PCAP-фильтры

Содержание

- Описание
- Примитивы
- Примеры

Описание

В текстовом виде PCAP-фильтр выглядит как выражение, состоящее из одного или нескольких примитивов. Примитивы в выражении определяют возможность приема фильтром входящего пакета. Каждый примитив определяет конкретный элемент пакета протокола стандартной структуры и его значение, сравниваемое фильтром со значением соответствующего элемента входящего пакета. Если значение примитива совпадает со значением элемента пакета, фильтр отмечает его как "логическую истину" (true) и переходит к сравнению следующего примитива. При совпадении всех значений выражения со значениями проверенных элементов пакета фильтр принимает решение о приеме данного пакета, в противном случае входящий пакет игнорируется.

Каждый примитив обычно состоит из одного или нескольких квалификаторов и следующего за ними идентификатора (имя или число). Всего имеется три типа квалификаторов:

- *"type"* – определяет тип имени или номера идентификатора. Возможные значения: "*host*" (хост), *"net"* (сеть), *"port"* (порт) или *"portrange"* (диапазон портов). Если квалификатор отсутствует, по умолчанию принимается *"host"*.
- *"dir"* – определяет возможное направление приема и передачи данных объектом, указанным в качестве идентификатора: к нему и/или от него. Допускается указание следующих значений: *"src"* (отправитель), *"dst"* (получатель), *"src and dst"* (отправитель и получатель), *"src or dst"* (отправитель или получатель). Если квалификатор не указан, по умолчанию принимается *"src or dst"*.
- *"proto"* – определяет тип протокола, используемого объектом, указанным в качестве идентификатора. Возможные значения: *"ether", "fddi", "ip", "arp", "rarp", "decnet", "lat", "sca", "moprc", "mopdl", "tcp"* и *"udp"*. При отсутствии квалификатора значение по умолчанию выбирается по максимальному соответствию указанному идентификатору.

Стоит отметить, что существуют некоторые специальные примитивы, которые не соответствуют шаблону: *"broadcast", "less", "greater"*, а также арифметические выражения. Подробное описание приведено ниже.

Более сложные выражения фильтра создаются с использованием слов *"and", "or"* и *"not"* для объединения примитивов. Примитивы можно группировать с помощью скобок и логических операций:

- отрицание ("!" или *"not"*);
- сложение ("&&" или "and");
- дизъюнкция ("||" или "or").

Отрицание имеет самый высокий приоритет. Сложение и дизъюнкция имеют одинаковый приоритет в выражении и читаются слева направо.

> **ВНИМАНИЕ**
>
> Если в фильтре есть несколько одинаковых повторяющихся квалификаторов, то для сокращения записи их можно не писать.

Аббревиатуры *"ip", "arp", "rarp", "atalk", "aarp", "iso", "stp", "ipx", "netbeui"* являются сокращениями для "*ether proto p*", где "*p*" один из указанных протоколов. *"tcp", "udp", "icmp"* являются сокращениями для "*ip proto p*", где "*p*" - один из указанных выше протоколов. "*clnp*", "*esis*", "*isis*" являются сокращениями для *"iso proto p"*, где "*p*" - один из указанных выше протоколов.

Примитивы

Примитив	Описание
dst host HOST	Истинно, если поле IP-пакета "адрес получателя" (IPv4) совпадает со значением идентификатора *"HOST"* (может указываться имя или адрес хоста).
src host HOST	Истинно, если поле IP-пакета "адрес отправителя" совпадает со значением идентификатора *"HOST"*.
host HOST	Истинно, если поле IP-пакета "адрес отправителя", либо поле IP-пакета "адрес получателя" совпадает со значением идентификатора *"HOST"*.

