличие в вашем ПК беспроводной платы может быть рискованным. В наше время многие ПК-блокноты поставляются со встроенными беспроводными передатчиками, поэтому желательно их отключить, если пользователи не собираются их применять

Encryption – Показывает, какой тип шифрования используется в сети (если используется). Это очень важно, поскольку, если сеть не шифруется, то посторонние могут извлечь ваш сетевой трафик прямо из эфира и прочитать его. Они могут также войти в вашу сеть, если отсутствуют другие средства защиты

SNR – Отношение сигнал/шум. Характеризует уровень помех и шума на входе приемника беспроводной платы

Signal – Уровень мощности сигнала на входе приемника

Noise – Уровень шума на входе приемника

Latitude – Широта, если вы применяете вместе с NetStumbler приемник GPS
Longitude – Долгота, если вы применяете вместе с NetStumbler приемник GPS

First seen – Показания системных часов, когда был впервые принят сигнал радиомаяка сети

Last seen – NetStumbler обновляет это значение всякий раз, когда вы входите в зону приема точки доступа

Beacon – Частота посылки сигнала радиомаяка в миллисекундах

По мере проведения аудита, основной экран NetStumbler заполнится обнаруживаемыми беспроводными сетями. В левой стороне экрана отображаются обнаруженные сети. Можно упорядочить их с помощью различных фильтров, выбрать их по каналам, SSID и нескольким другим критериям. Можно задать фильтры, чтобы отображались только сети, в которых

шифрование включено или выключено, инфраструктурные или одноранговые (произвольные), допускающие CF-опрос (предоставление дополнительной информации при запросе) или нет, с подразумеваемым или переустановленным значением SSID.

На панели в нижней части основного экрана можно видеть состояние своей беспроводной сетевой платы. Если она функционирует нормально, то вы увидите иконку, мигающую примерно каждую секунду, и количество видимых в данный момент активных точек доступа. Если возникает проблема с интерфейсом между сетевой платой и программным обеспечением, то вы увидите это здесь. С правой стороны нижней панели находятся координаты GPS, если используется устройство глобального позиционирования.

Мигание показывает, как часто вы опрашиваете точки доступа. NetStumbler – средство активного сканирования сетей, поэтому он постоянно посылает пакеты "Hello", чтобы проверить, ответит ли какая-нибудь беспроводная сеть. Другие беспроводные средства, такие как Kismet, являются пассивными, так как они только принимают сигналы радиомаяка. Недостаток активных средств - возможный пропуск некоторых точек доступа, настроенных не отвечать на опрос; достоинство же в том, что некоторые точки доступа посылают сигналы радиомаяка так редко, что с помощью пассивных средств вы можете никогда их не поймать. Помните также, что активный опрос может вызывать срабатывание беспроводных систем обнаружения вторжения, однако очень немногие организации применяют подобные системы, а если вы используете NetStumbler только как средство оценивания собственной сети, то скрытность не должна быть важна.

Если в этом режиме щелкнуть мышью на какой-либо сети, будет показан график отношения сигнал/шум за период времени, когда вы наблюдали сеть. Это позволяет увидеть, насколько силен сигнал в различных областях (рисунок 5.2).

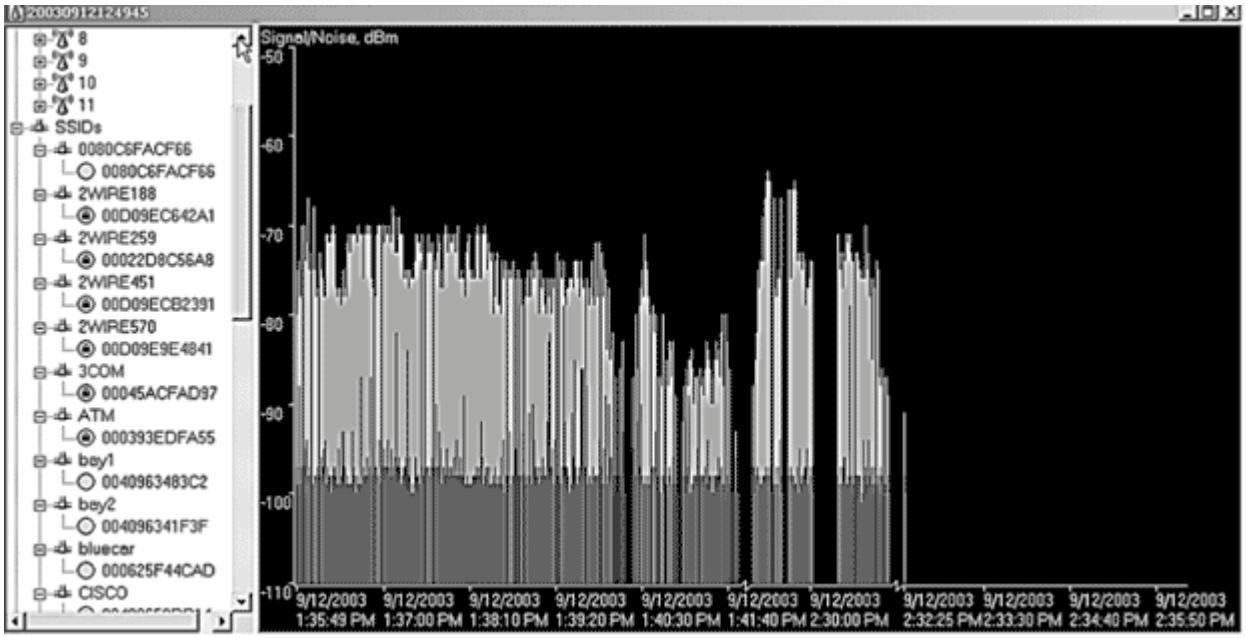


Рисунок 5.2. График сигнала NetStumbler.

Опции NetStumbler

Чтобы вывести диалоговое окно для задания опций NetStumbler, выберите подменю Options в меню View. В таблице 5.1 перечислены вкладки и возможные значения.

Таблица 5.1 – Опции NetStumbler

Вкладка	Описание
General	Задает частоту опроса точек доступа. Можно также задать автоматическую подстройку с учетом вашей скорости, если применяется система глобального позиционирования. Имеется опция автоматического реконфигурирования вашей платы, когда найдена новая сеть, но вы, вероятно, не захотите этого делать в насыщенной области: если вокруг много точек доступа, то конфигурация платы будет изменяться каждые несколько секунд и это замедлит работу компьютера. Кроме того, программное обеспечение может сконфигурировать плату для чужой сети, и тогда вы неумышленно станете нарушителем
GPS	Настраивает приемник GPS для взаимодействия с NetStumbler. Я использовал карманное устройство GPS Meridian с последовательным кабелем. Пришлось задать лишь правильный порт и параметры коммуникации, и NetStumbler сразу начал импортировать данные
Scripting	Настройка вызова внешних процедур. Можно использовать Visual Basic или любые другие языки на Windows-платформе для выполнения дополнительных действий с выдачей NetStumbler. Внешние программы также могут использовать эту функциональность
MIDI	Можно настроить NetStumbler для проигрывания отношения сигнал/шум как файла MIDI. Не думаю, что это стоит делать в области с множеством сетей, поскольку может стать очень шумно, но предполагаю, что поиск ускользающего сигнала по звуку способен быть эффективным

Сохранение сеансов NetStumbler

NetStumbler автоматически начинает сохранять сеанс всякий раз, как вы его открываете. Это позволяет анализировать сеансы NetStumbler позднее. По умолчанию сеансы сохраняются в собственном формате NetStumbler. Можно также сохранять сеансы как текст для импорта в электронную таблицу или текстовый процессор, и в формате wi-scan, который является активно развивающимся файловым стандартом для журналов анализа беспроводных сетей. Можно также экспортировать их в некоторые другие форматы.

Для каждого сеанса NetStumbler выводит вверху окна уникальный номер, являющийся комбинацией даты и времени. Это полезно при отслеживании сеансов и результатов. При желании можно заменить это имя на более содержательное.

Теперь, имея множество данных о периметре беспроводной сети, желательно сгенерировать некоторые отчеты либо для руководства, либо для заказчика, если вы работаете как консультант. Если имеются данные глобального позиционирования, можно построить наглядные карты с помощью программы Microsoft MapPoint и рассмотренного ниже средства с открытыми исходными текстами.

2.3. MAC Address Changer

Предназначена для смены MAC-адреса сетевого интерфейса. Запустите MAC Address Changer двойным щелчком на ярлыке. Откроется окно, представленная на рисунке 5.3.

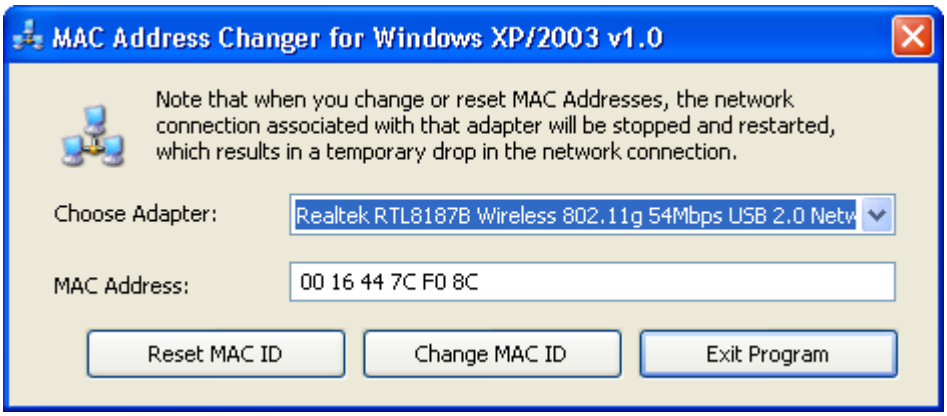


Рисунок 5.3.

В списке Choose Adapter выберите сетевой интерфейс, которому необходимо сменить MAC-адрес. В строке MAC Address отобразится текущий адрес. Введите новый MAC с пробелом в качетсве разделителя байт и нажмите Change MAC ID. В случае успешной смены адреса вы увидите следующее сообщение, представленное на рисунке 5.4.

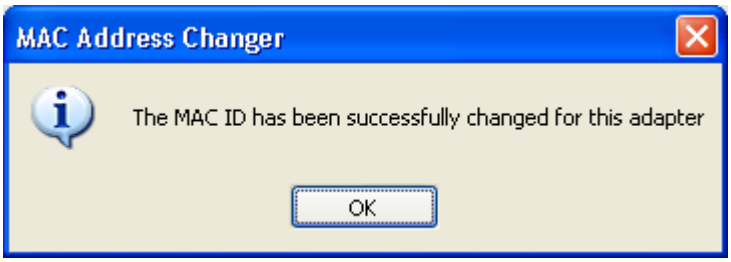


Рисунок 5.4.

Завершите работу с программой, нажав на кнопку «Exit Program». Чтобы вернуть заводские настройки, нажмите на кнопку «Reset MAC ID».

2.4. WireShark

Wireshark является сетевым анализатором и позволяет перехватывать и разбирать пакеты, показывая в наглядном виде структуру пакета и информацию, содержащуюся в нём. Запустите Wireshark. Вы увидите следующее окно.

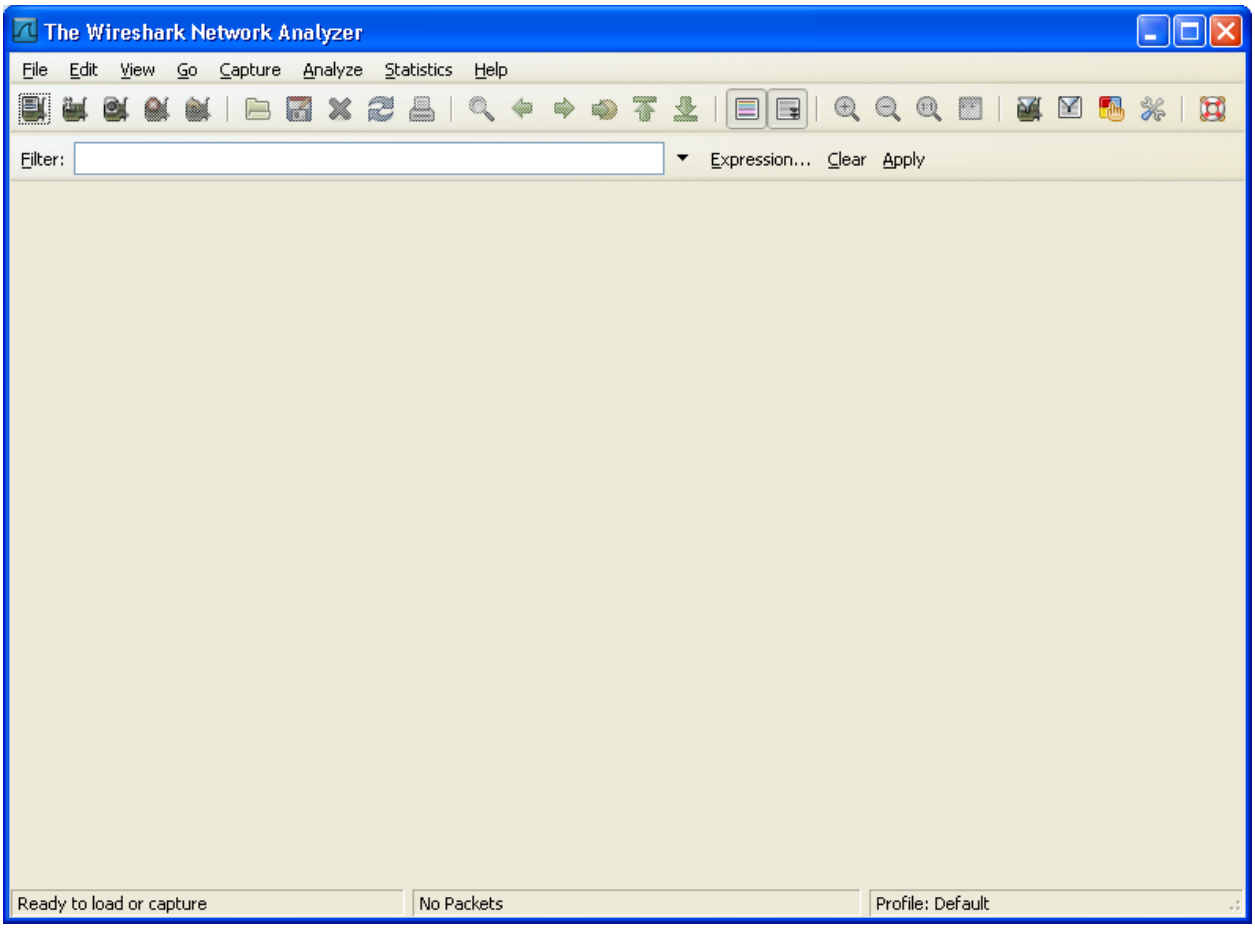


Рисунок 5.5.

Для начала перехвата пакетов перейдите в меню “Capture → Interfaces…”. Вы увидите следующее окно.

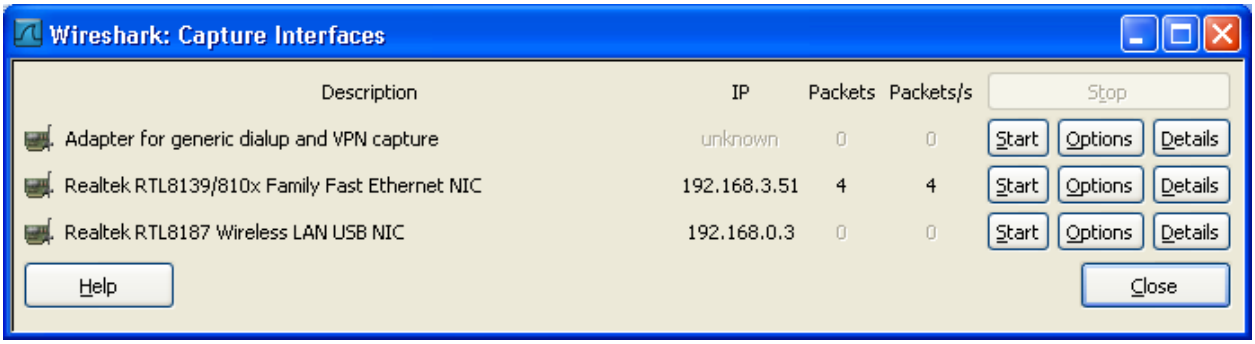


Рисунок 5.5.

Нажмите кнопку Start, расположенную напротив имени интерфейса, пакеты с которого необходимо перехватывать. Начнётся перехват пакетов и одновременный анализ. Чтобы остановить захват, выберите пункт меню “Capture → Stop”. В главном окне отобразятся результаты перехвата (рисунок 5.6).

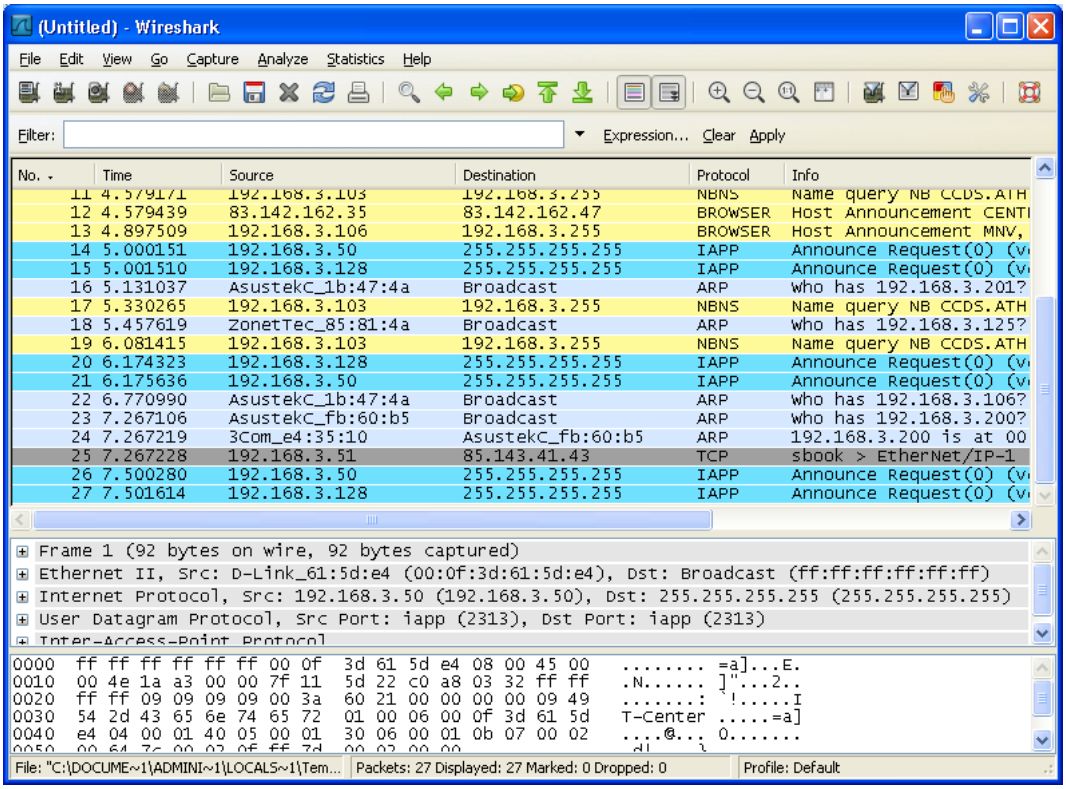


Рисунок 5.6.

Главное окно разделено на 3 части:

- ✓ список перехваченных пакетов;
- ✓ заголовки различных уровней модели OSI, содержащиеся в пакете;
- ✓ содержимое пакета в шестнадцатеричном и текстовом видах.

При выборе определённого заголовка или его части будет выделена соответствующая ему часть пакета (рисунок 5.7).

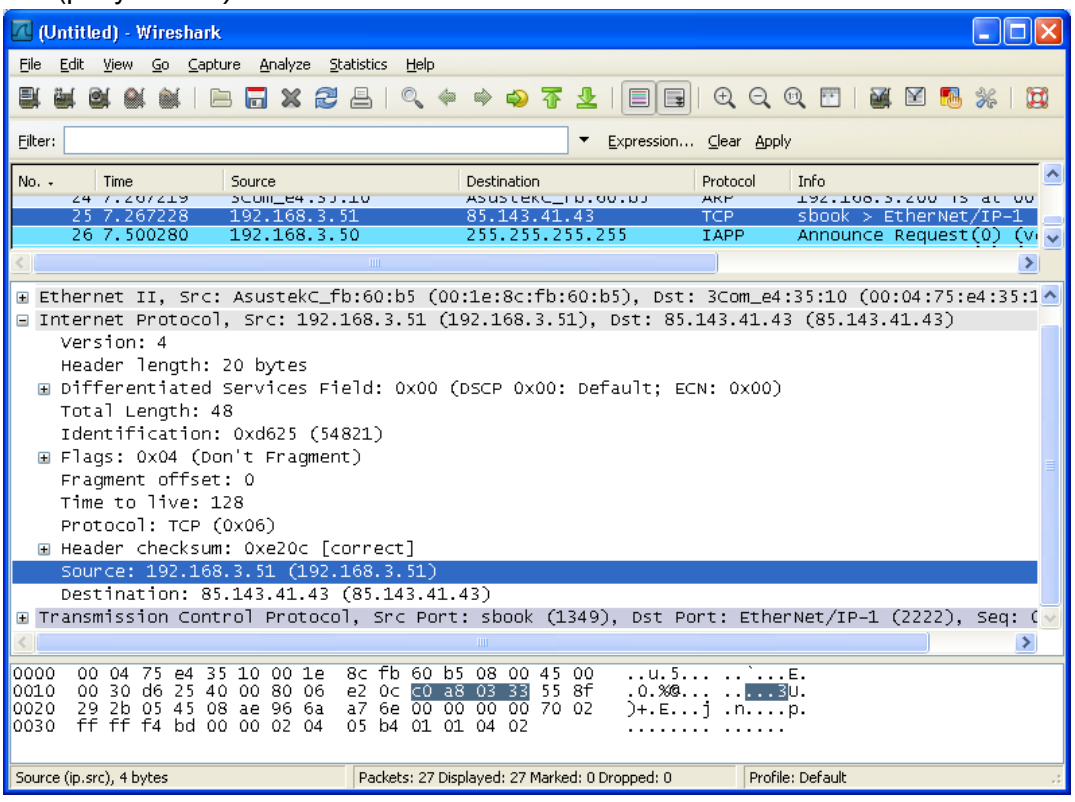


Рисунок 5.7.

