

Введение

LanTopolog 2 версия 2.xx

Автор: Юрий Волокитин

Лицензия: Условно-бесплатная

LanTopolog - средство автоматического построения физической топологии компьютерной сети, отображения структуры сети в виде дерева коммутаторов с нумерацией портов и с распределением компьютеров по портам коммутаторов.

Системные требования: Windows Vista/2008/7/8/2012/10/2016

Возможности LanTopolog:

- автоматическое построение физической топологии компьютерной сети на основе данных, собранных с коммутаторов по протоколу SNMP
- отображение схемы сети в двух-панельном браузере
- показывает все устройства на всех портах коммутаторов, их имена и адреса IP
- отображение номеров VLAN, портов LACP, скорости портов
- отображение производителей сетевых устройств
- постоянный мониторинг состояния сетевых устройств с помощью ICMP
- добавление в схему любых данных, привязанных к mac адресу в в импортируемом файле
- публикация схемы сети на web сервере
- поиск в базе данных LanTopolog в том числе и через web браузер
- регистрация состояния тревоги в ситуациях, которые LanTopolog оценивает как неисправность сетевого оборудования
- ведение журнала событий LanTopolog
- автоматическое добавление компьютеров в схему сети по мере их подключения к сети с записью в журнале об обнаружения нового mac адреса
- индикация состояния тревоги и оповещение администраторов с помощью e-mail
- экспорт списка коммутаторов, таблицы соединений коммутаторов, списка VLAN, списка портов в csv файл
- экспорт списка компьютеров в csv файл
- инвентаризация компьютеров в сети предприятия средствами WMI
- мониторинг сетевого трафика, что позволяет узнать источник трафика с точностью до порта коммутатора
- оповещение администраторов о превышении заданных порогов трафика
- простой интерфейс
- программа не производит никаких записей в системные области (реестр, системные папки) и является портативной
- программа безопасна и не имеет функций передачи данных через интернет

Вопросы и пожелания по LanTopolog шлите support@lantopolog.com

Сайт программы www.lantopolog.com/rus/

Лицензия

Лицензионное соглашение к программе LanToroLog 2 версии 2.xx

Все авторские права на программу LanToroLog 2 принадлежат Волокитину Юрию.

Использование программы LanToroLog означает, что вы принимаете условия данного соглашения.

Программа распространяется по принципу shareware в виде Демо-версии, которую Вы можете использовать неограниченно долго.

Для использования программы без функциональных ограничений Вам необходимо зарегистрировать свою копию программы, оплатив стоимость лицензионного ключа.

Для всей локальной сети, которая может включать до 10000 управляемых коммутаторов, нужна одна лицензия.

Лицензионный ключ привязывается к коммутаторам, которые вы выбрали при регистрации и не может быть использован в другой сети. Число коммутаторов для привязки к лицензии ограничено тремя. Если все три коммутатора будут заменены, то ваша копия LanToroLog станет незарегистрированной и для регистрации нужно будет купить лицензию заново. В дальнейшем вы можете добавлять новые коммутаторы к вашей сети - при этом ваша лицензия останется действительной. Программа может одновременно выполняться на неограниченном числе компьютеров с одним и тем же лицензионным ключом.

Вы не можете эмулировать, изменять, декомпилировать, дизассемблировать, изучать код программы. Любое такое нелегальное использование означает автоматическое и немедленное прекращение действия настоящего соглашения.

LanToroLog распространяется по принципу "AS IS".

Никаких гарантий не предусматривается. Вы используете LanToroLog на свой риск.

Автор не отвечает ни за какие потери или искажение данных, любую упущенную выгоду, вызванные использованием или неправильным использованием программы LanToroLog.

Вы можете распространять Демо-версию LanToroLog свободно при условии того, что настоящий дистрибутив не изменен.

Все обновления LanToroLog 2 бесплатны.

Все права, явно не предусмотренные данным соглашением, сохраняются за Волокитиным Юрием.

Если вы не согласны с этим лицензионным соглашением, вам необходимо прекратить использование LanToroLog.

