Layer-2 Network Guard

Руководство пользователя

Оглавление

1 Общие сведения

L2NG предназначен для защиты Ethernet сетей с **неуправляемым сетевым оборудованием** от несанкционированного доступа, контроля и защиты от смены IP или MAC адресов пользователями сети, программного отключения пользователей от сети (без вмешательства на физическом уровне), контроля и запрета использования PPPoE сервисов в сети, контроля и запрета использования Broadcast/Multicast сервисов (Netbios, различные безсерверные чаты и т.д.)

L2NG использует эффективные алгоритмы и методы блокирования/отключения узлов (Double-sided ARP spoofing, MAC spoofing, 802.3x Flow Control) с учетом особенностей работы низкоуровневых сетевых протоколов наиболее распространенных операционных систем (Windows 9x/2000/XP/2003/Vista, FreeBSD и Linux).

2 Область применения

L2NG контролирует единый бродкастдомен сети. В случае нескольких подсетей (бродкастдоменов) необходимо использовать L2NG в каждом сегменте сети.

Типичными задачами для L2NG могут являться:

- контроль/запрет смены MAC/IP адресов в сети;
- контроль/запрет назначения определенных диапазонов адресов;
- контроль/запрет несанкционированного доступа/подключения;
- запрет на назначение адресов и создание IP сети в сегменте;
- отключение от сети за неуплату абонентских взносов (в случае коммерческих сетей);
- запрет использования неразрешенных в сети безсерверных чатов (Vypress, BorgChar, Nassi и т.д.);
- запрет использования Netbios (Microsoft Networks);
- запрет подключения к интернет провайдерам по PPPoE протоколу (например с компьютера ребенка и т.д.)

3 Требования к ОС и ПО

Требования к ОС: Windows-2000/XP/2003.

Требования к дополнительному ПО: необходима установленная библиотека WinPcap версии 4.0

4 Установка программы

Программа распространяется в виде одного файла-дистрибутива. Для установки достаточно запустить установочный файл L2NG-X.X.exe (где X.X – номер версии), все необходимые шаги будут выполнены мастером.

5 Обзор L2NG

L2NG состоит из клиентской и сервисной частей:

Клиентская часть (l2ng.exe) предназначена для управления, настройки, визуального наблюдения, контроля и анализа работы сервисной части.

Сервисная часть (l2ngsrv.exe) является Win32 сервисом и управляется операционной системой. Стандартные операции управления сервисом (запустить, остановить, перезапустить) рекомендуется производить с помощью клиентской части. Сервисная часть предназначена для **автономной работы**.

6 Настройка сервисной части

Внешний вид окна опций (меню Service->Options) показан на рис. 1.

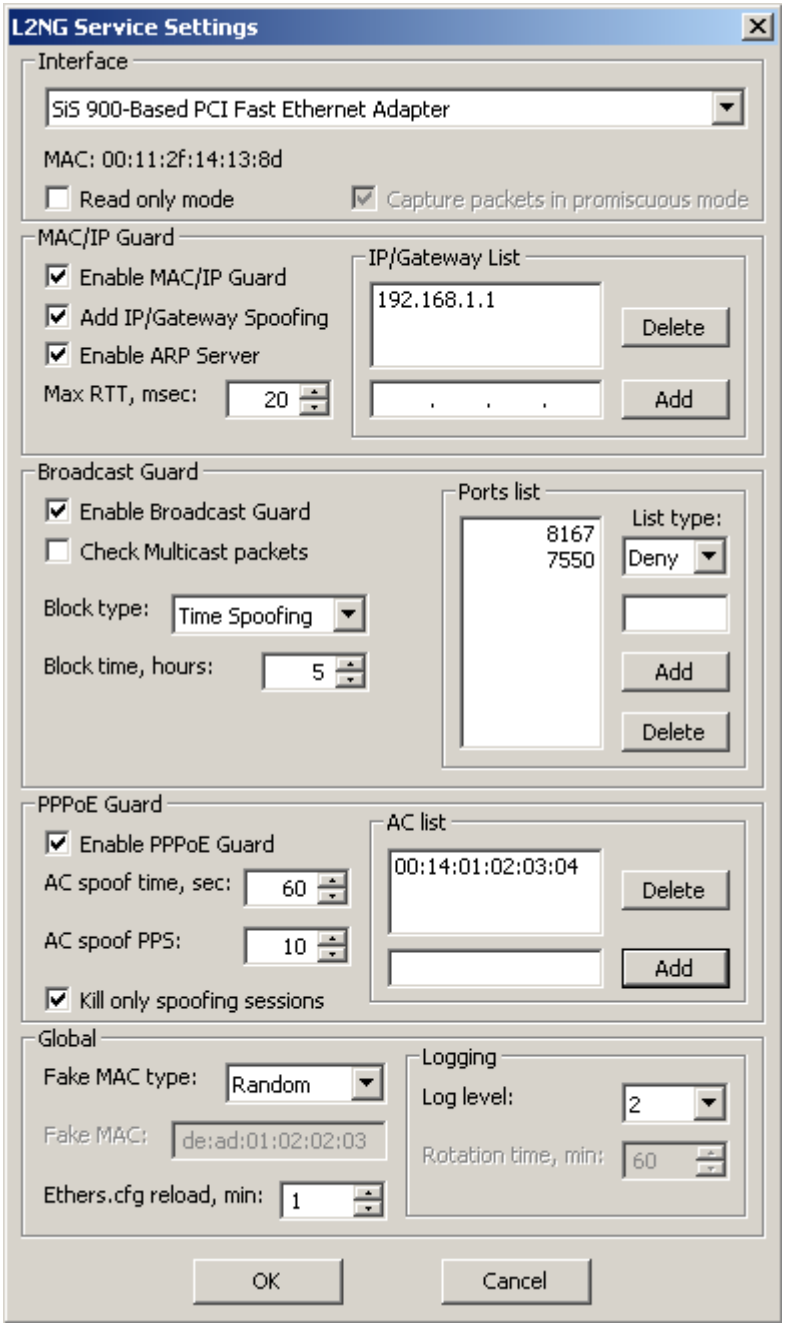


Рис. 1 Окно опций сервиса (меню Service->Options)

Порядок настройки сервисной части (меню Service->Options):

1. Выбрать необходимый сетевой интерфейс (Interface). В зарегистрированной версии программы необходимо выбрать зарегистрированный сетевой интерфейс (MAC адрес интерфейса должен совпадать с MAC адресом, на который зарегистрирована программа).
2. Включить требуемые режимы работы L2NG (MAC/IP Guard, Broadcast Guard, PPPoE Guard) и, при необходимости, произвести соответствующие настройки данных режимов.

