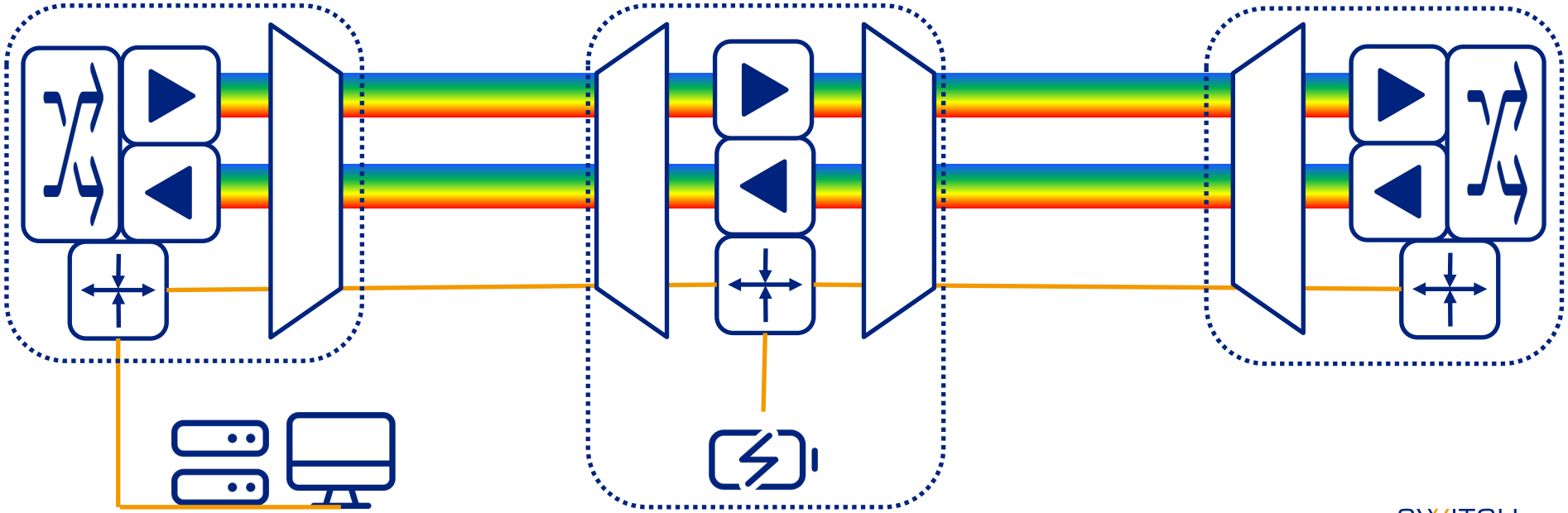
Frequency Dissemination Remote Management

