# LANeye 2.3

**A software that makes**

# Network Intrusion Detection

**simple enough for none professionals.**

## Prevent unauthorized access to your network.

LANeye monitors the network traffic. If a new unknown computer tries to gain access to the network LANeye will immediately detect that. LANeye will alert you about the intrusion and block the intruding computer access to the network.

You decide if the new computers shall be part of your familiar computers.

**LANeye - A new unique concept for network protection.**

# LANeye protects your network from intrusion in three steps.

| Detect | Alarm | Block |
|---|---|---|
| LANeye detects if unknown computers tries to gain access to your network or wireless LAN. | | LANeye prevent connecting computers from accessing your shared files, folders and printers. |
| LANeye detects if familiar computers behaves suspicious when connecting to your network or WLAN. | LANeye alerts you and log intrusions. | LANeye prevent connecting computers from gaining access to a valid IP address on your network. |

## Do unauthorized use your WLAN?

  With LANeye you have a complete view over what devices that connects to your network. LANeye not only detects computers. LANeye will detect network printers, routers, WLAN access points and all other devices that communicates on your network.

  When LANeye detects a new device, LANeye will mark that device as unknown. LANeye places all unknown devices on a list. Unknown devices will automatically be blocked. For a unknown device to be accepted on the network you will have to move the unknown device to the familiar list.

## LANeye is not a firewall.

  LANeye work differently from a traditional firewall. LANeye will not block network traffic. Instead LANeye monitors the network traffic. When an unwanted computer tries to gain access to the network LANeye will interfere in the logon procedure and send access denial packets to the unwanted computer.

## Run LANeye on any computer.

  Detecting and blocking will work undependably of what computer LANeye runs on.

## LANeye do not use any access codes, no encryption or passwords.

LANeye only use the basic functionality of the networking protocols to protect your LAN.

# Why use LANeye?

**Computer network and security.**
Company have been using computer networks for many years. Now computer networks become common in home environment. Most people knows that firewalls and Antivirus software are needed to protect there networks and computers from threats coming from the Internet.

**When setting up a network.**
Choosing wireless network technology today is common and that introduces new security problems.

In a cable network you have a fairly good view and control over what devices that are connected to your network.

Fairly in respect to that in the early days of high speed internet access, Internet service providers connected there customers to a for the customer invisible local network. Some of us remember browsing the network neighborhood finding your neighbors computers and easily accessing their shared files and folders.

This problem still exists and the best way to separate your private network is by using a hardware firewall/router.

**When installing a wireless network.**
When installing a wireless network you have provided your surrounding with a potential connection to your network. This connection often resides behind your firewall on the inside. Your firewall will protect you from Internet access but not the access from computers in the range of your wireless LAN.

- OK, then I have to setup the wireless access point outside my firewall.
Well that's possible but that will limit the access to locally shared files and folders in an undesirable way.

Wireless vendors configures there product for accessibility and not security due to reduce the complexity of installing wireless equipment.

In principle that means no security.

LANeye is not designed to replace the build in security system in wireless equipment. Encryption and other restriction shall be used. LANeye shall be used as an extra protection shield and will protect your network if there is security flaws in your equipment or if someone have figure out your encryption password.

**Unauthorized computer may try to access your network** by wire or by your wireless access point as shown in the picture. For LANeye it makes no difference how the access is made. LANeye will detect intrusion for both situations and protect you network. LANeye holds a list over familiar computers. This list is easy to maintain from within the user interface.

When a new unknown computer tries to gain access to your network LANeye checks to see if the computer is listed among the familiar computers. If not, LANeye will defend your network against the intruding computer by sending friendly but firm messages to the unknown computer that it is not welcome on this network. The intruding computer may try several times and LANeye will defend your network every time until you mark the new computer as familiar.
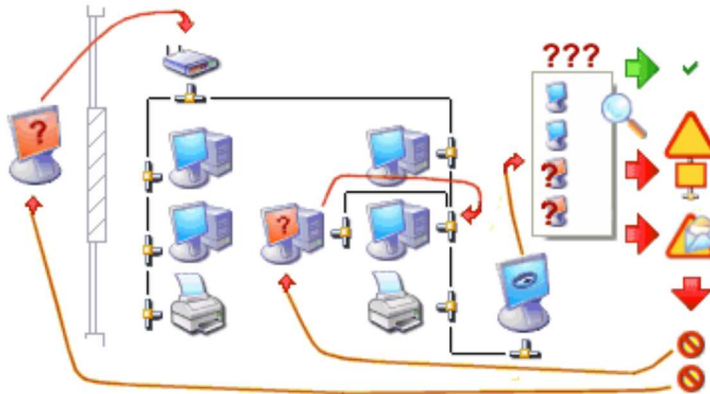
- **Use Firewall** to stop unwanted visits from the Internet.
- **Use Antivirus** to stop unwanted code to execute on your computer.
- **Use LANeye** to stop unwanted computers on your network.

