Глава 10. Уровень приложений

Материалы для инструктора

CCNA Routing and Switching

Введение в сетевые технологии (v6.0)

Материалы для инструкторов. Глава 10. Руководство по планированию

- Эта презентация PowerPoint состоит из двух частей:
- Руководство по планированию для инструкторов
  - Ознакомительная информация по главе
  - Методические пособия
- Презентация перед классом для инструктора
  - Дополнительные слайды, которые можно использовать в классе
  - Начало на слайде № 12

- **Примечание.** Перед предоставлением общего доступа удалите руководство по планированию из данной презентации.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 10. Уровень приложений

Introduction to Networks 6.0. Руководство по планированию

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 10. Упражнения

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
10.0.1.2	Упражнение в аудитории	Исследование приложений	Необязательно
10.1.1.4	Интерактивное упражнение	Приложение и презентация (протоколы и стандарты)	Рекомендуется
10.1.2.5	Лабораторная работа	Изучение функции обмена файлами по сетям P2P	Необязательно
10.2.1.7	Packet Tracer	Интернет и электронная почта	Необязательно
10.2.2.4	Инструмент проверки синтаксиса	Команды DNS интерфейса командной строки в Windows и Linux	Рекомендуется
10.2.2.7	Cisco Packet Tracer	DHCP-серверы и DNS-серверы	Необязательно
10.2.2.8	Лабораторная работа	Изучение разрешения DNS	Рекомендуется
10.2.3.3	Packet Tracer	FTP	Необязательно
10.2.3.4	Лабораторная работа	Изучение FTP	Рекомендуется

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 10. Упражнения (продолжение)

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
10.3.1.1	Упражнение в аудитории	За работу!	Необязательно
10.3.1.2	Cisco Packet Tracer	Изучение работы сети	Необязательно
10.3.1.3	Многопользовательский режим программы Cisco Packet Tracer	Учебный модуль	Необязательно
10.3.1.4	Многопользовательский режим программы Cisco Packet Tracer	Реализация услуг	Необязательно

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 10. Проверочная работа

- После прохождения главы 10 учащиеся должны пройти проверку на знание материала главы 10.
- Для неформальной оценки успехов учащихся можно использовать контрольные работы, лабораторные работы, работу с симулятором Packet Tracer и другие упражнения.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 10. Практические рекомендации

Прежде, чем излагать материал главы 10, обратите внимание на следующее:

- Инструктор должен пройти проверку на знание материала главы 10 «Проверочная работа».
- Цели этой главы:
  - Объяснить, каким образом взаимодействуют функции уровня приложений, уровня представления и сеансового уровня, для предоставления приложениям конечного пользователя доступа к сетевым сервисам.
  - Объяснить, как распространенные протоколы уровня приложений взаимодействуют с приложениями конечных пользователей.
  - Объяснить, как работают веб-протокол и протокол электронной почты.
  - Объяснить принципы работы протоколов DNS и DHCP.
  - Объяснить, как работают протоколы передачи файлов.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 10. Практические рекомендации (продолжение)

- На уровне приложений данные вводятся в сеть данных. Для начала обсудите популярные сетевые и интернет-приложения. В качестве примера можно привести веб-обозреватели, электронную почту, Telnet и т. д.
- Объясните студентам, что понимание служб и протоколов чрезвычайно важно, поскольку сетевым трафиком можно управлять в зависимости от используемой службы и соответствующего протокола. Следовательно, различные типы сетевого трафика могут определяться протоколом, который используется для передачи трафика.
- В одноранговых сетях каждый компьютер может быть либо клиентом, либо сервером. Поскольку каждое устройство может выполнять обе задачи, они называются одноранговыми узлами.
- Убедитесь, что студенты не путают одноранговую сеть с клиентами файлообменных сетей, такими как Gnutella или BitTorrent.
- Клиенты файлообменных сетей предоставляют пользователям возможность непосредственного обмена определенными типами файлов в одноранговых или в клиент-серверных сетях.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 10. Практические рекомендации (продолжение)

- Объясните, что основная задача службы DNS — упростить взаимодействие пользователя и системы путем преобразования URL-адресов, которые используются приложениями, в IP-адреса, необходимые для сети передачи данных.
- Используя программу Wireshark, выполните захват потока пакетов к одному из известных веб-сайтов. Обратите внимание на запрос DNS IP-адреса, отправленный на URL-адрес веб-сайта, и на ответ с IP-адресом.
- Обсудите три протокола электронной почты и объясните различия между протоколами POP и IMAP.
  - При использовании IMAP: в клиентское приложение загружаются копии сообщений. Исходные сообщения остаются на сервере до тех пор, пока они не будут удалены вручную.
- Объясните, что задача DHCP — упростить взаимодействие пользователя и сети путем автоматического получения IP-адреса для компьютера.
  - После включения компьютера, на котором настроено использование DCHP, он отправляет DCHP-запрос для получения IP-адреса. После этого любой доступный DHCP-сервер отправляет IP-адрес (а также другие сведения о конфигурации IP).
- Протокол DHCP — DORA — Discover, Offer, Request, Acknowledge (Открытие, предложение, запрос, подтверждение)

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 10. Дополнительная помощь

- Дополнительные справочные материалы, содержащие различные стратегии обучения, в том числе планы занятий, описание аналогий для сложных понятий и темы обсуждений, доступны на веб-сайте сообщества сертифицированных сетевых специалистов (CCNA) по адресу https://www.netacad.com/group/communities/community-home.
- Практические рекомендации специалистов со всего мира для обучения по программе CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna
- Если вы хотите поделиться с другими преподавателями планами занятий и другой полезной информацией, вы можете разместить её на сайте сообщества CCNA.
- Студенты могут записаться на курс **Introduction to Packet Tracer** (Введение в Packet Tracer) (для самостоятельного изучения)

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

CISCO

Глава 10. Уровень приложений

Название учебного плана

Введение в сетевые технологии (v6.0)

Глава 10. Разделы и задачи

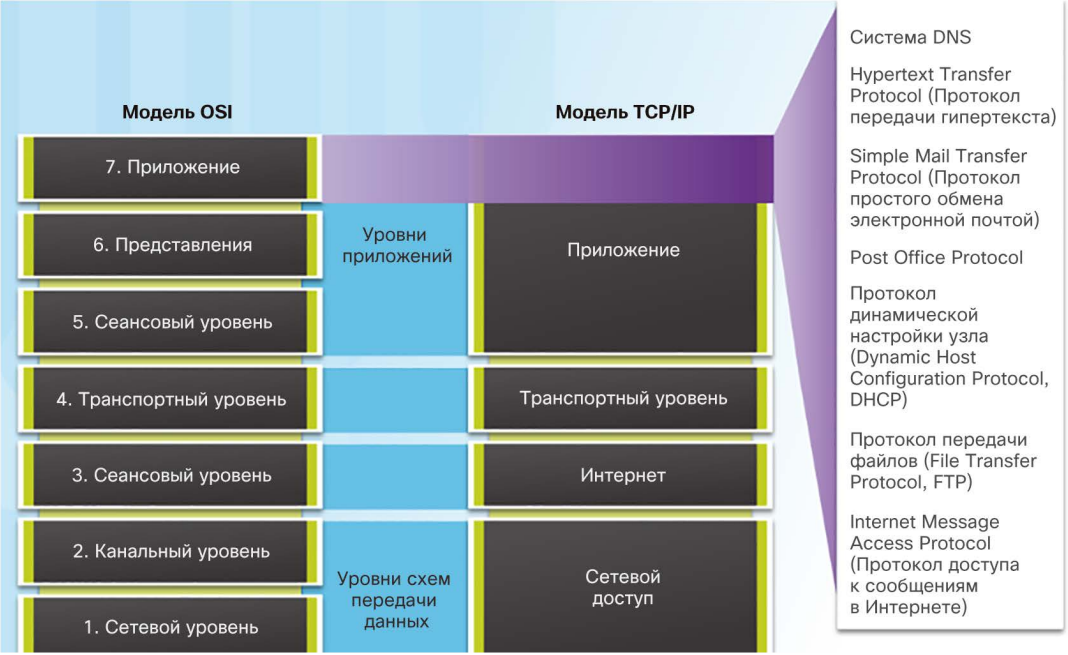
- 10.1. Протоколы уровня приложений
  - Объяснить, как на уровне приложений поддерживается работа приложений конечного пользователя.
    - Объяснить, каким образом взаимодействуют функции уровня приложений, уровня представления и сеансового уровня, для предоставления приложениям конечного пользователя доступа к сетевым сервисам
    - Объяснить, как распространенные протоколы уровня приложений взаимодействуют с приложениями конечных пользователей.
- 10.2. Общеизвестные протоколы и службы уровня приложений
  - Объяснить, как работают общеизвестные протоколы уровня приложений TCP/IP.
    - Объяснить, как работают веб-протокол и протокол электронной почты.
    - Объяснить принципы работы протоколов DNS и DHCP.
    - Объяснить, как работают протоколы передачи файлов.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

