

# Fully meshed dynamically switched QKD Metro network

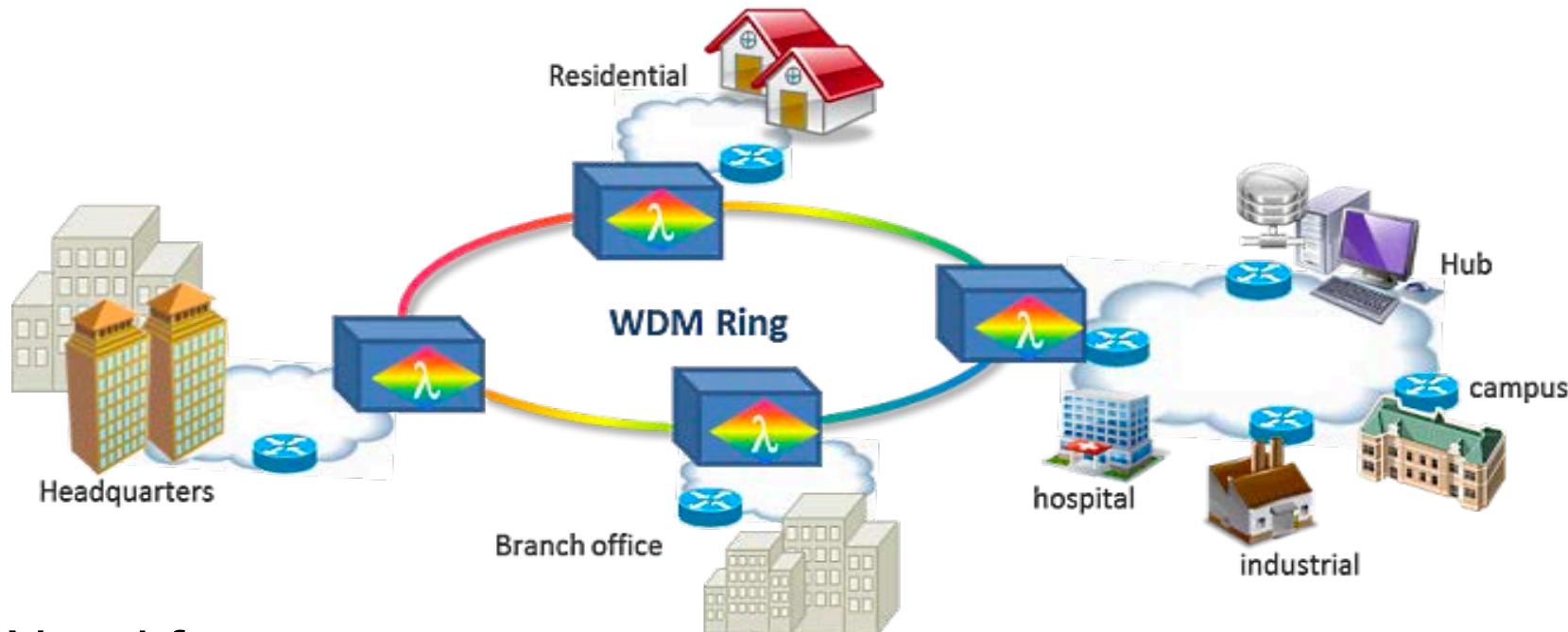
Dr. George T. Kanellos

Prof. Reza Nejabati

Prof. Dimitra Simeonidou



# Dynamic Optical Networking for the Metro/Edge



Need for:

- High Bandwidth
- Low Latency
- Very Dynamic



Dynamic Optical Networking  
for metro/edge

*Security?*



# Dynamic QKD networking

---

- **Compatibility with classical optical networks**

Allow co-existence of classical-quantum channels

- **Fit dynamic networking scenarios**

Overcome physical transmission and switching limitations

## Enablers:

### Shorter Reach (<20km) + Low loss OXC

- unamplified classical channels ( $\rightarrow$  no ASE)
- lower power classical channels ( $\rightarrow$  low crosstalk)
- Reduced insertion losses
- Negligible fiber non-linearities

### Advanced Management Schemes

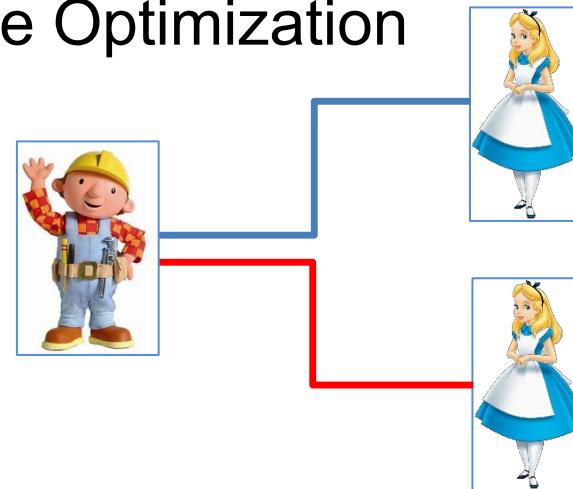
- SDN to decide and implement routing
- Optimal Path Computation
- Re-arrange wavelengths to minimize non-linearities (FWM)



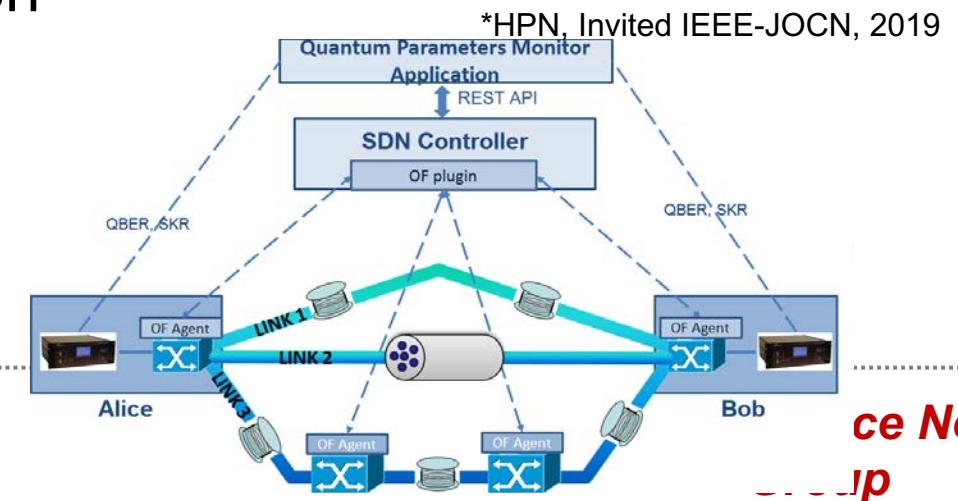
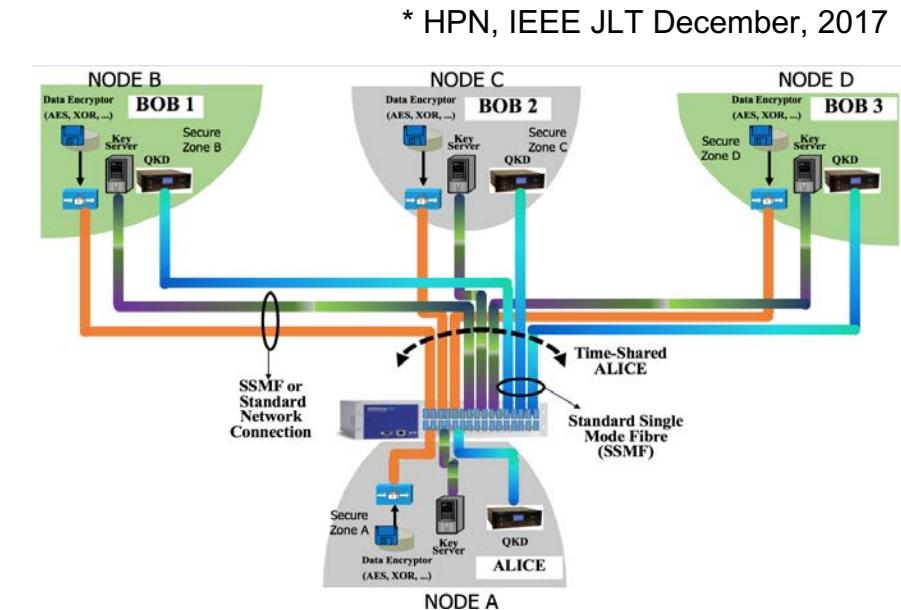
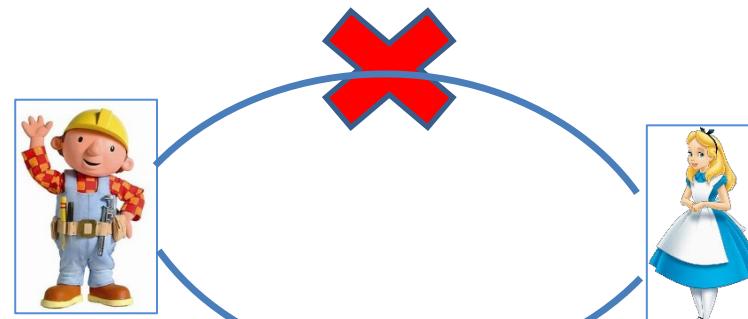
# Dynamic QKD networking