Построение схемы сети

Для построения схемы сети следуйте инструкциям на закладках Step 1, Step 2, Step 3

Step 1

1. Specify ranges of IP addresses for switch discovery

Введите диапазон(ы) IP адресов, в которых будет производится поиск коммутаторов. Задайте параметры доступа по SNMP для каждого диапазона ("read community string" или user/password в случае SNMPv3)

2. Discover the switches

Выполнить поиск коммутаторов во всех диапазонах ("Discover within all the ranges") или только в отмеченных галочкой ("Discover within the checked ranges")

Если какие-либо коммутаторы не обнаруживаются, проверьте доступ к коммутатору по SNMP любой другой утилитой SNMP. Например этой:

<https://www.paessler.com/tools/snmptester>

Программа может отображать на схеме точки доступа, поддерживающие SNMP.

Для этого включите опцию "Try to discover access points"

3. Check that all switches are present within the list of discovered devices

Убедитесь, что все коммутаторы появились в таблице справа. Удалите из таблицы устройства, не являющиеся коммутатором или точкой доступа.

Step 2

1. Collect SNMP data from the switches

Нажмите эту кнопку для сбора с коммутаторов данных, необходимых для построения топологии сети. Если для какого-либо коммутатора значение в колонке "Number of Learned MACs" (количество мак-адресов в таблице коммутатора) равно нулю, то проверьте доступ по SNMP к ветке SNMP MIB OID 1.3.6.1.2.1.17.4.3.1.2 и 1.3.6.1.2.1.17.7.1.2.2.1.2) с помощью любой другой утилиты SNMP. Например этой:

<https://www.paessler.com/tools/snmptester>

Step 3

1. Discover the Topology

Нажмите эту кнопку для запуска процесса построения топологии сети.

По окончании процесса в этом же окне появится схема сети, как ее распознала программа. На этом этапе вы можете изменить выбор коммутатора в качестве корневого узла (root node на закладке Step2) и еще раз нажать "Discover the Topology"

2. Apply the New Topology

Нажмите эту кнопку для сохранения распознанной схемы в качестве рабочей.

Результат построения схемы сети - на закладке Network Browser

Пояснения к схеме

На схеме отображаются только те порты коммутаторов, которые присутствуют в таблицах коммутации. То есть неиспользуемые порты не отображаются.

При использовании SNMPv3 для получения данных VLAN с коммутаторов Cisco необходимо в настройках коммутаторов задать "context" как описано здесь:
<http://www.switchportmapper.com/support-mapping-a-cisco-switch-using-snmpv3.htm>

Стек коммутаторов отображается на схеме как один коммутатор с одним IP адресом. При этом нумерация портов этого коммутаторов нарушается.

Алгоритм, применяемый для построения топологии, не гарантирует точное воспроизведение фактической топологии.

Применяйте следующие рекомендации для более точного распознавания топологии:

- увеличьте время хранения динамических MAC адресов через настройки коммутаторов
 - во время выполнения этапа "Step 2", "Collect SNMP data from the switches" большинство компьютеров в сети должно быть включено
 - в качестве корневого узла в дереве топологии выбирайте коммутатор, через который проходит трафик от наибольшего числа компьютеров. Это обычно ближайший к маршрутизатору коммутатор (если маршрутизатор имеется). Для выбора коммутатора в качестве корневого отметьте его галочкой на шаге 2.
 - желательно, чтобы компьютер, на котором работает LanTopolog, был подключен к сети как можно ближе к корневому коммутатору
 - включите на коммутаторах LLDP (CDP)
 - в построенной схеме могут быть соединения, в которых вместо номеров портов стоят символы "xx" - эти соединения LanTopolog не смог распознать. Вы можете добавить в ручную таблицу соединений такие нераспознанные соединения (Options - Discovery - View/edit connection list) и повторить построение (Step 2 - Discover Topology).
- Пример: 172.16.25.243 port 6 - 172.16.25.248 port 27

Программа отображает на схеме внутреннюю (SNMP) нумерацию портов, которая может отличаться от нумерации портов на панели коммутатора. В случае путаницы в нумерации портов смотрите описание порта или имя порта (port description, port name).

