Application Layer Protocol Negotiation

A TLS extension for application layer protocol negotiation within the TLS handshake

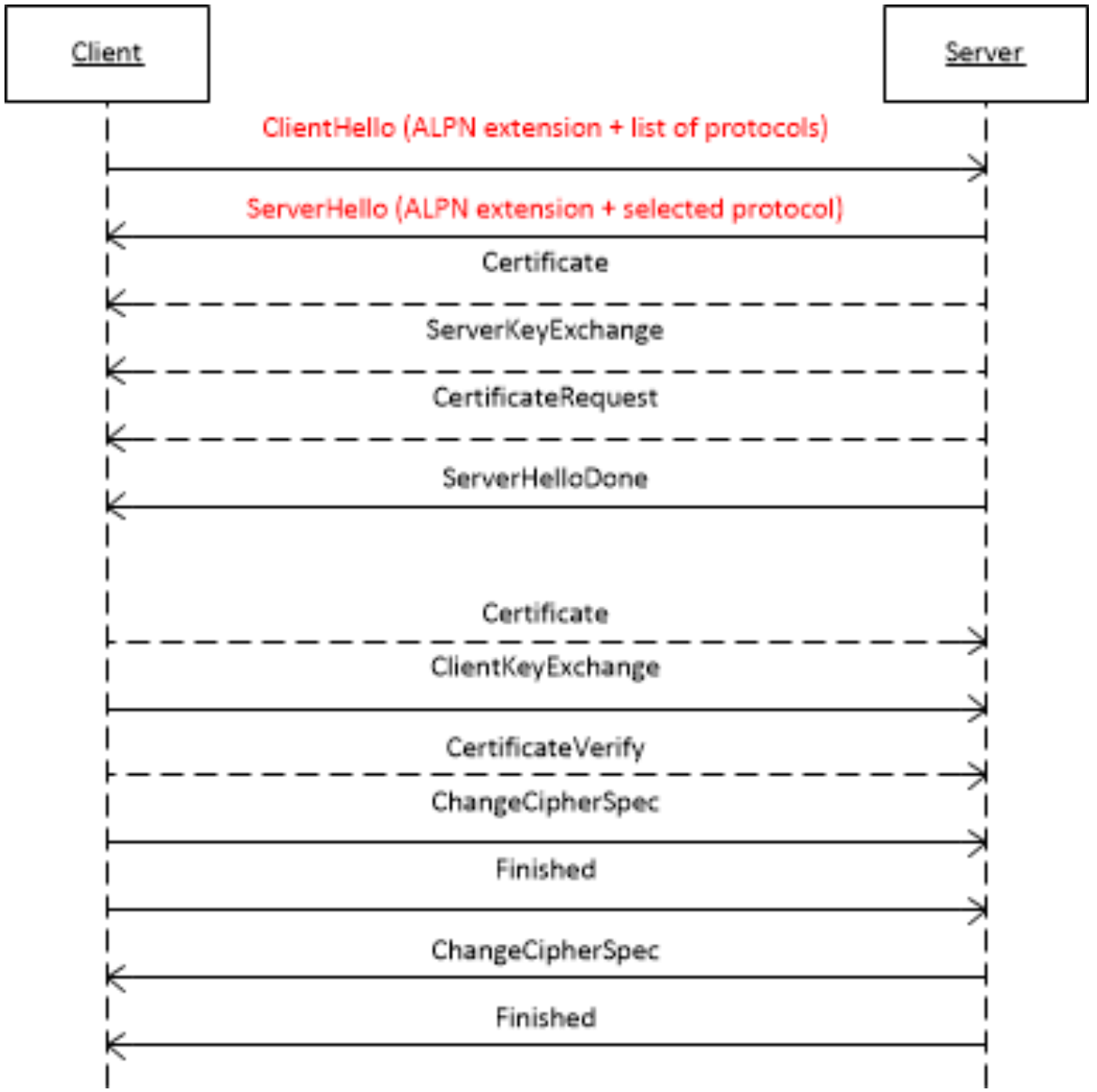
Background and Design Goals

HTTPBis WG requested TLS support for negotiating application layer protocols such as HTTP 1.1 and HTTP 2.0.

