



Глава 11. Так выглядит сеть



Введение в сетевые технологии

Cisco | Networking Academy®
Mind Wide Open™



Глава 11

11.1 Создание и рост

11.2 Обеспечение безопасности сети

11.3 Производительность базовой сети

11.4 Управление файлами конфигурации IOS

11.5 Интегрированные службы маршрутизации

11.6 Резюме



Глава 11. Задачи

- Распознавание устройств и протоколов, используемых в небольших сетях
- Объясните, каким образом небольшая сеть служит в качестве основы для более обширных сетей.
- Объясните необходимость принятия основных мер безопасности сетевых устройств.
- Определите уязвимости в сетевой безопасности, а также основные методы минимизации последствий, вызванных подобными нарушениями.



Глава 11. Задачи (продолжение)

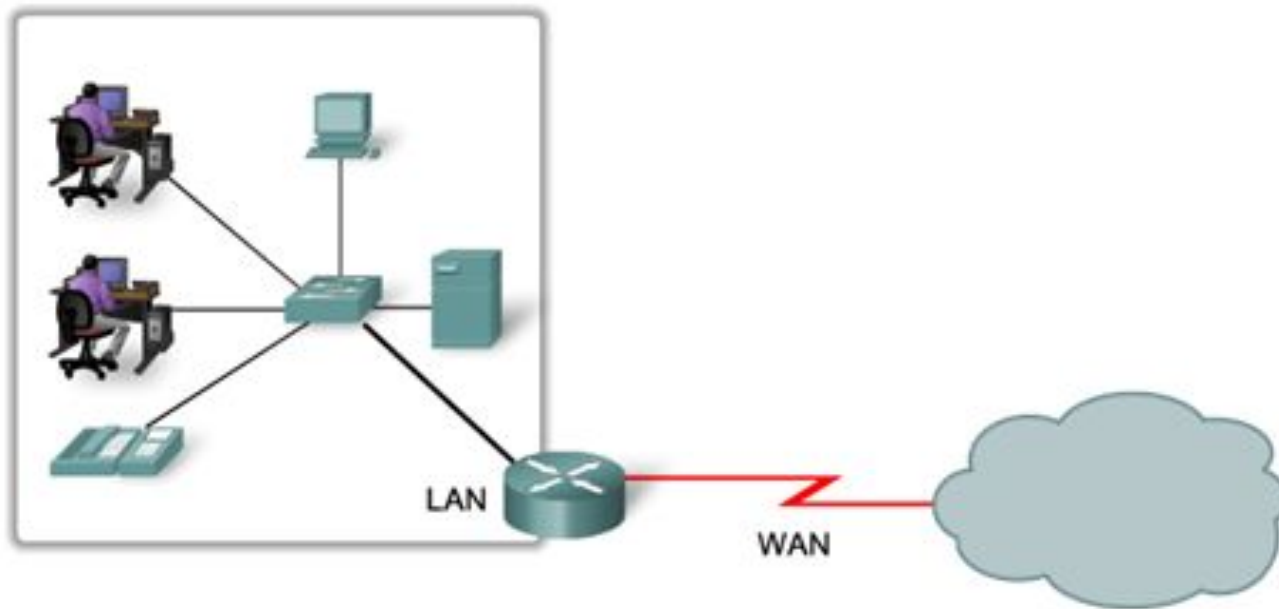
- Используйте результаты, полученные с помощью команд `ping` и `tracert`, для определения относительной производительности сети.
- Используйте основные команды `show` для проверки параметров конфигурации и состояния интерфейса устройства.
- Объясните работу файловых систем на маршрутизаторах и коммутаторах.
- Примените команды резервного копирования и восстановления файла конфигурации IOS.



Устройства, используемые в небольшой сети

Топологии небольших сетей

- Типичная топология небольшой сети





Устройства, используемые в небольшой сети

Выбор устройств для небольшой сети

- Факторы, которые следует учитывать при выборе промежуточных устройств



Объём затрат



Количество портов



Скорость



Возможности расширения/модульность



Возможности управления



Устройства, используемые в небольшой сети

Адресация в небольших сетях

- Схему IP-адресации необходимо планировать, документировать и обслуживать с учётом типа устройств, получающих адрес.
- Примеры устройств, которые будут включены в проект IP-сети:
 - оконечные пользовательские устройства;
 - серверы и периферийные устройства;
 - узлы с доступом через Интернет;
 - промежуточные устройства.
- Спланированные схемы IP-адресации позволяют администратору:
 - отслеживать устройства и устранять неполадки;
 - контролировать доступ к ресурсам.

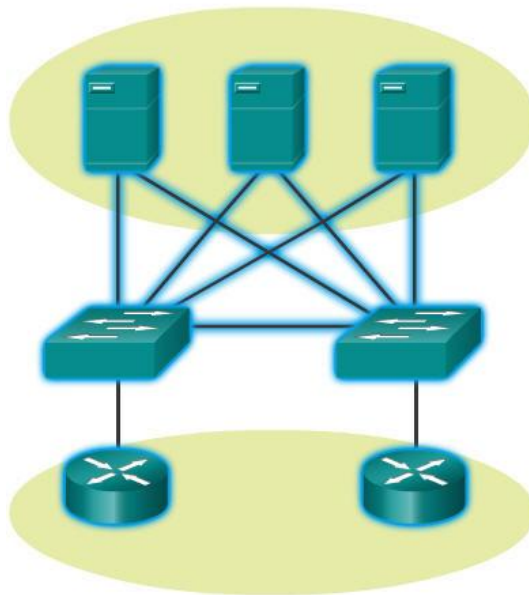


Устройства, используемые в небольшой сети

Резервирование в небольших сетях

- Резервирование позволяет устранить единые точки отказа.
- Также при этом повышается надёжность сети.

Резервирование для серверной фермы





Устройства, используемые в небольшой сети

Рекомендации по проектированию небольших сетей

- В проект сети необходимо включить следующие пункты:

обеспечение защиты файловых и почтовых серверов, имеющих центральное местоположение;

защита расположения посредством физических и логических мер безопасности;

резервирование в рамках серверной фермы;

настройка резервных путей к серверам.