Пояснения к некоторым полям:

25Feb - дата последнего успешного ответа на команду ping. Если IP адрес компьютера неизвестен, то это дата последнего обнаружения MAC- адреса в таблицах коммутаторов
15:50 - время последнего успешного ответа на команду ping (сегодня)
18:30y - время последнего успешного ответа на команду ping (вчера)

Если компьютер отвечает на команду ping, то для него на схеме самая правая цифра означает время ответа на команду ping в миллисекундах.

Общие настройки

Map Display Options

Здесь вы можете включить опции для отображения на схеме следующих данных:

- расположение коммутатора (редактируемое поле Location в настройках коммутатора)
- описание коммутатора (модель коммутатора)
- описание порта
- имя порта
- ваши комментарии к порту (port alias)
- производитель сетевого устройства (определяется по MAC адресу)
- VLAN ID
- размер шрифта на схеме сети

Map Colors

Выбор цвета для фона и диаграмм трафика.

Log Options

События в журнале LanTopolog автоматически удаляются, если они старше заданного количества дней.

Database maintenance

MAC адреса удаляются из базы LanTopolog, если они не обнаруживаются в течении заданного количества дней.

Настройки для инвентаризации компьютеров

Run computer discovery every ... hour(s)

Интервал в часах, с которым повторяется процесс обнаружения в сети новых MAC адресов, определения их места на схеме, а также IP адресов и имен компьютеров. Если программа не может точно определить место компьютера на схеме сети, то этот компьютер помещается в ветку схемы под названием "Pseudo device as temporary location" (псевдоустройство для временного хранения). Это происходит, если в момент опроса MAC адрес компьютера отсутствует в таблице коммутатора, к которому он подключен. Попробуйте следующие рекомендации:

- увеличьте время хранения динамических MAC адресов через настройки коммутаторов
- почаще запускайте процесс обнаружения в сети новых MAC адресов (по расписанию каждый час или вручную) и со временем большинство компьютеров встанет на свои места на схеме.

Цикл процесса резолвинга имен компьютеров может занять несколько часов в зависимости от числа компьютеров в вашей сети.

WMI credential

- аккаунт для сбора данных о компьютерах средствами WMI
Если поля не заполнены, то применяются права текущего пользователя. Отсутствие данных WMI у компьютера обычно говорит об отсутствии доступа к WMI этого компьютера. Проверить доступ можно командой Windows wmic:

```
wmic /node:<имя ПК или IP> ComputerSystem get DNSHostName
```

Эту команду следует запускать на компьютере, на котором работает Lantopolog.

Notify when a new MAC address is discovered

- извещать об обнаружении в сети нового MAC адреса. Способы оповещения смотрите здесь: меню - Service - Options - Alarms - Alarm Notification.

Use manually edited connection list

При построении топологии использовать таблицу соединений, редактируемую вручную. Используйте эту опцию если на карте остались нераспознанные соединения, отмеченные как 'xx'.

View/edit connection list - редактировать эту таблицу.

Пример: 192.168.0.1 port 12 - 192.168.0.2 port 50

Слева от символа '-' должен быть коммутатор, расположенный выше в дереве коммутаторов, справа - соответственно ниже.

Настройки для Web сервера

LanToroLog не может выполнять роль Web сервера и поэтому использует внешний Web сервер для публикации схемы сети.

Save network map as htm/php in order to publish it on the Web server

Включите эту опцию для постоянного обновления схемы сети на Web сервере. Задайте расширение для сохраняемых файлов (**htm** или **php**).

В поле 1 укажите путь к папке, в которую программа сохраняет htm/php страницы.

В случае, если Web сервер расположен на другом компьютере сети, то это будет путь к общей папке на компьютере с Web сервером, например \\сервер\общая_папка

В поле 2 укажите локальный путь к папке с файлами LanToroLog на компьютере с Web сервером. Если Web сервер находится на том же компьютере, что и LanToroLog то это поле совпадает с полем 1

В поле 3 укажите web адрес для папки с файлами LanToroLog

В поле 4 укажите HTTP http адрес для скрипта ltsearch.cgi

Функция поиска работает, если файл ltsearch.cgi скопировать в папку для скриптов Web сервера. Если Web сервер находится на машине Linux то файл ltsearch.cgi нужно скачать отсюда: <https://www.lantopolog.com/linux/ltsearch.cgi>