**Security threats comes not only from the outside.** In a company network the inner threat is often grater than the outer threats. Employees may easily, often without thinking, expose the network to security risks now when laptop computers have become so common. Ask your self the following questions:

- Do the company allow employees to use company laptops at home?
- Do the company allow there laptops to be used on public networks (airports ..) when employees travels?

Security levels on other networks can not be predicted. Always treat computers that has been on unfamiliar networks as a potential threats:

- Login information may have been revealed.
- Security flaws may be exploited and unwanted code may be implanted.
- Security in home networks are often much lower than in the company network.

**LANeye detects differences during network logons.** It is becoming more and more common that intruders tries to gain access to company networks by mimic a familiar computer. LANeye will detect that. This function is called Hijack detection and if a familiar computer shows an unexpected behavior during logon, LANeye will start block this computer even if it is on the familiar list. Do not look at this as a drawback. Use this feature to protect the company network and block computers that been on another network as a quarantine function. If an employee uses the company laptop at his/her own home network and bring the computer back to work, the computer will be blocked. This gives the IT department time to check the computer for unfriendly code before it can be used on the company network.

---

- **Use LANeye** to prevent computers that have been used on other networks from gaining access to your network.

---

## How does LANeye work?

When computers communicate on a network the network data packets are sent out without really knowing if someone is listening.

All computers that are connected to the network are able to hear all traffic on the network. What one computer send out reaches all the other computers.

For computers to be able to separate information from each other every computer have its own unique ID called MAC-address (Media Access Control address). MAC-addresses are closely related to the hardware and is not the same thing as IP-addresses. Computers uses the MAC-address to distinguish what data packets to compute and not compute. When a computer talks to another computer the sending computer places it own MAC-address in the data packet and the MAC-address of the receiving computer. The receiving computer then knows that the data packet are meant for him and who to send a reply to.

In a network where switches are used to connect computers together, not all computers will hear every other computer. The switch will only forward traffic that belongs to computers behind it to reduce the amount of data traffic.

When this is true for most traffic this is not true for broadcast packets.

When a computer logons to a network it sends out broadcast packets, telling all the others on the network that there is a new computer here. The switches will allow these broadcast messages to reach all computers on the network and that's how LANeye can detect all computers on the network.

Before the connecting computer can start to communicate on the network it has to negotiate with the other computers what name and IP address to use.

By several broadcast messages the new computer letting every other computer know what name, domain, workgroup and IP address the new computer will use. LANeye collect this information and if the computer is unknown, LANeye will send denial data packets to the new computer, telling it that the name and IP-address is not allowed. That leads to that the new computer can not used these name and IP addresses and without name and address the new computer can not communicate. On repeated requests LANeye will again tell the computer that the requested address and name are not allowed.

LANeye will only send denial packets during the connection phase. If a computer have successfully establish a connection on the network LANeye will not block that computer.

# Program description

**LANeye monitors the network traffic.** The program starts every time the computer boots up and works in the background. The information LANeye gathers is saved to a surrounding file.

In the program main view you can see what detection and blocking functions that are activated.

**Alarm** will show up as a visual sign and alarm may be sent by email to given addresses.

**LANeye main windows** is divided in two major views. On the left there is a tree view of all computers and other devices that has been detected by LANeye. The right side present different views depending on what node in the left side tree that is selected.

**Network Surveillance**                          **Activated**

**Intrusion Detection**
☑ Detect new unknown computers            Activated
☑ Detect MAC-address hijacking            Activated
☑ Detect suspicious logon attempts        Activated

