Benefits of routing over secure transport

Olivier Bonaventure
UCLouvain & WELRI

IETF123, July 2025

Agenda

- **Secure transport in a routing context**
- OSPF and BGP over secure transport

Security techniques in routing protocols

- Mainly per-packet authentication
  - RIP: Keyed MD5 in RFC2082
  - OSPF: ~~Keyed MD5 in RFC2328~~, HMAC in RFC5709, IPSec RFC4552
  - IS-IS: ~~password RFC1195~~, HMAC RFC5304
  - LDP: HMAC authentication RFC7349
  - Babel: MAC authentication RFC8967
  - BGP: ~~Keyed MD5 RFC2385~~, TCP-AO RFC5925
- Only packets with a valid authentication are accepted by routers

IS-IS Fast flooding

- ISO10589 (1992 and 2002)
  - Flow control: send one LSP at most every 33 msec
  - Faster flow control: bursts of LSPs, but not more than 10 in a row
- Faster IS-IS flooding (2005)
  - For fast convergence, remove these old timers
    - Francois, Pierre, Clarence Filsfils, John Evans, and Olivier Bonaventure. "Achieving sub-second IGP convergence in large IP networks." ACM SIGCOMM Computer Communication Review 35, no. 3 (2005): 35-44. https://doi.org/10.1145/1070873.1070877
- RFC9681 (Dec. 2024)
  - Introduces Flooding Parameters TLV to control the IS-IS timers on a per-adjacency and add receive window and congestion control…

Flow and congestion control

- Solved problems in IETF transport protocols
  - TCP
  - SCTP
  - QUIC
- Mature implementations with huge operational experience
  - Should be reused by routing protocols when flow control or congestion control are required

Candidate secure transport protocols

TLS over TCP

- TCP is general purpose
  - Already used for BGP, LDP
  - Mature code, decades of use
- TLS certificates
- TLS secures the payload
  - But not the TCP header
- TCP supports only one bytestream
- TCP mainly inside kernel
- No multicast support

TLS over SCTP

QUIC

- QUIC is targeted for HTTP/3
  - New use cases like BGP/QUIC
  - Several recent implementations
- TLS certificates
- QUIC includes TLS to secure
  - Payload and (most of) header
- QUIC supports multiple bytestreams and datagrams
- QUIC mainly in userspace
- **Multicast** QUIC extension
  - https://datatracker.ietf.org/doc/html/draft-navarre-quic-flexicast

Strengthening TLS over TCP

- It is possible to couple TLS with TCP-AO
- In a nutshell
  - TCP connection starts using well-known AO key (packets unprotected)
  - TLS derives per-connection TCP-AO key from TLS secret
  - Remaining TCP segments are protected by negotiated TCP-AO key (packets protected)
- Protocol details
  - https://datatracker.ietf.org/doc/draft-piraux-tcp-ao-tls/
- Implementation and experience

Thomas Wirtgen, Nicolas Rybowski, Cristel Pelsser, and Olivier Bonaventure. 2024. The Multiple Benefits of a Secure Transport for BGP. *Proc. ACM Netw.* 2, CoNEXT4, Article 36 (December 2024), 23 pages. https://doi.org/10.1145/3696406

https://cristel.pelsser.eu/publication/wirtgen-2024/

Agenda

- Secure transport in a routing context
- **BGP and OSPF over secure transport**

The Multiple Benefits of a Secure Transport for BGP

- Scientific paper co-authored with Thomas Wirtgen, Nicolas Rybowski and Cristel Pelsser, presented at CoNext'24 last year

Thomas Wirtgen, Nicolas Rybowski, Cristel Pelsser, and Olivier Bonaventure. 2024. The Multiple Benefits of a Secure Transport for BGP. *Proc. ACM Netw.* 2, CoNEXT4, Article 36 (December 2024), 23 pages. https://doi.org/10.1145/3696406

- Key findings
  - TCP-AO key derived from TLS
  - Extensions to BIRD BGP daemon
    - https://github.com/IPNetworkingLab/BGPoTLS
    - https://github.com/IPNetworkingLab/BGPoQUIC
  - BGP performance suffers a bit due to the utilization of TLS