Протоколы в небольших сетях

Стандартные приложения в небольших сетях

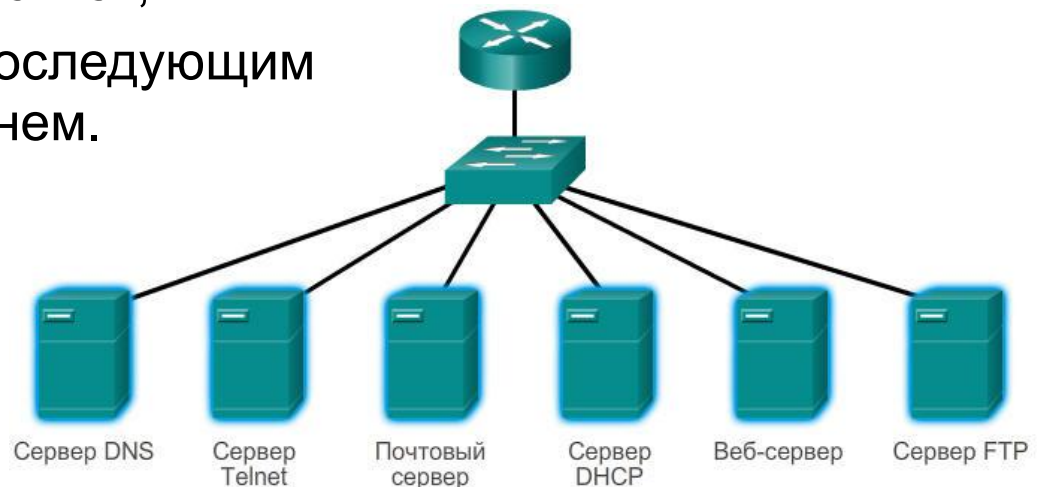
- **Приложения Network-Aware** — это программные приложения, используемые для обмена данными по сети.
- **Службы уровня приложения** — это программы, которые взаимодействуют с сетью и подготавливают данные к передаче.



Протоколы в небольших сетях

Стандартные протоколы в небольших сетях

- Сетевые протоколы определяют:
 - процессы на каждой из сторон сеанса обмена данными;
 - типы сообщений;
 - синтаксис сообщений;
 - значение информационных полей;
 - способы отправки сообщений и предполагаемый ответ;
 - взаимодействие с последующим более низким уровнем.





Приложения реального времени в небольших сетях

- **Инфраструктура:** требует оценки, чтобы подтвердить возможность поддержки предлагаемых приложений реального времени.
- В организациях, которые до сих пор используют телефоны, внедряется протокол VoIP
- IP-телефония: самостоятельно выполняет преобразование голосовых данных в IP
- Протоколы передачи видеоданных в реальном времени: использование транспортного протокола реального времени (RTP) и управляющего транспортного протокола реального времени (RTSP)



Расширение до более крупных сетей

Масштабирование небольших сетей

Важные рекомендации при расширении до более крупных сетей:

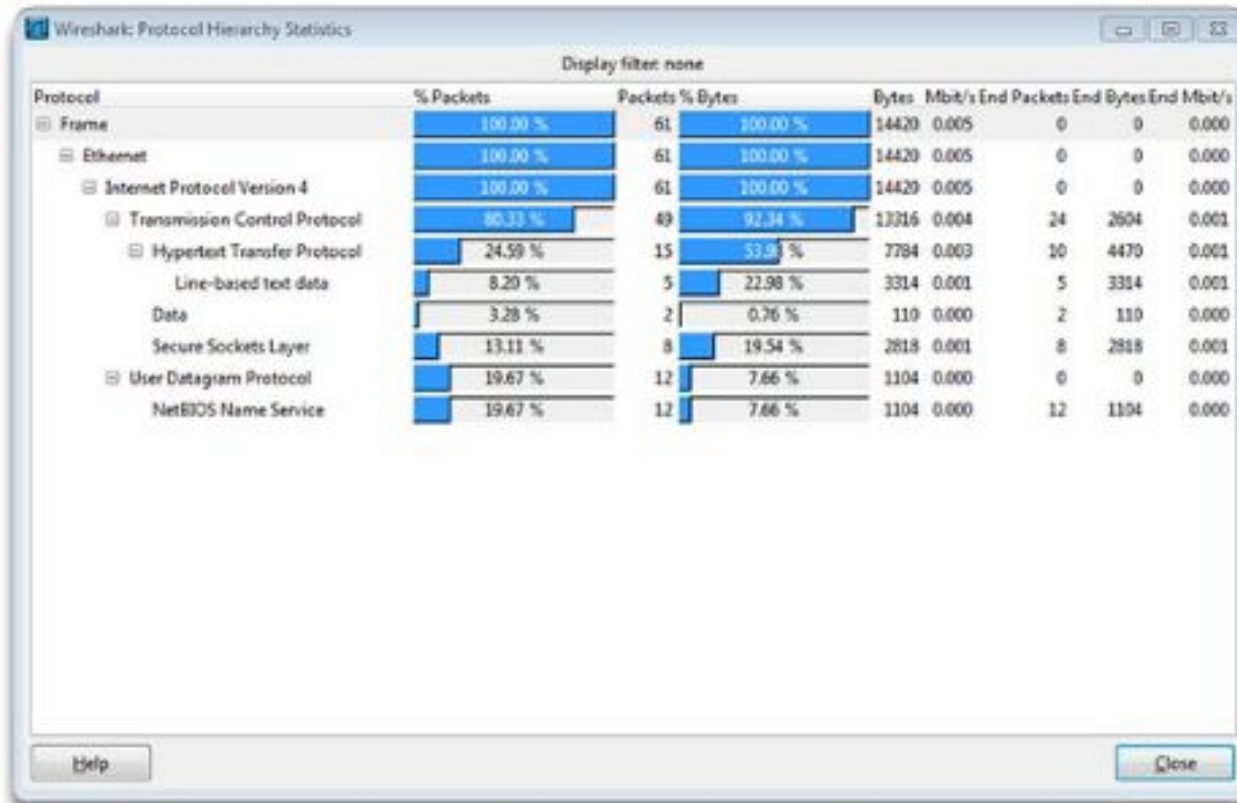
- документация (физическая и логическая топология);
- опись устройств (список устройств, которые используют сеть или являются её частью);
- бюджет (детализированный бюджет на ИТ, включая годовой бюджет на закупку оборудования на финансовый год);
- анализ трафика (необходимо задокументировать протоколы, приложения и службы, а также соответствующие требования к трафику).



