Introducing LanTopoLog

LanTopoLog 2 version 2.xx

Author: Yuriy Volokitin

License: Shareware
The network topology discovery function works without any limitations in the unregistered version so LanTopoLog provides a free network mapper for an unlimited time.

System requirements: Windows Vista/2008/7/8/2012/10/2016

LanTopoLog 2 is an application that provides
physical network topology discovery, visualization and monitoring.

Key features

- Automatic physical network topology discovery based on SNMP
- Provides detailed and searchable physical network topology map
  so you can quickly isolate network connectivity failures
- LanTopoLog Switch Port Mapper tool maps the physical port connections of a switch
  to MAC and IP addresses of the attached devices
- LanTopoLog works with any model of switch
- Shows VLAN assignment, port status, port's current speed, LACP ports
- Detecting new devices in the network and notifying of this event
- Import allows you to add custom data to the map
- Icon context menu for custom command
- LanTopoLog also includes network monitoring tools
- Monitoring device's state (active/inactive) in real-time using ICMP
- Generating alarms when there are failures in the network
- E-mail alerts notifying
- Web browser-based access from anywhere in the network
- LanTopoLog uses WMI queries to collect computer inventory information
- Export switch list and switch connection table to csv file
- Resolve ip to name, export computer list to csv file
- Network traffic monitoring
- Monitoring invalid and dropped packets (ifInErrors, ifInDiscards)
- Notify the administrator when traffic thresholds are exceeded
- Easy-to-use interface
- The program do not write anything to the operating system area (registry, system folders)
  and is portable
- The program is safe to use and does not send any data to anywhere.

Website www.lantopolog.com

Feel free to email me any errors or comments to support@lantopolog.com

License

LanTopoLog 2 License Agreement

LanTopoLog 2 version 2.xx

LICENSE

You are hereby licensed to use the Demo version of the Software for an unlimited period. When you purchase LanTopoLog, you will receive a license key file that will convert the demo into the full version. The license key is bound to up to 3 switches that you select during the registration process. At least one of them must always be present on the LanTopoLog map (although may be temporarily turned off), otherwise your copy of LanTopoLog is not considered registered. If all 3 of these switches are replaced then you will need to purchase the new license. In the future you can add new switches to your network, however, your license remains valid. You need only one license for local network with up to 10000 managed switches.
One license allows you to run LanTopoLog on multiple computers simultaneously.

Restrictions

You may not emulate, rent, lease, sell, modify, decompile, disassemble, reverse engineer, create derivative works based on the Software, or transfer the licensed program, or any subset of the licensed program. The Software, in whole or in part, may not be incorporated with or into any other software product. Any such unauthorized use shall result in immediate and automatic termination of this license.

Disclaimer of Warranty

This Software is provided "AS IS" and without warranty of any kind, express, implied or otherwise, including without limitation, any warranty of merchantability or fitness for a particular purpose. The entire risk arising out of use or performance of the Software remains with you.

Distribution

The LanTopoLog 2 Demo version may be freely distributed, provided distribution package is not modified and form a complete package when distributed. This license must be included with all copies of the Software, and may not be modified from its original format as created by the Licensor.
All updates to the LanTopoLog 2 are free.

If you do not agree with the terms of this license you must cease to use the product.

Discovery steps

To perform the network topology discovery follow the instructions
in the tabs "Step 1", "Step 2", "Step 3".

Step 1

1. Specify the ranges of the IP addresses for switch discovery.
For example: 192.168.0.* 192.168.0.100-200 172.16.200-255.*
Set SNMP access parameters for each range ("read community string" or user/password in case of SNMPv3)

2. Discover the switches
Click "Discover within all the ranges" or "Discover within the marked ranges"
Discovered switches will be added to the list of SNMP devices (see table right).
If some of your switches are not discovered then test SNMP access to these switches with any other SNMP utility. For example https://www.paessler.com/tools/snmptester
To discover routers and access points which support SNMP turn on option
"Discover routers and access points"

3. Check that all switches are present within the list of discovered devices.
If it is not so, then repeat the Step 1 - Sub-Step 1,2

Step 2

1. Click "Collect SNMP data from the switches"
In this step the program gathers bridge forwarding table data from the switches.
If the value in the field "Number of Learned MACs" is null then test access to SNMP Bridge MIB information (MIB OID 1.3.6.1.2.1.17.4.3.1.2 and 1.3.6.1.2.1.17.7.1.2.2.1.2) with any other SNMP utility.

