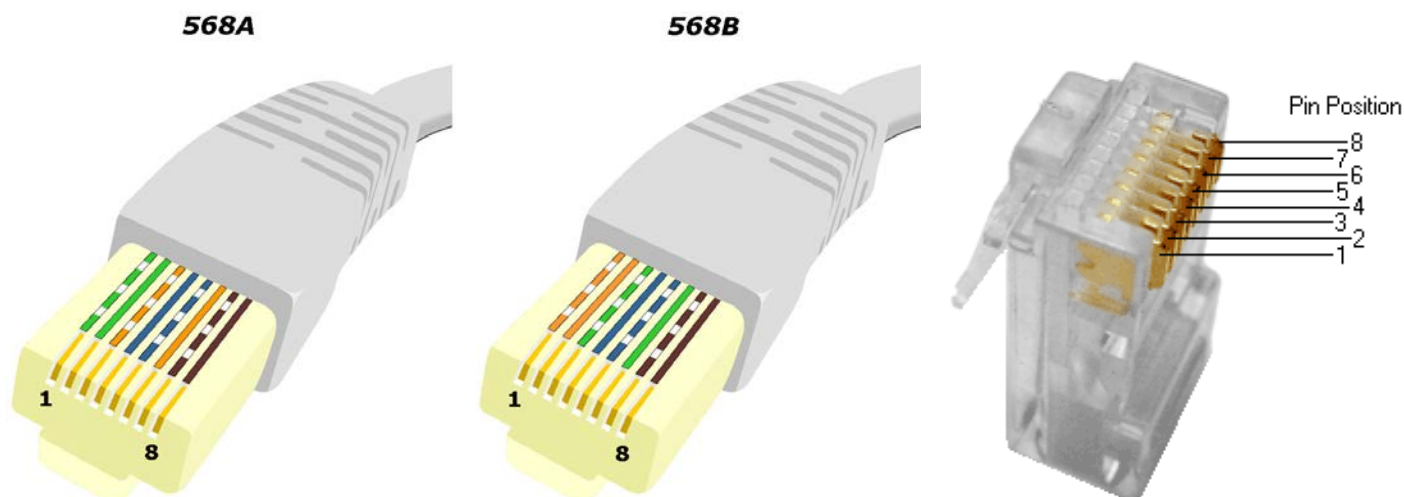


Для изучения курса потребуется стенд, состоящий из 2-х, а в некоторых случаях из 3-х компьютеров, соединенных сетью. Для простых примеров подойдут две рабочие станции, с установленной ОС Windows XP. Для соединения компьютеров в сеть потребуется необходимой длины 8-ми жильный кабель витой пары (Twisted Pair) категории CAT5e (полоса частот 100 МГц, скорость передачи данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар) и соответствующее число 8-контактных коннекторов 8P8C(**8**Position**8**Contact), которые обычно называют RJ-45 (хотя это несколько неверно, RJ-45-это розетка). Существует две разновидности обжимки витой пары – это EIA/TIA-568A и EIA/TIA-568B. Вторая используется чаще.

Нумерация контактов ведется слева направо, при этом коннектор располагается защелкой вверх (на рисунке защелка коннектора расположена внизу, а должна быть наверху при таком расположении проводников кабеля)!!!



Для подключения компьютеров к коммуникационному оборудованию (коммутатор, хаб) необходимо изготовить **прямой кабель** (патч-корд(соединительный шнур), patching cord,), длиной не более 100 метров. На обоих концах обжимаем по EIA/TIA-568B (для соединения оборудования, работающего на скорости до 100 Мбит/с):

1.	Оранжево-белый (TX+)	*	1.	Оранжево-белый (TX+)
2.	Оранжевый (TX-)	*	2.	Оранжевый (TX-)
3.	Зелено-белый (RX+)	*	3.	Зелено-белый (RX+)
4.	Синий (GRD)		4.	Синий (GRD)
5.	Сине-белый (GRD)		5.	Сине-белый (GRD)
6.	Зеленый (RX-)	*	6.	Зеленый (RX-)
7.	Коричнево-белый (GRD)		7.	Коричнево-белый (GRD)
8.	Коричневый (GRD)		8.	Коричневый (GRD)

Для соединения оборудования, работающего на скорости до 100 Мбит/с достаточно использовать только две пары – оранжевая и зеленая (контакты 1, 2, 3, 6), то есть с помощью одного кабеля можно подключить два ПК, при этом, для обжима второго разъема, место Оранжевой пары занимает Коричневая, а место Зеленой - Синяя. При этом схема подключения к контактам сохраняется – используются 1, 2, 3 и 6 контакты. **Внимание:** на самом деле не важно какого цвета провода уложены в каналы коннектора, главное чтобы на втором конце кабеля в те же самые каналы коннекторы были помещены провода того же цвета, что и в первом коннекторе.

