Занятие 17.

Тема: **Сетевое администрирование Linux. Протокол TCP. Занятие первое.**

Вид занятия: лекция, практическое занятие.

Учебные вопросы:

1. Структура полного адреса в протоколе TCP. Понятие TCP-соединения. Структура TCP-пакета.
2. Распространенные TCP-сервисы.
3. Telnet: xinetd, in.telnetd. SSH: sshd.

Время: 90 минут

Литература:

1. Cysco systems и др. - Руководство по технологиям объеденненных сетей, 3-е издание. : Пер. с англ. - М. : Издательский дом “Вильямс”, 2002. - 1040 с. : ил. - парал. тит. англ.

2. Кирх. О, Доусон Т. - Linux для профессионалов. Руководство администратора сети, второе издание. - СПб.: Питер, 2001. - 496 с.; ил.

Ход занятия.

1. TCP (Trasmission Control Protocol, протокол управления передачей) обеспечивает надежную передачу данных в среде IP. TCP относится к транспортному уровню OSI. Этот протокол предоставляет такие услуги как потоковая передача данных, надежность, эффективное управление потоком, дуплексный режим.

Формат пакета TCP:

<---------- 32 бита ---------->

Порт источника			Порт приемника
Порядковый номер			
Номер подтверждения			
Сдвиг данных	Резервные	Флаги	Окно
Контрольная сумма			Указатель срочности
Параметры			
Данные			

Порт источника и порт приемника – точки, в которых процессы верхнего уровня принимают услуги TCP.

Порядковый номер – Обычно номер первого байта в сообщении. Может также использоваться для обозначения исходного порядкового номера в передаче.

Номер подтверждения – порядковый номер следующего байта данных, который ожидает получить приемник.

Сдвиг данных – Число 32-разрадных слов в заголовке TCP.

Резервные – Область, зарезервированная для использования в будущем.

Флаги – Различная управляющая информация, в том числе биты SYN, ACK и FIN.

Окно – Размер приемного окна (буфера памяти) приемника.

Контрольная сумма – Показывает, не был ли заголовок поврежден при передаче.

Указатель срочности – Указывает на первый байт срочных данных в пакете.

Параметры – Различные дополнительные параметры TCP.

Данные – Информация верхнего уровня.

В протоколе TCP принято понятие ***потока –*** последовательности битов переменной длины, передающихся между двумя объектами. Именно поток является единой и неделимой частью TCP-соединения. Одним словом, понимать под одним целым необходимо связку IP:TCPпорт-IP2:TCPпорт2, а не IP:TCPпорт, как в протоколе UDP. Это обозначает, что несколько клиентов могут одновременно работать с одной службой на одном сервере и одном порту, так как IP1:TCPпорт1-IP2:TCPпорт2 и IP1:TCPпорт1-IP3:TCPпорт3, будут различными потоками, не пересекающимися друг с другом.

Установка соединения в протоколе TCP происходит по механизму *трёхэтапной синхронизации (three-way handshake).* Этот механизм синхронизирует обе стороны, позволяя им согласовать начальные порядковые номера. Он также обеспечивает готовность сторон к приему/передаче, чтобы избежать передачи лишних пакетов при установке и после разрыва соединения.

Первых хост (А) открывает соединение, посылая второму хосту (Б) пакет с начальным номером соединения и установленным флагом SYN. Хост Б получает SYN-пакет, записывает номер (X) отвечает пакетом с порядковым номером X+1 и установленными битами SYN и ACK. Также хост Б указывает номер подтверждения (Y). Если этот номер равен, например, 40, то это означает что хост принял 39 байт и ожидает 40-й байт. Эта технология называется подтверждением передачи данных. Затем хост А подтверждает прием всех байтов, посланных хостом Б, указывая номер подтверждения Y+1 и устанавливая флаг ACK. Только после этого начинается передача данных.

Протокол TCP обеспечивает надежную передачу данных за счет следующей технологии: если после отправки пакета через заданный промежуток времени (таймаут) не придет подтверждения передачи (пакета с установленным флагом ACK), то пакет будет отправлен снова. Эта технология называется ***подтверждением приема и повторной передачей (Positive Acknowledgment and Retransmission, PAR).***

Присваивая каждому пакету порядковый номер, PAR позволяет хостам отслеживать пакеты, потерянные или дублированные вследствие сетевых задержек или сбоев.

Скользящее окно TCP позволяет использовать пропускную способность сети более эффективно, поскольку с его помощью хосты могут отправлять несколько пакетов не дожидаясь подтверждения. Окно измеряется в байтах, которые может послать отправитель во время ожидания подтверждения передачи данных. Размер окна определяется во время установки соединения, но может изменяться во время передачи. Если размер окна равен 0, то передача данных запрещена.

Предположим, что TCP-отправителю надо переслать с помощью скользящего окна последовательность байт (пронумерованных от 1 до 10) получателю с размером окна 5. Отправитель помещает в окно первые 5 байт, передает и ждет подтверждения. После того, как он получит пакет с флагом ACK и номером подтверждения, равным 6, то отправитель передает байты с 6 по 10. Получатель отправляет ACK с номером подтверждения равным 11, и указывает что размер окна равен 0. В этом случае отправитель будет ожидать пакета ACK с номером подтверждения 11 и ненулевым размером окна перед началом передачи.

2. Распространенные TCP-сервисы, это практически все, что средний пользователь знает сегодня об интернет:

WWW (World Wide Web, всемирная паутина) – самый распространенный сервис в Интернет, построенный на протоколе уровня приложений HTTP. Использует порт TCP80.

FTP (File Tranfer Protocol – протокол передачи файлов) – используется для передачи фало по сети и организации интернет-файлархивов. Использует порты TCP20-21

SMTP (Simple Mail Tranfer Protocol – простой протокол передачи почты) – используется для отправки сообщений локального пользователя и передачи электронной почты между серверами. Работает на порту TCP25.

POP3 (Post Office Protocol v.3 – Протокол офисной почты версии 3) – используется для получения почты конечными пользователями. Использует порт TCP110

IRC (Internet Relayed Chat – Разговор через интернет в реальном времени) – чат-протокол, один из самых распространенных сервисов в интернет. Использует порты TCP194, TCP6660-6667.

3. Немного подробнее хотелось бы поговорить о нескольких сервисах интерактивного доступа на базе TCP, и о структуре запуска интернет-сервисов в Linux. На сегодняшний день широко распространены 3 сервиса интерактивного доступа к командной строке: RSH (Remote SHell - удаленная оболочка), Telnet и SSH (Secure SHell – защищенная оболочка). SSH является развитием RSH. Протоколы очень похожи, за исключением того, что в SSH принято шифрование как пароля и имени пользователя, так и передаваемых данных, что позволило ему практически повсеместно вытеснить RSH. Сервисы RSH и SSH – это Unix-ориентированные протоколы, которые сравнительно редко встречаются в других системах. В отличие от них сервис Telnet применяется на многих платформах, в том числе и на Windows.

В большинстве случаев TCP-службы в Linux работают как демоны и сами осуществляют передачу данных по сети. Однако в некоторых случаях используется демон интернет xinetd, который обеспечивает работу по сети, а программы, функционирущие с ним обмениваются данными по каналам, образованным дескрипторами файлов 0 (стандартный ввод), 1 (стандартный вывод) и 2 (стандартный поток ошибок). Обычно, сервичы, работающие с xinetd имеют в своем имени приставку in. Так, например, файл службы Telnet называется in.telnetd.