3. Операционная система Cisco IOS

1. Принципы работы с ОС IOS

IOS (Internetwork Operating System, операционная система для объединённых сетей) — операционная система, управляющая устройствами производства Cisco. Существует несколько веток разработки этой ОС, отличающейся поддерживаемыми функциями. Образ IOS хранится в файле, который находится на флеш-диске. Ни в коем случае не извлекайте флеш-диск, когда питание на устройство подано, это приведёт к повреждению файловой системы!
При загрузке IOS считывает конфигурационный файл с флеш-диска. Изначально такой файл отсутствует, получить доступ по сети к устройству нельзя, поэтому первоначальная настройка выполняется с помощью последовательного интерфейса (на устройстве порт обозначен как Console, используется специальный кабель-переходник DCE, оконцованный с одной стороны вилкой RJ-45, а с другой — штекером DB-9). Подключение к console выполняется с помощью программы screen:

```
screen /dev/ttyS0 9600
```

где /dev/ttyS0 — имя порта (в данном случае первый COM-порт), а 9600 — скорость соединения (можно опустить). Если установить соединение до включения питания, то можно увидеть процесс загрузки. По окончании распаковки IOS в память и чтения конфигурационного файла будет выдано приглашение нажать Enter для начала работы с командной строкой. Если вы подключились к console после загрузки, то ничего выведено не будет, однако нажать Enter надо.
Для управления устройством используется командный интерпретатор IOS. Командный интерпретатор выдаёт следующее приглашение:

```
Router>
```

Здесь Router — имя (hostname) устройства, а «>» - приглашение, указывающее на то, что работа выполняется в непривилегированном режиме. Вэтом режиме нельзя просмотреть или изменить конфигурацию устройства, однако можно просматривать его состояние.
Команда имеет следующую структуру:

```
Router>show ip interface Ethernet 0/0
```

Здесь show — непосредственно команда (вывести некоторую информацию), ip — уточнение запроса (информация, относящаяся к протоколу ip), interface — уточнение предыдущего параметра (информация, относящаяся к интерфейсам), Ethernet 0/0 — имя объекта, над которым надо выполнить команду (интерфейс Ethernet, находящийся в модуле 0, имеющий номер 0). Таким образом, эта команда означает «показать информацию об IP-интерфейсе Ethernet номер 0 из модуля 0». IOS при успешном выполнении команды обычно не выдаёт никаких сообщений (если это не команда show). Если команда синтаксически неверна, то будет выведено следующее сообщение:

```
Router>show the ip interface Ethernet 0/0
      ^
% Invalid input detected at '^' marker.
```

Это значит, что возникла ошибка при чтении команды в месте, отмеченном маркером «^».
Чтобы получить подсказку о команде, во время ввода наберите вопросительный знак («?»).
Командный интерпретатор запоминает введённые команды. К ранее выполненным командам можно вернуться с помощью клавиш со стрелками вверх и вниз. Для перемещения по тексту команды применяются клавиши со стрелками вправо и влево. Клавиша Tab позволяет завершить ввод термина, набранного не полностью. При это если введённые символы не позволяют однозначно завершить термин, будут дополнены только те символы, которые

являются общими для команд (например, при вводе s и нажатии Tab интерпретатор не сможет дополнить ввод до show, так как есть ещё команда set. Их общая часть — s). Если введённые символы позволяют однозначно определить подразумеваемый термин, то его (термин) можно не вводить до конца. Так, следующие команды идентичны:

```
Router>show ip interface Ethernet 0/0
Router>sh ip int eth0/0
```

Если во время работы с интерпретатором на экран было выведено сообщение от маршрутизатора (например, уведомление об отключении интерфейса), которое перекрыло текущий ввод, комбинация клавиш Ctrl+R позволит вернуть введённый текст.
Действие любой команды можно отменить, выполнив эту команду со словом no в начале:

```
Router>ip address 192.168.1.1 255.255.255.0
Router>no ip address 192.168.1.1 255.255.255.0
```

IOS имеет 16 уровней привилегий (от 0 до 15). Режим, о котором говорилось выше (непривилегированный) — режим 1 уровня (пользовательский режим). В этом режиме нельзя выполнять отладку, выполнять некоторые информационные команды (show), и изменять конфигурацию. Привилегированный режим является режимом 15 уровня и позволяет выполнять любые действия. Переход в привилегированный режим выполняется с помощью команды enable (en). При переходе в режим enable может быть запрошен пароль. Приглашение в режиме enable меняется на следующее:

```
Router>enable
Password:
Router#
```

Для предотвращения несанкционированного доступа к режиму enable можно установить пароль на переход в этот режим:

```
Router#enable secret <пароль>
```

Для изменения конфигурации требуется перейти в режим настройки. Для этого выполните следующую команду:

```
Router#configure terminal
или:
Router#conf t
```

Слово «terminal» в команде означает, что настройка будет выполняться вводом команд вручную. После перехода в режим настройки приглашение снова изменится:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Маршрутизатор перешёл в режим настройки глобальной конфигурации, то есть команды в этом режиме позволяют изменить конфигурацию устройства в целом. Для настройки отдельных параметров используется режим настройки конфигурации интерфейса (не всегда относится к сетевым интерфейсам). Чтобы перейти в этот режим, надо указать, с помощью какого интерфейса будет выполняться настройка. Например, команда для перехода к настройке ethernet-интерфейса выглядит следующим образом:

```
Router(config)#interface Ethernet0/0
Router(config-if)#
```

Режим настройки интерфейса относится не только к сетевым интерфейсам. В этом режиме также настраиваются маршрутизирующие протоколы, списки доступа и другие функции и объекты, например:

```
Router(config)#ip access-list standard test
Router(config-std-nacl)#exit
Router(config)#router rip
Router(config-router)#exit
Router(config)#subscriber-policy 1
Router(config-policy)#exit
Router(config)#
```

При смене режима меняется и приглашение. Для выхода из режима настройки интерфейса применяется команда exit. Для выхода из режима enable используется команда end или сочетание клавиш Ctrl+Z. В режиме настройки конфигурации нельзя применять команды show.
В IOS имеется два типа конфигурации — running-config (текущая конфигурация) и startup-config (загрузочная конфигурация). running-config используется до перезагрузки устройства, поэтому все изменения которые требуется применять при загрузке устройства, должны быть сохранены в startup-config следующей командой:

```
Router#copy running-config startup-config
или:
Router#copy run st
```

Чтобы сохранить текущую конфигурацию в произвольный файл (этот файл не будет прочтён при загрузке), выполните следующую команду:

```
Router#copy running-config filename
```

Файл конфигурации является простым текстовым файлом, поэтому его можно просматривать и редактировать обычными текстовыми редакторами.
Просмотреть текущую конфигурацию можно следующей командой:

```
Router#show running-config
или:
Router#sh run
```

Просмотреть версию IOS можно следующей командой:

```
Router>show version
```

2. Локальные пользователи

```
! Создание нового пользователя
! Пароль будет храниться в файле конфигурации в открытом виде
(config)# username <имя пользователя> password <пароль>
! Включение хранения паролей в хешированном виде
(config)# service password-encryption
! Назначение начального уровня привилегий
(config)# username <имя пользователя> privilege <уровень>
```

3. Интерфейсы

Маршрутизатор оборудован следующими интерфейсами:

- Порт console. Предназначен для управления устройством с помощью непосредственного соединения кабелем-адаптером DCE, оконцованным с одной стороны вилкой RJ-45, а с другой — разъёмом DB-9;
- Порт AUX. Предназначен для подключения маршрутизатора к модему для удалённого управления устройством с помощью терминала;
- Порты Ethernet.

Задать пароль на установление терминального соединения через порт console[1]:

```
! Переход в режим enable
> enable
! Переход в режим глобальной настройки
# configure terminal
! Переход в режим настройки канала console
(config)# line console 0
! Задание пароля
(config-line)# password <пароль>
```

В дальнейшем шаги по переходу в режим enable и глобальной настройки будут опускаться.

Во время настройки при вводе доменных имён пользователь может опечататься. Чтобы не ждать, пока устройство будет безуспешно пытаться разрешить несуществующее имя, можно выполнить следующую команду:

```
(config)# no ip domain lookup
```

Учтите, что устройство после этой команды перестанет пытаться разрешать имена.

Ethernet-интерфейсы именуются по следующей схеме:
<тип_подключения><номер_модуля>/<номер_порта_в_модуле>

Типы подключения перечислены в следующей таблице:

Тип подключения	Мнемоники
Ethernet 10 Mbit/s	Ethernet (e)
FastEthernet 10/100 Mbit/s	FastEthernet (fa)
GigabitEthernet 10/100/1000 Mbit/s	GigabitEthernet (gi)

Тип подключения можно сокращать до минимально уникальной длины.

Настроить сетевой интерфейс:

```
! Переход в режим настройки сетевого интерфейса
! Приводится пример для интерфейса FastEthernet0/0
(config)# interface FastEthernet0/0
! или, кратко
(config)# interface fa0/0
```

1 Строки, начинающиеся с восклицательного знака, IOS не обрабатывает. Можно считать их комментариями

```
! Можно ввести описание интерфейса
(config-if)# description <описание>
! Задание IP-адреса
(config-if)# ip address <адрес> <маска>
! Например, ip address 10.0.0.1 255.0.0.0
! Для получения адреса по dhcp выполните команду ip address dhcp
```

По умолчанию сетевые интерфейсы выключены. Активировать интерфейс:

```
(config-if)# no shutdown
```

Сбросить настройки интерфейса:

```
(config)# default interface <имя>
```

Просмотреть информацию об интерфейсах:

```
# show interface <имя>
! Показать информацию об интерфейсе, относящуюся к протоколу IP
# show ip interface <имя>
```

Для указания параметров DNS применяются следующие команды (из режима глобальной настройки):

```
! Используемый DNS-сервер
(config)# ip name-server <адрес>
! DNS-имя устройства
(config)# hostname <имя>
! Домен, к которому принадлежит устройство
(config)# ip domain name <имя>
```

В IOS имеются утилиты ping и traceroute для проверки связности:

```
> ping <IP-адрес_или_имя>
> traceroute <IP-адрес_или_имя>
```

Прервать выполнение команды traceroute (trace) можно с помощью сочетания клавиш Ctrl+Shift+6.

Настроить удалённый доступ по протоколу telnet:

```
! Переход в режим настройки виртуального телетайпа (vty)
! Команда указывает диапазон настраиваемых линий
! Количество линий определяет максимальное число одновременных подключений
! Обычно линий 16, но на некоторых устройствах только 5
! Для настройки конкретной линии укажите только один номер (line vty 0)
(config)# line vty 0 4
! Не запрашивать пароль
(config-line)# no login
! или использовать локальный список пользователей (по умолчанию)
```

```
(config-line)# login local
! Задать уровень привилегий, выдаваемых при подключении
! По умолчанию - 1
(config-line)# privilege level <уровень>
! Время, после которого сеанс будет разорван в любом случае
(config-line)# absolute-timeout <время_в_минутах>
```

4. Журналирование

Все системные сообщения и выходные сообщения от debug-команд отправляются в процесс журналирования. Путём настройки этого процесса можно добиться вывода журналов в буфер, на экран терминала или на syslog-сервер. По умолчанию включен вывод журнальных сообщений на экран терминала, выводятся сообщения уровня опасности debug.

Для Cisco уровни опасности сообщений называются следующим образом:

Уровень	Числовой код	Смысл
emergencies	0	Система нестабильна
alerts	1	Требуется немедленно принять меры
critical	2	Критическое состояние
errors	3	Произошла ошибка
warnings	4	Предупреждение об ошибке
notifications	5	Нормальное, но требующее внимания событие
informational	6	Информационное сообщение
debugging	7	Отладочное сообщение

IOS различает следующие facility:

facility	Смысл
auth	Система аутентификации
cron	Системный планировщик cron
daemon	Системная служба (демон)
kern	Ядро
local0-local7	Локально определённые сообщения
lpr	Система линейной печати
mail	Почтовая система
news	Система USENET
sys9-sys14	Системные сообщения
syslog	Служба syslog
user	Пользовательский процесс
uucp	Система UUCP

Управление журналированием

Отключить вывод журнальных сообщений на консоль:

```
(config)# no logging console
```

Настроить вывод журнальных сообщений:

```
! Вывод в буфер в памяти коммутатора
! Буфер может иметь размер от 4096 до 2147483647 байт
```

```
(config)# logging buffered <размер_буфера>
! Вывод в файл
(config)# logging file flash:<имя_файла>
! Выбор минимального уровня опасности выводимых сообщений
! Для последовательного терминала (по умолчанию debugging)
(config)# logging console <уровень>
! Для консоли (telnet, ssh, …) (по умолчанию debugging)
(config)# logging monitor <уровень>
```

Настроить отправку журнальных сообщений на syslog-сервер:

```
! Указание адреса syslog-сервера
(config)# logging <адрес>
! Выбор минимального уровня опасности выводимых сообщений
! По умолчанию informational
(config)# logging trap <уровень>
! Выбор facility для отправки сообщений (по умолчанию local7)
(config)# logging facility <facility>
```

Просмотр настройки журналирования

Вывести состояние процесса журналирования:

```
# show logging
```

5. VLAN

В данном разделе рассматриваются VLAN протокола IEEE 802.1Q

По умолчанию все порты коммутатора включены в VLAN с vlan-id 1 и именем VLAN0001. Новым VLAN по умолчанию присваиваются имена вида VLANxxxx, где xxxx — vlan-id, дополненный слева нулями до 4 знаков.

Общий порядок создания VLAN таков:

- Создать VLAN.
- Добавить в неё порты.

При добавлении очередного порта в VLAN можно выбрать один из двух режимов:

1) access — режим порта доступа. Такой порт снимает тег 802.1Q с исходящего пакета.
2) trunk — режим магистрального порта. Такой порт не трогает тег 802.1Q ни на каких пакетах.

Для VLAN ID корректным является диапазон от 1 до 4094. VLAN ID в диапазоне 1002-1005 являются зарезервированными и не должны использоваться. VLAN ID в диапазоне 1006-4094 относятся к расширенному диапазону. VLAN ID расширенного диапазона могут использоваться только тогда, когда коммутатор находится в прозрачном режиме VTP (то есть VTP отключен). VTP (VLAN Trunking Protocol) — протокол Cisco, предназначенный для анонсирования другим коммутаторам доступных VLAN ID. Аналогичный открытый протокол — GVRP (GARP VLAN Registration Protocol). По умолчанию VTP отключен. Перевести VTP в прозрачный режим можно следующей командой:

```
(config)# vtp mode transparent
```

Параметр <*vlan-list*> может раскрываться как перечень VLAN ID (<*vlan-id1*>,<*vlan-id3*>,...,<*vlan-idN*>) или как диапазон (<*vlan-id1*>-<*vlan-idN*>), пробелы между элементами не ставятся.

Управление VLAN

Создать VLAN в режиме config-vlan:

```
! Переход в режим config-vlan
(config)# vlan <vlan-id>
! Задание имени VLAN (необязательно)
(config-vlan)# name <имя>
```

Создать VLAN в режиме vlan database (не рекомендуется, так как этот режим устарел и будет исключён в одном из будущих выпусков IOS):

```
! Переход в режим vlan database
# vlan database
! Создать одну VLAN
(vlan)# vlan <vlan-id> [name <имя>]
! Создать диапазон VLAN
(vlan)# vlan <vlan-id1> end <vlan-idN>
```

Добавить порт доступа в VLAN:

```
! Переход в режим настройки интерфейса
(config)# interface <имя_интерфейса>
! Выбор режима access
(config-if)# switchport mode access
! Выбор VLAN, в которую входит порт
(config-if)# switchport access vlan <vlan-id>
```

Добавить магистральный порт в VLAN:

```
! Переход в режим настройки интерфейса
(config)# interface <имя_интерфейса>
! Выбор типа инкапсуляции 802.1Q на порту
(config-if)# switchport trunk encapsulation dot1q
! Также может быть выбрана инкапсуляция
! по протоколу Cisco – ISL (Inter-Switch Link)
! или negotiate – автосогласование типа инкапсуляции
!
! Выбор режима trunk
(config-if)# switchport mode trunk
```

Настроить список допустимых VLAN на магистральном порту:

```
! Переход в режим настройки интерфейса
(config)# interface <имя_интерфейса>
! Добавление в список нескольких VLAN
(config-if)# switchport trunk allowed vlan add <vlan-list>
! Добавление в список всех возможных VLAN
(config-if)# switchport trunk allowed vlan all
! Добавление в список всех возможных VLAN, кроме перечисленных
(config-if)# switchport trunk allowed vlan except <vlan-list>
! Удаление из списка нескольких VLAN
(config-if)# switchport trunk allowed vlan remove <vlan-list>
! Установка native VLAN (VLAN, меткой которой помечаются непомеченные пакеты)
(config-if)# switchport trunk native vlan <vlan-id>
```

Просмотр конфигурации VLAN

Просмотр списка всех настроенных VLAN:

```
#show vlan
```

Просмотр информации о конкретной VLAN ID:

```
#show vlan id <vlan-id>
```

Просмотр информации о состоянии порта:

```
# show interface <имя> switchport
```

6. STP

В коммутаторах Cisco вместо протокола STP (IEEE 802.1d) обычно применяется протокол PVST+ (Per-VLAN Spanning Tree); название обычно сокращают до PVST. Этот протокол предназначен для создания отдельного экземпляра протокола STP для каждого VLAN. Протокол был разработан Cisco, так как на момент стандартизации STP комитет IEEE не стандартизовал VLAN. Протокол PVST позволяет отдельно управлять состоянием порта в разных VLAN, тем самым выравнивая нагрузку. Так, например, трафик чётных VLAN может быть перенаправлен через один порт, а нечётных — через другой.

В протоколе RSTP (IEEE 802.1w) также не предусмотрено использование нескольких экземпляров протокола на порту, поэтому Cisco разработала протокол RPVST (Rapid PVST, также имеет название PVRST, Per-VLAN Rapid Spanning Tree) на основе RSTP.

Протокол MSTP (IEEE 802.1s, в терминологии Cisco — MIST, Multiple Instances of Spanning Trees) поддерживается устройствами Cisco, однако для его настройки требуется выполнить больший объём работы, так как требуется определять связку каждой VLAN с назначенными экземплярами протокола RSTP, в отличие от PVST и RPVST(PVRST). Использование MSTP подразумевает создание нескольких экземпляров протокола RSTP.

В данном разделе параметр *<vlan-id>* может быть заменён на указание конкретного номера VLAN или на указание списка VLAN перечислением (*<vlan-id1>*, *<vlan-id3>*, …, *<vlan-idN>*) или диапазоном (*<vlan-id1>*-*<vlan-idN>*).

Настройка STP и RSTP

Однозначно задать использование протоколов STP и PVST:

```
(config)# spanning-tree mode pvst
```

По умолчанию включен на VLAN 1 (которая включает в себя все порты коммутатора).

Однозначно задать использование протоколов RSTP и RPVST(PVRST):

```
(config)# spanning-tree mode rapid-pvst
```

Включить использование протокола STP в определённых VLAN:

```
(config)# spanning-tree vlan <vlan-id>
```

Назначить приоритет коммутатора:

```
(config)# spanning-tree vlan <vlan-id> priority <приоритет>
```

По умолчанию коммутатор получает приоритет 32768. При настройке приоритетов вручную важно следить за тем, чтобы назначаемый приоритет не был выше, чем приоритеты корневых мостов. Приоритет может принимать значения от 0 до 61440 с инкрементом 4096 (4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440).

Назначить коммутатор основным корневым мостом:

```
(config)# spanning-tree vlan <vlan-id> root primary [diameter <диаметр>]
```

Параметром diameter можно задать диаметр сети (диаметр — расстояние в количестве коммутаторов между двумя самыми удалёнными друг от друга узлами в пределах от 2 до 7, по умолчанию 7), что заставит коммутатор пересчитать таймеры STP для большей производительности. Задание диаметра применяется только для корневого моста, так как именно он управляет таймерами всех остальных мостов, использующих STP. Приоритет основного корневого моста по умолчанию 24576.

Назначить коммутатор запасным корневым мостом:

```
(config)# spanning-tree vlan <vlan-id> root secondary
```

Приоритет резервного корневого моста по умолчанию 28672.

Назначить приоритет порта:

```
! для конкретного порта
#interface <номер_порта>
(config-if)# spanning-tree port-priority <приоритет>
! или для VLAN
(config)# spanning-tree vlan <vlan-id> port-priority <приоритет>
```

Приоритет может принимать значения от 0 до 240 с инкрементом 16 (0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240), по умолчанию 128.