Пример расшивки прямого кабеля для подключения двух ПК на одном кабеле:

1.	Оранжево-белый (TX+)	*	1.	Оранжево-белый (TX+)
2.	Оранжевый (TX-)	*	2.	Оранжевый (TX-)
3.	Зелено-белый (RX+)	*	3.	Зелено-белый (RX+)
4.			4.	
5.			5.	
6.	Зеленый (RX-)	*	6.	Зеленый (RX-)
7.			7.	
8.			8.	

1.	Коричнево-белый (TX+)	*	1.	Коричнево-белый (TX+)
2.	Коричневый (TX-)	*	2.	Коричневый (TX-)
3.	Сине-белый (RX+)	*	3.	Сине-белый (RX+)
4.			4.	
5.			5.	
6.	Синий (RX-)	*	6.	Синий (RX-)
7.			7.	
8.			8.	

Для соединения 2-х компьютеров без посредников (коммутатор, хаб) необходимо изготовить **перекрестный кабель** (Ethernet 100Base-T crossover cable) или **кроссовый кабель**. В отличие от прямого кабеля в перекрестном кабеле всегда используются все 8 жил. Этим же кабелем соединяются два хаба (без использования сетевого порта - uplink-порт). **Большинство сетевых устройств способно автоматически определить метод обжима кабеля и подстроиться под него (Auto MDI/MDI-X), то есть 2 ПК можно попытаться соединить прямым кабелем.**

Для скорости 100 Мбит/с перекрестный кабель с одной стороны обжимается по EIA/TIA-568B, а с другой стороны как EIA/TIA-568A:

EIA/TIA-568B		EIA/TIA-568A	
1.	Оранжево-белый (TX+)	1.	Зелено-белый (RX+)
2.	Оранжевый (TX-)	2.	Зеленый (RX-)
3.	Зелено-белый (RX+)	3.	Оранжево-белый (TX+)
4.	Синий (GRD)	4.	Синий (GRD)
5.	Сине-белый (GRD)	5.	Сине-белый (GRD)
6.	Зеленый (RX-)	6.	Оранжевый (TX-)
7.	Коричнево-белый (GRD)	7.	Коричнево-белый (GRD)
8.	Коричневый (GRD)	8.	Коричневый (GRD)

Для соединений на скоростях до 1000Мбит/с при изготовлении перекрестного кабеля одну сторону надо обжать по стандарту EIA/TIA-568B, а вторую так:

EIA/TIA-568B			
1.	Оранжево-белый (TX+)	1.	Зелено-белый (RX+)
2.	Оранжевый (TX-)	2.	Зеленый (RX-)
3.	Зелено-белый (RX+)	3.	Оранжево-белый (TX+)
4.	Синий (GRD)	4.	Коричнево-белый (GRD)
5.	Сине-белый (GRD)	5.	Коричневый (GRD)
6.	Зеленый (RX-)	6.	Оранжевый (TX-)
7.	Коричнево-белый (GRD)	7.	Синий (GRD)
8.	Коричневый (GRD)	8.	Сине-белый (GRD)



Обжимка кабеля производится с использованием специального инструмента – Кримпера (англ. crimp - обжим, опрессовка, в простонародии «обжимка»).