10.1. Протоколы уровня приложений

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

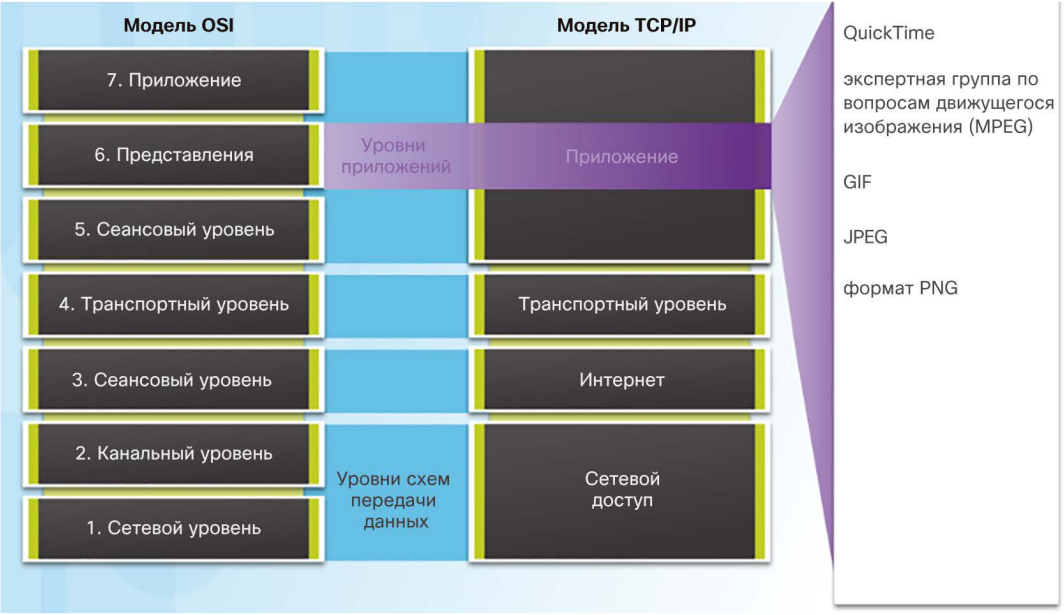
Уровень приложений



- Уровень приложений:
  - Ближайший к конечному пользователю.
  - Используется для обмена данными между программами, исполняемыми на хосте источника и хосте назначения.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

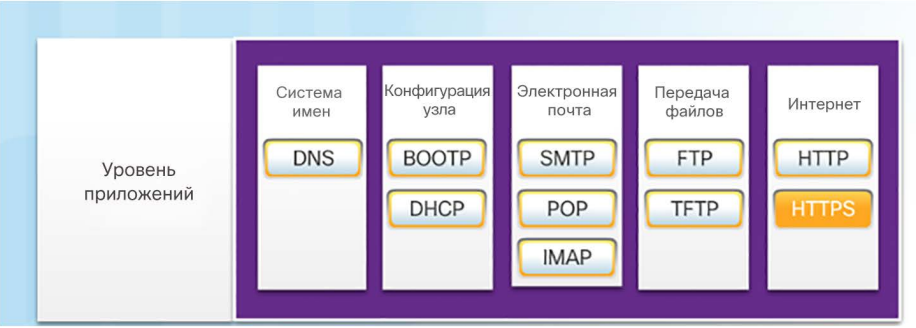
Уровень представления и сеансовый уровень



- Функция уровня представления:
  - Форматирование данных из исходного устройства в форме, совместимой с получающим устройством.
  - Сжатие данных.
  - Шифрование данных.
- Функция сеансового уровня
  - Создание и поддержание диалогов между исходными и конечными приложениями.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Протоколы уровня приложений TCP/IP

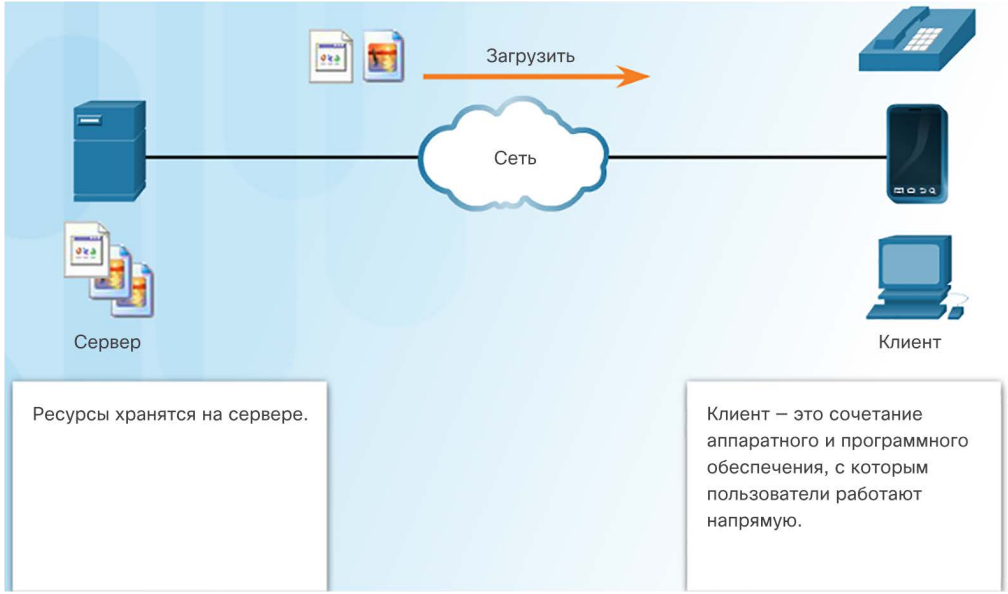


- Сервер доменных имен (DNS) TCP, UDP 53 — преобразует доменные имена, например cisco.com, в IP-адреса.
- (BOOTP) — протокол Bootstrap — BOOTP был замещен протоколом DHCP.
- Протокол динамической настройки узла (DHCP) UDP, клиент 68, сервер 67 — динамически присваивает IP-адреса клиентским станциям при запуске.
- Упрощенный протокол электронной почты (SMTP) TCP 25 — позволяет клиентам отправлять электронные сообщения на почтовый сервер.
- Почтовый протокол (POP) TCP 110 — позволяет клиентам получать электронные письма с почтового сервера.
- Протокол доступа к сообщениям в сети Интернет (IMAP) TCP 143 — позволяет клиентам получать электронные письма с почтового сервера, при этом электронные письма остаются на сервере.
- Протокол передачи файлов (FTP) TCP 20 и 21 — надежный протокол доставки файлов с подтверждением, ориентированный на установление соединения.
- Простейший протокол передачи файлов (TFTP) UDP 69 — простой протокол передачи файлов без установления соединения.
- Протокол передачи гипертекстовой информации (HTTP) TCP 80, 8080 — набор правил для обмена текстом, графическими изображениями и т. д. в Интернете.
- Протокол защищенной передачи гипертекстовой информации (HTTPS) TCP, UDP 443 — использует шифрование и аутентификацию для безопасного обмена данными.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Модель «клиент-сервер»

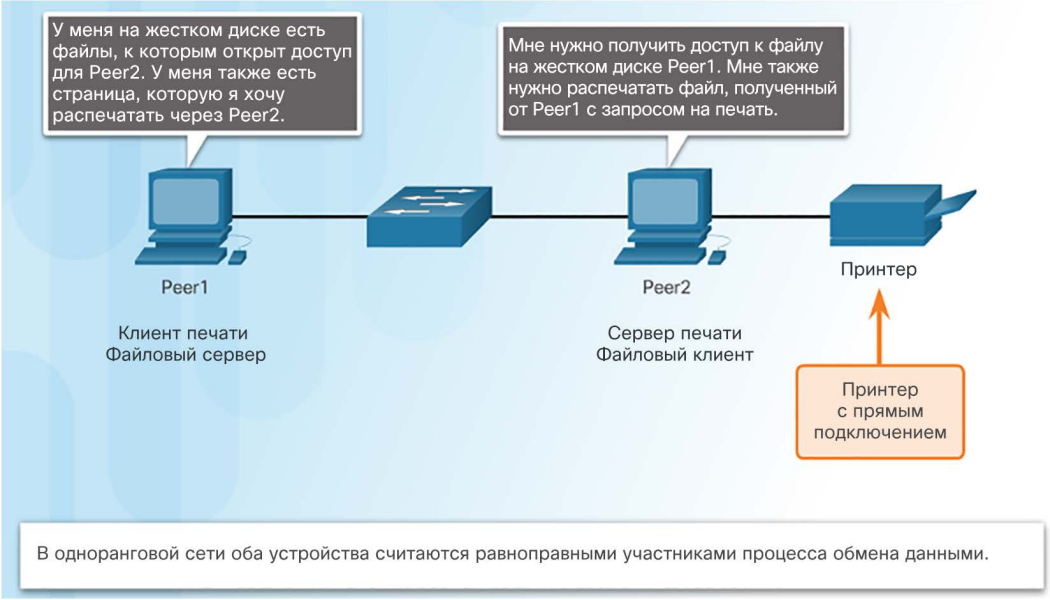
- Считается, что процессы модели «клиент — сервер» происходят на уровне приложений.
- Протоколы уровня приложений описывают формат запросов и ответов между клиентами и серверами.
- Примером сети типа «клиент-сервер» является использование службы электронной почты для отправки, получения и хранения электронных писем



© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Одноранговые сети

- Доступ к данным с однорангового устройства осуществляется без использования выделенного сервера.
- Каждое устройство (называемое одноранговым) может выполнять функции как сервера, так и клиента.



