BY Developers FOR Developers

Storage Developer Conference
September 22-23, 2020

SMB over QUIC
Files without VPN

Sudheer Dantuluri, Thomas Salemy
Microsoft Corp.

Agenda

- QUIC Overview
- Motivation
- SMB over QUIC
- Integration
- Certificate Management
- Performance
- Demo

QUIC Overview

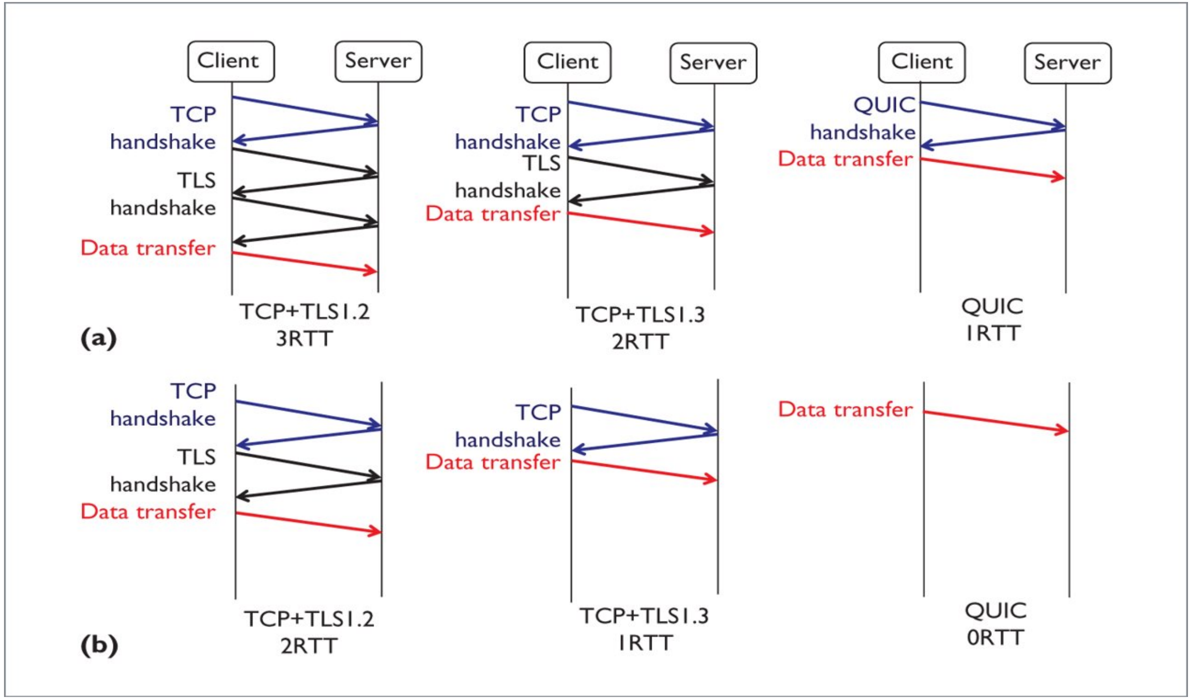
High Level Overview
QUIC

- New secure networking transport on top of UDP. Basis for HTTP/3.
- Faster connection set up
  - 1 Round Trip(1-RTT) for initial connections.
  - 0-RTT for resumed connections.
- Better Security
  - Provides mutual auth, TLS 1.3
  - Mitigates MITM attacks as most of the packet is encrypted

QUIC Overview Continued.