Step 3

1. Click "Discover the Topology"
Compare the discovered topology with the actual topology. If necessary, edit the connection list (menu - Service - Options - Discovery - View/edit connection list)
and click "Discover the Topology" again.
2. Click "Apply the New Topology" to save the new topology map.

The discovered topology is shown in the tab "Network Browser".

Notices

The program displays the switch port if at least one MAC address is detected on this port.

In case of SNMPv3:
Cisco switches are not typically configured for reading of all the Bridge-MIB information on a per-VLAN basis when using SNMPv3.
In this case you need to configure an SNMPv3 context as described here:
http://www.switchportmapper.com/support-mapping-a-cisco-switch-using-snmpv3.htm

The algorithm used to discover network topology is not 100% reliable for mapping the entire network and some connections may remain undiscovered (labeled as xx).
There are some recommendations that may reduce the number of unknown connections:
- increase the length of time the switch keeps dynamic MAC addresses in memory before discarding.
- run the discovery process when the majority of computers are alive
- assign manually the root node on the Step 2. The root node switch should be the switch with maximum traffic load
- the computer where you are running LanTopoLog should be connected as near as possible to the root node switch
- enable LLDP (CDP) on the switches
- use manually edited connection list (Options - tab Discovery-...). Add unknown connections to the manually edited connection list. Example:

    172.16.25.243 port 6 - 172.16.25.248 port 27
    172.16.25.243 port 57 - 172.16.25.248 port 83

The program displays internal (SNMP) numbering of ports that may differ from port numbering on the switch front panel. See port description and port name if there is a confusion between snmp port number and real port number.

Some data interpretation:
02Feb - date of last successful ping. If IP address is not resolved then it is SNMP-based discovery date
15:50 - time of last successful ping (today).
18:30y - time of last successful ping (yestoday).

The program displays the ping response time in millisecond (number to the right of each machine).

Options - General

All options in this tab are obvious and are not described in detail.

Options - Discovery

Set these options to discover new computers and other end devices.

Schedule the discovery process. Also, you can run the discovery immediately
(menu - Service - Run Computer Discovery Now).
If the discovery process is already running, then this menu item is inactive.

LanTopoLog uses WMI queries to collect computer inventory information.
WMI queries use current user credentials.
However, you can specify alternate credentials when querying remote computers.

During the discovery process, the program retrieves the MAC address table from
a switches via SNMP. If the MAC address of the computer absent from the table of the switch then the program cannot determine the proper location of that computer and move it to the "Pseudo device as temporary location".
There are some recommendations to avoid this problem:
- through the switch settings increase the length of time the switch keeps dynamic MAC addresses in memory before discarding.
- run the discovery process when the majority of computers are alive
It takes some time to move the most of computers to its proper place on the map.
The program uses SNMP oid 1.3.6.1.2.1.17.4.3.1.2 and 1.3.6.1.2.1.17.7.1.2.2.1.2
to get bridge MAC address table. The most of switches support these oids.
If the switch doesn't support these oids then the program cannot locate devices connected to this switch.

In case of SNMPv3:
Cisco switches are not typically configured for reading of all the Bridge-MIB information on a per-VLAN basis when using SNMPv3.
In this case you need to configure an SNMPv3 context as described here:
http://www.switchportmapper.com/support-mapping-a-cisco-switch-using-snmpv3.htm

During the discovery process, the program tries to resolve a MAC address to an IP address and host name. It can take a few hours until the resolving cycle is finished.

On this option page you can manually set connections between switches
("View/Edit connection list" button). Use this option if some connections remain undiscovered (labeled as xx). Example:
192.168.0.1 port 12 - 192.168.0.2 port 50
The upper (in the tree) switch must be on the left side of the '-' character, the lower switch must be on the right side of the '-' character.
This option allows you to add non-SNMP device to the main map. In the example above the device 192.168.0.2 may not support SNMP.

Options - Web

LanTopoLog cannot act as a Web server.
In order to publish LanTopoLog web pages use any external Web server.