Настроить таймеры STP (указаны описание, минимальное-максимальное значение, значение по умолчанию):

```
! Максимальное время пребывания в состояниях listening и learning
! до перехода в состояние forwarding (4-30, 15)
(config)# spanning-tree vlan <vlan-id> forward-time <значение>
! Интервал между отправкой Hello BPDU (1-10, 2)
(config)# spanning-tree vlan <vlan-id> hello-time <значение>
! Таймаут получения BPDU от корневого коммутатора до пересчёта дерева (6-40, 20)
(config)# spanning-tree vlan <vlan-id> max-age <значение>
```

Назначить стоимость интерфейса:

```
(config)# spanning-tree vlan <vlan-id> cost <стоимость>
```

По умолчанию используются значения из следующей таблицы:

Скорость интерфейса	Стоимость
10 Мбит/с	100
100 Мбит/с	19
1 Гбит/с	4
10 Гбит/с	2

Настройка MSTP

Однозначно задать использование протокола MSTP:

```
(config)# spanning-tree mode mst
```

Перейти в режим настройки MSTP:

```
(config)# spanning-tree mst configuration
(config-mst)#
```

Настроить параметры MSTP (должны совпадать у всех коммутаторов, охваченных MSTP):

```
(config-mst)# name <имя_региона>
(config-mst)# revision <ревизия>
```

Длина имени региона — не более 32 символов, номер ревизии может принимать значения в диапазоне от 0 до 65535.

Задать привязку VLAN к экземплярам протокола RSTP:

```
! перечислением номеров vlan
(config-mst)# instance <номер_экземпляра> vlan <vlan-id>, <vlan-id>, ...
! или указанием диапазона
(config-mst)# instance <номер_экземпляра> vlan <vlan-id1>-<vlan-idN>
```

Номер экземпляра может принимать значения в диапазоне от 1 до 15

Назначить коммутатор основным корневым мостом:

```
(config)# spanning-tree mst <номер_экземпляра> root primary [diameter <диаметр>]
```

Диаметр можно указать только для экземпляра с номером 0.

Назначить коммутатор запасным корневым мостом:

```
(config)# spanning-tree mst <номер_экземпляра> root secondary
```

Назначить приоритет порта:

```
#interface <номер_порта>
(config-if)# spanning-tree mst <номер_экземпляра> port-priority <приоритет>
```

Назначить приоритет коммутатора:

```
(config-if)# spanning-tree mst <номер_экземпляра> priority <приоритет>
```

Настроить таймеры STP для всех экземпляров:

```
(config)# spanning-tree mst forward-time <значение>
(config)# spanning-tree mst hello-time <значение>
(config)# spanning-tree mst max-age <значение>
```

Технология Cisco STP Root Guard

Технология Root Guard предназначена для предотвращения возможности выбора случайного коммутатора сети в качестве корневого вместо текущего корневого моста в том случае, если приоритет этого случайного коммутатора меньше, чем у текущего корневого моста. Технология должна настраиваться на всех устройствах, которые используют STP. Суть технологии заключается в жёстком назначении конкретному интерфейсу роли Root Port (корневого порта).

Включить Root Guard на коммутаторе:

```
(config)# interface GigabitEthernet0/8
(config-if)# spanning-tree rootguard
```

Просмотр состояния STP

Показать подробную информацию обо всех интерфейсах и виртуальных сетях, на которых включен протокол STP:

```
Switch# show spanning-tree
```

Показать подробную информацию о конкретном интерфейсе:

```
Switch# show spanning-tree interface <интерфейс>
```

Показать подробную информацию о конкретной виртуальной сети:

```
Switch# show spanning-tree vlan <vlan-id>
```

Включить отладку процедуры внесения изменений в топологию:

```
Switch# debug spantree events
```

Включить отладку процедуры рассылки BPDU:

```
Switch# debug spantree tree
```

7. SPAN

SPAN (Switched Port Analyser, анализатор коммутируемого порта) — технология зеркалирования порта в терминологии Cisco. Источником пакетов может быть отдельный порт или VLAN. Сеансом SPAN (SPAN session) называется сочетание источника (порта или VLAN) и приёмника. В рамках сеанса нельзя одновременно использовать источник-порт иисточник-VLAN. Выходных портов также может быть несколько, но не более 64. Если пропускная способность выходного порта ниже, чем у входного, то сеанс SPAN, объединяющий эти порты, может терять пакеты, однако не повлияет на работу входного порта. Для работы SPAN необходимо, чтобы источник и приёмник были активны.

По умолчанию перед отправкой пакета на порт-приёмник с пакета снимается тег VLAN (ISL или 802.1Q). Также невозможно следить за пакетами протоколов 2 уровня, таких как STP. Однако ключ `encapsulation replicate` изменяет поведение SPAN таким образом, что пакет передаётся на выходной порт неизменённым и перехватываются пакеты всех протоколов.

По умолчанию SPAN отключен.

Управление SPAN

Создать сеанс SPAN:

```
! Указание входного порта или VLAN
! Номер сеанса принимает значения от 1 до 66
(config)# monitor session <номер_сеанса> source (interface <имя>|vlan <vlan-id>)
! Включение зеркалирования нескольких портов (или VLAN)
! «,» и «-» обрамляются пробелами
(config)# monitor session <номер_сеанса> source interface <имя> , <имя> - <имя>
! Задание списка VLAN, трафик которых перехватывается на порту
(config)# monitor session <номер_сеанса> filter vlan <vlan-id> , <vlan-id> -
<vlan-id>
! Задание фильтра на направление трафика
! Любое
(config)# monitor session <номер_сеанса> source interface <имя> both
! Входящий
(config)# monitor session <номер_сеанса> source interface <имя> rx
! Исходящий
(config)# monitor session <номер_сеанса> source interface <имя> tx
!
! Указание выходного порта
(config)# monitor session <номер_сеанса> destination interface <имя>
[encapsulation replicate]
! Указание нескольких выходных портов
(config)# monitor session <номер_сеанса> destination interface <имя> , <имя> -
<имя> [encapsulation replicate]
```

Просмотр состояния SPAN

Вывести сведения обо всех сеансах SPAN:

```
# show monitor
```

Вывести сведения о конкретном сеансе SPAN:

```
# show monitor session <номер_сеанса>
```

8. Коммутация 3 уровня

Чтобы включить функции маршрутизации на порту коммутатора, можно пойти двумя путями:

- объединить порт (группу портов) в VLAN. VLAN по умолчанию являются интерфейсом 3 уровня;
- перейти в режим настройки порта и выполнить команду `no switchport`.

После создания интерфейса 3 уровня с ним можно работать как с интерфейсом маршрутизатора. Однако предварительно требуется включить функции третьего уровня командой `ip routing`. После этой команды можно добавлять статические маршруты или использовать протокол RIP.

9. NAT

Для функционирования NAT маршрутизатор должен знать, какие интерфейсы подключены к внутренним сетям, а какие — к внешним.

Управление NAT

Указать внешние и внутренние интерфейсы:

```
! Внутренний интерфейс
(config)# interface <имя>
(config-if)# ip nat inside
! Внешний интерфейс
(config)# interface <имя>
(config-if)# ip nat outside
```

Внутренних и внешних интерфейсов может быть более, чем по одному.

Создать правило статической трансляции адресов (однозначное соответствие между адресом из внутренней сети и адресом из внешней сети):

```
(config)# ip nat inside source static <внутренний_адрес> <внешний_адрес>
```

Создать правило динамической трансляции «сеть в сеть»:

```
! Создание диапазона внешних адресов
Router(config)#ip nat pool <имя_диапазона> <начальный_IP-адрес>
<конечный_IP-адрес> netmask <маска>
! Создание стандартного ACL, содержащего разрешающую запись для внутренней сети
(config)# access-list <номер_ACL> permit <адрес_источника>
<инвертированная_маска_источника>
! Создание правила NAT
(config)# ip nat inside source list <номер_ACL> pool <имя_диапазона>
```

Создать правило динамической трансляции «сеть в адрес»:

- если внешний адрес динамический

```
(config)# ip nat inside source list <номер_ACL> interface
<имя_внешнего_интерфейса>
```

- (дополнительно) если внешний адрес статический

```
! Создание диапазона адресов, содержащего единственный адрес
(config)# ip nat pool <имя_диапазона> <IP-адрес> <IP-адрес> netmask <маска>
! Создание правила NAT
(config)# ip nat inside source list <номер_ACL> pool <имя_диапазона>
```

Сделать порт узла, находящегося за транслятором, доступным извне (перенаправление порта, port forward):

```
(config)# ip nat inside source static (tcp|udp) <внутренний_адрес> <порт>
(<внешний_адрес> <порт> | interface <имя_интерфейса>)
```

Например, чтобы в условиях динамического внешнего адреса, принадлежащего интерфейсу FastEthernet0/0, сделать доступным порт 22/tcp хоста 192.168.1.1 извне, применяется следующая команда:

```
Router(config)#ip nat inside source static tcp 192.168.1.1 22 interface fa0/0
```

Очистить таблицу трансляций:

```
! Удаление всех записей
# clear ip nat translation *
! Удаление одной записи о внутренней трансляции
# clear ip nat translation inside <внешний_адрес> <внутренний_адрес>
! Удаление одной записи о внешней трансляции
# clear ip nat translation outside <внутренний_адрес> <внешний_адрес>
```

Просмотр состояния NAT

Вывести список активных трансляций:

```
# show ip nat translations
```

Вывести статистику:

```
# show ip nat statistics
```

10. IGMP

По умолчанию перехват пакетов протокола IGMP включен глобально на коммутаторе и для каждого VLAN.

Управление IGMP

Включить перехват IGMP (если выключен):

```
! Глобально для коммутатора
(config)# ip igmp snooping
! Для конкретной VLAN
! Требуется предварительно глобально включить IGMP
(config)# ip igmp snooping vlan <vlan-id>
```

Статически включить интерфейс в Multicast-группу:

```
(config)# ip igmp snooping vlan <vlan-id> static <IP-адрес_группы> interface
<имя_интерфейса>
```

Включить функцию Immediate Leave. Эта функция позволяет исключить порт из Multicast-группы, как только на порт приходит сообщение IGMP Leave. Полезно, если к порту подключено не более одного конечного узла:

```
(config)# ip igmp snooping vlan <vlan-id> immediate-leave
```

Просмотр сведений о настройке IGMP Snooping

Вывести глобальные настройки IGMP:

```
# show ip igmp snooping
```

Вывести настройки IGMP для конкретной VLAN:

```
# show ip igmp snooping vlan <vlan-id>
```

Вывести таблицы IGMP по Mutlicast-группам:

```
# show ip igmp snooping groups
```

11. Статическая маршрутизация

Управление статическими маршрутами

Создать статический маршрут:

```
(config)# ip route <адрес_назначения> <маска_адреса_назначения>
<адрес_маршрутизатора> [<метрика>] [permanent]
```

Опция permanent указывает на то, что маршрут требуется сохранить, даже если интерфейс, к которому относится этот маршрут, становится неработоспособным. Рекомендуется не использовать эту опцию.

Пример создания статического маршрута:

```
(config)# ip route 192.168.1.0 255.255.255.0 192.168.1.10
```

Создать маршрут по умолчанию:

```
(config)# ip default-gateway 192.168.1.10
```

Просмотр таблицы маршрутизации

Вывести таблицу маршрутизации:

```
# show ip route
```

Вывести маршруты только в определённую сеть:

```
# show ip route <адрес_сети>
```

12. EIGRP

EIGRP (Enhanced Internal Gateway Routing Protocol) — усовершенствованный дистанционно-векторный протокол динамической маршрутизации, разработанный компанией Cisco. Основные особенности:

- применение многоадресных рассылок обновлений маршрутов;
- отправка обновлений маршрутов только в случае обнаружения изменения;
- обновление таблиц только в тех маршрутизаторах, которым требуется информация об изменении топологии;
- малое время сходимости протокола;
- исключение циклов из топологии.

Для передачи обновлений используется протокол RTP. Этот протокол обеспечивает гарантированную доставку пакетов (reliable multicast, технология Cisco) и сохранение порядка пакетов.

Существует 5 типов сообщений:

3) Hello — с помощью этих сообщений маршрутизаторы обнаруживают соседей. Отправляются с помощью multicast, не требуют подтверждения.
4) Update — содержит обновления маршрутов. Отправляется только тем маршрутизаторам, которым надо узнать об этом обновлении. Используется unicast или multicast. На это сообщение должен быть отправлен ответ ACK.
5) Query — отправляется соседям, когда маршрутизатор не может определить возможного преемника (feasible successor) для маршрута (запасного маршрутизатора для данного направления), с вопросом, нет ли у них возможного преемника для этого маршрута. Обычно используется multicast. На это сообщение должен быть отправлен ответ ACK.
6) Reply — отправляется в ответ на Query строго тому, кто отправил Query. На это сообщение должен быть отправлен ответ ACK.
7) ACK — сообщение, подтверждающее получение сообщений Update, Query или Reply. Используется негарантированная доставка.

По умолчанию период отправки hello-пакета — 5 секунд. Если в течение hold time (по умолчанию 15 секунд, 3 hello-интервала) от соседа не пришло ни одного hello, он считается отключенным. Маршрутизатор получает значения интервалов hello и hold time от соседа.

Чтобы установить соседские отношения, маршрутизаторы должны быть в одной автономной системе и пройти аутентификацию.

Метрика EIGRP составляется из следующих параметров:

1. Bandwidth — наименьшая пропускная способность канала из сообщённых участниками канала;
2. Delay — суммарная задержка прохождения всего пути;
3. Reliability — наихудший показатель надежности на всем пути на основании сообщённых интервалов keepalive;
4. Loading — наихудший показатель загрузки канала на всем пути на основании текущей загрузки канала (в пакетах/с) и настроенной на интерфейсе bandwidth.

По умолчанию используются первые две характеристики. Использование прочих характеристик приводит к частому пересчёту маршрутов.

Настройка EIGRP

Включить EIGRP:

```
! Включение протокола EIGRP
(config)# router eigrp <номер_автономной_системы>
! Перечисление сетей, в которых работает протокол
(config-router)# network <адрес_сети> netmask <маска_сети>
```

Изменить таймеры протокола для конкретного интерфейса:

```
! Переход в режим настройки интерфейса
(config)# interface <имя_интерфейса>
! Задание интервала Hello
(config-if)# ip hello-interval eigrp <номер_АС> <время_в_секундах>
! Задание интервала Hold
(config-if)# ip hold-time eigrp <номер_АС> <время_в_секундах>
```

Просмотр состояния EIGRP

Вывести информацию о соседях:

```
# show ip eigrp neighbors
```

Вывести информацию об интерфейсах, на которых работает EIGRP:

```
# show ip eigrp interfaces
```

Вывести таблицу топологии EIGRP:

```
# show ip eigrp topology
```

Вывести таблицу маршрутов, полученных по EIGRP:

```
# show ip route eigrp
```

13. OSPF

Управление OSPF

Включить протокол OSPF:

```
! Разрешение использования протокола OSPF
(config)# router ospf <идентификатор_процесса>
! Связывание сетей с номерами областей
(config-router)# network <адрес_сети> <маска_адреса_сети> area
<идентификатор_области>
```

Идентификатор процесса является числом. Идентификатор области может записываться как в виде числа, так и в виде октетов (как IP-адрес).

Пример настройки OSPF:

```
(config)# router ospf 1
(config-router)# network 192.168.1.0 255.255.255.0 area 1
(config-router)# network 192.168.2.0 255.255.255.0 area 0.0.0.2
```

Задать идентификатор маршрутизатора (Router ID) вручную:

```
(config)# router ospf <идентификатор_процесса>
(config-router)#router-id <IP-адрес>
```

Если Router ID не указан, то в качестве этого идентификатора будет назначен наибольший IP-адрес из всех настроенных.

Настройка интерфейса, участвующего в процессе OSPF:

```
(config)# interface <имя>
! Приоритет маршрутизатора
! Влияет на выборы DR в сети интерфейса
! Если priority=0, интерфейс не участвует в выборах
(config-if)# ip ospf priority <приоритет>
! Стоимость пути
! Чем меньше значение, тем приоритетнее путь
(config-if)# ip ospf cost <стоимость>
! Интервал повторной передачи в секундах
(config-if)# ip ospf retransmit-interval <время>
! Интервал передачи сообщений Hello в секундах
(config-if)# ip ospf hello-interval <время>
! Время в секундах, по истечении которого отказ интерфейса регистрируется
! По умолчанию, в 4 раза больше hello-interval
(config-if)# ip ospf dead-interval <время>
! Отключение аутентификации
(config-if)# ip ospf authentication null
! Включение аутентификации открытым текстом
```

```
(config-if)# ip ospf authentication
(config-if)# ip ospf authentication-key <пароль>
! Включение аутентификации хешами MD5
(config-if)# ip ospf authentication message-digest
(config-if)# ip ospf message-digest-key <номер_ключа> md5 <ключ>
```

Принудительно перезапустить алгоритм SPF:

```
# clear ip ospf process
```

Включить распространение других маршрутов, полученных из прочих источников, через процесс OSPF:

```
(config)# router ospf <идентификатор_процесса>
! Распространение маршрутов к подключенным сетям
(config-router)# redistribute connected
! Распространение статических маршрутов
(config-router)# redistribute static
! Распространение маршрутов BGP
(config-router)# redistribute bgp
! Распространение маршрутов EIGRP
(config-router)# redistribute eigrp
```

Просмотр состояния OSPF

Вывести информацию о протоколе:

```
# show ip ospf
```

Вывести информацию об известных граничных маршрутизаторах:

```
# show ip ospf border-routers
```

Вывести информацию о процессе OSPF на интерфейсе:

```
# show ip ospf interface <имя>
```

Показать известных соседей:

```
# show ip ospf neighbor
```

Вывести подробную информацию о соседе:

```
# show ip ospf neighbor <IP-адрес_соседа>
```

Показать маршруты, полученные по OSPF:

```
# show ip route ospf
```

14. BGP

Управление BGP

Включить и настроить BGP:

```
! Создание процесса BGP и указание номера автономной системы (АС)
(config)# router bgp <номер_АС>
! Ручное указание идентификатора маршрутизатора
! Автоматически будет выбран наибольший IP-адрес из настроенных
(config-router)# router-id <IP-адрес>
! Указание соседа
(config-router)# neighbor <IP-адрес> remote-as <номер_удалённой_АС>
! Задание описания (комментария) для соседа
(config-router)# neighbor <IP-адрес> description <описание>
! Включение аутентификации соседа
(config-router)# neighbor <IP-адрес> password <пароль>
! Изменение таймеров keepalive и hold глобально
! По умолчанию keepalive – 60 секунд, hold – 180 секунд
(config-router)# timers bgp <интервал_keepalive> <интервал_hold>
! Изменение таймеров keepalive и hold для конкретного соседа
(config-router)# neighbor <IP-адрес> timers bgp <интервал_keepalive>
<интервал_hold>
! Ручное задание веса маршрута
(config-router)# neighbor <IP-адрес> weight <вес>
! Указание сетей, которые надо анонсировать
(config-router)# network <адрес_сети> netmask <маска_адреса_сети>
```

Включить распространение других маршрутов, полученных из прочих источников, через процесс BGP:

```
(config)# router bgp <номер_АС>
! Распространение маршрутов к подключенным сетям
(config-router)# redistribute connected
! Распространение статических маршрутов
(config-router)# redistribute static
! Распространение маршрутов OSPF
(config-router)# redistribute ospf
! Распространение маршрутов EIGRP
(config-router)# redistribute eigrp
```

Применить изменения, сделанные в конфигурации протокола BGP:

```
! Полный сброс результатов работы протокола
# clear ip bgp *
```

```
! Полный сброс результатов работы протокола для конкретного соседа
# clear ip bgp <адрес_соседа>
```

Просмотр состояния BGP

Вывести информацию о протоколе:

```
# show ip bgp
```

Вывести краткую информацию о соседях:

```
# show ip bgp summary
```

Вывести детальную информацию о соседях:

```
# show ip bgp neighbors
```

Показать маршруты, полученные от конкретного соседа:

```
# show ip bgp neighbors <IP-адрес_соседа> routes
```

Показать маршруты, анонсируемые конкретному соседу:

```
# show ip bgp neighbors <IP-адрес_соседа> advertised-routes
```

Показать маршруты, полученные по BGP:

```
# show ip route bgp
```

15. Port Security

По умолчанию Port Security отключен на всех портах. Port Security не может быть включен на выходном порту SPAN. Для включения Port Security необходимо задать значение параметра switchport mode (access или trunk), так как Port Security не может быть включен на порту с настройками по умолчанию.

Управление Port Security

Включить Port Security на порту:

```
! Переход в режим настройки интерфейса
(config)# interface <имя>
! Выбор режима работы порта
(config-if)# switchport mode (access|trunk)
! Включение Port Security
(config-if)# switchport port-security
! Указание максимального количества запоминаемых MAC-адресов
(config-if)# switchport port-security maximum <значение>
! Указание максимального количества запоминаемых MAC-адресов для конкретной VLAN
! vlan-list может содержать список VLAN, разделённых запятыми, или диапазон
(config-if)# switchport port-security maximum <значение> vlan <vlan-list>
```

Задание реакции коммутатора на нарушение защиты Port Security:

```
! Запрет пакетов от неизвестного источника без уведомления
! Для магистрального порта VLAN срабатывает при нарушении защиты
! хотя бы в одной VLAN, поэтому не рекомендуется для switchport trunk
(config-if)# switchport port-security violation protect
! Запрет пакетов от неизвестного источника с уведомлением
! (SNMP trap, запись в syslog, инкремент счётчика нарушений)
(config-if)# switchport port-security violation restrict
```

Чтобы снять ограничение, вызванное реакциями protect или restrict, нужно удалить часть легитимных MAC-адресов или повысить количество запоминаемых.

```
! Перевод порта в состояние «отключен из-за ошибки»
(config-if)# switchport port-security violation shutdown
! Перевод порта в состояние «отключен из-за ошибки» только в той VLAN,
! в которой обнаружено нарушение
(config-if)# switchport port-security violation shutdown vlan
```

Чтобы вывести интерфейс из состояния «отключен из-за ошибки», нужно в режиме настройки этого интерфейса последовательно выполнить команды `shutdown` и `no shutdown`, либо из режима enable выполнить команду `errdisable recovery cause psecure-violation`.