## Operational Advantages:

- 1) Resource Usage Optimization  
→ sharing



- 2) Path optimization and DOS Attack mitigation  
→ rerouting



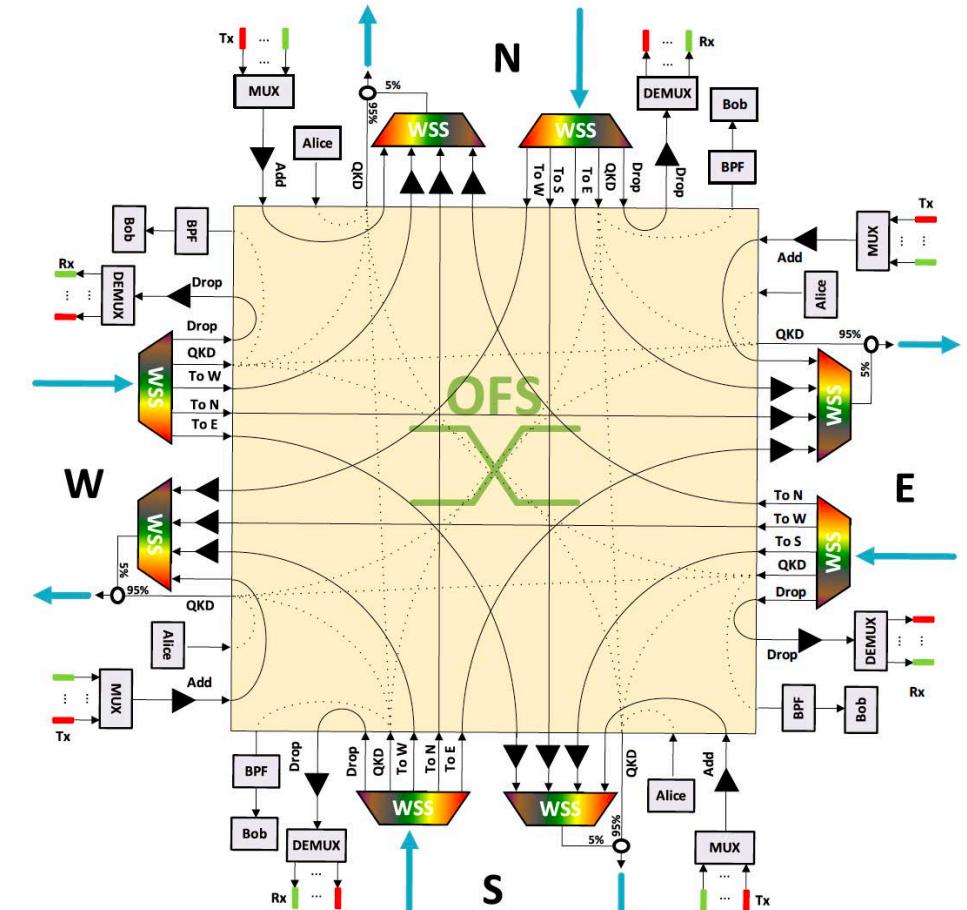
# The Q-ROADM

Challenge:

dynamic, flexible, simultaneous quantum and classical resource allocation

Our contribution:

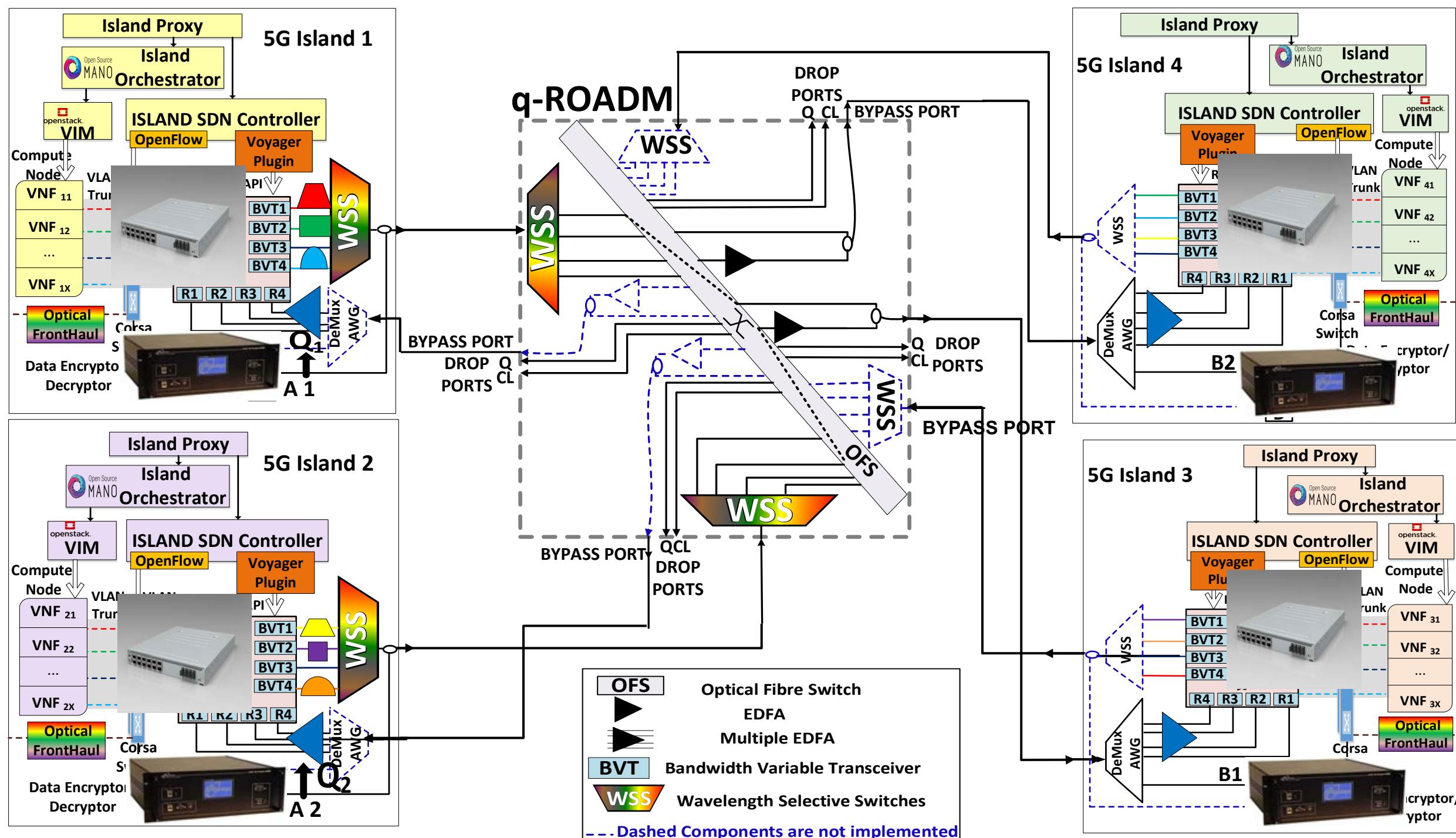
- Four-degree quantum- reconfigurable add/drop multiplexer (ROADM)
- Low loss ROADM design ( $< 5.3\text{dB}$  loss for QKD channel)
- Flexigrid classical channels routing
- Any combination of classical and quantum channels on the same port
- Dynamically reconfigurable routing of quantum channels



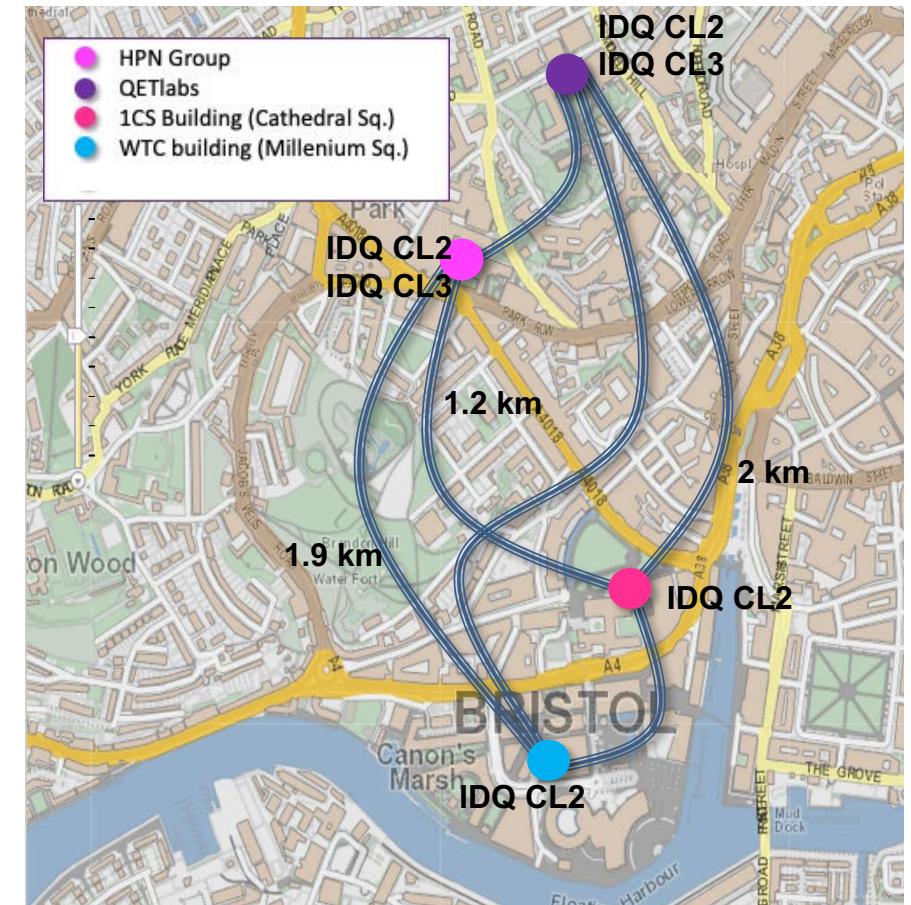
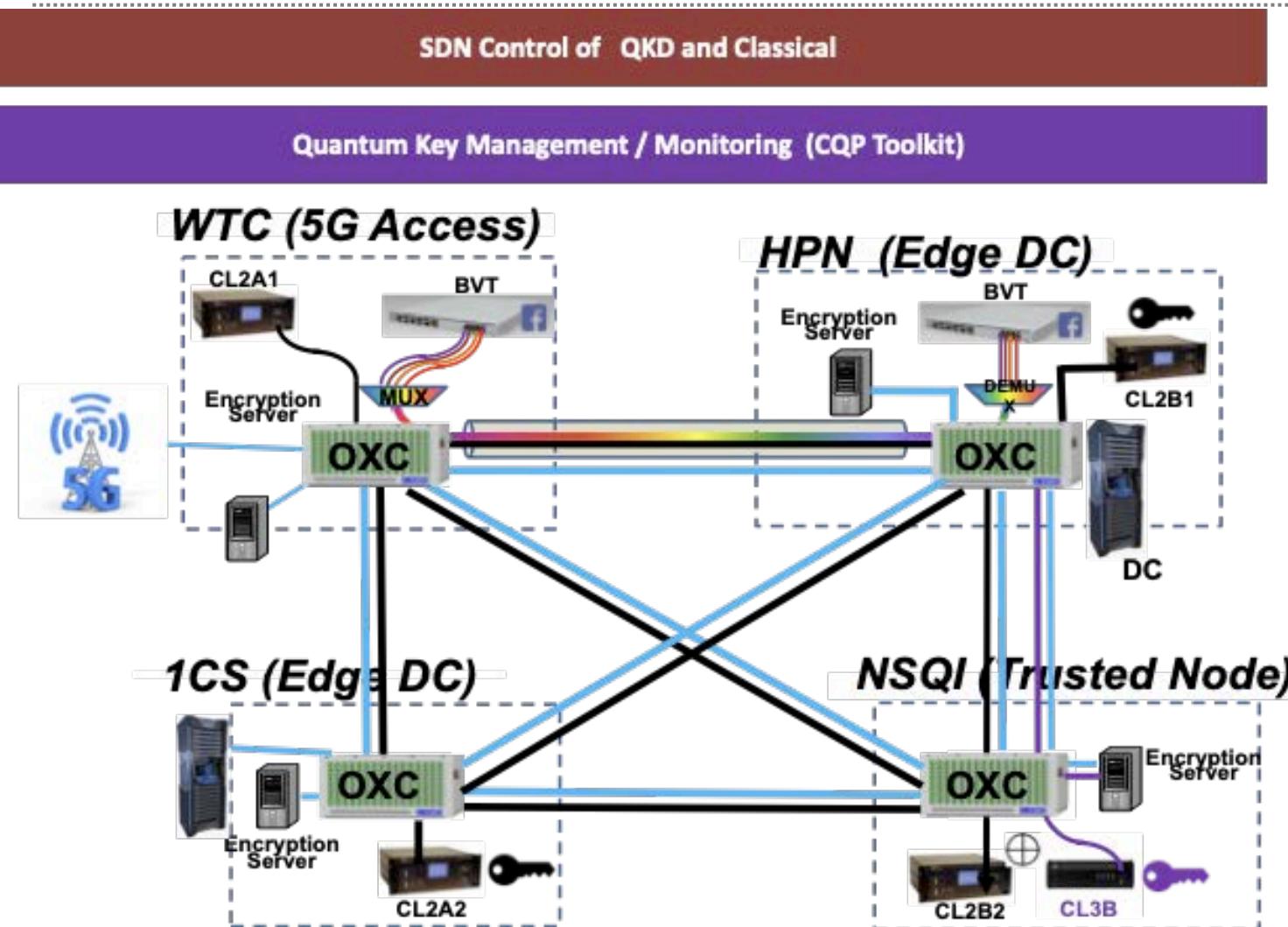
- HPN, invited IEEE JLT, July 2019



SMART  
INTERNET  
LAB



# Demo2: Fully meshed dynamically switched QKD Metro network



# Demo2: Fully meshed dynamically switched QKD Metro network

---

## GOALS:

### 1. Demonstrate Classical-Quantum Channel **Co-Existence** over Mesh Network

- 4x100G (QPSK) Unamplified Optical Channels
- 1x Quantum Ch. (IDQ CL.2)
- 2x optical switches

### 2. Demonstrate Q-Ch. **Denial of Service Mitigation** over Mesh Network

- Quantum Channel Rerouted over Mesh Network
- 3x optical switches

### 3. Demonstrate **QKD Resource Usage Optimization** using dynamic QKD switching

- 2x QKD pairs → 4x QKD links

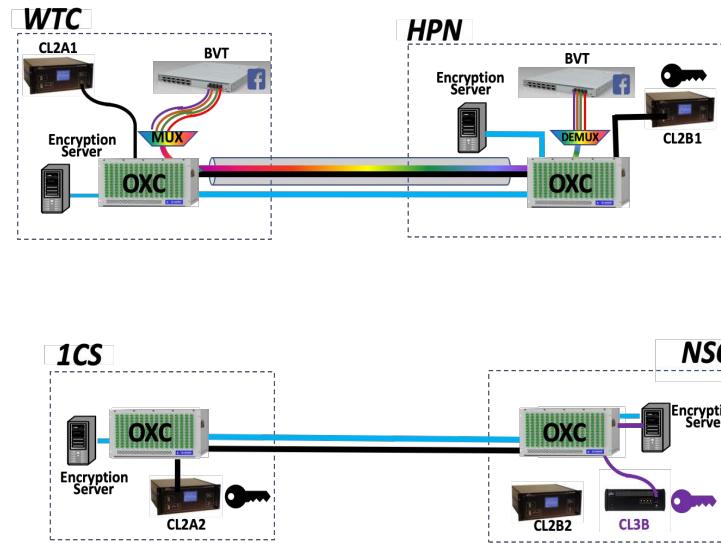
### 4. Software Defined Control plane:

- Monitor the q-channel
- rerouting

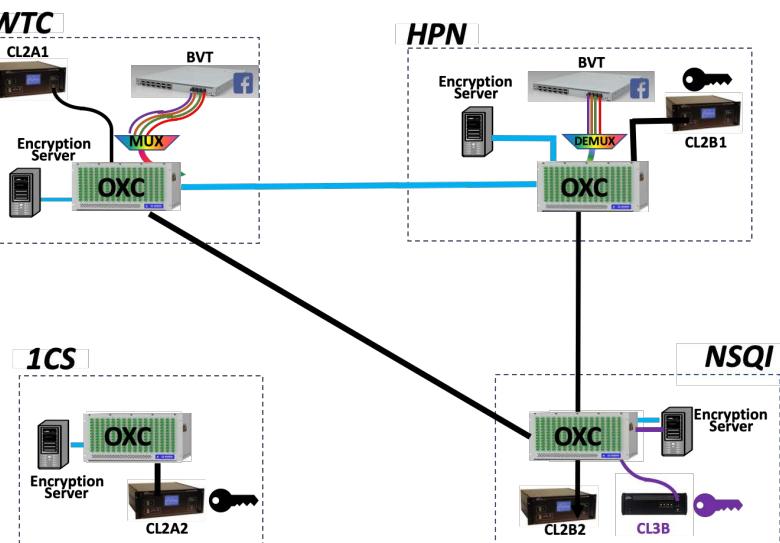


# Demo 2 Scenario

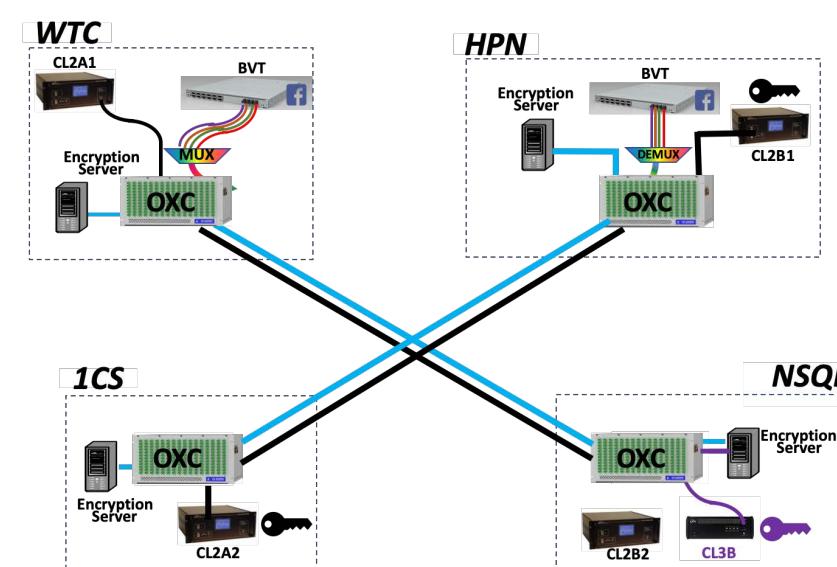
Step 0



Step 1



Step 2



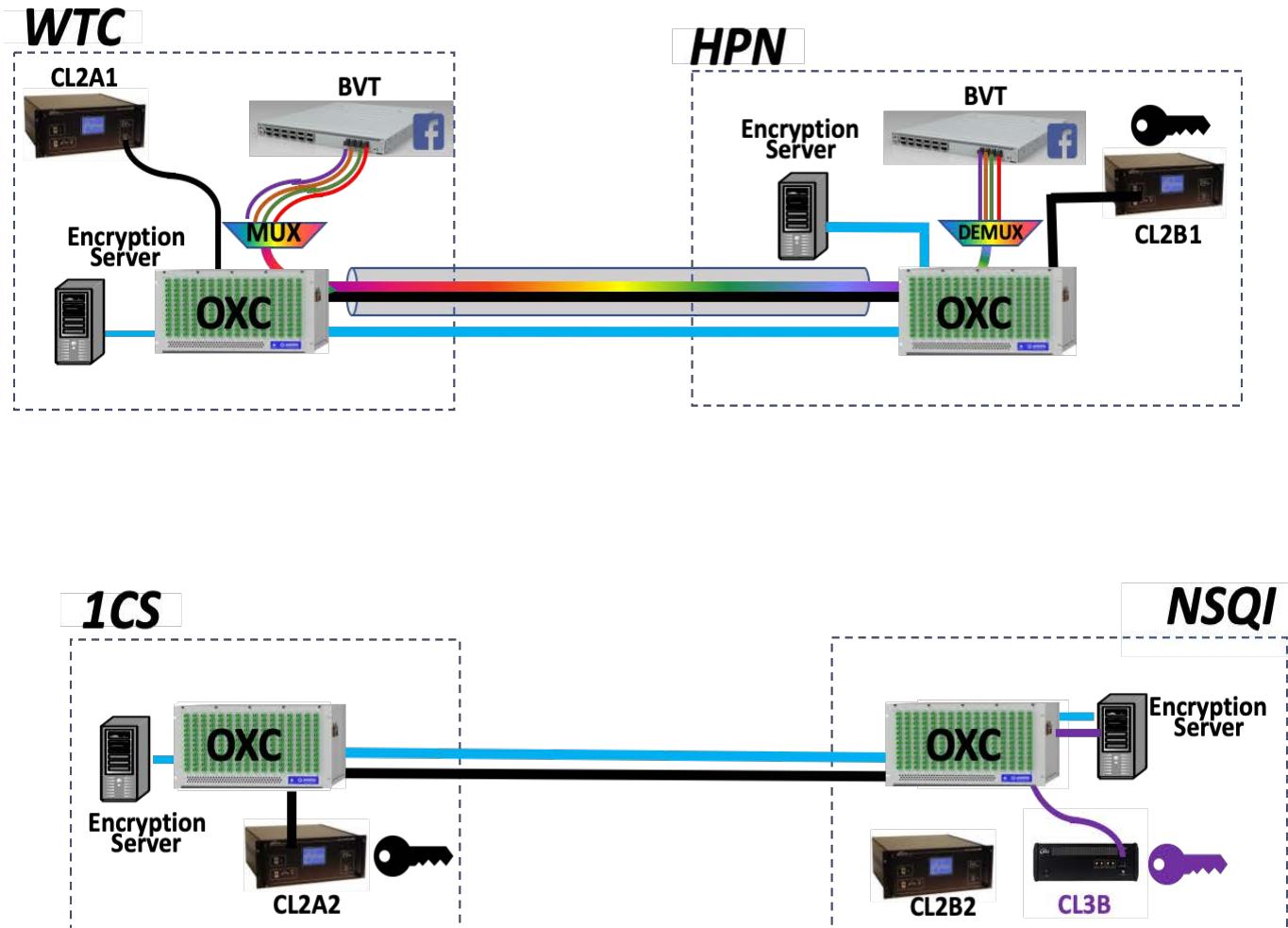
- 2 Secure Links established
- WTC-HPN
- 1CS-NSQI
- Co-existence in WTC-HPN

- DOS Attack and mitigation
- WTC-HPN link co-existing channels violate Q-Ch
- SDN controller reroutes Q-ch
- Q-ch new path through 3 switches

- Establish 2 new Secure links
- WTC-NSQI
- 1CS-HPN



# Demo 2 - Step 0



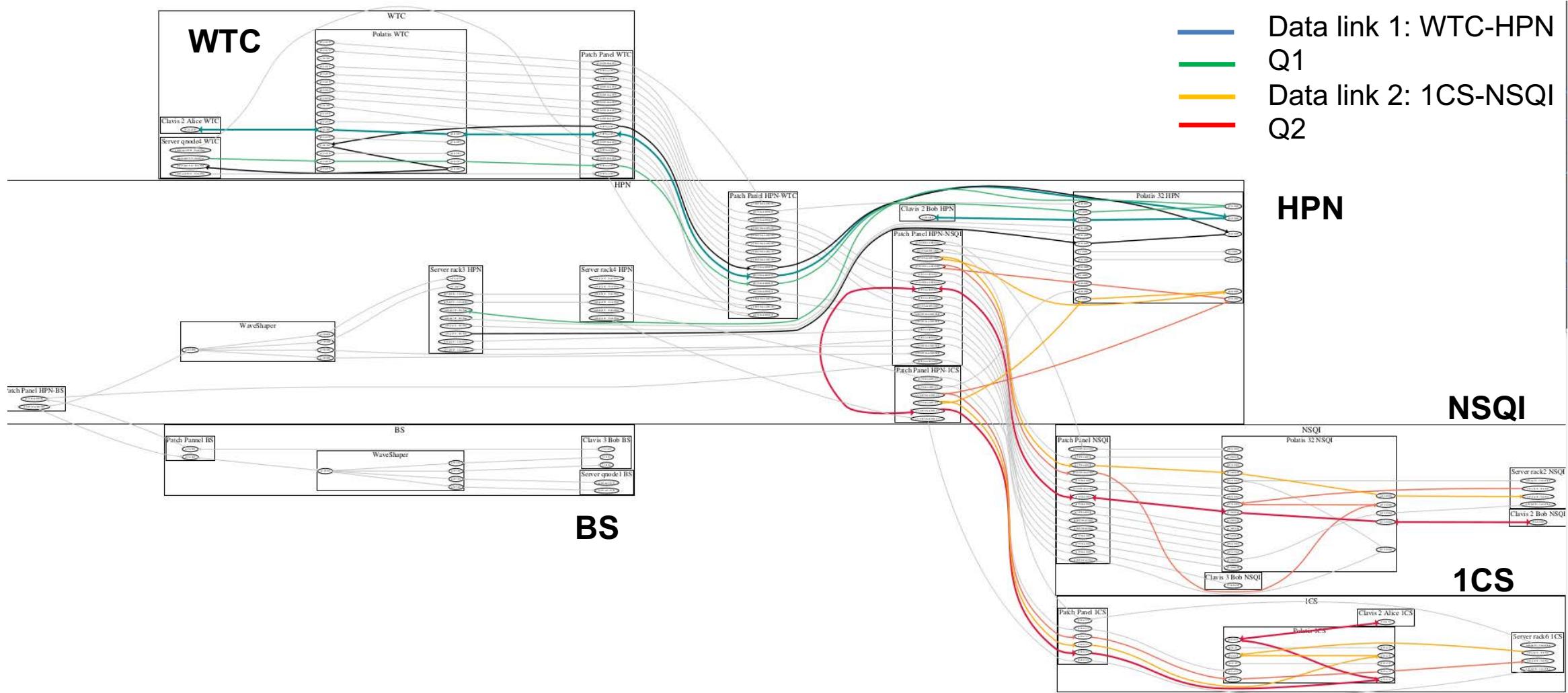
## Step 0 Flowchart:

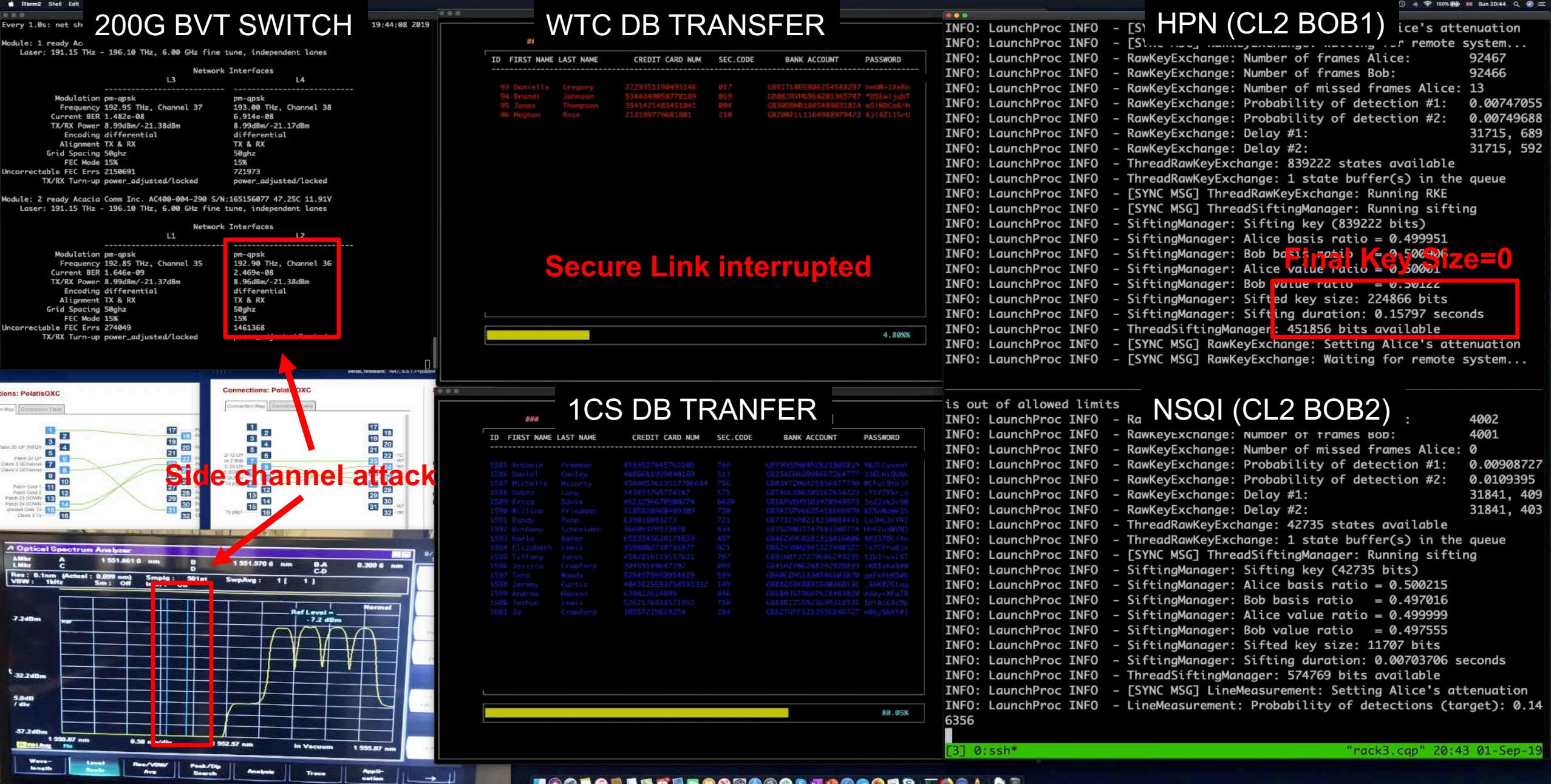
User defines 2 Secure Links  
WTC-HPN (Co-exist)  
1CS-NSQI

DOS Attack:  
Co-exist Cl-Ch. Shifts w/l close  
to Q-ch

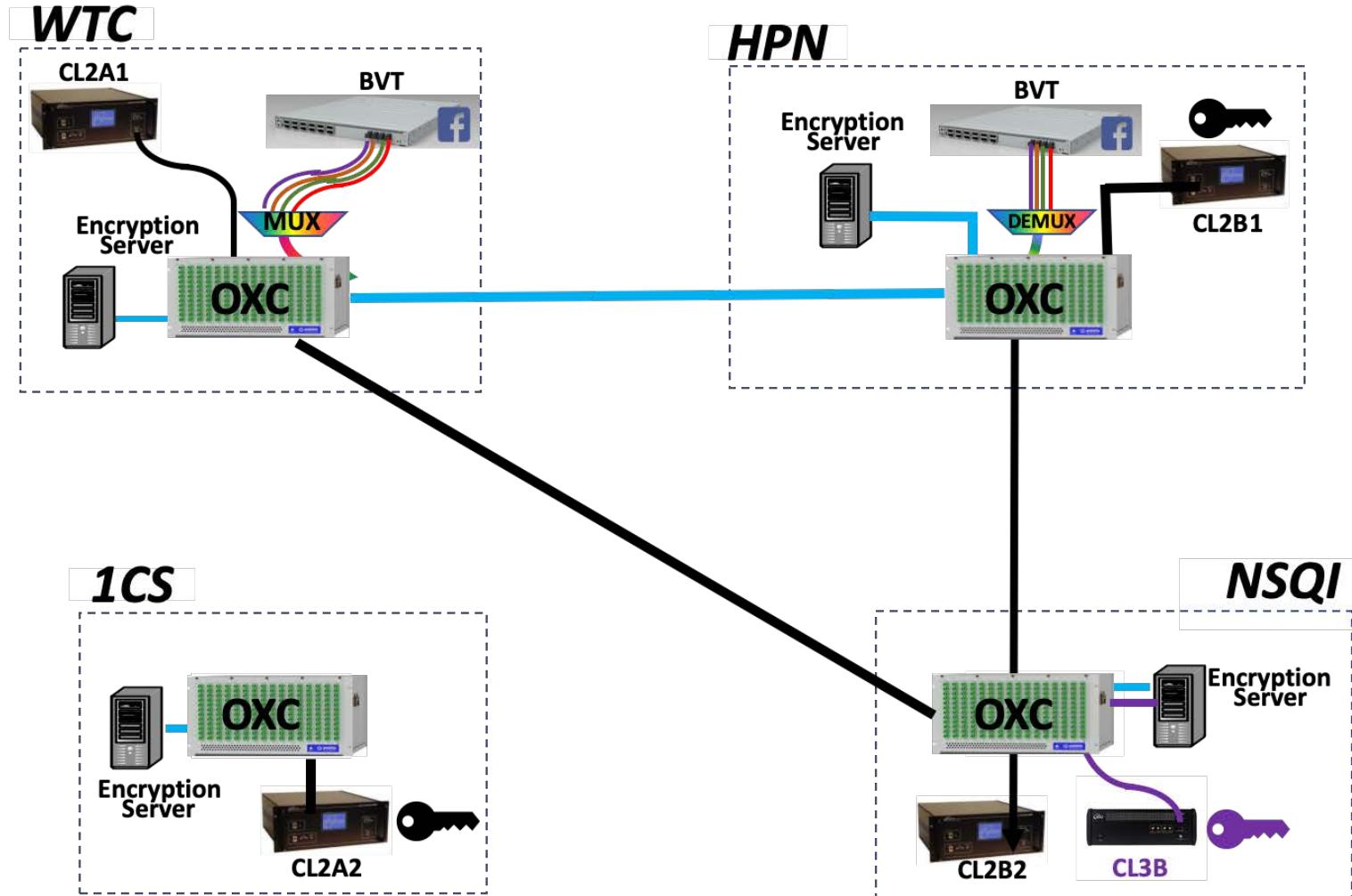
Q-ch error msg:  
Final key size=0  
Secure Link 1 interrupted

