The Benefits of Using TLS for BGP

September 19, 2024

Thomas Wirtgen, Nicolas Rybowski, Cristel Pelsser, Olivier Bonaventure

UCLouvain

wel Research Institute

Network operators' configuration habits

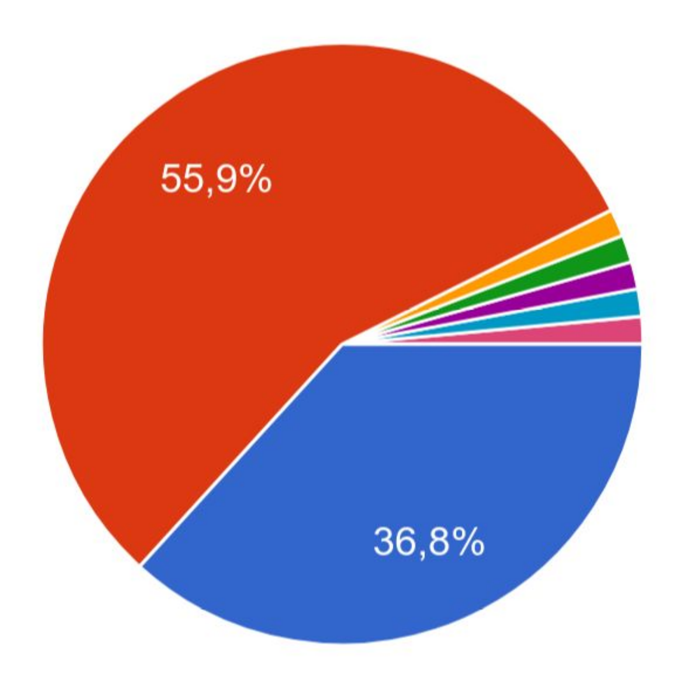
- We conducted a small survey across network operators
- From July to August 2024
  - Questions related to the configuration of BGP
  - 30 questions
  - 68 answers so far

→ **Two interesting outcomes from this survey**

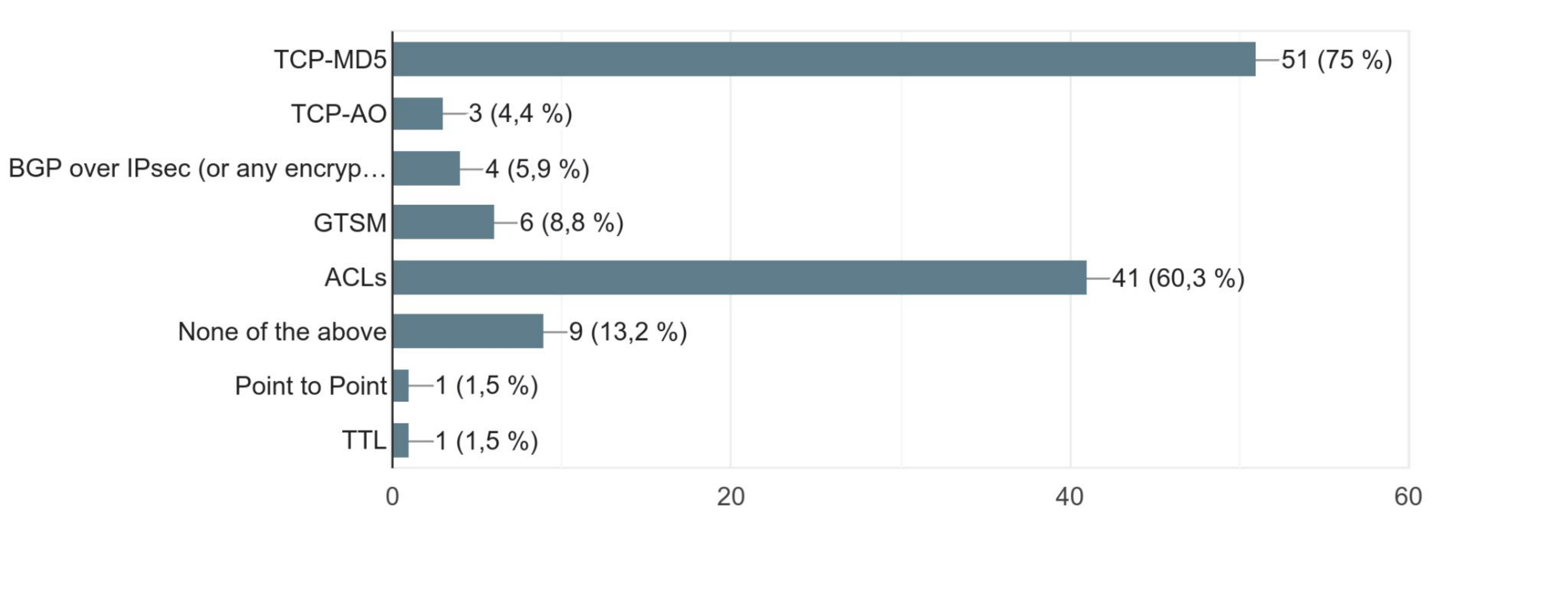
1. How BGP sessions are configured ?