Расширение до более крупной сети

Анализ протоколов в небольшой сети

- Сведения, собранные посредством анализа протоколов, можно использовать при принятии решений относительно более эффективного управления трафиком.

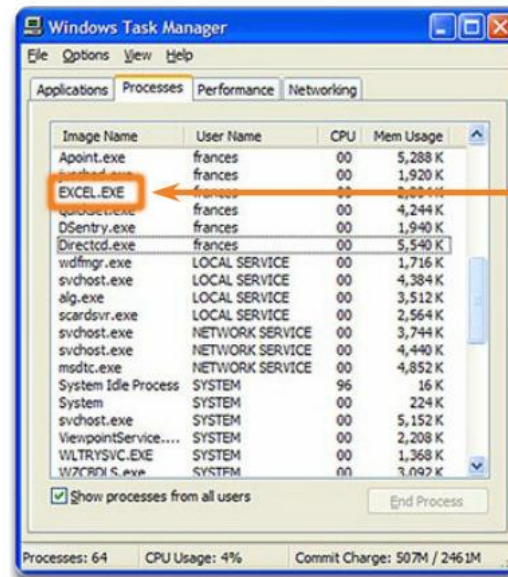




Расширение до более крупной сети

Непрерывное развитие требований к протоколам

- Сетевые администраторы могут получить «снимки» схемы потребления сотрудниками ИТ-приложений.
- Снимки позволяют отслеживать потребление ресурсов и требования к потокам трафика.
- Снимки предоставляют информацию о требуемых изменениях сети.



Процессы представляют собой отдельные программы, работающие одновременно.

К процессам относятся:

- 1 Приложения
- 2 Службы
- 3 Системные операции
- 4 Одна программа может быть запущена несколько раз, каждая из них — в рамках собственного процесса



Меры обеспечения безопасности сетевых устройств

Угрозы сетевой безопасности

- Категории угроз сетевой безопасности



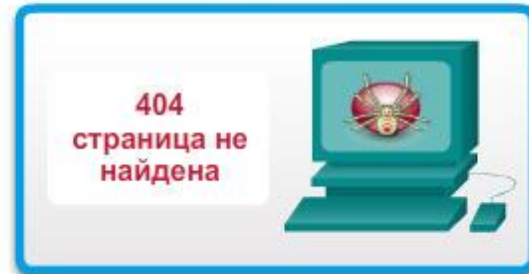
Хищение информации



Потеря данных и манипуляции с данными



Кража личной информации



Прекращение обслуживания



Меры обеспечения безопасности сетевых устройств

Физическая безопасность

Существует четыре класса физических угроз:

- угрозы для аппаратного обеспечения: физическое повреждение серверов, маршрутизаторов, коммутаторов, кабельных линий и рабочих станций;
- угрозы со стороны окружающей среды: предельные температуры (слишком высокие или слишком низкие) или крайние значения влажности (слишком низкая или слишком высокая);
- электрические угрозы: пики напряжения, недостаточное напряжение в сети (провалы напряжения), колебания напряжения (шум) и полное отключение питания;
- эксплуатационные угрозы: ненадлежащее обращение с ключевыми электрическими компонентами (электростатический разряд), отсутствие важных запасных деталей, неправильная прокладка кабелей и недостаточная маркировка.



Меры обеспечения безопасности сетевых угроз

Типы уязвимостей в системе безопасности

- Уязвимости в отношении технологии
- Уязвимости в отношении конфигурации
- Уязвимости в отношении политики безопасности

Уязвимости в системе безопасности сети:

Уязвимости протоколов TCP/IP

- Протокол HTTP (протокол передачи гипертекста), протокол FTP (протокол передачи файлов) и протокол ICMP (протокол управляющих сообщений в Интернете) отличаются низким уровнем безопасности.
- Простой протокол управления сетью (SNMP) и упрощённый протокол передачи почты (SMTP) относятся к изначально небезопасной структуре, на базе которой был разработан протокол TCP.

Уязвимости операционной системы

- Во всех операционных системах существуют проблемы безопасности, которые необходимо устранить.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8
- Эти проблемы задокументированы в архивах группы CERT на веб-сайте <http://www.cert.org>.

Уязвимости сетевого оборудования

Различные типы сетевого оборудования (маршрутизаторы, межсетевые экраны и коммутаторы) имеют свои уязвимости, которые необходимо распознать и обеспечить надлежащую их защиту. К таким слабым местам относятся: защита паролем, отсутствие аутентификации, протоколы маршрутизации и пробелы в межсетевых экранах.



Уязвимости и сетевые атаки

Вирусы, черви и троянские программы

- Вирус — вредоносная программа, которая присоединяется к другой программе с целью выполнения конкретной нежелательной функции на рабочей станции.
- Троянская программа — приложение, которое целиком написано таким образом, чтобы выглядеть как другое приложение, в то время как на самом деле оно является инструментом атаки.
- Черви — это независимые программы, которые атакуют систему и пытаются нанести вред, используя определенные уязвимости в целевой системе. Червь копирует свою программу с атакующего узла на выбранную в качестве жертвы систему, чтобы запустить цикл повторно.



Уязвимости и сетевые атаки

Сетевая разведка



Интернет-запросы



Эхо-тестирование
адресов



Сканирование портов



Анализаторы пакетов





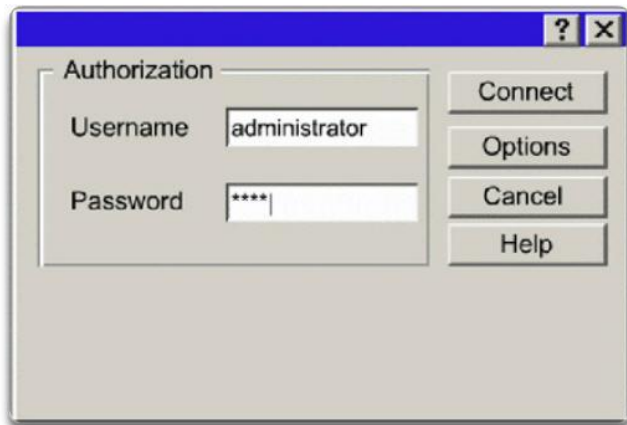
Уязвимости и сетевые атаки

Атаки доступа

Подбор пароля

Злоумышленники могут подобрать пароль несколькими способами.