- Improvements over HTTP2 and TCP
  - No head-of-line blocking
  - Better transitions between networks
  - Loss recovery
    - more SACK blocks
    - no retransmission ambiguity
    - latest congestion control
  - Portability and agility (UDP and user-mode)
- Being standardized by IETF

QUIC connection latency reduction: 0-RTT



Motivation

Problems

- SMB cannot be easily used over the internet
  - Need for VPNs for remote traffic
  - Cannot be used to access cloud providers

SMB over QUIC Overview

Advantages

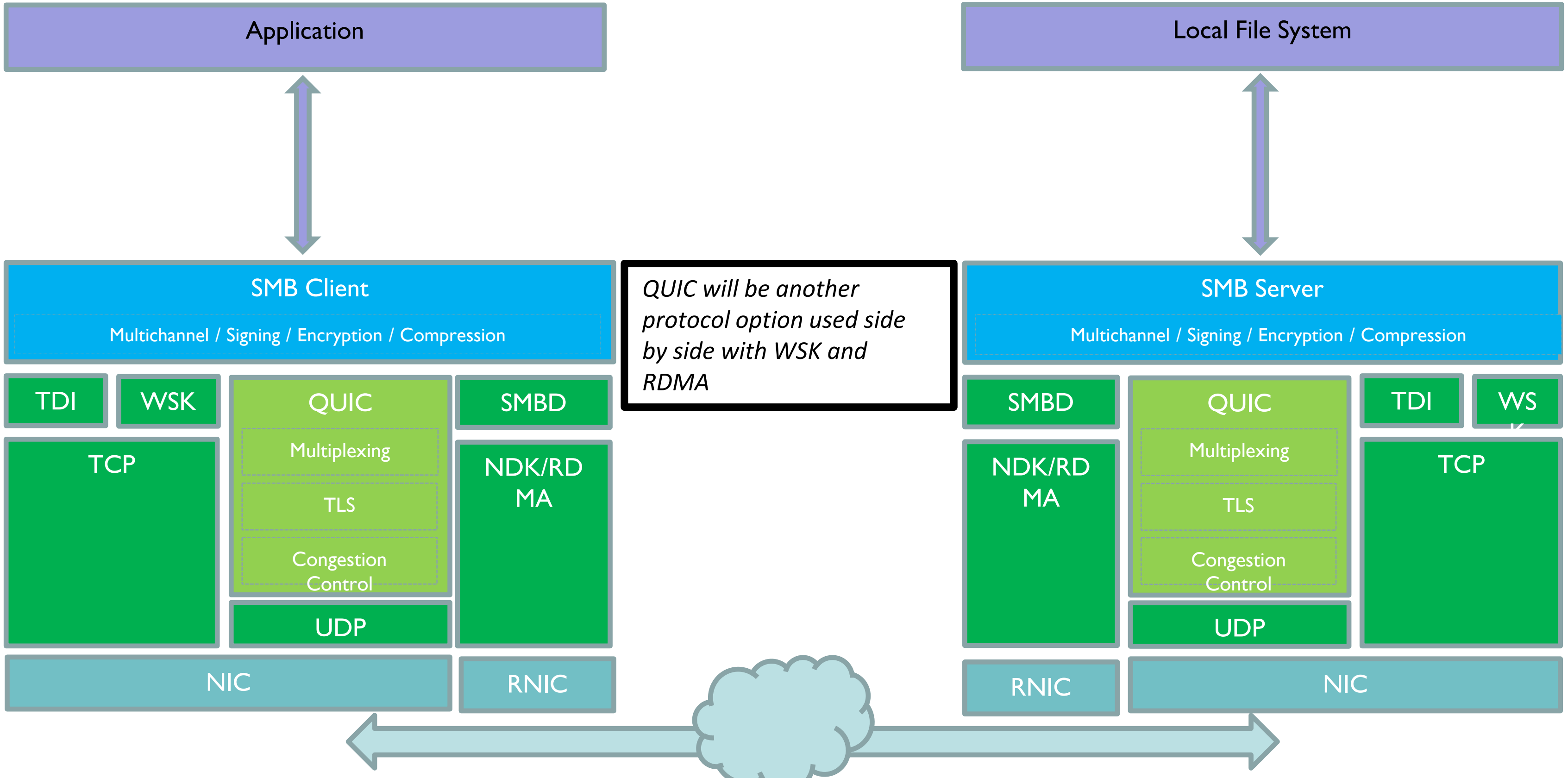
- Security
  - Prevents Server Spoofing
  - QUIC connection is always protected by TLS 1.3 encryption.
- Portability
  - Cases where SMB Port: 445 is blocked, SMB over QUIC (UDP:443) will work
  - Google experiments show a 93% connection success rate when connecting to port 443.
  - Windows kernel QUIC implementation allows multiplexing of multiple protocols on UDP port 443 using ALPN.