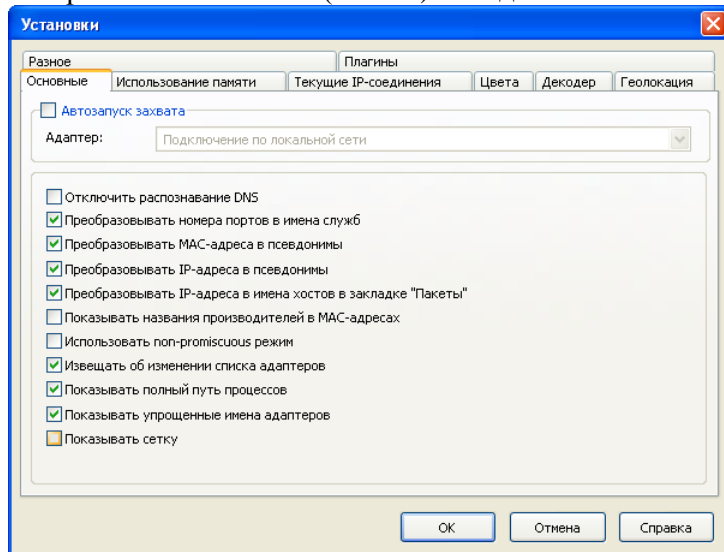
Настройка сети в ОС Windows XP:

1. Соединить перекрестным (можно попытаться и прямым) кабелем 2 ПК.
2. Убедиться в подключении сетевых интерфейсов: Пуск – Панель управления - Сетевые подключения – Подключение по локальной сети – ПКМ – Включить.
3. Настроить параметры протокола TCP/IP: Пуск – Панель управления - Сетевые подключения – Подключение по локальной сети – ПКМ – Свойства – вкладка «Общие» - Протокол Интернета (TCP/IP) – Свойства – Общие – Использовать следующий IP-адрес - IP-адрес: 192.168.0.1 (для первого ПК, 192.168.0.2 для второго ПК) – Маска подсети: 255.255.255.0 – ОК.
4. Удостовериться в том, что оба компьютера находятся в одной рабочей группе: Пуск – Панель управления – Система – вкладка «Имя компьютера» - Изменить.
5. Отключаем антивирусы (KAV) и файрвол (после успешного соединения можно перевести их в штатный режим работы): Пуск – Панель управления – Брандмауэр Windows – Выключить (Не рекомендуется) – ОК.
6. Включить пользователя «Гость»: Пуск – Панель управления – Администрирование – Управление компьютером – Локальные пользователи и группы – Пользователи – ПКМ на «Гость» - Свойства – вкладка «Общие» - снять отметку с «Отключить учетную запись».
7. В локальной политике безопасности устанавливаем назначения прав доступа: Пуск – Панель управления – Администрирование – Локальная политика безопасности – Локальные политики - Назначение прав пользователя:
 - Доступ к компьютеру из сети: Необходимо добавить пользователя «Гость» или «Все».
 - Отказ в доступе к компьютеру из сети: необходимо удалить пользователя «Гость».
8. В локальной политике безопасности устанавливаем параметры сетевого доступа: Пуск – Панель управления – Администрирование – Локальная политика безопасности – Локальные политики - Параметры безопасности:
 - Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей - Гостевая.
 - Сетевой доступ: разрешать анонимный доступ к общим ресурсам – COMCFG, DFS\$.
 - Сетевой доступ: разрешать применение разрешений для всех к анонимным пользователям - Включить.

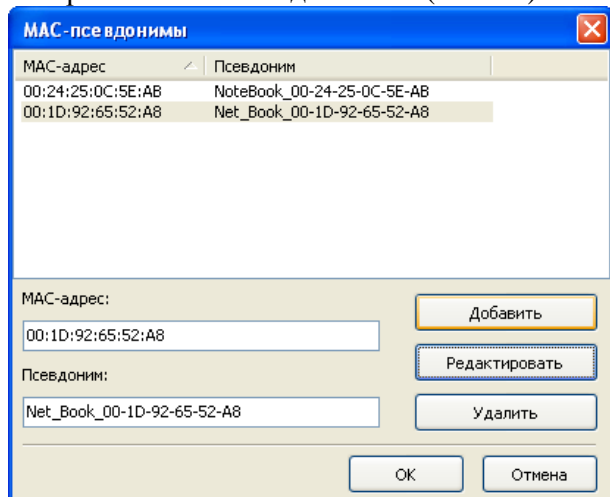
Для контроля наличия соединения на канальном уровне можно использовать команду «ping 192.168.0.x -t», указав в качестве аргумента IP-адрес второго ПК. Наличие ответа говорит о наличии соединения. Провести проверку доступности второго ПК через «Сетевое окружение».