GÉANT Infoshare, 21.6.2022 fabian.mauchle@switch.ch

SWITCH

DWDM Management

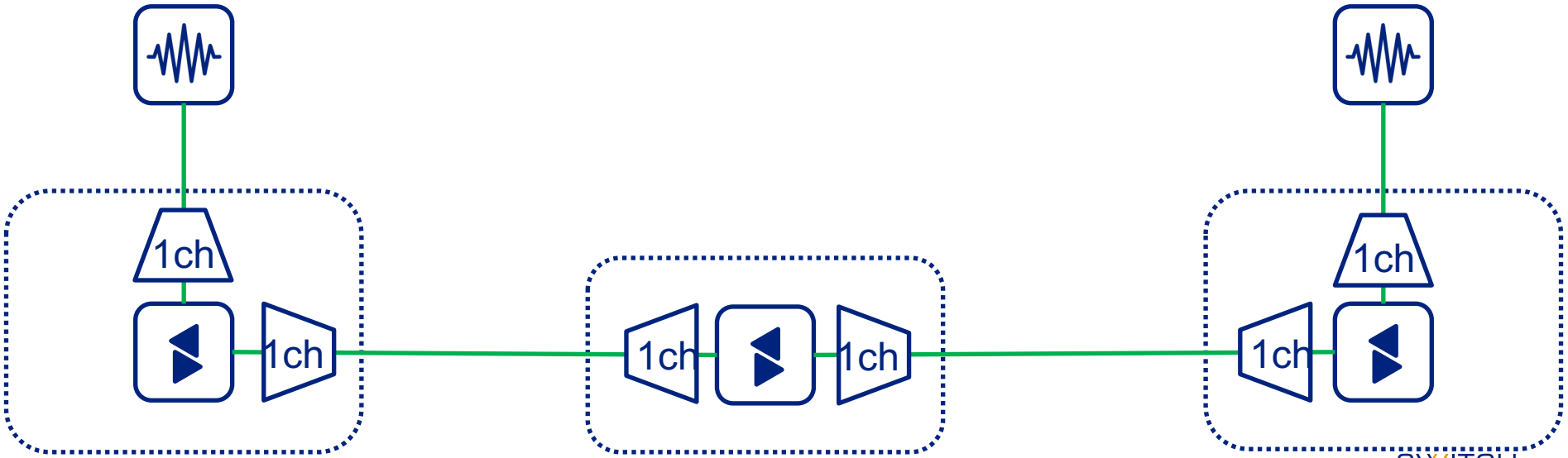
→ DWDM systems include IP based management network (DTN, OSC)
→ Transmitted on side-channel (1510nm, 1610nm) on same fiber, 100Mbit to 1000Mbit
→ Additional ethernet interface to connect other site equipment (user port, in-band port)



SWITCH

Frequency Dissemination

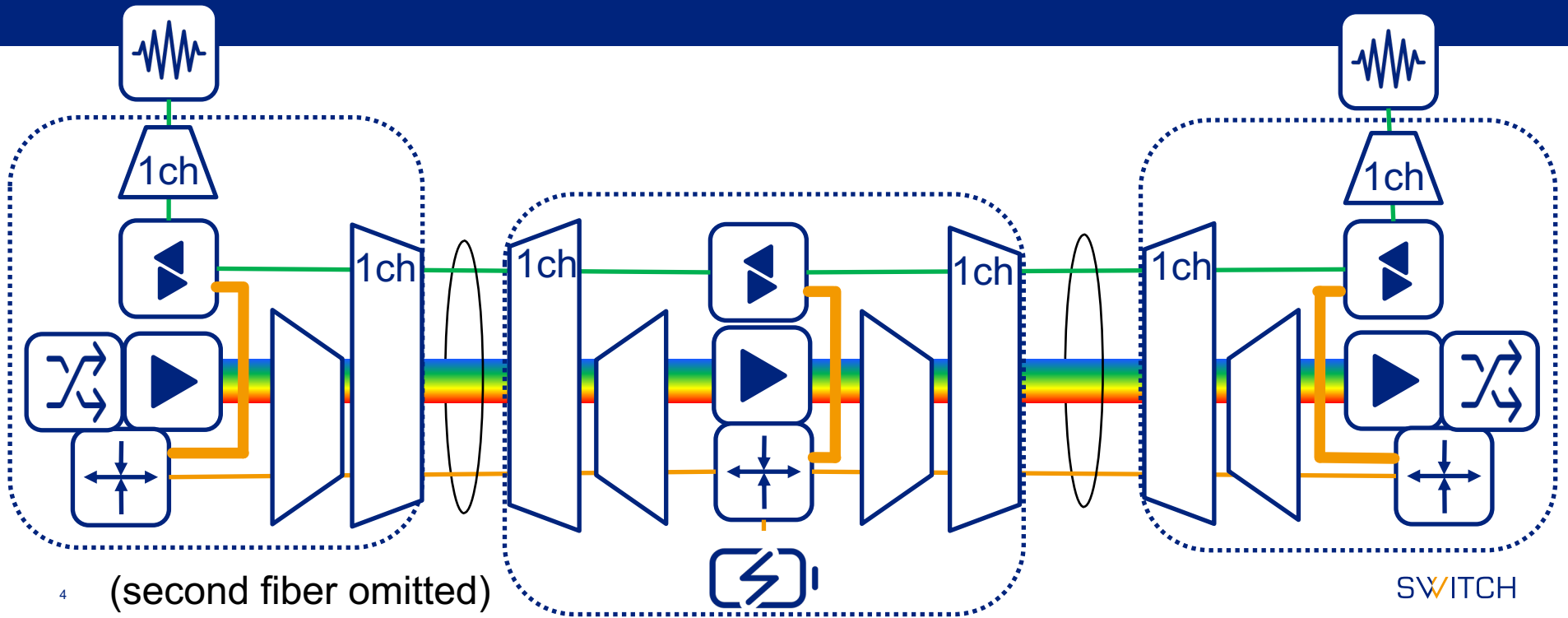
→ Single channel spectrum, single fiber, bidir amplifiers
→ No management channel, local management per site (more like early 2000’ DWDM)
→ End site / customer site need management too
→ Bidir amplifiers need narrow spectrum isolation (using single-channel DWDM OADMs)



