ANTCOLONY

TCP/IP и tcpdump

Подсказки для системных администраторов

Разделы:

ANTCOLONY

tcpdump Usage

```
tcpdump [-aenStvx] [-F file]
[-i int] [-r file] [-s snaplen]
[-w file] ['filter_expression']
```

-e	Отображает заголовок канала передачи данных
-F	Выражение фильтра в файле
-i	Прослушивает интерфейс int
-n	Не разрешает IP-адреса
-r	Считывает пакеты из файла
-s	Получает snaplen байт из каждого пакета
-S	Использует абсолютные номера последовательности TCP
-t	Не выводит временную метку
-v	Подробный режим
-w	Записывает пакеты в файл
-x	Отображает в шестнадцатеричном формате
-X	Отображает в шестнадцатеричном формате и ASCII

Акронимы

AH	Authentication Header (RFC 2402)
ARP	Address Resolution Protocol (RFC 826)
BGP	Border Gateway Protocol (RFC 1771)
CWR	Congestion Window Reduced (RFC 2481)
DF	Don’t Fragment bit (IP)
DHCP	Dynamic Host Configuration Protocol (RFC 2131)
DNS	Domain Name System (RFC 1035)
ECN	Explicit Congestion Notification (RFC 3168)
EIGRP	Extended IGRP (Cisco)
ESP	Encapsulating Security Payload (RFC 2406)
FTP	File Transfer Protocol (RFC 959)
GRE	Generic Routing Encapsulation (RFC 2784)
HTTP	Hypertext Transfer Protocol (RFC 1945)
ICMP	Internet Control Message Protocol (RFC 792)
IGMP	Internet Group Management Protocol (RFC 2236)
IGRP	Iterior Gateway Routing Protocol (Cisco)
IMAP	Internet Message Access Protocol (RFC 2060)
IP	Internet Protocol (RFC 791)
ISAKMP	Internet Security Association & Key Management Protocol (RFC 2408)
L2TP	Layer 2 Tunneling Protocol (RFC 2661)

Акронимы 01

NNTP	Network News Transfer Protocol (RFC 977)
OSPF	Open Shortest Path First (RFC 1583)
POP3	Post Office Protocol v3 (RFC 1460)
RFC	Request for Comments
RIP	Routing Information Protocol (RFC 2453)
LDAP	Lightweight Directory Access Protocol (RFC 2251)
SKIP	Simple Key-Management for Internet Protocols
SMTP	Simple Mail Transfer Protocol (RFC 821)
SNTP	Simple Network Management Protocol (RFC 1157)
SSH	Secure Shell
SSL	Secure Sockets Layer (Netscape)
TCP	Transmission Control Protocol (RFC 793)
TFTP	Trivial File Transfer Protocol (RFC 1350)
TOS	Type of Service field (IP)
UDP	User Datagram Protocol (RFC 768)