Turn on option "Save network map as htm/php in order to publish it on the Web server"
for continuously updating LanTopoLog web pages and set files extension (htm or php).

In the field 1 enter the path where LanTopoLog htm/php files are to be saved.
May be network path (e.g., \\server\sharename)

In the field 2 enter the local path corresponding to LanTopoLog folder web address
on the Web server machine. If LanTopoLog and Web server reside on the same machine then enter the same path as in the field 1.

In the field 3 enter LanTopoLog folder web address.

In order to enable search function copy the file ltsearch.cgi into the Web server script directory.
For Linux Web Server download ltsearch.cgi from https://www.lantopolog.com/linux/ltsearch.cgi
In the field 4 enter HTTP address for the ltsearch.cgi

The following are typical values for Apache Web Server:
1. C:\Apache24\htdocs\ltl
2. C:\Apache24\htdocs\ltl
3. http://hostname.domain/ltl
4. http://hostname.domain/cgi-bin/ltsearch.cgi

The following are typical values for 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

The following are typical values for Linux Web Server:
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

The HTTP address for the LanTopoLog map: http://hostname.domain/ltl/nettop.htm(php)

You can restrict access to LanTopoLog webpages using PHP. For this you need to add custom php code to LanTopoLog php files. See the file ..\LanTopoLog2\Import\rename_add_php.txt for further instructions.

Options - Traffic

Traffic (Bandwidth) Monitor

Traffic diagrams show the bandwidth usage of each port in the last hour.
The figure (scale) near the axis of the diagram shows the value of the port bandwidth:
100M means 100Mbps
1G means 1Gbps
and so on
If the total incoming and outgoing traffic on the port exceeds this figure, the scale may change to 200M, 2G, and so on.

Set the threshold for the bandwidth usage value and the time interval during which this value is averaged. If the average value exceeds the specified threshold, then it will be recorded in the LanTopoLog event log, and if "Notify when the average bandwidth usage exceeds the threshold" option is enabled, this will notify the Administrators.

Monitoring ifInErrors, ifInDiscards counters

The alerts are sent when the percentage of invalid or dropped packets exceeds the specified thresholds.

Options - Alarms

Alarm Notification

Choose the method of alarm notification (play sound, execute program/script, send email).

Send Email Options

You can specify more than one email address.
Define the settings of your SMTP server for the alarm notification via email.

If you monitor your network via Web browser you can also receive alarm sound notification from LanTopoLog. For this in the LanTopoLog Web Options window select option "Save as php".
Also cookies and autoplay audio must be enabled in your Web browser.

Options - Ping monitor

Ping options

Ping Monitor checks if hosts are up and notify when the ping test fails.

Set time interval between two consecutive checks of a monitored object
and number of ping attempts before marking a device as "down".

Notify when the ping test fails - Set notify options on the "Alarm" tab.

Edit the list of monitored hosts.

The switches are not shown in the list of monitored hosts, but Ping Monitor checks them, too.
In some cases it is desirable to stop notification for certain switches.
Add IP addresses for those switches into the list of monitored hosts
and put a '-' character before the address (example: -192.168.0.1).

Indirectly determining the hub or unmanaged switch failure

The program tries to determine hub or unmanaged switch failure using the indirect method.
An alarm occurs if the majority of computers that stop responding during
the short time are connected to the same hub or unmanaged switch.
Define the thresholds:
The percentage of computers that stop responding
The number of computers that stop responding
This function depends on option:
Time interval between two consecutive checks of a monitored object
To enable this alarm do not set this interval more than 5 minutes.

Import Export

IP, Hostname Import

If not all IPs and Hostnames get resolved automatically then use the import from MAC-IP-Hostname file. To add computer IP addresses and Hostnames to the network topology map perform the import procedure (menu - File - Import - IP, Hostname Import).
The data fields must be separated by the field delimiter (space ; ,).
The import file can be created with Nmap (use the –oN option to save the Nmap scan result) or with Advanced IP Scanner (save the scan result as a CSV file). The domain(workgroup) and username also can be imported from Advanced IP Scanner scan result file.

Custom Data Import

To add custom data to the network map perform the import procedure (menu - File - Import - Custom Data Import).
Use CSV file to import data. The CSV file must contain a column for the MAC address.
For each column you can set the width you want to see on the network map.
To hide certain columns from displaying set the column width of 0.