Настройка сетевого анализатора пакетов CommView:

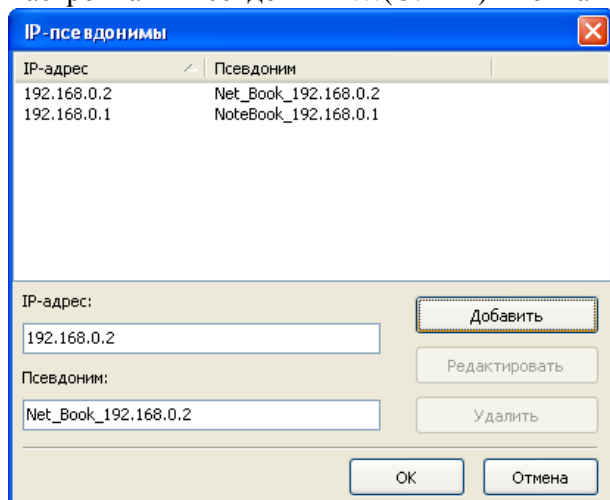
1. Запуск приложения: Пуск-Все программы-CommView-CommView.
2. Настройка-Установки...(Ctrl+O)-вкладка «Основные»- кнопка «ОК»:



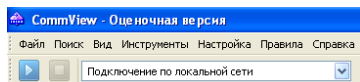
3. Настройка-MAC-псевдонимы...(Ctrl+M)-кнопка «Добавить»-кнопка «ОК»:



4. Настройка-IP-псевдонимы...(Ctrl+B)-кнопка «Добавить»-кнопка «ОК»:

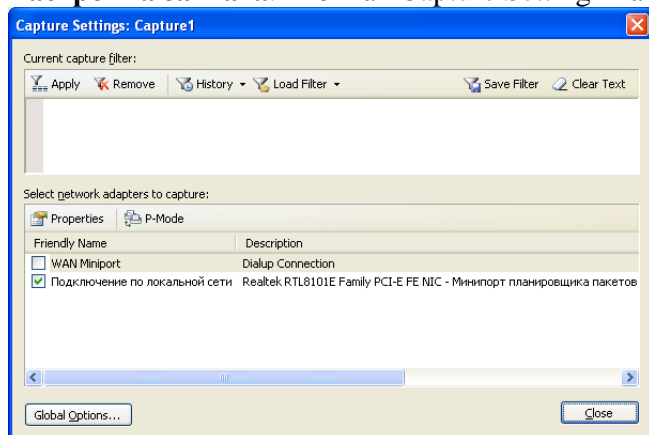


5. Начать захват пакетов: Файл-Начать захват(Ctrl+S):



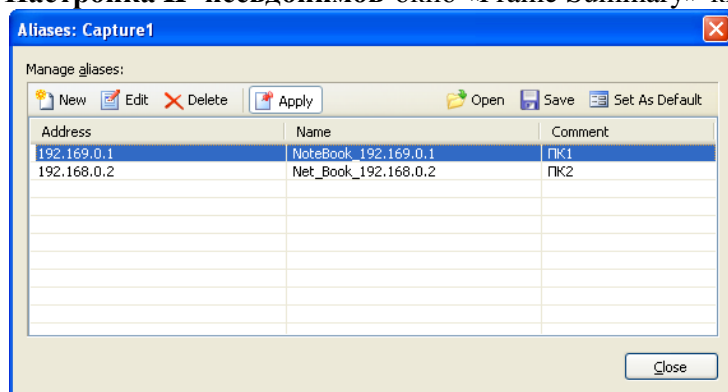
Настройка сетевого анализатора пакетов Microsoft Network Monitor:

1. **Запуск приложения:** Пуск-Все программы-Microsoft Network Monitor 3.4-Microsoft Network Monitor 3.4.
2. File-New-Capture(Ctrl+N).
3. **Установка удобного расположения окон:** кнопка «Layout» (оформление) на панели-Developer.
4. **Настройка захвата:** кнопка «Capture Setting» на панели:



Для продолжения настроек нажать кнопку «Global Options...». Доступ к глобальным опциям можно получить нажав в меню Tools-Options...