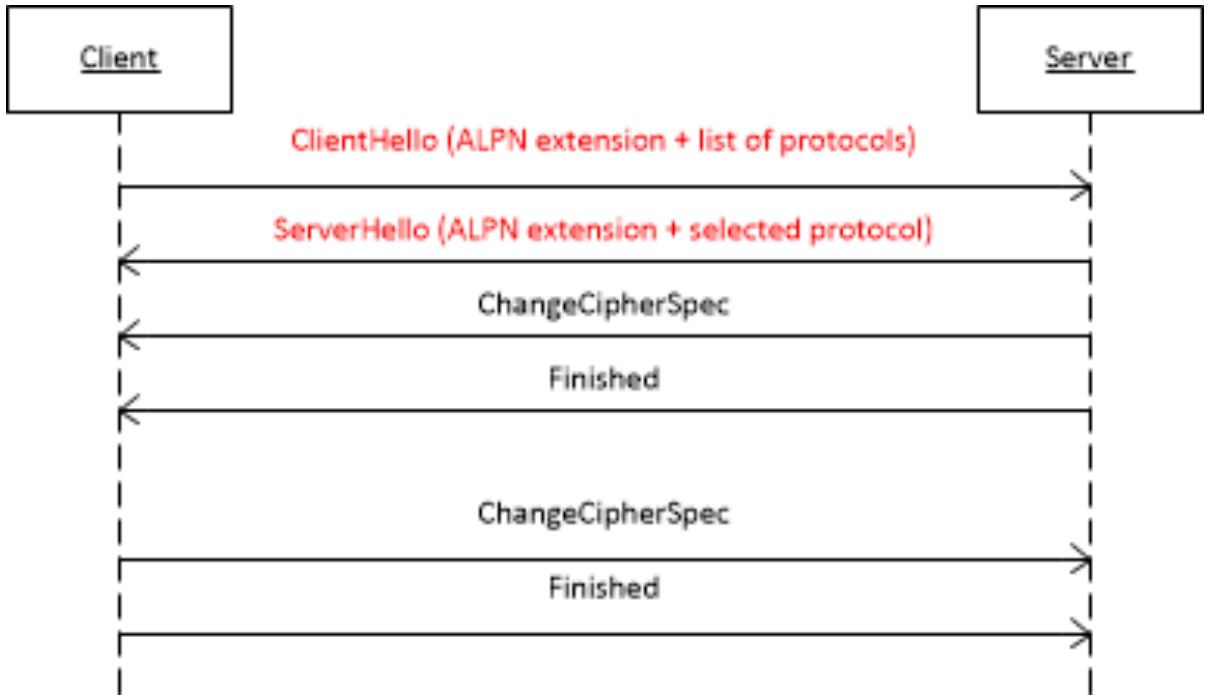
Design goals:

- Negotiate application layer protocol for the connection.
- Minimize connection latency.
- Align with existing TLS extensions.

Full TLS Handshake with ALPN



Abbreviated TLS Handshake with ALPN



ALPN Extension Structure

- The "extension_data" field of the ALPN extension SHALL contain a "ProtocolNameList" value.

```
opaque ProtocolName<1..2^8-1>;
struct {
      ProtocolName protocol_name_list<2..2^16-1>
} ProtocolNameList;
```

- When sent with the ClientHello message, "ProtocolNameList" contains the list of protocols advertised by the client, in descending order of preference.
- When sent with the ServerHello message, "ProtocolNameList" MUST contain exactly one "ProtocolName“ representing the selected protocol.

Protocol IDs and Protocol Selection

- Protocols are named by IANA registered, opaque, non-empty byte strings.
- A namespace for experimental protocols, which are not registered by IANA, starting with: 0x65, 0x78, 0x70 ("exp").
- If the server supports no protocols that the client advertises, the server SHALL respond with a fatal "no_application_protocol" alert.

ALPN Design Considerations

- Protocol selection on the server allows certificate to be chosen based on the negotiated protocol.
- The negotiated protocol is known after the first network roundtrip.
- The "extension_data" field of the ALPN extension allows re-use of the existing parsers.
- TLS renegotiation can be used to negotiate an application protocol with confidentiality.

Available Implementations

- MS Open Tech has contributed an open-source reference implementation of ALPN.
- Available as OpenSSL, Apache and mod_spdy patches:

http://html5labs.interopbridges.com/prototypes/alpn/alpn/info

Links and Contact Information

- ALPN Draft: http://datatracker.ietf.org/doc/draft-friedl-tls-applayerprotoneg
- OpenSSL/Apache implementation of ALPN by MS Open Tech: http://html5labs.interopbridges.com/prototypes/alpn/alpn/info

- Stephan Friedl sfriedl@cisco.com
- Andrei Popov andreipo@microsoft.com