Title

ВНИМАНИЕ

Любое вышеуказанное выражение можно дополнить с помощью префиксов *"ip", "ip6", "arp", "rarp".*

ether dst EHOST	Истинно, если поле "адрес получателя" канального уровня совпадает со значением идентификатора "*EHOST*". *"EHOST"* должен быть представлен в следующем формате: XX:XX:XX:XX:XX:XX.
ether src EHOST	Истинно, если поле "адрес отправителя" канального уровня совпадает со значением идентификатора "*EHOST*".
ether host EHOST	Истинно, если поля "адрес отправителя" или "адрес получателя" канального уровня совпадают со значением идентификатора *"EHOST".*
dst net NET	Истинно, если поле "адрес получателя" заголовка IP-пакета содержит заданный адрес, принадлежащий диапазону указанной сети "*NET*".
src net NET	Истинно, если поле "адрес отправителя" заголовка IP-пакета содержит заданный адрес, принадлежащий диапазону указанной сети "*NET*" .
net NET	Истинно, если поля "адрес отправителя" или "адрес получателя" содержат заданный адрес, принадлежащий диапазону указанной сети "*NET*".
net net mask NETMASK	Истинно, если IP-адрес содержит заданный адрес, принадлежащий диапазону указанной сети *"NET"* с определенной маской *"NETMASK".* Можно дополнить примитивами "*src"* и "*dst".*
net NET/LEN	Истинно, если IP-адрес содержит заданный адрес, принадлежащий диапазону указанной сети *"NET"* с определенной длиной маски *"NET/LEN"*. Можно дополнить примитивами "*src"* и "*dst".*
dst port PORT	Истинно, если порт получателя заголовка UDP или TCP содержит заданный номер порта "*PORT*".
src port PORT	Истинно, если порт отправителя заголовка UDP или TCP содержит заданный номер порта "*PORT*".
port PORT	Истинно, если порт отправителя или получателя заголовка UDP или TCP содержит заданный номер порта "*PORT*".
dst portrange PORT1-PORT2	Истинно, если поле "порт получателя" заголовка UDP или TCP входит в заданный диапазон портов "*PORT1-PORT2*".
src portrange PORT1-PORT2	Истинно, если поле "порт отправителя" заголовка UDP или TCP входит в заданный диапазон портов "*PORT1-PORT2*".
portrange PORT1-PORT2	Истинно, если поля "порт получателя" или "порт отправителя" заголовка UDP или TCP входят в заданный диапазон портов "*PORT1-PORT2*" .

ВНИМАНИЕ

Любые вышеуказанные выражения, связанные с фильтрацией по номеру портов/диапазону портов можно дополнить ключевыми словами "*tcp"* и "*udp",* в этом случае фильтрация будет дополнительно выполняться по значению протокола.

less LENGTH	Истинно, если длина пакета меньше или равна "*LENGTH*". Это аналогично следующему выражению: "*len <= length*".
greater LENGTH	Истинно, если длина пакета больше или равна *"LENGTH"*. Это аналогично следующему выражению: "*len >= length*".
ip proto PROTOCOL	Истинно, если в поле *"PROTOCOL"* заголовка IP-пакета содержится идентификатор указанного протокола. "*PROTOCOL"* - не только численные значения, но и стандартные имена протоколов: *"icmp", "icmp6", "igmp", "igrp", "pim", "ah", "esp", "vrrp", "udp"* или *"tcp"*. Стоит иметь в виду, что символьные имена "*tcp", "udp"* и *"icmp"* также являются ключевыми, и перед ними должен быть помещен символ обратного слэша (\). Обратите внимание, что этот примитив не исследует всю цепочку заголовков протокола.