Добавить легитимный MAC-адрес на порту:

```
! Для всех VLAN
```

```
(config-if)# switchport port-security mac-address <MAC-адрес>
! Для конкретных VLAN
(config-if)# switchport port-security mac-address <MAC-адрес> vlan <vlan-id>
```

Очистить список всех MAC-адресов, учтённых Port Security:

```
# clear port-security all
```

Просмотр состояния Port Security

Вывести настройки Port Security для коммутатора в целом:

```
# show port-security
```

Вывести настройки Port Security для конкретного порта:

```
# show port-security interface <имя>
```

Вывести заданные вручную легитимные MAC-адреса для порта:

```
# show port-security interface <имя> address
```

Вывести максимальное количество легитимных MAC-адресов на VLAN для интерфейса:

```
# show port-security interface <имя> vlan
```

16. 802.1X

Для работы протокола 802.1X необходимо настроить механизмы AAA (Аутентификация, Авторизация, Аккаунтинг). По умолчанию механизмы AAA отключены и протокол 802.1X неактивен. Порт, являющийся магистральным портом VLAN, и зеркалирующие порты не могут участвовать в процедурах 802.1X.

Коммутатор, выполняющий процедуры 802.1X, обычно работает с RADIUS-сервером. Естественно, перед настройкой 802.1X необходимо указать RADIUS-сервер с помощью команды `radius-server`.

Настройка 802.1X

Включить использование протокола 802.1X для аутентификации на порту:

```
! Создание новой модели AAA
(config)# aaa new-model
! Создание списка методов аутентификации для новой модели
! Вариант списка методов для аутентификации через локальную базу пользователей
(config)# aaa authentication dot1x (<имя_списка>|default) local
! Вариант списка методов для аутентификации через RADIUS-сервер
(config)# aaa authentication dot1x (<имя_списка>|default) group radius
! Добавление адреса RADIUS-сервера для аутентификации
! Обычно RADIUS-сервер работает на порту 1812
! В ключе учитываются проблемы в середине и конце!
(config)# radius-server host <адрес> auth-port <порт_сервера> key <ключ>
! Вариант списка методов для отключения аутентификации
(config)# aaa authentication dot1x (<имя_списка>|default) none
! Активация использования 802.1X на коммутаторе
(config)# dot1x system-auth-control
! Настройка порта на использование 802.1X
! Перед выполнением команды убедитесь, что порт переведён в режим access!
(config)# interface <имя>
(config-if)# dot1x port-control auto
```

Включить принудительную периодическую аутентификацию:

```
! Переход в режим настройки порта
(config)# interface <имя>
! Включение периодической реаутентификации
(config-if)# dot1x reathentication
! Задание периода принудительной повторной аутентификации
! От 1 до 65535, по умолчанию 3600
(config-if)# dot1x timeout reauth-period <период_в_секундах>
```

Вручную инициировать принудительную аутентификацию на порту:

```
# dot1x re-authenticate interface <имя>
```

Настроить время до повтора попытки аутентификации на порту после неудачной попытки:

```
(config)# interface <имя>
! От 1 до 65535, по умолчанию 60
(config-if)# dot1x timeout quiet-period <период_в_секундах>
```

Установить максимальное количество попыток реаутентификации:

```
(config)# interface <имя>
! От 1 до 10, по умолчанию 2
(config-if)# dot1x max-reauth-req <количество>
```

Позволить нескольким клиентам проходить аутентификацию на одном порту независимо (по MAC-адресам):

```
(config)# interface <имя>
(config-if)# dot1x host-mode multi-host
! Отключение эту возможности
(config-if)# dot1x host-mode single-host
```

Сбросить настройки 802.1X интерфейса:

```
(config)# interface <имя>
(config-if)# dot1x default
```

Включить процедуру учёта (accounting) аутентификации на порту через RADIUS-сервер:

```
(config)# interface <имя>
(config-if)# aaa accounting dot1x default start-stop group radius
(config-if)# aaa accounting system default start-stop group radius
```

Просмотр состояния 802.1X

Показать сведения о версии используемого протокола:

```
#show dot1x
```

Показать все сведения о настройке 802.1X:

```
#show dot1x all
```

Показать статистику 802.1X для всех портов:

```
#show dot1x all statistics
```

Показать сведения о настройке и состоянии конкретного порта:

```
#show dot1x interface <имя>
```

Показать статистику 802.1X для конкретного порта:

```
#show dot1x interface <имя> statistics
```

17. ACL

В IOS ACL именуются по номерам. Номера ACL образуют диапазоны, имеющие строго определённое назначение. В таблице приведены только те диапазоны, которые поддерживаются коммутаторами Catalyst 2960 и 3560:

Диапазон	Назначение
1-99	Основной диапазон стандартных IP ACL
100-199	Основной диапазон расширенных IP ACL
1300-1999	Дополнительный диапазон стандартных IP ACL
2000-2699	Дополнительный диапазон расширенных IP ACL

Остальные диапазоны относятся к устаревшим и/или малоприменяемым протоколам, таким как IPX и DECnet.

Для Catalyst при указании маски в ACL применяется инвертированная маска (то есть вместо 255.255.255.0 требуется указывать 0.0.0.255). Если маска не указывается, то по умолчанию подставляется 0.0.0.0. Для ASA указывается неинвертированная маска.

Каждый ACL может содержать несколько записей (Access List Entry, ACE). Записи добавляются в список последовательно, одна за одной. Нет возможности удалить запись из списка без удаления самого списка. Если при добавлении ACE в ACL этот ACL не существовал, он будет создан. Последней записью автоматически включается ACE, запрещающая все пакеты.

Управление ACL

Стандартный ACL позволяет указывать только адрес отправителя и инвертированную маску в качестве параметра. Создать стандартный ACL:

```
! Добавление разрешающей ACE в ACL
(config)# access-list <номер_ACL> permit <источник> [<инвертированная_маска>]
! Создание запрещающей ACE в ACL
(config)# access-list <номер_ACL> deny <источник> [<инвертированная_маска>]
```

Поле «источник» может записываться в нескольких форматах:

- IP-адрес, записанный октетами;
- ключевое слово «any», означающее запись 0.0.0.0 255.255.255.255, то есть любой адрес;
- ключевое слово «host», после которого указан адрес узла. Такой формат автоматически устанавливает поле «маска» в 0.0.0.0.

Расширенный ACL позволяет указывать адреса отправителя и получателя, а также протокол. Список протоколов и их мнемоник представлен в таблице:

Протокол	Мнемоника
AH (IPSec)	ahp
EIGRP	eigrp
ESP (IPSec)	esp
GRE	gre

ICMP	icmp
IGMP	igmp
IP (любой протокол)	ip
OSPF	ospf
TCP	tcp
UDP	udp

Создать расширенный ACL:

```
(config)# access-list <номер_ACL> (deny|permit) <протокол> <источник>
<инвертированная_маска> <получатель> <инвертированная маска>
```

В расширенном ACL также можно указать и порт для протоколов TCP и UDP:

```
(config)# access-list <номер_ACL> (deny|permit) <протокол> <источник>
<инвертированная_маска> [<оператор_сравнения> <порт>] <получатель>
<инвертированная_маска> [<оператор_сравнения> <порт>]
```

Оператор сравнения может быть следующим:

Оператор	Мнемоника
Равно (=)	eq
Больше (>)	gt
Меньше (<)	lt
Не равно (≠)	neq
Отрезок	range

Отрезок требует указания двух номеров портов — начала отрезка и его конца.

Правила для записи полей «источник» и «получатель» такие же, как и для записи поля «источник» в стандартных ACL.

Пример стандартного ACL:

```
! Разрешить пакеты от узла 192.168.0.1
(config)# access-list 10 permit host 192.168.0.1
! Запретить пакеты от сети 192.168.0.0/24
(config)# access-list 10 deny 192.168.0.0 0.0.0.255
! Запретить пакеты от любых источников
! Такое правило добавляется в конец автоматически
(config)# access-list 10 deny any
```

Пример расширенного ACL:

```
! Разрешить пакеты от узла 192.168.0.1 узлу 192.168.1.1 по протоколу TCP
(config)# access-list 110 permit tcp host 192.168.0.1 host 192.168.1.1
! Разрешить пакеты от любого узла любову узлу
! по протоколу UDP с портов младше 1024 на порты старше 1024
! Порт 1024 в данной ACE не учтён!
(config)# access-list 110 permit udp any lt 1024 any gt 1024
```

```
! Запретить ICMP от любых источников в сеть 192.168.0.0/24
(config)# access-list 110 deny icmp any 192.168.0.0 0.0.0.255
```

Применение ACL

Применение ACL для контроля telnet-линий

```
! Переход в режим настройки telnet-линий
(config)# line vty 0 4
! Указание ACL для контроля входящего трафика
(config-line)# access-class <номер_ACL> in
! Указание ACL для контроля исходящего трафика
(config-line)# access-class <номер_ACL> out
```

Применение ACL для контроля портов

ACL могут применяться:

8) для контроля входящего трафика на портах 2 уровня;
9) для контроля исходящего и входящего трафика на портах 3 уровня;

ACL порта 2 уровня приоритетнее ACL VLAN и входящего ACL для порта 3 уровня.

```
! Переход в режим настройки интерфейса
(config)# interface <имя>
! Указание ACL
(config-if)# ip access-group <номер_ACL> (in|out)
```

Просмотр настройки ACL

Вывести список созданных ACL:

```
#show access-lists
```

Вывести список только IP ACL:

```
#show ip access-lists
```

Вывести информацию только о конкретной ACL:

```
#show access-lists <номер_ACL>
```

Вывести информацию только о конкретной IP ACL:

```
#show ip access-lists <номер_ACL>
```

18. DHCP

По умолчанию на коммутаторах DHCP-сервер включен, но не настроен. DHCP-сервер, встроенный в коммутатор, является полнофункциональным DHCP-сервером. Если он не сможет удовлетворить запрос, то может перенаправить этот запрос другим DHCP-серверам.

Управление DHCP-сервером

Включить DHCP-сервер:

```
(config)# service dhcp
```

Указать расположение базы привязок. База привязок — это файл, в котором хранятся сведения о связке между IP-адресом, MAC-адресом, временем аренды, интерфейсом и VLAN. Файл формируется коммутатором автоматически и может храниться на FTP-, TFTP-, RCP-сервере или на локальном флеш-диске.

```
(config)# ip dhcp database <url>
```

Примеры <url>:

- ftp://myserver/filename
- rcp://1.2.3.4/filename
- flash:/database

Если вы не хотите хранить эту базу, требуется отключить функцию журналирования конфликтов адресов:

```
(config)# no ip dhcp conflict logging
```

После указания подсети для пула адресов DHCP-сервер полагает, что все адреса из пула доступны для выдачи. Ограничить список адресов, доступных для аренды:

```
(config)# ip dhcp excluded-address (<адрес>|<начало_диапазона>)
[<конец_диапазона>]
```

Если указать и начало, и конец диапазона, то из адресов, доступных для аренды, будут изъяты все адреса, входящие в диапазон.

Настроить диапазон адресов для аренды:

```
! Создать новый диапазон
(config)# ip dhcp pool <имя>
! Задать список адресов
(dhcp-config)# network <адрес_сети> (<маска>|</длина_маски>)
! Установить опцию «Имя домена»
(dhcp-config)# domain-name <имя_домена>
! Указать список DNS-серверов
(dhcp-config)# dns-server <адрес1> [<адрес2> <адрес3> …]
! Указать маршрутизатор по умолчанию
(dhcp-config)# default-router <адрес1> [<адрес2> <адрес3> …]
! Указать время аренды адреса (по умолчанию 1 день)
(dhcp-config)# lease (<дней> [<часов> <минут>]|infinite)
```

Чтобы задать привязку конкретного IP-адреса к MAC-адресу клиента, нужно создать новый

диапазон для каждой такой привязки следующим образом:

```
! Создать новый диапазон
(config)# ip dhcp pool <имя>
! Указать выдаваемый адрес
(dhcp-config)# host <IP-адрес>
! Указать MAC-адрес клиента в формате 01aa.bbcc.ddee.ff,
! где aabbccddeeff – MAC-адрес клиента, а 01 – тип среды (Ethernet)
(dhcp-config)# client-identifier <MAC-адрес>
! Установить опцию «Имя домена»
(dhcp-config)# domain-name <имя_домена>
! Указать список DNS-серверов
(dhcp-config)# dns-server <адрес1> [<адрес2> <адрес3> …]
! Указать маршрутизатор по умолчанию
(dhcp-config)# default-router <адрес1> [<адрес2> <адрес3> …]
! Указать время аренды адреса (по умолчанию 1 день)
(dhcp-config)# lease (<дней> [<часов> <минут>]|infinite)
```

Сброс списка выданных адресов:

```
! Сбросить весь список
# clear ip dhcp binding
! Сбросить информацию о конкретном адресе
# clear ip dhcp binding <IP-адрес>
```

Просмотр состояния DHCP-сервера

Показать все выданные адреса:

```
# show ip dhcp binding
```

Показать физический адрес узла, которому был выдан указанный IP-адрес:

```
# show ip dhcp binding <IP-адрес>
```

Показать список возникших конфликтов при назначении адресов:

```
# show ip dhcp conflict
```

Показать статистику:

```
# show ip dhcp server statistics
```

19. SNMP

Управление SNMP

Включить доступ к системной информации по протоколу SNMP (версии 1 или 2):

```
(config)# snmp-server community <имя_сообщества> (ro|rw)
```

Пример:

```
! Сообщество с именем com_public имеет возможность читать данные
(config)# snmp-server community com_public ro
! Сообщество с именем com_private имеет возможность читать данные
! и изменять настройки
(config)# snmp-server community com_private rw
```

Просмотр состояния SNMP

Вывести список созданных сообществ:

```
# show snmp community
```

20. Синхронизация системных часов с NTP-сервером

Управление NTP

Включить синхронизацию системных часов с NTP-сервером:

```
! Задание временной зоны относительно GMT
(config)# clock timezone MSK 3
! Задание NTP-сервера
(config)# ntp server <IP-адрес>
```

Просмотр состояния NTP

Показать текущее время:

```
# show clock
```

Показать настройки протокола NTP:

```
# show ntp status
# show ntp association
# show ntp association detail
```

21. QoS

Процедуры QoS для транзитного пакета разбиваются на несколько задач:

- классификация (classification) — исследовать пакет и выработать метку QoS на основе ACL;
- анализ на соответствие политике (policing) — сравнить скорость входящего потока с допустимой скоростью, установленной политикой, и решить, попадает пакет под действие политики или нет;
- отметка (mark) — на основе результата анализа на соответствие политике и настроек принять решение о пропускании пакета, его отметке или отбрасывании;
- создание входных очередей и диспетчеризация (ingress queueing and scheduling) — на основе метки QoS решить, в какую входящую (ingress) очередь поместить пакет, и обслужить очереди согласно установленным весам;
- создание выходных очередей и диспетчеризация (egress queueing and scheduling) — на основе метки QoS решить, в какую выходящую (egress) очередь поместить пакет, и обслужить очереди согласно установленным весам.

Для классификации используются стандартные и расширенные ACL. Если в ACL пакет совпадает с permit-ACE, то выполняется действие, связанное с этим ACL. Если пакет совпадает с deny-ACE, то анализ этого ACL прекращается и начинается анализ следующего ACL. Если среди всех заданных ACL не обнаружилось permit-ACE, то процедуры QoS для этого пакета не выполняются. При наличии нескольких ACL их просмотр прекращается после первой найденной permit-ACE. К ACL присоединяется политика, которая объединяет выделенные ACL пакеты в группу (например, устанавливает значение поля DSCP) или ограничивает скорость потока группы (rate-limit). После этого политика соединяется с портом и становится действующей.

Классификация также может выполняться на основе классовых карт (class map).

Анализ на соответствие политике подразумевает создание объекта-ограничителя (policer), который определяет доступную для класса полосу пропускания. Объект-ограничитель, анализируя пакет за пакетом, принимает решения, попадает пакет под политику или нет и какие действия необходимо с ним выполнить в случае превышения допустимой полосы — пропустить пакет без изменений, отбросить его или пропустить, изменив значение DSCP.

На физических портах можно создать следующие типы объектов-ограничителей:

10) индивидуальный — ограничения по полосе пропускания применяются к каждому классу отдельно;
11) суммарный — ограничения по полосе пропускания накладываются на суммарный поток классов.

На виртуальных интерфейсах возможно создание только индивидуальных объектов-ограничителей.

Для ограничения потоков используется алгоритм «дырявого ведра». Можно представить очередь как ведро с небольшим отверстием в основании. Вне зависимости от заполненности ведра через отверстие поток будет вытекать с фиксированной скоростью (в идеальных физических условиях). Если очередной пакет не помещается в «ведро» (то есть очередь переполнена), он считается не подходящим под политику и принимается решение о действии (пропускание, отбрасывание или замена поля). Настраивается как глубина «ведра», так и размер «отверстия».

Для очередей исходящих пакетов могут использоваться два режима разделения полосы —

урезание (shaping) или разделение (sharing). В режиме урезания каждый класс получает свою гарантированную полосу и не может превысить её. В режиме разделения каждый класс получает гарантированную полосу, однако если другие классы не используют выделенную им полосу целиком, то некоторые классы могут временно использовать часть полосы, выделенной другим классам. Для входящих очередей применяется только режим разделения.

Отбрасывание пакетов при заполнении очереди происходит по алгоритму WTD (Weighted Tail Drop, взвешенное отбрасывание хвоста). В соответствии с этим алгоритмом очередь имеет 3 порога, с которыми ассоциированы характеристики класса (DSCP или CoS). После достижения очередного порога начинают отбрасываться пакеты, принадлежащие ассоциированным с достигнутым порогом классам. Таким образом более приоритетные пакеты отбрасываются позже менее приоритетных.

По умолчанию процедуры QoS отключены. После разрешения использовать QoS по умолчанию трафик обслуживается без применения ограничителей (поля DSCP и CoS устанавливаются в 0), то есть изменений не происходит. По умолчанию имеются две входящие очереди следующих характеристик:

Параметр	Очередь 1	Очередь 2
Размер буфера	90%	10%
Выделенная полоса пропускания	4	4
Приоритетная полоса пропускания	0	10
Первый порог отбрасывания алгоритма WTD	100%	100%
Второй порог отбрасывания алгоритма WTD	100%	100%

Таким образом, очередь 2 — приоритетная, то есть пакеты из неё будут обслужены как можно скорее. Связь порогов алгоритма WTD с классами следующая (из таблицы не вытекает связь значений CoS и DSCP):

CoS	DSCP	Очередь — порог WTD
0-4	0-39	1-1
5	40-47	2-1
6,7	48-63	1-1

По умолчанию имеются четыре выходные очереди со следующими характеристиками:

Параметр	Очередь 1	Очередь 2	Очередь 3	Очередь 4
Размер буфера	25%	25%	25%	25%
Первый порог отбрасывания алгоритма WTD	100%	200%	100%	100%
Второй порог отбрасывания алгоритма WTD	100%	200%	100%	100%
Резервный размер буфера	50%	50%	50%	50%
Максимальный размер буфера	400%	400%	400%	400%
Веса для урезания	25	0	0	0
Веса для разделения	25	25	25	25

Таким образом, очереди разделяют общий буфер, по умолчанию занимают по четверти его длины, но могут увеличиваться до 4 раз. Все порты по умолчанию включены в очередь 1. Связь порогов алгоритма WTD с классами следующая (из таблицы не вытекает связь значений CoS и DSCP):

CoS	DSCP	Очередь — порог WTD
0,1	0-15	2-1
2,3	16-31	3-1
4	32-39	4-1
5	40-47	1-1
6,7	48-63	4-1

Настройка QoS

Включить процедуры QoS на устройстве:

```
(config)# mls qos
```

Разрешить использование QoS для VLAN (по умолчанию запрещено для всех интерфейсов):

```
(config)# interface <имя>
(config-if)# mls qos vlan-based
```

Настроить состояние доверия (trust state) портов (по умолчанию все порты являются недоверенными):

```
(config)# interface <имя>
(config-if)# mls qos trust [cos | dscp | ip-precedence]
```

Если параметр доверия не указан, по умолчанию выбирается dscp. Параметр определяет, в соответствии с каким полем будет происходить классификация входящего пакета. Для нетегированного пакета используется значение CoS по умолчанию (по умолчанию установлено в 0).

Настроить CoS по умолчанию:

```
(config)# interface <имя>
(config)# mls qos cos (<cos_по_умолчанию> | override)
```

Установленный ключ override сбрасывает предыдущее состояние доверия пакета и перезаписывает (или устанавливает, если пакет нетегирован) значение CoS установленным значением по умолчанию. По умолчанию такое поведение отключено.

Отключить изменение поля DSCP пакета (функция «прозрачный режим DSCP»):

```
(config)# mls qos
(config)# no mls qos rewrite ip dscp
```

По умолчанию прозрачный режим DSCP отключен (то есть поле DSCP может изменяться).