6.1 Глобальные опции

Interface - сетевой интерфейс который непосредственно подключен к контролируемому сегменту.

Read Only mode - режим "только чтение". Данный режим предназначен для проверки правильности настроек, изучения работы L2NG, мониторинга сегмента и т.д. Фактического блокирования узлов в данном режиме не производится.

Capture packets in promiscuous mode - захват пакетов в "неразборчивом" режиме (отключается фильтр на собственный MAC адрес на сетевом адаптере). В настоящее время используется для PPPoE Guard и захвата Multicast фреймов.

Fake MAC type - тип обманного (фальшивого) MAC адреса. Может принимать два значения: *Random* или *Manual*. При типе *Random* MAC адрес генерируется автоматически, случайным образом. *Manual* - ручное задание адреса. Рекомендуемый тип - *Random*.

Fake MAC - задается вручную (при **Fake MAC type** = *Manual*). Может использоваться для специфических целей (допустим для перехвата пакетов от нелегитимных узлов с целью анализа).

Ethers.cfg reload - время автоматической перезагрузки файла конфигурации сети в случае его изменения, задается в минутах. При перезагрузке конфигурации очищается черный список Broadcast Guard и очищается Log-буфер. При задании 0 перезагрузка отключается.

Log level - уровень детализации лог-файла:

- *Log level 1* - в лог-файл пишутся только уникальные за определенное время записи. Время задается в параметре **Rotation Time**, в минутах. По истечении данного времени буфер, в котором запоминаются уникальные записи, очищается. Например: если **Rotation time** = 60 min и пользователь запускает запрещенный чат три раза подряд, то в лог-файле появится запись только о первом запуске. По прошествии 60 минут лог-буфер очистится и, если пользователь снова запустил чат - данный факт снова отразится в логе. Данный уровень детализации рекомендуется использовать только после полной настройки и тестирования программы;
- *Log level 2* - в лог файл пишутся абсолютно все записи. При данном уровне дета-

лизации размер лог-файла может быстро расти.

6.2 Опции MAC/IP Guard

Enable MAC/IP Guard - включение режима MAC/IP Guard.

MAC/IP Guard (стражник) следит за адресным пространством сети. В зависимости от конфигурации сети (ethers.cfg) стражник либо разрешает использование данных адресов, либо запрещает (блокирует), либо восстанавливает правильные соответствия адресов в случае обнаружения ARP атак (Anti ARP Spoofing).

Max RTT, msec - (Maximum Round Trip Time) максимальное время оборота - это максимальное время транспортировки данных от узла отправителя до узла назначения и обратно с учетом времени, затраченного узлом назначения на подготовку ответа. Данный параметр определяет максимальное время оборота между самыми удаленными узлами сегмента, задается в миллисекундах. Очень грубо данное время можно измерить стандартной командой ping (ICMP ping), более точно - arpping (ARP ping). Измерения необходимо производить в наиболее загруженное время. При измерениях с помощью ICMP ping рекомендуется выставить среднее значение, при ARP ping - максимальное. Значение по умолчанию - 20 миллисекунд, подходит для большинства FastEthernet сетей.

Add IP/Gateway Spoofing - для нелегитимных узлов включает дополнительное блокирование заданных IP адресов/шлюзов. В **IP/Gateway List** прописываются необходимые адреса или шлюзы. Если в сети имеется шлюз доступа в Интернет, либо в другую подсеть - то его следует добавить в список. Данное, дополнительное блокирование "действует" только на те узлы, которые в настоящий момент включены и их требуется заблокировать от сети как можно быстрей.

Enable ARP Server - включчение функции интеллектуального ARP сервера.

Интеллектуальный ARP сервер отвечает только на легитимные запросы и посылает только легитимные ответы (в контексте данной, конкретной ситуации и конфигурации сети).

При запуске программы из файла конфигурации сети (ethers.cfg) загружается первоначальная конфигурация для ARP сервера. В дальнейшем происходит процесс обучения ARP сервера: все ARP запросы анализируются на "легитимность" (в соответствии с заданной конфигурацией сети) и, если запрос является легитимным - ARP сервер добавляет данное соответствие в свою базу для дальнейших ответов.

При запросе ARP сервер сначала анализирует легитимность запроса. Если запрос легитимный - то просматривается база легитимных ответов. Если на данный запрос существует легитимный ответ - сервер отвечает на этот запрос. Если запрос нелегитимный, либо в базе сервера нет легитимного ответа - ARP сервер не отвечает.

В отличии от классического ARP сервера, который отвечает на все запросы и только тогда, когда администратор явно указал соответствие, интеллектуальный ARP сервер сначала проводит анализ запроса и ответа (являются ли они легитимными в данный момент) и способен обучаться конфигурации сети в разрешенных администратором рамках (ethers.cfg).

Включение данной функции совместно с MAC/IP Guard повысит безопасность сети и позволит противостоять некоторым видам ARP атак.

6.3 Опции Broadcast Guard

Enable Broadcast Guard - включить режим контроля широковещательных пакетов. В настоящее время контролируются только широковещательные UDP пакеты.

Check Multicast packets - включить проверку Multicast пакетов (например при запрете Multicast чатов).

Ports list - список портов. Данный список может быть двух видов: список запрещенных (*deny*) портов и список разрешенных (*allow*) портов.

List type - тип списка: *Deny* - запрещенный, *Allow* - разрешенный.

Кнопки Add, Delete - для добавления/удаления порта из списка.

Пример1: Необходимо запретить пользователям Vypress и BorgChat. Для этого необходимо поставить тип списка *Deny* и добавить порты 8167 и 7550 для Vypress и BorgChat соответственно. Все остальные широковещательные UDP сервисы разрешены.

Пример2: Необходимо разрешить пользователям только Netbios протокол (Microsoft Networks) и BorgChat. Необходимо поставить тип списка *Allow* и добавить порты 138 и 7550. Все остальные широковещательные UDP сервисы (включая всевозможные чаты и т.д.) запрещены.

Block type - тип блокирования. В настоящий момент может принимать два значения: *Time Spoofing* и *802.3x Flow Control*.