ANTCOLONY

Заголовок UDP

Bit Number

```
                1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Порт источника	Порт назначения
Длина	Контрольная сумма

Информация о заголовке UDP

Общие UDP-порты хорошо известного сервера

7	echo	138	netbios-dgm
19	chargen	161	snmp
37	time	162	snp-trap
53	domain	500	isakmp
67	bootps (DHCP)	514	syslog
68	bootpc (DHCP)	520	rip
69	tftp	33434	traceroute
137	netbios-ns		

Длина

(Количество байт во всей дейтаграмме, включая заголовок; минимальное значение = 8)

Контрольная сумма

(охватывает псевдозаголовок и всю UDP-дейтаграмму целиком)

ARP

Bit Number

1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Тип аппаратного адреса		Тип адреса протокола
Длина апп.адреса	Длина прот. адреса	Операция
Аппаратный адрес источника		
Аппаратный адрес источника (прод.)		Протокольный адрес источника
Протокольный адрес источника (прод.)		Аппаратный адрес назначения
Аппаратный адрес назначения (прод.)		
Протокольный адрес назначения		

Параметры ARP (для Ethernet и IPv4)

Тип аппаратного адреса

1 Ethernet
6 IEEE 802 LAN

Тип протокольного адреса

2048 IPv4 (0×0800)

Длина аппаратного адреса

6 for Ethernet/IEEE 802

Длина протокольного адреса

4 for IPv4

Операция

1 Request
2 Reply

DNS

Bit Number

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Длина (только TCP)															
ID.															
QR	Opcode				AA	TC	RD	RA	Z			RCODE			
QDCOUNT															
ANCOUTE															
NSCOUNT															
ARCOUNT															
Раздел вопроса															
Раздел ответа															
Авторитетный раздел															
Раздел с дополнительной информацией															

Параметры DNS

Query/Response

0 Query
1 Response

Opcode

0 Standard query (QUERY)
1 Inverse query (IQUERY)
2 Server status request (STATUS)

AA

A (1 = Authoritative Answer)

TC

(1 = TrunCation)

DNS 01

RD

(1 = Recursion Desired)

RA

(1 = Recursion Available)

Z

(Reserved; set to 0)

Response code

0 Нет ошибки
1 Ошибка формата
2 Ошибка сервера
3 Не существует домена (NXDOMAIN)
4 Не реализован тип запроса
5 Запрос отклонён

QDCOUNT

(Количество записей в секции вопроса)

ANCOUNT

(Количество ресурсных записей в разделе ответа)

NSCOUNT

(Количество ресурсных записей серверов имён в авторитетном разделе)

ARCOUNT

(Количество ресурсных записей в разделе с дополнительной информацией)

ICMP

Bit Number

1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Тип	Код	Контрольная сумма
Другая информация, относящаяся к сообщению...		

Тип Имя/Коды (Code=0, если не указано иное)

0 Ответ эхо
3 Сеть недостижима
- 0 Сеть недостижима
- 1 Хост недостижим
- 2 Протокол недостижим
- 3 Порт недостижим
- 4 Необходима фрагментация и установлен флаг DF
- 5 Ошибка маршрутизации по исходному маршруту
- 6 Неизвестная сеть назначения
- 7 Неизвестный хост назначения
- 8 Изоляция исходного хоста
- 9 Сеть запрещена администратором
- 10 Хост запрещён администратором
- 11 Сеть недостижима для TOS
- 12 Хост недостижим для TOS
- 13 Общение запрещено администратором

4 Ограничение источника
5 Переадресация
0 Переадресация дейтаграммы для сети
1 Переадресация дейтаграммы для хоста
2 Переадресация дейтаграммы для TOS и сети
3 Переадресация дейтаграммы для TOS и хоста
8 Эхо
9 Объявление маршрутизатора
10 Выбор маршрутизатора
11 Превышено время
- 0 Время жизни истекло в пути
- 1 Превышено время сборки фрагментов

ICMP 01

12 Проблема с параметром
- 0 Указатель указывает на ошибку
- 1 Отсутствует обязательный параметр
- 2 Неправильная длина

13 Временная метка
14 Ответ временной метки
15 Запрос информации
16 Ответ информации
17 Запрос маски адреса
18 Ответ маски адреса
30 Трассировка маршрута

Заголовок IP

Bit Number

1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Версия	IHL	Тип сервиса	Полная длина	
Идентификация			Флаги	Фрагментарный сдвиг
Время жизни		Протокол	Контрольная сумма заголовка	
Адрес источника				
Адрес назначения				
Опции (опционально)				

Содержимое IP заголовка

Версия

4 IP version 4

Длина интернет-заголовка

Количество 32-битных слов в заголовке IP;
минимальное значение = 5 (20 байт) и
максимальное значение = 15 (60 байт)

Type of Service (PreDTRCx) → Differentiated Services

Precedence (000-111)	000
D (1 = минимизировать задержку)	0
T (1 = максимизировать пропускную способность)	0
R (1 = максимизировать надежность)	0
C (1 = минимизировать затраты)	1 = ECN поддержка
x (зарезервировано и установлено на 0)	1 = наблюдается перегрузка

Полная длина

Количество байт в пакете; максимальная длина = 65 535

Флаги (xDM)

x (зарезервировано и установлено в 0)
D (1 = Не фрагментировать)
M (1 = 1 = Больше фрагментов)

Заголовок IP 01

Фрагментарный сдвиг

Положение этого фрагмента в исходной дейтаграмме, в блоках по 8 байт

Протокол

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Контрольная сумма заголовка

Охватывает только заголовок IP

Адресация

NET_ID		RFC 1918 PRIVATE ADDRESSES
0-127	Class A	10.0.0.0-10.255.255.255
128-191	Class B	172.16.0.0-172.31.255.255
192-223	Class C	192.168.0.0-192.168.255.255
224-239	Class D	(multicast)
240-255	Class E	(experimental)

HOST_ID

0	Значение сети; Broadcast (old)
255	Broadcast

Опции (0-40 байт; дополнено до 4-байтовой границы)

0 Конец листа опций	68 Временная метка
1 Нет операции (панель)	131 Свободный исходный маршрут
7 Запись маршрута	137 Строгий исходный маршрут

Заголовок TCP

Bit Number

1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Порт источника			Порт назначения
Порядковый номер			
Номер подтверждения			
Сдвиг (длина заголовка)	Reserved	Флаги	Окно
Контрольная сумма			Указатель срочности
Опции (опционально)			

Содержимое TCP заголовка

Распространенные TCP-порты сервера

7 echo
19 chargen
20 ftp-data
21 ftp-control
22 ssh
23 telnet
25 smtp
53 domain
79 finger
80 http
110 pop3
111 sunrpc
119 nntp
139 netbios-ssn
143 imap
179 bgp
389 ldap
443 https (ssl)
445 microsoft-ds
1080 socks

Сдвиг

Количество 32-битных слов в заголовке TCP;
минимальное значение = 5

Reserved

4 бита; установлено в 0

Заголовок TCP 01

Флаги (CEUAPRSF)

Биты ECN (используются при использовании ECN; иначе 00)
CWR (1 = отправитель сократил окно перегрузки вдвое)
ECN-Echo (1 = получатель сократил окно перегрузки вдвое)
U (1 = Обратиться к указателю срочности, уведомить серверное приложение о срочных данных)
A (1 = Обратиться к полю подтверждения)
P (1 = Отправить данные)
R (1 = Сбросить соединение)
S (1 = Синхронизировать порядковые номера)
F (1 = Больше данных нет; Завершить соединение)

Контрольная сумма

Охватывает псевдо заголовок и весь сегмент TCP

Указатель срочности

Смещение указателя на срочные данные

Опции

0 Конец листа опций
1 Нет операции (панель)
2 Максимальный размер сегмента
3 Масштаб окна
4 Selective ACK ok
8 Временная метка