SWITCH

Integrate Management

→ Integrate bidir amplifier management in existing DWDM management
→ Bidir spectrum isolation (DWDM OADMs) double as multiplexers
  → RAMAN amplifiers might use midstage extension port



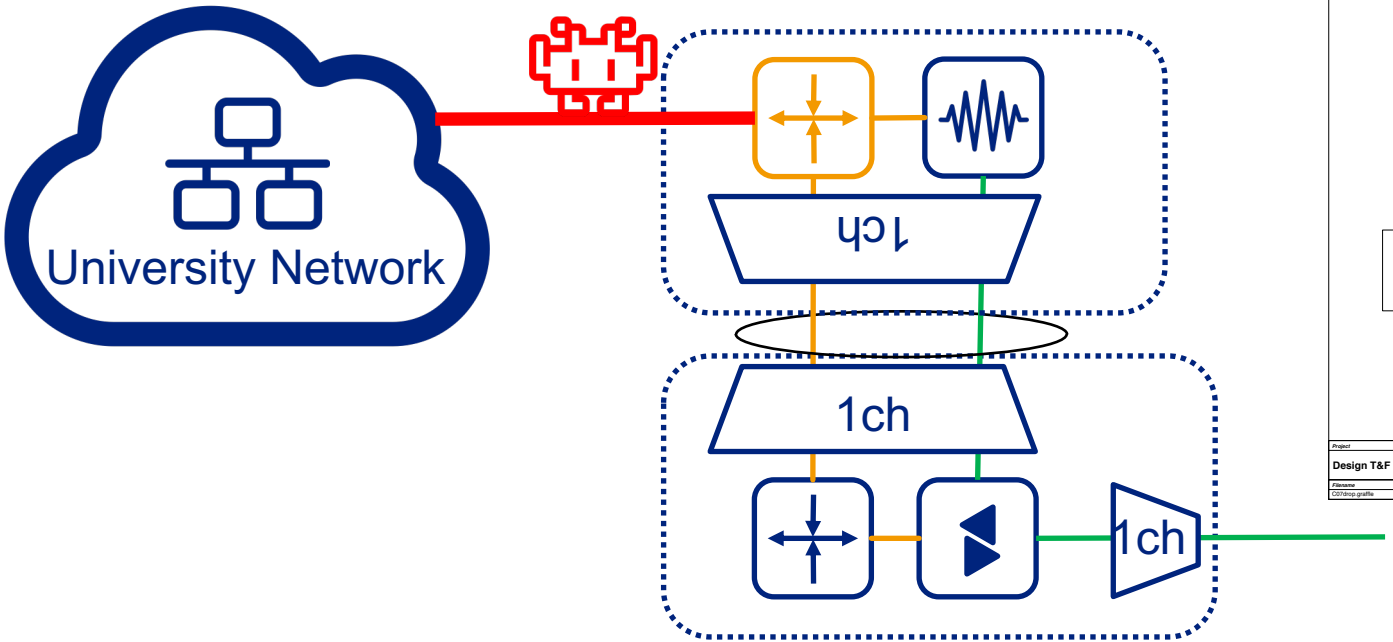
(second fiber omitted)