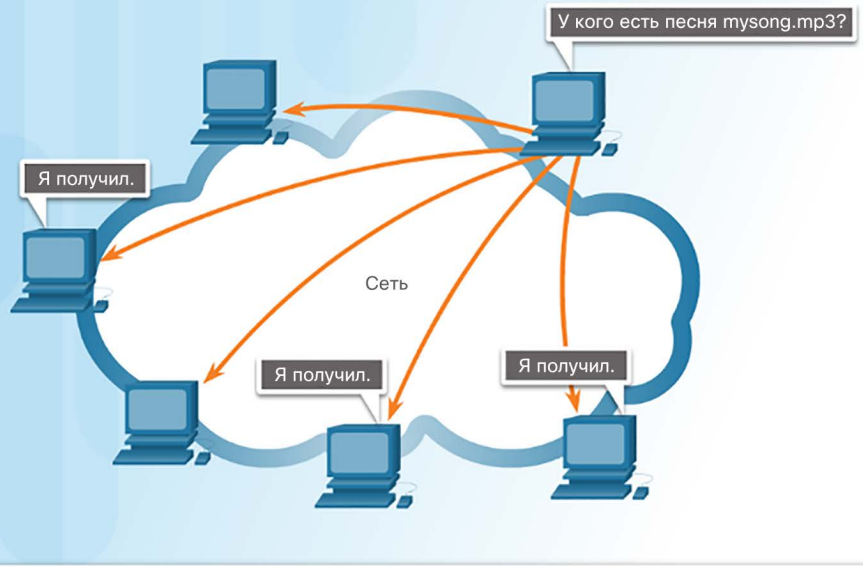
© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Одноранговые приложения

- Одноранговое приложение (P2P) позволяет устройству выступать в роли как клиента, так и сервера в пределах одного сеанса связи.
- Для P2P-приложений требуется, чтобы каждое конечное устройство предоставляло пользовательский интерфейс и запускало сервис в фоновом режиме.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Наиболее распространенные одноранговые приложения



Приложение Gnutella позволяет P2P-приложениям выполнять поиск по общим ресурсам нескольких одноранговых узлов.

- Наиболее распространенные P2P-сети:
  - G2
  - Bitcoin
  - BitTorrent
  - eDonkey
- Некоторые P2P-приложения разработаны на основе протокола Gnutella, который предполагает обмен целыми файлами между пользователями.
- Многие P2P-приложения позволяют пользователям совместно использовать части множества файлов в одно и то же время. Это технология BitTorrent.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Изучение функции обмена файлами по сетям P2P

Cisco Networking Academy®

Mind Wide Open™

Lab - Researching Peer-to-Peer File Sharing

Objectives

Part 1: Identify P2P Networks, File Sharing Protocols, and Applications

Part 2: Research P2P File Sharing Issues

Part 3: Research P2P Copyright Litigations

Background / Scenario

Peer-to-peer (P2P) computing is a powerful technology that has many uses. P2P networks can be used to share and exchange files, and other electronic materials.

The use of P2P networks to upload, download, or share copyrighted material, such as movies, music, and software, can violate the rights of copyright owners. In the P2P file-sharing context, infringement may occur when one person purchases an authorized copy and then uploads it to a P2P network to share with others. Both the individual who makes the file available and those making copies may be found to have infringed the rights of the copyright owners and may be violating copyright law.

Another problem with P2P file sharing is that very little protection is in place to ensure that the files exchanged in these networks are not malicious. P2P networks are an ideal medium for spreading malware, such as computer viruses, worms, Trojan horses, spyware, adware, and other malicious programs.

In this lab, you will research available P2P file sharing software and identify issues that can arise from the use of this technology.

Required Resources

Device with Internet access

Part 1: Identify P2P Networks, File Sharing Protocols, and Applications

In Part 1, you will research P2P networks and identify popular P2P protocols and applications.

Step 1: Define P2P networking.

a. What is a P2P network?

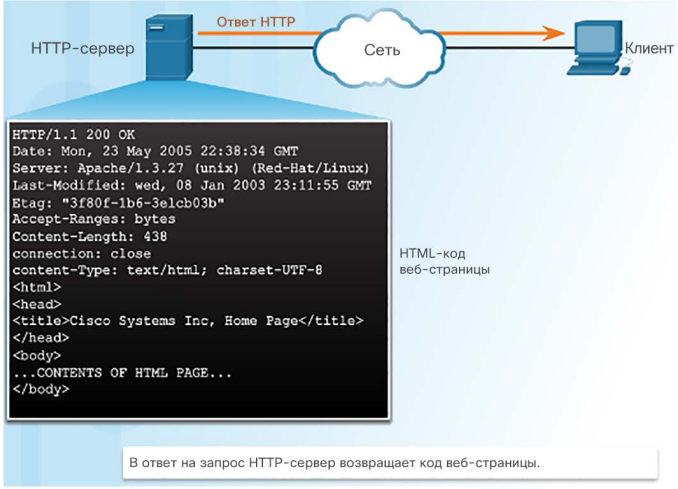
© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

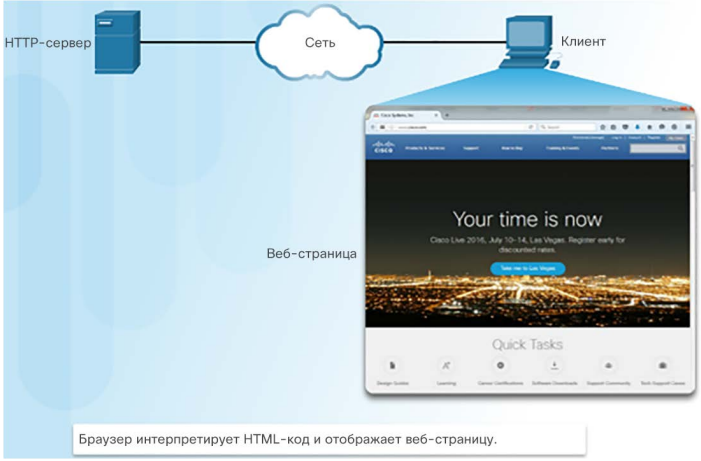
10.2. Общеизвестные протоколы и службы уровня приложений

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Протокол передачи гипертекста (HTTP) и язык гипертекстовой разметки (HTML)

- После ввода в адресной строке веб-адреса или универсального указателя ресурса (URL) веб-обозреватель устанавливает соединение по протоколу HTTP с веб-сервисом, запущенным на сервере.