🟥 **Manually using CLI or WEB interface**

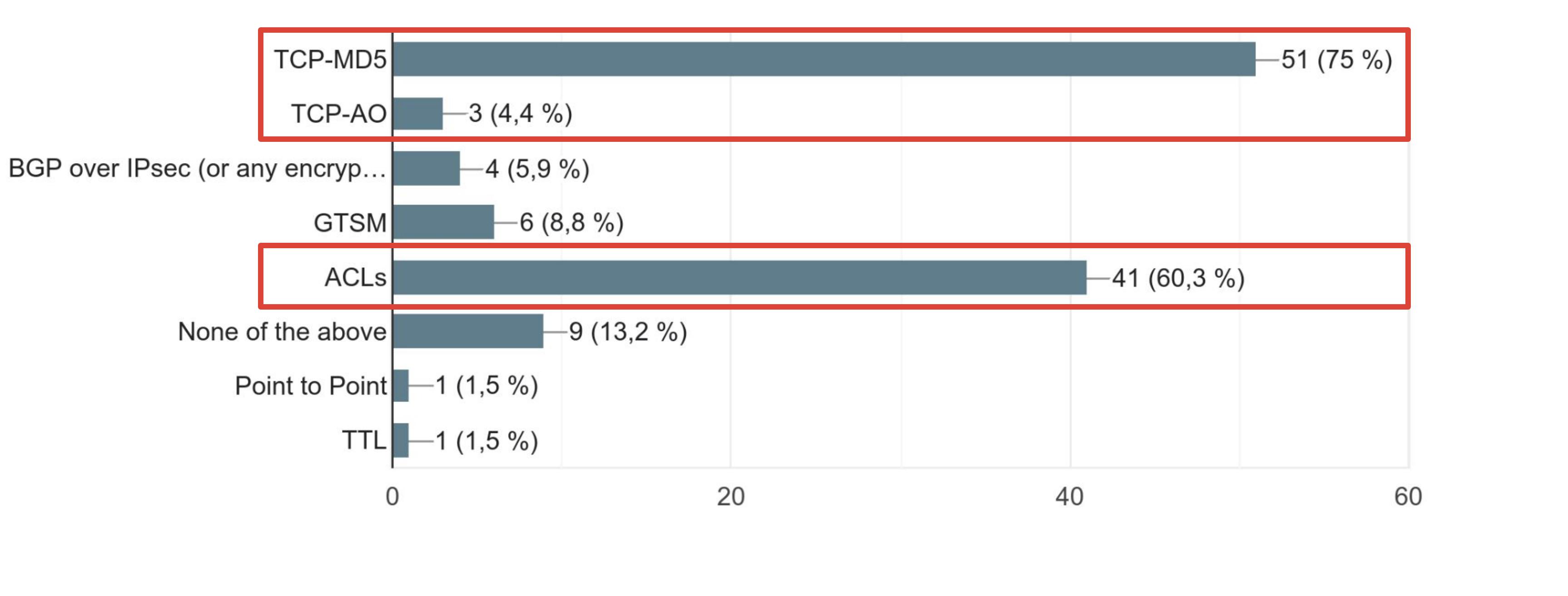
🟦 Automation tools



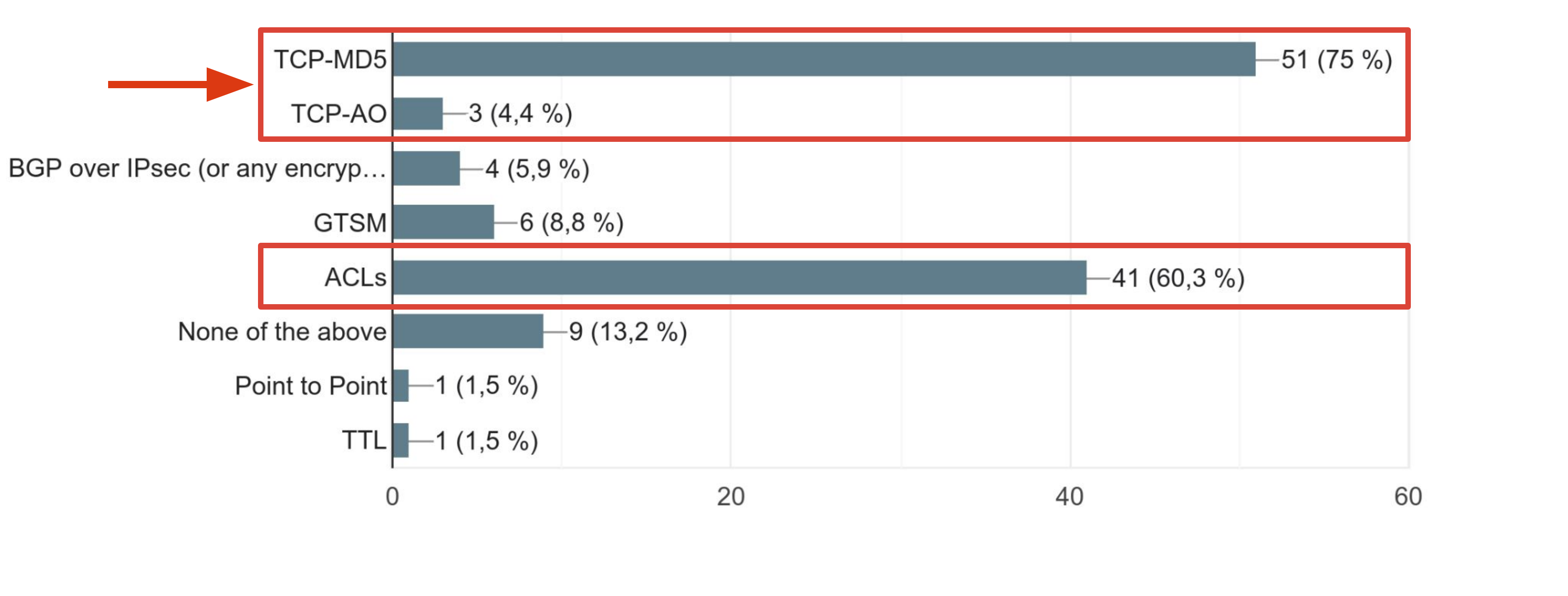
2. What BGP transport protection do you use ?



2. What BGP transport protection do you use ?



2. What BGP transport protection do you use ?



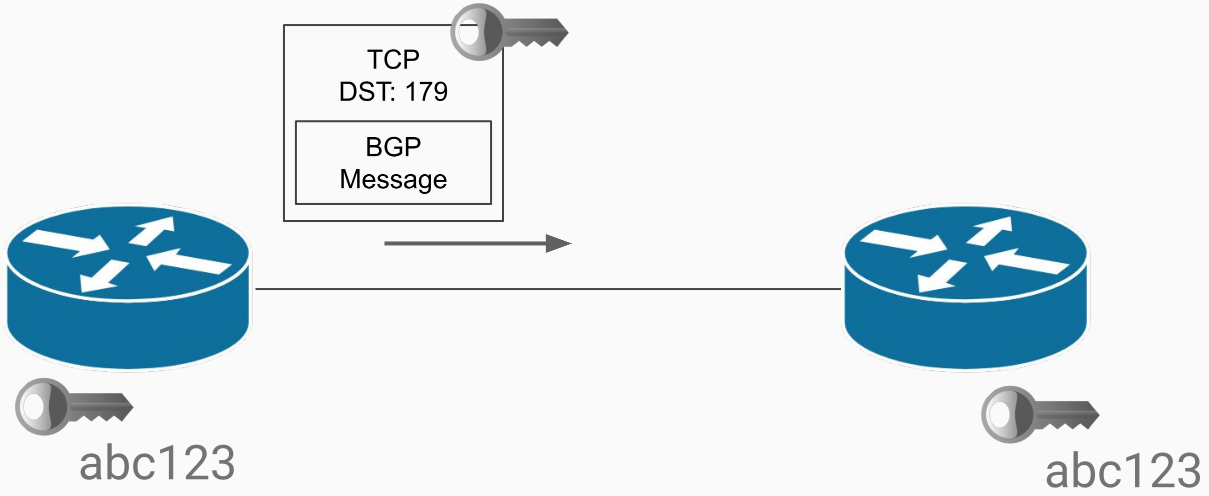
What we learned ?

- > 50% configures their border routers manually
- > 80% uses TCP authentication (TCP-MD5 or TCP-AO)

What we learned ?

- > 50% configures their border routers manually
- > 80% uses TCP authentication (TCP-MD5 or TCP-AO)

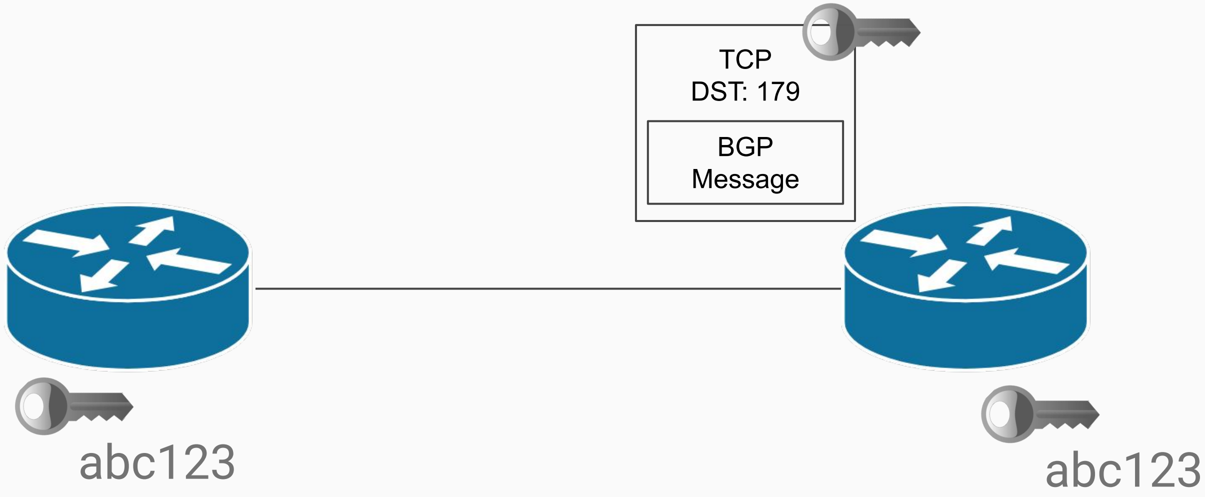
Routers must agree on the TCP-{MD5,AO} key to use beforehand



What we learned ?