Export

The program can export computer list, switch list, switch connection table, port list, VLAN list (menu - File - Export - Export).

The Import and Export procedures can be performed automatically according with the schedule.

Demo limitations

The unregistered version has the following limitations:
Some time after the program starts:
- the right pane of the network browser becomes non resizable
- web publishing is disabled
- VLAN IDs are no longer displayed
- search function stop working
- display "demo" instead of real data

The unregistered version allows you to test all functionality of the program.
When you purchase LanTopoLog 2, you will receive a license key file
that will convert the demo into the full version.

How to Get a License Key

When you purchase LanTopoLog 2, you will receive the license key file
that will convert the demo into the full version.
You need only one license for local network with up to 10000 managed switches.

Follow the instructions below.

1. Discover your network with demo version of LanTopoLog 2
   and save the discovered topology (click "Apply the New Topology").
   Open the registration form (menu - Help - How to Get a License Key) .
   Select from the list up to 3 switches using checkboxes.
   Your license key file will be bound to these switches.
   At least one of them must always be present on the LanTopoLog map
   (although may be temporarily turned off), otherwise your copy of LanTopoLog 2
   is not considered registered.
   If all 3 of these switches will be replaced then you will need to purchase the new license.

2. Network ID string will appear in the field below.
   Send Network ID string via email to the sales@lantopolog.com
   (copy the string and paste into the email)

3. Purchase LanTopoLog 2 through the program site www.lantopolog.com
   Avoid buying from any company not listed in www.lantopolog.com

4. After you have made payment, your license key file will be emailed to you.
   Copy the license key file to the folder that is opened when clicking
   "this folder" link on the registration form and restart the program.
   For installable version this folder is
   C:\Users\<user>\AppData\Local\LanTopoLog2\lantopolog.lic
   For portable version this folder is
   ..\folder where you unzip the downloaded file\Lantopolog2xx\LanTopoLog2\lantopolog.lic

Note: The license key is bound to the MAC address of the switch, so you can change any switch settings (IP address, Name, etc) - the license key remains valid.
In the future you can add new switches to your network, however, your license key remains valid.

Updating the program. Moving the data.

Updating to the new version

All updates are free.

Installable version:
Stop the program (if it is running) and install the new version.
The new version will keep the data and settings of the previous one.

Portable version:
Unzip the new version zip file to any directory.
If you'd like to keep the old data, move the old data files to the new location (see below).

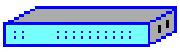
Moving the data

Installable version:
LanTopoLog data files are located in
C:\Users\<user>\AppData\Local\LanTopoLog2\

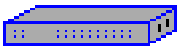
Portable version:
LanTopoLog data files are located in
..\folder where you unzip the downloaded file\Lantopolog2xx\LanTopoLog2\

The folder ..\LanTopoLog2\ is created after the first run of the program.
If you wish to keep the data and settings, replace the new folder ..\LanTopoLog2\
with the old one.

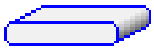
Icon legend



Switch, the ping is successful.



Switch, the ping is unsuccessful.



An access point or other device that supports SNMP, the ping is successful.

An access point or other device that supports SNMP, the ping is unsuccessful.

Socket

Hub, unmanaged switch, wireless access point, ...
The program displays this icon if two or more MACs are detected on the switch port.

End device (computer, printer, mobile device), the ping is successful.

End device, the ping is unsuccessful.

Mark the device that is monitored via ICMP ping.

Tools

Alarm icon. Ping Monitor displays the red icon when a switch stops responding to ping. See the log for details.

Alarm icon. Traffic monitor displays the yellow icon when traffic load exceeded the configured threshold. Also, Ping Monitor displays the yellow icon when a monitored host stops responding to ping. See the log for details.

The switch or monitored host resume responding to ping.

- Icon for the new MAC address. To remove the icon, click "Show New" button, then "Clear New" button.

Bar chart of traffic load for the last 60 minutes. Y axis scale is 100M (100 Mbit/sec). In the 1 hour chart the 1 pixel represents 1 minute.
The dashed line shows the port bandwidth usage threshold specified in Options (Options - Traffic).
The arrow to the right means that the outgoing traffic on the port prevails over the inbound traffic (calculated as the average for the time interval specified in the traffic options).