TCP Flags: PSH and URG

packetlife.net/blog/2011/mar/2/tcp-flags-psh-and-urg

By stretch | Wednesday, March 2, 2011 at 3:58 a.m. UTC

The TCP header contains several one-bit boolean fields known as *flags* used to influence the flow of data across a TCP connection. Ignoring the CWR and ECE flags added for congestion notification by RFC 3168, there are six TCP control flags. Four of these, listed below, are used to control the establishment, maintenance, and tear-down of a TCP connection, and should be familiar to anyone who has performed even rudimentary packet analysis.

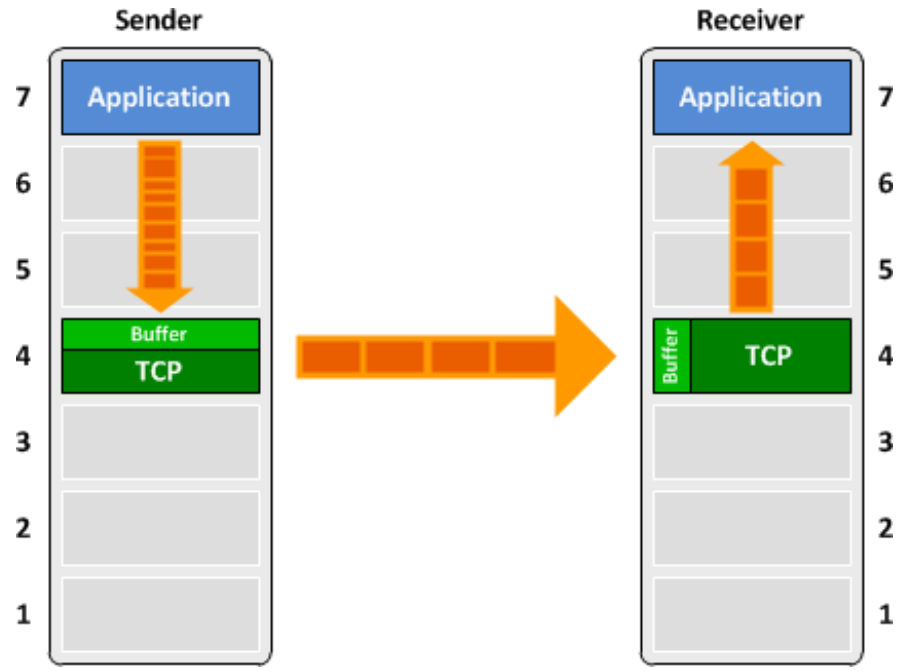
- **SYN** - Initiates a connection
- **ACK** - Acknowledges received data
- **FIN** - Closes a connection
- **RST** - Aborts a connection in response to an error

The other two flags, PSH (push) and URG (urgent), aren't as well-known. They are the focus of today's article.

The PSH Flag

To understand the function of the PSH flag, we first need to understand how TCP buffers data. TCP operates at layer four of the OSI model; it presents to upper layers a simple socket which can be read from and written to, masking the complexities of packet-based communications. To allow applications to read from and write to this socket at any time, buffers are implemented on both sides of a TCP connection in both directions.

The diagram below shows how data is buffered by the sender before sending, and by the receiver upon reception.