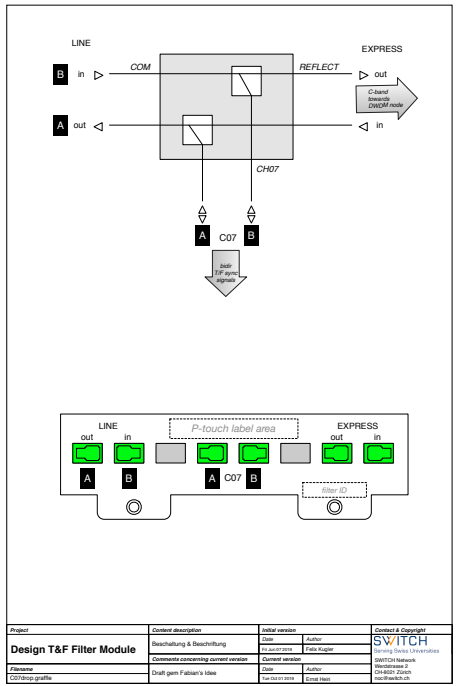
SWITCH

End-Site Management

→ Use same 1ch DWDM-OADM to multiplex management network
→ Add switch/router on end-site

→ Do **NOT** connect to university's network (local admin won't like you as a backdoor)

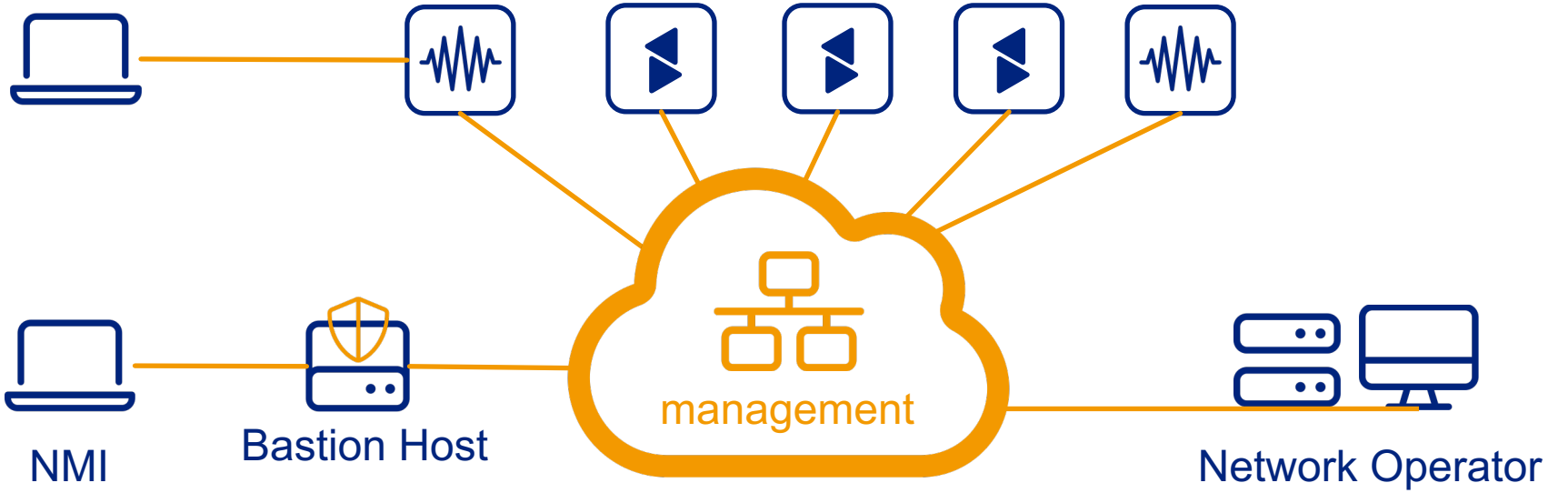




Remote Management

→ NMI personnel needs access (outside management network)