Time Spoofing - Double-sided ARP spoofing на необходимое время. Принцип действия: узел, на котором установлено запрещенное приложение помещается в черный список на заданное в **Block time** время. Все обращения данного узла к дугим, либо любого другого узла к данному блокируются. Если по истечении времени блокирования данный узел не завершит выполнение запрещенного приложения - время блокирования автоматически устанавливается на значение заданное в **Block time**, счетчик снова начинает идти с нуля. Как только пользователь завершает выполнение запрещенного приложения, так по истечении времени **Block time** блокирование прекращается.

802.3x Flow Control - данный вид блокирования является наиболее эффективным методом, сетевой адаптер блокируемого узла должен поддерживать функции управления потоком (почти все современные сетевые адаптеры). При данном виде блокирования может наблюдаться небольшая загрузка сегмента.

Block time - время блокирования. Для *Time Spoofing* задается в часах, для 802.3x

Flow Control - в минутах.

6.4 Опции PPPoE Guarg

Enable PPPoE Guard - включить режим контроля/запрета использования PPPoE сервисов.

AC List - список PPPoE концентраторов. Должен присутствовать минимум один концентратор. Список всех доступных PPPoE концентраторов можно получить с помощью программы «PPPoE Monitor».

AC Spoof time - время спуфинга (MAC Spoofing) коммутаторов, расположенных на пути к концентратору. Задается в секундах.

AC Spoof PPS - количество пакетов в секунду. Данное значение зависит от загруженности сегмента. Необходимо подбирать экспериментально. Слишком большое значение может оказывать некоторую нагрузку на сегмент.

Kill only spoofing sessions - завершать только те сессии, которые действительно были перехвачены спуфингом. Отключение этой опции будет завершать абсолютно все сессии узлов которых нет в ethers.cfg. Такое может произойти в следствии неправильной настройки оборудования со стороны провайдера. Рекомендуется всегда включать данную опцию.

7 Файл конфигурации ethers.cfg

В файле конфигурации ethers.cfg описываются узлы контролируемого сегмента.

Формат файла ethers.cfg:

MAC-адрес IP-адрес [Тип записи] [Текстовое описание]

Поля в [ ] скобках не обязательны.

Синтаксис полей

MAC адрес:

1) 00:01:02:03:04:05 - заданный MAC адрес;
2) * - любой MAC адрес;
3) $ - Learning MAC. Принцип работы похож на функцию коммутаторов MAC Learning. В файл конфигурации на место знака $ автоматически прописывается первый MAC адрес, соответствующий заданному IP адресу.

IP-адрес:

1) 192.168.1.1 - заданный IP адрес;
2) 192.168.1.0/24 - заданная подсеть 192.168.1.0/255.255.255.0 (192.168.1.0-192.168.1.255);

3) 192.168.1.1-192.168.1.100 - заданный диапазон;
4) * - любой IP адрес.

Тип записи:

1) 0 - данный узел, либо подсеть, либо диапазон блокирован;
2) 1 - данный узел, либо подсеть, либо диапазон разрешен;
3) 2 - для данного узла, либо подсети, либо диапазона блокирован только PPPoE (L2);
4) 3 - для данного узла, либо подсети, либо диапазона будет производиться контроль широковещательных пакетов (фукнция Broadcast Guard). Если в файле конфигурации хоть один раз указан тип записи «3», то проверка широковещательных пакетов будет производиться только для соответствующих записей. Если тип записи «3» не указан ни разу, и функция Broadcast Guard включена – то контроль широковещательных пакетов будет производиться для всей сети, а не для отдельно взятых адресов.
5) пустое поле - значение по умолчанию 1

Текстовое описание:

1) либо пустое поле, либо любой текст.

Файл конфигурации читается сверху вниз, символ '#' является комментарием. Порядок следования различного типа записей неважен.

Поиск производится в следующей последовательности:

1) соответствия MAC/IP;
2) соответствия $/IP;
3) соответствия MAC/Диапазон(подсеть);
4) соответствия MAC/*;
5) соответствия */IP;
6) соответствия */Диапазон(подсеть);
7) соответствия */*.

Если в конфигурации присутствуют не все типы записей - то поиск производится только по заданным типам (например: в конфигурации заданы только соответствия MAC/IP - поиск будут производиться только по первому пункту).

Пример: имеем локальную сеть 192.168.1.0/24, возможные конфигурации:

1) полное описание сети:

```
00:11:2f:14:13:8d    192.168.1.2 # Свой MAC и IP
00:c0:26:a7:c6:49    192.168.1.1 # Сервер
00:60:08:bd:63:6b    192.168.1.6 #
00:c0:26:72:df:92    192.168.1.6 # данный IP может иметь два MAC
00:30:84:89:14:b1    192.168.1.9 # IP1 Данный MAC может иметь несколько IP
00:30:84:89:14:b1    192.168.1.10 # IP2
00:30:84:89:14:b1    192.168.1.11 # IP3
00:30:84:89:14:b1    192.168.1.12 # IP4
00:13:d4:e7:42:76         *      # Этот MAC может иметь любой IP
      *              192.168.1.4 # Этот IP может иметь любой MAC
# и т.д.
```

2) блокирование одного узла без полного описания сети:

```
00:11:2f:14:13:8d    192.168.1.2          # Свой MAC и IP
00:c0:26:a7:c6:49    192.168.1.1          # Сервер
00:13:d4:e7:42:76    192.168.1.10    0    # Указываем тип 0 (болокирован)
       *                  *              # Все остальные узлы разрешены
```

В данном случае узлу, который необходимо отключить (заблокировать) необходимо указать тип записи «0».

3) разрешить пользователям назначать адреса только из определенного диапазона:

```
      *            192.168.1.1-192.168.1.254    1    # Указываем тип 1 (разрешен)
      *                  *                      0    # Указываем тип 0 (блокирован)
```

В типичной конфигурации, например для домовой сети, прописываются жесткие соответствия MAC и IP адресов. Для подключения нового пользователя к сети необходимо прописать его конфигурацию (соответствие MAC/IP) в ethers.cfg, для отключения (например за неуплату) - удалить его соответствие либо изменить тип его MAC/IP пары на '0'.