Downsides

- Poorer perf than SMB-encrypted
  - No hardware offload support
- Kerberos cannot be used without means to reach KDC from the client so it defaults to NTLM
  - NTLM exchanges are tunneled inside TLS 1.3 connection.
  - WIP – KDC proxy to work over QUIC
- TLS Encryption is machine to machine rather than user to machine.

Integration

SMB/QUIC: Components

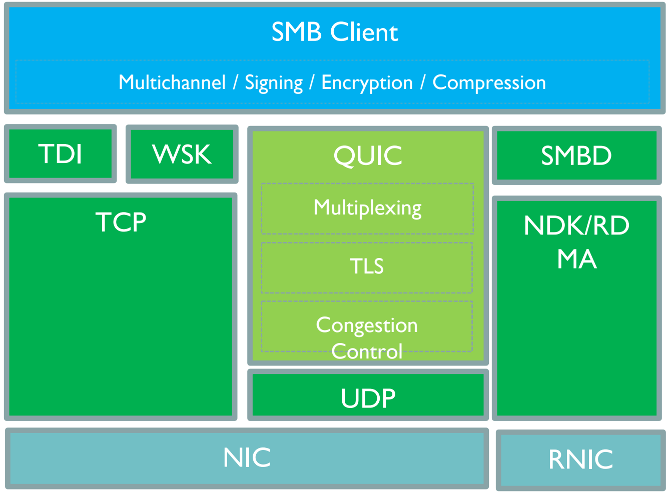


QUIC will be another protocol option used side by side with WSK and RDMA

SMB Protocol Stack

- SMB will be layered on top of the QUIC stack.
  - No difference for multichannel
  - No SMB signing/encryption by default
  - SMB over QUIC will use the server certificate to make sure there is no server spoofing attack.
  - No changes to SMB authentication
  - QUIC multisession is not used on the server.
  - Negotiable SMB Connection Setting context for secure connections
    - Client must append the negotiation context ID=0x0006 to learn if the transport layer security is accepted.

SMB/QUIC: Client.



1. Client opens \\ServerName\Share\foo.tst

2. Client resolves ServerName using DNS

3. Client fires parallel connect attempts using TCP/IP and QUIC

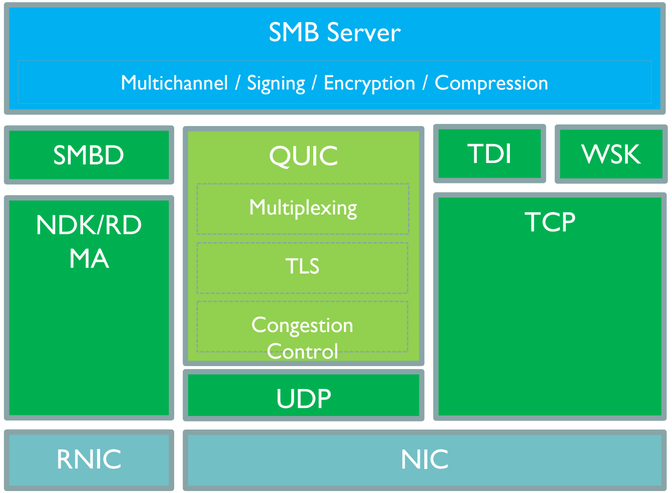
4. Client will start using whatever channel was connected first

5. Client's multichannel will negotiate interfaces with server and will select most optimal protocols

6. Client send streams/SMB messages

- Client does not know if server supports QUIC at all or supports only TCP or only QUIC so it has to attempt both.
- By default TCP/IP is given a bit of head start to establish a connection.

