IP Proxying Support for HTTP

draft-age-masque-connect-ip

Tommy Pauly, David Schinazi, Alex Chernyakhovsky,
Mirja Kühlewind, Magnus Westerlund
MASQUE
IETF 112, November 2021, Virtual

CONNECT-IP... haven’t I seen many proposals for this before?

The various proposals joined forces to have a single document!

Motivation

Allow generic IP proxying through HTTP proxies, not just connections to a single TCP/UDP target

- VPN use cases (meeting the requirements in ip-proxy-reqs)
- CONNECT-like proxy for arbitrary IP protocols (mirror CONNECT-UDP)

Scope

Extended CONNECT protocol, mirroring CONNECT-UDP

Proxies entire IP packets in HTTP Datagrams (no compression in base draft)

Request, assign, and route based on fields in the IP header only

- Source address, destination address, next protocol

Out of scope

IP header compression

ICMP signalling (should be another document common for UDP and IP)

Integration with protocol-specific port numbers

What's defined?

"connect-ip" upgrade/protocol token

target and ipproto URI variables

ADDRESS_ASSIGN, ADDRESS_REQUEST, ROUTE_ADVERTISEMENT capsules

IP_PACKET HTTP datagram format

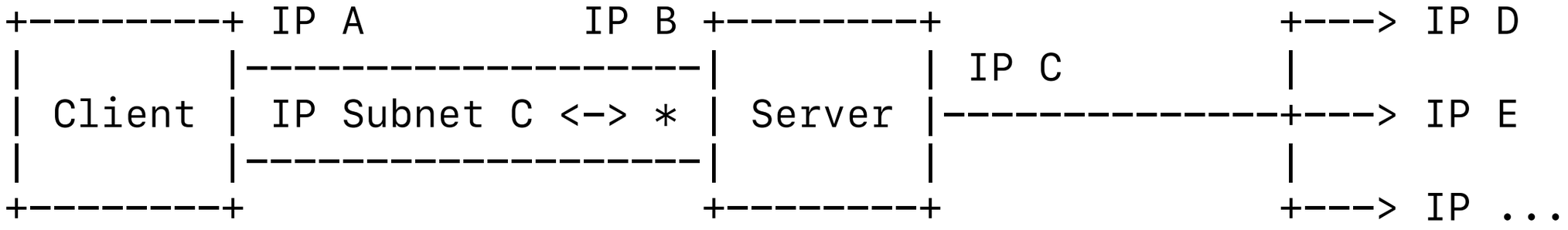
Limiting routing

Not everything is a full tunnel!

- Clients can limit the scope of requests via target and ipproto URI variable
- Endpoints limit the source address used by peers with ADDRESS_ASSIGN
- Endpoints limit the destination address used by peers with ROUTE_ADVERTISEMENT

Limited scope allows a proxy to share IP addresses between multiple clients, like CONNECT and CONNECT-UDP

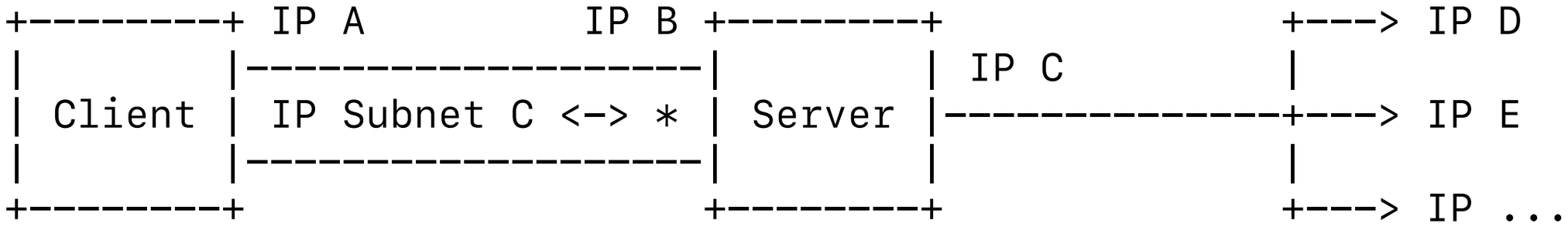
VPN




```
STREAM(44): HEADERS
:method = CONNECT
:protocol = connect-ip
:scheme = https
:path = /vpn
:authority = server.example.com

STREAM(44): CAPSULE
Capsule Type = REGISTER_DATAGRAM_CONTEXT
Context ID = 0
Context Extension = {}
```