- > 50% configures their border routers manually
- > 80% uses TCP authentication (TCP-MD5 or TCP-AO)

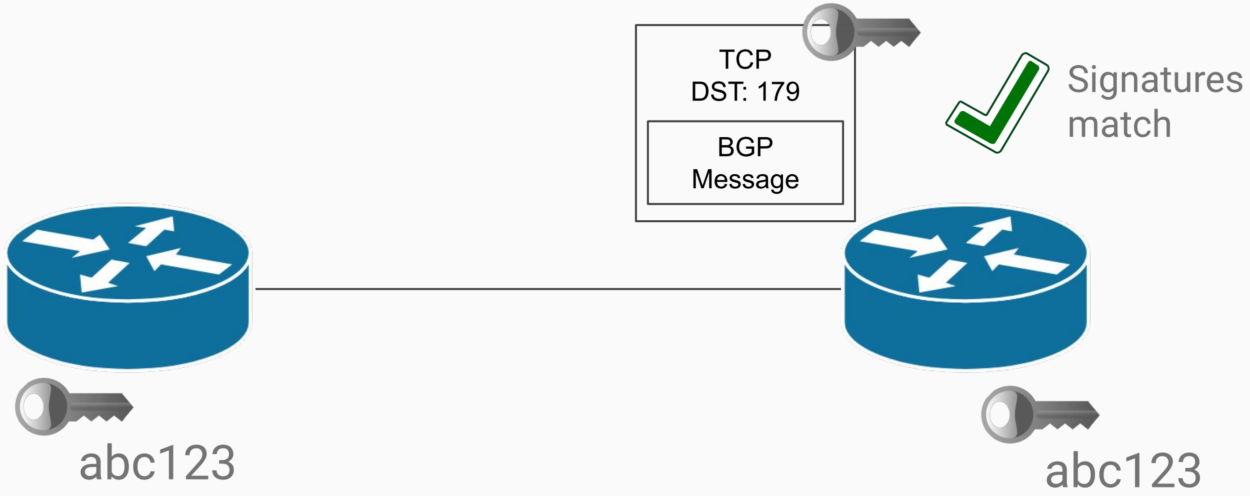
Routers must agree on the TCP-{MD5,AO} key to use beforehand



What we learned ?

- > 50% configures their border routers manually
- > 80% uses TCP authentication (TCP-MD5 or TCP-AO)

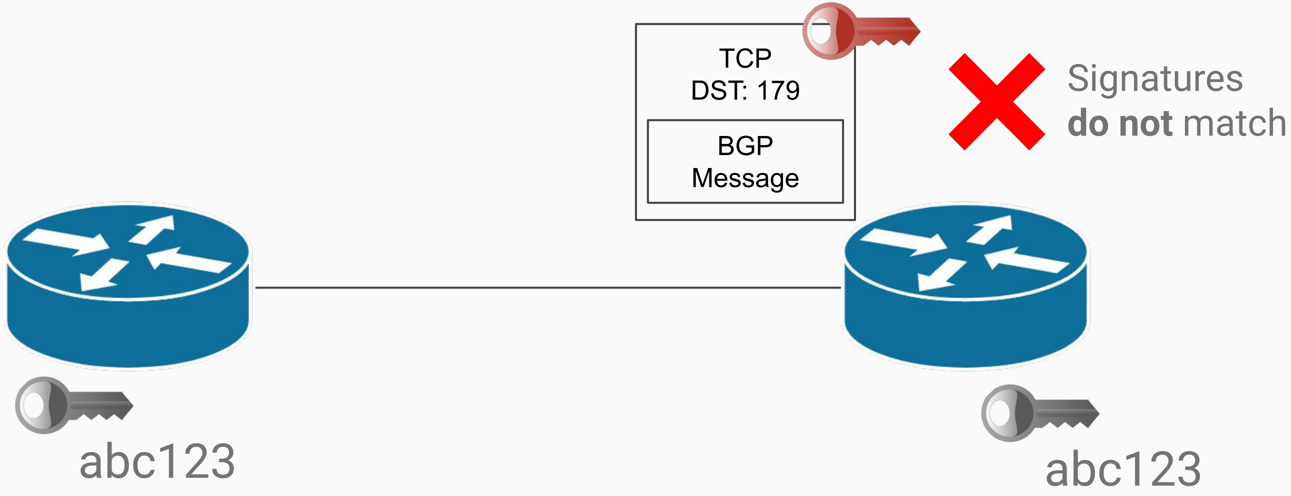
Routers must agree on the TCP-{MD5,AO} key to use beforehand



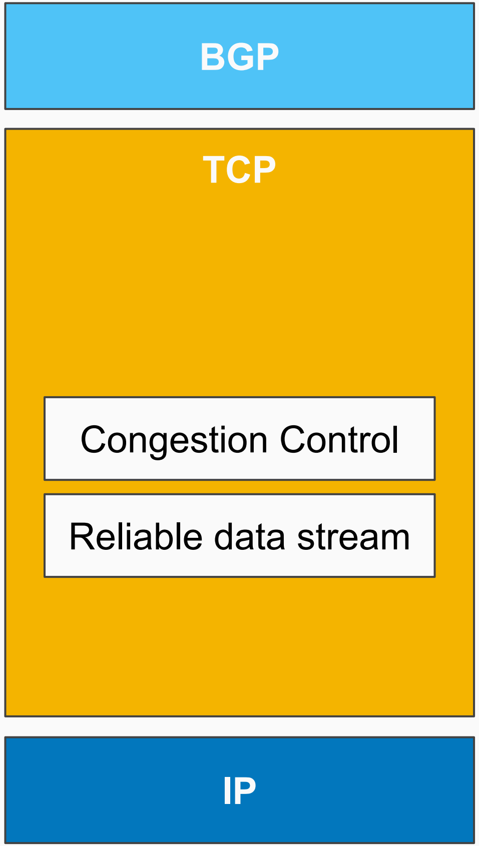
What we learned ?

- > 50% configures their border routers manually
- > 80% uses TCP authentication (TCP-MD5 or TCP-AO)

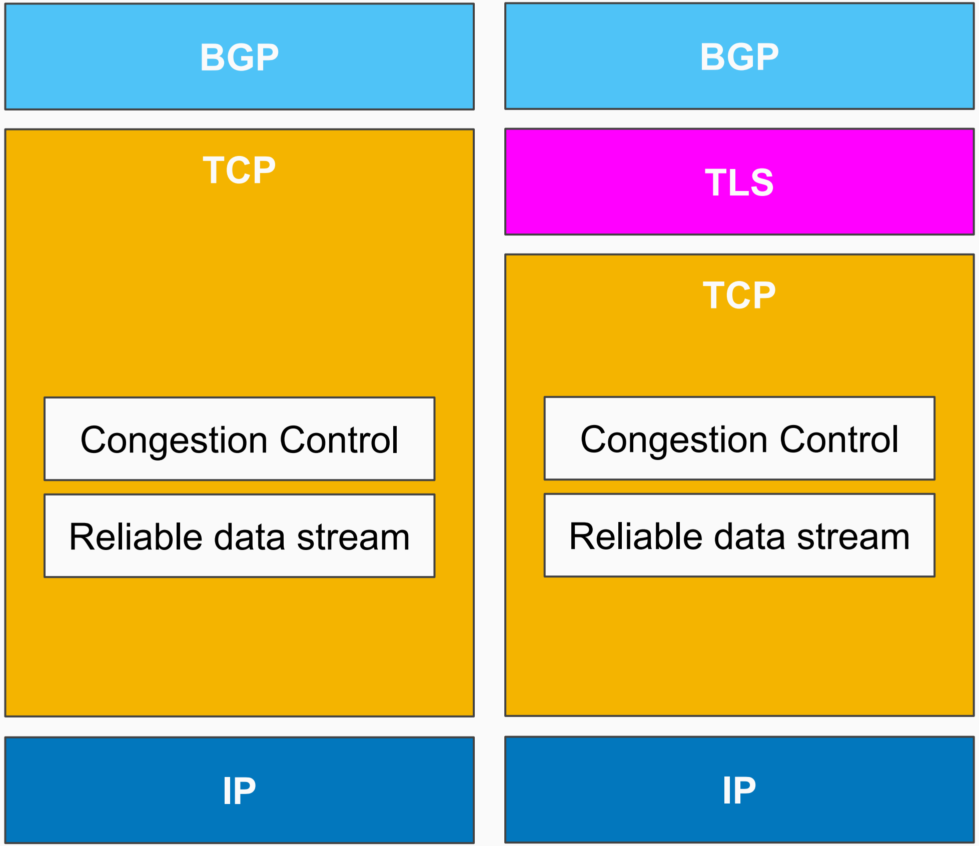
Routers must agree on the TCP-{MD5,AO} key to use beforehand