Создать классовую карту:

```
(config)# class-map [match-all | match-any] <имя_классовой_карты>
(config-cmap)# match (access-group <номер_ACL> | ip dscp <список_значений> | ip precedence <список_значений>)
```

Ключ match-all задаёт логическую операцию И для всех правил классовой карты (включен по умолчанию). Ключ match-any задаёт логическую операцию ИЛИ для всех правил классовой карты. Команда match создаёт очередное правило классовой карты. Команд match для каждой

классовой карты может быть несколько. В списках значений разделителем является пробел.

Пример классовой карты, построенной на основе списка доступа:

```
! Расширенный список доступа, выделяющий пакеты со значением DSCP=10
(config)# access-list 103 permit ip any any dscp 10
(config)# class-map class1
(config-cmap)# match access-group 103
(config-cmap)# end
```

Примеры классовых карт, не использующей списки доступа:

```
! Классовая карта, выделяющая пакеты со значением DSCP 10, 11 или 12
(config)# class-map class2
(config-cmap)# match ip dscp 10 11 12
(config-cmap)# exit
! Классовая карта, выделяющая пакеты со значением IP Precedence 5, 6 или 7
(config)# class-map class3
(config-cmap)# match ip precedence 5 6 7
(config-cmap)# exit
```

Для классификации, применения политик и отметки пакетов применяются карты политик (policy map, PMAP). К входящему направлению порта может быть применена только одна PMAP. PMAP и состояние доверия могут работать одновременно, в этом случае сначала применяется PMAP. Неклассифицированный трафик, проходя через PMAP, рассматривается как классифицированный по умолчанию (настраивается в PMAP). В одном PMAP может настраиваться несколько классов.

Создать и настроить policy map:

```
! Создание PMAP
(config)# policy-map <имя_PMAP>
! Указание класса трафика и переход в режим настройки этого класса
! Если после class ничего не указано, считается, что настраивается класс по
умолчанию
(config-pmap)# class [<имя_классовой_карты> | class-default]
! Выбор «режима доверия» - параметра, по которому генерируется метка QoS
! По умолчанию порт находится в недоверительном режиме
! Если после trust ничего не указано, выбирается dscp
(config-pmap-c)# trust [cos | dscp | ip-precedence]
! Классификация трафика путём установки нового значения dscp или ip precedence
! Несовместима с trust
(config-pmap-c)# set (dscp <новое_dscp> | ip precedence <новое_ip_precedence>)
! Определение объекта-ограничителя
(config-pmap-c)# police <скорость_в_битах/с> <допустимое_превышение_в_битах/с>
[exceed-action (drop | policed-dscp-transmit)]
! Скорость варьируется в пределах от 8000 до 10000000000 (10 Гбит/с)
```

```
! Допустимое превышение варьируется от 8000 до 1000000 (1 Мбит/с)
! exceed-action задаёт действие при превышении полосы
! exceed-action drop – отбросить пакет
! exceed-action policed-dscp-transmit – снизить значение dscp
!
! Выход в режим настройки PMAP
(config-pmap-c)# exit
! Выход в режим глобальной настройки
(config-pmap)# exit
! Переход в режим настройки интерфейса
(config)# interface <имя>
! Связывание PMAP со входной очередью интерфейса
(config-if)# service-policy input <имя_PMAP>
```

Пример PMAP, ограничивающей скорость передачи трафика в сеть 10.1.0.0/16 до 1 Мбит/с + 1 Кбит/с:

```
(config)# access-list 1 permit 10.1.0.0 0.0.255.255
(config)# class-map ipclass1
(config-cmap)# match access-group 1
(config-cmap)# exit
(config)# policy-map flow1t
(config-pmap)# class ipclass1
(config-pmap-c)# trust dscp
(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
(config-pmap-c)# exit
(config-pmap)# exit
(config)# interface gigabitethernet0/1
(config-if)# service-policy input flow1t
```

Настройка агрегированных политик:

```
! Создание агрегированной политики
(config)# mls qos aggregate-policer <имя_политики> <скорость_в_битах/с>
<допустимое_превышение_в_битах/с> exceed-action (drop | policed-dscp-transmit)
! Дальше идёт обычный процесс настройки ограничительной PMAP:
!  создание и заполнение классовой карты
(config)# class-map [match-all | match-any] <имя_классовой_карты>
(config-cmap)# match ...
!  создание PMAP
(config)# policy-map <имя_PMAP>
(config-pmap)# class [<имя_классовой_карты> | class-default]
```

```
! Задание использования агрегированной политики

(config-pmap-c)# police aggregate <имя_агрегированной политики>

! Выход в режим настройки PMAP

(config-pmap-c)# exit

! Выход в режим глобальной настройки

(config-pmap)# exit

! Переход в режим настройки интерфейса

(config)# interface <имя>

! Связывание PMAP со входной очередью интерфейса

(config-if)# service-policy input <имя_PMAP>
```

Распределить классы по входящим очередям и определить пороги WTD:

```
! Не забывайте, что входящих очередей только 2 и порогов тоже 2

! Распределение классов по критерию DSCP

(config)# mls qos srr-queue input dscp-map queue <номер_очереди> threshold
<номер_порога> <значение_dscp№1> ... <значение_dscp№8>

! Распределение классов по критерию CoS

(config)# mls qos srr-queue input cos-map queue <номер_очереди> threshold
<номер_порога> <значение_cos№1> ... <значение_cos№8>

! Задание порогов WTD для очереди

(config)# mls qos srr-queue input threshold <номер_очереди> <порог1> <порог2>
```

Пример распределения классов:

```
! Классы со значением DSCP 0-6 попадают в очередь 1 на порог 1

(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6

! Классы со значением DSCP 20-26 попадают в очередь 1 на порог 2

(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25
26

! Порог 1 – 50%, порог 2 - 70%

(config)# mls qos srr-queue input threshold 1 50 70
```

Распределить буфер между входящими очередями:

```
(config)# mls qos srr-queue input buffers <буфер1_в_процентах>
<буфер2_в_процентах>
```

Распределить полосу пропускания между входящими очередями:

```
! Полоса задаётся взвешенным значением, то есть в долях в пределах от 1 до 100

(config)# mls qos srr-queue input bandwidth <полоса_очереди1> <полоса_очереди2>
```

Задать полосу пропускания для приоритетной очереди и назначить одну из очередей в качестве приоритетной:

```
(config)# mls qos srr-queue input priority-queue <номер_очереди> bandwidth
<полоса_в_долях>
```

Настройки исходящих буферов считаются компанией Cisco оптимальными и не рекомендуются к изменению. Однако если требуется, их можно изменить.

Распределить буфер между исходящими очередями и задать пороги WTD:

```
! Существует два набора по 4 очереди

! Каждый интерфейс входит в один из этих наборов

! и наследует настройки очередей этого набора

! Размеры буферов для очередей 1, 3 и 4 изменяются от 0 до 99

! Размер буфера для очереди 2 изменяется от 1 до 100

(config)# mls qos queue-set output <номер_набора> buffers <размер_буфера1_в_долях>
... <размер_буфера2_в_долях>

! Пороги изменяются в пределах от 1% до 3200%

! Резервное превышение изменяется в пределах от 1% до 100%

! Максимальное превышение изменяется в пределах от 1% до 3200%

(config)# mls qos queue-set output <номер_набора> threshold <номер_очереди>
<порог1_в_процентах> <порог1_в_процентах> <резервное_превышение>
<максимальное_превышение>

! Переход в режим настройки интерфейса

(config)# interface <имя>

! Привязка интерфейса к набору очередей

(config)# queue-set <номер_набора>
```

Распределить классы по выходными очередям:

```
! Распределение классов по критерию DSCP

(config)# mls qos srr-queue output dscp-map queue <номер_очереди> threshold
<номер_порога> <значение_dscp№1> ... <значение_dscp№8>

! Распределение классов по критерию CoS

(config)# mls qos srr-queue output cos-map queue <номер_очереди> threshold
<номер_порога> <значение_cos№1> ... <значение_cos№8>
```

Определить правила урезания (shaping) полосы пропускания на интерфейсе:

```
(config)# interface <имя>

! Настройка весов очередей в режиме ограничения полосы

! Единица делится на введённое значение веса

! Полученное число является назначенной долей полосы пропускания

! Вес изменяется в пределах от 0 до 65535

! Вес, равный 0, означает, что очередь находится

! в режиме разделения полосы (sharing)

(config-if)# srr-queue bandwidth shape <вес_очереди1> <вес_очереди2>
<вес_очереди3> <вес_очереди4>
```

Настроить доли полосы для очередей в режиме разделения полосы:

```
(config)# interface <имя>

! Настройка весов очередей в режиме разделения полосы

! Вес изменяется в пределах от 1 до 255

(config-if)# srr-queue bandwidth share <вес_очереди1> <вес_очереди2>
<вес_очереди3> <вес_очереди4>
```

Ограничить полосу для выходной очереди:

```
(config)# interface <имя>
! Задание процента скорости порта, до которого требуется ограничить скорость
! Вес варьируется в пределах от 10% до 90%
(config-if)# srr-queue bandwidth limit <вес>
```

Просмотр информации о QoS

Показать настроенные классовые карты:

```
# show class-map
```

Показать глобальную конфигурацию QoS:

```
# show mls qos
```

Показать настроенные агрегированные политики:

```
# show mls qos aggregate-policer
```

Показать настройки входных очередей:

```
# show mls qos input-queue
```

Показать настройки QoS для порта:

```
# show mls qos interface [<имя>]
```

Показать настройки выходных очередей:

```
# show mls qos queue-set [<номер_набора>]
```

Показать настроенные PMAP:

```
# show policy-map
```

4. Управление беспроводными функциями

1. Введение

По умолчанию устройство не имеет SSID. Перед включением беспроводного интерфейса требуется задать SSID. По умолчанию беспроводной интерфейс выключен.

Включить беспроводной интерфейс:

```
! 0 – интерфейс 2.4 ГГц (b/g)
! 1 – интерфейс 5 ГГц (a)
(config)# interface dot11radio (0 | 1)
! SSID не длиннее 32 символов, регистрозависимый
(config-if)# ssid <ssid>
! Включение интерфейса
(config-if)# no shutdown
```

Выбрать режим работы:

```
(config)# interface dot11radio (0 | 1)
! Точка доступа
(config-if)# station-role root
! Повторитель
! Порты Ethernet будут автоматически отключены
(config-if)# station-role root repeater
! Беспроводной клиент
(config-if)# station-role non-root
```

Выбрать канал:

```
! least-congested выбирает наименее загруженный канал при загрузке
(config-if)# channel <частота> | least-congested
```

Список каналов 802.11:

Канал 802.11b/g	Частота 802.11b/g	Канал 802.11a	Частота 802.11a
1	2412	34	5170
2	2417	36	5180
3	2422	38	5190
4	2427	40	5200
5	2432	42	5210
6	2437	44	5220
7	2442	46	5230
8	2447	48	5240
9	2452	52	5260
10	2457	56	5280

11	2462	60	5300
12	2467	64	5320
13	2472	100	5500
14	2484	104	5520
		108	5540
		112	5560
		116	5580
		120	5600
		124	5620
		128	5640
		132	5660
		136	5680
		140	5700
		149	5745
		153	5762
		157	5785
		161	5805
		165	5825

Настроить шифрование WEP:

```
(config)# interface dot11radio (0 | 1)
! 1-4 – индекс ключа
! 40-битный ключ записывается 10 шестнадцатиричными символами
! 128-битный ключ записывается 26 шестнадцатиричными смиволами
! 0|7 – выбор режима хранения ключа:
!  0 – в незашифрованном виде
!  7 – в зашифрованном виде
(config-if)# encryption key 1-4 size (40 | 128) <ключ> [0 | 7]
```

Выбрать набор шифросредств:

```
(config)# interface dot11radio (0 | 1)
! Выбрать одновременно TKIP и CCMP или WEP40 и WEP128 нельзя
(config-if)# encryption mode ciphers ([aes-ccm | tkip]) ([wep128 | wep40])
```

Совместимые с WPA шифросредства:

```
encryption mode ciphers aes-ccm
encryption mode ciphers aes-ccm wep128
encryption mode ciphers aes-ccm wep40
encryption mode ciphers aes-ccm tkip
encryption mode ciphers aes-ccm tkip wep128
```

```
encryption mode ciphers aes-ccm tkip wep128 wep40
encryption mode ciphers tkip wep128 wep40
```

Выбор режима аутентификации:

```
! Переход в режим настройки SSID
(config)# dot11 ssid <ssid>
! Открытая аутентификация
(config-ssid)# authentication open
! Аутентификация общим ключом
(config-ssid)# authentication shared
! Аутентификация WPA
! Чтобы включить шифрование WPA, требуется разрешить открытую аутентификацию
(config-ssid)# authentication key-management wpa
```

Настроить шифрование WPA-PSK:

```
(config)# interface dot11radio (0 | 1)
(config-if)# ssid <ssid>
! Задать ключ WPA-PSK
! 0|7 – выбор режима хранения ключа:
!  0 – в незашифрованном виде
!  7 – в зашифрованном виде
! Ключ в режиме hex записывается строго 64 шестнадцатиричными символами
! Ключ в режиме ascii записывается алфавитно-цифровыми символами
! и знаками препинания в строку длиной от 8 до 63 символов
(config-ssid)# wpa-psk (hex | ascii) [0 | 7] <ключ>
```

2. Cisco WAP4410N

Cisco WAP4410N — беспроводная точка доступа, поддерживающая стандарты IEEE 802.11b/g/n. Поддерживает технологию MIMO (Multiple-in-Multiple-out), как того требует стандарт 802.11n, и потому оснащена 3 всенаправленными антеннами с коэффициентом усиления 2 дБ. Имеет возможность получать электропитание от порта Ethernet (технология Power over Ethernet).

Внешний вид

На лицевой панели находятся 4 светодиода. Пояснение режимов их работы приведено ниже

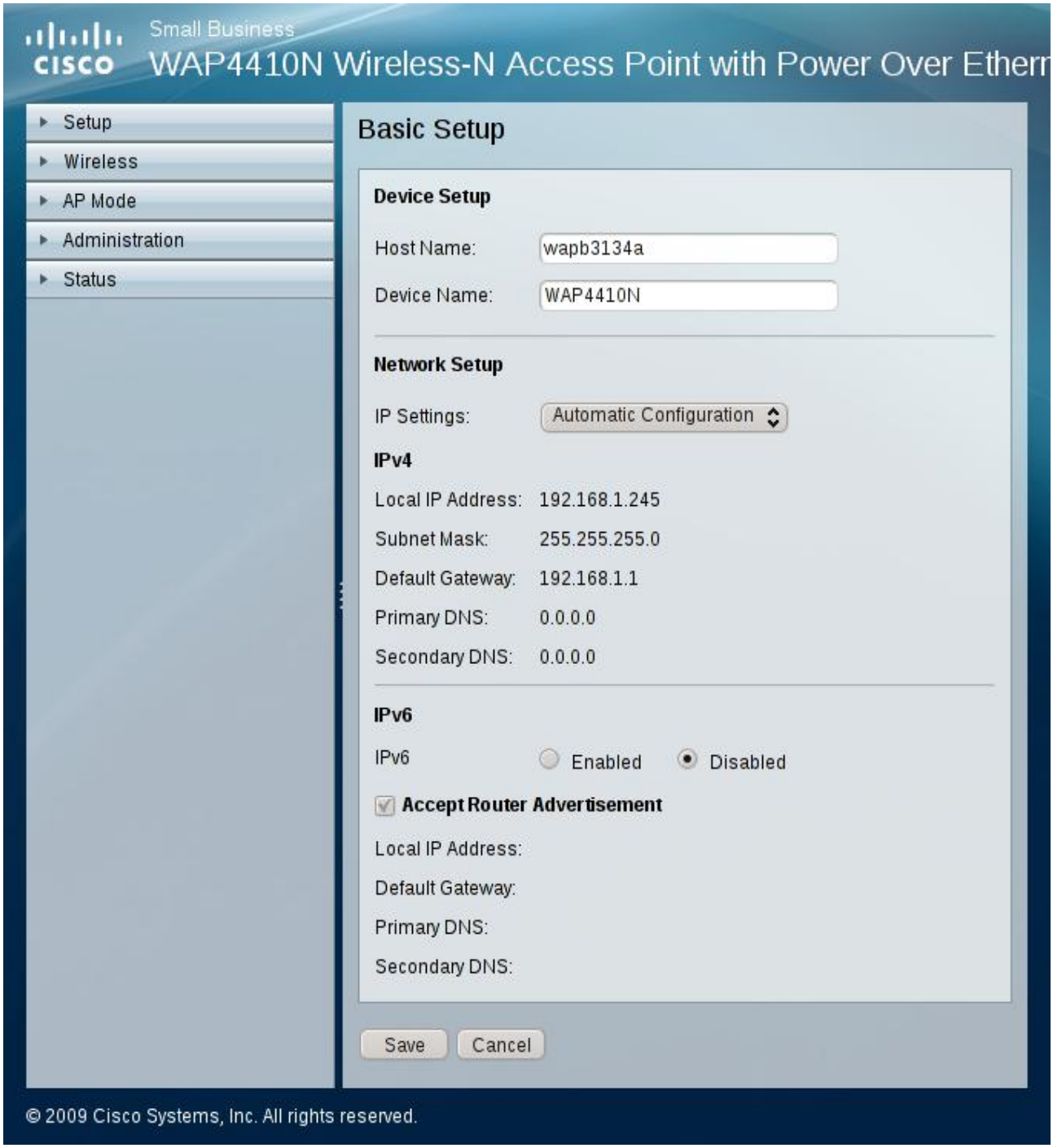
Светодиод	Режим работы	Пояснение
Power	Горит зелёным	Устройство включено
PoE	Горит зелёным	На устройство подано питание через порт Ethernet (PoE)
Wireless	Горит зелёным	Беспроводной модуль активен
	Моргает зелёным	Идёт обмен данными по беспроводной сети
Ethernet	Горит зелёным	Проводная сеть подключена
	Моргает зелёным	Идёт обмен данными по проводной сети

На задней панели находятся 3 гнезда для антенн, порт Ethernet, гнездо для подключения адаптера питания и кнопка Reset. Если нажать кнопку Reset на 10 секунд, то устройство вернётся к заводским настройкам.

Управление

Устройство управляется через веб-интерфейс. Соедините устройство с компьютером через порт Ethernet для первоначальной настройки. IP-адрес порта Ethernet по умолчанию — 192.168.1.245. Обратитесь к этому адресу через браузер. Вы увидите экран, на котором вам будет предложено ввести аутентификационные данные:

Логин и пароль по умолчанию - «admin». После успешной аутентификации вы увидите следующий экран:



На этом экране вы можете выполнить следующие настройки:

- Host Name — имя узла. Это имя используется при регистрации на DHCP-сервере.
- Device Name — имя устройства. Это имя используется, чтобы администратору было проще различать одинаковые точки доступа.
- IP Settings — выбор способа настройки параметров протокола IP:
  - Automatic Configuration — получение настроек от DHCP-сервера.
  - Static IP Address — настройка вручную.
- IPv6 — ключ, определяющий, будет ли устройство использовать протокол IPv6.

Если вы выбрали значение «Static IP Address» в поле «IP Settings», то станут доступны для изменения следующие настройки:

12) Local IP Address — IPv4-адрес устройства. Так как устройство является точкой доступа, этот адрес принадлежит одновременно и проводному, и беспроводному интерфейсам.
13) Subnet Mask — маска подсети.
14) Default Gateway — шлюз по умолчанию.
15) Primary DNS Server — первичный сервер DNS.
16) Secondary DNS Server — вторичный сервер DNS.

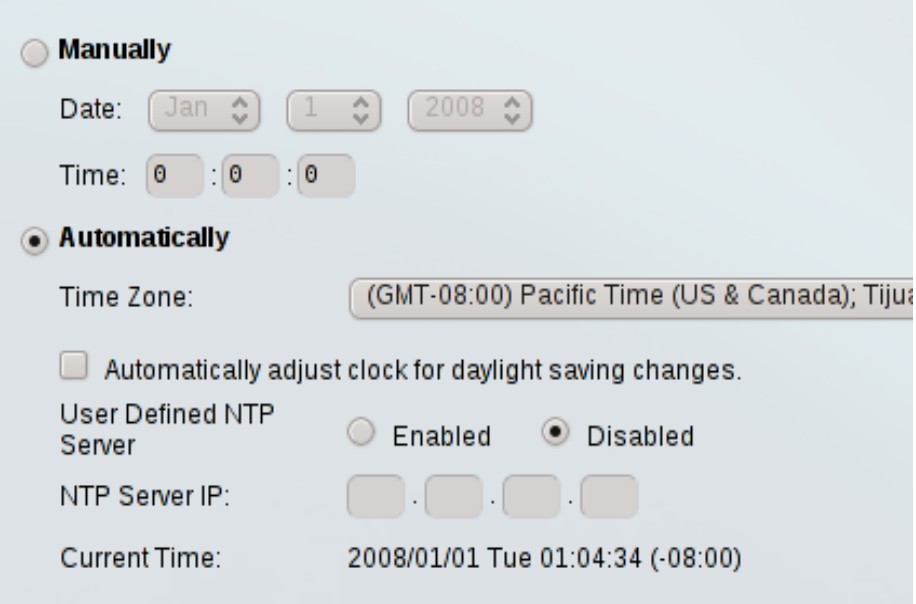
После того, как вы выполнили все настройки, нажмите кнопку Save.