VPN

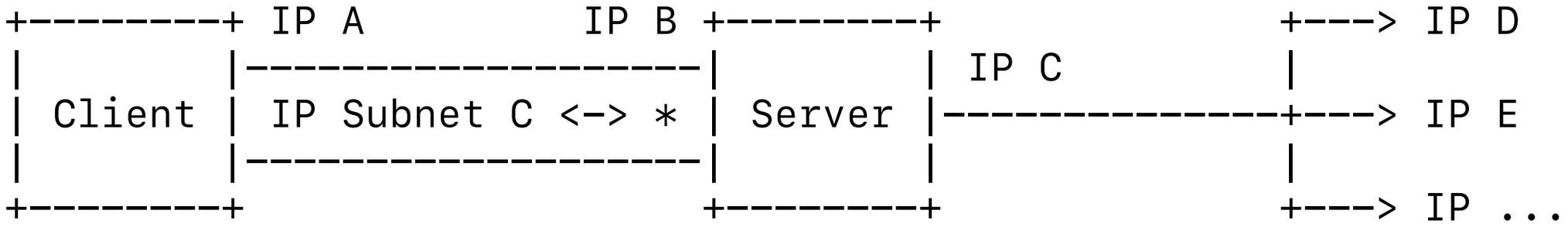



```
STREAM(44): HEADERS
:status = 200

STREAM(44): CAPSULE
Capsule Type = ADDRESS_ASSIGN
IP Version = 4
IP Address = 192.0.2.11 // IP C
IP Prefix Length = 32

STREAM(44): CAPSULE
Capsule Type = ROUTE_ADVERTISEMENT
(IP Version = 4
 Start IP Address = 0.0.0.0
 End IP Address = 255.255.255.255
 IP Protocol = 0) // Any
```

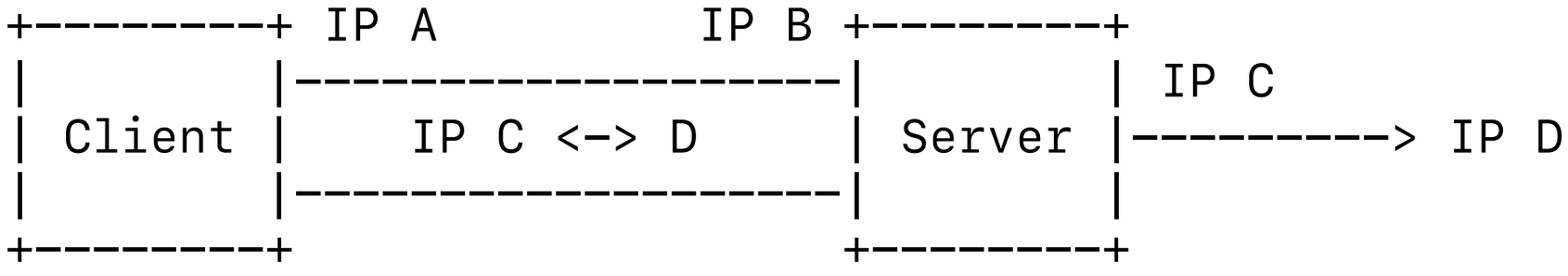
VPN




```
DATAGRAM
Quarter Stream ID = 11
Context ID = 0
Payload = Encapsulated IP Packet
```

```
DATAGRAM
Quarter Stream ID = 11
Context ID = 0
Payload = Encapsulated IP Packet
```

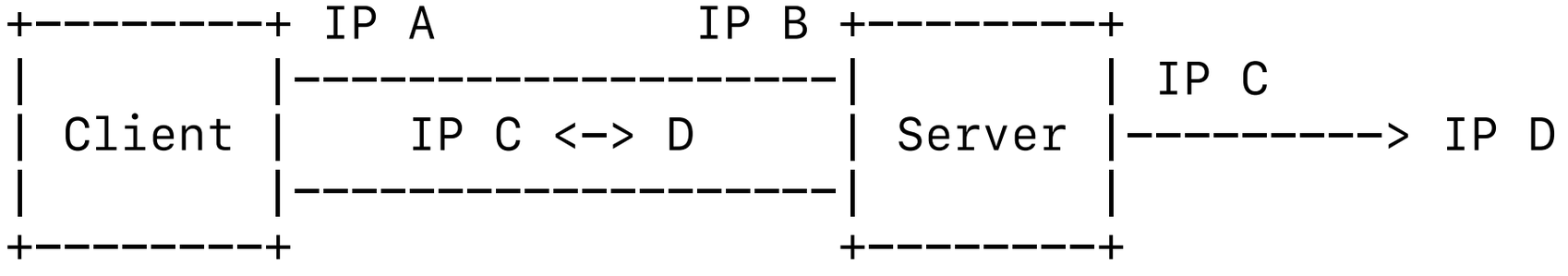
IP Flow Forwarding




```
STREAM(44): HEADERS
:method = CONNECT
:protocol = connect-ip
:scheme = https
:path = /proxy?target=target.example.com&ipproto=132 // SCTP
:authority = server.example.com

STREAM(44): CAPSULE
Capsule Type = REGISTER_DATAGRAM_CONTEXT
Context ID = 0
Context Extension = {}
```

IP Flow Forwarding

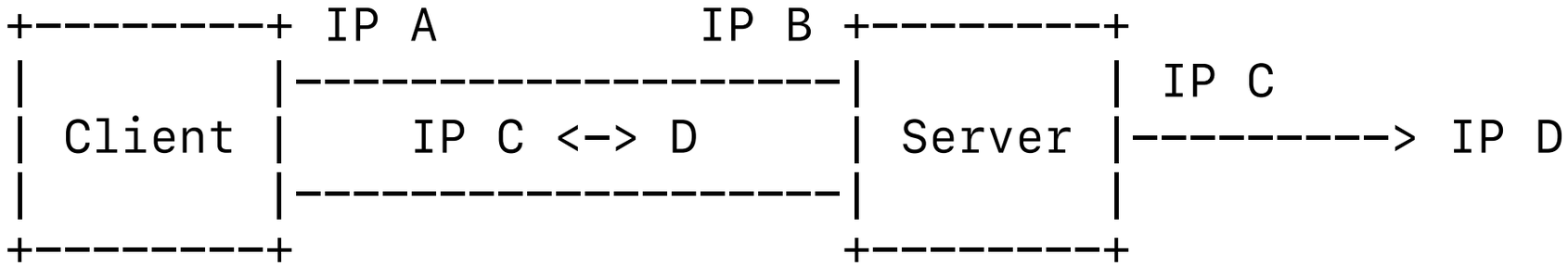



```
STREAM(44): HEADERS
:status = 200

STREAM(44): CAPSULE
Capsule Type = ADDRESS_ASSIGN
IP Version = 6
IP Address = 2001:db8::1234:1234 // IP C
IP Prefix Length = 128

STREAM(44): CAPSULE
Capsule Type = ROUTE_ADVERTISEMENT
(IP Version = 6
 Start IP Address = 2001:db8::3456
 End IP Address = 2001:db8::3456 // IP D
 IP Protocol = 132)
```