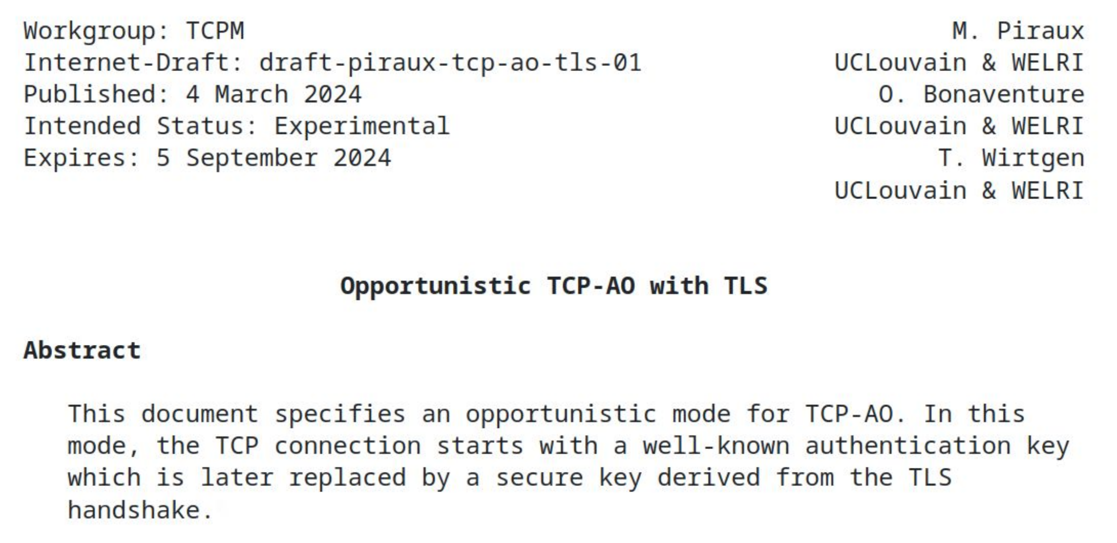
BGP over TCP



BGP over TCP/TLS



Opportunistic TCP-AO with TLS



```
Workgroup: TCPM                                              M. Piraux
Internet-Draft: draft-piraux-tcp-ao-tls-01              UCLouvain & WELRI
Published: 4 March 2024                                   O. Bonaventure
Intended Status: Experimental                           UCLouvain & WELRI
Expires: 5 September 2024                                     T. Wirtgen
                                                        UCLouvain & WELRI
```

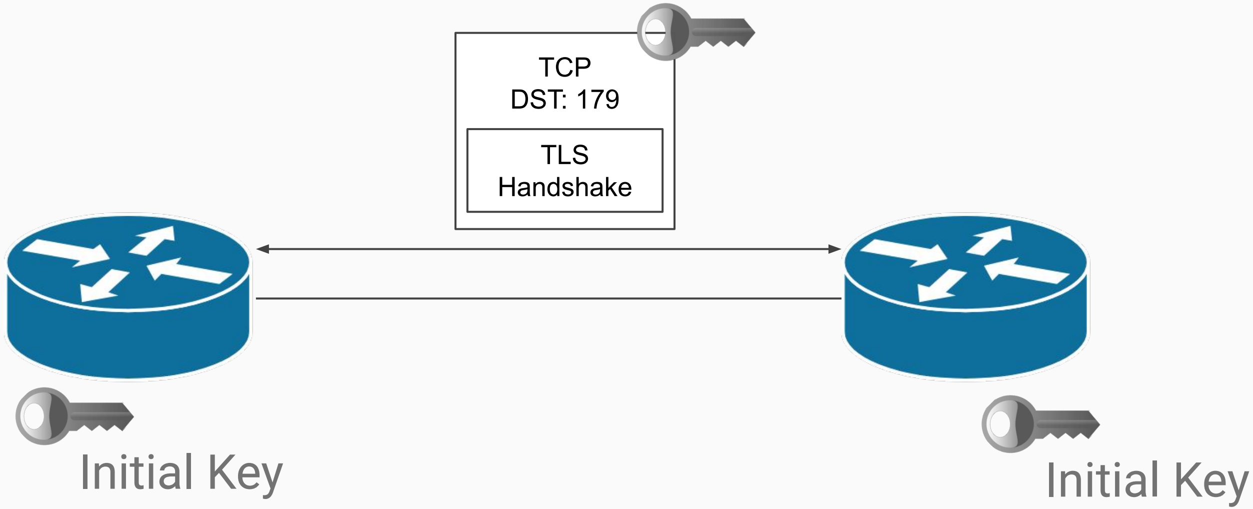
Opportunistic TCP-AO with TLS

Abstract

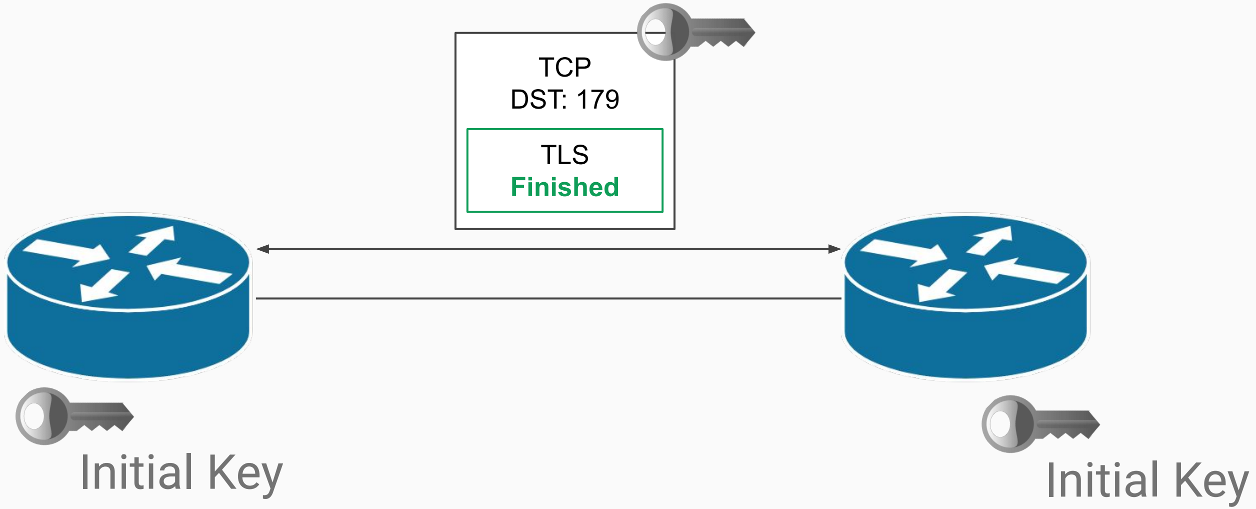
This document specifies an opportunistic mode for TCP-AO. In this mode, the TCP connection starts with a well-known authentication key which is later replaced by a secure key derived from the TLS handshake.

The TCP-{AO,MD5} key is **automatically** derived from the TLS master secret (using a TLS exporter)

Opportunistic TCP-AO with TLS (cont.)