5. **Настройка IP-псевдонимов-окно «Frame Summary»-кнопка «Aliases»-Manage Aliases-New-Save:**



Псевдонимы можно назначать в режиме анализа пакетов следующий образом: В окне «Frame Summary» выбрать на нужной строке IP-адрес источника (Source) или назначения (Destination), нажать ПКМ и в меню выбрать «Create Alias for "xxxx" Address».

6. **Установка текущего представления:** В окне «Frame Summary» нажав кнопку «Columns» можно выбрать один из нескольких способов представления информации. Для тонкой доводки можно с помощью мыши переносить столбцы или ПКМ удалять их вообще (Remove Column «xxxxxxxxxxxx»). Кроме этого, в окне «Frame Summary», нажав ПКМ на строке заголовков и выбрав в контекстном меню пункт «Choose Columns...» можно настроить текущее представление.
7. **Управление автопрокруткой:** В окне «Frame Summary» нажать кнопку «Autoscroll».
8. **Управление отображением информации:** Tools-Options...-вкладка «Parser Profiles»: выбрать «Default»-кнопка «Set As Active»-кнопка «OK».
9. **Начать захват пакетов:** Capture-Start(F5).
10. **Управление цветом (очень удобно!):** В окне «Frame Summary» на выбранной строке нажимаем ПКМ на интересующем нас поле, например, «ARP» в столбце «Protocol Name». В контекстном меню выбрать «Add `Protocol Name` as Color Rule». В окне «Add New Color Rule» автоматически будет размещено регулярное выражение «ProtocolName == "ARP"». В секции «Color» выбираем цвет и нажимаем «OK». В результате все строки в окне «Frame Summary» относящиеся к протоколу ARP будут подсвечены выбранным цветом. Для быстрой отмены цветового правила необходимо в окне «Frame Summary» на подсвеченной строке нажать ПКМ и выбрать «Disable This Color Rule».

11. **Поиск информации в окне «Frame Summary»:** В окне «Frame Summary» нажать кнопку «Find», в окне «Find Frame» задать выражение для поиска, например, «IPv4.Address == 10.123.199.9». Строка может иметь и следующий вид: «ipv4.Address==10.123.199.9». Во время набора команды возникают вспомогательные меню, облегчающий ввод. Нажать кнопку «Find». Курсор в окне «Frame Summary» переместится на необходимую позицию.
12. Для высокопроизводительного захвата трафика можно применить утилиту командной строки: «C:\Program Files\Microsoft Network Monitor 3\nmcap.exe». Для вывода ключей: «nmcap /Usage».
13. **Фильтрация трафика.** View-Network Conversations(сетевое общение). Появится окно с группировкой кадров по процессам или приложениям. Мощным инструментом является экранный фильтр (Display Filter): View-Display Filter-Регулярное выражение. Например, для отображения в окне «Frame Summary» только кадров с IP-адресом источника равным 10.123.199.9 надо в окне «Display Filter» записать следующее выражение «IPv4.SourceAddress == 10.123.199.9» и нажать кнопку «Apply». Несколько примеров регулярных выражений (см. встроенную справку - F1: MNM-Using Network Monitor-Using Filters-Examples Filters):
 - IPv4.Address == 192.168.0.1 – отображение кадров с указанным адресом во входящих и исходящих IP-адресов.
 - IPv4.Address==10.0.0.1 and IPv4.Address==10.0.0.222 – просмотр трафика между двумя хостами.
 - Ethernet.DestinationAddress!= BROADCAST – запрет отображения бродкастов. То же самое: Ethernet.DestinationAddress != 0xFFFFFFFFFFFF или Ethernet.DestinationAddress!=FF-FF-FF-FF-FF-FF.
 - Ethernet.Address == 01-02-03-04-05-06 – кадры с указанным входящим или исходящим MAC-адресом.
 - ProtocolName == "ARP" - отображение кадров с протоколом ARP.
 - IPv4.SourceAddress == 10.123.199.9 and ProtocolName == "TCP" - кадры с указанным исходящим IP-адресом и протоколом TCP.
 - ARP.SendersIp4Address == 10.123.199.9 - кадры с указанным исходящим IP-адресом и протоколом ARP.