Для облегчения создания файла конфигурации можно использовать MAC Learning. Для этого необходимо прописать весь диапазон используемых (разрешенных) адресов сети с указанием в поле MAC адреса знака «$»:

```
00:01:02:03:04:05    192.168.1.1 # Сервер L2NG
$    192.168.1.2 # Пользователь 1
$    192.168.1.3 # Пользователь 2
$    192.168.1.4 # Пользователь 3
$    192.168.1.5 # Пользователь 4
$    192.168.1.6 # Пользователь 5
$    192.168.1.7 # Пользователь 6
$    192.168.1.8 # Пользователь 7
# и т.д.
```

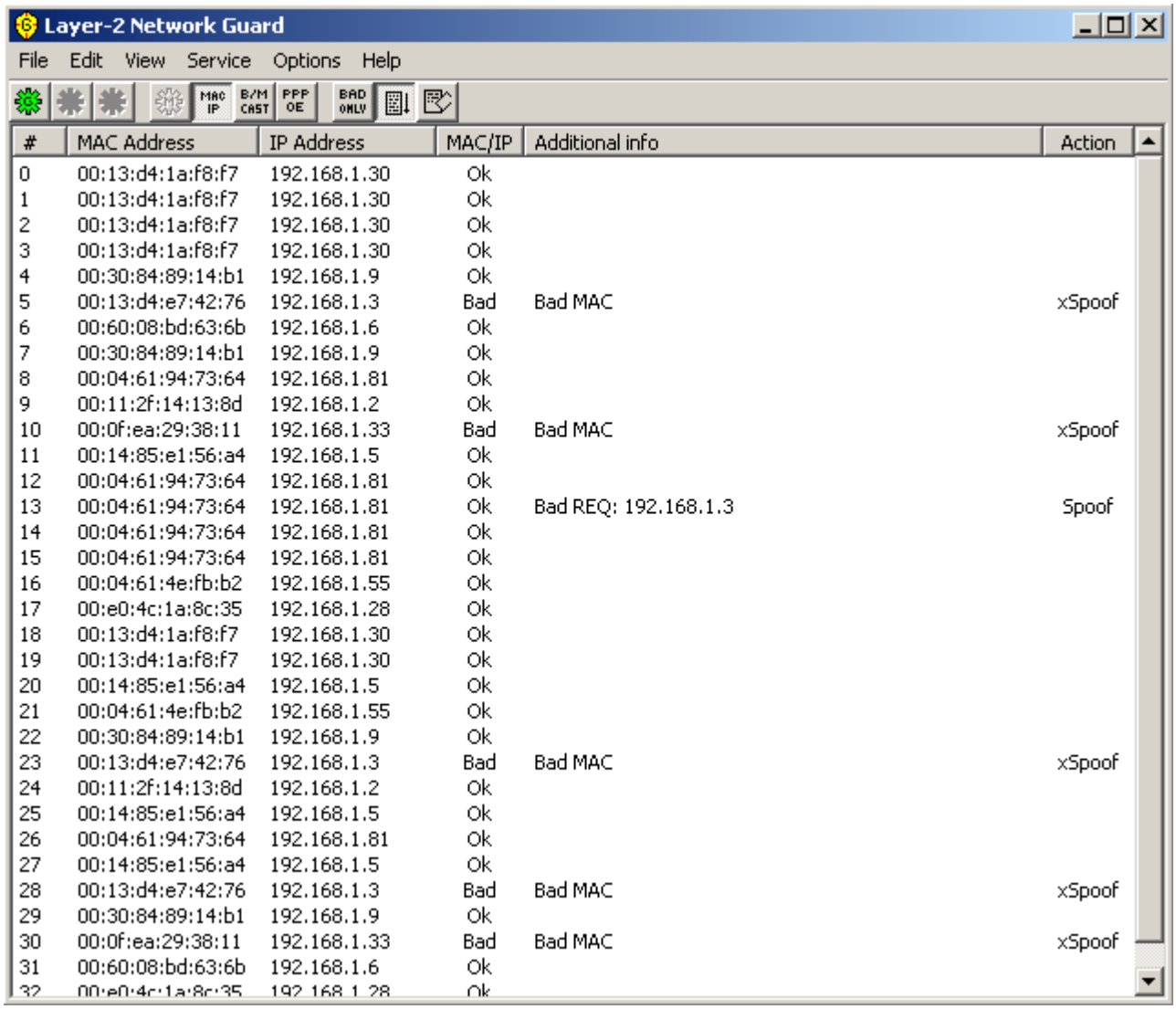
После запуска L2NG начнет «изучать» сеть и прописывать на место «$» найденные MAC адреса. Прописывается первый найденный MAC адрес соответствующий указанному IP адресу в конфигурации (MAC/IP пара).

MAC Learning так же удобно использовать при подключении новых пользователей.

Обучаемый MAC адрес «$» возможен только для конкретно заданного IP адреса. Для подсетей, диапазонов адресов или «любых» («*») IP указание знака «$» в поле MAC адреса недопустимо и будет пропущено при парсинге файла конфигурации.

8 Пример работы MAC/IP Guard

На рис.2 показан результат работы MAC/IP Guard. IP адрес 192.168.1.3 отключен, все остальные узлы разрешены.



#	MAC Address	IP Address	MAC/IP	Additional info	Action
0	00:13:d4:1a:f8:f7	192.168.1.30	Ok		
1	00:13:d4:1a:f8:f7	192.168.1.30	Ok		
2	00:13:d4:1a:f8:f7	192.168.1.30	Ok		
3	00:13:d4:1a:f8:f7	192.168.1.30	Ok		
4	00:30:84:89:14:b1	192.168.1.9	Ok		
5	00:13:d4:e7:42:76	192.168.1.3	Bad	Bad MAC	xSpoof
6	00:60:08:bd:63:6b	192.168.1.6	Ok		
7	00:30:84:89:14:b1	192.168.1.9	Ok		
8	00:04:61:94:73:64	192.168.1.81	Ok		
9	00:11:2f:14:13:8d	192.168.1.2	Ok		
10	00:0f:ea:29:38:11	192.168.1.33	Bad	Bad MAC	xSpoof
11	00:14:85:e1:56:a4	192.168.1.5	Ok		
12	00:04:61:94:73:64	192.168.1.81	Ok		
13	00:04:61:94:73:64	192.168.1.81	Ok	Bad REQ: 192.168.1.3	Spoof
14	00:04:61:94:73:64	192.168.1.81	Ok		
15	00:04:61:94:73:64	192.168.1.81	Ok		
16	00:04:61:4e:fb:b2	192.168.1.55	Ok		
17	00:e0:4c:1a:8c:35	192.168.1.28	Ok		
18	00:13:d4:1a:f8:f7	192.168.1.30	Ok		
19	00:13:d4:1a:f8:f7	192.168.1.30	Ok		
20	00:14:85:e1:56:a4	192.168.1.5	Ok		
21	00:04:61:4e:fb:b2	192.168.1.55	Ok		
22	00:30:84:89:14:b1	192.168.1.9	Ok		
23	00:13:d4:e7:42:76	192.168.1.3	Bad	Bad MAC	xSpoof
24	00:11:2f:14:13:8d	192.168.1.2	Ok		
25	00:14:85:e1:56:a4	192.168.1.5	Ok		
26	00:04:61:94:73:64	192.168.1.81	Ok		
27	00:14:85:e1:56:a4	192.168.1.5	Ok		
28	00:13:d4:e7:42:76	192.168.1.3	Bad	Bad MAC	xSpoof
29	00:30:84:89:14:b1	192.168.1.9	Ok		
30	00:0f:ea:29:38:11	192.168.1.33	Bad	Bad MAC	xSpoof
31	00:60:08:bd:63:6b	192.168.1.6	Ok		
32	00:e0:4c:1a:8c:35	192.168.1.28	Ok		