Слева находятся закладки, определяющие раздел настроек. Эти закладки организованы следующим образом:

5. Setup — основные настройки
    1. Basic Setup — базовые настройки
    2. Time — настройки времени
    3. Advanced — расширенные основные настройки
6. Wireless — настройка беспроводных функций
    1. Basic Settings — базовые настройки
    2. Security — настройки безопасности
    3. Connection Control — настройки контроля соединения
    4. Wi-Fi Protected Setup — настройки функции WPS
    5. VLAN and QoS — настройки VLAN и QoS
    6. Advanced Settings — расширенные беспроводные настройки
7. AP Mode — выбор режима работы устройства
8. Administration — администрирование устройства
    1. Management — управление функциями администрирования
    2. Log — настройки журналирования
    3. Diagnostics — функции диагностики сети
    4. Factory Default — сброс до заводских настроек
    5. Firmware Upgrade — обновление микропрограммы
    6. Reboot — перезагрузка
    7. Configuration Management — управление сделанной настройкой
9. Status — состояние устройства
    1. Local Network — состояние сетевых интерфейсов
    2. Wireless — состояние беспроводных функций
    3. System Performance — статистика

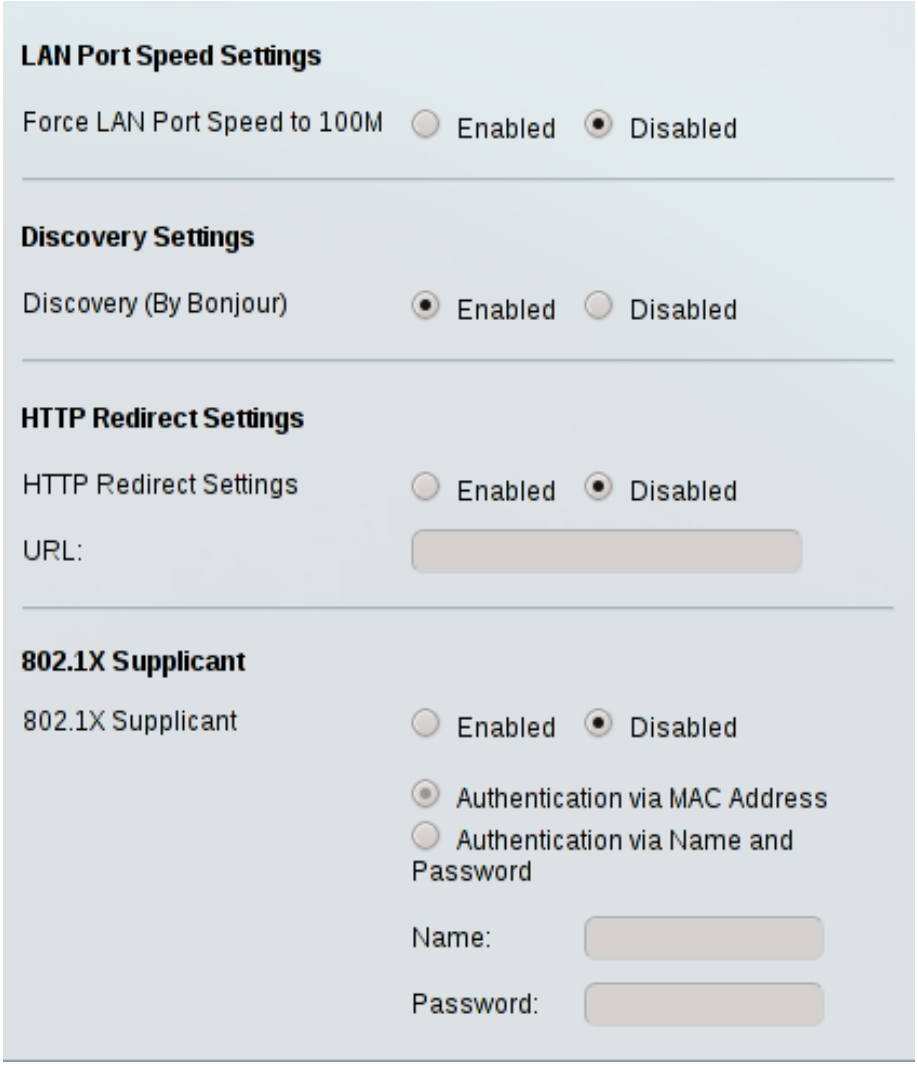
Экран «Setup/Basic Setup» был рассмотрен выше. Ниже рассматриваются следующие экраны.

Setup/Time



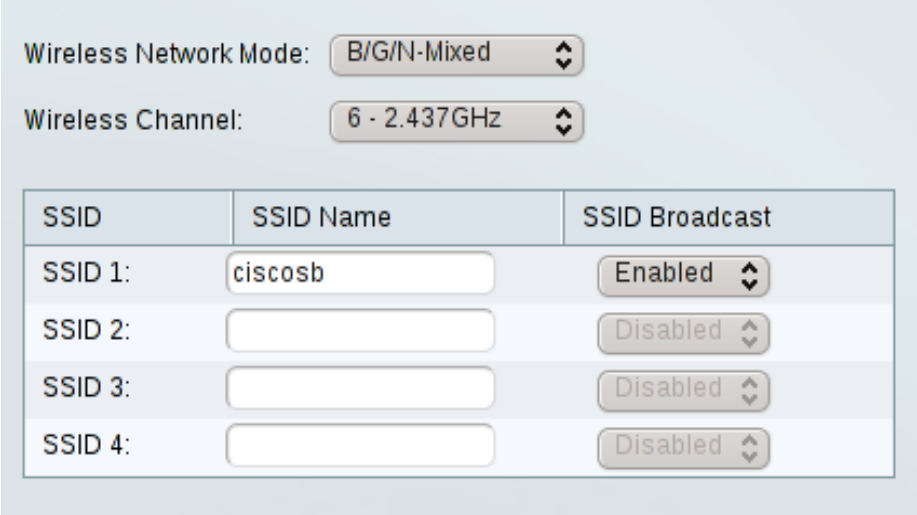
- Manually — ручное задание даты и времени
  - Date — дата
  - Time — время
- Automatically — получение даты и времени по протоколу NTP
  - Time Zone — часовой пояс
  - Automaticaly adjust... - автоматический переход на летнее время
  - User Defined NTP Server — ключ, определяющий возможность указать свой NTP-сервер. Иначе используется сервер, адрес которого записан в микропрограмме
  - NTP Server IP — адрес NTP-сервера
- Current Time — текущие время и дата

Setup/Advanced



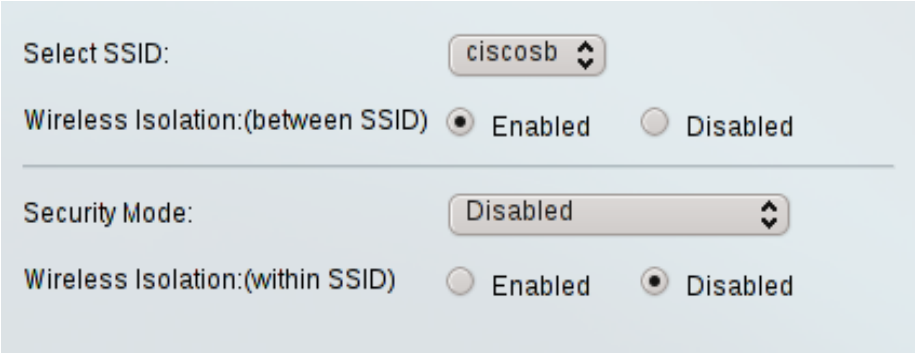
- Force LAN Port Speed to 100M — ключ, определяющий, будет ли устройство фиксировать скорость Ethernet-порта на 100 Мбит/с или выбирать скорость процедурой согласования
- Discovery (by Bonjour) — ключ, определяющий анонсирование устройства в сети по протоколу Apple Bonjour/Avahi
- HTTP Redirect Settings — ключ, определяющий необходимость перенаправления HTTP-запросов к устройству на некоторый адрес
  - URL — адрес, на который будут перенаправлены HTTP-запросы
- 802.1X Supplicant — ключ, определяющий необходимость использования протокола 802.1X для получения доступа к проводной сети
  - Authentication via MAC Address — аутентификация MAC-адресом
  - Authentication via Name and Password — аутентификация учётной парой
    - Name — логин
    - Password — пароль

Wireless/Basic Settings

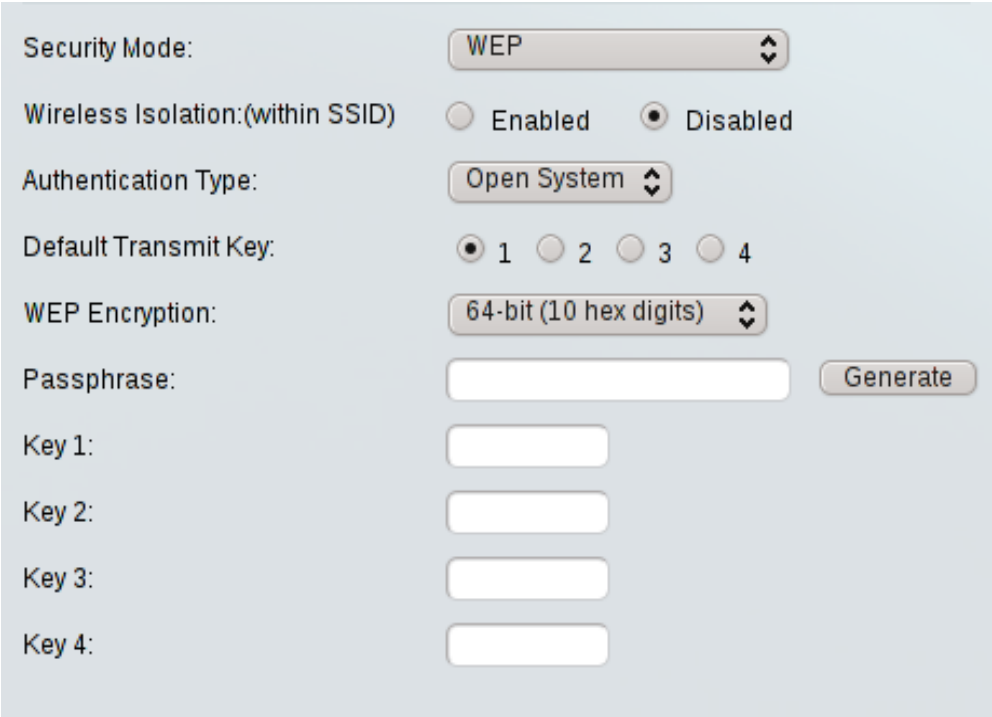


- Wireless Network Mode — станадарт(ы), который(е) использует передатчик
  - B-Only — только IEEE 802.11b
  - G-Only — только IEEE 802.11g
  - N-Only — только IEEE 802.11n
  - B/G-Mixed — IEEE 802.11b/g
  - B/G/N-Mixed — IEEE 802.11b/g/n
- Wireless Channel — канал, на котором осуществляется работа беспроводного модуля
- SSID Name (1-4) — устройство поддерживает настройку до 4 беспроводных сетей.
  - SSID Broadcast — для каждого SSID можно настроить, будет ли этот SSID передаваться в эфир

Wireless/Security

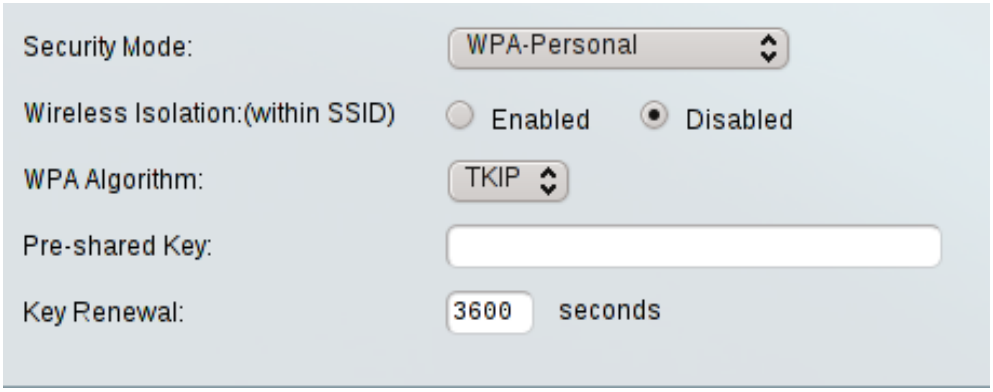


- Select SSID — SSID, для которой будут настраиваться режимы обеспечения безопасности (если у вас настроено несколько SSID)
- Wireless Isolation (between SSID) — ключ, определяющий, могут ли клиенты разных SSID взаимодействовать между собой
- Wireless Isolation (within SSID) — ключ, определяющий, могут ли клиенты одной SSID взаимодействовать между собой (полезно запретить взаимодействие клиентов публичной точки доступа)
- Security Mode — режим обеспечения безопасности:
  - Disabled — функции безопасности трафика отключены
  - WEP — включено шифрование механизмом WEP



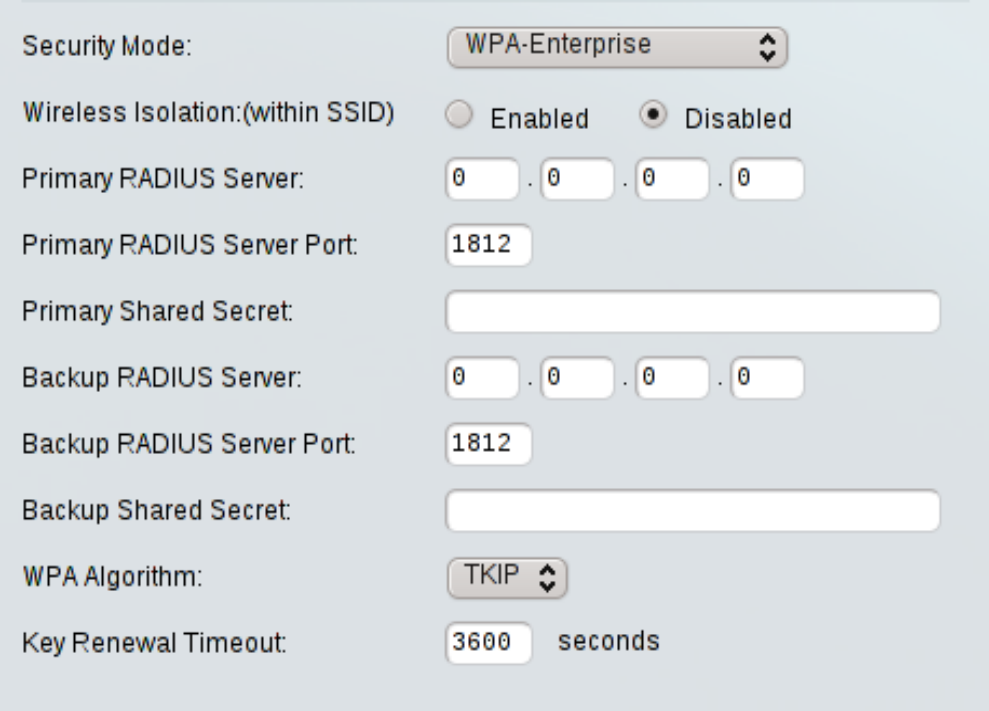
- Authentication Type — режим аутентификации при ассоциации
  - Open System — ассоциация разрешена всем, кто знает SSID
  - Shared Key — ассоциация разрешена тем, кто корректно осуществит взаимодействие с использованием WEP, передав обратно контрольную строку, отправленную устройством
- Default Transmit Key — ключ, используемый для шифрования исходящего трафика
- WEP Encryption — длина ключа WEP (64 бита, записывается 10 шестнадцаритичными символами, или 128 бит, записывается 26 шестнадцатиричными символами)
- Key1-Key4 — ключи шифрования
- Passphrase и кнопка Generate — генерация ключей WEP из парольной фразы

- WPA-Personal — включено шифрование механизмом WPA-PSK



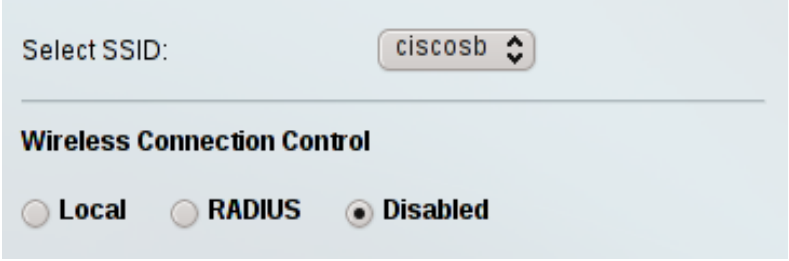
- WPA Algorithm — алгоритм, используемый для шифрования (TKIP/RC4 или CCMP/AES)
- Pre-shared Key — ключ WPA-PSK
- Key Renewal — период обновления ключей

- WPA2-Personal — включено шифрование механизмом WPA2-PSK (настройки не отличаются от настроек WPA-PSK, используется только алгоритм шифрования CCMP/AES)
- WPA2-Personal Mixed — включено шифрование механизмом WPA2-PSK (настройки не отличаются от настроек WPA-PSK, используются оба алгоритма шифрования — и TKIP, и CCMP/AES, по выбору беспроводного клиента)
- WPA-Enterprise — включено шифрование механизмом WPA с использованием RADIUS-серверов

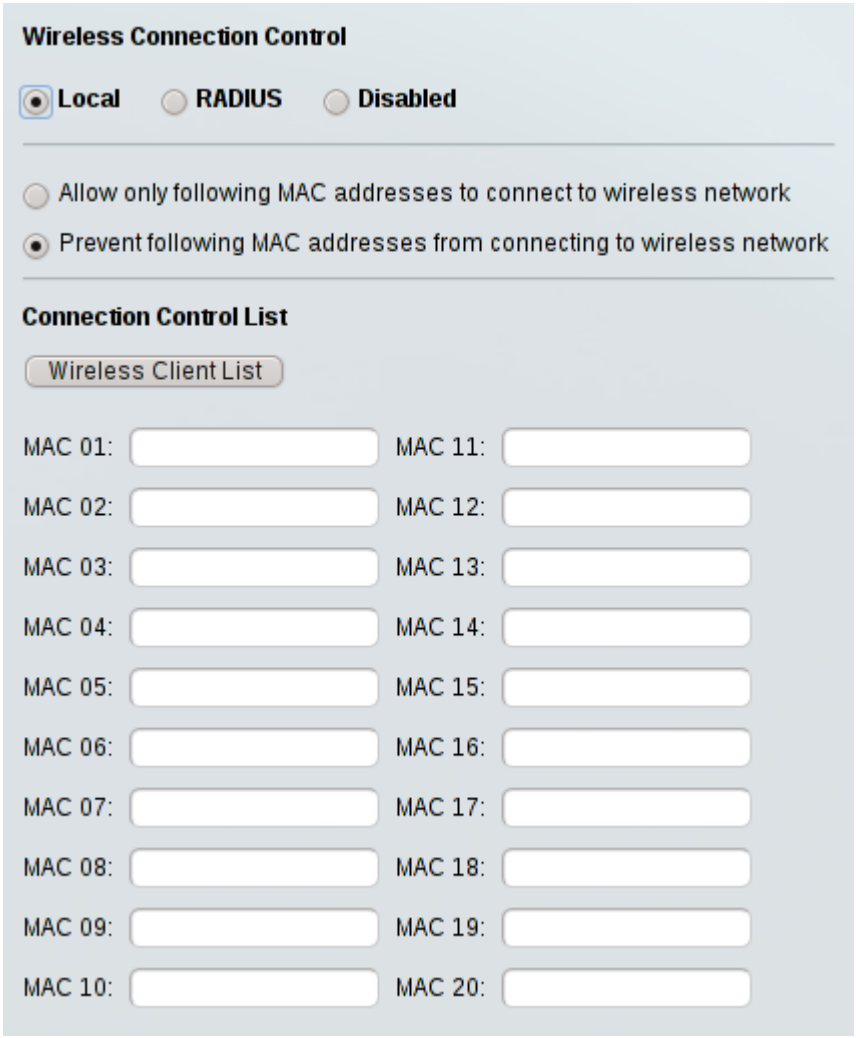


  - Primary RADIUS Server — адрес основного RADIUS-сервера
  - Primary RADIUS Server Port — порт, на котором работает основной RADIUS-сервер
  - Primary Shared Secret — ключ для связи с основным RADIUS-сервером
  - Backup RADIUS Server — адрес запасного RADIUS-сервера
  - Backup RADIUS Server Port — порт, на котором работает запасной RADIUS-сервер
  - Backup Shared Secret — ключ для связи с запасным RADIUS-сервером
  - WPA Algorithm — алгоритм, используемый для шифрования (TKIP/RC4 или CCMP/AES)
  - Key Renewal — период обновления ключей
- WPA2-Enterprise — включено шифрование механизмом WPA2 с использованием RADIUS-серверов (настройки не отличаются от настроек WPA-PSK, используется только алгоритм шифрования CCMP/AES)
- WPA2-Personal Mixed — включено шифрование механизмом WPA2 с использованием RADIUS-серверов (настройки не отличаются от настроек WPA-PSK, используются оба алгоритма шифрования — и TKIP, и CCMP/AES, по выбору беспроводного клиента)
- RADIUS — аутентификация через RADIUS-сервер, шифрование не используется

Wireless/Connection Control



- Select SSID — SSID, для которой будут настраиваться режимы контроля доступа (если у вас настроено несколько SSID)
- Wireless Connection Control — режим контроля доступа:
  - Disabled — контроль доступа отключен
  - Local — контроль MAC-адреса