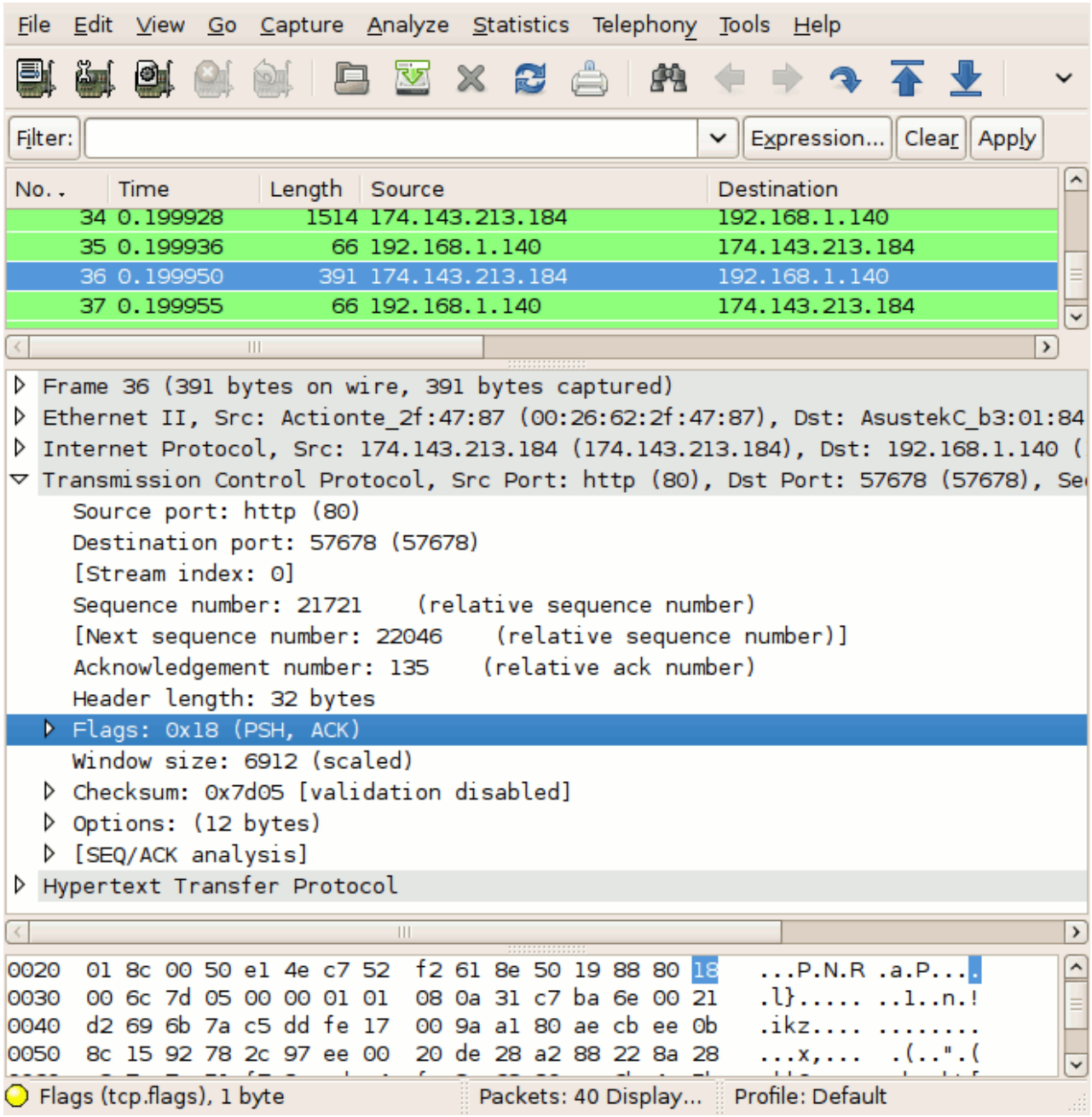


Buffers allow for more efficient transfer of data when sending more than one maximum segment size (MSS) worth of data (for example, transferring a large file). However, large buffers do more harm than good when dealing with real-time applications which require that data be transmitted as quickly as possible. Consider what would happen to a Telnet session, for instance, if TCP waited until there was enough data to fill a packet before it would send one: You would have to type over a thousand characters before the first packet would make it to the remote device. Not very useful.

This is where the PSH flag comes in. The socket that TCP makes available at the session level can be written to by the application with the option of "pushing" data out immediately, rather than waiting for additional data to enter the buffer. When this happens, the PSH flag in the outgoing TCP packet is set to 1 (on). Upon receiving a packet with the PSH flag set, the other side of the connection knows to immediately forward the segment up to the application. To summarize, TCP's push capability accomplishes two things:

- The sending application informs TCP that data should be sent immediately.
- The PSH flag in the TCP header informs the receiving host that the data should be pushed up to the receiving application immediately.

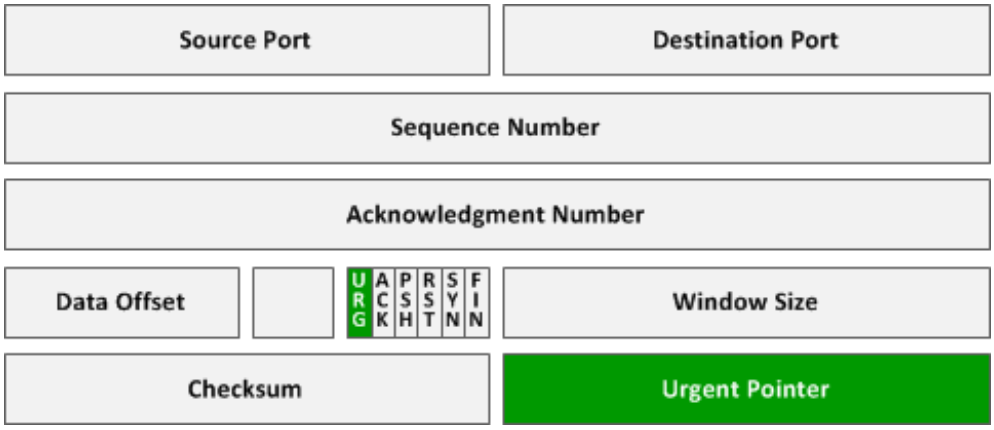
We can see an example of the PSH flag being used in this packet capture of an HTTP GET request. In packet #4, we see that the initial HTTP request has its PSH flag set, indicating that the client has no further data to add and the request should be sent up to the application (in this case, a web daemon) immediately. We also see that the server has set the PSH flag on packet #36, which contains the last bytes of the file requested. Again, the PSH flag is used to inform the receiver that the sender has no further data to transmit (for now).



As mentioned, the PSH flag is also used to facilitate real-time communication via TCP. This packet capture of a short Telnet session shows that all packets carrying Telnet data have the PSH flag set to prevent key presses from being buffered by TCP.

The URG Flag

The URG flag is used to inform a receiving station that certain data within a segment is urgent and should be prioritized. If the URG flag is set, the receiving station evaluates the urgent pointer, a 16-bit field in the TCP header. This pointer indicates how much of the data in the segment, counting from the first byte, is urgent.



The URG flag isn't employed much by modern protocols, but we can see an example of it in the Telnet packet capture referenced earlier. The 0xFF character sent in packet #86 is precedes the Telnet command 0xF2 (242) in packet #70 denoting a data mark. Per RFC 854, this command should be sent with the TCP URG flag set. The urgent pointer in packet #68 indicates that the first byte of the segment (which in this case is the entire segment) should be considered urgent data.

Admittedly, this is probably not the most illustrative example of the URG flag, but it was surprisingly difficult to find other uses of it in real-world captures.

For more discussion of the PSH and URG functions of TCP, check out The TCP/IP Guide online.