Рис.2 Результат работы MAC/IP Guard

По результатам видно, что заблокировано несколько запросов с IP 192.168.1.3. Так же заблокирован запрос с IP 192.168.1.81 т.к. данный узел пытался резрешить (ARP Request) MAC адрес отключенного IP.

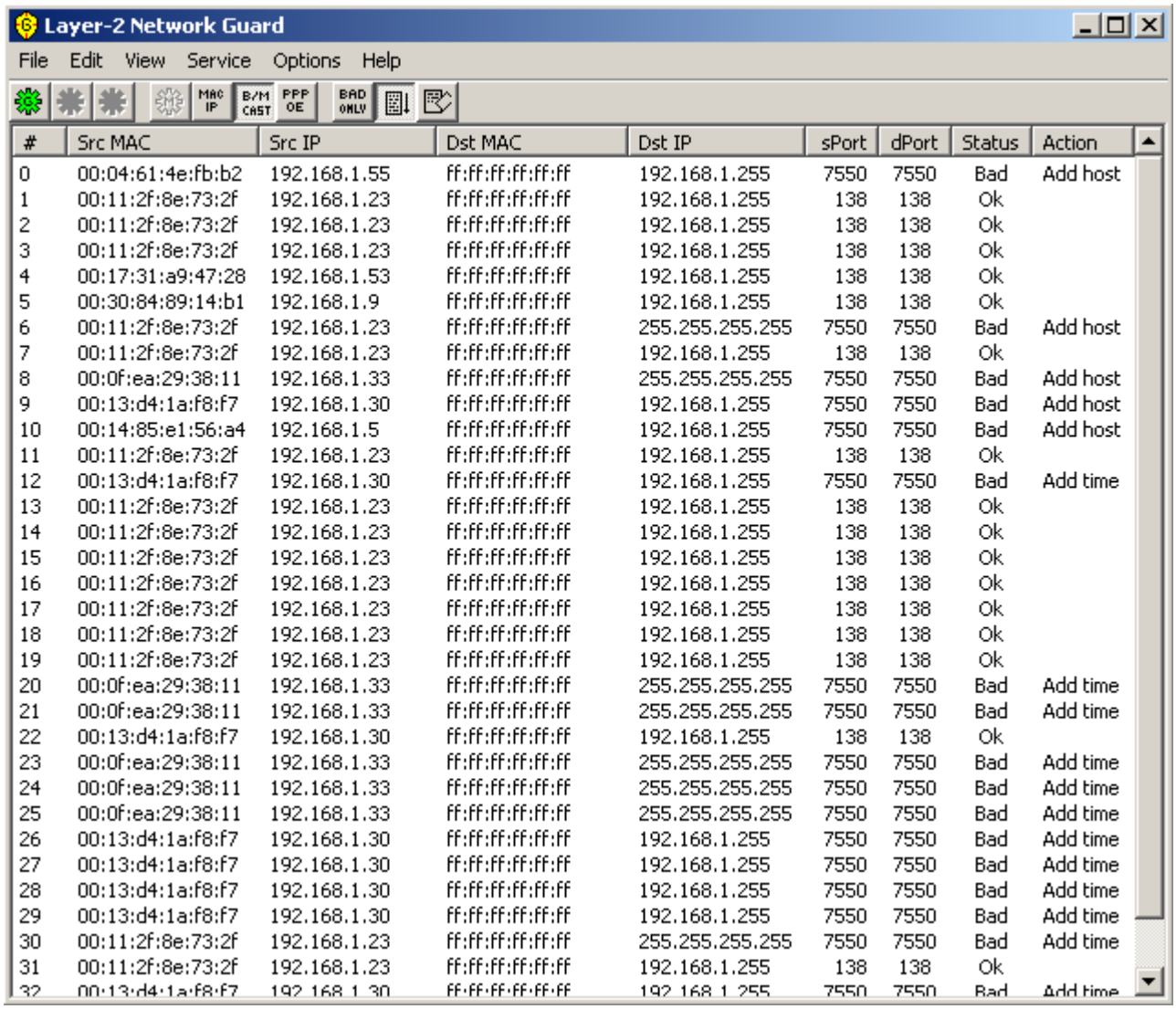
Поле **MAC/IP** может принимать три значения: *BAD* – неверное соответствие (неверный MAC либо неверный IP), *OK* – верное сооветствие и *Learn* – обучение (программа записала в файл конфигурации соответствующий MAC адрес).

Поле **Additional info** содержит дополнительные сведения, какой из адресов неверный (MAC или IP) и запрашиваемый адрес, в случае если запрашивается (ARP Request) запрещенный (нелегитимный) адрес.

Поле **Action** может принимать два значения: *xSpoof* - Double-sided ARP spoofing, *Spoof* - One-sided ARP Spoofing.

9 Пример работы Broadcast Guard

На рис.3 проказан результат запрета BorgChat в сети. Тип блокирования *Time Spoofing*. В данной, конеретной сети BorgChat установлен на каждом компьютере, поэтому в черный список добавляются все узлы.



