Владивостокский государственный университет экономики и сервиса
Институт информатики инноваций и бизнес систем

Предмет:
«Технологии Интернет»

Руководитель: Сачко Максим Анатольевич, старший преподаватель

Тема 1

Стек протоколов TCP/IP

Содержание:

Стек протоколов TCP/IP

TCP/IP - набор средств низкого уровня, которые обеспечивают передачу данных между компьютерами через Интернет.

Сервисы Интернет и прикладные программы, которые изучаются в настоящем курсе, пользуются TCP/IP для взаимодействия между собой - аналогично как люди пользуются телефонной сетью.

1. Уровни стека TCP/IP

TCP/IP устроен в виде многоуровневой системы, где каждый уровень выполняет свою функцию по обеспечению передачи данных между компьютерами. Детали работы каждого уровня скрыты от других уровней; каждый уровень взаимодействует только со своими соседними уровнями сверху и снизу.

Особенности TCP/IP

- открытые стандарты протоколов, разрабатываемые независимо от программного и аппаратного обеспечения;
- независимость от физической среды передачи;
- система адресации, позволяющая уникально идентифицировать каждый компьютер в Интернет;
- стандартизованные протоколы прикладного уровня, реализующие сервисы Интернет.

Стек протоколов TCP/IP

Network Access Layer

Функции:

- отображение IP-адресов в физические адреса сети (MAC-адреса);
- инкапсуляция IP-дейтаграмм (datagrams) в кадры (frames) для передачи по физическому каналу и передача кадров;

На этом уровне работает протокол ARP, осуществляющий отображение адресов IP->MAC.

Функции протокола IP в Internet Layer

- определение дейтаграммы - основного блока передачи данных в Интернет;
- определение схемы адресации в Интернет;
- передвижение данных между транспортным уровнем и уровнем доступа к среде передачи;
- маршрутизация дейтаграмм;
- фрагментация дейтаграмм на границе сред с различными размерами блока передаваемых данных и сборка фрагментированных дейтаграмм в месте назначения.

2. Протокол ICMP

Вторым важным протоколом межсетевого уровня является протокол управляющих сообщений Интернет — **ICMP** *(Internet Control Message Protocol)*, являющийся неотъемлемой частью модуля IP.

Протокол ICMP доставляет диагностические и управляющие сообщения от одного IP-адреса к другому. Сообщения делятся на типы, определяемые номерами, внутри типов сообщения идентифицируются числовыми кодами или именами.

Примеры сообщений ICMP

Source Quench (4) - слишком быстрое прибытие дейтаграмм; отправляется узлом назначения на узел-источник, если первый не успевает обрабатывать поступающие данные.

Destination Unreachable (3) - узел назначения недоступен.

Redirect (5) - изменить маршрут; отправляется маршрутизатором при необходимости использовать другой маршрут.

Echo (8,0) - эхо; используется программой ping.

Transport Layer

Протоколы транспортного уровня обеспечивают прозрачную доставку данных *(end-to-end delivery service)* между двумя процессами. Процесс внутри хоста идентифицируется номером, который называется номером порта. Таким образом, роль адреса на транспортном уровне выполняет номер порта.

Совокупность IP-адреса и номера порта называется **сокетом** *(socket).* Как IP адрес уникально определяет в Интернет IP-интерфейс *(хост),* сокет уникально идентифицирует в Сети конкретный процесс.

3. Протокол UDP

UDP (User Datagram Protocol, протокол пользовательских дейтаграмм) является *ненадежным* протоколом *без установления соединения*.

UDP получает от прикладного процесса данные для пересылки в виде отдельных несвязанных сообщений, снабжает их минимальным заголовком, в котором указываются номера портов отправителя и получателя и передает пакет на уровень IP.