SMB/QUIC: Server



1. Server opens endpoints listening on UDP 443

2. Server receives new QUIC connection requests

3. Server finds the certificate for the new QUIC connection

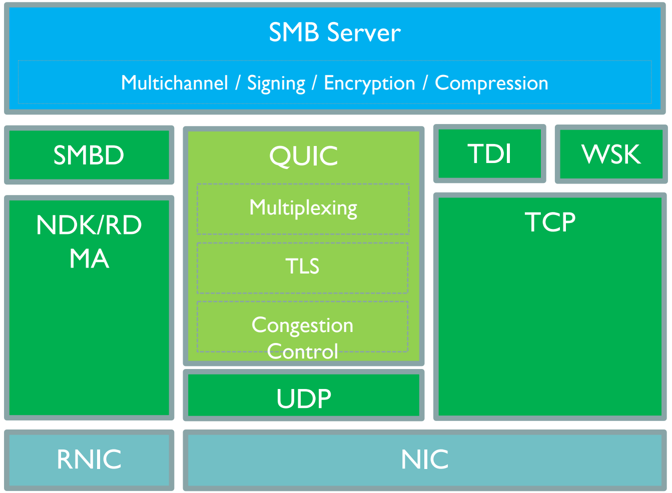
4. Server accept the connection

5. Server receives QUIC streams/SMB messages

- Server starts both TCP/IP and QUIC listeners by default.
- Server can selectively start TCP/IP or QUIC listeners or both.

Certificate Management

SMB/QUIC: Server Management



Server supports multiple Secure Principal Names.

By default SMB server assumes there are no certificates associated with the principal names.

SMB Server creates a listening QUIC socket, but it does not register any certificates so any attempt to connect will fail at TLS.

User can associate a certificate with SPN using new management utility. Certificate will be installed into local machine store, and registered with QUIC. From this point on connections using QUIC to that SPN will pass TLS.

Or customer can disable the WSK listeners or disable TCP:445 on the corporate firewall. This will force QUIC when server is accessed from internet.

Powershell - SMB Server

- New-SmbServerCertificateMapping
- Remove-SmbServerCertificateMapping
- Get-SmbServerCertificateMapping
- Get-SmbServerConfiguration
  - RestrictNamedPipeAccessViaQuic
  - DisableSmbEncryptionOnSecureConnection
  - EnableSMBQUIC

Powershell – SMB Client

- New-SmbMapping –TransportType QUIC / net use /transport:quic
  - Complete validation of the server certificate on the client.
- New-SmbMapping –TransportType QUIC -SkipCertificateCheck
  - Also, "*net use /transport:quic /skipcertcheck*"
  - No validation of the server certificate on the client
  - Not recommended for internet facing servers.
  - Intended for within-enterprise use – communication channel is secure.
- Get-SmbMapping
  - Displays TransportType used for the mapping alongside other properties.
- Get-SmbClientConfiguration
  - ForceSMBEncryptionOverQUIC
  - SkipCertificateCheck

