I don't use this Protocol

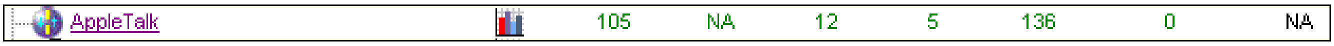
created by: Rainer Bemsel – **Version** 1.0 – **Dated:** June/03/2004

The purpose of this document is to describe some steps on "How to determine, who is sending out certain protocols."

Auto Discovery is a nice feature, when trying to figure out, what protocols are leaving or entering my WAN connection. When I started with Packeteer, a couple days later, I've connected a PaketShaper between my Home Network and my DSL router to see, what's going on. Protocols, like HTTP, FTP, SMTP, POP3 were expected. I also realized some "never-heard" protocols, which I figured out very quickly, what they are.

A good source to find out about "never-heard" protocols is www.protocols.com.

After 3 days discovering, all in a sudden, a protocol named **APPLETALK** appeared. **I don't use this protocol in my network!**



AppleTalk	105	NA	12	5	136	0	NA

So, who's sending this protocol was my next question. It's not a high load, so Top Talker and Top Listeners wouldn't tell me. My goal in this case was to view packet headers. PacketWise offers a feature called "**packet capture**", which I used to determine the sender.

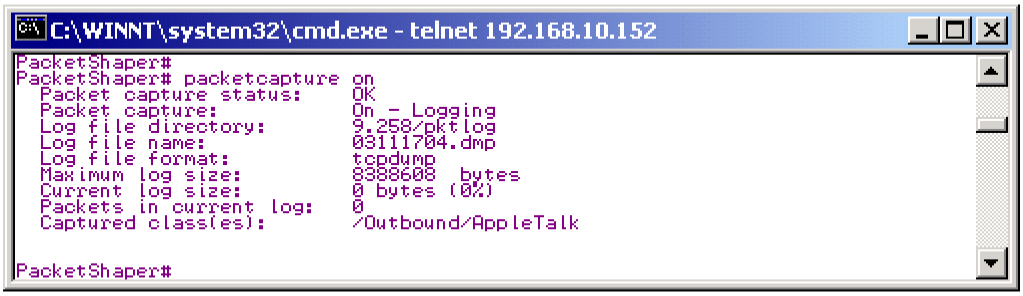
Turn packet capture on

If there is no class created, you have to create one first, before use packet capture, but because of discovery, a class for AppleTalk was already created automatically.

1. Telnet into the box

PacketWise stores captured packets in RAM. They are written to disk when the memory buffer is full or when you turn packet capture off.

Turn on packet capture, by running the CLI command **packetcapture on**



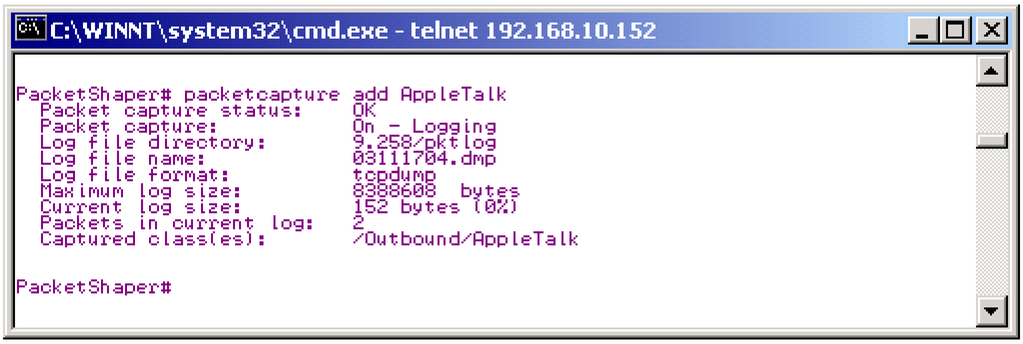
```
PacketShaper#
PacketShaper# packetcapture on
  Packet capture status:     OK
  Packet capture:            On - Logging
  Log file directory:        9.258/pktlog
  Log file name:             03111704.dmp
  Log file format:           tcpdump
  Maximum log size:          8388608  bytes
  Current log size:          0 bytes (0%)
  Packets in current log:    0
  Captured class(es):        /Outbound/AppleTalk


PacketShaper#
```

DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

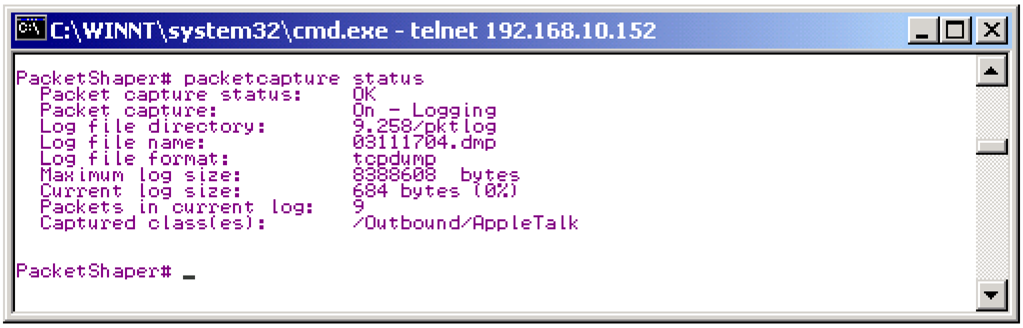
Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user

2. Add the class for capturing, by running CLI Command **packetcapture add AppleTalk** (or any other existing class)



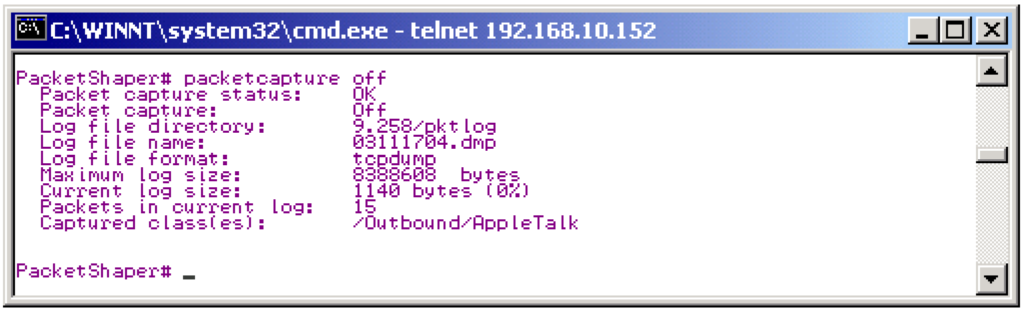
```
PacketShaper# packetcapture add AppleTalk
  Packet capture status:     OK
  Packet capture:            On - Logging
  Log file directory:        9.258/pktlog
  Log file name:             03111704.dmp
  Log file format:           tcpdump
  Maximum log size:          8388608  bytes
  Current log size:          152 bytes (0%)
  Packets in current log:    2
  Captured class(es):        /Outbound/AppleTalk

PacketShaper#
```

3. To verify, if packets are stored in current logfile, you can use CLI Command **packetcapture status**



```
PacketShaper# packetcapture status
  Packet capture status:     OK
  Packet capture:            On - Logging
  Log file directory:        9.258/pktlog
  Log file name:             03111704.dmp
  Log file format:           tcpdump
  Maximum log size:          8388608  bytes
  Current log size:          684 bytes (0%)
  Packets in current log:    9
  Captured class(es):        /Outbound/AppleTalk

PacketShaper# _
```

