NAME

SSL_client_version, SSL_get_version, SSL_is_dtls, SSL_version - get the protocol information of a connection

SYNOPSIS

#include <openssl/ssl.h>

int SSL_client_version(const SSL *s);

const char *SSL_get_version(const SSL *ssl);

int SSL_is_dtls(const SSL *ssl);

int SSL_version(const SSL *s);

DESCRIPTION

SSL_client_version() returns the numeric protocol version advertised by the client in the legacy_version field of the ClientHello when initiating the connection. Note that, for TLS, this value will never indicate a version greater than TLSv1.2 even if TLSv1.3 is subsequently negotiated. **SSL_get_version()** returns the name of the protocol used for the connection. **SSL_version()** returns the numeric protocol version used for the connection. They should only be called after the initial handshake has been completed. Prior to that the results returned from these functions may be unreliable.

SSL_is_dtls() returns one if the connection is using DTLS, zero if not.

RETURN VALUES

SSL_get_version() returns one of the following strings:

SSLv3
      The connection uses the SSLv3 protocol.

TLSv1
      The connection uses the TLSv1.0 protocol.

TLSv1.1
      The connection uses the TLSv1.1 protocol.

TLSv1.2
      The connection uses the TLSv1.2 protocol.

TLSv1.3
>   The connection uses the TLSv1.3 protocol.

unknown
>   This indicates an unknown protocol version.

SSL_version() and **SSL_client_version**() return an integer which could include any of the following:

SSL3_VERSION
>   The connection uses the SSLv3 protocol.

TLS1_VERSION
>   The connection uses the TLSv1.0 protocol.

TLS1_1_VERSION
>   The connection uses the TLSv1.1 protocol.

TLS1_2_VERSION
>   The connection uses the TLSv1.2 protocol.

TLS1_3_VERSION
>   The connection uses the TLSv1.3 protocol (never returned for **SSL_client_version**()).

SEE ALSO
ssl(7)

HISTORY
The **SSL_is_dtls()** function was added in OpenSSL 1.1.0.

COPYRIGHT