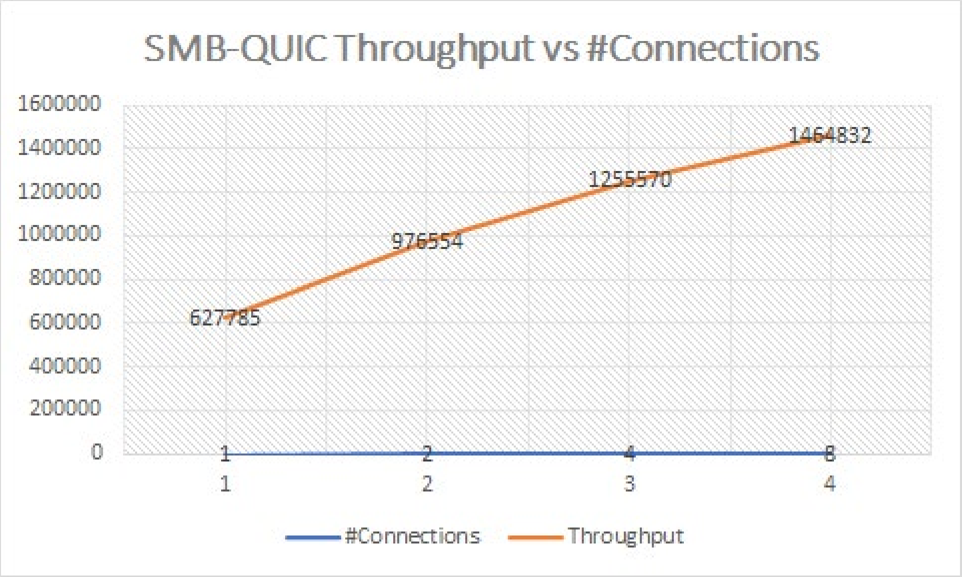
Certificate Usage

- Avoid self-signed certificates.
- Always use certificates from a trusted root authority