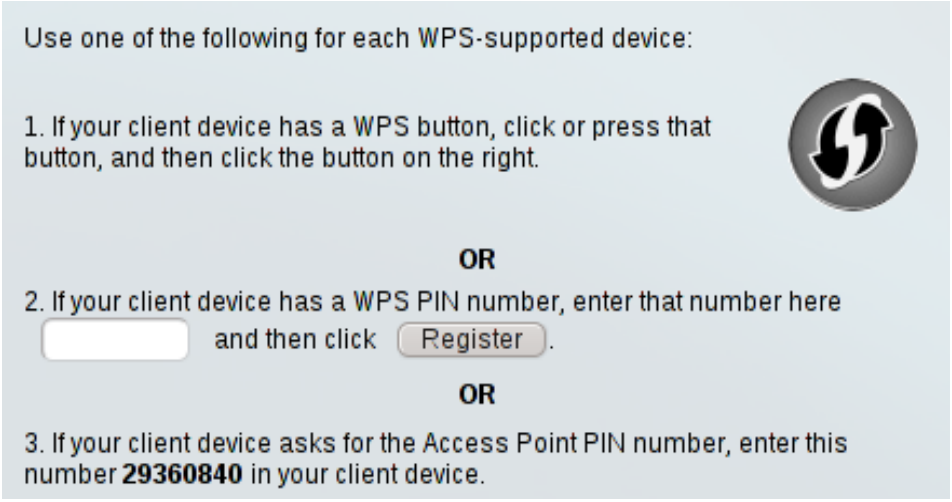


  - Allow only following MAC... — разрешить подключение только клиентиам с указанными MAC-адресами
  - Prevent following MAC... — запретить подключение только клиентиам с указанными MAC-адресами
  - Кнопка Wireless Client List — позволяет вывести список подключенных клиентов, чтобы выбрать интересующий MAC-адрес оттуда, а не вводить его руками

- RADIUS — аутентификация клиентов через RADIUS-сервер. Настройки аналогичны настройке RADIUS-сервера в Wireless/Security, в режиме WPA-Enterprise

Wi-Fi Protected Setup

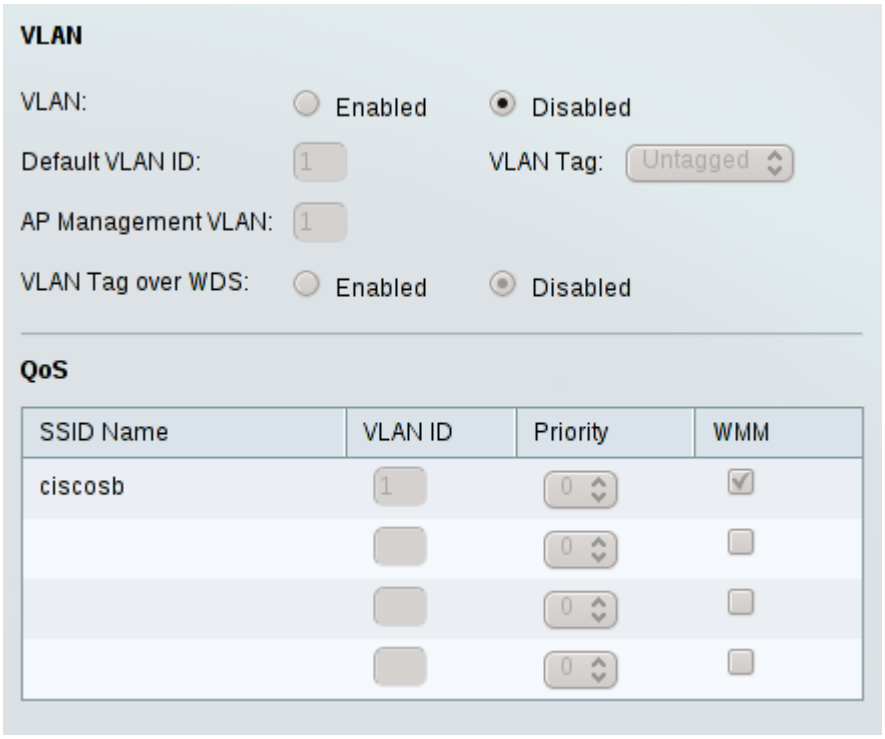
Wi-Fi Protected Setup (WPS) — техника, позволяющая соединить беспроводного клиента с точкой доступа, не настраивая клиента. Клинтское устройство должно или иметь кнопку запуска процедуры WPS, или иметь WPS PIN.



Варианты использования WPS:

- Если на устройстве есть кнопка, включающая WPS, нажмите её, а затем нажмите на картинку с двумя стрелками рядом с первым пунктом
- Если у клиента есть WPS PIN, введите его в поле и нажмите кнопку Register
- Если клиент запрашивает WPS PIN точки доступа, введите написанное на странице число

Wireless/VLAN and QoS

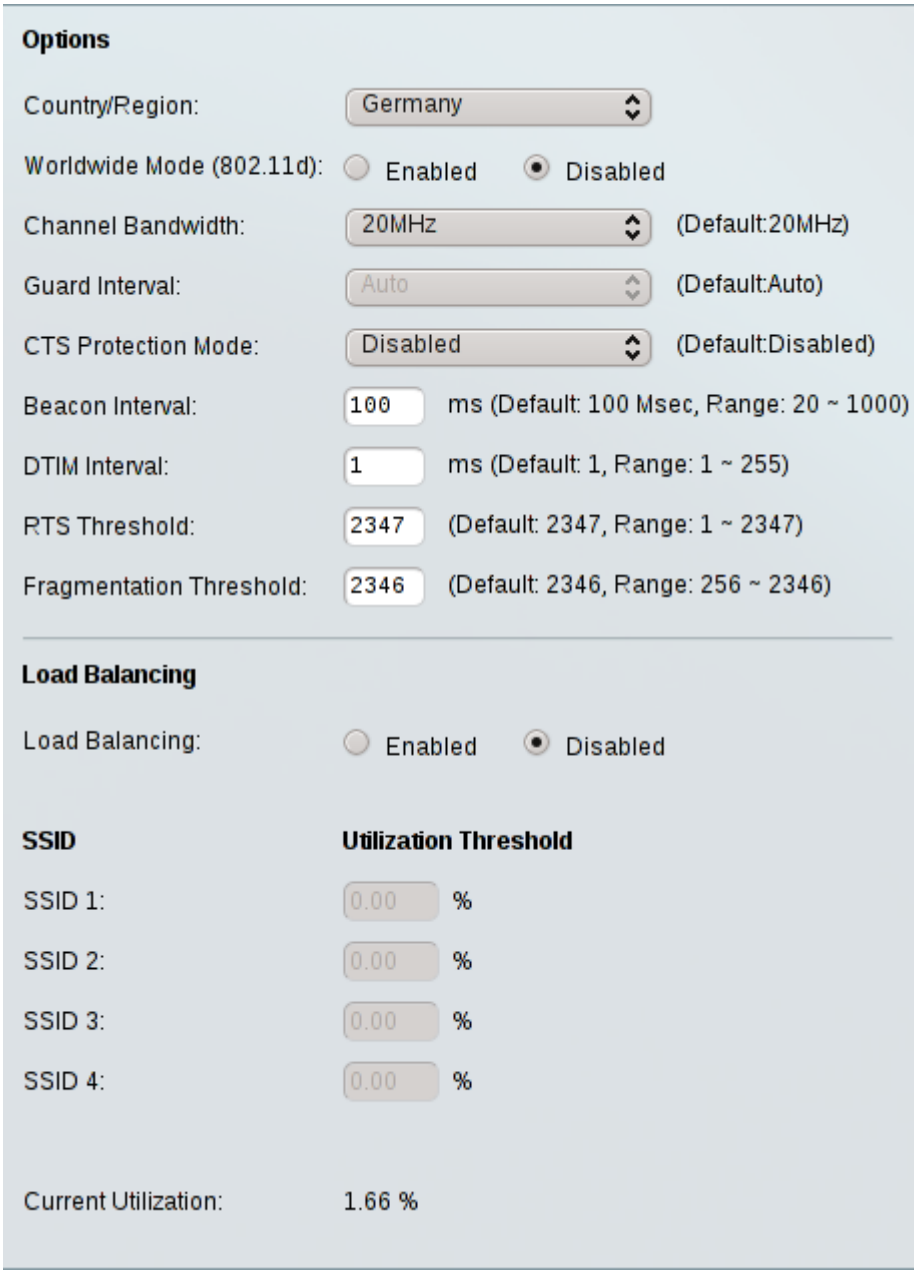


- VLAN — ключ, определяющий использование стандарта IEEE 802.1Q для тегирования

пакетов. На каждую SSID возможно использование одного VLAN

- Default VLAN ID — тег, которым будут маркироваться нетегированные пакеты
- VLAN Tag — режим работы
  - Untagged — перед отправкой пакета с него будет сниматься тег
  - Tagged — тег не будет изменяться
- AP Management VLAN — VLAN ID, из которого можно управлять устройством
- VLAN Tag over WDS — передать используемый VLAN ID через WDS
- QoS — настройки поля Priority в теге 802.1Q для различных VLAN
  - VLAN ID — тег VLAN, для которой настраивается QoS
  - Priority — устанавливаемое значение поля
  - WMM — использование расширения Wireless Multimedia (часть стандарта IEEE 802.11e), которое позволяет использовать приоритеты и процедуры QoS для беспроводной сети

Security/Advanced Settings



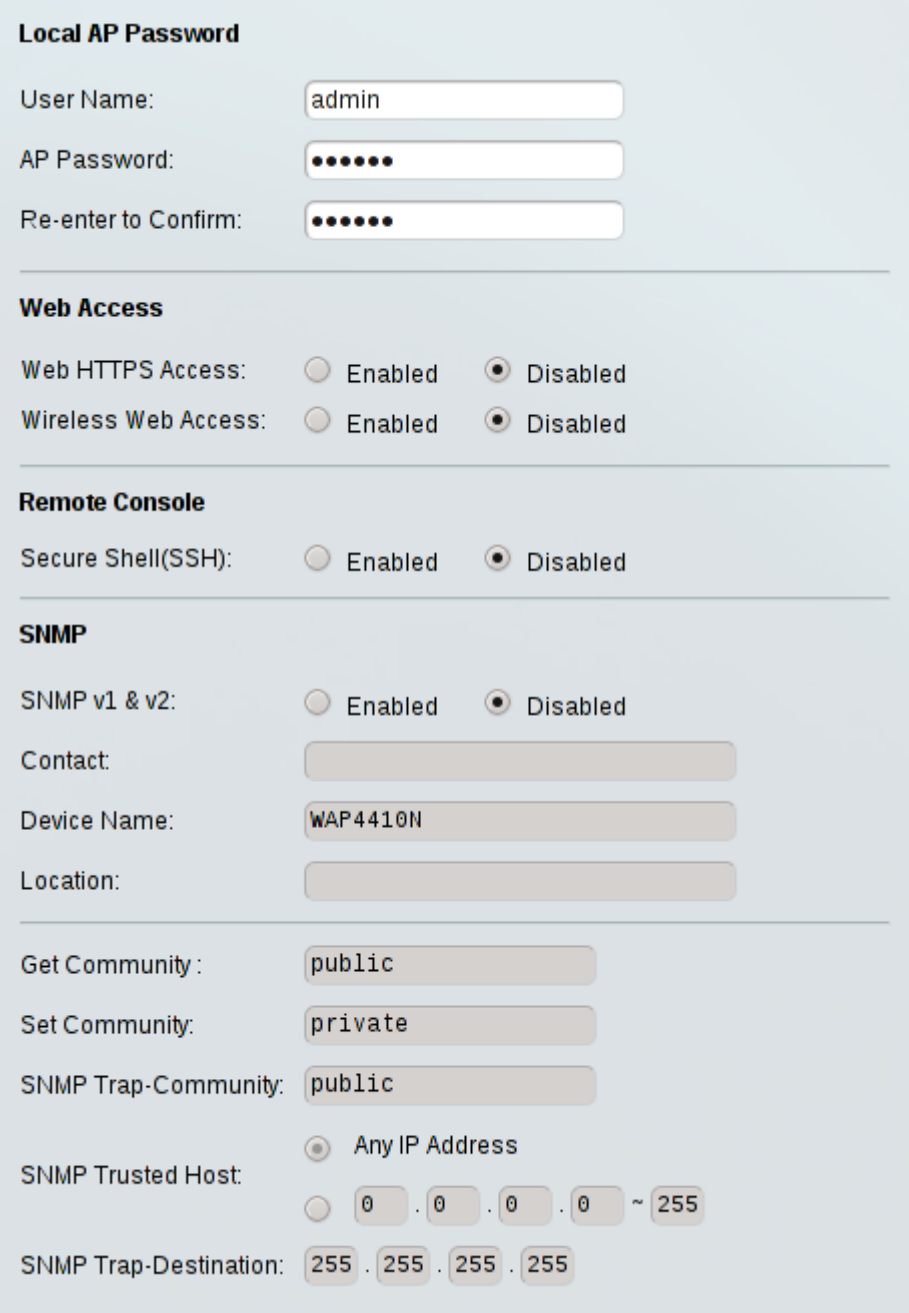
- Country/Region — определяет, какие каналы можно использовать в зависимости от правил законов страны. России в списке нет, следует выбирать Europe
- Worldwide Mode — включить использование стандарта IEEE 802.11d, позволяющего передавать код страны беспроводным клиентам. Клиенты должны поддерживать этот стандарт
- Channel Bandtwidth — ширина канала (20 МГц, 40 МГц или автоматический выбор) для стандарта 802.11n. В стандартах 802.11b/g ширина канала фиксирована на значении 20 МГц
- Guard Interval -
- CTS Protection Mode — режим защиты сигнала
  - Disabled — защита отключена. Если устройство работает на стандартах 802.11g/n, то устройства стандарта 802.11b будут создавать сильную помеху
  - Auto — защита включается при необходимости. В этом режиме чувствительность устройства в условиях сильного шума повышается, но сильно снижается скорость

- Beacon Interval — период между пакетами-маяками
- DTIM Interval — период между сообщениями о доставке трафика (Delivery Traffic Indication Message). Чем меньше значение, тем быстрее работает сеть, однако эти сообщения не дают беспроводному клиенту перейти в энергосберегающий режим
- RTS Threshold — максимальный размер передаваемого пакета. Рекомендуется изменять только в меньшую сторону в случае обнаружения проблем
- Fragmentation Threshold — максимальный размер фрагмента (от 256 до 2346)
- Load Balancing — включить или выключить режим балансировки нагрузки. Режим балансировки нагрузки управляет распределением ресурсов точки доступа между SSID

AP Mode

- Access Point — режим точки доступа
  - Allow wireless signal... — позволить указанным по MAC-адресу повторителям передавать сигнал
- Wireless WDS Repeater — режим повторителя, участвующего в формировании WDS (Wireless Distribution System). WDS позволяет подключать удалённых клиентов без необходимости подведения к удалённым точкам доступа проводной сети, однако WDS снижает производительность в 2 раза. Для работы в этом режиме требуется указать MAC-адрес удалённой точки доступа
- Wireless WDS Bridge — режим моста, участвующего в формировании WDS. К мосту не могут подключаться беспроводные клиенты. Для работы в этом режиме требуется указать список удалённых точек доступа
- Wireless Client/Repeater — режим беспроводного клиента или повторителя
  - Allow wireless station... — позволять беспроводным клиентам использовать устройство как точку доступа
  - Remote Access Point SSID — SSID беспроводной сети, к которой происходит подключение
  - Remote Access Point MAC — MAC-адрес точки доступа беспроводной сети, к которой происходит подключение
- Wireless Monitor — режим отслеживания вредоносных точек доступа
  - No Security — определять точки доступа, не использующие механизмы обеспечения безопасности трафика
  - Not in Legal AP List — определять точки доступа, не находящиеся в списке легальных точек доступа
  - Кнопка Define Legal AP — открыть окно редактирования списка легальных точек доступа

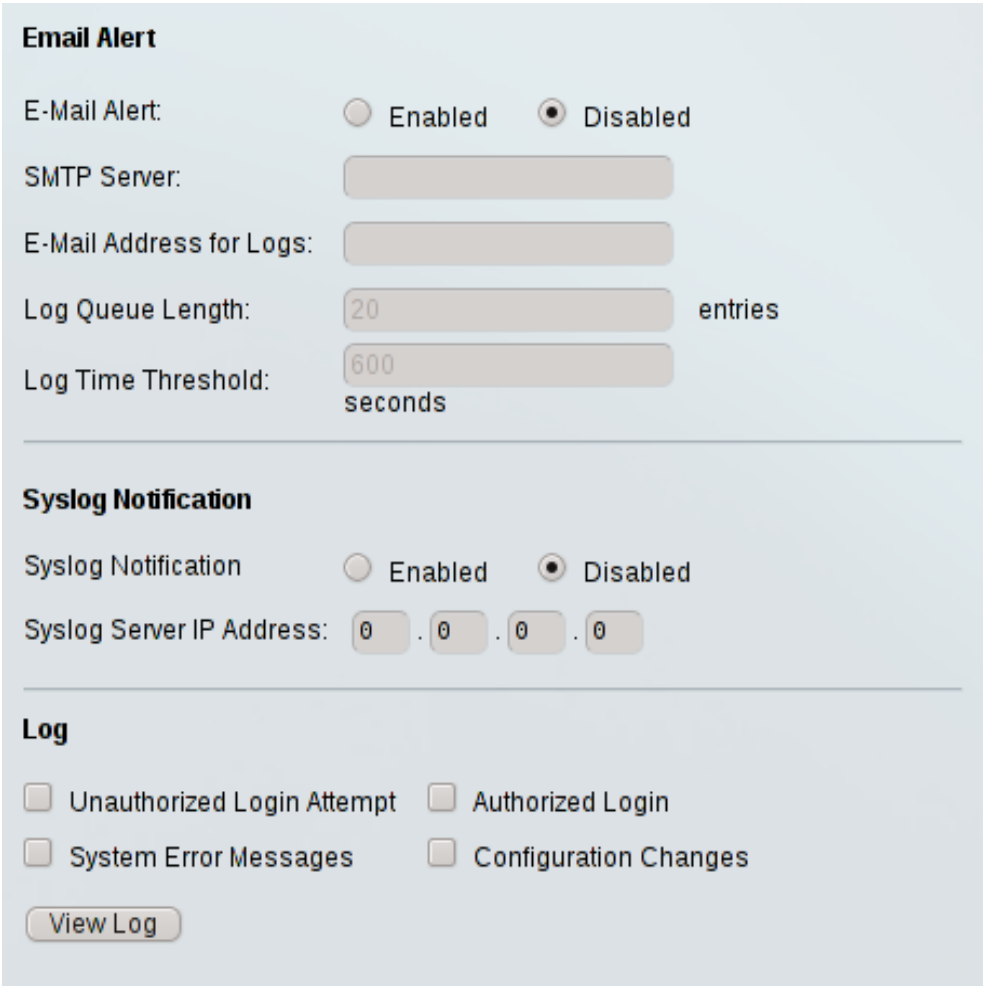
Administration/Management



- User Name — администраторский логин
- AP Password и Re-enter to Confirm — поля для ввода и подтверждения нового пароля
- Web HTTPS Access — включить использование протокола HTTPS для управления устройством
- Wireless Web Access — разрешить вход на веб-интерфейс через беспроводной канал
- Secure Shell(SSH) — разрешить использование SSH
- SNMP v1 & v2 — разрешить использование протоколов SNMPv1 и SNMPv2
- Contact — поле SNMP Sys-Contact
- Device Name — поле SNMP Sys-Name
- Location — поле SNMP Sys-Location
- Get Community — имя сообщества, которому разрешено делать Get-запросы

- Set Community — имя сообщества, которому разрешено делать Get- и Set-запросы
- SNMP Trap-Community — имя сообщества для отправки SNMP-уведомлений (SNMP Trap)
- SNMP Trusted Host — адреса узлов, с которых разрешено использование протокола SNMP
- SNMP Trap-Destination — адрес узла, которому отправляются SNMP Trap

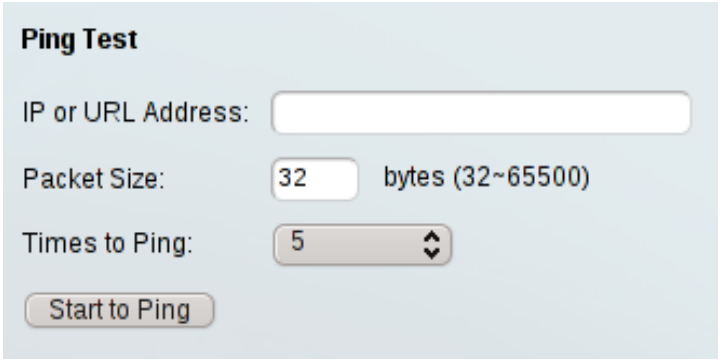
Administration/Log



- E-Mail Alert — включить отправку уведомлений на электронную почту
  - SMTP Server — сервер, через который будет происходить отправка писем
  - E-Mail address for Logs — адрес, от имени которого будут отправляться письма
  - Log Queue Length — количество записей журнала, которые будут отправляться в одной посылке
  - Log Time Threshold — период времени, за который будут отправлены журнальные сообщения
- Syslog Notification — включить использование сервера syslog
  - Syslog Server IP Address — адрес сервера syslog
- Log Unauthorized Login Attempt — записывать в журнал неудачные попытки аутентификации

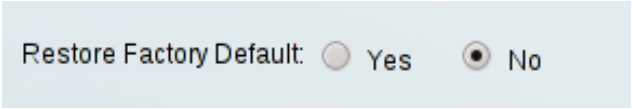
- Log System Error Messages — записывать в журнал системные ошибки
- Log Authorized Login — записывать в журнал удачные попытки аутентификации
- Log Configuration Changes — записывать в журнал изменения конфигурации
- Кнопка View Log — просмотреть журнальные записи

Administration/Diagnostics



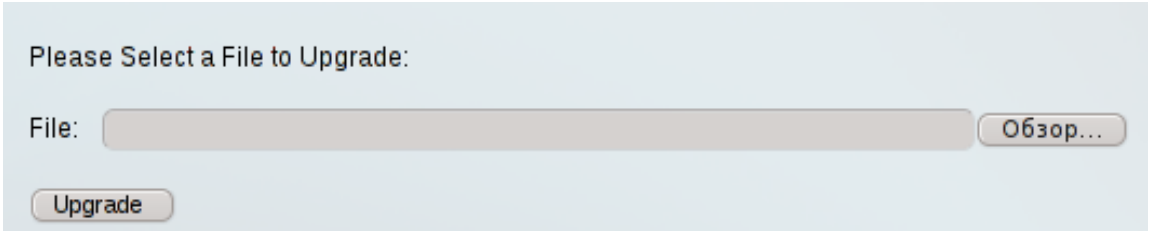
- IP or URL Address — адрес узла, которому надо отправить Ping-запрос
- Packet Size — размер пакета
- Times to Ping — количество отправляемых пакетов
- Кнопка Start to Ping — начать отправку пакетов

Administration/Factory Default



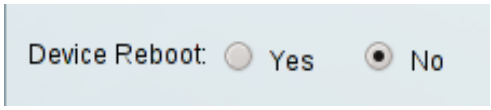
- Restore Factory Default — выставьте ключ в yes и нажмите на Save, чтобы осуществить возврат к заводским настройкам

Administration/Firmware Upgrade



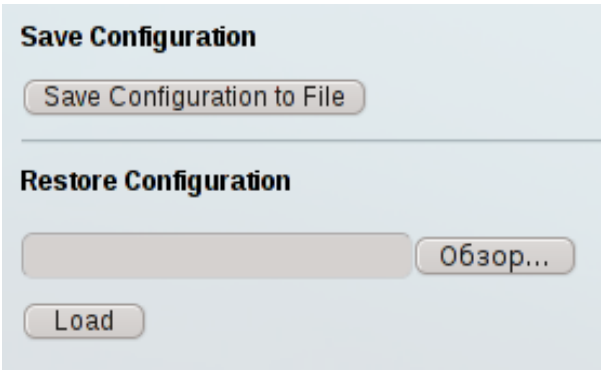
- File — выберите файл с микропрограммой, нажмите кнопку Upgrade и дождитесь окончания процесса прошивки. **Не отключайте питание устройства, пока процесс не закончится!**

Administration/Reboot



- Device Reboot — выберите yes и нажмите Save, чтобы перезагрузить устройство

Administration/Configuration Management



- Кнопка Save Configuration to File — позволит сохранить текущую конфигурацию в файл
- Restore Configuration — выберите файл с конфигурацией и нажмите кнопку Load, чтобы восстановить конфигурацию из файла

3. Linksys WRE54G

Linksys WRE54G — устройство, увеличивающее площадь покрытия беспроводной сети. Физически оно представляет собой ретранслятор (повторитель), перехватывающий пакеты определённой сети и отправляющий их дальше.