**Intrusion Prevention**
☑ Block access to local network           Activated
☑ Block IP-address handout                Activated
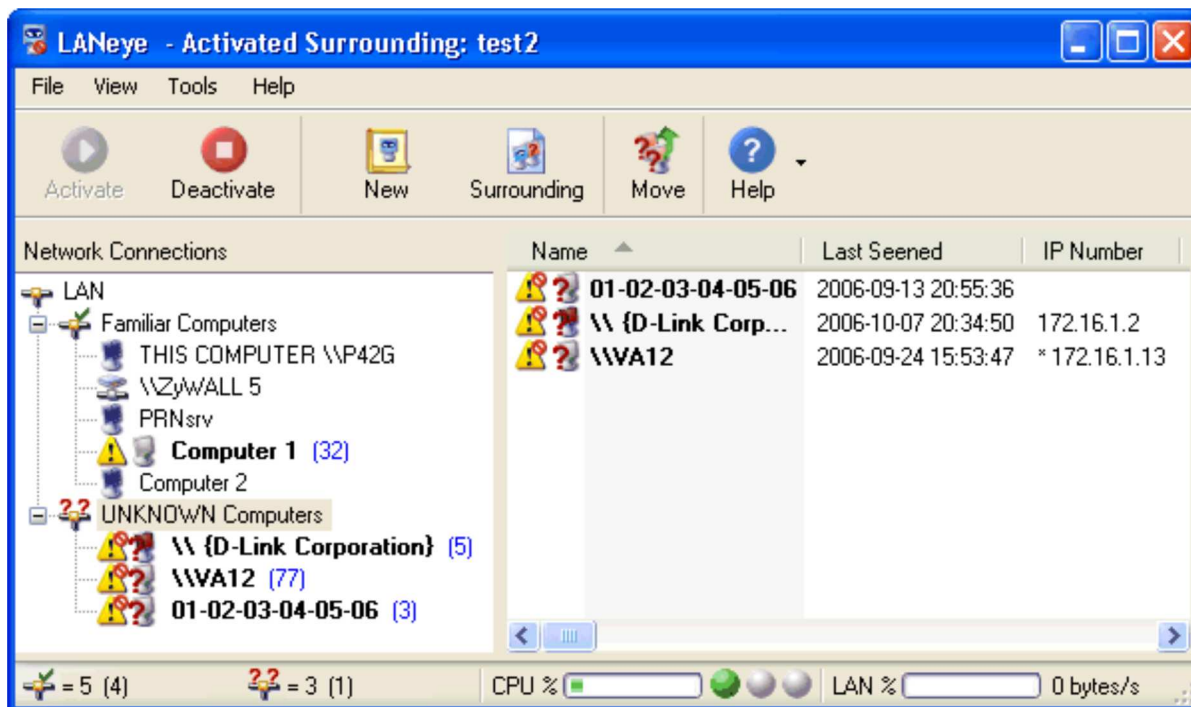


**The tree view node "UNKNOWN computers"** presents a list of computers that have not yet been verified. All new computers will be listed under this node. The warning sign shows that an intrusion has been detected and the blocking sign shows that the computer will be blocked when trying to connect to the LAN.

**The tree view node "Familiar computers"** present the list of computers that you have verified been part of your network. Computers listed here will be check by LANeye for MAC-address Hijacking and other suspicious logon behavior. Devices on this list may be blocked if they behave abnormal.

**The list view on the right** shows details of individual nodes in multiple columns. Manual blocking, types, familiar/unknown state of the device and more can be set via a property dialog. When moving a device from unknown to familiar, blocking will automatically be removed. At the same time, move a device from familiar to unknown will activate the logon blocking again.

**Incidents gets logged** when LANeye detects intrusion and blocks access. Every device has its own incident log. For every event in the incident log there is a short description about the event and what may have cause it. Unread incidents are marked as bold and unread and total numbers of incidents are counted.



**A description of an incident** gives a brief text about what may caused the incident and why LANeye was triggered.



**Statistics over the device** is collected and are shown as graph over different activities. The graph shows a device activity, intrusion statistics and blocking statistics.
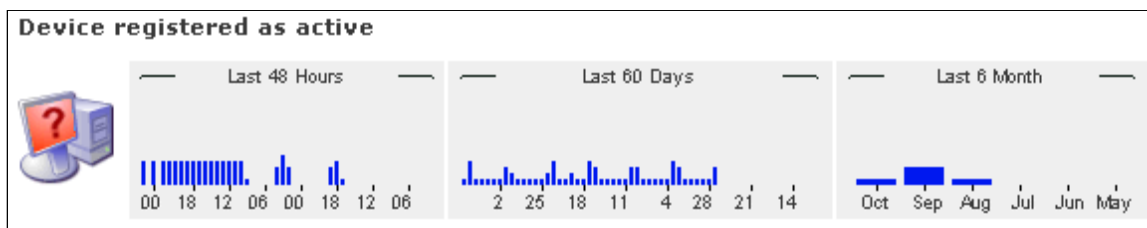


**Wizards to install and run LANeye** are included. In the wizard you select network adapter to be used. The wizard will scan your network in several different ways for the network devices to reveal them self. After a scan you have to walk trough the unknown list and mark devices as familiar.

# LANeye product variants

## LANeye 2.3 is available in two variants.

**LANeye 2.3 Small Network Edition.** This variant is aimed for small business and home networks.  Small Network Edition is easier to handle but still have all the detection and blocking functions. Advanced function to handle advanced clients are excluded.