4. When satisfied with the result, stop the tool by running the CLI Command **packetcapture off**

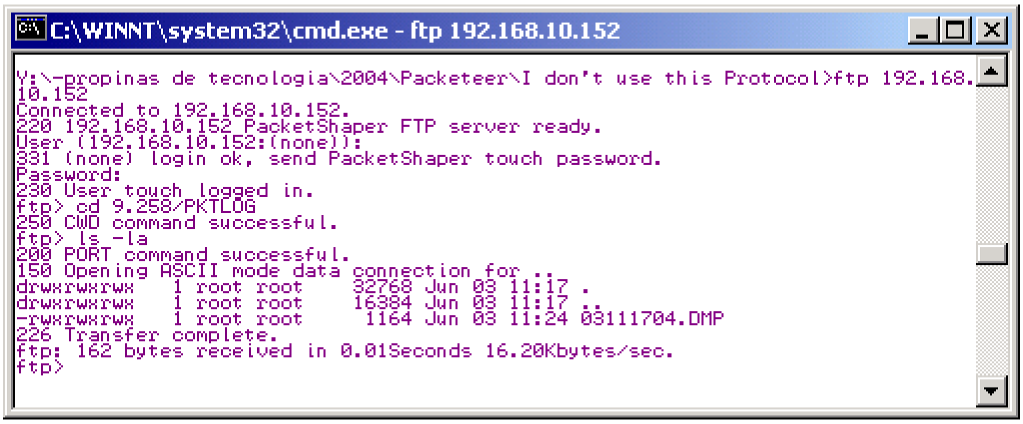


```
PacketShaper# packetcapture off
  Packet capture status:     OK
  Packet capture:            Off
  Log file directory:        9.258/pktlog
  Log file name:             03111704.dmp
  Log file format:           tcpdump
  Maximum log size:          8388608  bytes
  Current log size:          1140 bytes (0%)
  Packets in current log:    15
  Captured class(es):        /Outbound/AppleTalk

PacketShaper# _
```

Recognize the log file directory and log file name. 9.258 is the harddisk and **03111704**.dmp is the filename.

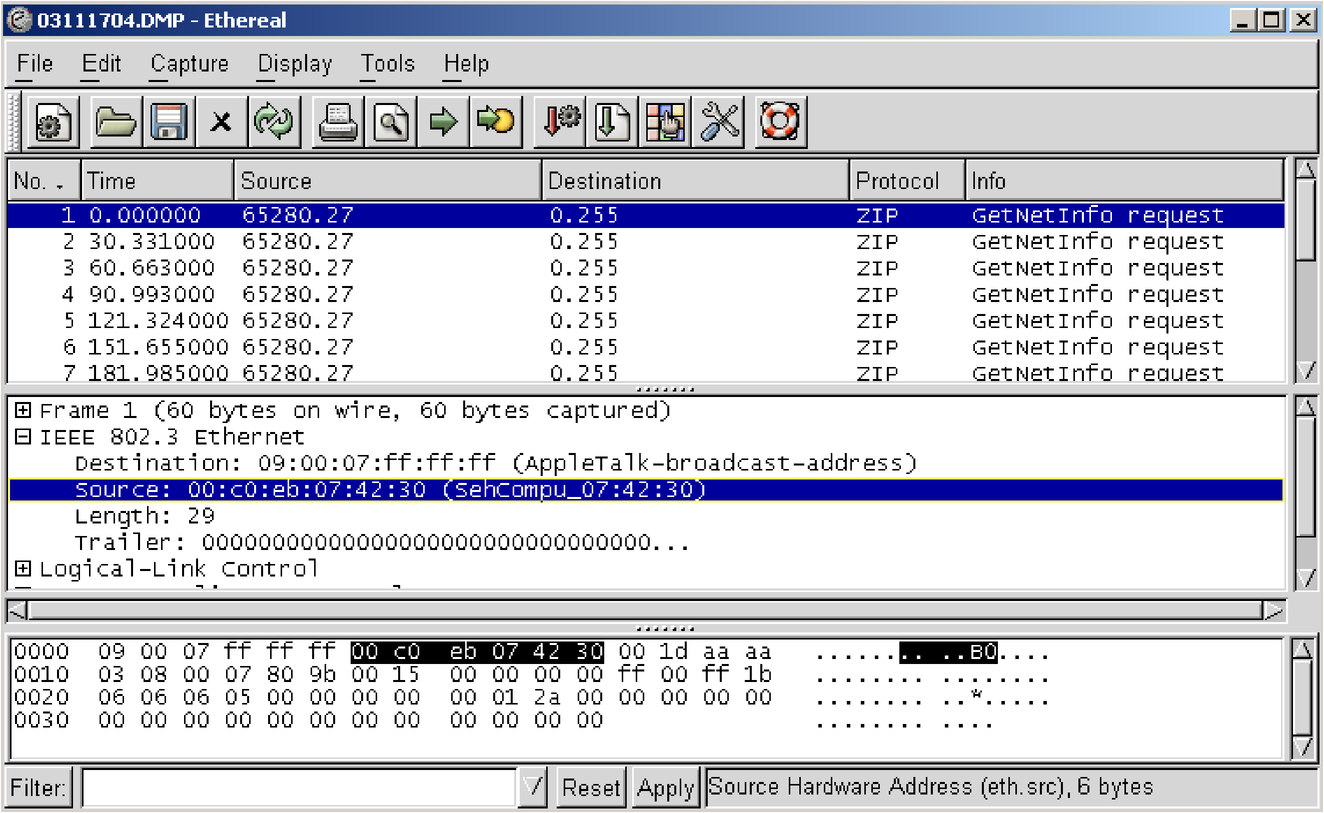
03 – refers to 3rd day of the month
111704 – refers to 11:17:04, when packet capture has been enabled