ip protochain PROTOCOL	Истинно, если пакет является пакетом IPv4 и содержит в цепочке заголовков протоколов заданный протокол "*PROTOCOL*".
ether broadcast	Истинно, если пакет является широковещательным пакетом Ethernet. Ключевое слово "*ether*" может быть опущено.
ether multicast	Истинно, если пакет является пакетом групповой рассылки (или широковещательным) Ethernet. Ключевое слово "*ether*" может быть опущено. Это сокращенная форма записи выражения "*ether[0] & 1 != 0*".
ip multicast	Истинно, если пакет является пакетом групповой рассылки (или широковещательным) в IPv4.
ether proto PROTOCOL	Истинно, если в поле "*protocol*" заголовка пакета содержится идентификатор указанного протокола "*PROTOCOL*". "*PROTOCOL*" может принимать не только численные значения, но и стандартные имена протоколов: *"icmp", "icmp6", "igmp", "igrp", "pim", "ah", "esp", "vrrp", "udp"* или *"tcp"*, но перед ними должен быть помещен символ обратного слэша (\).
svlan [vlan_id]	Истинно, если пакеты соответствуют IEEE 802.1Q с типом Ethernet заголовка 0x88A8. В случае соединения Ethernet ОС проверяет поле типа Ethernet для большинства протоколов. Исключения: • *"iso", "stp"* и *"netbeui"* - ОС проверяет кадр на соответствие стандарту 802.3, а затем проверяет заголовок LLC, как для FDDI, Token Ring и 802.11. • *"atalk"* - на AppleTalk ОС проверяет поле etype в кадре Ethernet, а также, для пакета SNAP-формата, FDDI, Token Ring и 802.11. • *"aarp"* - ОС проверяет на AppleTalk ARP как в кадре Ethernet, так и в стандарте 802.2 SNAP с OUI 0x000000. • *"ipx"* - ОС проверяет на IPX поле etype в кадре Ethernet, IPX DSAP в заголовке LLC, 802.3-без-LLC-заголовка инкапсуляцию IPX и IPX etype в кадре SNAP.
vlan [vlan_id]	Истинно, если пакеты соответствуют IEEE 802.1Q с типом Ethernet заголовка 0x8100. Если указан "*[vlan_id]*", то фильтруются кадры с указанным "*vlan_id*". **ВНИМАНИЕ** Обратите внимание, что выражение "*vlan [vlan_id]*" может использоваться более одного раза для фильтрации по иерархиям VLAN.
mpls [label_num]	Истинно, если пакеты являются пакетами MPLS. Если указана метка MPLS "*[label_num]*", то фильтроваться будут пакеты с указанной "*label_num*". **ВНИМАНИЕ** Обратите внимание, что выражение "*mpls [label_num]*" может использоваться более одного раза для фильтрации по иерархиям MPLS.
pppoed	Истинно, если пакеты являются пакетами PPP-over-Ethernet Discovery (Ethernet type 0x8863).
pppoes	Истинно, если пакеты являются пакетами PPP-over-Ethernet Session (Ethernet type 0x8864).
iso proto PROTOCOL	Истинно, если пакеты являются пакетами OSI, принадлежащими протоколу "*PROTOCOL*". Протокол может принимать численное значение или одно из следующих символьных: "*clnp*", "*esis*", "*isis*".

expr relop expr	Истинно, если "*relop*" принимает одно из следующих значений ">", "<", ">=", "<=", "=", "!=", а "*expr*" является арифметическим действием "+", "-", "*", "/", "&", "|", "<<", ">>". **ВНИМАНИЕ** Все сравнения беззнаковые, так что, например, 0x80000000 и 0xffffffff будут > 0. Чтобы получить доступ к данным внутри пакета, используется следующий синтаксис: "*proto* [*expr* : *size*]". • *"proto"* может принимать значения *"ether", "fddi", "tr", "wlan", "ppp", "slip", "link", "ip", "arp", "rarp", "tcp", "udp", "icmp"* и указывать уровень протокола для операции фильтрации. Значения *"ether", "fddi", "tr", "wlan", "ppp", "slip", "link"* относятся к канальному уровню. Стоит иметь в виду, что "*tcp", "udp"* и другие протоколы более высокого уровня применяются только к IPv4. • "*size*" является необязательным параметром и показывает размер пакета в байтах. Может быть равен 1, 2 или 4, по умолчанию 1. Длина пакета задается параметром "*len*". Возможны следующие смещения полей заголовка протокола: "*icmptype*" (поле типа ICMP), "*icmpcode*" (поле кода ICMP) и "*tcpflags*" (поле метки TCP): • Возможные значения поля типа ICMP: "*icmp-echoreply", "icmp-unreach", "icmp-sourcequench", "icmp-redirect", "icmp-echo", "icmp-routeradvert", "icmp-routersolicit", "icmp-timxceed", "icmp-paramprob", "icmp-tstamp", "icmp-tstampreply", "icmp-ireq", "icmp-ireqreply", "icmp-maskreq", "icmp-maskreply".* • Возможные значения поля метки TCP: *"tcp-fin", "tcp-syn", "tcp-rst", "tcp-push", "tcp-ack", "tcp-urg".*