→ Some bastion host, proxy, vpn needed
→ e.g SSH Jumphost / SOCKS5 Proxy + NFtables rules include SSH user-id



SWITCH

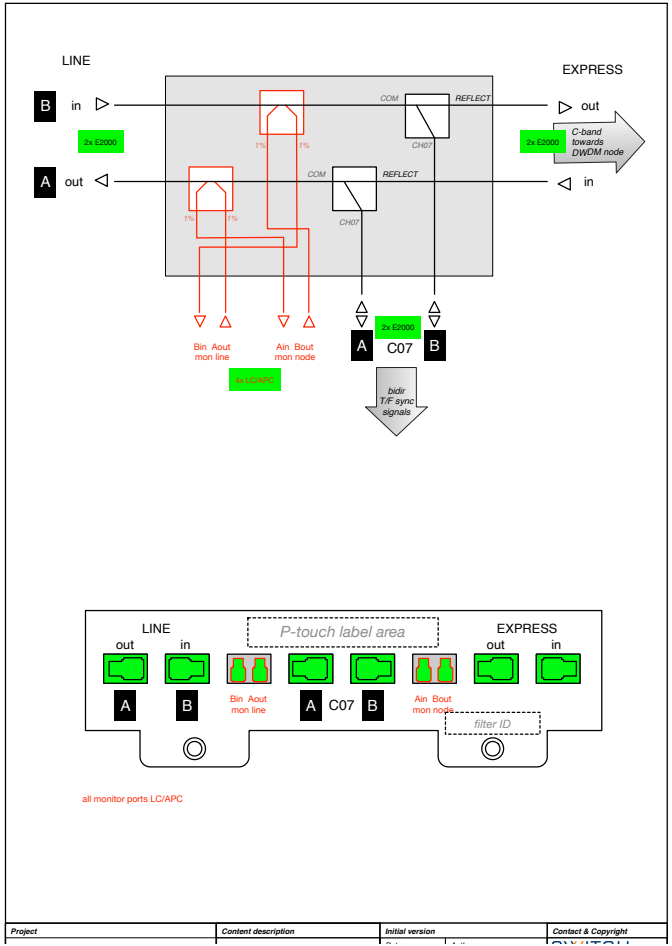
What we've learned

→ Amplifiers need little changes once link is established

→ NMI personnel mostly work directly from end-site (their lab)
→ Remote access works well enough

→ Integrate into NOC processes as spectrum service
  → not much insight besides light on/off
  → don't forget notifications when working on shared fiber

→ Taps on the OADM would be handy
  → debug spectrum (OSA) in-service
  → most DWDM equipment has them



SWITCH

Discussion

SWITCH

Bastion NFtables

```
#!/usr/sbin/nft -f

table inet filter {
 chain output {
  type filter hook output priority 0;
```

Log all connection attempts:

```
  ct state new log group 4 prefix "bastion new:" continue
```

Allow specific destination IP per user:

```
  ip addr <device-address> skuid <username> accept
```

Deny everything else and log it:

```
  log log group 4 prefix "bastion denied:" reject with
icmpx type admin-prohibited
 }
}
```

iptables equivalent:

```
-A OUTPUT -d <device-address> -m owner --uid-owner
<USERNAME> -j ACCEPT
```


SWITCH

Disclaimer

SWITCH is liable neither for the completeness, accuracy, correctness and continuous availability of the information given, nor for any loss incurred as a result of action taken on the basis of information provided in this or any other SWITCH publication. SWITCH expressly reserves the right to alter prices or composition of products or services at any time.