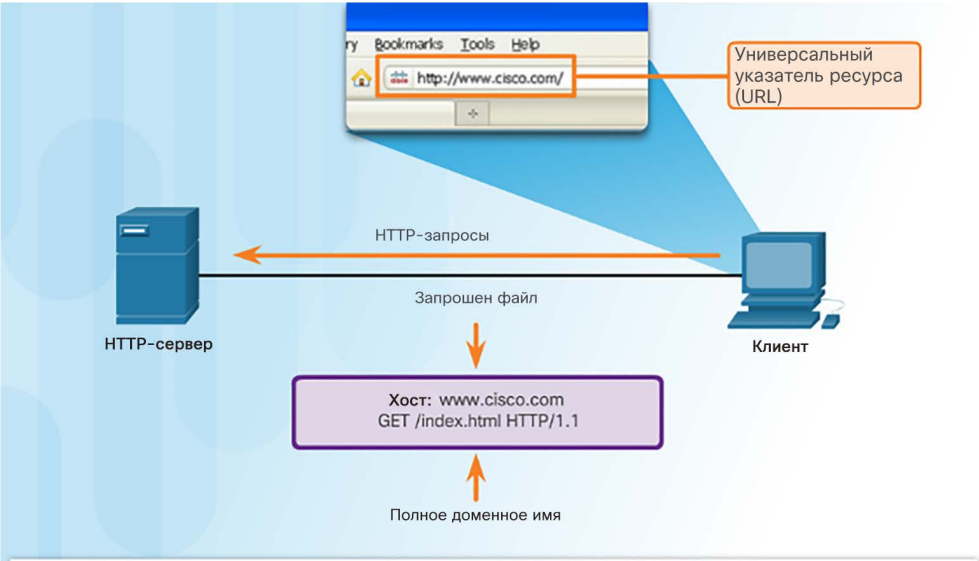




© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Протоколы HTTP и HTTPS

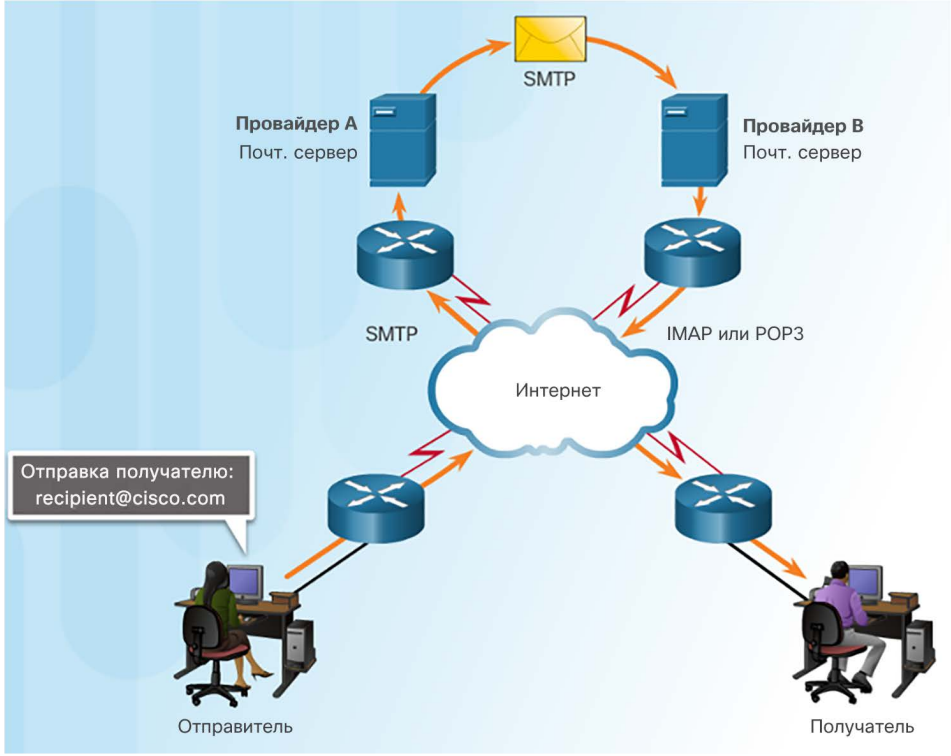
- Протокол HTTP основан на механизме «запрос-ответ».
- Есть три стандартных типа сообщений HTTP:
  - GET — это запрос данных клиентом.
  - POST — выгружает файлы данных на веб-сервер.
  - PUT — выгружает на веб-сервер ресурсы или содержимое.
- Протокол HTTP Secure (HTTPS) использует шифрование и аутентификацию для защиты данных.



При вводе http://www.cisco.com в адресной строке веб-обозревателя создается сообщение GET протокола HTTP.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Протоколы электронной почты

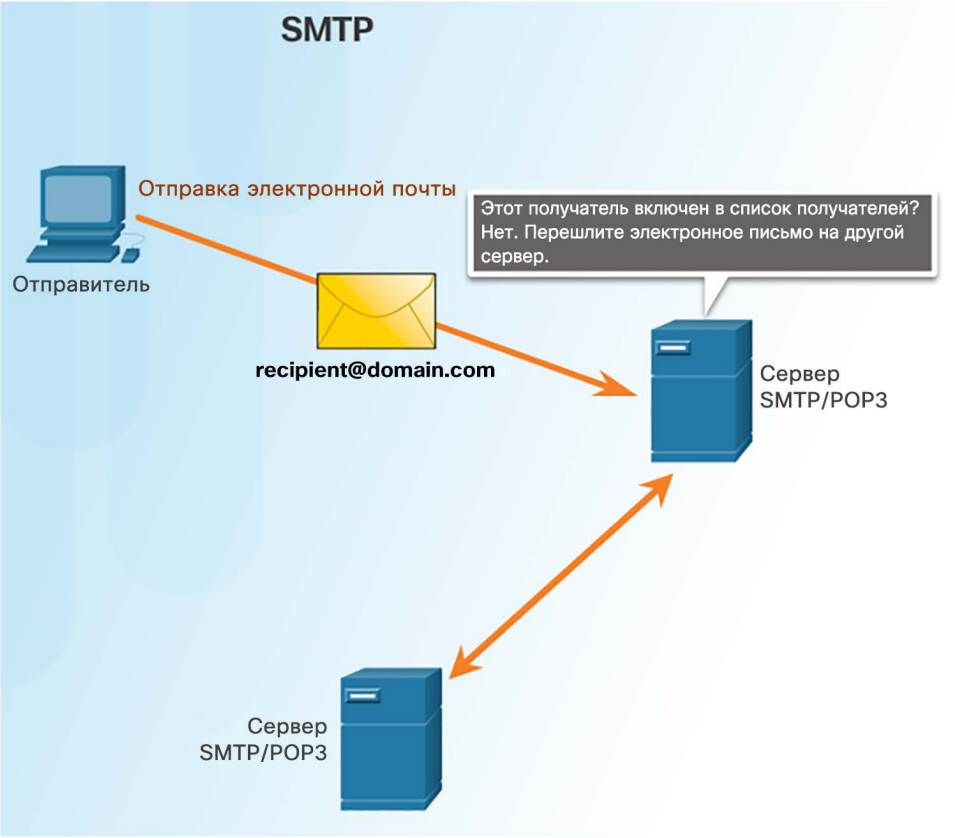


- Клиенты электронной почты для отправки и получения сообщений обращаются к серверам электронной почты.
- Серверы электронной почты взаимодействуют с другими серверами электронной почты для обмена сообщениями между доменами.
- Три протокола электронной почты:
  - Простой протокол электронной почты (SMTP) для отправки электронных писем.
  - Почтовый протокол (POP) для получения электронных писем.
  - Протокол доступа к сообщениям в сети Интернет (IMAP) для получения электронных писем.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