#	Src MAC	Src IP	Dst MAC	Dst IP	sPort	dPort	Status	Action
0	00:04:61:4e:fb:b2	192.168.1.55	ff:ff:ff:ff:ff:ff	192.168.1.255	7550	7550	Bad	Add host
1	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
2	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
3	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
4	00:17:31:a9:47:28	192.168.1.53	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
5	00:30:84:89:14:b1	192.168.1.9	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
6	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	255.255.255.255	7550	7550	Bad	Add host
7	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
8	00:0f:ea:29:38:11	192.168.1.33	ff:ff:ff:ff:ff:ff	255.255.255.255	7550	7550	Bad	Add host
9	00:13:d4:1a:f8:f7	192.168.1.30	ff:ff:ff:ff:ff:ff	192.168.1.255	7550	7550	Bad	Add host
10	00:14:85:e1:56:a4	192.168.1.5	ff:ff:ff:ff:ff:ff	192.168.1.255	7550	7550	Bad	Add host
11	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
12	00:13:d4:1a:f8:f7	192.168.1.30	ff:ff:ff:ff:ff:ff	192.168.1.255	7550	7550	Bad	Add time
13	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
14	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
15	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
16	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
17	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
18	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
19	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
20	00:0f:ea:29:38:11	192.168.1.33	ff:ff:ff:ff:ff:ff	255.255.255.255	7550	7550	Bad	Add time
21	00:0f:ea:29:38:11	192.168.1.33	ff:ff:ff:ff:ff:ff	255.255.255.255	7550	7550	Bad	Add time
22	00:13:d4:1a:f8:f7	192.168.1.30	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
23	00:0f:ea:29:38:11	192.168.1.33	ff:ff:ff:ff:ff:ff	255.255.255.255	7550	7550	Bad	Add time
24	00:0f:ea:29:38:11	192.168.1.33	ff:ff:ff:ff:ff:ff	255.255.255.255	7550	7550	Bad	Add time
25	00:0f:ea:29:38:11	192.168.1.33	ff:ff:ff:ff:ff:ff	255.255.255.255	7550	7550	Bad	Add time
26	00:13:d4:1a:f8:f7	192.168.1.30	ff:ff:ff:ff:ff:ff	192.168.1.255	7550	7550	Bad	Add time
27	00:13:d4:1a:f8:f7	192.168.1.30	ff:ff:ff:ff:ff:ff	192.168.1.255	7550	7550	Bad	Add time
28	00:13:d4:1a:f8:f7	192.168.1.30	ff:ff:ff:ff:ff:ff	192.168.1.255	7550	7550	Bad	Add time
29	00:13:d4:1a:f8:f7	192.168.1.30	ff:ff:ff:ff:ff:ff	192.168.1.255	7550	7550	Bad	Add time
30	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	255.255.255.255	7550	7550	Bad	Add time
31	00:11:2f:8e:73:2f	192.168.1.23	ff:ff:ff:ff:ff:ff	192.168.1.255	138	138	Ok	
32	00:13:d4:1a:f8:f7	192.168.1.30	ff:ff:ff:ff:ff:ff	192.168.1.255	7550	7550	Bad	Add time

Рис.3 Результат работы Broadcast Guard

В сети разрешен Netbios, поставлен запрет только на порт 7550 (BorgChat). Поле **Action** может принимать два значения: *Add host* - узел добавляется в черный список (с этого момента начинается его блокирование) и *Add time* - для данного узла увеличивается время блокирования.

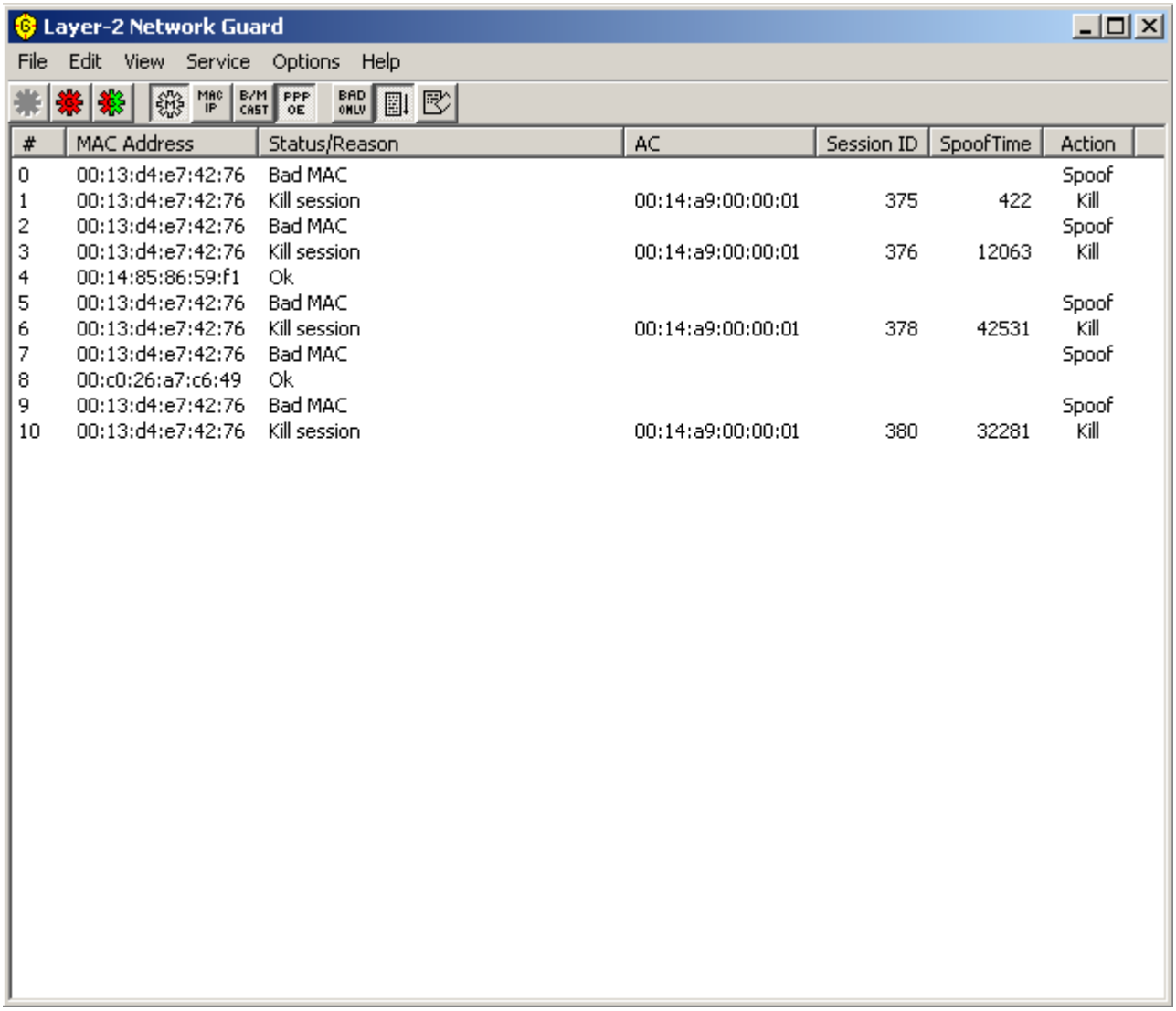
При типе блокирования *802.3x Flow Control* - у большинства записей поле **Action** будет *Add host*, т.к. при данном блокировании передача любых данных в сеть заблокированным узлом невозможна.

