

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

 ВНИМАНИЕ Любое вышеуказанное выражение можно дополнить с помощью префиксов "ip", "ip6", "arp", "rarp".	
ether dst EH OST	Истинно, если поле "адрес получателя" канального уровня совпадает со значением идентификатора "EHOST". "EHOST" должен быть представлен в следующем формате: XX:XX:XX:XX:XX.
ether src EH OST	Истинно, если поле "адрес отправителя" канального уровня совпадает со значением идентификатора "EHOST".
ether host E HOST	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", "igmp6", "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.

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

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

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
```

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.

```
pppoe && ppp proto 0x21
```