**Отладка проблем сетевых соединений станции после установки клиента Блокхост-сеть 2.0 (БХС) версии 1038.**

Иногда при установке клиента версии 1038 на рабочую станцию возникают проблемы с подключением к сети. Проблемы могут проявляться двумя разными случаями.

1. **Перебои в работе сетевого подключения.**

Проявление:

В этом случае при загрузке станции наступают кратковременные (от полутора до десяти минут) сбои в работе сети, станция не может открыть сетевые ресурсы, в журналах наблюдаются сбои при попытке применения доменных политик и подключений к сетевым сервисам. Спустя некоторое время сеть восстанавливается и работает без перебоев (до следующей перезагрузки).

Причина таких сбоев - наличие в привязках сетевых адаптеров служб-фильтров в остановленном состоянии. При наличии установленного клиента БХС такие привязки вызывают задержку в инициализации сетевого адаптера, причем никаких записей в логах попытка инициализации не оставляет. После успешной инициализации службы сеть возобновляет работу.

Устранение:

Для устранения этих проблем вам понадобиться консольная утилита enumnic.exe из сервисного набора БХС. Эта утилита выводит привязки служб к адаптерам машины, а также пишет, возможно ли изменение конфигурации адаптера. Вывод ее выглядит примерно так:

d:\distrib\BH\2018\enumiric\x64>D:\distrib\BH\2018\enumiric\x64\enumnic.exe

Filters for "Microsoft Kernel Debug Network Adapter":

00: {3BFD7820-D65C-4C1B-9FEA-983A019639EA} ms\_wfplwf\_lower WfpLwfs : Running (Boot)

01: {C477F579-9F31-474D-86CC-E1567F0BFD1D} KL\_KLIM6 KLIM6 : Running (System)

02: {7B810B33-B5CB-40DF-8DE0-D3C3081E7EA8} ms\_drvfltip DrvFltIP : Running (System)

03: {B5F4D659-7DAA-4565-8E41-BE220ED60542} ms\_pacer Psched : Running (System)

04: {B70D6460-3635-4D42-B866-B8AB1A24454C} ms\_wfplwf\_upper WfpLwfs : Running (Boot)

Filters for "Intel(R) Ethernet Connection (2) I219-V":

00: {3BFD7820-D65C-4C1B-9FEA-983A019639EA} ms\_wfplwf\_lower WfpLwfs : Running (Boot)

01: {C477F579-9F31-474D-86CC-E1567F0BFD1D} KL\_KLIM6 KLIM6 : Running (System)

02: {7B810B33-B5CB-40DF-8DE0-D3C3081E7EA8} ms\_drvfltip DrvFltIP : Running (System)

03: {B5F4D659-7DAA-4565-8E41-BE220ED60542} ms\_pacer Psched : Running (System)

04: {B70D6460-3635-4D42-B866-B8AB1A24454C} ms\_wfplwf\_upper WfpLwfs : Running (Boot)

Filters for "WAN Miniport (IP)":

00: {3BFD7820-D65C-4C1B-9FEA-983A019639EA} ms\_wfplwf\_lower WfpLwfs : Running (Boot)

01: {C477F579-9F31-474D-86CC-E1567F0BFD1D} KL\_KLIM6 KLIM6 : Running (System)

02: {7B810B33-B5CB-40DF-8DE0-D3C3081E7EA8} ms\_drvfltip DrvFltIP : Running (System)

03: {B5F4D659-7DAA-4565-8E41-BE220ED60542} ms\_pacer Psched : Running (System)

Filters for "WAN Miniport (IPv6)":

00: {3BFD7820-D65C-4C1B-9FEA-983A019639EA} ms\_wfplwf\_lower WfpLwfs : Running (Boot)

01: {C477F579-9F31-474D-86CC-E1567F0BFD1D} KL\_KLIM6 KLIM6 : Running (System)

02: {7B810B33-B5CB-40DF-8DE0-D3C3081E7EA8} ms\_drvfltip DrvFltIP : Running (System)

03: {B5F4D659-7DAA-4565-8E41-BE220ED60542} ms\_pacer Psched : Running (System)

Filters for "WAN Miniport (Network Monitor)":

00: {3BFD7820-D65C-4C1B-9FEA-983A019639EA} ms\_wfplwf\_lower WfpLwfs : Running (Boot)

01: {C477F579-9F31-474D-86CC-E1567F0BFD1D} KL\_KLIM6 KLIM6 : Running (System)