# Step 0 Actual Network topology





# Demo 2 Step 1



## Phase 1 Flowchart:

SDN controller detects Attack  
(msg: Final Key Size=0)

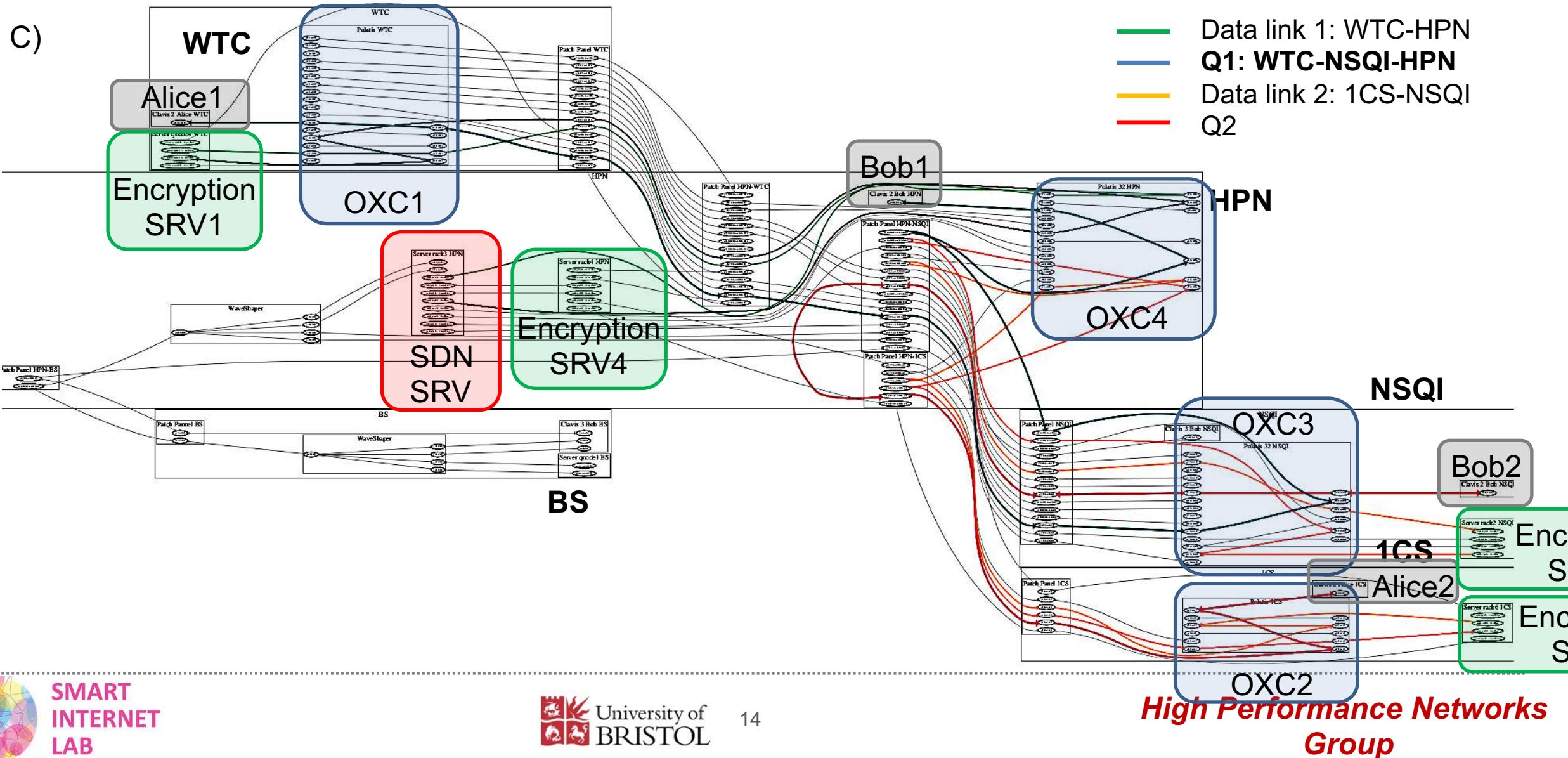
SDN Controller defines Q-ch  
rerouting through NSQI-HPN  
CI-Ch remains unaffected

SDN Controller Switches  
OXC1/OXC3 → establish WTC-  
NSQI for Q-ch  
OXC3/OXC4 → establish NSQI-  
HPN for Q-ch

**Key Points:**  
Secure Link 1 re-established



# Step 1 Actual Network topology



**NSQI OXC**

**HPN OXC**

**WTC OXC**

**WTC DB TRANSFER**

ID	FIRST NAME	LAST NAME	CREDIT CARD NUM	SEC. CODE	BANK ACCOUNT	PASSWORD
225	Jessica	Townsend	601123187294968	629	0B163LYC95498289179448	39d4ePnH2M
226	Lindsey	White	4517401226727	879	0B72FFHX79926298502469	8730mChEg
227	Samuel	Robinson	49166E3673186	228	0B3803WT7281858E3928	nfXaZ3zvHlK
228	Dionne	Dunn	676162111105	951	0B16NM453475456960837	0812AKHtE
229	Michael	Taylor	4676168794185	792	0B20FAKAC57801954127	*1HGReDqB
230	Owen	Harris	473963676508317	183	0B89jXWV4338843469381	yz5wMgnA7
231	Rachel	Kirby	50467986749126	985	0B55SDL15800148189199	HgtVMeoJX
232	Abigail	Montes	060457829236	757	0B36GRN12498013708988	2cdzpxK7E
233	James	Brody	468209476340375	194	0B44KLKR7748464942165	yBdqZwHfD

**Secure Link still interrupted**

**Secure Link re-initiated**

**Successful Key Generation**

**1CS DB TRANSFER**

ID	FIRST NAME	IT	PASSWORD
23	Samantha	Settimio	35791278441085998
24	Brinley	Schmidt	5103598791524797
25	Cory	Carter	38006484846127
26	Kathleen	Murphy	2315631494574
27	Tiffany	Harrow	5482702073343889
28	Evan	Bradford	08550000000000000000
29	Timothy	Burnett	4887312876196
30	Douglas	Spencer	9611532723W147
31	Vincent	Stanton	347064312776496
32	Condice	Gutierrez	421171047629136
33	Michael	Ross	4549903737844782
34	Eliot	Stone	36489018630434
35	Kelly	Burchfield	4436157634844141
36	Lisa	Morris	859

**Secure Link 2 Remains unaffected**

**INFO: LaunchProc INFO - [SYNC MSG] RawKeyExchange: Setting Alice's attenuation**

**INFO: LaunchProc INFO - ErrorCorrectionCascade: Bits processed: 901120**

**INFO: LaunchProc INFO - ErrorCorrectionCascade: Skipped bits: 3096**

**INFO: LaunchProc INFO - ErrorCorrectionCascade: Nbr of error corrected: 21692**

**INFO: LaunchProc INFO - ErrorCorrectionCascade: QBER: 0.0240723**

**INFO: LaunchProc INFO - ErrorCorrectionCascade: Nbr of communications: 4167**

**INFO: LaunchProc INFO - ErrorCorrectionCascade: Nbr of bits disclosed: 206582**

**INFO: LaunchProc INFO - ErrorCorrectionCascade: duration: 1.00991 seconds**

**INFO: LaunchProc INFO - [SYNC MSG] ThreadErrorCorrection: waiting for remote system...**

**INFO: LaunchProc INFO - ThreadErrorCorrection: 901120 bits available**

**INFO: LaunchProc INFO - [SYNC MSG] ThreadPrivacyAmplification: Running privacy amplification**

**INFO: LaunchProc INFO - PrivacyAmplification: Processing key (901120 bits)**

**INFO: LaunchProc INFO - PrivacyAmplification: Confirmation failed! Probably one or more errors have not been corrected.**