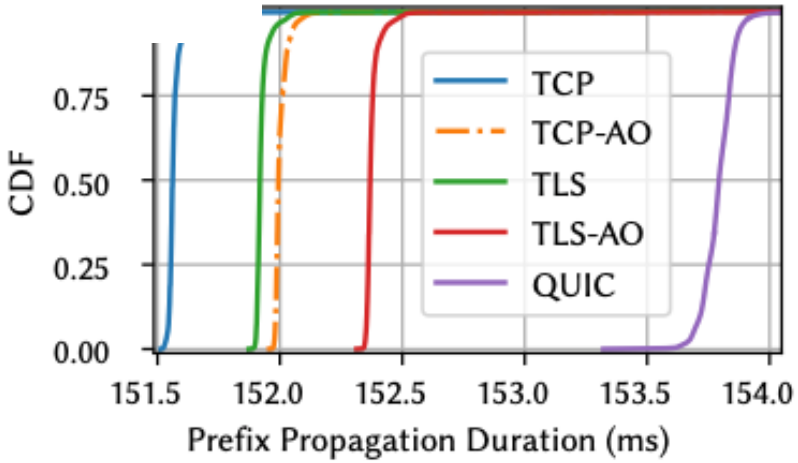


Fig. 5. Distribution of the time required to send one BGP Update every 50 ms according to the transport used in the topology described in Fig. 3. In total, 30 000 BGP updates are sent during the experiment.

https://cristel.pelsser.eu/publication/wirtgen-2024/

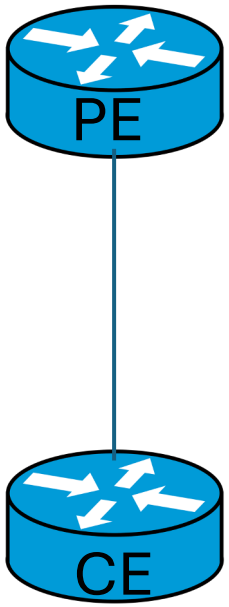
Main benefits of BGP over secure transport

- BGP routers exchange TLS certificates
- Can be used to authenticate a specific peer
  - Certificates bound to a specific IP address
  - Certificates distributed by an ISP to its own routers
  - Certificates distributed by an ISP to its peers/customers
- It is possible to extend certificates to exchange more information

See Jeff's slides

Using certificates to configure BGP sessions

- TLS certificate can include other types of information
  - router configuration commands/NETCONF
- Example
  - CE router configures QoS policies for inbound traffic on upstream PE

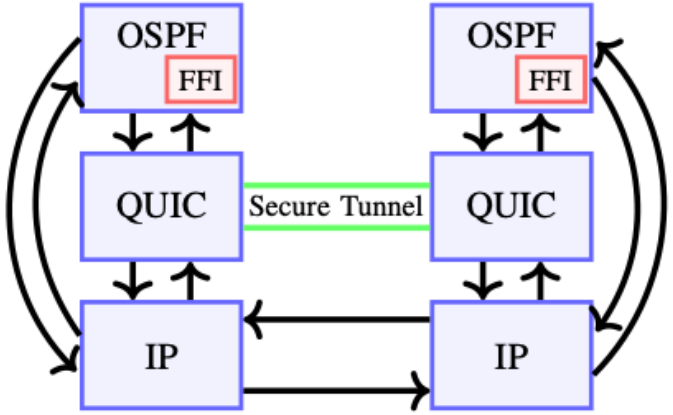


- PE router executes commands in TLS certificates when BGP session starts
- 1. ISP provides to its customer different TLS certificates with different QoS policies
  - Day time policy (prioritize interactive)
  - Night time policy
  - Videoconference policy, …
- 2. To activate a different QoS policy, CE changes TLS certificate and restarts BGP session
  - No interaction required with ISP

Many other possibilities described in the paper

OSPF over QUIC

- Main motivation
  - Extend OSPF to provide ordered FIB updates to avoid transition loops during planned topology changes



(a) High level design.

  - BIRD extension https://github.com/nrybowski/ofiquic-artefacts

- Details in :
  - Rybowski, Nicolas ; Pelsser, Cristel ; Bonaventure, Olivier. *oFIQUIC: Leveraging QUIC in OSPF for seamless network topology changes.* IFIP Networking http://hdl.handle.net/2078.1/286860

Conclusion

- Routing protocols SHOULD leverage existing secure transport protocols and not invent their own secure transport

- QUIC alone and TCP or SCTP with TLS bring
  - Efficient flow control working on a wide range of devices, from IoT to large servers
  - Efficient reliability techniques tuned for throughput and latency
  - Efficient congestion control if needed
  - Strong security features (once TCP-AO is coupled with TLS)
  - Mature implementations with operational experience