Opportunistic TCP-AO with TLS (cont.)



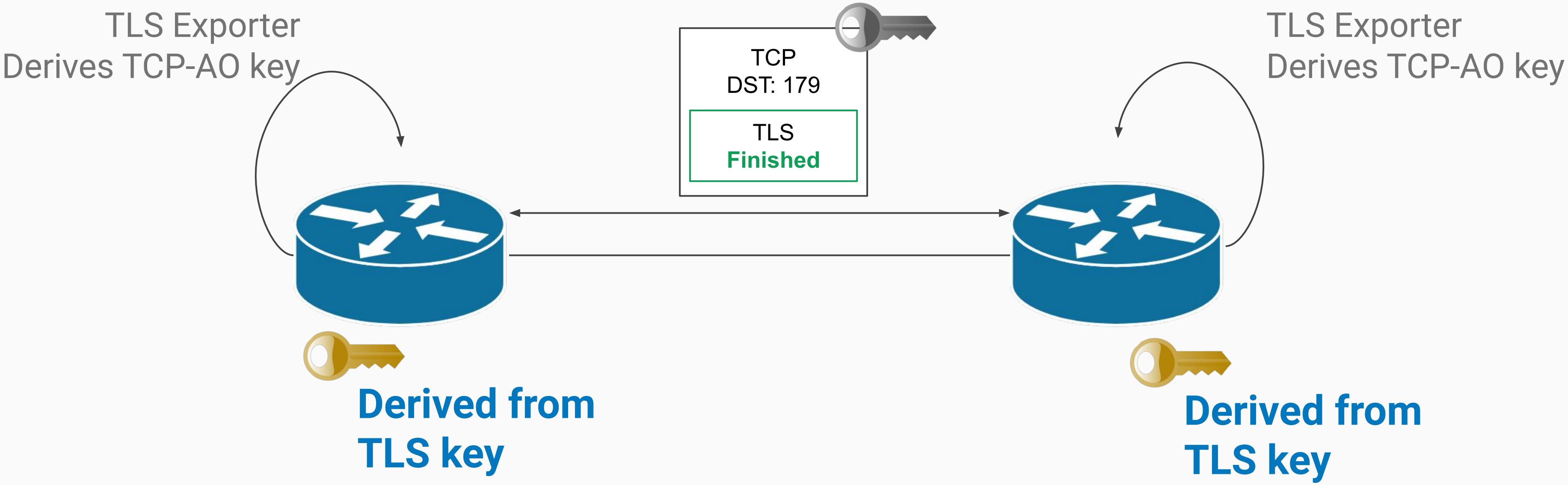
TCP
DST: 179

TLS
Finished

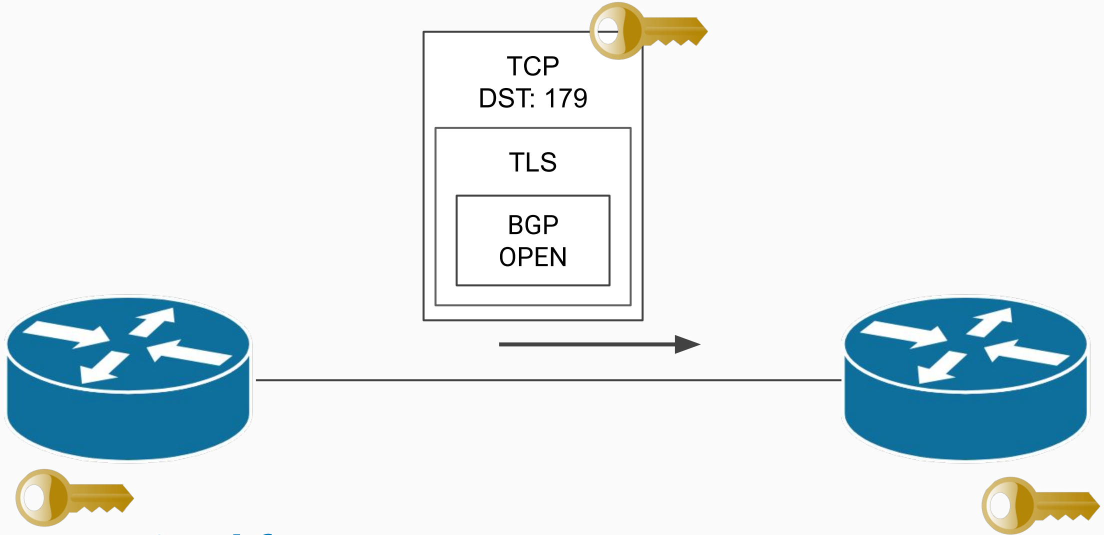
Initial Key

Initial Key

Opportunistic TCP-AO with TLS (cont.)



Opportunistic TCP-AO with TLS (cont.)



TCP
DST: 179

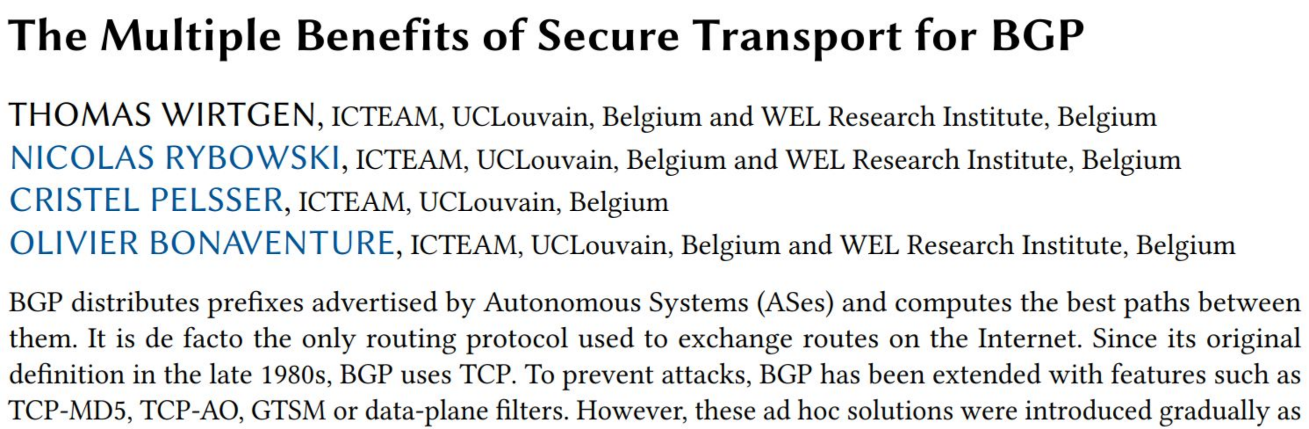
TLS

BGP
OPEN

Derived from TLS key

Derived from TLS key

TLS is the first step for BGP automation



The Multiple Benefits of Secure Transport for BGP

THOMAS WIRTGEN, ICTEAM, UCLouvain, Belgium and WEL Research Institute, Belgium
NICOLAS RYBOWSKI, ICTEAM, UCLouvain, Belgium and WEL Research Institute, Belgium
CRISTEL PELSSER, ICTEAM, UCLouvain, Belgium
OLIVIER BONAVENTURE, ICTEAM, UCLouvain, Belgium and WEL Research Institute, Belgium

BGP distributes prefixes advertised by Autonomous Systems (ASes) and computes the best paths between them. It is de facto the only routing protocol used to exchange routes on the Internet. Since its original definition in the late 1980s, BGP uses TCP. To prevent attacks, BGP has been extended with features such as TCP-MD5, TCP-AO, GTSM or data-plane filters. However, these ad hoc solutions were introduced gradually as

Will be published at the end of the year (CoNEXT 24')

We present a way to automatically configure BGP sessions using TLS certificates **without relying on another external platform**

TLS is the first step for BGP automation (cont.)

- The BGP configuration is authenticated and verified beforehand
- A TLS certificate allows configuring a BGP router
    - e.g., Changing QoS, deploying anycast services, etc.

TLS is the first step for BGP automation (cont.)

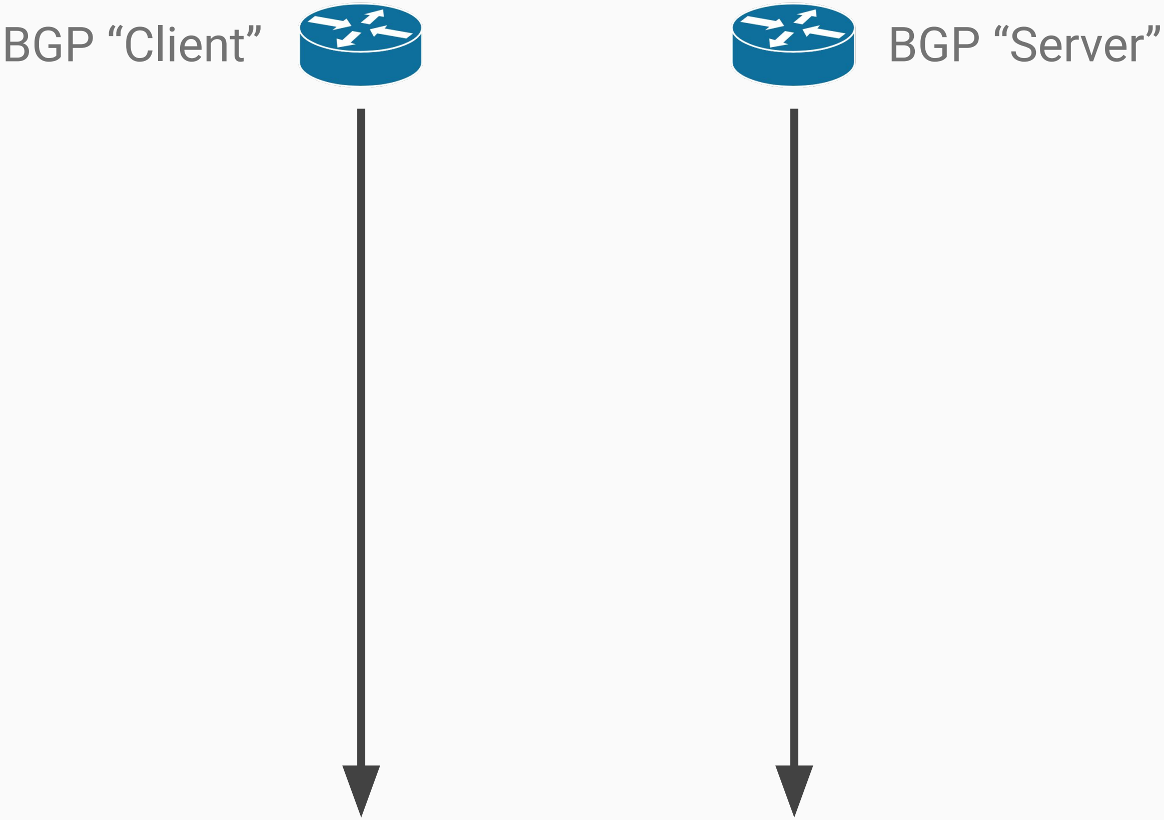
- The BGP configuration is authenticated and verified beforehand
- A TLS certificate allows configuring a BGP router
  - e.g., Changing QoS, deploying anycast services, etc.
- We provide new services for BGP

⇒ Come and see us if you would like to find out more

`thomas.wirtgen@uclouvain.be`

Backup Slides

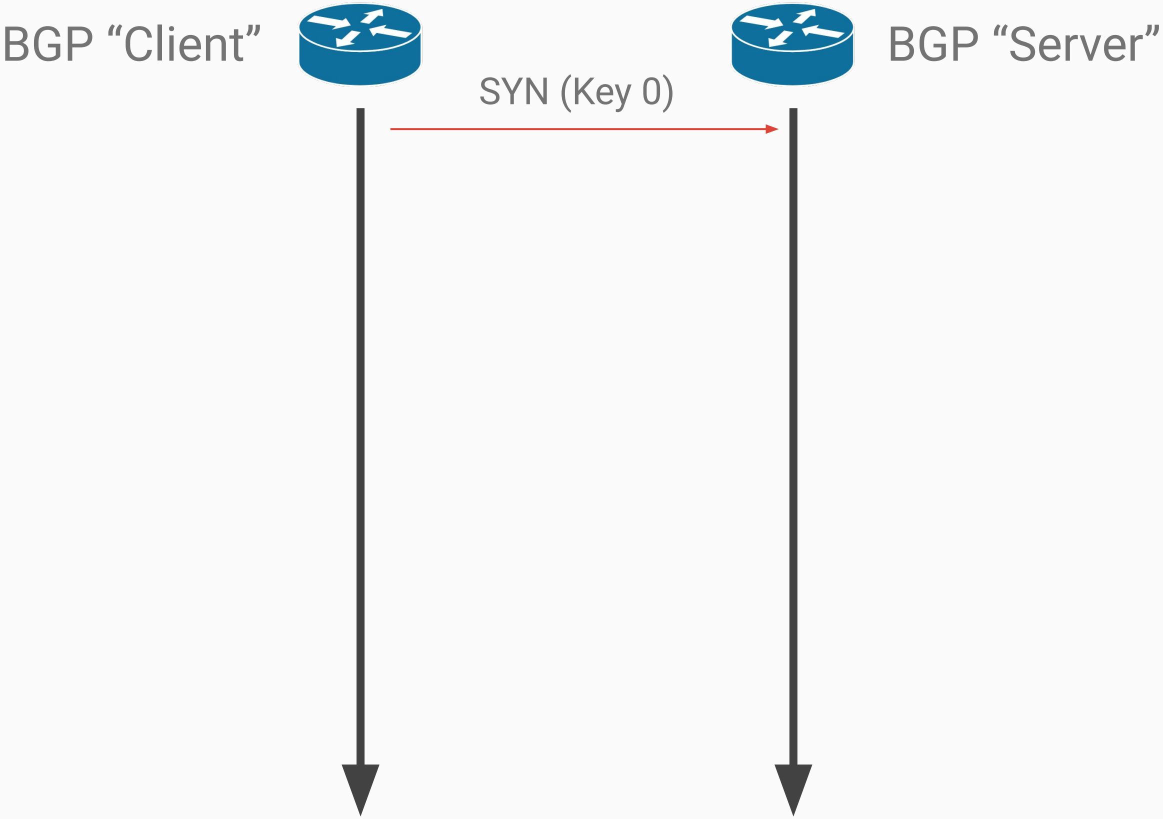
Opportunistic TCP-AO with TLS (cont.)



