IETF 126 Hackathon

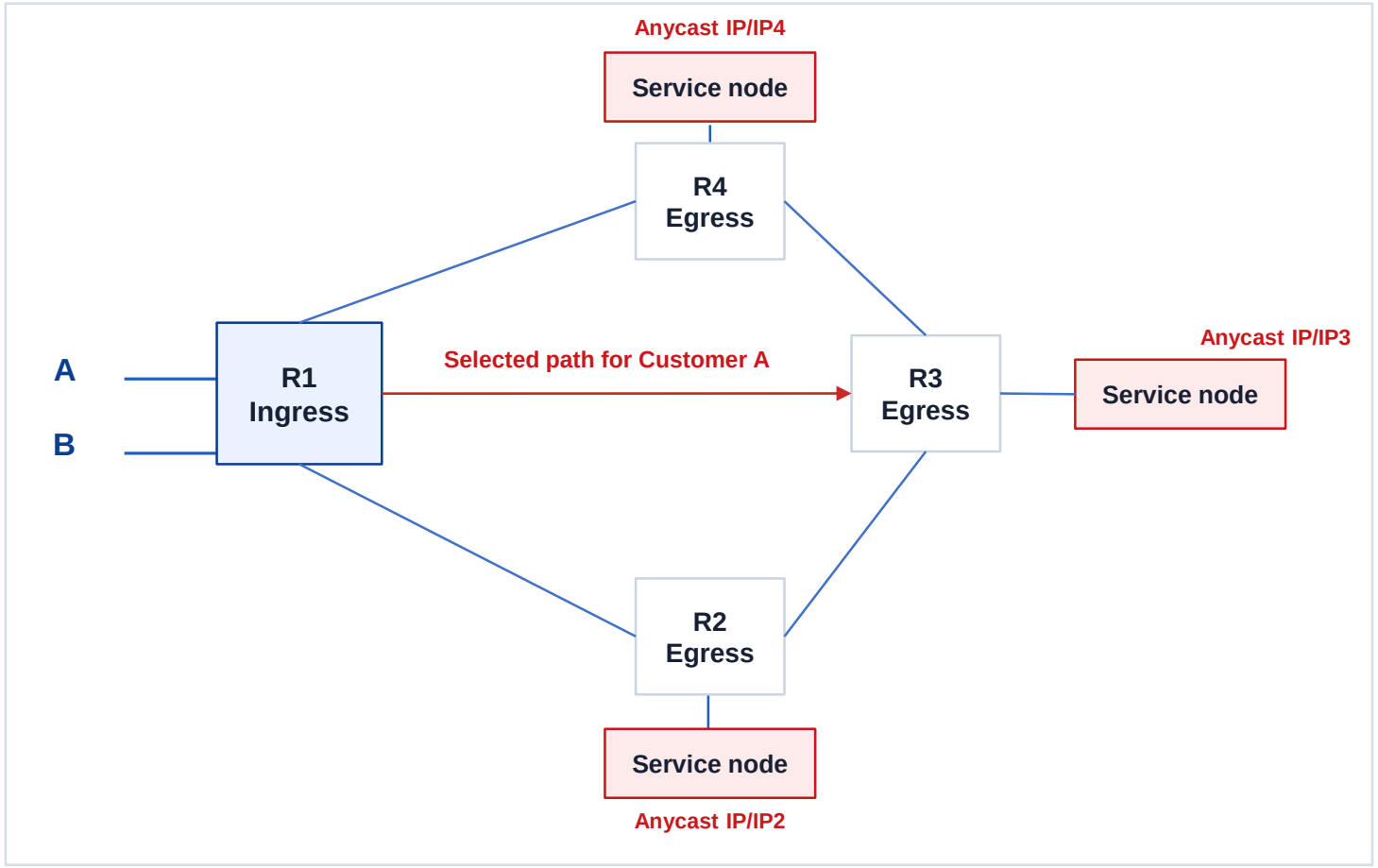
Service Affinity Solution based on TLS

(related work: draft-wang-tls-service-affinity)

Wei Wang (China Telecom)
Aijun Wang (China Telecom)
Zongbin Wang (Beijing Infosec Technologies Co., LTD.)
Mohit Sahni (Palo Alto Networks)
Ketul Sheth (Palo Alto Networks)

Service Affinity Use Case

Topology redrawn from the draft



Problem Statements

1. Services are deployed in different sites via Anycast Address
2. The ingress router can select the best service node, based on the real time network situation.
3. If the following packet of this session uses still the Anycast Address, it may be diverted to the other service node.

Service Affinity of one Session is Broken!

Why Existing Solutions Are Not Enough

Problem statement: dynamic cloud / edge / multi-homed service deployments

Existing approaches have operational limits

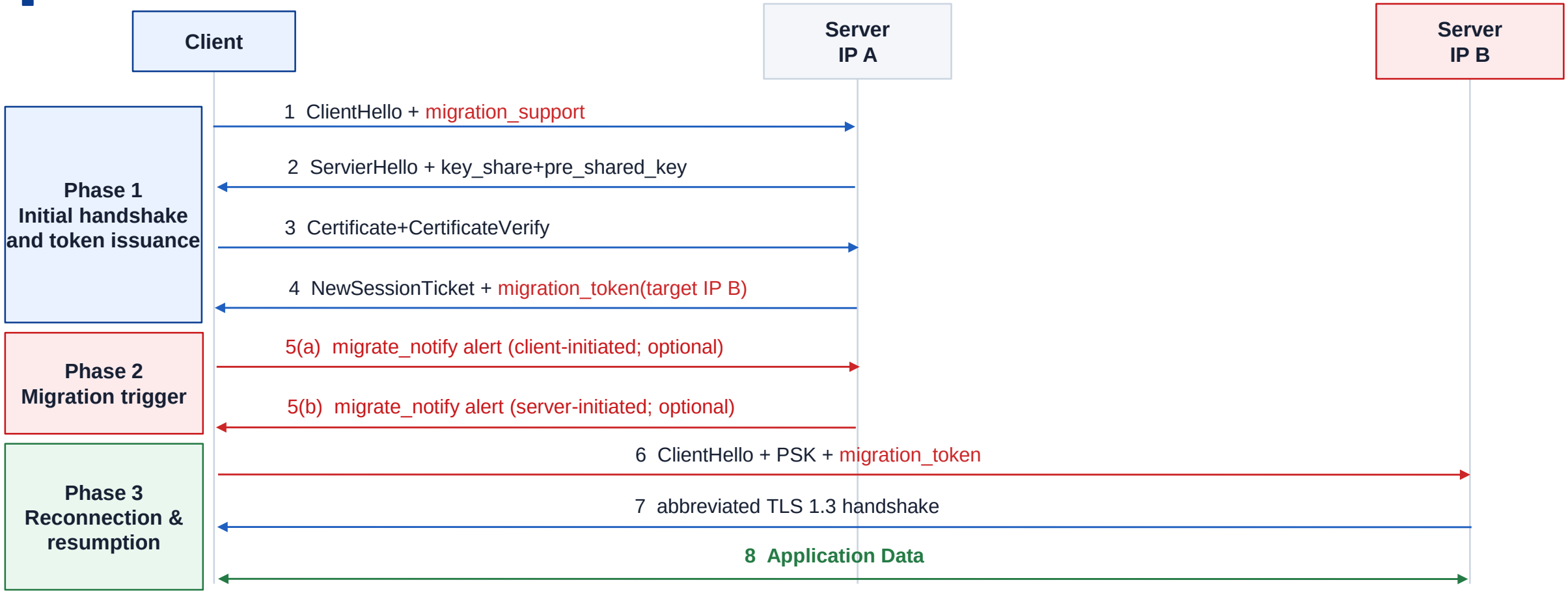
Approach	How it works	Main limitation	Impact
Network state table	Devices keep per-customer or per-flow affinity state	State grows with sessions; hard to adapt to dynamic resource changes	**Pressure on devices**
Load balancer	All packets traverse a front-end load balancer	Centralized path may become a traffic bottleneck	**Potential hotspot**
HTTP redirection	Application-layer redirect to another endpoint	Client/server do not fully perceive network and computing status	**Limited optimization**
DNS redirection	Change DNS resolution result to another server IP	DNS caching delays convergence and may keep old endpoints active	**Slow reaction**

Need: fast, secure, application-transparent migration without heavy per-flow state in the network

Procedure Overview

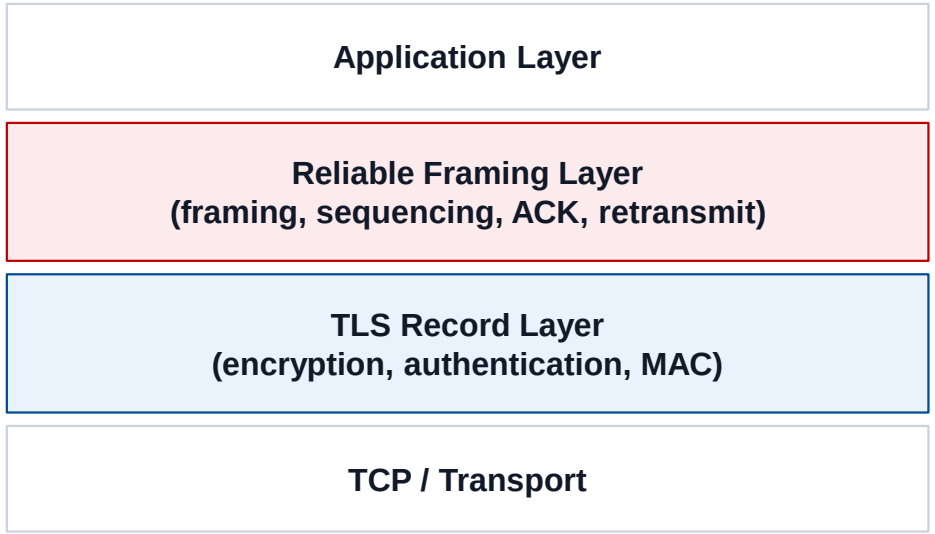
Three phases based on the overall message flow in the draft

Message flow



Reliable Framing Layer

Protocol stack



Frame header



Frame header: 11 bytes in total, including 3 types: DATA / ACK / FIN

magic: Frame magic number 0x4652 ("FR")

flags: Bitwise OR of frame type flags

sequence_number: Sequence number of this frame

length: Payload length in bytes (0 for ACK/FIN)

payload: Frame payload data

```
waj@LAPTOP-09T7970K:/mnt/d/IETF/tls_service_affinity$ make all certs test
mkdir -p bin
make: Nothing to be done for 'certs'.

========================================
  TLS Service Affinity - Full Test
========================================

Starting Server B on port 8444...
Starting Server A on port 8443...
Starting Client...
=== TLS Service Affinity Client (with Reliable Framing) ===
[Client] Server A: 127.0.0.1:8443
[Client] Server B (override): 127.0.0.1:8444
[Client] SSL context created with TLS 1.3

============================================================
  PHASE 1: Initial Handshake + Data Transfer (Server A)
============================================================

[Client] Connecting to Server A at 127.0.0.1:8443...
[Client] Performing TLS 1.3 handshake...
[Client] ✓ TLS 1.3 handshake completed
[Client] ✓ Session obtained (for PSK resumption)

[Client] Sending 5 data messages via Framing Layer...
[Client]   Sent seq#1: [MSG-1] Client data packet: user_id=1001, action=login
[Client]   Sent seq#2: [MSG-2] Client data packet: user_id=1001, action=query_balance
[Client]   Sent seq#3: [MSG-3] Client data packet: user_id=1001, action=transfer, amount=500
[Client]   Sent seq#4: [MSG-4] Client data packet: user_id=1001, action=query_history
[Client]   Sent seq#5: [MSG-5] Client data packet: user_id=1001, action=logout

[Client] Waiting for ACKs from Server A...
[Client] Received migration_token in NewSessionTicket (98 bytes)

[Client] Framing stats before migration:
[Client]   Messages sent: 5
[Client]   Send queue count: 5
[Client]   Queue[0]: seq=1, acked=1
[Client]   Queue[1]: seq=2, acked=1
[Client]   Queue[2]: seq=3, acked=1
[Client]   Queue[3]: seq=4, acked=0
[Client]   Queue[4]: seq=5, acked=0
[Client]   ACKed by server: 3
[Client]   UNACKED (need retransmit): 2
[Client] Initiating migration to Server B...
[Client] ✓ Received MigrationToken (98 bytes) in NewSessionTicket
[Client] ✓ Updated session with PSK ticket (for resumption)
[Client] Migration target: 127.0.0.1:8444
[Client] Disconnected from Server A
```

```
============================================================
  PHASE 2: Migration Trigger
============================================================

[Client] Server A sent migrate_notify alert.
[Client] Initiating migration to Server B...

============================================================
  PHASE 3: Reconnection + Automatic Retransmission (Server B)
============================================================

[Client] Connecting to Server B at 127.0.0.1:8444...
[Client] Configured PSK resumption with saved session
[Client] Performing TLS 1.3 handshake with Server B...
[Client] Adding migration_token to ClientHello (98 bytes)
[Client] ✓ TLS 1.3 handshake with Server B completed
[Client] NOTE: Full handshake performed (session not resumed)

  ┌──────────────────────────────────────────────────────────┐
  │       Data Continuity Check                              │
  ├──────────────────────────────────────────────────────────┤
  │  Unacknowledged frames from Server A: 2                  │
  │  Action: RETRANSMITTING to Server B...                   │
  │  Retransmitted frames: 2                                 │
  │  ✓ Zero data loss guaranteed!                            │
  └──────────────────────────────────────────────────────────┘

[Client] Sent new post-migration message (seq#6)
[Client] Received migration_token in NewSessionTicket (98 bytes)
[Client] Received migration_token in NewSessionTicket (98 bytes)
[Client]   Received: [Server-B-ACK] Processed seq#4 on Server B
[Client]   Received: [Server-B-ACK] Processed seq#5 on Server B
[Client]   Received: [Server-B-ACK] Processed seq#6 on Server B

[Framing] Statistics:
  Total sent:         6
  Total received:     3
  Total retransmitted: 2
  Unacknowledged:     0
  Next send seq:      7
  Next recv seq:      4

============================================================
  ✓✓✓ TLS SERVICE AFFINITY MIGRATION COMPLETE ✓✓✓
  ✓✓✓ DATA CONTINUITY VERIFIED - ZERO LOSS ✓✓✓
============================================================

[Client] All phases completed successfully.
```

--- Server A Log ---

```
=== TLS Service Affinity - Server A ===
[Server A] Listening on port 8443
[Server A] Migration target: 127.0.0.1:8444
[Server A] SSL context created with TLS 1.3
[Server A] Session ticket encryption key set (EVP callback)
[Server A] Ticket keys saved to ticket_keys.bin
[Server A] Ready for connections

[Server A] Performing TLS 1.3 handshake...
[Server A] Received migration_support extension in ClientHello
[Server A] TLS 1.3 handshake completed successfully
[Server A] Generating MigrationToken...
[Server A] Saved HMAC key to hmac_key.bin (for Server B)
[Server A] Generated MigrationToken for 127.0.0.1:8444 (expiry: 1784017456)
MigrationToken:
  target_address: 127.0.0.1:8444
  session_id (32 bytes): 6acc67449131a0f96dff5184b99fb326750113a39c75f93544d203e032b916bb
  expiry_timestamp: 1784017456
  nonce (16 bytes): eadbce151facff910b04fde186d61b52
  signature (32 bytes): 18e01e0ce2386b6c485ddbdd4edbfeae5239182d5e5a76304845ee4d593277ca
[Server A] Sending NewSessionTicket with migration_token...
[Server A] NewSessionTicket sent successfully
[Server A] Waiting for framed data...
[Server A] Adding migration_token to NewSessionTicket (98 bytes)
[Server A]   Received framed data (seq#1, 54 bytes): [MSG-1] Client data packet: user_id=1001, action=login
[Server A]   ✓ ACKed seq#1
[Server A]   Received framed data (seq#2, 62 bytes): [MSG-2] Client data packet: user_id=1001, action=query_balance
[Server A]   ✓ ACKed seq#2
[Server A]   Received framed data (seq#3, 69 bytes): [MSG-3] Client data packet: user_id=1001, action=transfer, amount=500
[Server A]   ✓ ACKed seq#3
[Server A]   Received framed data (seq#4, 62 bytes): [MSG-4] Client data packet: user_id=1001, action=query_history
[Server A]   ✗ NOT ACKing seq#4 (simulating pre-migration state)
[Server A]   Received framed data (seq#5, 55 bytes): [MSG-5] Client data packet: user_id=1001, action=logout
[Server A]   ✗ NOT ACKing seq#5 (simulating pre-migration state)

[Server A] Migration summary:
[Server A]   Frames received: 5
[Server A]   Frames ACKed: 3 (seq#1-3)
[Server A]   Frames NOT ACKed: 2 (seq#4-5) -> will be retransmitted to Server B
[Framing] Statistics:
  Total sent:         0
  Total received:     5
  Total retransmitted: 0
  Unacknowledged:     0
  Next send seq:      1
  Next recv seq:      6
[Server A] Connection closed
[Server A] Shut down
```

--- Server B Log ---

```
=== TLS Service Affinity - Server B ===
[Server B] Listening on port 8444
[Server B] SSL context created with TLS 1.3
[Server B] Session ticket key loaded (EVP callback)
[Server B] PSK session resumption is ENABLED
[Server B] Ready for incoming migrations

[Server B] Performing TLS 1.3 handshake (expecting PSK resumption)...
[Server B] Received migration_support extension in ClientHello
[Server B] Received migration_token in ClientHello (98 bytes)
[Client] Adding migration_token to ClientHello (98 bytes)
[Client] Adding migration_token to ClientHello (98 bytes)

┌──────────────────────────────────────────────────────────┐
│        TLS Session Resumption Status                     │
├──────────────────────────────────────────────────────────┤
│  ✗ Full handshake performed (NOT resumed)                │
│  ✗ Session ticket could not be decrypted                 │
│  ✗ Ensure ticket_keys.bin is shared from Server A        │
│  Handshake time: 1.88 ms                                 │
│  Negotiated protocol: TLSv1.3                            │
│  Cipher suite: TLS_AES_256_GCM_SHA384                    │
└──────────────────────────────────────────────────────────┘

[Server B] TLS 1.3 handshake completed successfully
[Server B] Validating MigrationToken...
MigrationToken:
  target_address: 127.0.0.1:8444
  session_id (32 bytes): 6acc67449131a0f96dff5184b99fb326750113a39c75f93544d203e032b916bb
  expiry_timestamp: 1784017456
  nonce (16 bytes): eadbce151facff910b04fde186d61b52
  signature (32 bytes): 18e01e0ce2386b6c485ddbdd4edbfeae5239182d5e5a76304845ee4d593277ca
[Server B] ✓ Token not expired (expires in 3598 seconds)
[Server B] ✓ Nonce is fresh (replay protection passed)
[Server B] Loaded HMAC key from hmac_key.bin
[Server B] ✓ Token signature is valid
[Server B] ✓ Session binding verified (via HMAC)
[Server B] ✓✓✓ MigrationToken validation PASSED ✓✓✓
[Server B] Session migrated from target: 127.0.0.1:8444
[Server B] ✓✓✓ MigrationToken validation PASSED
[Server B] Waiting for framed data (including retransmissions)...
[Server B]   Received framed data (seq#4, 62 bytes): [MSG-4] Client data packet: user_id=1001, action=query_history
[Server B]   ✓ ACKed seq#4
[Server B]   Received framed data (seq#5, 55 bytes): [MSG-5] Client data packet: user_id=1001, action=logout
[Server B]   ✓ ACKed seq#5
[Server B]   Received framed data (seq#6, 62 bytes): [MSG-NEW] Client data after migration: action=continue_session
[Server B]   ✓ ACKed seq#6
```

```
┌──────────────────────────────────────────────────────────┐
│ Data Continuity Report                                   │
├──────────────────────────────────────────────────────────┤
│ Total unique data frames received: 3                     │
│ ✓ Zero data loss confirmed!                              │
└──────────────────────────────────────────────────────────┘
```

```
[Framing] Statistics:
  Total sent:         3
  Total received:     3
  Total retransmitted: 0
  Unacknowledged:     3
  Next send seq:      4
  Next recv seq:      7
[Server B] Connection closed
[Server B] Shut down
waj@LAPTOP-09T7970K:/mnt/d/IETF/tls_service_affinity$
```