- Атаки методом грубой силы
- Троянские программы
- Анализаторы пакетов



Переадресация портов

Переадресация портов относится к атакам по типу злоупотребления доверием. При таких атаках скомпрометированный узел используется для передачи через межсетевой экран трафика, который в ином случае был бы сброшен. Риск такой атаки минимизируется в первую очередь за счёт использования правильно подобранных моделей доверия. Антивирусное



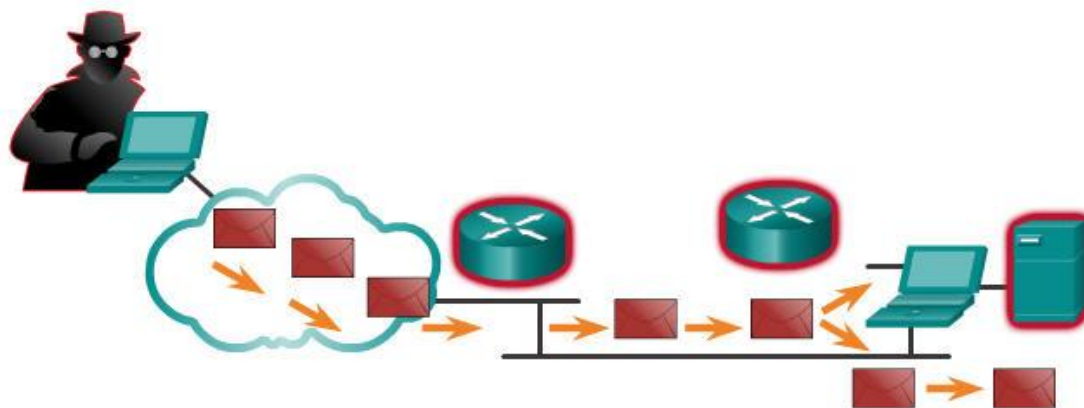


Уязвимости и сетевые атаки

Атаки типа «отказ в обслуживании» (DoS-атаки)

Атака типа «отказ в обслуживании»

Перегрузка ресурсов	Недопустимый формат данных
Дисковое пространство, пропускная способность, буферы	Слишком большие пакеты (например «смертельный эхо-запрос»)
Лавина эхо-запросов (например smurf-атака)	Совмещённый пакет (например «winuke»)
«Шторм пакетов» (например UDP-бомбы и фрэгглинг)	Необработанные данные (например «teardrop»)



Потребляя системные ресурсы, DoS-атаки препятствуют использованию службы правомочными пользователями.



Снижение риска сетевых атак

Резервное копирование, обновление и исправление

- Загружайте и устанавливайте актуальные последние версии антивирусного программного обеспечения.
- Установите обновлённые исправления безопасности





Снижение риска сетевых атак

Аутентификация, авторизация и учёт

Аутентификация, авторизация и учёт (AAA или «Три А»)

- **Аутентификация** — пользователи и администраторы должны подтвердить свою личность. Аутентификация осуществляется с помощью комбинаций имени пользователя и пароля, метода идентификации типа «запрос-ответ», карт-маркеров и других способов.
- **Авторизация** — ресурсы, доступ к которым разрешён для пользователя, и операции, которые пользователю разрешено выполнять.
- **Учёт** — записи, к которым пользователь осуществлял доступ, совокупное время доступа к ресурсу и внесённые изменения.



Снижение риска сетевых атак

Межсетевые экраны

Межсетевой экран размещён между двумя или более сетями. Он осуществляет контроль трафика и позволяет предотвратить несанкционированный доступ. Используются следующие методы:

- фильтрация пакетов;
- фильтрация приложений;
- фильтрация URL-адресов.
- Динамический анализ пакетов (SPI): входящие пакеты должны представлять собой легитимные отклики на запросы внутренних узлов.



Устройства защиты Cisco



Серверные межсетевые экраны



Беспроводные маршрутизаторы Linksys с интегрированным межсетевым экраном



Персональный межсетевой экран



Снижение риска сетевых атак

Безопасность оконечных точек

- К наиболее распространённым оконечным точкам относятся ноутбуки, настольные и планшетные ПК, сервера и смартфоны.
- В целях защиты своих устройств сотрудники должны соблюдать принятые в компании и задокументированные политики безопасности.
- Политики зачастую подразумевают использование антивирусного программного обеспечения и системы предотвращения вторжений на узлы.





Обеспечение безопасности устройств

Введение в принципы обеспечения безопасности устройств

- Сетевая безопасность подразумевает в том числе обеспечение безопасности устройств, включая оконечные и промежуточные устройства.
- Установленные по умолчанию имена пользователей и пароли необходимо немедленно изменить.
- Доступом к системным ресурсам должны обладать только лица, наделённые соответствующими правами.
- Все не востребуемые службы и приложения при возможности необходимо отключить или удалить.
- Необходимо устанавливать обновлённые исправления безопасности по мере их доступности.



Обеспечение безопасности устройств

Пароли

Ненадёжный пароль	Ненадёжность пароля
secret	Пароль — простое словарное слово
smith	Девичья фамилия матери
toyota	Марка автомобиля
bob1967	Имя и год рождения пользователя
Blueleaf23	Простые слова и цифры

Надёжный пароль	Надёжный пароль
b67n42d39c	Сочетает в себе буквы и цифры
12^h u4@1p7	Сочетает в себе буквы и цифры, специальные символы, а также пробел



Обеспечение безопасности устройств

Основные практические рекомендации по обеспечению безопасности

- Шифрование паролей
- Требования к минимальной длине паролей
- Блокирование атак методом грубой силы
- Использование баннерных сообщений
- Установление тайм-аута для режима EXEC

```
Router(config)#service password-encryption
Router(config)#security password min-length 8
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#line vty 0 4
Router(config-vty)#exec-timeout 10
Router(config-vty)#end
Router#show running-config
-more-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```



Обеспечение безопасности устройств

Включение SSH



```

R1#conf t
R1 (config)#ip domain-name span.com
R1 (config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1 (config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1 (config)#username Bob secret cisco
R1 (config)#line vty 0 4
R1 (config-line)#login local
R1 (config-line)#transport input ssh
R1 (config-line)#exit
    