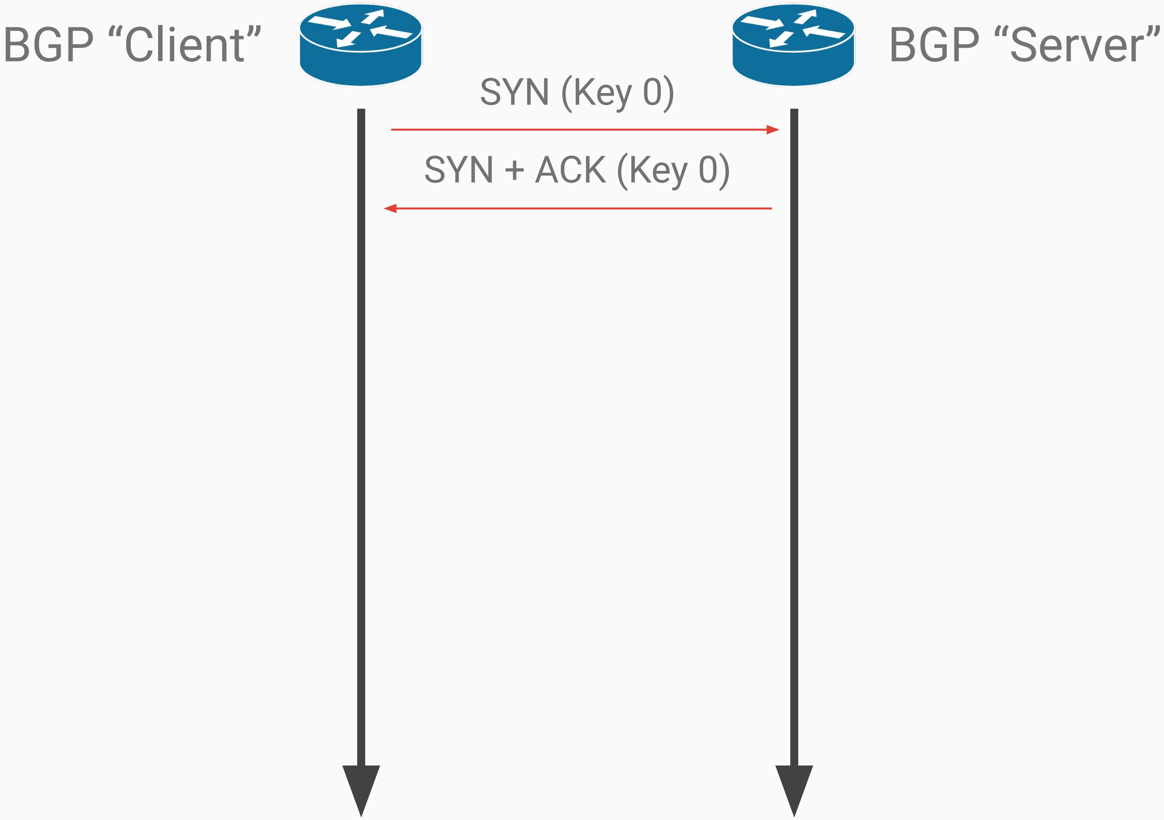
BGP “Client”

BGP “Server”

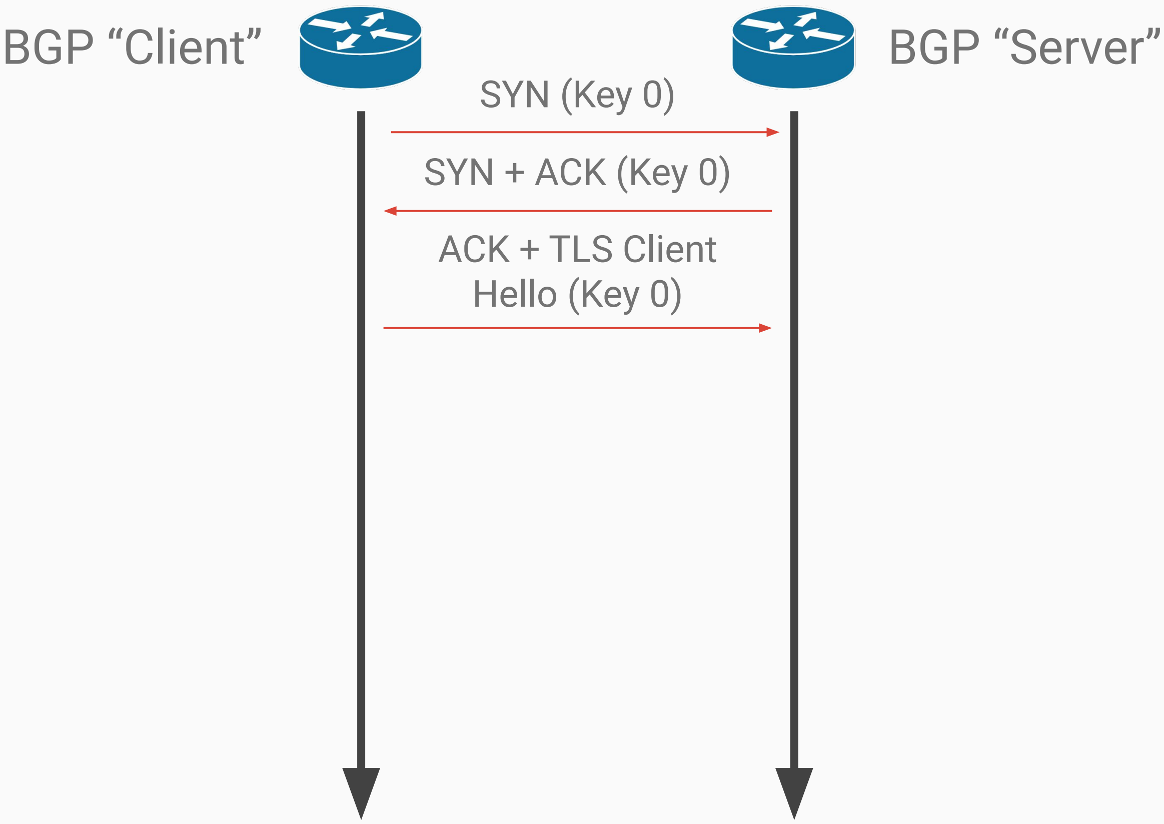
Opportunistic TCP-AO with TLS (cont.)



Opportunistic TCP-AO with TLS (cont.)



Opportunistic TCP-AO with TLS (cont.)



BGP “Client”

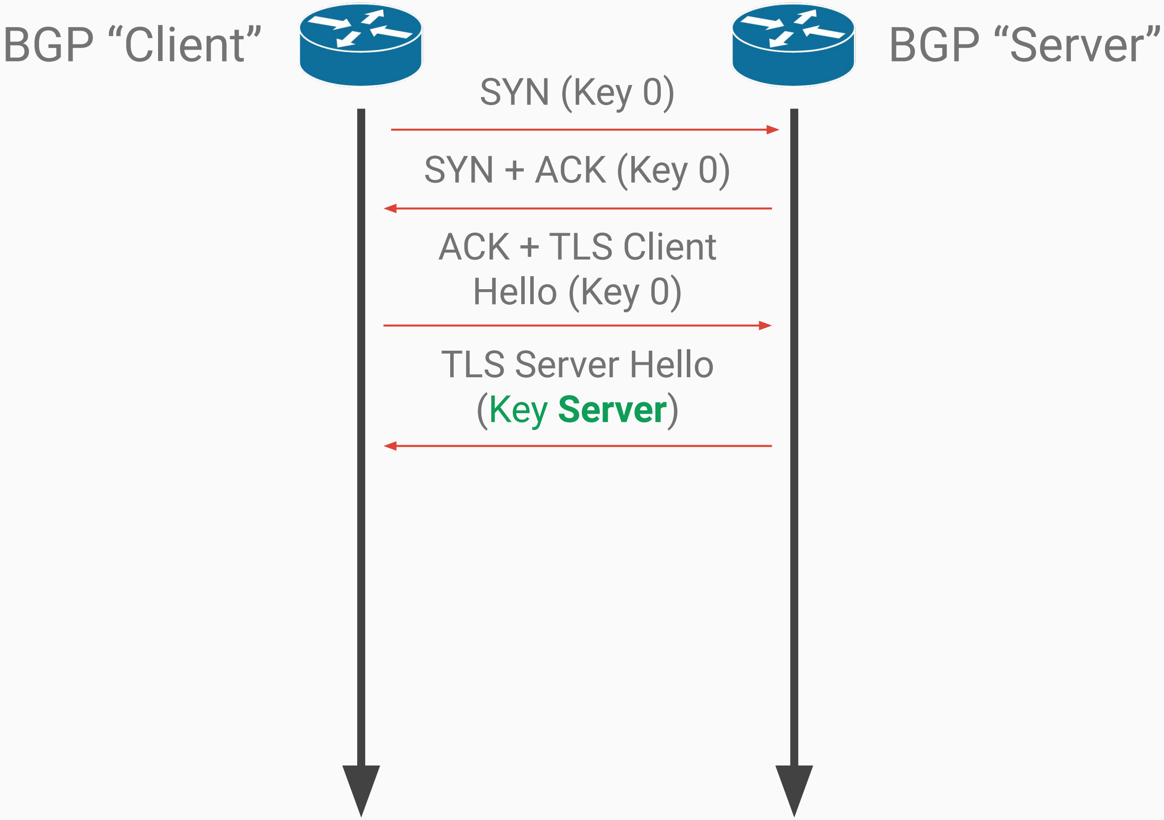
BGP “Server”

SYN (Key 0)

SYN + ACK (Key 0)

ACK + TLS Client Hello (Key 0)

Opportunistic TCP-AO with TLS (cont.)