5. FTP into the box and download the Dumpfile.



```
Y:\-propinas de tecnologia\2004\Packeteer\I don't use this Protocol>ftp 192.168.
10.152
Connected to 192.168.10.152.
220 192.168.10.152 PacketShaper FTP server ready.
User (192.168.10.152:(none)):
331 (none) login ok, send PacketShaper touch password.
Password:
230 User touch logged in.
ftp> cd 9.258/PKTLOG
250 CWD command successful.
ftp> ls -la
200 PORT command successful.
150 Opening ASCII mode data connection for ..
drwxrwxrwx   1 root root    32768 Jun 03 11:17 .
drwxrwxrwx   1 root root    16384 Jun 03 11:17 ..
-rwxrwxrwx   1 root root     1164 Jun 03 11:24 03111704.DMP
226 Transfer complete.
ftp: 162 bytes received in 0.01Seconds 16.20Kbytes/sec.
ftp>
```

6. Start Sniffer, EtherPeek or EtherReal and load the dumpfile



```
No. . Time        Source      Destination   Protocol  Info
    1 0.000000    65280.27    0.255         ZIP       GetNetInfo request
    2 30.331000   65280.27    0.255         ZIP       GetNetInfo request
    3 60.663000   65280.27    0.255         ZIP       GetNetInfo request
    4 90.993000   65280.27    0.255         ZIP       GetNetInfo request
    5 121.324000  65280.27    0.255         ZIP       GetNetInfo request
    6 151.655000  65280.27    0.255         ZIP       GetNetInfo request
    7 181.985000  65280.27    0.255         ZIP       GetNetInfo request
```

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊟ IEEE 802.3 Ethernet
     Destination: 09:00:07:ff:ff:ff (AppleTalk-broadcast-address)
     Source: 00:c0:eb:07:42:30 (SehCompu_07:42:30)
     Length: 29
     Trailer: 00000000000000000000000000000000...
⊞ Logical-Link Control
```

```
0000  09 00 07 ff ff ff 00 c0  eb 07 42 30 00 1d aa aa   ........ ..B0....
0010  03 08 00 07 80 9b 00 15  00 00 00 00 ff 00 ff 1b   ........ ........
0020  06 06 06 05 00 00 00 00  00 01 2a 00 00 00 00 00   ........ ..*.....
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Source Hardware Address (eth.src), 6 bytes

Based on my MAC Address Database, it was easy to find out, that my SEH Printserver had AppleTalk enabled. I disabled the protocol and eliminated a protocol, which **I do not need in my network!**