02: {7B810B33-B5CB-40DF-8DE0-D3C3081E7EA8} ms\_drvfltip DrvFltIP : Running (System)

03: {B5F4D659-7DAA-4565-8E41-BE220ED60542} ms\_pacer Psched : Running (System)

!!! Can NOT modify net config

В выводе утилиты нас будут интересовать службы, привязанные к физическому адаптеру нашей станции, так как именно на последнем происходят задержки в работе сети. Для определения проблемной службы необходимо выполнить следующую операцию: выявить статус каждой службы с помощью команды sc. Проверять статус службы можно выполняя команду sc queru ser\_name где ser\_name - имя службы. Последнее также можно узнать из утилиты enumeric, оно указана в четвертом (предпоследнем) столбце вывода.

Например, для MS\_NDISCAP это будет выглядеть следующим образом:

Sc query ndiscap

В результате выполнения такой команды по каждой службе можно получить ее статус:

C:\Users\konshin-a>Sc query ndiscap

SERVICE\_NAME: ndiscap

TYPE : 1 KERNEL\_DRIVER

STATE : 1 STOPPED

WIN32\_EXIT\_CODE : 1077 (0x435)

SERVICE\_EXIT\_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT\_HINT : 0x0

Обратите внимание, что статус службы ndiscap stopped. Именно службы в таком статусе и могут вызывать проблемы с инициализацией сетевых подключений, что приводит к перебоям в работе сети.

Чтобы решить описанную проблему, необходимо произвести старт службы, и сделать эту настройку для не дефолтной. Для этого надо выполнить еще две команды:

sc start ndiscap

Sc config ndiscap start= auto

После параметра start= обязательно нужно поставить пробел, иначе команда работать не будет. Обращаю ваше внимание, что для успешного выполнения этих команд командная строка должна быть запущена с правами локального администратора. Если после отладки одной службы проблема продолжает провялятся, то необходимо аналогичным образом проверить остальные привязки к адаптеру, и, если они остановлены, запустить их аналогично описанию выше.

1. **Отсутствие сетевого подключения**

Проявления:

После установки БХС версии 1038 на станции полностью пропадает возможность подключения ко всем сетевых соединениям. Список адаптеров, выводимой по команде ipconfig /all пуст. Какие-либо меры по попыткам восстановления сети (переустановка драйверов, включение или выключение адаптеров) к успеху не приводят.

Причина этого сбоя - наличие в привязках сетевых адаптеров служб-фильтров (на практике как правило присутствует одна такая служба) в частично удаленном состоянии. Это означает, что такая служба была некорректно удалена с данной станции в прошлом. При таком удалении привязка службы к адаптерам сохранилась, в то время как файлы драйверов были физически удалены из системы. При установке БХС попытка инициализации этой службы приводит к сбою работы всех адаптеров, и как следствие, отключению всей сети.

Устранение:

Для устранения этих проблем вам понадобятся утилиты enumnic.exe и bindview.exe. Сетевая конфигурация клиентов должна быть доступна для изменений (некоторые программы, такие как антивирус Касперского с включенным режимом самозащиты, блокируют возможность изменения сетевой конфигурации). Статус возможности изменения сетевой конфигурации можно посмотреть в утилите enumeric (выводится в последние строчки итога работы утилиты). Ни в коем не следует пытаться устранить проблемы с сетью, если вы не можете редактировать сетевую конфигурацию интерфейсов!

Необходимо запустить enumeric из командной строки и получить вывод всех привязок служб к сетевым интерфейсам станции. При анализе, как и в первом случае рекомендую обращать внимание на привязки к физическим адаптерам, так как именно они в первую очередь блокируются службой, удаление которой произведено некорректно. В конце вывода утилиты enumeric будет написано, можно ли поменять конфигурацию сети, примерно так:

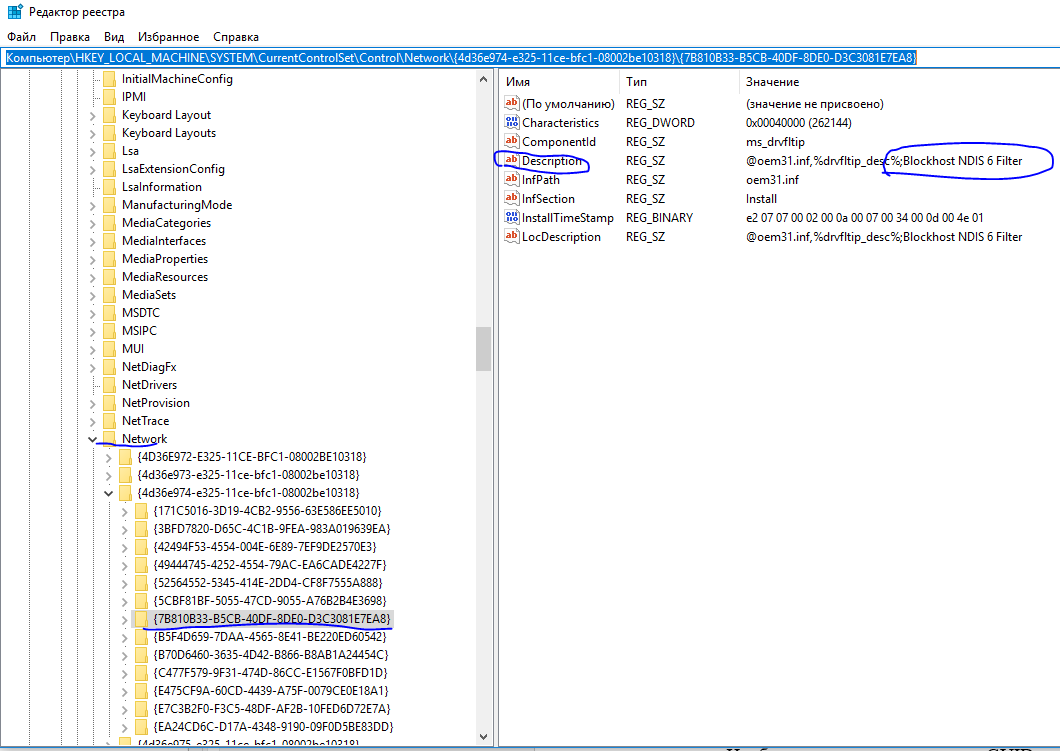
!!! Can modify net config

Если утилита напишет, что сетевую конфигурацию редактировать нельзя, то выполнения дальнейших инструкций необходимо прекратить до получение такой возможности. Также рекомендую удалить из системы приложение, которое блокирует доступ к редактированию сетевой конфигурации. Определить «проблемную» службу можно, использую команду sc start servicename где servicename - кодовое название службы из вывода enumeric (четвертый столбец из вывода утилиты).

Так как проблемная служба фактически наполовину удалена системой, то попытка ее запуска с помощью этой команды окончится ошибкой, в то время как другие службы будут запущены той же командой. Если же служба уже запущена, то sc выдаст следующее сообщение: «Одна копия службы уже запущена». Это значит, что служба запускается автоматически и корректно установлена на диагностируемой станции. Обращаю ваше внимание, что консоль, откуда вы выполняете попытку запуска служб, должна быть открыта с правами администратора, иначе результаты вывода sc могут быть некорректны.

Обнаружив службу, при запуске которой с помощью команды sc выдается ошибка, необходимо определить ее имя, чтобы мы смогли в дальнейшем отвязать ее от сетевых интерфейсов в системе. Сделать это можно с помощью ее guid, значения, которое утилита enumeric выводит сразу после FilterList (второй столбец вывода утилиты).

Необходимо скопировать GUID проблемной службы и в разделе \HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Network\ произвести поиск службы с таким GUID как на рисунке ниже.



Когда вы найдете службу по ее GUID, обратите внимание на строчку description в параметрах службы. В этой строчке будет ее имя, например, для службы со скрина это «Blockhost NDIS 6 Filter». В итоге у нас появилось имя проблемной службы, и мы можем приступать к следующей стадии – удаления привязки этой службы к сетевым интерфейсам системы.

Для этого нам понадобиться утилита bindview.exe. Выполните ее запуск с правами администратора (обязательное условие). Убедитесь предварительно, что сетевая конфигурация доступна для редактирования.



В меню утилиты выберите способ отображения «All services» и найдите имя службы, которое мы получили на предыдущем шаге. Выделите ее, как показано на рисунке. Далее следует выполнить команду uninstall, затем – save bindings. Это процедура удалит привязку проблемной службы к сетевым адаптерам, что должно восстановить работоспособность сетевых подключений. Закройте утилиту и выполните перезагрузку станции, после чего проблема должна устраниться.