```

- Шаг 1. Настройте доменное имя IP.
- Шаг 2. Создайте односторонние секретные ключи.
- Шаг 3. Подтвердите или создайте запись в локальной базе данных.
- Шаг 4. Включите поддержку входящих сеансов SSH VTY.



Ping

Интерпретация сообщений ICMP

- **!** – обозначает получение сообщения об эхо-отклике ICMP
- **.** – показывает истечение тайм-аута в ожидании сообщения эхо-ответа от протокола ICMP
- **U** — получено сообщение ICMP «Недоступно»

Проверка локального TCP/IP-стека

Эхо-тестирование локального узла подтверждает, что протокол TCP/IP установлен и исправно функционирует на адаптере локальной сети.

Отправка эхо-запроса по IP-адресу 127.0.0.1 приведёт к тому, что устройство выполнит эхо-тестирование в отношении себя самого.



Ping

Эффективное использование расширенного режима команды «ping»

- В Cisco IOS доступен «расширенный» режим команды «ping»

R2# ping

Protocol [ip]:

Target IP address: **192.168.10.1**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **10.1.1.1**

Type of service [0]:



Ping

Базовый уровень сети

Выполнение единой проверки

FEB 8, 2013 08:14:43

```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

MAR 17, 2013 14:41:06

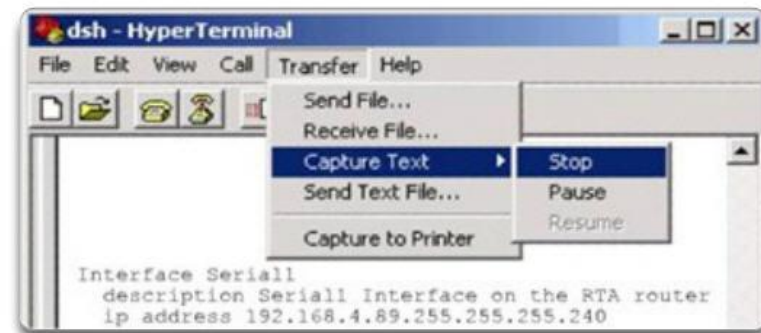
```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

Перехват эхо-запроса маршрутизатора: сохранение в текстовый файл



В сеансе работы с терминалом выполните следующие действия:

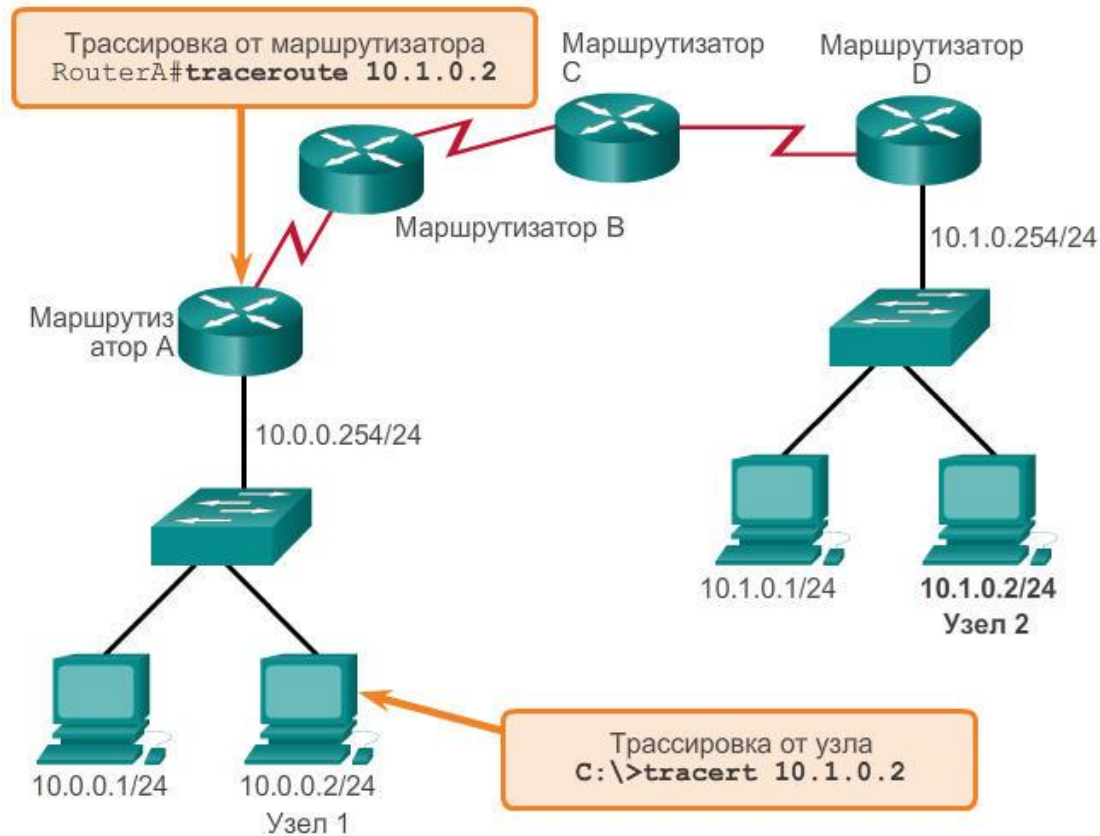
1. Иницируйте процесс захвата текста.
2. Выполните команду **ping** <ip address> .
3. Остановите процесс захвата текста.
4. Сохраните текстовый файл.



Tracert

Интерпретация сообщений команды tracert

Проверка пути к удалённому узлу





Команды show

Пересмотр наиболее распространённых команд «show»

- С помощью команды **show** можно отобразить состояние практически любого процесса или функции маршрутизатора.
- Часто используемые команды «show»:
 - show running-config**
 - show interfaces**
 - show arp**
 - show ip route**
 - show protocols**
 - show version**



Команды «show»

Просмотр настроек маршрутизатора с помощью команды «show version»

Версия Cisco IOS

Программа начальной загрузки

Образ Cisco IOS

ЦП и ОЗУ

Количество и тип физических интерфейсов

Объём памяти NVRAM

Объём флеш-памяти

Регистр конфигурации