Прикладные процессы на основе UDP

NFS (Network File System - сетевая файловая система),

TFTP (Trivial File Transfer Protocol - простой протокол передачи файлов),

SNMP (Simple Network Management Protocol - простой протокол управления сетью),

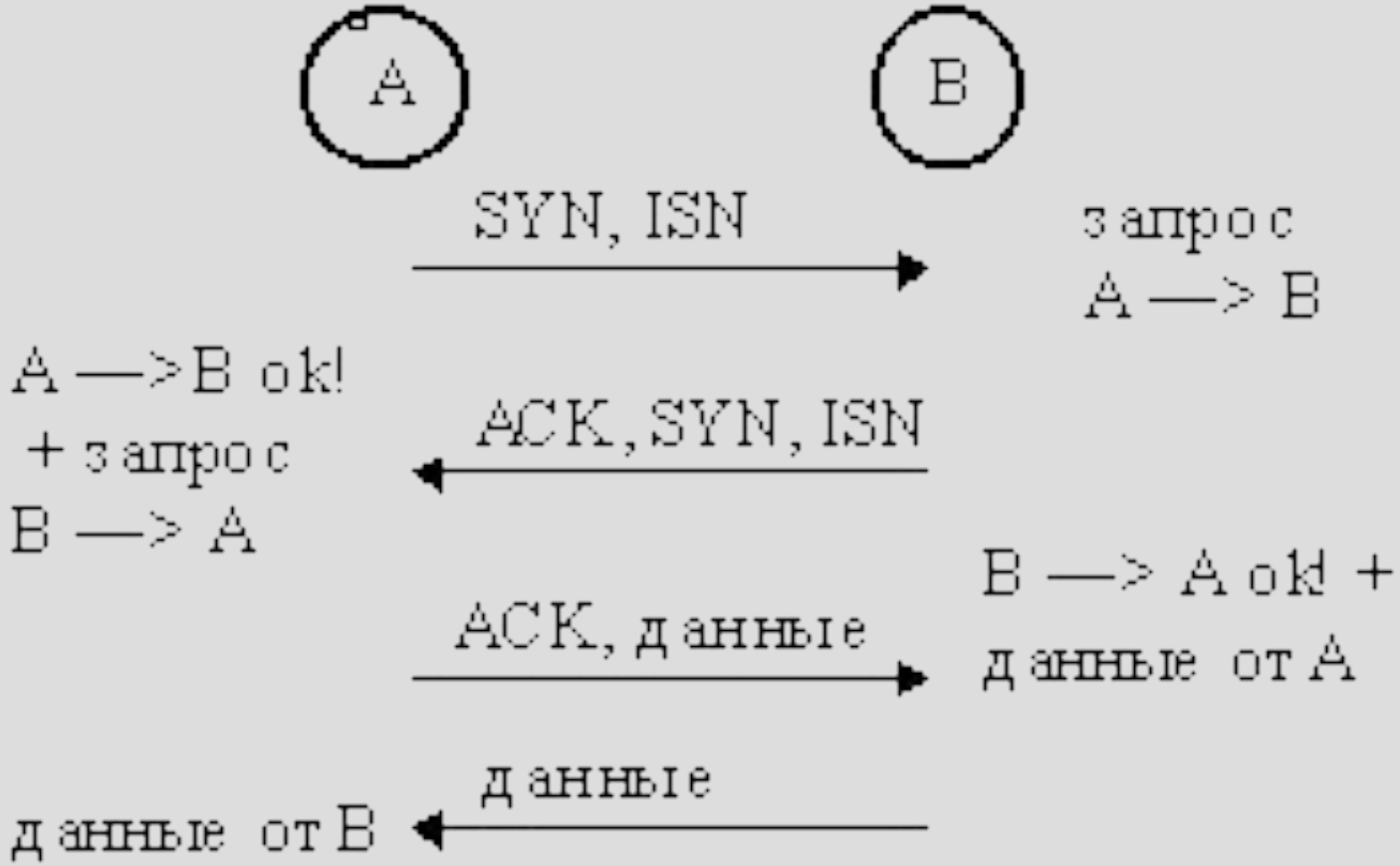
DNS (Domain Name Service - доменная служба имен).