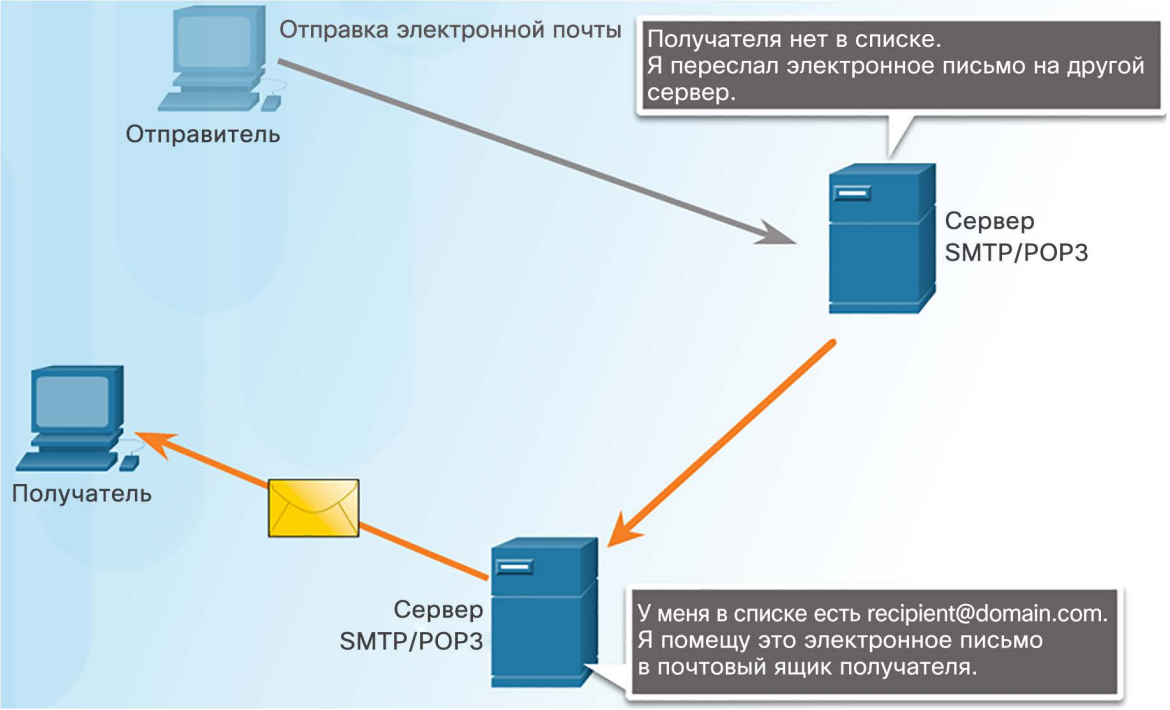
Принцип работы SMTP

- SMTP используется для отправки электронной почты



© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

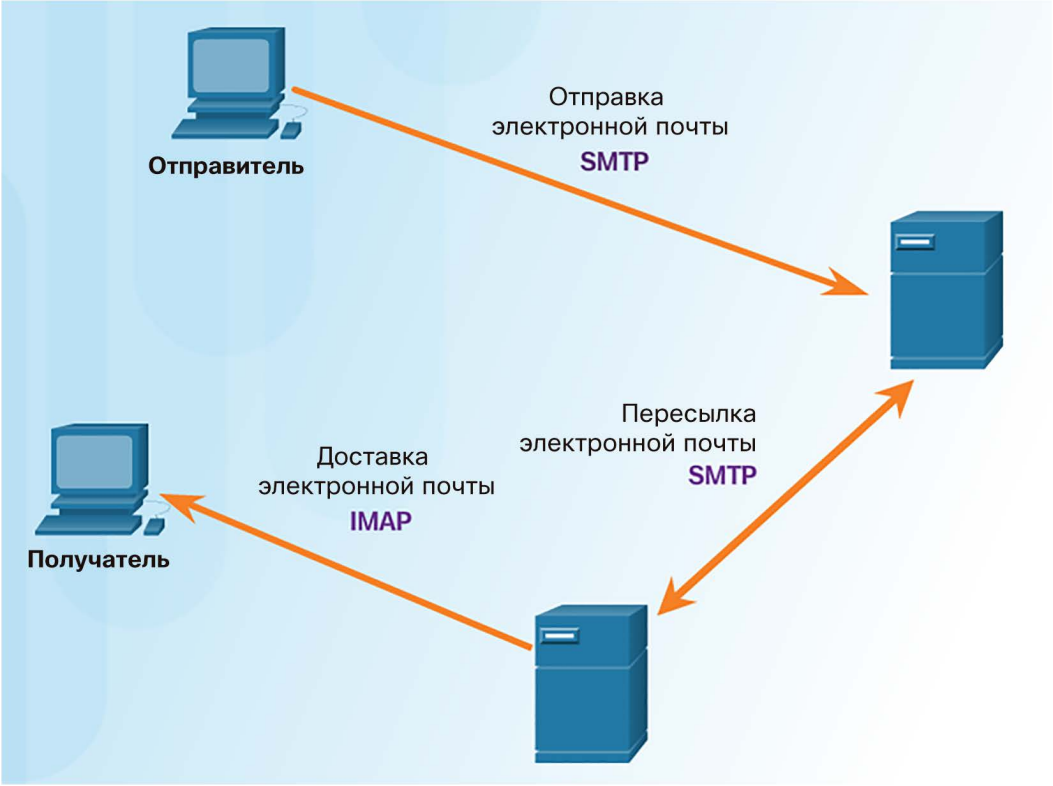
Принцип работы протокола POP



- Протокол POP используется для получения электронных писем от сервера электронной почты.
- Электронные письма загружаются с сервера на клиент и удаляются с сервера.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Принцип работы протокола IMAP



- Протокол IMAP используется для получения электронных писем от сервера электронной почты.
- Копии сообщений загружаются с сервера на клиент, а исходные сообщения хранятся на сервере.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

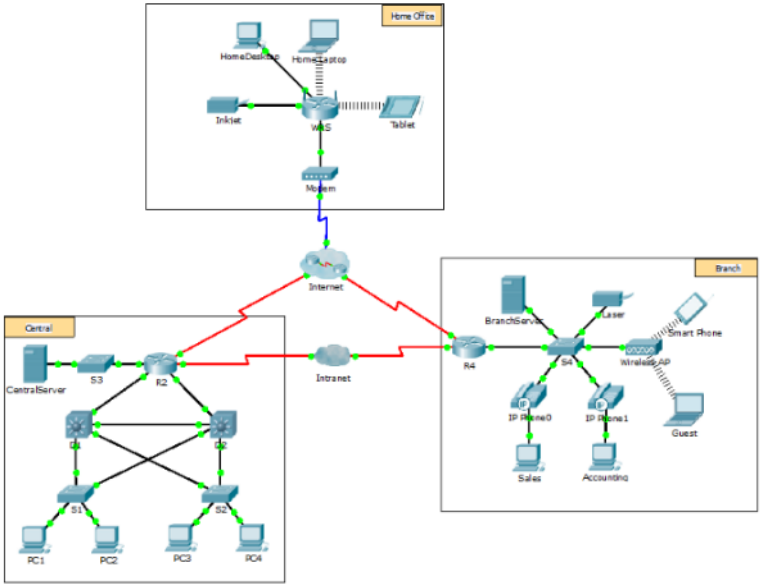
Packet Tracer. Интернет и электронная почта

Cisco Networking Academy®

Mind Wide Open™

Packet Tracer - Web and Email

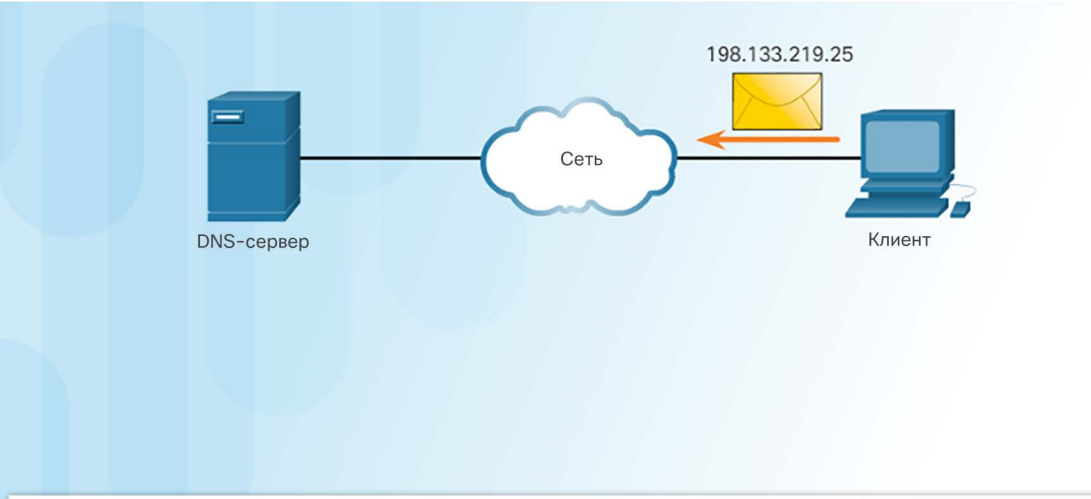
Topology



Objectives

Служба доменных имен

- Доменные имена преобразуют числовой адрес в простое и легко запоминаемое имя.
- Протокол DNS определяет автоматизированный сервис, который сопоставляет имена ресурсов с соответствующими числовыми сетевыми адресами.



Доменное имя преобразуется в числовой адрес соответствующего сетевого устройства по протоколу DNS.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Формат сообщений DNS

В службе DNS используется единый формат для:

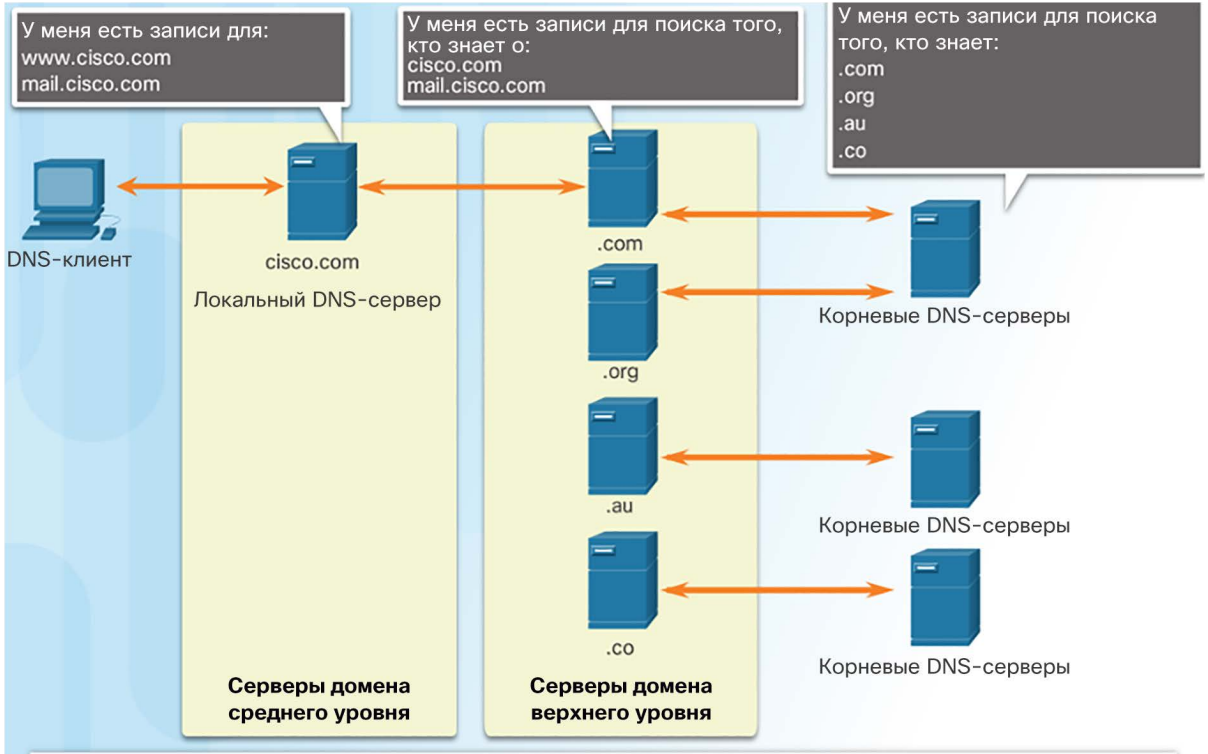
- Всех типов запросов клиента и ответов сервера
- Сообщений об ошибках
- Передачи сведений о записях ресурсов между серверами.

Заголовок	
Вопрос	Вопрос для сервера имен
Ответ	Записи ресурсов с ответом на вопрос
Полномочия	Записи ресурсов с информацией о полномочиях
Дополнительно	Записи ресурсов, содержащие дополнительные сведения

- Когда клиент обращается с запросом, процесс DNS-сервера сначала пытается разрешить запрошенное имя, просматривая свои записи.
- Если это не удается, данный процесс обращается к другим серверам, чтобы разрешить это имя.
- Сервер временно сохраняет запрошенный числовой адрес на случай повторного запроса этого же имени.
- На ПК с операционной системой Windows команда **ipconfig /displaydns** выводит на экран все записи DNS, сохраненные в кэше.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Иерархия DNS



Иерархия DNS-серверов содержит записи ресурсов, по которым имена сопоставляются с адресами.

Команда nslookup

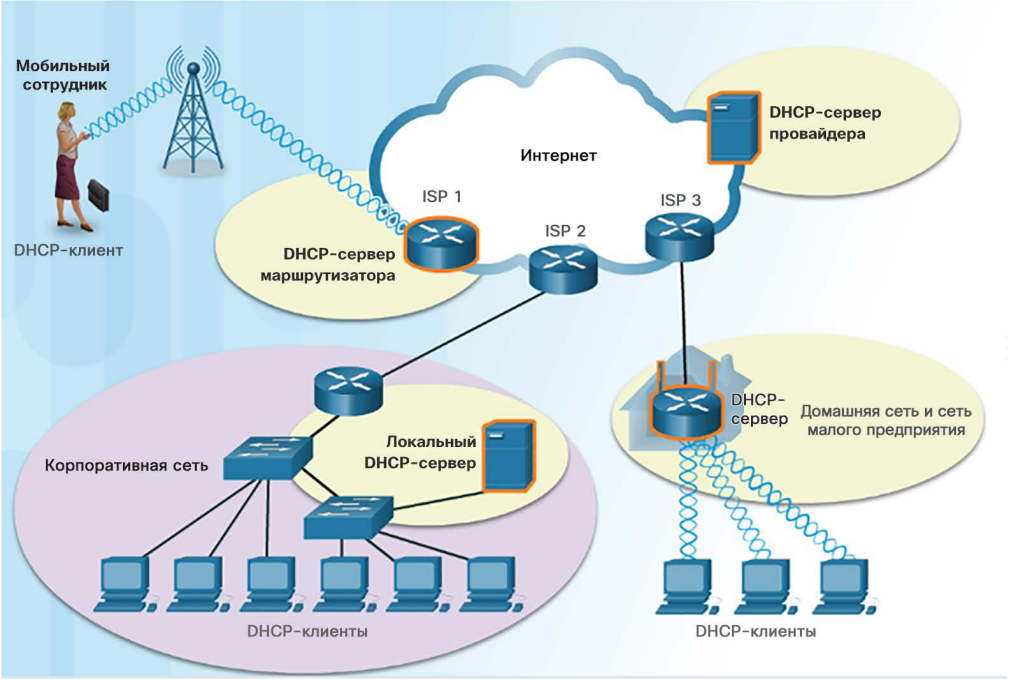
```
C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\bradfjoh>cd..

C:\Documents and Settings>nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183

> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183

Name:    www.cisco.com
Address:  198.133.219.25

> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183

Non-authoritative answer:
Name:    cisco.netacad.net
Address:  128.107.229.50

>
```

- Утилита **nslookup** позволяет пользователям вручную отправлять запросы серверам имен на преобразование конкретного имени хоста.
  - Ее также можно использовать для поиска и устранения неполадок с разрешением имен и проверки текущего состояния серверов имен.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

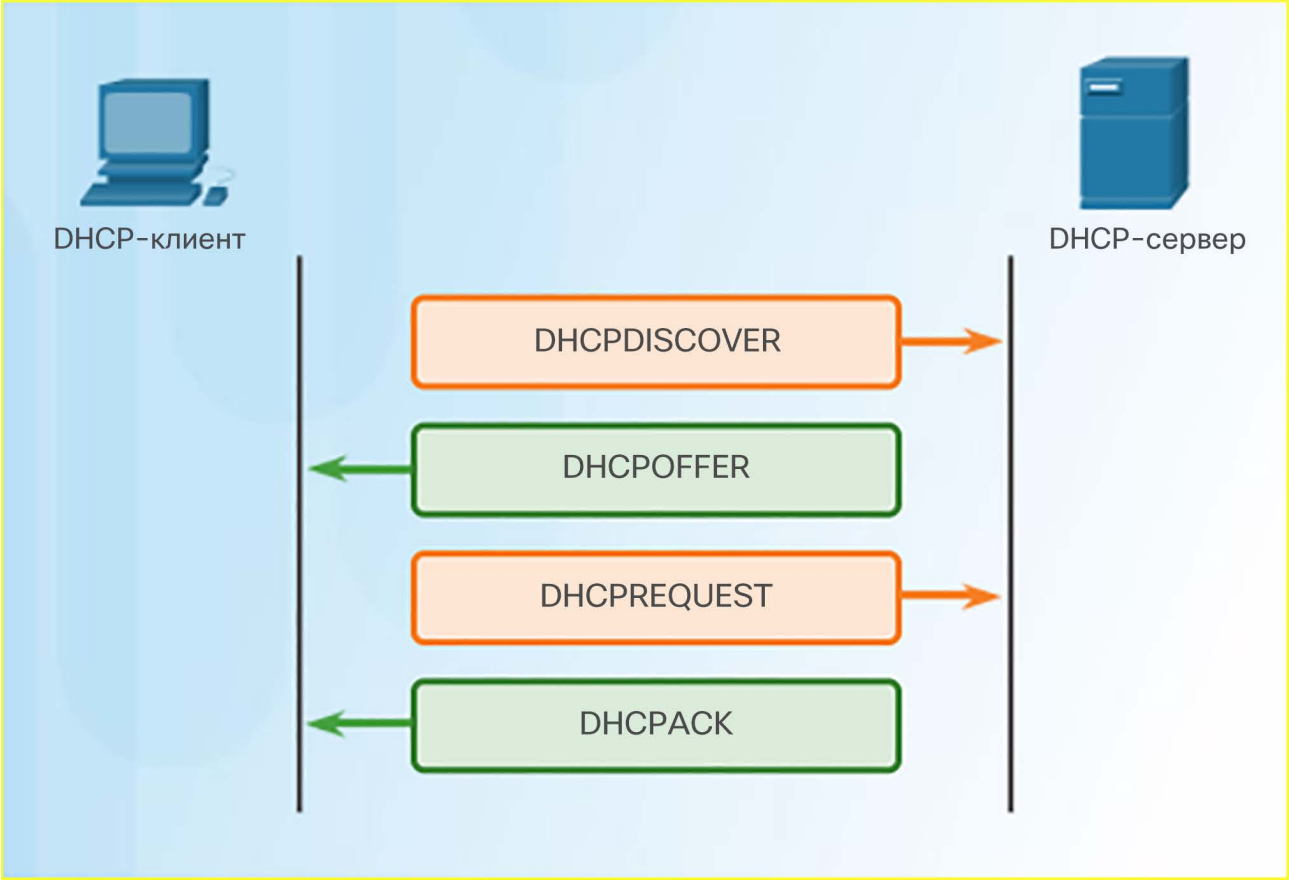
Протокол динамической настройки узлов (DHCP)

- Протокол динамической настройки узла (DHCP) для IPv4 автоматизирует назначение IPV4-адресов, масок подсети, шлюзов и других параметров IPv4.
- Назначенные DHCP адреса выдаются на определенный период времени, по истечении которого возвращаются в пул для повторного использования.
- Протокол DHCP обычно используется для устройств конечных пользователей. Статическая адресация применяется для сетевых устройств: шлюзов, коммутаторов, серверов и принтеров.
- DHCPv6 (DHCP для IPv6) предлагает аналогичные сервисы для клиентов IPv6.