```

Router#show version
Cisco Internetwork Operating System Software
IOS(tm)2500 Software (C2500-PL),Version 12.0(17a),RELEASE
SOFTWARE (fcl)
Copyright (c)1986-2002 by cisco Systems,Inc.
Compiled Mon 11-Feb-02 05:55 by kellythw
image text-base:0x00001000
ROM:system Bootstrap,Version 11.0(10c),SOFTWARE
BOOTFLASH :3000 Bootstrap Software (IGS-BOOT-R),Version
11.0(10c),RELEASE SOFTWARE (fcl)
System image file is "flash:c2500-i-1.120-17a.bin"
cisco 2500 (68030 processor(revision N) With 2048K/2048K
bytes of memory.
processor bord ID 08860060,with hardware revision 00000000
Bridging software.
X.25 software,version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile Configuration memory.
8192K bytes of processor board system flash (Read ONLY)
Configuration register is 0x2102
Router#
    
```



Команды «show»

Просмотр настроек коммутатора с помощью команды «show version»

```

Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE2,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh
Image text-base: 0x00003000, data-base: 0x00AA2F34

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE
SOFTWARE (fc1)

Switch uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-25.SEE2/c2960-lanbase-
mz.122-25.SEE2.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K
bytes of memory.
Processor board ID FOC1107Z9ZN
Last reset from power-on
1 Virtual Ethernet interface
  
```



Команды узла и IOS

Параметры команды ipconfig

- ipconfig - отображает IP-адрес, маску подсети, шлюз по умолчанию.
- ipconfig /all – также отображает MAC-адрес.
- Ipconfig /displaydns - отображает все кэшируемые записи DNS в системе Windows.

```

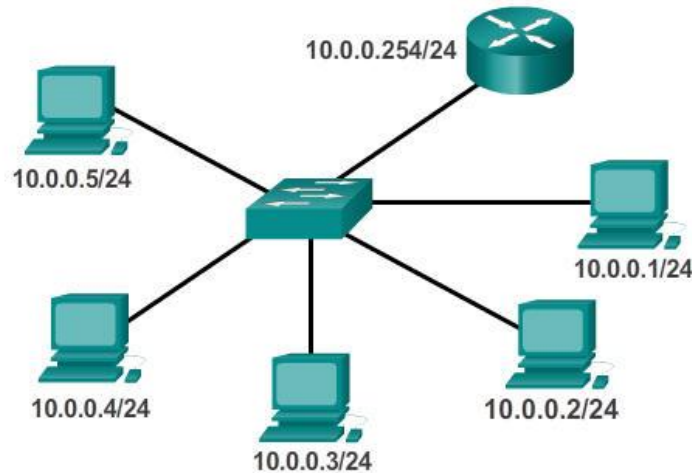
C:\>ipconfig /all
Ethernet adapter Network Connection:
    Connection-specific DNS Suffix: example.com
    Description . . . . . : Intel(R)
    PRO/Wireless 3945ABG Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-FB
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.2.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.2.3.254
    DHCP Server . . . . . : 10.2.3.69
    DNS Servers . . . . . : 192.168.226.120
    Lease Obtained. . . . . : Thursday, May 03,
                             2007 3:47:51 PM
    Lease Expires . . . . . : Friday, May 04,
                             2007 6:57:11 AM

C:\>
    
```



Команды узла и IOS

Параметры команды «arp»



```

c:\>arp -a
Internet Address Physical Address Type
10.0.0.2         00-08-a3-b6-ce-04 dynamic
10.0.0.3         00-0d-56-09-fb-d1 dynamic
10.0.0.4         00-12-3f-d4-6d-1b dynamic
10.0.0.254      00-10-7b-e7-fa-ef dynamic
  
```

Пара MAC-адрес/IP-адрес





Команды узла и IOS

Параметры команды «show cdp neighbors»

```

R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
S3                Fas 0/0        151        S I         WS-C2950   Fas 0/6
R2                Ser 0/0/1      125        R           1841       Ser 0/0/1

R3#show cdp neighbors detail

Device ID: R2
Entry address(es):
  IP address : 192.168.1.2
Platform: Cisco 1841, Capabilities: Router Switch IGMP
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
    
```




Использование команды «show ip interface brief»

- Можно использовать для проверки статуса всех сетевых интерфейсов на маршрутизаторе или коммутаторе.

```

Router1#show ip interface brief
Interface                IP-Address      OK?  Method  Status        Protocol
FastEthernet0/0          192.168.254.254 YES  NVRAM    up             up
FastEthernet0/1/0        unassigned      YES  unset   down          down
Serial0/0/0               172.16.0.254   YES  NVRAM    up             up
Serial0/0/1               unassigned      YES  unset   administratively down  down
-----
Router1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
-----
Router1#traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
 0 172.16.0.253 8 msec 4 msec 8 msec
 1 10.0.0.254 16 msec 16 msec 8 msec
 2 192.168.0.1 16 msec * 20 msec
    
```



Файловые системы маршрутизатора и коммутатора

Файловые системы маршрутизатора

- show file systems:** команда перечисляет все доступные файловые системы на маршрутизаторе Cisco 1941.

```

Router# show file systems
File Systems:

      Size (b)      Free(b)      Type  Flags  Prefixes
      -          -          -      -      -
      -          -          opaque rw      archive:
      -          -          opaque rw      system:
      -          -          opaque rw      tftpvs:
      -          -          opaque rw      null:
      -          -          network rw      tftp:
* 256487424      183234560    disk  rw      flash0: flash:#
      -          -          disk  rw      flash1:
      262136      254779      nvram rw      nvram:
      -          -          opaque wo      syslog:
      -          -          opaque rw      xmodem:
      -          -          opaque rw      ymodem:
      -          -          network rw      scp:
      -          -          network rw      ftp:
      -          -          network rw      http:
      -          -          network rw      https:
      -          -          opaque ro      tar:
      -          -          network rw      https:
      -          -          opaque ro      cns:
  
```

- * Символ * указывает на то, что данная файловая система является текущей по умолчанию



Файловые системы маршрутизатора и коммутатора

ФайЛОВЫЕ СИСТЕМЫ КОММУТАТОРА

- **show file systems:** команда перечисляет все доступные файловые системы на коммутаторе Catalyst 2960.