3. Протокол TCP

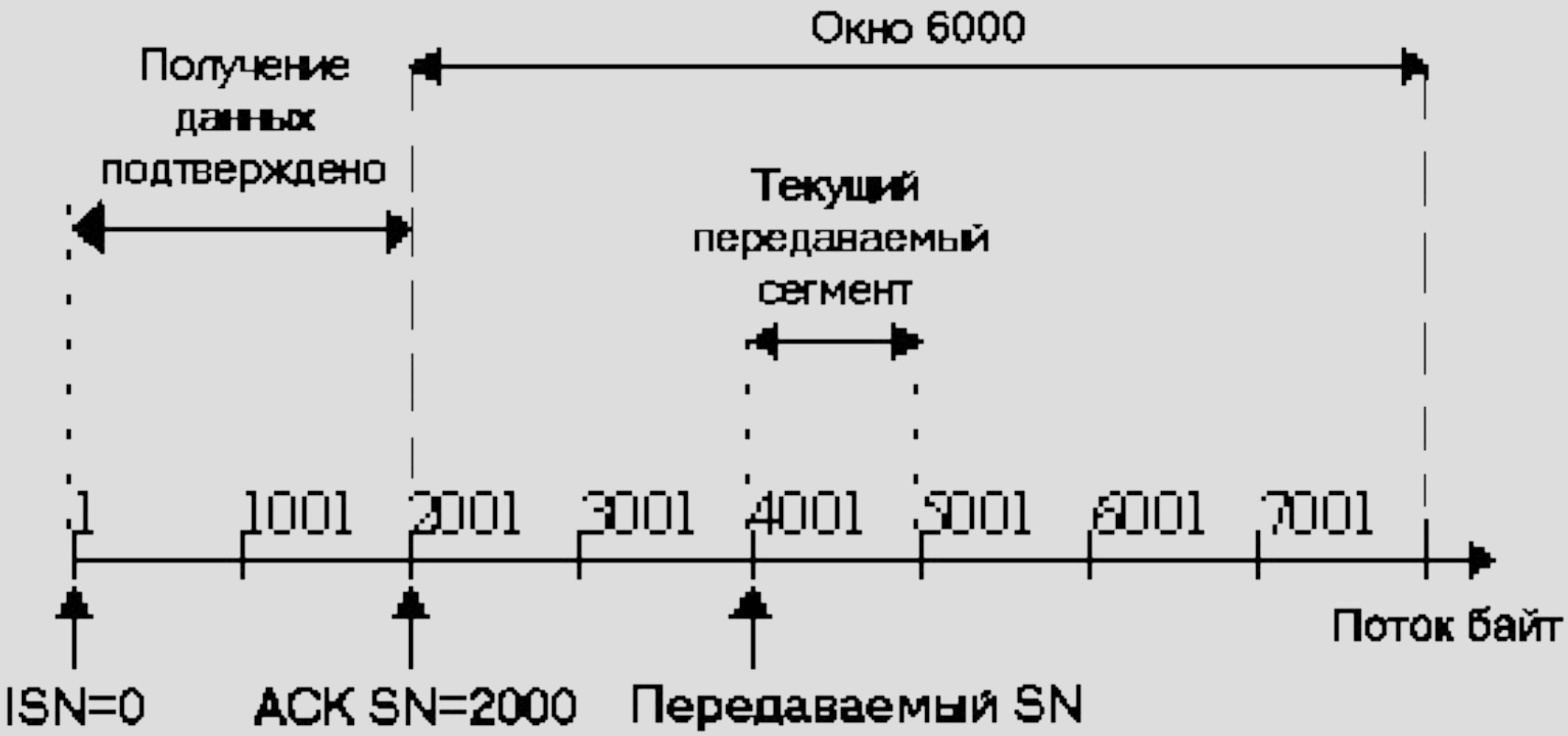
TCP (Transmission Control Protocol - протокол контроля передачи) - *надежный* байт-ориентированный (byte-stream) протокол *с установлением соединения*.

Протокол TCP осуществляет передачу данных, получаемых от прикладного процесса. Поток данных разбивается модулем TCP на сегменты. Передача сегментов осуществляется между сокетами с предварительным выполнением диалоговой процедуры установления соединения и с контролем успешной доставки сегментов в процессе пересылки.

Установка TCP-соединения



Метод скользящего окна



IP-адресация

Каждому узлу Интернет (точнее, каждому IP-интерфейсу) присваивается уникальный 32-битный адрес, состоящий из адреса сети, в которой находится компьютер, и номера компьютера в этой сети. Сетевая маска (32 бита) позволяет отделить адрес сети от номера компьютера. В каждой сети определяется широковещательный адрес ("всем узлам этой сети").

IP-адрес - 32-битный идентификатор IP-интерфейса, состоящий из адреса сети и номера хоста. Местоположение границы между двумя частями адреса может быть различным в разных адресах и определяется разными способами в классовой и бесклассовой модели.