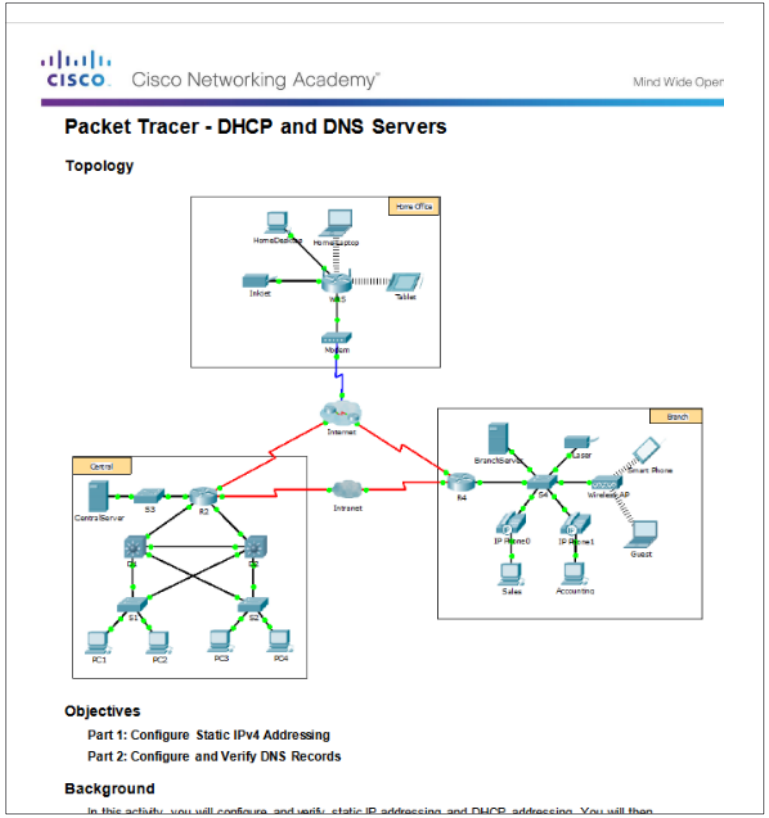


© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Принцип работы протокола DHCP



Packet Tracer. Серверы DHCP и DNS



Cisco Networking Academy

Mind Wide Oper

Packet Tracer - DHCP and DNS Servers

Topology

Home Office

Internet

Branch

Central

Intranet

Objectives

Part 1: Configure Static IPv4 Addressing

Part 2: Configure and Verify DNS Records

Background

In this activity, you will configure and verify, static IP addressing and DHCP addressing. You will then

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Лабораторная работа. Наблюдение за преобразование имен с помощью DNS

Cisco Networking Academy® Mind Wide Open™

Lab - Observing DNS Resolution

Objectives

Part 1: Observe the DNS Conversion of a URL to an IP Address

Part 2: Observe DNS Lookup Using the nslookup Command on a Web Site

Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers

Background / Scenario

The Domain Name System (DNS) is invoked when you type a Uniform Resource Locator (URL), such as http://www.cisco.com, into a web browser. The first part of the URL describes which protocol is used. Common protocols are Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), and File Transfer Protocol (FTP).

DNS uses the second part of the URL, which in this example is www.cisco.com. DNS translates the domain name (www.cisco.com) to an IP address to allow the source host to reach the destination host. In this lab, you will observe DNS in action and use the **nslookup** (name server lookup) command to obtain additional DNS information. Work with a partner to complete this lab.

Required Resources

1 PC (Windows 7 or 8 with Internet and command prompt access)

Part 1: Observe the DNS Conversion of a URL to an IP Address

a. Click the **Windows Start** button, type **cmd** into the search field, and press Enter. The command prompt window appears.

b. At the command prompt, ping the URL for the Internet Corporation for Assigned Names and Numbers (ICANN) at **www.icann.org**. ICANN coordinates the DNS, IP addresses, top-level domain name system management, and root server system management functions. The computer must translate www.icann.org into an IP address to know where to send the Internet Control Message Protocol (ICMP) packets.

The first line of the output displays www.icann.org converted to an IP address by DNS. You should be able to see the effect of DNS, even if your institution has a firewall that prevents pinging, or if the destination server has prevented you from pinging its web server.

Note: If the domain name is resolved to an IPv6 address, use the command **ping -4 www.icann.org** to translate into an IPv4 address if desired.

```
C:\>ping www.icann.org

Pinging www.vip.icann.org [192.0.32.7] with 32 bytes of data:
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=24ms TTL=246
Reply from 192.0.32.7: bytes=32 time=28ms TTL=246

Ping statistics for 192.0.32.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 28ms, Average = 24ms
```

Record the IP address of www.icann.org.

Все права защищены. Конфиденциальная информация Cisco

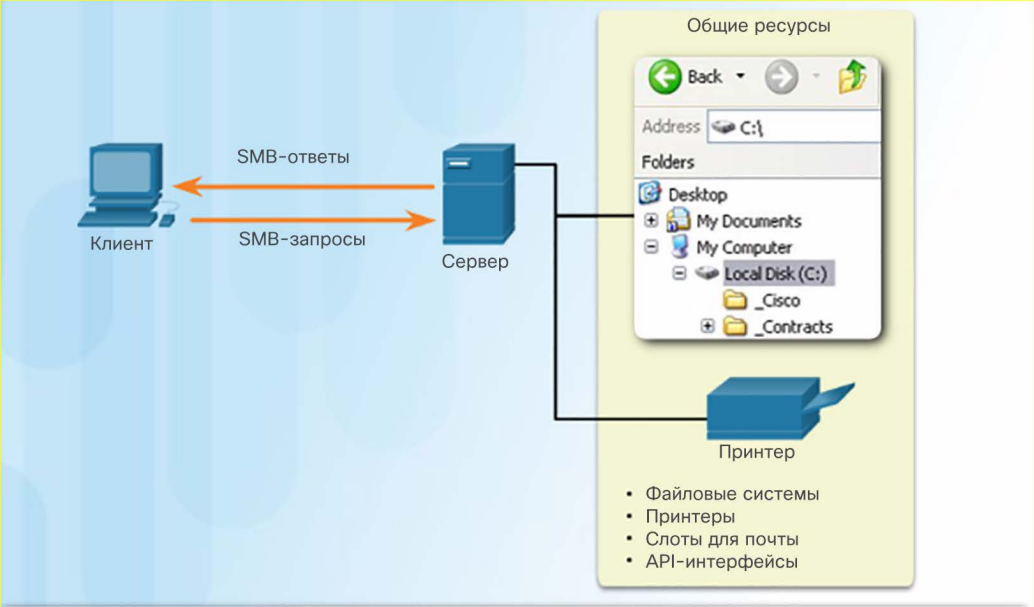
Протокол передачи файлов

- Для FTP требуется два подключения между клиентом с сервером: одно для команд и ответов, другое для передачи фактических данных.
  - Клиент устанавливает первое подключение к серверу для контроля трафика через TCP-порт 21.
  - Затем клиент устанавливает второе соединение с сервером для непосредственной передачи данных через порт 20 протокола TCP.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Протокол SMB

- Протокол SMB — это клиент-серверный протокол обмена файлами.
  - Общий доступ к файлам и сервисам печати на основе SMB является отличительной особенностью сетей Microsoft.
  - Клиенты устанавливают долговременное соединение с серверами и затем могут получать доступ к ресурсам на сервере аналогично доступу к ресурсам на клиентском хосте.