```
Switch#show file systems
File Systems:

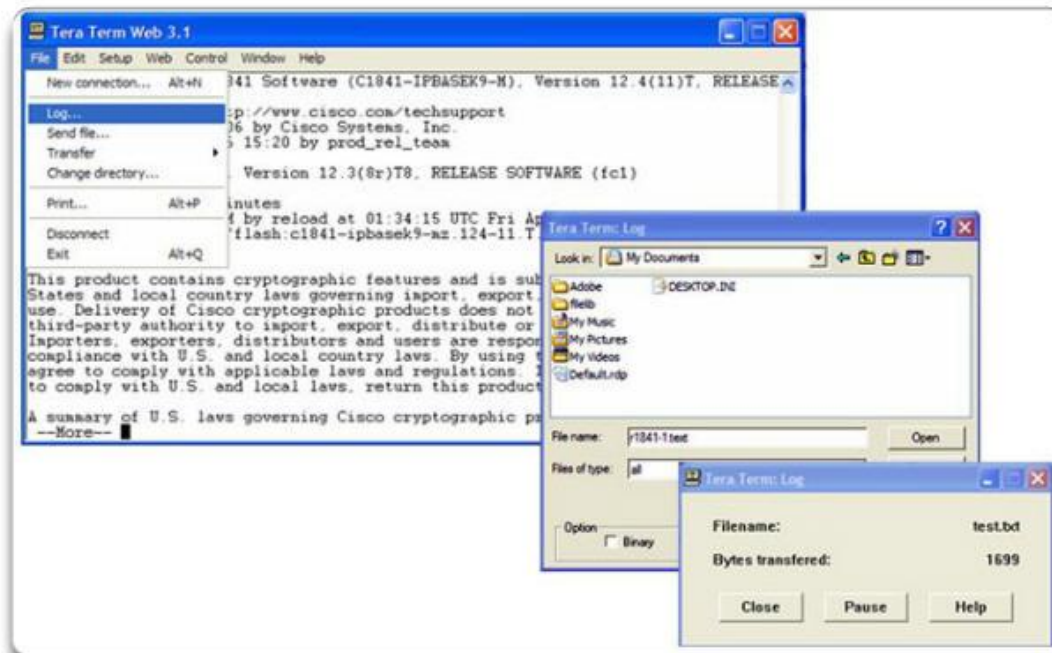
  Size(b)   Free(b)   Type   Flags  Prefixes
*  32514048  20887552  flash  rw     flash:
    -        -         opaque rw     vb:
    -        -         opaque ro     bs:
    -        -         opaque rw     system:
    -        -         opaque rw     tmpsys:
    65536    48897    nvram  rw     nvram:
    -        -         opaque ro     xmodem:
    -        -         opaque ro     ymodem:
    -        -         opaque rw     null:
    -        -         opaque ro     tar:
    -        -         network rw     tftp:
    -        -         network rw     rcp:
    -        -         network rw     http:
    -        -         network rw     ftp:
    -        -         network rw     scp:
    -        -         network rw     https:
    -        -         opaque ro     cns:
```



Резервное копирование и восстановление файлов конфигурации

Резервное копирование и восстановление с помощью текстовых файлов

Сохранение текстового файла в программе Tera Term



1. Запустите процесс журнала.
2. Выполните команду **show running-config**.
3. Закройте журнал.



Резервное копирование и восстановление файлов конфигурации

Резервное копирование и восстановление с помощью протокола TFTP

- Файлы конфигурации можно хранить на сервере TFTP (простой протокол передачи файлов).
- `copy running-config tftp` — сохранение запущенной конфигурации на TFTP-сервер
- **`copy startup-config tftp`** — сохранение конфигурации загрузки на TFTP-сервер

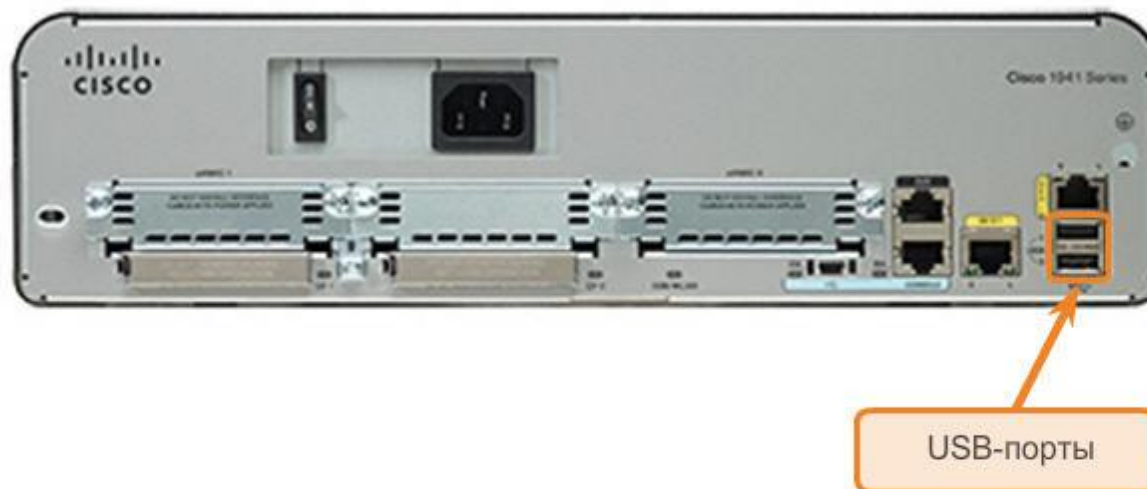
```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm]
Writing tokyo.2 !!!!!!! [OK]
```



Резервное копирование и восстановление файлов конфигурации

Использование интерфейсов USB на маршрутизаторах Cisco

- USB-накопитель должен быть отформатирован в формате FAT16.
- Он может содержать несколько копий Cisco IOS и несколько конфигураций маршрутизатора.
- Позволяет администратору быстро и удобно перемещать конфигурации с одного маршрутизатора на другой.





Резервное копирование и восстановление файлов конфигурации

Резервное копирование и восстановление с помощью протокола USB

```
R1#copy running-config usbflash0:
Destination filename [running-config]? R1-Config
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```

Копирование на USB-накопитель, файл ещё не существует.

```
R1#copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
```

Копирование на USB-накопитель, тот же файл конфигурации уже существует на диске.



Интегрированный маршрутизатор

Многофункциональное устройство

- Сочетает в себе функции коммутатора, маршрутизатора и точки беспроводного доступа.
- Предоставляет функции маршрутизации, коммутации и беспроводного подключения.
- Беспроводные маршрутизаторы Linksys имеют простую конструкцию и используются в домашних сетях
- В линейке продуктов интегрированных маршрутизаторов Cisco (ISR) доступен широкий ассортимент продуктов, пригодных для использования как в небольших офисных сетях, так и в сетях большего масштаба.

