Лабораторная работа № 1
Программные средства анализа сетей с коммутацией пакетов. Анализатор пакетов Ethereal

Цель работы: анализ работы локальной сети с использованием программного пакета Ethereal.

Средства мониторинга и анализа

Процесс контроля работы сети обычно делят на два этапа – мониторинг и анализ.

На этапе мониторинга выполняется более простая процедура – процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т.п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления её с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадёжной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Основная концепция архитектуры WinPCAP

Архитектура WinPCAP дополняет стандартные функции операционных систем семейства Win32 возможностью принимать и передавать данные по сети, минуя стек протоколов операционной системы и взаимодействуя непосредственно с сетевым адаптером компьютера. Более того, она предоставляет приложениям API (Application Programming Interface – Интерфейс программирования приложений) высокого уровня для управления низкоуровневыми процессами. WinPCAP состоит из трех компонентов: драйвер устройства захвата пакетов (packet.vxd), низкоуровневая динамическая библиотека (packet.dll) и статическая библиотека высокого уровня (libpcap).

Структура стека захвата пакетов

Для перехвата пакетов, передаваемых по сети, приложению необходимо взаимодействовать непосредственно с сетевым оборудованием. По этой