SMB – это протокол типа «запрос-ответ» для обмена данными между клиентом и сервером. Серверы могут предоставлять свои ресурсы клиентам в сети.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

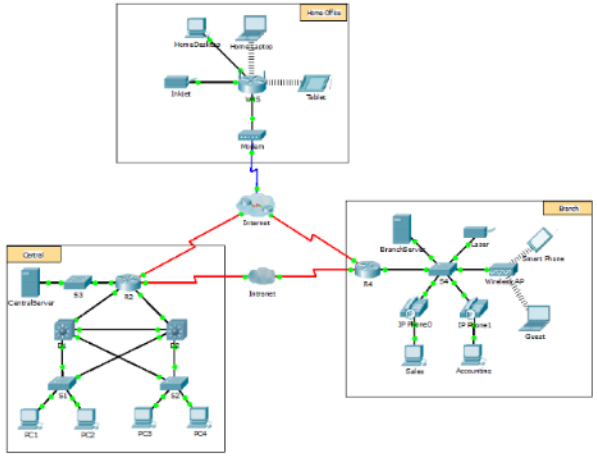
Packet Tracer. Протокол FTP

Cisco Networking Academy®

Mind Wide Open®

Packet Tracer - FTP Servers

Topology



Objectives

Part 1: Configure FTP Services on Servers

Part 2: Upload a File to the FTP Server

Part 3: Download a File from the FTP Server

Background

In this activity, you will configure FTP services. You will then use the FTP services to transfer files between clients and the server.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Лабораторная работа. Изучение протокола FTP

Cisco Networking Academy™ Mind Wide Open™

Lab - Exploring FTP

Objectives

Part 1: Use FTP from a Command Prompt

Part 2: Use FTP in a Browser

Part 3: Download an FTP File Using WS_FTP LE (Optional)

Background / Scenario

The File Transfer Protocol (FTP) is part of the TCP/IP suite. FTP is used to transfer files from one network device to another network device. Windows includes an FTP client application that you can execute from the command prompt. There are also free graphical user interface (GUI) versions of FTP that you can download. The GUI versions are easier to use than typing from a command prompt. FTP is frequently used for the transfer of files that may be too large to send using email.

When using FTP, one computer is normally the server and the other computer is the client. When accessing the server from the client, you need to provide a username and password. Some FTP servers have a user named **anonymous**. You can access these types of sites by simply typing "anonymous" for the user, without a password. Usually, the site administrator has files that can be copied but does not allow files to be posted with the anonymous user. Furthermore, FTP is not a secure protocol because the data is not encrypted during transmission.

In this lab, you will learn how to use anonymous FTP from the Windows command-line C:\> prompt. You will access an anonymous FTP server using your browser. Finally, you will use the GUI-based FTP program, WS_FTP LE.

Required Resources

1 PC (Windows 7 or 8 with access to the command prompt, Internet access, and WS_FTP LE installed (optional))

Part 1: Use FTP from a Command Prompt

a. Click the **Windows Start** button, type **cmd** in the search field, and press **Enter** to open a command window.

b. At the C:\> prompt type **ftp ftp.cdc.gov**. At the prompt that says **User (ftp.cdc.gov:(none)):** type **anonymous**. For the password, do not type anything. Press **Enter** to be logged in as an anonymous user.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User1>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

10.3. Обзор

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

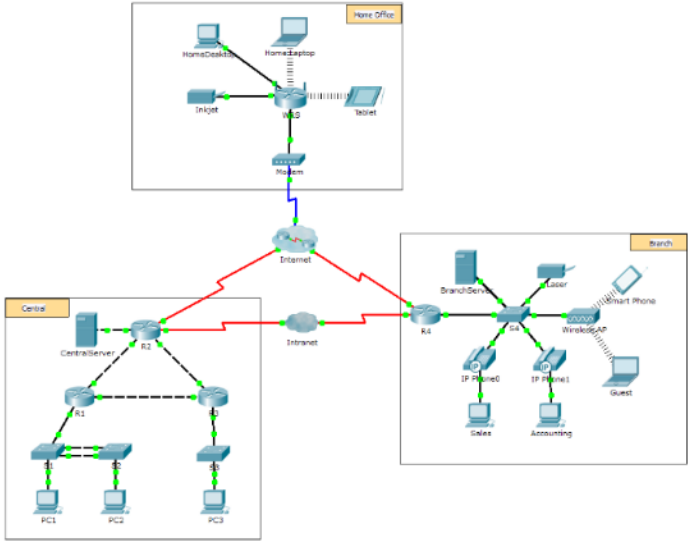
Packet Tracer. Изучение работы сети

Cisco Networking Academy®

Mind Wide Open™

Packet Tracer - Explore a Network

Topology



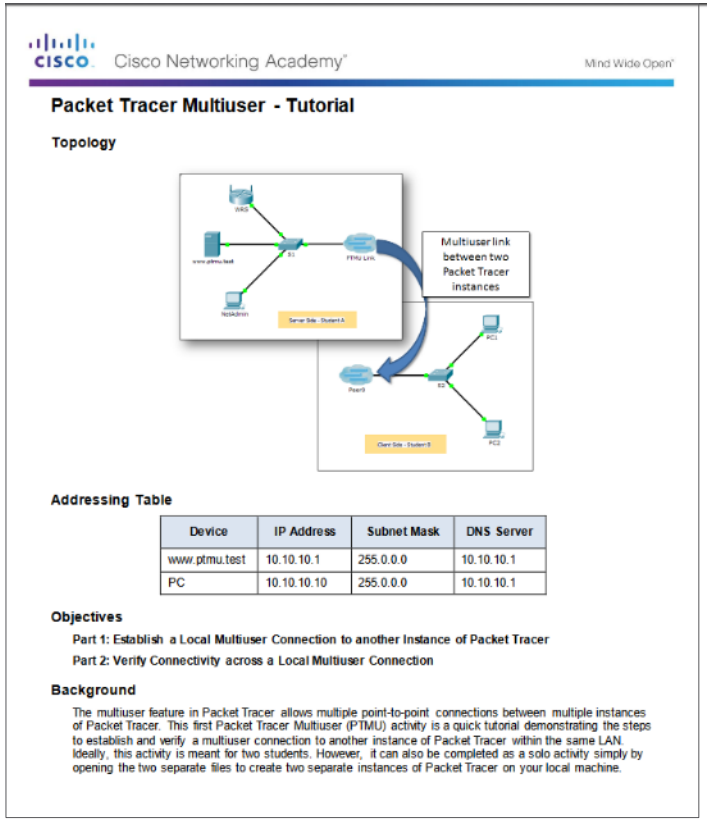
Objectives

Part 1: Examine Internetwork Traffic at Branch

Part 2: Examine Internetwork Traffic to Central

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Многопользовательский режим Packet Tracer. Краткое руководство



Cisco Networking Academy™ Mind Wide Open™

Packet Tracer Multiuser - Tutorial

Topology

Addressing Table

Device	IP Address	Subnet Mask	DNS Server
www.ptmu.test	10.10.10.1	255.0.0.0	10.10.10.1
PC	10.10.10.10	255.0.0.0	10.10.10.1

Objectives

Part 1: Establish a Local Multiuser Connection to another Instance of Packet Tracer

Part 2: Verify Connectivity across a Local Multiuser Connection

Background

The multiuser feature in Packet Tracer allows multiple point-to-point connections between multiple instances of Packet Tracer. This first Packet Tracer Multiuser (PTMU) activity is a quick tutorial demonstrating the steps to establish and verify a multiuser connection to another instance of Packet Tracer within the same LAN. Ideally, this activity is meant for two students. However, it can also be completed as a solo activity simply by opening the two separate files to create two separate instances of Packet Tracer on your local machine.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

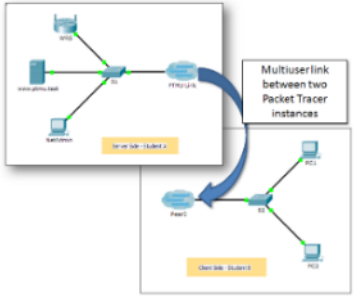
Многопользовательский режим Packet Tracer. Внедрение служб

Cisco Networking Academy®

Mind Wide Open®

Packet Tracer Multiuser - Implement Services

Topology



Addressing Table

Device	IP Address	Subnet Mask
Server Side Player		
WRS	172.16.1.254	255.255.255.0
S1	172.16.1.1	255.255.255.0
www.ptmu.test	172.16.1.5	255.255.255.0
NetAdmin	DHCP Assigned	DHCP Assigned
Client Side Player		
S2	172.16.1.2	255.255.255.0
PC1	DHCP Assigned	DHCP Assigned
PC2	DHCP Assigned	DHCP Assigned

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Заключение

Глава 10. Уровень приложений

- Объяснить, как на уровне приложений поддерживается работа приложений конечного пользователя.
- Объяснить, как работают общеизвестные протоколы уровня приложений TCP/IP.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Новые термины и команды

- протокол начальной загрузки (BOOTP)
- протокол SMTP
- протокол POP
- протокол доступа к сообщениям в Интернете (IMAP)
- протокол FTP
- простейший протокол передачи файлов (TFTP)
- клиент-сервер
- Протокол SMB

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

CISCO