Лекция 3

IT Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved.

Сетевая адресация

- Устройства, подключенные к сети, имеют два адреса, которые аналогичны отпечаткам пальцев человека и его почтовому адресу.
- Эти два типа адресов — **MAC-адрес** (сокращение от Media Access Control – управление доступом к среде передачи) и **IP-адрес**. MAC-адрес прошит на сетевой интерфейсной плате (NIC) производителем.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

IP-адреса

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

IP-адреса

- В начале 1990-х годов возникла обеспокоенность по поводу нехватки сетевых адресов IPv4.
- Инженерная группа по развитию Интернета (IETF) начала поиски альтернативных решений.
- Это привело к разработке решения, которое сейчас известно как протокол IP версии 6 (IPv6).
- В настоящее время адреса IPv6 используются параллельно с адресами IPv4 и уже начинают их вытеснять.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Формат адреса IPv4

- IPv4-адрес состоит из 2 частей. Первая идентифицирует сеть. Вторая — узел в этой сети. Обе части являются обязательными.
- Когда компьютер подготавливает данные к отправке по сети, он должен определить, следует ли отправлять данные непосредственно получателю, которому они предназначены, или на маршрутизатор. Он отправит данные непосредственно получателю, если получатель находится в одной сети с ним. В противном случае он отправит данные на маршрутизатор. Маршрутизатор использует сетевую часть IP-адреса для маршрутизации трафика между различными сетями.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Маска подсети

	Сетевая часть		Узловая часть
192.168.200.8	11000000.10101000.11001000	.	00001000
255.255.255.0	11111111.11111111.11111111	.	00000000
192.168.200.0	11000000.10101000.11001000	.	00000000

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Классовая и бесклассовая адресация IPv4

Маска подсети	Двоичное представление	Префикс
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Форматы адресов IPv6

- Длина IPv6-адресов составляет 128 бит, написанных в виде строки шестнадцатеричных значений. Каждые 4 бита представляются одной шестнадцатеричной цифрой, образуя 32 шестнадцатеричных значения. **2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d** полностью развернутые адреса IPv6.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Статическая адресация

- В сети с небольшим числом узлов можно легко настроить нужные IP-адреса для каждого устройства вручную. Адреса должен назначать сетевой администратор, разбирающийся в методах IP-адресации и умеющий выбирать корректный адрес для каждой сети. Назначаемый IP-адрес должен быть уникален для каждого узла в одной сети или подсети. Этот метод называется статической IP-адресацией.

Динамическая адресация

Если к локальной сети подключено большое число компьютеров, настройка IP-адресов для каждого узла вручную может занимать много времени и часто связана с ошибками. Сервер DHCP автоматически назначает IP-адреса, что упрощает процесс адресации. Автоматическая настройка некоторых параметров TCP/IP также снижает риск назначения дублированных или недопустимых IP-адресов.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Динамическая адресация

После загрузки компьютер непрерывно запрашивает IP-адрес от сервера DHCP, пока не получит его. Если компьютеру не удается связаться с сервером DHCP для получения IP-адреса, ОС Windows назначает автоматический частный IP-адрес (APIPA). Это адрес типа link-local (адрес для использования в пределах локального сегмента сети), он находится в диапазоне от 169.254.0.0 до 169.254.255.255. Термин link-local означает, что компьютер может обмениваться данными только с компьютерами, подключенными к той же сети в том же диапазоне IP-адресов.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

ICMP

Протокол ICMP используется устройствами в сети для отправки на компьютеры и серверы управляющих сообщений и сообщений об ошибках. Существует несколько способов использования ICMP, например: объявление об ошибках сети, объявление о перегрузке сети и устранение неисправностей.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Роль транспортного уровня

Транспортный уровень отвечает за установление временного сеанса связи и передачу данных между двумя приложениями Как показано на рисунке, транспортный уровень — это канал между уровнем приложений и нижними уровнями, которые отвечают за передачу данных по сети.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Функции транспортного уровня

Отслеживание сеансов связи между приложениями. Устройство может отслеживать несколько приложений, использующих сеть одновременно.

Сегментирование данных и их последующая сборка. Отправляющее устройство разделяет данные приложений на блоки подходящего размера. Принимающее устройство собирает сегменты в данные приложения.

Идентификация приложений. Чтобы переслать потоки данных соответствующим приложениям, транспортному уровню необходимо определить целевое приложение. Для этого транспортный уровень присваивает каждому приложению отдельный идентификатор — номер порта.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Протоколы транспортного уровня

Передача с использованием **TCP** аналогична отправке пакетов с трекингом, путь которых отслеживается от отправителя до получателя. Если заказ разбит на несколько частей, заказчик может зайти на веб-сайт транспортной компании и посмотреть порядок доставки.
TCP использует следующие три основные операции для обеспечения надежности:
Отслеживание количества сегментов, отправленных на то или иное устройство тем или иным приложением.

Подтверждение полученных данных.

Повторная передача сегментов с неподтвержденными данными по истечении определенного времени ожидания.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Протоколы транспортного уровня

Работу протокола **UDP** можно сравнить с отправкой по почте обычного, не заказного, письма. Отправитель не знает, сможет ли адресат получить письмо, а почтовое отделение не несет ответственность за отслеживание письма или информирование отправителя о том, доставлено ли письмо по адресу.

Он обеспечивает только основные функции для обмена сегментами данных между приложениями. При этом данный протокол отличается незначительными накладными расходами и практически отсутствием проверки данных. UDP известен как протокол негарантированной доставки данных. Применительно к компьютерным сетям негарантированная доставка считается ненадежной, поскольку при этом отсутствует подтверждение о получении отправленных данных на узле назначения.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Номера портов

В протоколах TCP и UDP используются номера портов источника и назначения для отслеживания сеансов связи между приложениями. **Номер порта источника связан с отправляющим приложением на локальном устройстве. Номер порта назначения связан с приложением назначения на удаленном устройстве.** Например, при использовании веб-браузера, можно открыть несколько вкладок одновременно. Номера портов назначения — 80 для обычного веб-трафика и 443 для защищенного веб-трафика. Однако порты источника будут разными для каждой открытой вкладки. Благодаря этому компьютер узнает, на какую вкладку браузера доставлять веб-содержимое. Аналогично, другие сетевые приложения, такие как электронная почта и передача файлов, имеют собственные номера портов. Список общеизвестных номеров портов показан на рисунке.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential