STORAGE DEVELOPER CONFERENCE
SDC EMEA 21
BY Developers FOR Developers
Virtual Conference
June 8, 2021

SMB over QUIC

Obaid Farooqi
Microsoft

What I am going to cover

- SMB over a new transport QUIC
- AES-GMAC Signing

Problems fixed by SMB over QUIC

- SMB uses TCP port 445
- Port 445 is blocked by firewalls on the Internet
- SMB over Internet either requires VPN
- Or requires port 445 to be opened in firewall

SMB over QUIC Details

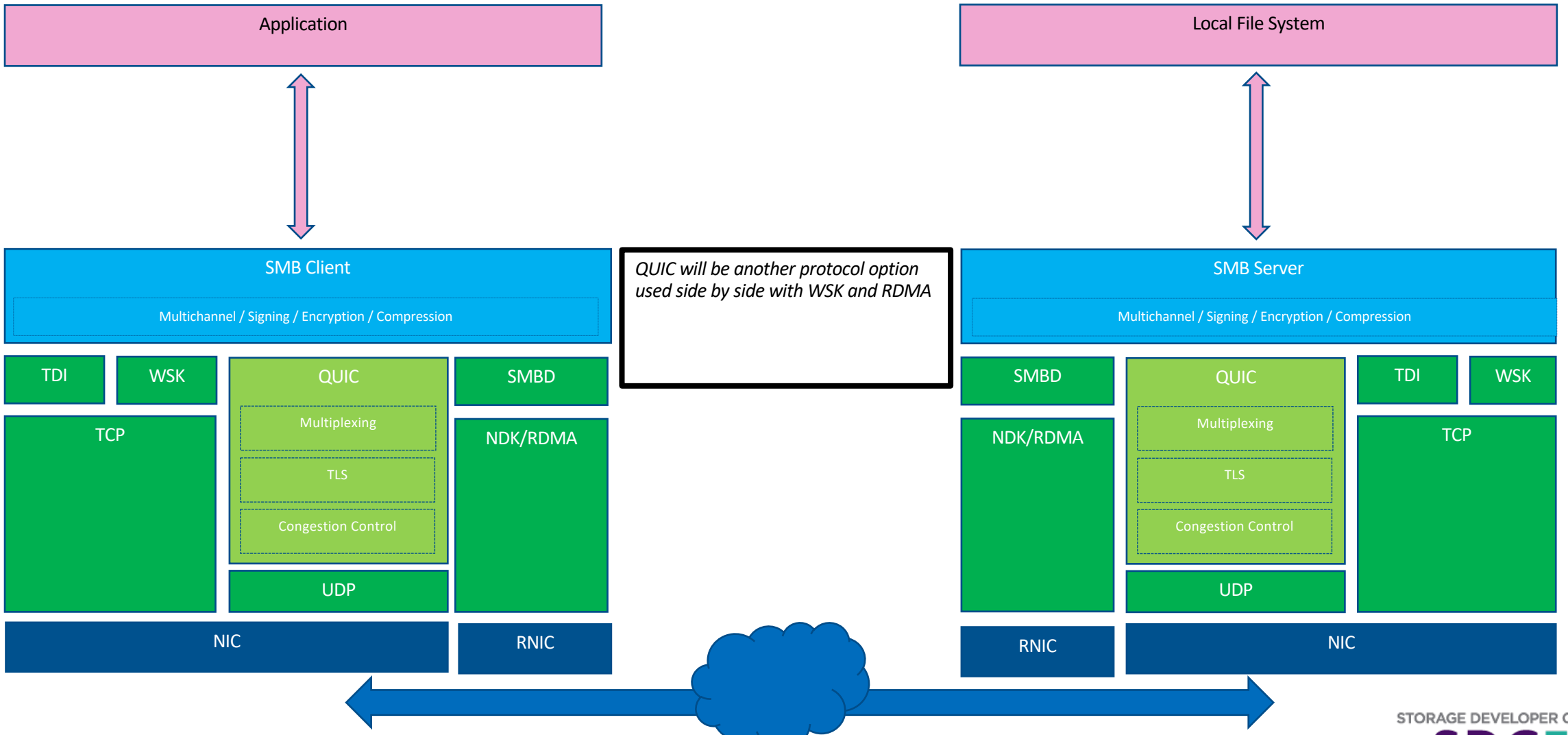
What is SMB over QUIC?

- QUIC is a new **transport** for SMB
- Available in Windows 10 21H1 and Windows Server 2022 and later
- Offers all the SMB goodness to remote workers and cloud users (VPN not needed!)
- Encapsulates every single SMB message so no malicious actor can sniff the file data and authentication payloads
- Makes NTLM more secure
- QUIC selected seamlessly; no user configuration required

A quick overview of QUIC

- Secure networking **transport** leveraging UDP
- Faster connection set up compared to TLS on TCP
  - 1 Round Trip(1-RTT) for initial connections.
  - 0-RTT for resumed connections.
  - No TCP Handshake
- Built in TLS1.3 security
- Provides mutual authentication
- Mitigates MITM attacks
- No TCP head-of-line blocking

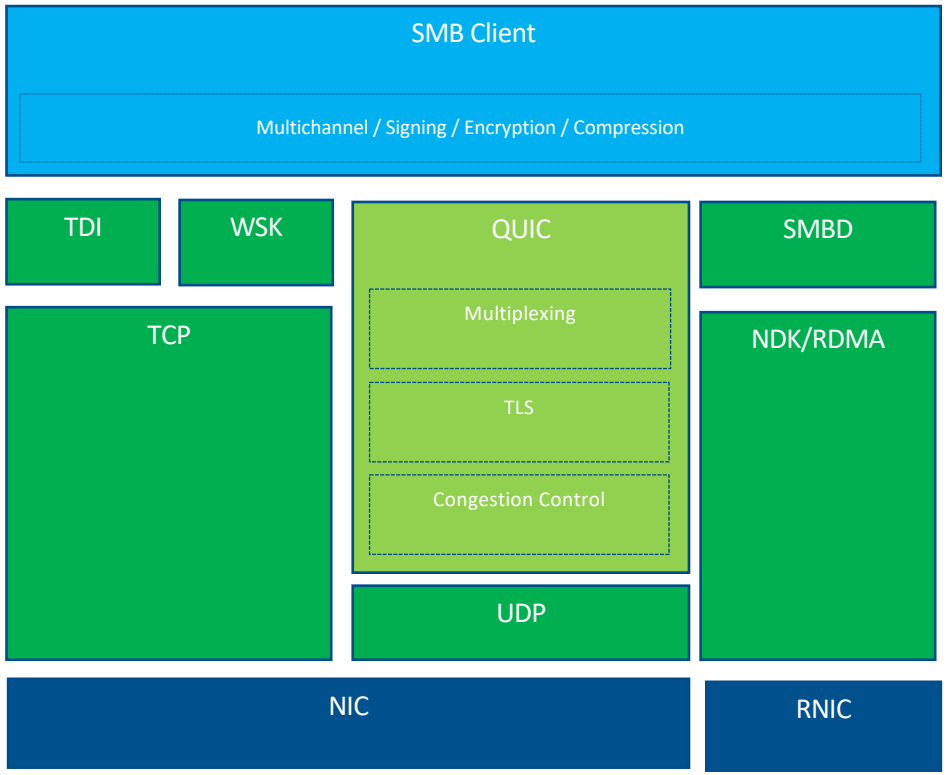
SMB/QUIC: Components



SMB-over-QUIC: What's different?

- SMB will be layered on top of the QUIC stack.
- Multichannel works as usual
- No SMB signing/encryption by default
- No changes to SMB authentication

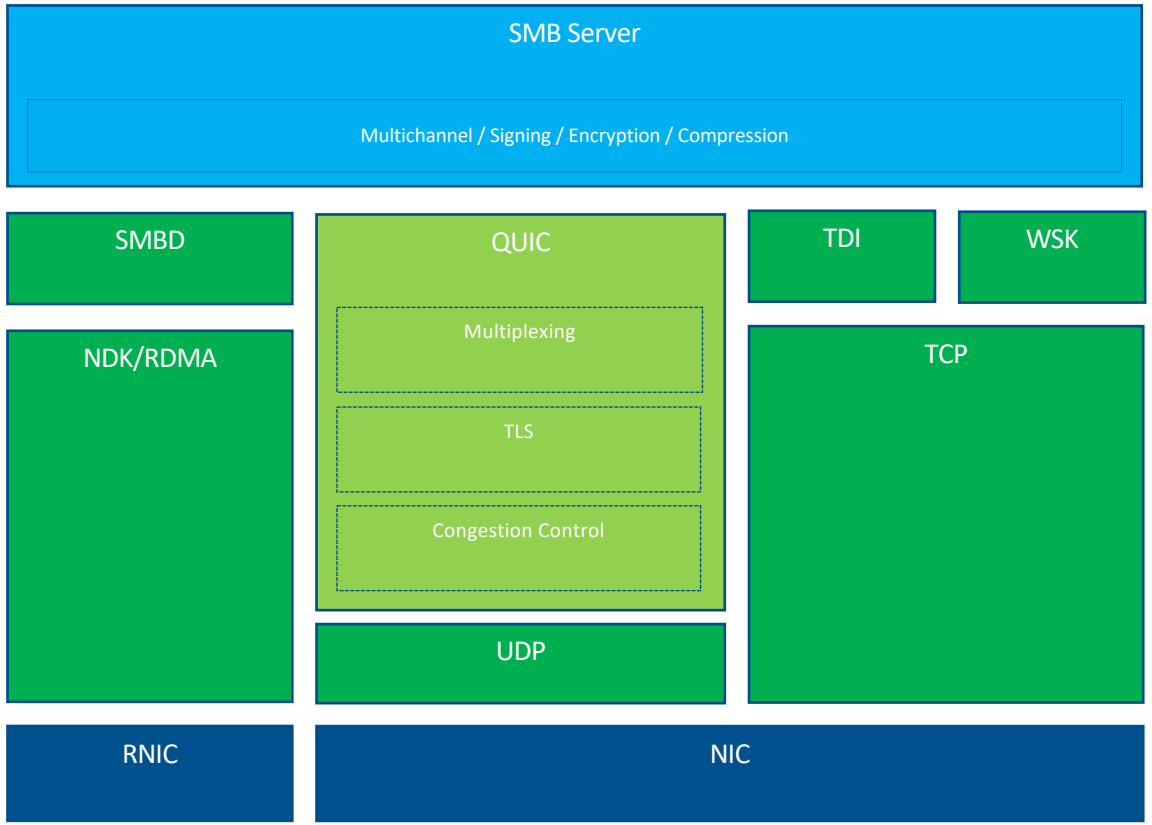
SMB/QUIC: Client



1. *Client opens \\ServerName\Share\foo.tst*
2. *Client resolves ServerName using DNS*
3. *Client attempts TCP and QUIC simultaneously**
4. *Client will start using whichever connects first*
5. *Client's multichannel will negotiate interfaces with server and will select most optimal protocols*
6. *Client sends SMB messages*

- Client does not know if server supports QUIC at all or supports only TCP or only QUIC so it attempts both.
- *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 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.

SMB Encryption on QUIC

- QUIC provides built-in TLS 1.3 encryption
- SMB over QUIC has two types of encryptions
  - Encryption offered by SMB
  - Encryption offered by QUIC transport
- Technically, both can be present simultaneously
- Double encryption imposes performance penalty

Disabling SMB Encryption on QUIC

- When client connects over QUIC
  - Client sends a negotiate transport context (NTC)
  - This indicates that client will accept QUIC encryption instead
  - Server must accept transport security
  - Server and client will not use SMB encryption over QUIC
- There are configuration options that control this behavior
- By default, SMB encryption is disabled on QUIC
- If ForceSMBEncryptionOverQUIC is set, client will skip NTC which will result in SMB encryption on QUIC

SMB2_TRANSPORT_CAPABILITIES

- Defined in MS-SMB2 section 2.2.3.1.5
- Contains flag
  - SMB2_ACCEPT_TRANSPORT_LEVEL_SECURITY
- Only possible value for this flag is 0x00000001
- Indicating that client will accept QUIC encryption and SMB encryption is not needed
- SMB encryption will be disabled over QUIC

Certificate Management

Server Certificate for QUIC

- QUIC comes with TLS1.3 built-in
- TLS requires certificates to function
- Certificate acquisition and installation is an explicit step
- Self signed certificate can be used but not recommended.

Additions to `net use` command

- **`net use /transport:quic`**
  - Forces client to use QUIC even if TCP is also available
- **`net use /transport:quic /skipcertcheck`**
  - Disables cert validation

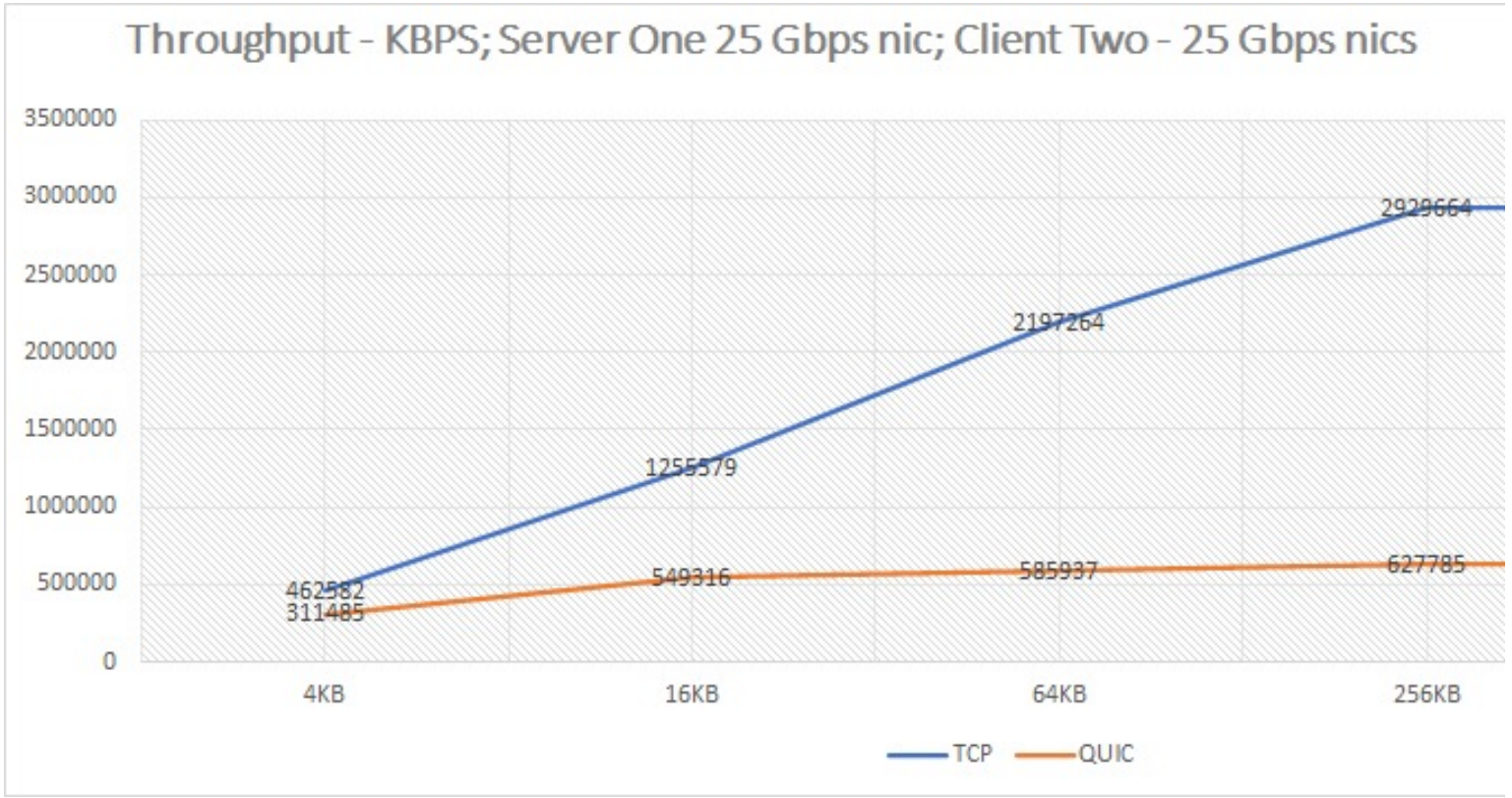
Performance

Performance comparison

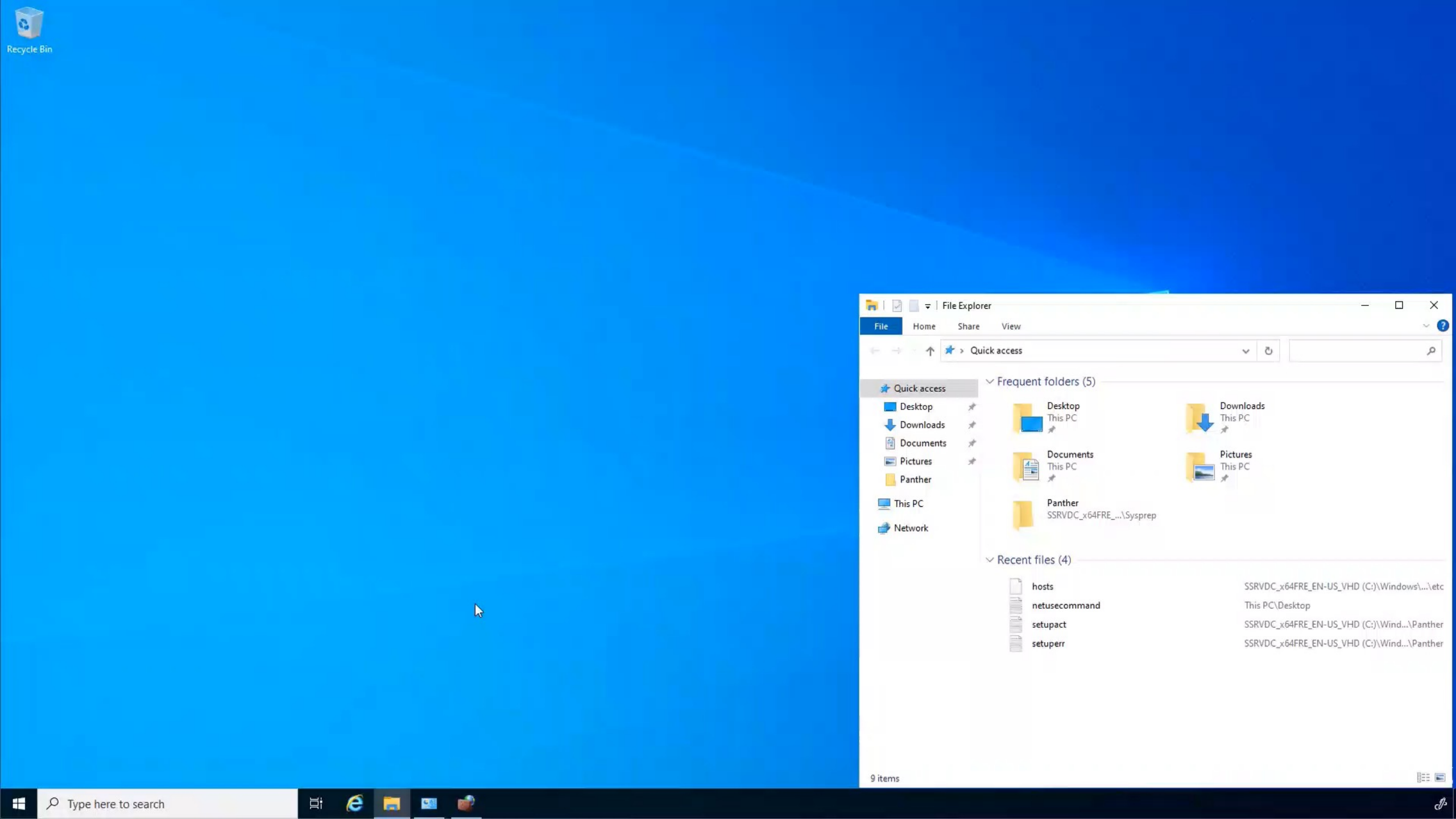
- The standard is Encrypted SMB over TCP (ESOT)
- SMB over QUIC is slower than ESOT
- The reason is in the encryption/decryption layer
- SMB encryption is asynchronous
- SMB encryption utilizes multiple processors