Пример полей для Web сервера Apache:

1. C:\Apache24\htdocs\ltl
2. C:\Apache24\htdocs\ltl
3. http://hostname.domain/ltl
4. http://hostname.domain/cgi-bin/ltsearch.cgi

Пример полей для Microsoft IIS Web Server:

1. c:\inetpub\wwwroot\ltl
2. c:\inetpub\wwwroot\ltl
3. http://hostname.domain/ltl
4. http://hostname.domain/scripts/ltsearch.cgi

Пример полей для Web сервера на машине Linux

1. \linux_machine\share_name_for_ltl
2. /var/www/html/ltl
3. http://hostname.domain/ltl
4. http://hostname.domain/cgi-bin/ltsearch.cgi

HTTP адрес для просмотра схемы LanToroLog:

<http://hostname.domain/ltl/nettop.htm/php>

Вы можете ограничить доступ к страницам LanToroLog средствами PHP.

Для этого вам нужно добавить свой php код к файлам LanToroLog

Для этого вставьте свой код в файл ..\LanToroLog2\Import\rename_add_php.txt и переименуйте этот файл в add_php.txt

Настройки монитора трафика

Traffic (Bandwidth) Monitor

Диаграммы трафика показывают использование полосы пропускания каждого порта за последний час.

Цифра(масштаб) возле оси диаграммы показывает величину полосы пропускания порта:

100M означает 100Mbps

1G означает 1Gbps

и так далее

Если суммарный входящий и исходящий трафик на порту превышает эту цифру, то масштаб может измениться на 200M, 2G и так далее.

Задайте порог величины использования полосы пропускания и интервал времени, в течении которого эта величина усредняется. Если усредненная величина превысит заданный порог, то это зафиксировано в журнале событий LanTopolog, а если включена опция

"Notify when the average bandwidth usage exceeds the threshold",
то об этом также будут оповещены администраторы.

Monitoring iflnErrors, iflnDiscards counters

- Мониторинг ошибочных и потерянных пакетов

The number of iflnErrors packets exceeds ... % of input packets

Здесь задайте процент количества входящих пакетов, полученных с ошибкой, от общего числа входящих пакетов. Превышение этого порога зафиксировано в журнале событий LanTopolog, а если включена опция

"Notify when the number of invalid or dropped packets exceeds the threshold",
то также об этом будут оповещены администраторы.

The number of iflnDiscards packets exceeds ... % of input packets

Здесь задайте процент количества "потерянных" пакетов от общего числа входящих пакетов. Превышение этого порога зафиксировано в журнале событий LanTopolog, а если включена опция

"Notify when the number of invalid or dropped packets exceeds the threshold",
то также об этом будут оповещены администраторы.

Настройка оповещений

Alarm Notification

Выберите способ оповещения администраторов о событиях тревоги (звуковой сигнал, запуск вашего скрипта или программы, извещение по почте). Для оповещения по почте настройте клиент SMTP (Send Email Options). В настройках почты в поле "Send email to" можно указать несколько адресатов.

В случае публикации схемы LanToroLog на Web сервере вы также можете получать звуковой сигнал о потере доступа к коммутатору. Для этого в Web настройках LanToroLog выберете расширение php для записи Web страниц на Web сервер. Кроме того в Web браузере, используемом для просмотра страниц LanToroLog, должен быть разрешен прием cookies и разрешено автоматическое проигрывание звуков.

Настройка Ping Monitor

Time interval between two consecutive checks of a monitored object

- период повтора цикла проверки доступа к компьютерам сети.

Для обнаружения одновременного пропадания доступа к группе компьютеров (из-за неполадок сетевого оборудования) не рекомендуется задавать эту величину больше 5 минут.

Number of ping attempts before marking a device as "down"

- число неудачных попыток ping, после которых генерируется сообщение администратору. Опции оповещения настраиваются на закладке "Alarm".

Notify when ping test fails (set notify options on the "Alarm" ' tab)

- включить оповещение администраторов.

Нажмите "**Edit list of monitored hosts**" для редактирования списка объектов мониторинга. Хотя коммутаторы отсутствуют в этом списке, Ping Monitor также контролирует доступ к ним с помощью ICMP. Иногда желательно отключить оповещения о пропадании ответов от некоторых коммутаторов.

Для этого добавьте IP адрес такого коммутатора в "list of monitored hosts", но перед адресом вставьте символ "-". Пример: -192.168.0.1

На схеме отображается время ответа на команду ping (цифра справа в миллисекундах) для тех компьютеров, у которых LanTopolog смог определить IP адрес.

Indirectly determining hub or unmanaged switch failure

- определение отказа хаба или неуправляемого коммутатора косвенным способом. Сигнал тревоги взводится, если происходит одновременное пропадание доступа к группе компьютеров, подключенных к одному и тому же хабу или неуправляемому коммутатору. Здесь вы можете задать пороговые значения количества пропавших компьютеров (**The number of computers that stop responding is more than**) и их процент от общего числа в группе

(**The percentage of computers that stop responding is more than**)

При превышении этих порогов событие фиксируется в журнале и происходит оповещение администраторов, если включена опция

Notify when ping test fails

Кроме того на схеме проблемный порт помечается желтым значком в виде колокольчика. Если какой-либо коммутатор перестает отвечать на команду ping, то это событие также фиксируется и коммутатор помечается красным значком в виде колокольчика.

Импорт Экспорт

IP, Hostname Import

- Импорт таблицы MAC-IP-Hostname

Если у вас есть таблица MAC-IP или MAC-IP-Hostname, то вы можете импортировать эту таблицу (меню - File - Import - IP, Hostname Import)).

Это может помочь в случаях, когда программа не может автоматически определить IP адрес и имя компьютера.

Файл для импорта должен быть в текстовом формате с разделителем пробел, ";" или ","

Также возможен импорт IP и Hostname из файла, созданного утилитой Nmap

(<https://nmap.org>). В опциях утилиты nmap задайте вывод результатов сканирования в файл в формате "normal" (опция -oN <файл>). Также возможен импорт IP и Hostname из файла, созданного программой Advanced IP Scanner. Для этого сохраните результат сканирования как csv файл. Домен(workgroup) и логин также импортируются из файла Advanced IP Scanner.

Import Custom Data

- Импорт любых данных

Если у вас есть таблица, в которой для каждого mac адреса есть какие-то данные (например фамилия пользователя, логин, здание, помещение), то вы может добавить эти данные в схему сети (меню - File - Import - Custom Data Import).

Файл для импорта должен быть в формате csv с разделителем пробел, ";" или ","

Хотя бы один столбец в импортируемом файле должен содержать MAC адрес.

Ширину столбцов на схеме можно задать в настройках импорта.

Export

- Экспорт

Здесь вы можете экспортировать список компьютеров, список коммутаторов, таблицу соединений коммутаторов, список всех портов, список VLAN в файл .csv

Все процедуры импорта и экспорта могут выполняться автоматически по расписанию (см. Options - Discovery - Computer Discovery) или запускаться вручную.

Ограничения демо-версии

Демо-версия имеет следующие ограничения:

Через некоторое время после запуска программы:

- диаграммы трафика не отображаются
- невозможно изменить ширину правого окна браузера схемы сети
- невозможна публикация веб-страниц на веб-сервере
- номера VLAN не отображаются на схеме
- функция поиска прекращает работать
- часть данных на карте сети заменяется словом "demo"

Демо-версия дает возможность оценить всю функциональность программы.

После покупки LanToroLog вы получите регистрационный ключевой файл, который превратит демо-версию в полнофункциональную версию

Как получить лицензионный ключ

После покупки LanTopoLog вы получите лицензионный ключевой файл, который превратит демо-версию в полнофункциональную версию.