Примеры

Фильтрация, запрещающая приём трафика, в котором есть данные, принадлежащие порту 80 ("*udp*" или "*tcp*"). В данном примере приведён полный синтаксис команды "*ipfw*", в последующих примерах параметры самой команды будут опущены.

```
ipfw add reject -f "port 80"
```

Если в фильтре есть несколько одинаковых повторяющихся классификаторов, то для сокращения записи их можно указать один раз.

```
net 192.168.0.0/24 and (tcp port 21 or tcp port 20 or tcp port 25 or tcp port 80 or tcp port
110)
```

Можно сократить:

```
net 192.168.0.0/24 and (tcp port 21 or 20 or 25 or 80 or 110)
```

Выражение, исключающее пакеты, в которых есть IP-адреса "*1.1.1.1*" и "*1.1.1.2*".

```
not (host 1.1.1.1 and host 1.1.1.2)
```

Можно сократить:

```
not (host 1.1.1.1 and 1.1.1.2)
```

Не допускается сокращение, указанное ниже:

```
not host 1.1.1.1 and 1.1.1.2
```

В этом случае будут пропущены пакеты, в которых нет первого IP-адреса и есть второй.
Так же не допускается сокращение:

```
not (host 1.1.1.1 or 1.1.1.2)
```

В этом случае будут исключены пакеты, в которых есть хотя бы один из указанных IP-адресов.

Фильтрация трафика, в котором в качестве адреса (отправителя или получателя) стоит IP-адрес "*192.168.0.1*".

```
host 192.168.0.1
```

Фильтрация трафика, в котором в качестве адреса получателя стоит IP-адрес из сети "*172.16.0.0/16*" (точнее, находится в диапазоне от "*172.16.0.0*" до "*172.16.255.255*").

```
dst net 172.16.0.0/16
```

Фильтрация трафика, принадлежащего сети "*192.168.0.0/24*" (отправитель или получатель), передающего данные по протоколу TCP и использующего порт 21.

```
net 192.168.0.0/24 and tcp port 21
```

Фильтрует весь многоадресный трафик.

```
ether[0] & 1 != 0
```

Title

Фильтрует все IPv4-пакеты.

```
ip[0] & 0xf != 5
```

Фильтрует только нефрагментированные IPv4-дейтаграммы и отбрасывает фрагментированные IPv4-дейтаграммы. Эта проверка неявно применяется к операциям фильтрации tcp и udp. *"tcp[0]"* всегда учитывает первый байт TCP-заголовка и никогда не учитывает первый байт промежуточного фрагмента.

```
ip[6:2] & 0x1fff = 0
```

Фильтрует пакеты с меткой VLAN 200, инкапсулированные в сервисный VLAN 100.

```
svlan 100 && vlan 200
```

Фильтрует пакеты IPv4, инкапсулированные в VLAN 300.

```
vlan 300 && ip
```

Фильтрует все пакеты, инкапсулированные сервисным VLAN 100.

```
svlan 100
```

Фильтрует пакеты с внешней меткой 100000 и внутренней меткой 1024.

```
mpls 100000 && mpls 1024
```

Фильтрует пакеты от/к сетевому узлу "*192.9.200.1*" с внутренней меткой 1024 и без внешней метки.

```
mpls && mpls 1024 && host 192.9.200.1
```

Фильтрует кадры IPv4, инкапсулированные в PPPoE.

```
pppoes && ppp proto 0x21
```