Внешний вид

Устройство оснащено двумя индикаторами — Link и Activity. Значение цвета и режима горения индикаторов приведено в таблице ниже.

Режим работы индикатора Link	Значение
Горит синим	Устройство включено и подключено к работоспособной сети
Горит красным	Устройство включено, но не нашло сеть, к которой можно подключиться

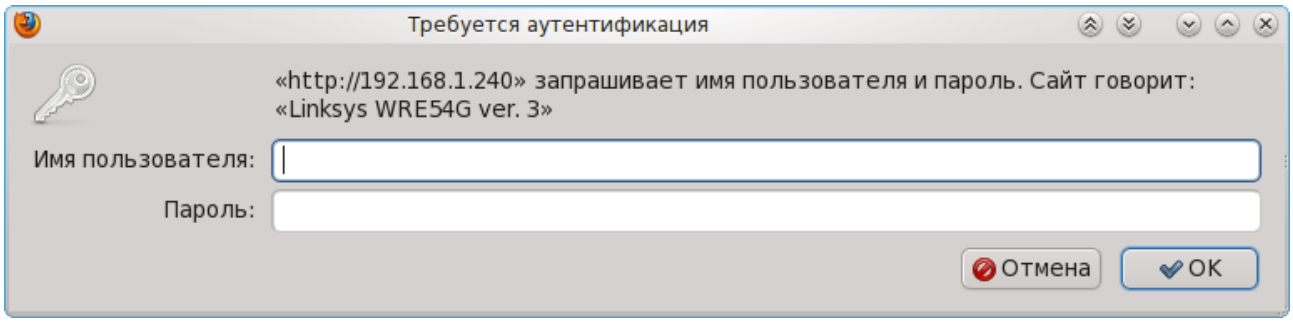
Режим работы индикатора Activity	Значение
Не горит	Устройство не готово к работе
Горит синим	Устройство готово к работе
Моргает синим	В сети есть активность

Настройка

Настройка устройства может выполняться двумя способами — автонастройкой и через веб-интерфейс.

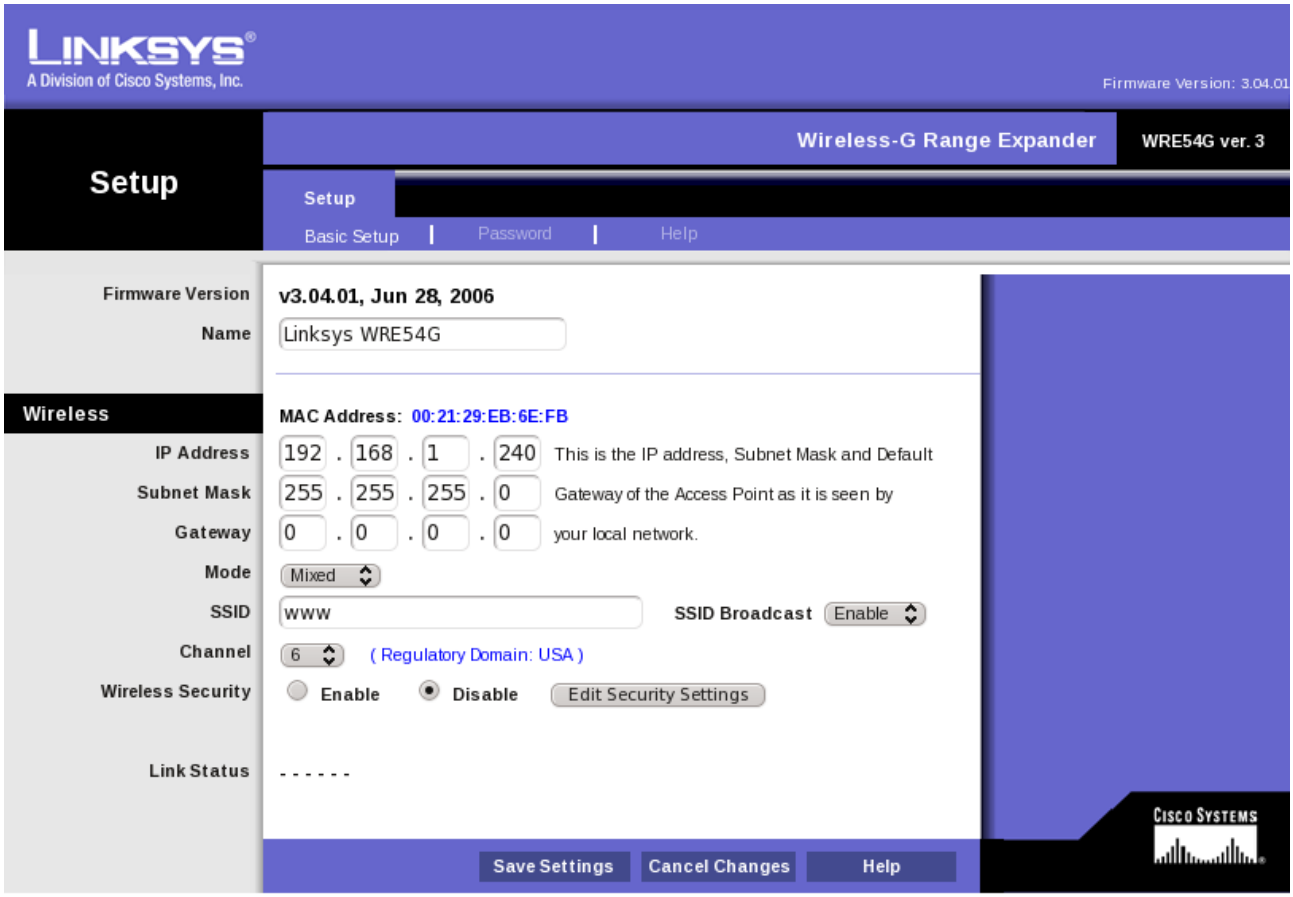
Автонастройка
Автонастройка возможна, если ваша сеть не использует шифрование. Нажмите кнопку Auto Configuration, расположенную на торце устройства. Устройство найдёт первую незашифрованную сеть, к которой оно может подключиться, и начнёмт выполнять свою функцию.

Веб-интерфейс
Управление устройством осуществляется через веб-интерфейс. Подключите кабель Ethernet прямого направления (с одинаково обжатыми концами). После этого откройте в браузере страницу по адресу 192.168.1.240 (адрес по умолчанию). Вам будет выдан запрос на ввод



логина и пароля:

Введите аутентификационные данные (по умолчанию логин пустой, пароль «admin»). Откроется главное окно настройки устройства:

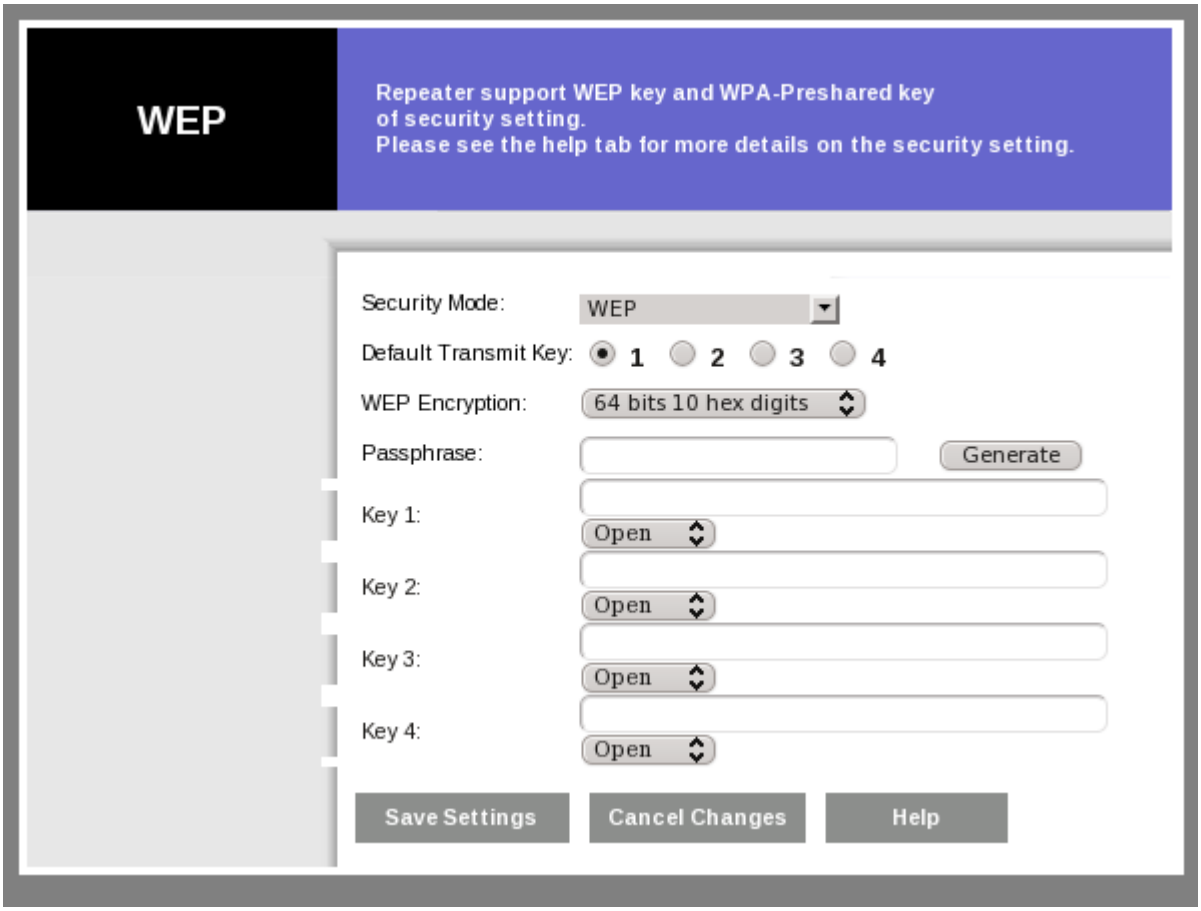


На этом экране вы можете изменить следующие настройки:

- Name — символьное имя устройства.
- IP Address — сетевой адрес устройства. Нужен только для управления.
- Subnet Mask — маска подсети.
- Gateway — шлюз по умолчанию.
- Mode — режим работы устройства:
  - B-Only — работа только в режиме 802.11b;
  - G-Only — работа только в режиме 802.11g;
  - Mixed — поддержка одновременно обоих режимов.
- SSID — имя беспроводной сети, зону покрытия которой вы хотите увеличить.
- SSID Broadcast — управление передачей имени сети в пакетах-маяках.
- Channel — канал, на котором работает устройство.
- Wireless Security — управление использованием алгоритмов обеспечения безопасности трафика (WEP/WPA-PSK).

Строки Firmware Version и Link Status отображают версию микропрограммы (прошивки) и уровень сигнала соответственно.

Если вы включили использование алгоритмов обеспечения безопасности трафика, нажмите на кнопку Edit Security Settings, чтобы перейти к настройке алгоритмов. Вы увидите следующее окно (по умолчанию открывается окно для настройки WEP):



На этом экране вы можете изменить следующие настройки:

17) Security Mode — алгоритм обеспечения безопасности. Поддерживаются WEP и WPA-PSK. Далее идёт описание настроек WEP, настройки WPA перечислены ниже.

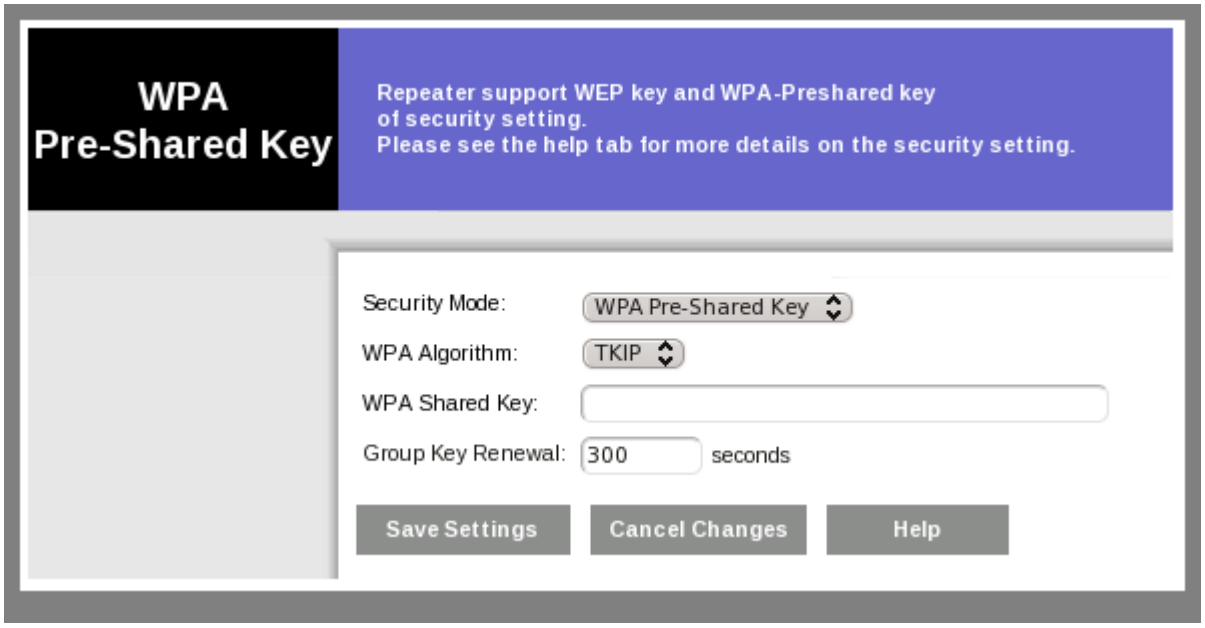
18) Default Transmit Key — индекс ключа, который используется для шифрования исходящих пакетов.

19) WEP Encryption — длина ключа WEP (64 бита = 10 шестнадцатиричных символов или 128 бит = 26 шестнадцатиричных символов)

20) Passphrase и Generate — с помощью этих органов управления можно сгенерировать ключ WEP из парольной фразы.

21) Key 1-Key 4 — ключи соответствующих индексов. Для каждого ключа можно задать режим аутентификации — открытая аутентификация (ассоциация разрешена после предоставления корректного SSID) или аутентификация с общим ключом (ассоциация разрешена после расшифровки контрольного пакета).

Если выбрать алгоритм обеспечения безопасности WPA, вы увидите следующее окно:

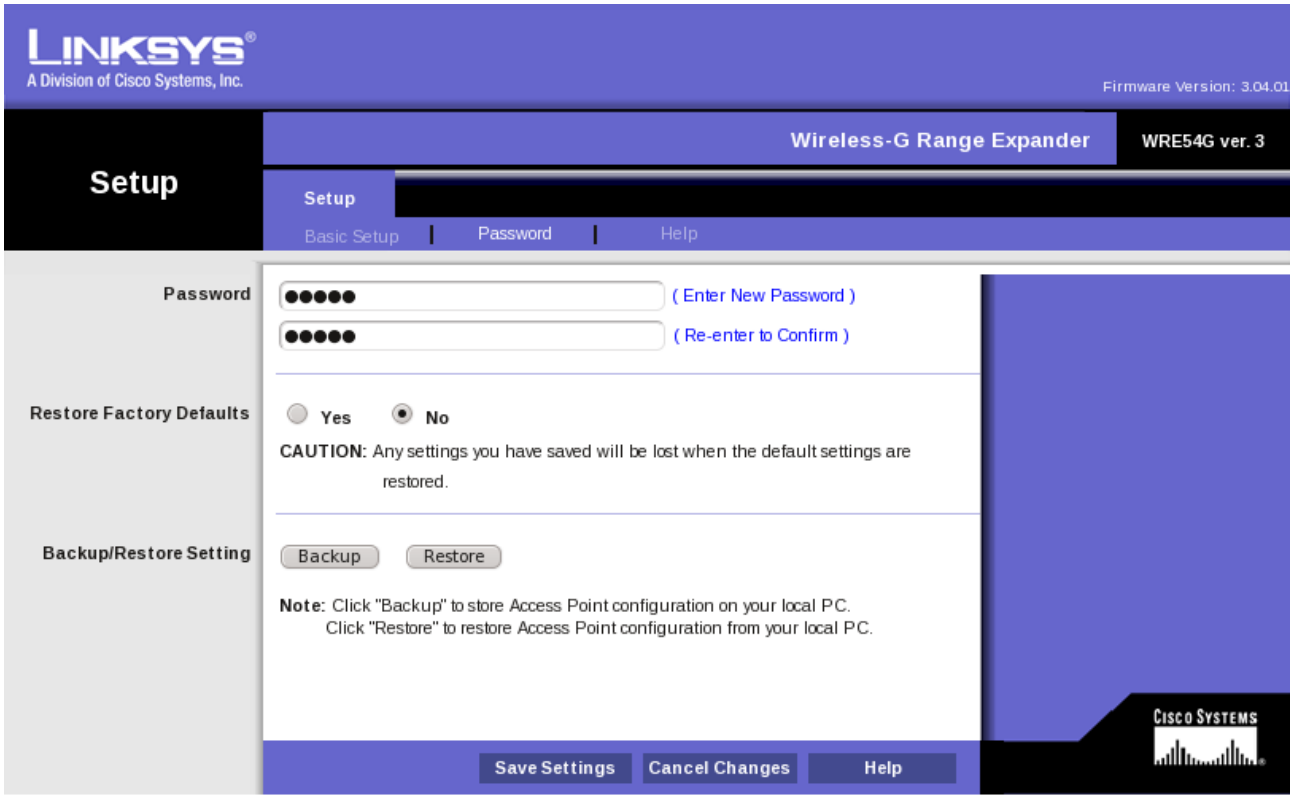


На этом экране вы можете изменить следующие настройки:

10. WPA Algorithm — алгоритм шифрования, применяемый в WPA (TKIP или CCMP/AES).
11. WPA Shared Key — общий ключ шифрования.
12. Group Key Renewal — период обновления группового ключа в секундах.

После изменения настроек на любом экране для их сохранения нажмите кнопку Save Settings.

На главном экране есть закладка Password. Перейдя на неё, вы увидите следующее окно:



В этом окне вы можете сменить пароль (поля Password), вернуться к заводским настройкам путём выбора Yes в пункте Restore Factory Defaults и нажатия на кнопку Save Settings и сохранить настройки в файл или восстановить их из файла с помощью кнопок Backup и Restore соответственно.

Сброс настроек

Чтобы вернуться к настройкам по умолчанию, когда нет возможности попасть в веб-интерфейс, нажмите кнопку Reset, расположенную на торце устройства рядом с кнопкой Auto Configuration, примерно на 10 секунд.