Для получения лицензионного ключа следуйте инструкции:

1. Выполните распознавание схемы сети с помощью демо версии LanTopoLog 2 и сохраните ее (нажмите "Apply the New Topology")
Откройте форму регистрации (меню - Help - How to Get a License Key).
В появившемся списке отметьте галочкой от 1 до 3 коммутаторов.
Ваш лицензионный ключ будет привязан к этим коммутаторам.
Хотя бы один из этих коммутаторов должен будет всегда присутствовать на схеме LanTopoLog (хотя временно может быть и выключен), иначе ваша копия LanTopoLog будет считаться незарегистрированной.
2. В поле ниже появится идентификатор вашей сети (Network ID string).
Вышлите почтой этот идентификатор на адрес sales@lantopolog.com (скопируйте и вставьте в письмо)
3. Произведите покупку лицензии.
Ссылки для покупки приведены на www.lantopolog.com/rus/buy.html
Покупайте LanTopoLog только у продавцов, перечисленных на www.lantopolog.com
4. После получения оплаты вам будет выслан лицензионный ключевой файл.
Скопируйте этот файл в папку, которая откроется при нажатии на ссылку "this folder" на форме регистрации и перезапустите LanTopoLog.
Для версии с инсталлятором эта папка здесь:
C:\Users\<user>\AppData\Local\LanTopoLog2\lantopolog.lic
Для портативной версии эта папка здесь:
..\папка куда распакован скачанный zip файл\lantopolog2xx\LanTopoLog2\lantopolog.lic

Заметьте, что лицензионный ключ привязан к MAC адресу коммутатора, то есть вы можете менять любые настройки коммутатора (IP адрес, имя и т.д.) - при этом ваша лицензия останется действительной.
В дальнейшем вы можете добавлять новые коммутаторы к вашей сети - при этом ваша лицензия также останется действительной

Обновление программы. Перенос данных.

Обновление программы до новой версии

Все обновления бесплатны.

Версия с инсталлятором

Остановите программу, если она запущена. Установите новую версию.

При этом все данные и настройки сохраняются

Портативная версия

Распакуйте файл с портативной версией в любую папку.

Если необходимо сохранить прежние данные, то переместите старую папку с данными \LanTopoLog2\ в новое место (см. ниже)

Перенос данных.

Версия с инсталлятором

Файлы с данными расположены здесь:

C:\Users\<user>\AppData\Local\LanTopoLog2\

Портабельная версия

Файлы с данными расположены здесь:

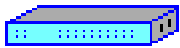
..\папка куда распакован файл с портативной версией\lantopolog2xx\LanTopoLog2\

Папка ..\LanTopoLog2\ создается при первом запуске программы.

Если необходимо перенести данные, то замените содержимое новой папки

..\LanTopolog2\ содержимым старой папки ..\LanTopoLog2\

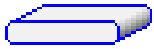
Значение иконок на схеме



Коммутатор, ответ на команду ping успешный.



Коммутатор, на команду ping не отвечает.



Точка доступа или другое устройство, поддерживающее SNMP, ответ на команду ping успешный.



Точка доступа или другое устройство, поддерживающее SNMP, на команду ping не отвечает.



Разъем подключения



Хаб, неуправляемый коммутатор, беспроводная точка доступа,... Программа отображает эту иконку, если обнаруживает, что к порту коммутатора подключены 2 и более компьютера.



Компьютер, принтер, мобильное устройство. Ответ на команду ping успешный.



Компьютер,... На команду ping не отвечает.



Компьютер,... Есть данные инвентаризации WMI.



Инструменты



Иконка тревоги. Ping Monitor отображает эту иконку, если коммутатор не отвечает на команду ping.



Иконка тревоги. Монитор трафика отображает эту иконку, если загрузка трафика превысила заданные в опциях пороги. Также эту иконку отображает Ping Monitor, если на команду ping не отвечает хост из списка мониторинга.



Коммутатор или хост из списка мониторинга возобновил ответ на команду ping.



Обнаружен новый MAC адрес. Удалить эту пометку можно, если нажать кнопку "Show New", а затем "Clear New"



Диаграмма трафика на порту за последний час. Цифра у оси (100M) - это скорость порта и масштаб диаграммы (100Mbit/sec). Пунктирная линия показывает порог использования полосы пропускания порта, заданный в опциях (Options - Traffic). Стрелка вправо означает, что исходящий трафик на порту преобладает над входящим (подсчитывается как средний за интервал времени, заданный в опциях трафика).