Performance comparison with TCP

- TCP with SMB Encryption turned on.



Demo


Recycle Bin
File Explorer
File
Home
Share
View
Quick access
Quick access
Desktop
Downloads
Documents
Pictures
Panther
This PC
Network
Frequent folders (5)
Desktop
This PC
Downloads
This PC
Documents
This PC
Pictures
This PC
Panther
SSRVDC_x64FRE_...\Sysprep
Recent files (4)
hosts
SSRVDC_x64FRE_EN-US_VHD (C:)\Windows\...\etc
netusecommand
This PC\Desktop
setupact
SSRVDC_x64FRE_EN-US_VHD (C:)\Wind...\Panther
setuperr
SSRVDC_x64FRE_EN-US_VHD (C:)\Wind...\Panther
9 items
Type here to search

AES-GMAC Signing

New Signing Algorithm: AES-GMAC

- Supported in Window 10 v21H1 and Windows Server 2022 and later
- Most preferred algorithm for signing
- Id for AES-GMAC is 0x0002 in SMB2_SIGNING_CAPABILITIES context
- Nonce (IV) for AES-GMAC is derived from MessageId (more on next slide)

Construction of IV (Nonce)

- Following struct is used for IV value:

```
typedef struct SMB_CRYPTO_IV_128
{
    ULONGLONG MessageId;
    ULONG ServerToClient : 1;
    ULONG CancelRequest : 1;
    ULONG Reserved1 : 30;
    ULONG Reserved2;
}
```

- The value for Reserved1 and Reserved2 is zero
- ServerToClient is 0 for request and 1 for response
- CancelRequest is 1 for CancelRequest, otherwise 0

AES-GMAC Signing: things to note

- Windows sets only first 12 bytes of Nonce
- No check is made for Nonce overflow

Questions?

- For questions about SMB-over-QUIC, please contact nedpyle@microsoft.com
- For any follow up question on this presentation or any question on open specifications, please contact: dochelp@microsoft.com

References

- [MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3
  [MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3 | Microsoft Docs

- Ned Pyle Blog entry on SMB-over-QUIC:
  SMB over QUIC: Files Without the VPN (microsoft.com)

Please take a moment to rate this session.

Your feedback is important to us.