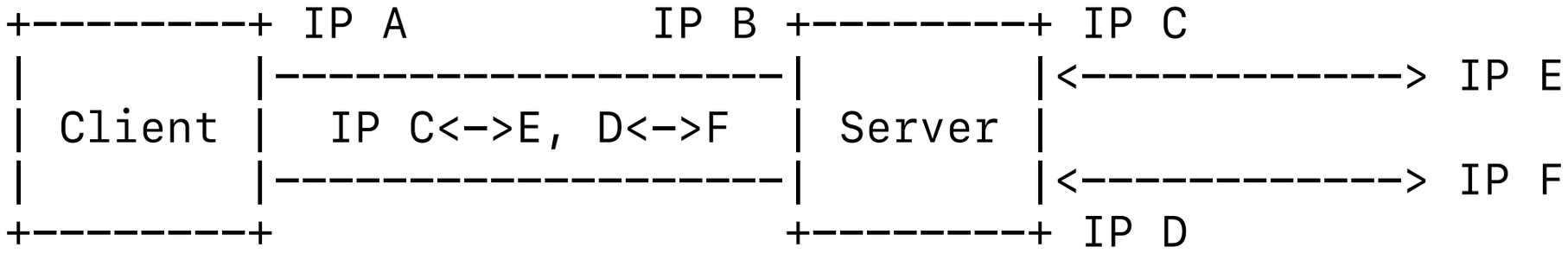
IP Flow Forwarding



DATAGRAM
Quarter Stream ID = 11
Context ID = 0
Payload = Encapsulated SCTP/IP Packet

DATAGRAM
Quarter Stream ID = 11
Context ID = 0
Payload = Encapsulated SCTP/IP Packet

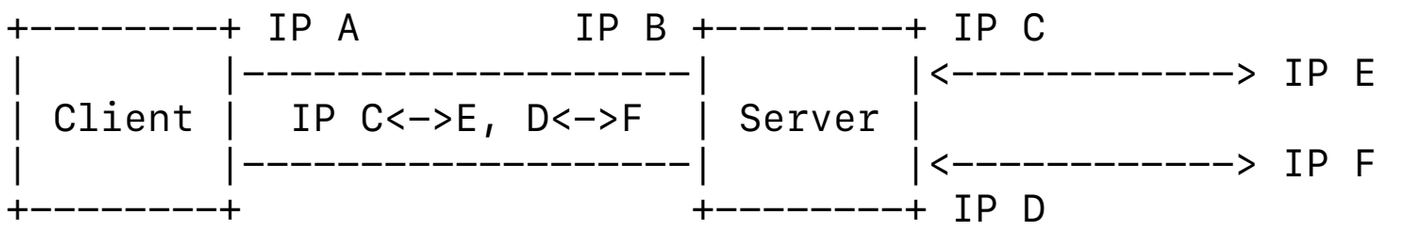
Proxied Connection Racing




```
STREAM(44): HEADERS
:method = CONNECT
:protocol = connect-ip
:scheme = https
:path = /proxy?ipproto=17
:authority = server.example.com

STREAM(44): CAPSULE
Capsule Type = REGISTER_DATAGRAM_CONTEXT
Context ID = 0
Context Extension = {}
```

Proxied Connection Racing




```
STREAM(44): HEADERS
:status = 200

STREAM(44): CAPSULE
Capsule Type = ADDRESS_ASSIGN
IP Version = 4
IP Address = 192.0.2.3
IP Prefix Length = 32

STREAM(44): CAPSULE
Capsule Type = ADDRESS_ASSIGN
IP Version = 6
IP Address = 2001:db8::1234:1234
IP Prefix Length = 128

STREAM(44): CAPSULE
Capsule Type = ROUTE_ADVERTISEMENT
(IP Version = 4
 Start IP Address = 198.51.100.2
 End IP Address = 198.51.100.2
 IP Protocol = 17)
(IP Version = 6
 Start IP Address = 2001:db8::3456
 End IP Address = 2001:db8::3456
 IP Protocol = 17)
```

Next Steps

Is this the right starting place for the protocol?

Ready to adopt?