Performance

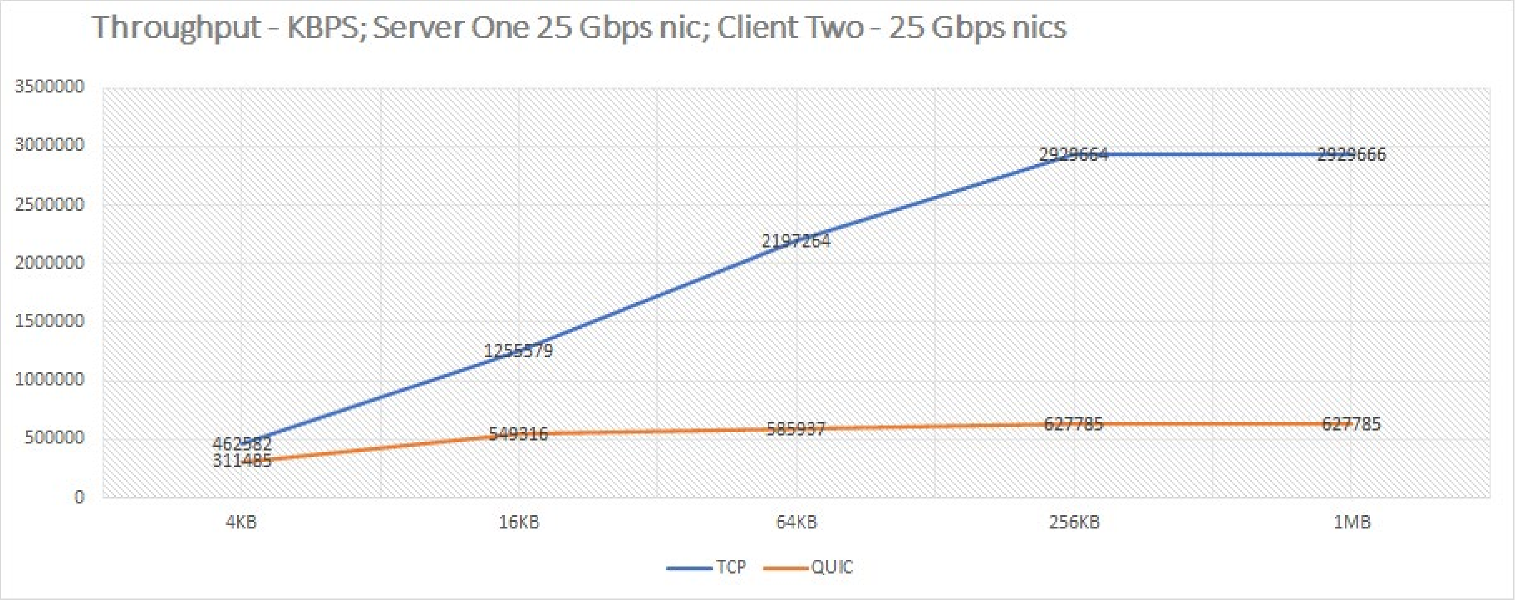
Performance - QUIC

- Queue Depth – 512
- Storage – ramdisk

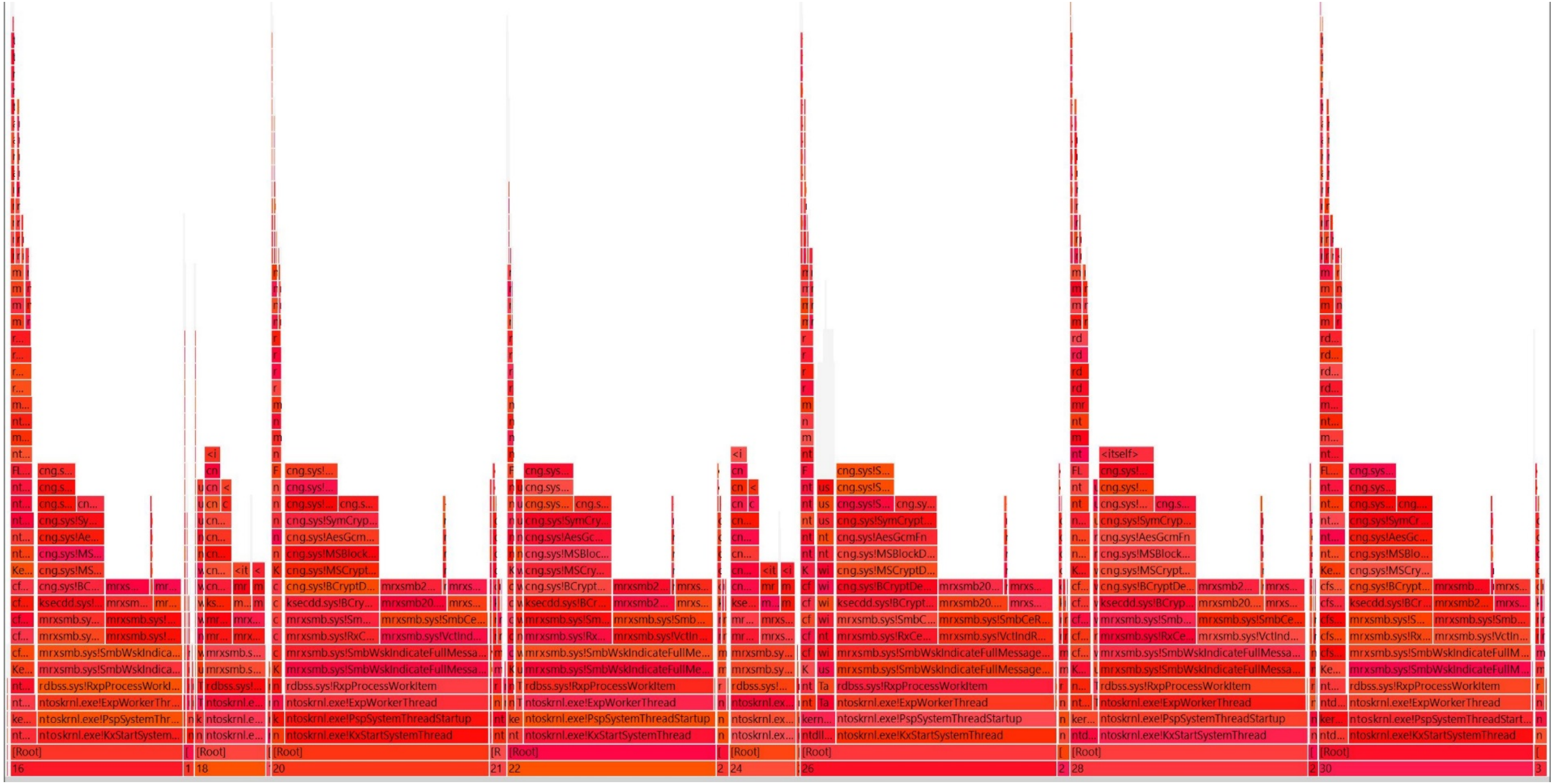


Performance comparison with TCP

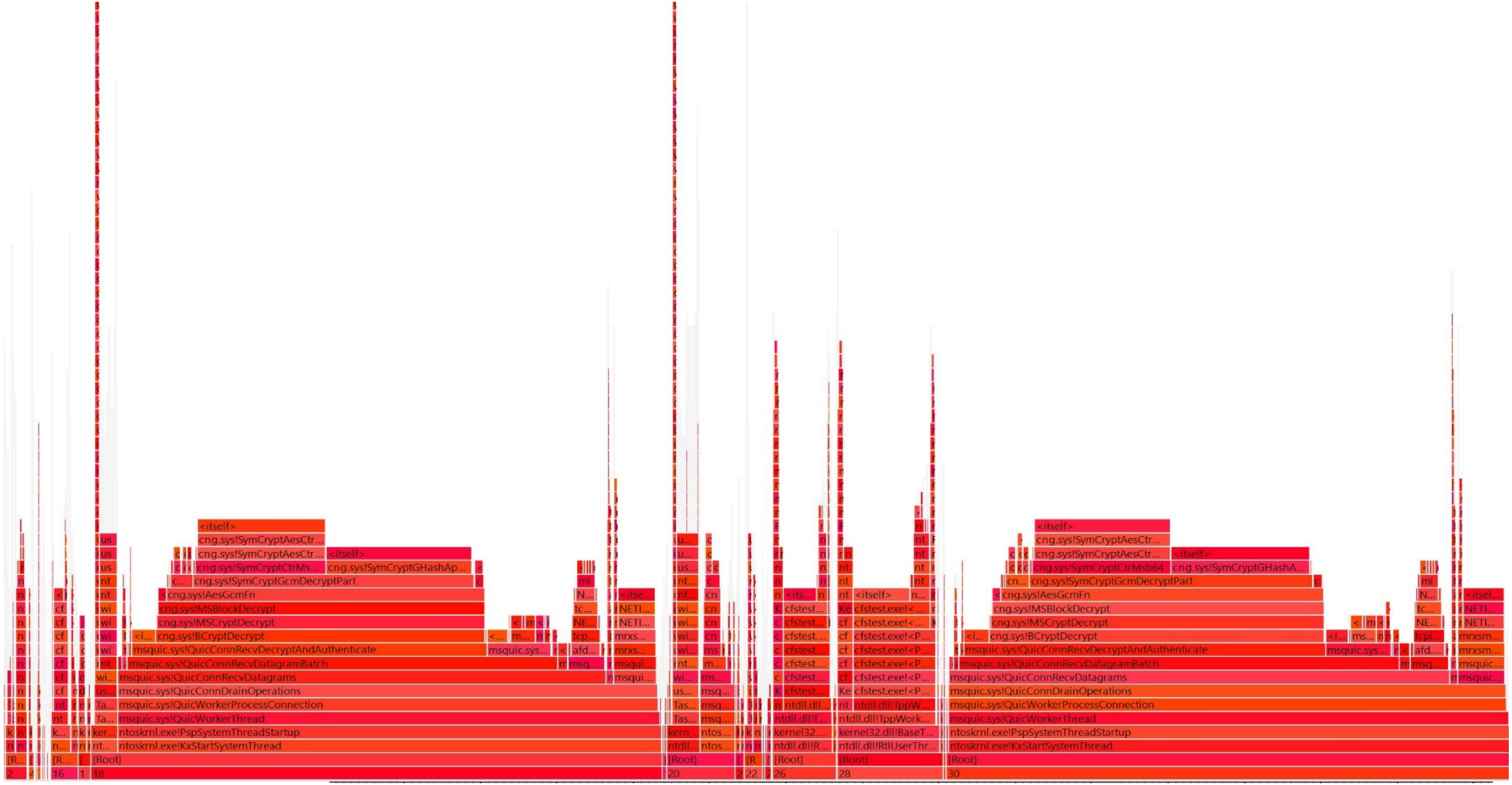
- TCP with SMB Encryption turned on.



SMB TCP Client flame (Encryption : ON)



SMB QUIC flame



Demo

Want to know more?

- For more information and release details - please contact **nedpyle@microsoft.com**

Q&A?

Please take a moment
to rate this session.

Your feedback matters to us.