BGP “Client”

BGP “Server”

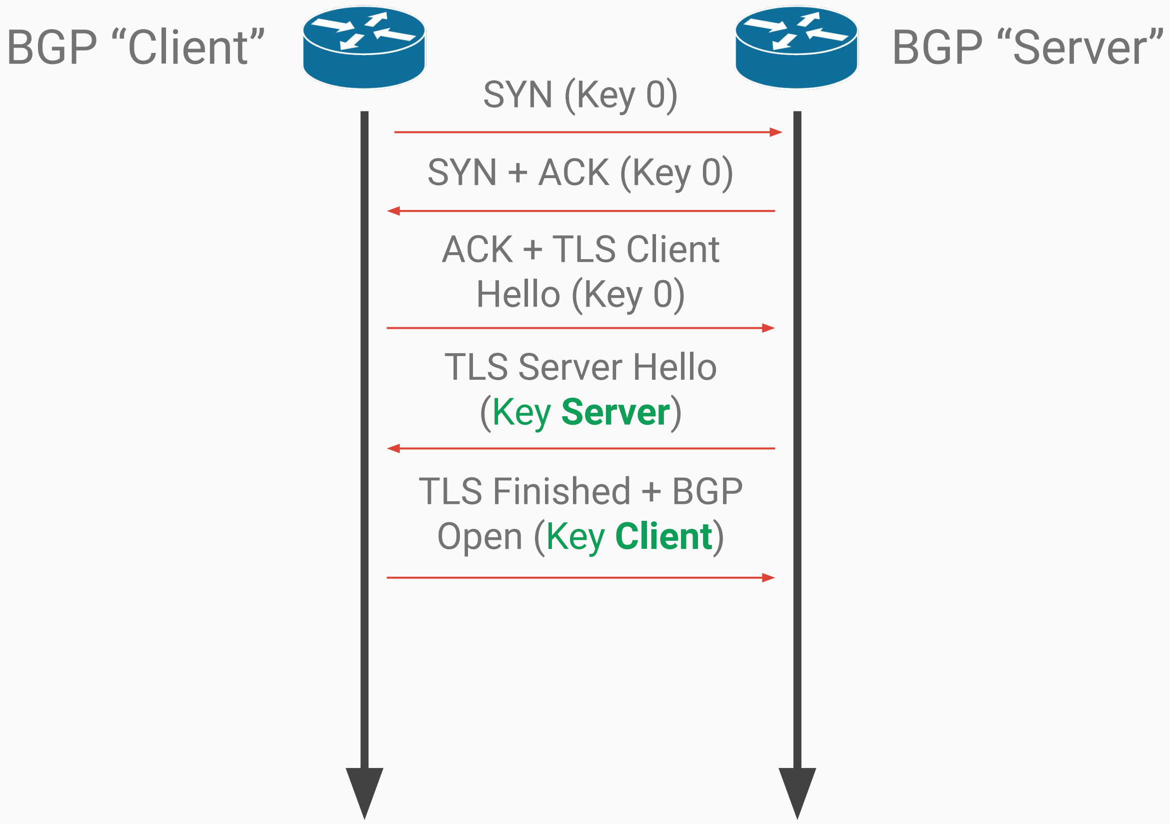
SYN (Key 0)

SYN + ACK (Key 0)

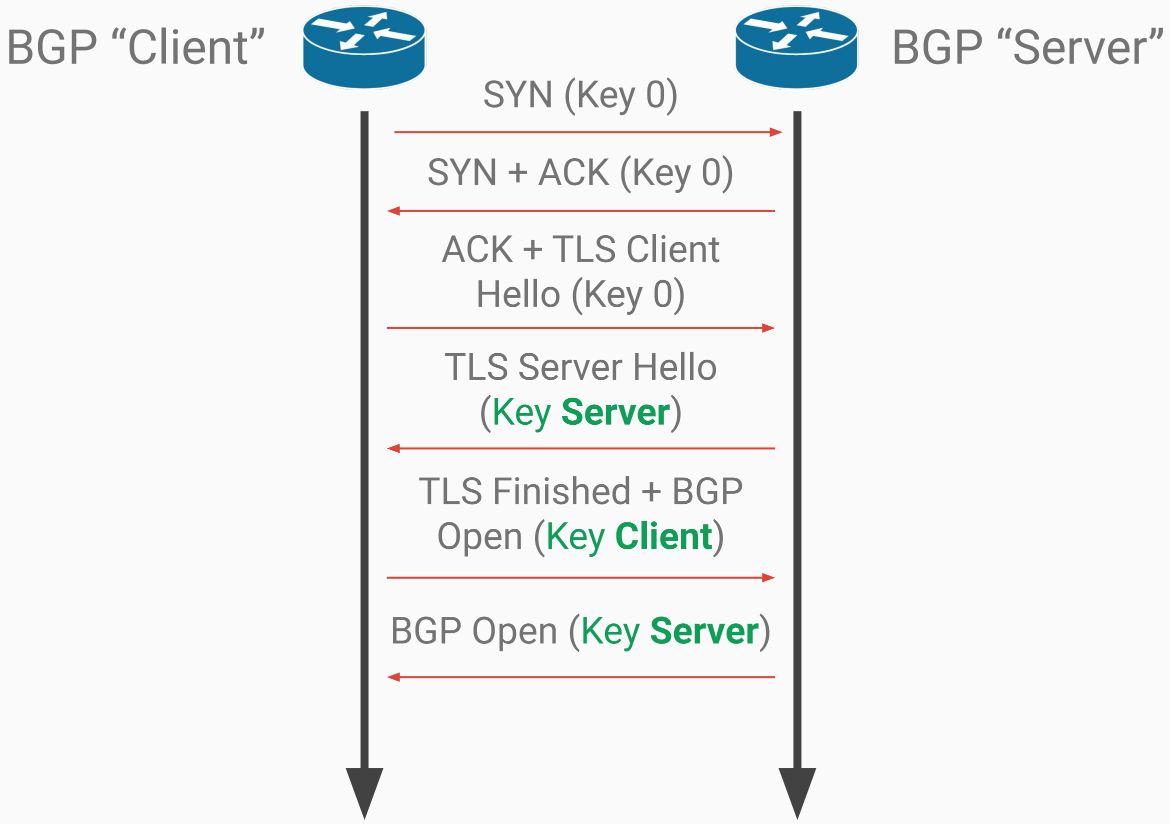
ACK + TLS Client Hello (Key 0)

TLS Server Hello (Key **Server**)

Opportunistic TCP-AO with TLS (cont.)


BGP “Client”
BGP “Server”
SYN (Key 0)
SYN + ACK (Key 0)
ACK + TLS Client Hello (Key 0)
TLS Server Hello (Key **Server**)
TLS Finished + BGP Open (Key **Client**)

Opportunistic TCP-AO with TLS (cont.)



BGP “Client”

BGP “Server”

SYN (Key 0)

SYN + ACK (Key 0)

ACK + TLS Client Hello (Key 0)

TLS Server Hello (Key **Server**)

TLS Finished + BGP Open (Key **Client**)

BGP Open (Key **Server**)