Linksys: Model WRT300N2

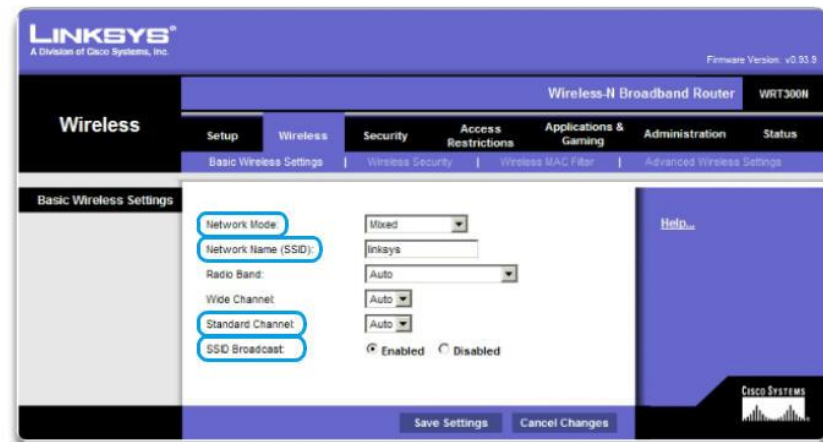




Интегрированный маршрутизатор

Функции беспроводного подключения

- **Режим беспроводной сети:** большинство интегрированных беспроводных маршрутизаторов поддерживают стандарты 802.11b, 802.11g и 802.11n
- **Идентификатор набора услуг (SSID) —** чувствительное к регистру буквенно-числовое имя домашней беспроводной сети.
- **Беспроводной канал —** спектр РЧ, разделённый на каналы.



Щёлкните любой параметр беспроводной сети, чтобы получить дополнительную информацию.



Интегрированный маршрутизатор

Базовый уровень безопасности беспроводной сети

- Изменение значений по умолчанию
- Отключение широковещательной рассылки SSID
- Настройка шифрования с использованием WEP или WPA
- **Протокол обеспечения конфиденциальности, сопоставимой с проводными сетями (WEP):** использует предварительно определённые ключи для шифрования и расшифровки данных. На всех беспроводных устройствах, для которых разрешён доступ к сети, необходимо ввести один и тот же ключ WEP.
- **Защищённый доступ к Wi-Fi (WPA):** также использует ключи шифрования длиной от 64 до 256 бит. Каждый раз при установлении соединения с точкой доступа генерируются новые ключи. Следовательно, уровень безопасности повышается.



Интегрированный маршрутизатор

Настройка интегрированного маршрутизатора

- Доступ к маршрутизатору обеспечивается путём подключения компьютера с помощью кабеля к одному из портов LAN Ethernet маршрутизатора.
- Подключаемое устройство автоматически получает от интегрированного маршрутизатора данные об IP-адресации.
- В целях безопасности измените имя пользователя и пароль по умолчанию, а также IP-адрес устройства Linksys по умолчанию.

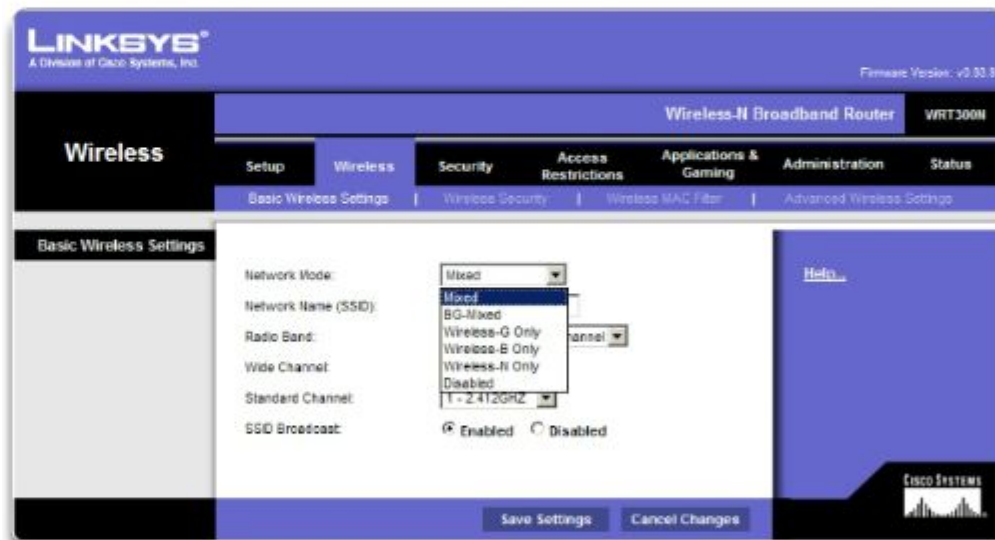




Интегрированный маршрутизатор

Включение беспроводной сети

- Настройка режима беспроводной сети
- Настройка идентификатора SSID
- Настройка канала РЧ
- Настройка всех желаемых параметров шифрования для системы безопасности





Интегрированный маршрутизатор

Настройка параметров клиента беспроводной сети

- Параметры конфигурации клиента беспроводной сети должны соответствовать параметрам беспроводного маршрутизатора.
 - SSID (Имя сети)
 - Настройки системы безопасности
 - Канал
- Программное обеспечение клиента беспроводной сети может быть интегрированным в операционную систему устройства или автономным, загружаемым служебным ПО беспроводной связи.





Глава 11. Заключение

- Качественный проект сети подразумевает надёжность, масштабируемость и доступность.
- Необходимо обеспечить защиту сети от вирусов, троянских программ, червей и сетевых атак.
- ЗадOCUMENTИРУЙТЕ данные производительности базовой сети.
- Проверьте подключение к сети, используя команды «ping» и «tracert».
- Используйте команды IOS для мониторинга и просмотра данных о сети и сетевых устройствах.
- Создайте резервные копии файлов конфигурации, используя протоколы TFTP или USB.
- Домашние сети и малые предприятия зачастую используют интегрированные маршрутизаторы, которые предоставляют функции коммутатора, маршрутизатора и точки беспроводного доступа.

Cisco | Networking Academy[®]

Mind Wide Open[™]