

Understanding the NNTP Protocol

Don Parker

NNTP or Network News Transfer Protocol as it is also known, is not a widely known protocol. Typically this is a service that is offered by your ISP and also is one that has spawned its own industry. Company's such as Supernews and Easynews have grown out of the popularity that are the alt.binaries.* groups. If you are lucky though your ISP offers you good NNTP servers to use. What are binary newsgroups though? Well simply put, they are just as their name indicates ie: binary newsgroups. By binary I mean that you could download pictures, programs, movies, music and so on ie: a binary transfer. There is pretty everything you would ever hope to find in the binary newsgroups. A fair amount of the stuff there is copyrighted material, which should not be downloaded either. Largely due to the wide variety of material made available via the binary groups is why they are so popular with people. What actually makes up the protocol that is used to access these groups and in turn download from them? Well that is what we are going to find out in this article!

On with the Show

Well NNTP like almost every protocol follows the client/server model and is also an application layer protocol, as defined by the OSI Reference Model. The protocol uses TCP as its transport protocol and of course the IP protocol for routing purposes. NNTP also allows for both the sending and receipt of information. In other words it will allow you to post messages to newsgroups, as well as download from them, whether that download be an ASCII one or binary in nature. Port 119 is the port associated with NNTP servers, which are also commonly known as USENET newsgroups.

Similar in nature as mentioned earlier to other application layer protocols, NNTP also has a series of status codes, much like HTTP. These status codes are used to convey various conditions back to the NNTP client. The various status codes are grouped as seen below;

```
1xx - Information message
2xx - Command is ok
3xx - Command is ok, continue
4xx - Command ok, but could not be processed
5xx - Command not processed (normally due to a server side error)
```

These messages are quite often seen when you are downloading or uploading material. They will be displayed in your NNTP client. One of the most popular clients is Grabit, but there is also NewsBin Pro. NNTP is also a little similar to HTTP in that it has some commands which are similar to the GET, POST, and HEAD of HTTP for example. The NEXT command in NNTP signifies move on to the "next" article in the newsgroup. That command is pretty much straightforward. There is also the POST command, which much it implies, is for posting to a newsgroup. That post could be a request for a specific TV show episode that you missed of your favourite show and lucky for you there is a newsgroup for it. In that case you would post a message requesting somebody upload that tv show episode, which someone hopefully recorded. A complete list of commands and their function can be found here. You should never be afraid to read the specific RFC for a protocol. They are usually quite well written and easy to understand. Besides you really need to read them, as they are the definitive source of information when it comes to protocols.

What does a NNTP Packet Look Like?

Well much like any IP based protocol NNTP has a familiar look to it. There is the IP header, followed by the TCP header, which in turn is followed by the application layer data. In this case that would be the NNTP data. We will look at two example packets below. Please note that I will comment on the packet directly beneath it.

Understanding the NNTP Protocol

Don Parker

```
16:18:31.062500 IP (tos 0x0, ttl 128, id 49613, offset 0, flags [none],
proto: UDP (17), length: 81) 192.168.1.102.1050 > 24.153.22.67.53: 30312+ A?
nntp.slnt.phub.net.cable.rogers.com. (53)
0x0000: 4500 0051 c1cd 0000 8011 87e4 c0a8 0166 E..Q.....f
0x0010: 1899 1643 041a 0035 003d 30c9 7668 0100 ...C...5.=0.vh..
0x0020: 0001 0000 0000 0000 046e 6e74 7004 736c .....nntp.sl
0x0030: 6e74 0470 6875 6203 6e65 7405 6361 626c nt.phub.net.cabl
0x0040: 6506 726f 6765 7273 0363 6f6d 0000 0100 e.rogers.com....
0x0050: 01 .
```

The packet above us right now was generated when I invoked my NNTP client, which is the aforementioned Grabit in my case. First thing that happens is that my computer asks my ISP to resolve to an IP address where the NNTP news server is that we see in the underlined ASCII. Once my running process of Grabit receives the "A" ie: DNS answer record it connects to the NNTP server.

```
16:18:31.250000 IP (tos 0x0, ttl 128, id 49636, offset 0, flags [DF], proto:
TCP (6), length: 53) 192.168.1.102.1638 > 216.196.97.142.119: P, cksum
0xda64 (correct), 1259902493:1259902506(13) ack 3731847953 win 65514
0x0000: 4500 0035 cle4 4000 8006 3c7d c0a8 0166 E..5..@...<}...f
0x0010: d8c4 618e 0666 0077 4b18 961d de6f 7b11 ..a..f.wK....o{.
0x0020: 5018 ffea da64 0000 4d4f 4445 2052 4541 P....d..MODE.REA
0x0030: 4445 520d 0a DER..
```

After the TCP/IP handshake is complete with the NNTP server, my client issues the READER command. In this case that means that it wants to download the header files. You will note that the underlined portion is where the UDP header is, and that the bolded part is where the NNTP data begins and goes on to the end of the packet.

```
16:18:31.296875 IP (tos 0x0, ttl 128, id 49646, offset 0, flags [DF], proto:
TCP (6), length: 72) 192.168.1.102.1638 > 216.196.97.142.119: P, cksum
0xaa51 (correct), 1259902506:1259902538(32) ack 3731847976 win 65491
0x0000: 4500 0048 cle4 4000 8006 3c60 c0a8 0166 E..H..@...<`...f
0x0010: d8c4 618e 0666 0077 4b18 962a de6f 7b28 ..a..f.wK..*o{(
0x0020: 5018 ffd3 aa51 0000 4752 4f55 5020 616c P....Q..GROUP.al
0x0030: 742e 6269 6e61 7269 xxxx xxxx xxxx xxxx t.binaries.xxxxxx
0x0040: xxxx xxxx xxxx xxxx xxxxxxxx
```

In the above packet we see that my client has requested that a specific news group be updated. The NNTP server will in turn download to my client an updated list of files that are in that specific binary newsgroup. Once that is complete you are free to pick and choose exactly what files you would like to download.

It bears noting that the alt.binary newsgroups are by and large much like the wild west of yesteryear. Within the digital confines of these groups are some unsavory characters, posting content that is very much illegal. If you are a parent you would be well advised to keep a close eye on your children's voyages into these groups. The NNTP protocol is a means by which one can access almost every kind of media, from movies to pictures, to full fledged programs. Realize as well that downloading a warez copy of a copyrighted product is theft. On that note I hope that this introduction to the NNTP protocol was of interest to you and as always I welcome your feedback. Till next time!