- For networks with up to ten (10) devices. (MAX 25 devices can be handled).

**LANeye 2.3 Professional Edition.**  This variant is aimed for larger networks and networks with advanced clients.

- Handles large networks.
- Excluding filters for VPN / SAN (Storage Area Network) / Virtual machines like VMware.
- Excluding filters for none-hijacked IP-address that allows users to user there company laptops at home.
- Support for multi surroundings.

| LANeye product variant matrix<br>Shows the difference in functionality between the listed variants. | LANeye 1.6 | LANeye 2.3<br>Small Network<br>Edition | LANeye 2.3<br>Professional<br>Edition |
|---|---|---|---|
| **Product version name** | | | |
| Detecting new unknown computers | ✔ | ✔ | ✔ |
| Detecting potential MAC-address hijacking | – | ✔ | ✔ |
| Detecting suspicious logons | – | ✔ | ✔ |
| Block access to the network | – | ✔ | ✔ |
| Block IP-address negotiations | – | ✔ | ✔ |
| Local alarm | ✔ | ✔ | ✔ |
| Alarm by E-mail | ✔ | ✔ | ✔ |
| Traffic log | ✔ | ✔ | ✔ |
| Traffic log to printer | ✔ | – | – |
| Detailed device information | – | ✔ | ✔ |
| Statistics | – | ✔ | ✔ |
| Incident log with descriptions | – | ✔ | ✔ |
| Support for multiple surroundings | ✔ | – | ✔ |
| Network size (Number of devices) | Unlimited. | **MAX 25** | Unlimited. |
| Custom defined device types | – | – | ✔ |
| Excluding filters for VPN/SAN/Virtual Machines | – | – | ✔ |
| Excluding filters for hijack detection | – | – | ✔ |

## LANeye 2.3 Specification

| | |
|---|---|
| Intrusion detection | Sensitivity can be set to three (3) different levels and includes:<br>- Detection of new unknown MAC-addresser<br>- Detection of unexpected IP-address request during logons.<br>- Detection of name, workgroup or domain changes upon logon.<br>- Detection of unexpected reconnect attempts in short time periods.<br>Professional Edition have excluding filters for:<br>- Hijack warnings and suspicious logons.<br>- IP-address lists to handle laptops that are used on different networks. |
| Logon blocking | Activates automatically when intrusion is detected or by manual activation.<br>- Blocks access to the network by NetBT defending name.<br>- Blocks access to a valid IP-address by defending ARP. |
| Alarm | Activates when intrusion is detected or blocking is performed:<br>- Visual and sound signal (or .wav file) on local computer.<br>- E-mail. Send an email by SMTP with or without authentication. |
| Log | - Incident log, logs events, intrusion and blocking.<br>- System log, shows LANeye activities (start/stop/alarm/...) |
| Traffic view | - Sender and receiver MAC, IP addresser, protocol type IP/Ethernet.<br>- UDP/TCP sender and receiver port number.<br>- UDP/TCP traffic types  (http/pop/netbios/ftp/smtp/ssh/telnet/...).<br>- Ethernet traffic types (IP/ARP/IPX/IPNG/NOVELL/SNMP/...). |
| Traffic filter | - Multicast packet filter.<br>- Local-administrated packet filter.<br>- Only sent packets filter. |
| Device information | - Date when the device was first send and last active.<br>- Network names  (CIFS/SMB/NETbios/DHCP/DNS)<br>- Vendor, Operating system, How IP address was provided.<br>- Type of device. If device have DHCP server, Class ID, CIFS services<br>- MAC-address, IP-address, Subnet mask, Domain, Workgroup, DNS |
| Indicators | CPU utilization and LAN-adapter utilization. |
| Surrounding support | Small Network Edition handle only one (1) surrounding.<br>Professional Edition handles multiple surroundings. |
| Auto start | Starts and activates during boot up. |
| System | Runs in the background. Easy to reach from the system tray. System tray indication for current activities, number of devices and alarms. |
| Help system | - Built in incident help for every incident event type. Short descriptions about what caused the event and what may be a natural cause or suspicious event.<br>- Built in introduction wizard.<br>- Built in HTML context sensitive help.<br>- Built in wizards to train LANeye on your network. |

## LANeye 2.3 System requirements

| | |
|---|---|
| Operating system | Windows 7, Vista, XP, 2000 with IE 5 or higher. |
| Network | Ethernet |
| Hardware | CPU 500MHz minimum, recommended 1GHz or faster.<br>Graphics SVGA (800x600) 256 color or higher.<br>Network adapter. (works with onboard, USB, PC-Card and WLAN cards) |

LANeye, a product from ProPrat, Stockholm Sweden
www.proprat.com | contact@proprat.com