Например, адрес

10100000010100010000010110000011

записывается как

10100000.01010001.00000101.10000011

=

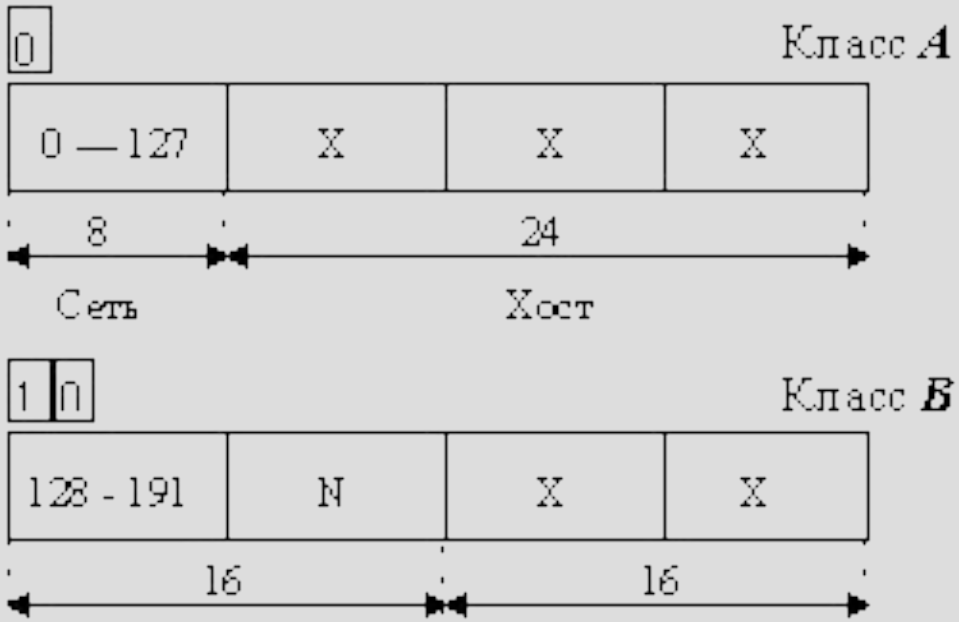
160.81.5.131

6. Классовая и бесклассовая адресация

Классовая адресация - способ построения адреса, когда граница между адресом сети и номером хоста в IP-адресе проходит по границе октета (между битами 7 и 8, или 15 и 16, или 23 и 24), при этом местоположение этой границы определяется значением страшего октета.

Бесклассовая адресация (CIDR) - способ построения адреса, граница между адресом сети и номером хоста в IP-адресе проходит в произвольном месте. Местоположение границы определяется сетевой маской, которая в этом случае прилагается к IP-адресу.

Классы IP-адресов



Запись адресов в бесклассовой модели

Для удобства записи IP-адрес в модели CIDR часто представляется в виде a.b.c.d / n, где a.b.c.d — IP адрес, n — количество бит в сетевой части.

Пример: **137.158.128.0/17**

Маска сети для этого адреса: 17 единиц (сетевая часть), за ними 15 нулей (хостовая часть), что в октетном представлении равно

11111111.11111111.10000000.00000000 =

255.255.128.0.

Пример

IP = 205.37.193.134/26

IP = 205.37.193.134 netmask = 255.255.255.192

в двоичном виде:

IP = 11001101 00100101 11000111 10000110

маска = 11111111 11111111 11111111 11000000

network = 11001101 00100101 11000111 11000000

Вопросы для самопроверки:

1. Опишите функции слоев стека TCP/IP и их взаимосвязь.
2. Что такое маска сети?
3. В чем состоит сущность процесса IP-маршрутизации?
4. Каковы задачи протокола IP? TCP? В чем их отличие друг от друга?
5. Каковы недостатки протокола IP? Подходы к их решению.
6. Каковы недостатки протокола TCP? Подходы к их решению.
7. Как приложение взаимодействует со стеком TCP/IP?

Рекомендуемая литература:

1. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб: "Питер", 2005.
2. К. Хант. Персональные компьютеры в сетях TCP/IP: Руководство администратора сети/ Пер. с англ. – СПб.: ЗАО "ЭлектроникаБизнесИнформатика", Киев: "BHV", 2003.
3. Золотов С. Протоколы Internet: Руководство для профессионалов. – СПб.: BHV-СПб, 2004.

- **Использование материалов презентации**

- Использование данной презентации, может осуществляться только при условии соблюдения требований законов РФ об авторском праве и интеллектуальной собственности, а также с учетом требований настоящего Заявления.

- Презентация является собственностью авторов. Разрешается распечатывать копию любой части презентации для личного некоммерческого использования, однако не допускается распечатывать какую-либо часть презентации с любой иной целью или по каким-либо причинам вносить изменения в любую часть презентации. Использование любой части презентации в другом произведении, как в печатной, электронной, так и иной форме, а также использование любой части презентации в другой презентации посредством ссылки или иным образом допускается только после получения письменного согласия авторов.