Перед использованием Broadcast Guard в домовых сетях рекомендуется сначала предупредить всех пользователей о запрете, допустим чата. Компьютеры пользователей с запрещенными приложениями (чатами и т.д.) будут полностью заблокированы до тех пор, пока пользователь не отключит чат и не пройдет время **Block Time** после последнего включения.

Особенностью запрета широковещательных сервисов является то, что блокируется не сам сервис (чат в данном случае), а **полностью компьютер пользователя**.

10 Пример работы PPPoE Guard

На рис.4 показан результат работы PPPoE Guard. В данном примере узлу с MAC адресом 00:13:e4:e7:42:76 запрещено пользоваться PPPoE сервисами (подключаться к провайдеру интернет), всем остальным узлам разрешено.



#	MAC Address	Status/Reason	AC	Session ID	SpoofTime	Action
0	00:13:d4:e7:42:76	Bad MAC				Spoof
1	00:13:d4:e7:42:76	Kill session	00:14:a9:00:00:01	375	422	Kill
2	00:13:d4:e7:42:76	Bad MAC				Spoof
3	00:13:d4:e7:42:76	Kill session	00:14:a9:00:00:01	376	12063	Kill
4	00:14:85:86:59:f1	Ok				
5	00:13:d4:e7:42:76	Bad MAC				Spoof
6	00:13:d4:e7:42:76	Kill session	00:14:a9:00:00:01	378	42531	Kill
7	00:13:d4:e7:42:76	Bad MAC				Spoof
8	00:c0:26:a7:c6:49	Ok				
9	00:13:d4:e7:42:76	Bad MAC				Spoof
10	00:13:d4:e7:42:76	Kill session	00:14:a9:00:00:01	380	32281	Kill

Рис. 4 Результат работы PPPoE Guard

Поле **AC** - концентратор доступа, к которому подключался пользователь.

Поле **Session ID** – идентификатор принудительно завершенной сессии данного пользователя.

Поле **SpoofTime** - время MAC Spoofing (коммутационных таблиц концентраторов) в миллисекундах.

Поле **Action** может принимать два значения: **Spoof** - начало процесса спуфинга, **Kill** - принудительное завершение сессии.

При отключении заблокированного узла появление записи о принудительном завершении сессии не является обязательным, т.к. заблокированный узел может не перейти на стадию Session PPPoE протокола, либо процесс хендшейка вообще зависнет.

Для правильной работы PPPoE Guard необходим точно заданный MAC адрес PPPoE концентратора провайдера.

11 Автономный режим работы сервиса

После необходимой настройки сервисной части и тестирования работы L2NG с помощью GUI клиента (l2ng.exe) тип запуска сервиса можно изменить на Авто. Сервисная часть будет работать автономно с указанными настроками и автоматически запускаться при загрузке компьютера.

Все сообщения сервисной части записываются в лог файл l2ng.log. Пример лог-файла:

```
2006.11.16 16:48:37 *** Layer-2 Network Guard v-0.2 ***
2006.11.16 16:48:37 * Ethernet adapter:  Registered
2006.11.16 16:48:37 * MAC/IP Guard: Enable
2006.11.16 16:48:37 * Broadcast Guard:   Enable
2006.11.16 16:48:37 * PPPoE Guard:  Enable
2006.11.16 16:48:37 * ReadOnly mode:     Disable
2006.11.16 16:48:37 INFO: loaded 32 MAC/IP pairs
2006.11.16 16:50:01 MAC/IP: Bad MAC: 00:13:d4:e7:42:76 192.168.1.3
2006.11.16 16:50:01 MAC/IP: Bad MAC: 00:0f:ea:29:38:11 192.168.1.33
2006.11.16 16:53:55 BCAST: Bad Port: 00:04:61:4e:fb:b2 192.168.1.55: -> 7550
2006.11.16 16:54:10 BCAST: Block: 00:04:61:4e:fb:b2 192.168.1.55
2006.11.16 16:54:10 BCAST: Block: 00:04:61:4e:fb:b2 192.168.1.55
2006.11.16 16:54:29 BCAST: Bad Port: 00:11:2f:8e:73:2f 192.168.1.23: -> 7550
2006.11.16 16:54:29 BCAST: Bad Port: 00:0f:ea:29:38:11 192.168.1.33: -> 7550
2006.11.16 16:54:29 BCAST: Bad Port: 00:13:d4:1a:f8:f7 192.168.1.30: -> 7550
2006.11.16 16:54:30 BCAST: Bad Port: 00:14:85:e1:56:a4 192.168.1.5: -> 7550
2006.11.16 17:27:35 PPPoE: Bad MAC: 00:13:d4:e7:42:76
2006.11.16 17:27:35 PPPoE: Kill Session_ID: 375 Host: 00:13:d4:e7:42:76 AC:
00:14:a9:00:00:01 SpoofTime: 422 ms
2006.11.16 17:28:20 PPPoE: Bad MAC: 00:13:d4:e7:42:76
2006.11.16 17:28:32 PPPoE: Kill Session_ID: 376 Host: 00:13:d4:e7:42:76 AC:
00:14:a9:00:00:01 SpoofTime: 12063 ms
2006.11.16 17:29:06 PPPoE: Bad MAC: 00:13:d4:e7:42:76
2006.11.16 17:29:48 PPPoE: Kill Session_ID: 378 Host: 00:13:d4:e7:42:76 AC:
00:14:a9:00:00:01 SpoofTime: 42531 ms
```

В лог файле отражаются все события по блокированию узлов в зависимости от включенной детализации (**Log level**), включенные режимы работы сервиса и информация о регистрации.

12 Правовые аспекты использования L2NG

L2NG предназначен исключительно для целей управления, администрирования, мониторинга и изучения сетей.