**INFO: LaunchProc INFO - PrivacyAmplification: Generated 0 secret bits.**

**INFO: LaunchProc INFO - PrivacyAmplification: Final key size: 0**

**INFO: LaunchProc INFO - PrivacyAmplification: duration: 2.00341 seconds**

**INFO: LaunchProc INFO - [SYNC MSG] RawKeyExchange: Waiting for remote system...**

**INFO: LaunchProc INFO - [S] NSQI (CL2 BOB2) : remote system...**

**INFO: LaunchProc INFO - Ra 94166**

**INFO: LaunchProc INFO - Ra 94165**

**INFO: LaunchProc INFO - RawKeyExchange: Number of missed frames Alice: 1**

**INFO: LaunchProc INFO - RawKeyExchange: Probability of detection #1: 0.0087847**

**INFO: LaunchProc INFO - RawKeyExchange: Probability of detection #2: 0.0120398**

**INFO: LaunchProc INFO - RawKeyExchange: Delay #1: 31841, 337**

**INFO: LaunchProc INFO - RawKeyExchange: Delay #2: 31841, 304**

**INFO: LaunchProc INFO - ThreadRawKeyExchange: 1021513 states available**

**INFO: LaunchProc INFO - ThreadRawKeyExchange: 1 state buffer(s) in the queue**

**INFO: LaunchProc INFO - [SYNC MSG] ThreadSiftingManager: Running sifting**

**INFO: LaunchProc INFO - SiftingManager: Sifting key (1021513 bits)**

**INFO: LaunchProc INFO - SiftingManager: Alice basis ratio = 0.50005**

**INFO: LaunchProc INFO - SiftingManager: Bob basis ratio = 0.499904**

**INFO: LaunchProc INFO - SiftingManager: Alice value ratio = 0.500015**

**INFO: LaunchProc INFO - SiftingManager: Bob value ratio = 0.496585**

**INFO: LaunchProc INFO - [SYNC MSG] ThreadRawKeyExchange: Running RKE**

**INFO: LaunchProc INFO - SiftingManager: Sifted key size: 279547 bits**

**INFO: LaunchProc INFO - SiftingManager: Sifting duration: 0.14122 seconds**

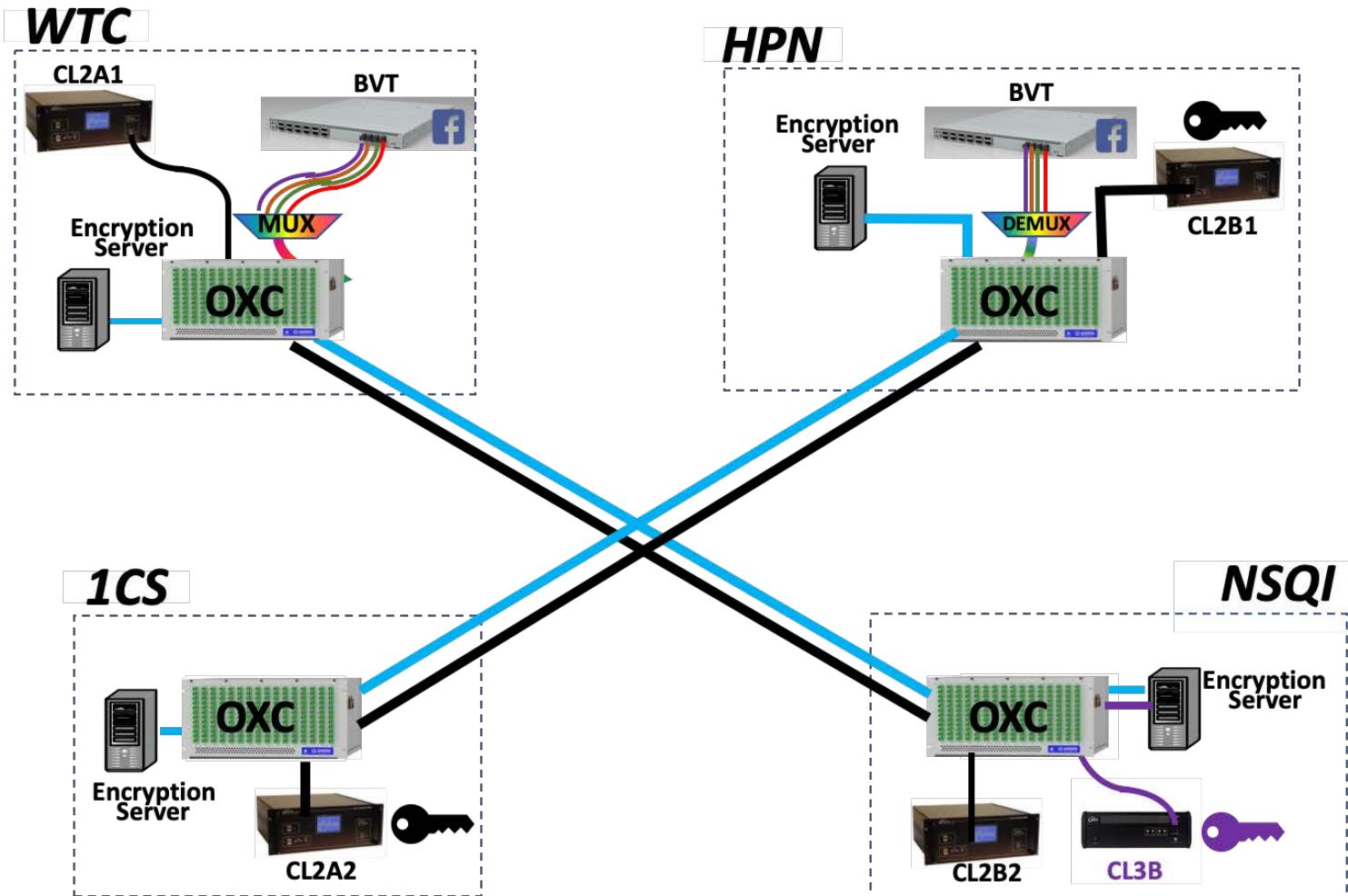
**INFO: LaunchProc INFO - ThreadSiftingManager: 561952 bits available**

**INFO: LaunchProc INFO - [SYNC MSG] RawKeyExchange: Setting Alice's attenuation**

**INFO: LaunchProc INFO - [SYNC MSG] RawKeyExchange: Waiting for remote system...**

"rack3.cap" 20:57 01-Sep-19

# Demo 2 Step 2



## Phase 2 Flowchart:

User defines new Secure Links

SDN Controller Switches  
OXC2/OXC4 → 1CS-HPN (Green)

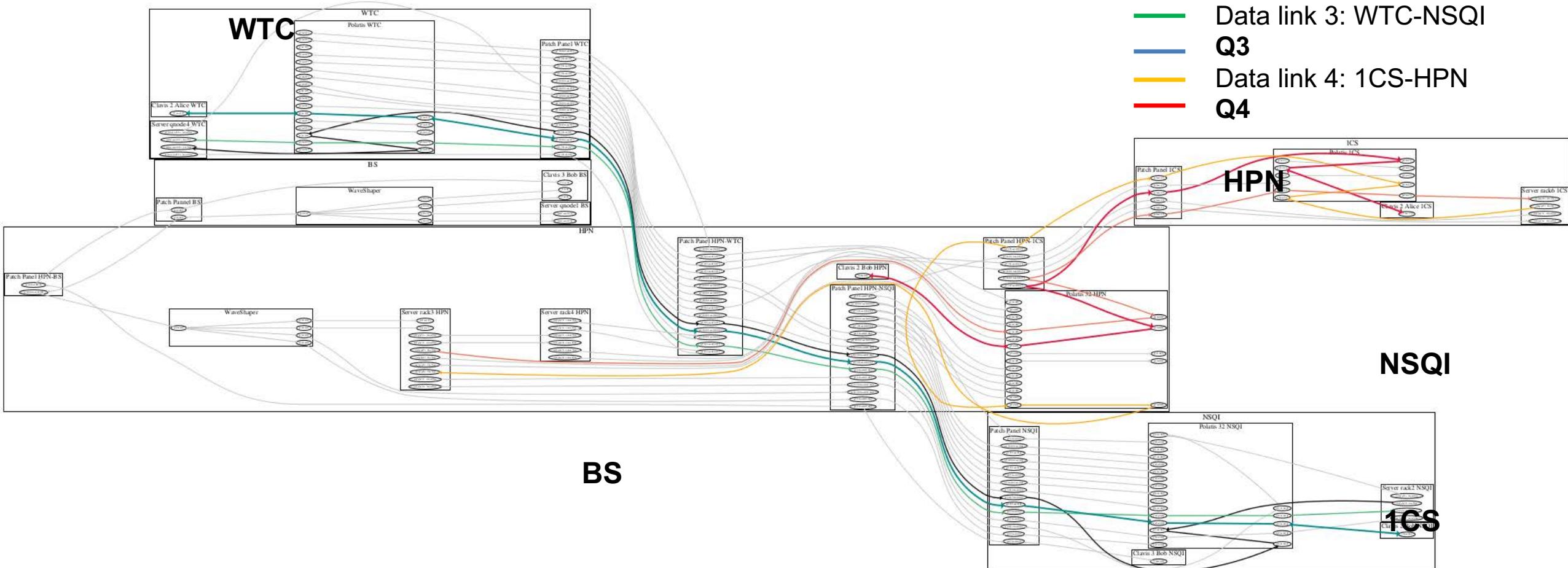
SDN Controller Switches  
OXC3 → WTC-NSQI (Yellow)

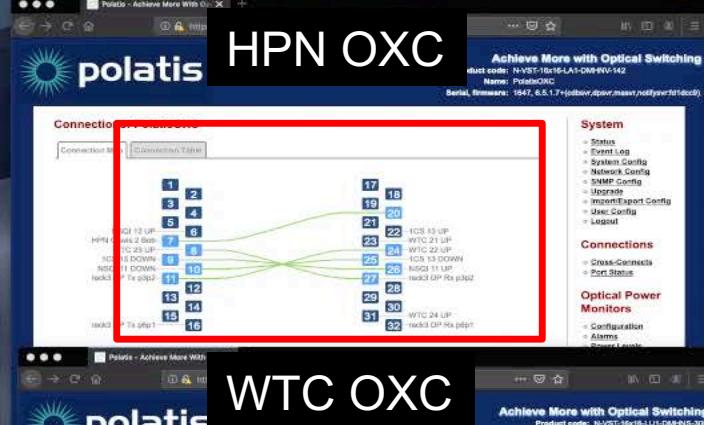
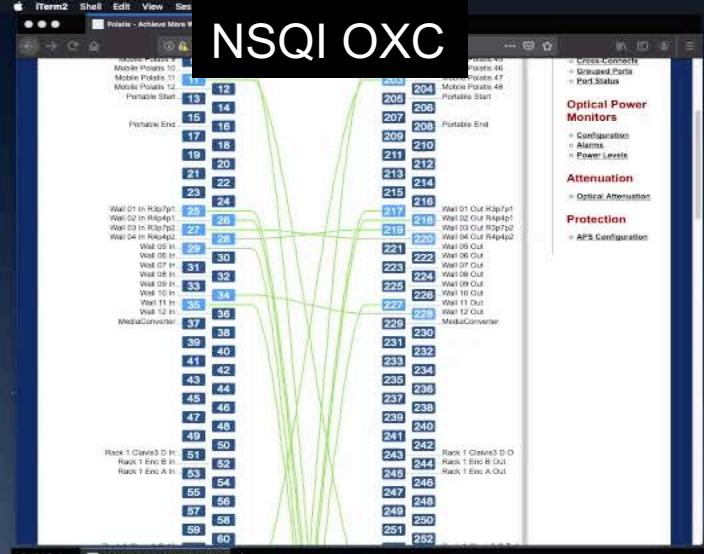
## Key Points:

2 New Secure Links established



# Step 2 Actual Network topology





# WTC DB TRANSFER

# SecureLink 4 initiated

# Secure Link 1 interrupted

# 1CS DB TRANSFER

**Secure Link 3 initiated**

## Secure Link 2 interrupted

ID	FIRST NAME	LAST NAME	CREDIT CARD NUM	SEC. CODE	BANK ACCOUNT	PASSWORD
237	Amines	John	4123589765432109	86	12345678901234567890	5526 M#JdgpxvxB
238	Kathy	Practer	55389671515320696	368	GB13VWFK8172244099334	1913 k!TwNdi+j4#
239	Nathan	Proctor	6583828458192501	793	GB13VWFK8172244099334	jBfLICj59Pbd
240	Thomes	King	5566677314365318	547	GB13VWFK8172244099334	#29NNrxQd
241	Jenni fer	Bernard	35156677314365318	783	GB13VWFK8172244099334	#BBrp+jzPn
242	Allison	Rohinson	35156677314365318	783	GB13VWFK8172244099334	vL+8tgDxCT
243	Mary	Boyer	35929618198624440	789	GB13VWFK8172244099334	U7fKcX<1sQ
244	Treacy	MILLER	6504946755001	456	GB14XH1665547560071	vgJu-5wds
245	Nancy	Boyd	3504144520943474	372	GB13VWFK8172244099334	2338-WQn+d
246	Cheryl	Brashaw	3504144520943474	456	GB13VWFK8172244099334	HQ73JRA14467039483
247	Nataly	Atkinson	350449374373283	2672	GB05FJWV593001575779	+wVtLc18G
248	Christopher	Romero	3515524742801344	187	GB140AHk44577529885	HeMMN9yQ8
249	George	Ruminez	30261307587395	901	GB02FC0A3685954517944	F5Y5Nzrfw&
250	Thomas	Frozier	3552657150824528	295	GB14E9IK0W81308535876	L1TfMukk6
251	Sondra	Cook	414432805636	7653	GB44AZJL2128595061608	13x3teLtu7\$0

# Secure Link 4 initiated

# Secure Link 1 interrupted

12.55%

## HPN (CL2 BOB1)

Link 3 initialization

**SKR=3kB/s**

HPN (CL2 BOB1) ice's attenuation  
- [S]... remote system...  
- [S]... remote system...  
- RawKeyExchange: Number of frames Alice: 93895  
- RawKeyExchange: Number of frames Bob: 93895  
- RawKeyExchange: Number of frames Alice: 11  
- RawKeyExchange: Probability of detection #1: 0.0035050  
- RawKeyExchange: Probability of detection #2: 0.0032290  
- RawKeyExchange: Delay #1: 33651, 65  
- RawKeyExchange: Delay #2: 33651, 55  
- ThreadRawKeyExchange: 505208 states available  
- ThreadRawKeyExchange: 1 state buffer(s) in the queue  
- [SYNC MSG] ThreadRawKeyExchange: Running RKE  
- [SYNC MSG] ThreadSiftingManager: Running sifting  
- SiftingManager: Sifting key (505208 bits)  
- SiftingManager: Alice basis ratio = 0.499967  
- SiftingManager: Bob basis ratio = 0.499745  
- SiftingManager: Alice value ratio = 0.500000  
- SiftingManager: Bob value ratio = 0.500007  
- SiftingManager: Sifted key size: 136570 bits  
- SiftingManager: Sifting duration: 0.135212 seconds  
- ThreadSiftingManager: 819258 bits available  
- [SYNC MSG] RawKeyExchange: Setting Alice's attenuation  
- [SYNC MSG] RawKeyExchange: Waiting for remote system...

Secure Link 3 initialization

SKR=3kB/s

```
[S] NSQI (CL2 BOB2) : remote system...  
[S] LaunchProc INFO - Ra 94084  
[S] LaunchProc INFO - RawKeyExchange: number of frames Bob: 94083  
[S] LaunchProc INFO - RawKeyExchange: Number of missed frames Alice: 0  
[S] LaunchProc INFO - RawKeyExchange: Probability of detection #1: 0.0095488  
[S] LaunchProc INFO - RawKeyExchange: Probability of detection #2: 0.0124500  
[S] LaunchProc INFO - RawKeyExchange: Delay #1: 31841, 23  
[S] LaunchProc INFO - RawKeyExchange: Delay #2: 31841, 20  
[S] LaunchProc INFO - ThreadRawKeyExchange: 1050708 states available  
[S] LaunchProc INFO - ThreadRawKeyExchange: 1 state buffer(s) in the queue  
[S] LaunchProc INFO - [SYNC MSG] ThreadSiftingManager: Running sifting  
[S] LaunchProc INFO - [SYNC MSG] ThreadRawKeyExchange: Running RKE  
[S] LaunchProc INFO - SiftingManager: Sifting key (1050708 bits)  
[S] LaunchProc INFO - SiftingManager: Alice basis ratio = 0.499975  
[S] LaunchProc INFO - SiftingManager: Bob basis ratio = 0.500355  
[S] LaunchProc INFO - SiftingManager: Alice value ratio = 0.49977  
[S] LaunchProc INFO - SiftingManager: Bob value ratio = 0.498018  
[S] LaunchProc INFO - SiftingManager: Sifted key size: 267706 bits  
[S] LaunchProc INFO - SiftingManager: Sifting duration: 0.135703 seconds  
[S] LaunchProc INFO - ThreadSiftingManager: 577278 bits available  
[S] LaunchProc INFO - [SYNC MSG] RawKeyExchange: Setting Alice's attenuation  
[S] LaunchProc INFO - RawKeyExchange: Setting Bob's attenuation
```

Secure Link 4 initialization

SKR=1KB/s

"rack3\_cnp" 21:21 01-Sep-1

# *High Performance Networks Group*

# Summary

---

- First public, field-deployed QKD switched mesh network
- Optical switch in each node
- Co-existence capabilities



# Acknowledgements



SMART  
INTERNET  
LAB



QUANTUM  
COMMUNICATIONS  
HUB



## High Performance Networks Group



Mr Anderson  
Bravalheri



Dr. Emilio  
Hugues Salas



Dr Rodrigo  
Stange Tessinari



Dr Djeylan Aktas



Mr Richard Collins



SMART  
INTERNET  
LAB