Во избежании использовании программы в корыстных и иных вредительских целях бесплатная версия распространяется с урезанным кодом. В данной версии не присутствует реального блокирующего кода, однако доступны абсолютно все функции, позволяющие вести контроль и мониторинг сети.

Полнофункциональная версия с блокирующим кодом не распространяется свободно. Каждая копия программы привязывается только к одному сетевому интерфейсу, указанному при регистрации, и высылается лично автором.

Перед использованием полнофункциональной версии программы следует ознакомиться с выдержкой из Уголовного Кодекса:

Выдержка из **Уголовного Кодекса Российской Федерации**:

Глава 28. Преступления в сфере компьютерной информации

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторжности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Автор снимает с себя всю ответственность за любые последствия при использовании данного программного обеспечения.

Лицензионное соглашение прилагается к ПО.

13 Лицензионное соглашение

```
/* Layer-2 Network Guard
*
* Copyright (C) 2006-2007 Alexander A. Burylov
*
* ПРИ ИСПОЛЬЗОВАНИИ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ССЫЛОК,
* ОБЗОРОВ И ПРОЧИХ УПОМИНАНИЙ О ДАННОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ ДОЛЖНЫ
* СОБЛЮДАТЬСЯ СЛЕДУЮЩИЕ УСЛОВИЯ:
*
* 1. ЗАПРЕЩЕНО ИЗМЕНЕНИЕ И ДОБАВЛЕНИЕ КАКИХ-ЛИБО ФАЙЛОВ ВХОДЯЩИХ В СОДЕРЖИМОЕ
* ОРИГИНАЛЬНОГО АРХИВА;
* 2. ЗАПРЕЩЕНА ДЕКОМПИЛЯЦИЯ, ОТЛАДКА, ИЗМЕНЕНИЕ АЛГОРИТМОВ И ПРОЧИЕ
* ВМЕШАТЕЛЬСТВА ВО ВРЕМЯ РАБОТЫ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ;
* 3. ПРИ ОБЗОРАХ, ССЫЛКАХ И ПРОЧИХ ОФИЦИАЛЬНЫХ УПОМИНАНИЯХ О ДАННОМ
* ПРОГРАММНОМ ОБЕСПЕЧЕНИИ ДОЛЖНЫ СОБЛЮДАТЬСЯ АВТОРСКИЕ ПРАВА НА ДАННОЕ
* ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ С УКАЗАНИЕМ АВТОРА;
* 4. ИМЯ АВТОРА НЕ МОЖЕТ ИСПОЛЬЗОВАТЬСЯ ДЛЯ КОММЕРЧЕСКОЙ ИЛИ ЛЮБОГО ДРУГОГО
* ВИДА ДЕЯТЕЛЬНОСТИ БЕЗ ПИСЬМЕННОГО РАЗРЕШЕНИЯ АВТОРА.
*
* ОТСУТСТВИЕ ГАРАНТИЙ И ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ:
* ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ ВАМ НА ПРИНЦИПЕ <КАК ЕСТЬ>, И АВТОР
* НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ ОТНОСИТЕЛЬНО ЕГО ИСПОЛЬЗОВАНИЯ ИЛИ РАБОЧИХ
* ХАРАКТЕРИСТИК. АВТОР НЕ ГАРАНТИРУЕТ И НЕ МОЖЕТ ГАРАНТИРОВАТЬ РАБОЧИЕ
* ХАРАКТЕРИСТИКИ И РЕЗУЛЬТАТЫ, КОТОРЫЕ МОГУТ БЫТЬ ПОЛУЧЕНЫ ВАМИ ПРИ
* ИСПОЛЬЗОВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. АВТОР НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, НЕ
* УСТАНАВЛИВАЕТ УСЛОВИЙ, НЕ ДЕЛАЕТ НИКАКИХ ЗАЯВЛЕНИЙ, НИ ПРЯМО ВЫРАЖЕННЫХ, НИ
* ПОДРАЗУМЕВАЕМЫХ, ПО ЗАКОНУ, ОБЩЕМУ ПРАВУ, ОБЫЧАЮ, ПРАКТИКЕ ИЛИ ИНЫМ ОБРАЗОМ
* В ОТНОШЕНИИ КАКИХ БЫ ТО НИ БЫЛО ВОПРОСОВ, ВКЛЮЧАЯ, НО, НЕ ОГРАНИЧИВАЯСЬ
* ТОЛЬКО ЭТИМ, НЕНАРУШЕНИЕ ПРАВ ТРЕТЬИХ ЛИЦ, УДОВЛЕТВОРИТЕЛЬНОЕ КАЧЕСТВО ИЛИ
* ПРИГОДНОСТЬ ДЛЯ ЛЮБОЙ КОНКРЕТНОЙ ЦЕЛИ. АВТОР НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ
* НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД ВАМИ ЗА КАКОЙ БЫ ТО НИ БЫЛО УЩЕРБ, ПРЕТЕНЗИИ ИЛИ
* РАСХОДЫ, РАВНО КАК И В СВЯЗИ С КАКИМ БЫ ТО НИ БЫЛО КОСВЕННЫМ ИЛИ СЛУЧАЙНЫМ
* УЩЕРБОМ, УПУЩЕННОЙ ВЫГОДОЙ, УТРАТОЙ СБЕРЕЖЕНИЙ, НАРУШЕНИЕМ РАБОТЫ СЕТЕЙ ИЛИ
* ЛЮБОГО ДРУГОГО ОБОРУДОВАНИЯ, А ТАКЖЕ ПО ЛЮБЫМ ПРЕТЕНЗИЯМ КАКИХ БЫ ТО НИ БЫЛО
* ТРЕТЬИХ ЛИЦ.
* В СЛУЧАЕ НЕСОГЛАСИЯ С ДАННЫМ ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ ИЛИ КАКОЙ-ТО
* ЕГО ЧАСТЬЮ, КАКИМ БЫ ТО НИ БЫЛО СПОСОБОМ ИСПОЛЬЗОВАТЬ ИЛИ ХРАНИТЬ ДАННОЕ
* ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫ НЕ ИМЕЕТЕ ПРАВА.
*
*/
```

14 Контакты

Основной сайт программы: http://l2nt.info

Техническая поддержка: support@l2nt.info

По вопросам приобретения полнофункциональной (лицензионной) версии L2NG необходимо обращаться по адресу: support@l2nt.info

Принимаются все вопросы, замечания, пожелания, запрос новых возможностей и т.д.