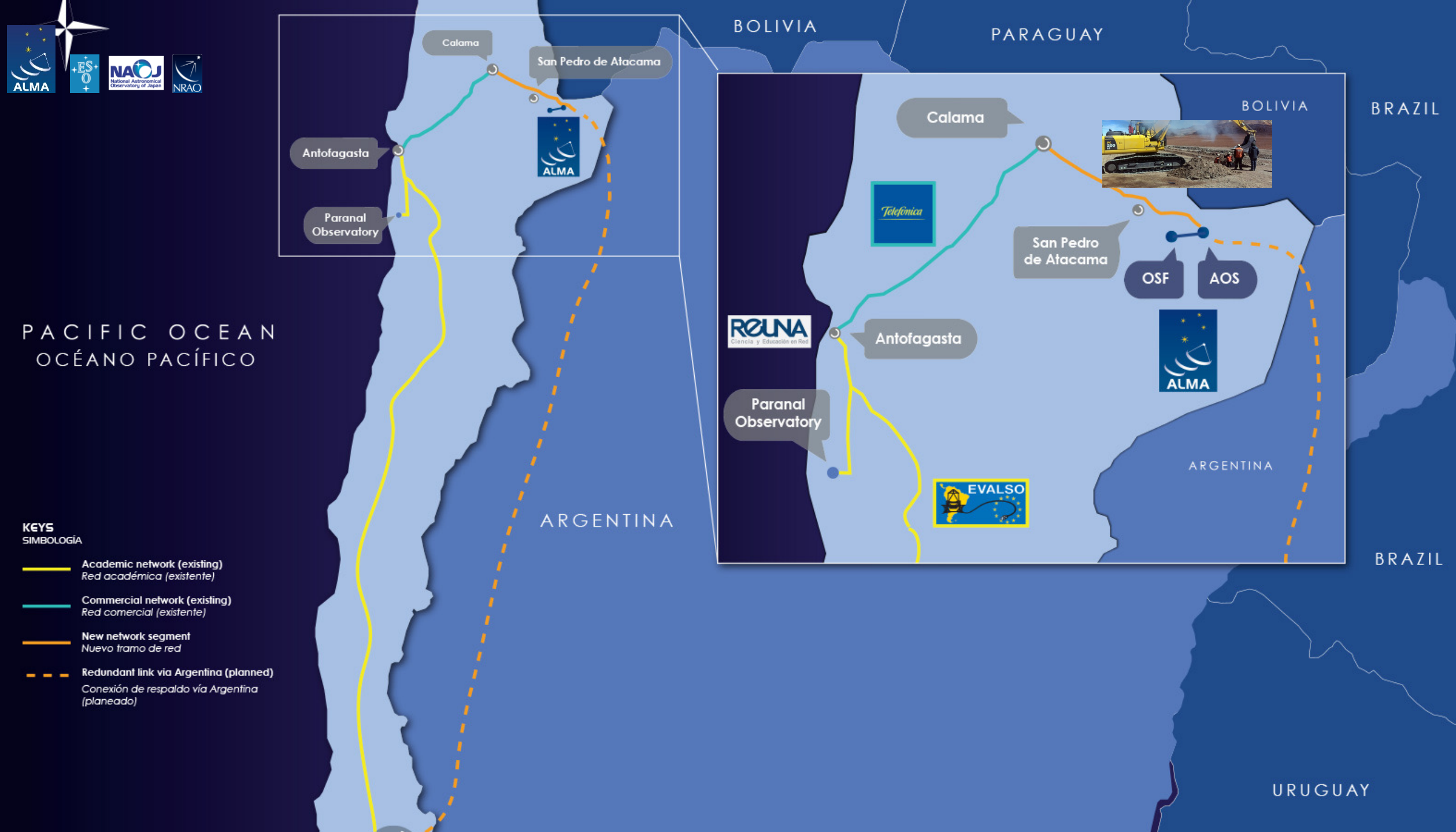
Joint ALMA Observatory
Update 2023

Jorge Ibsen

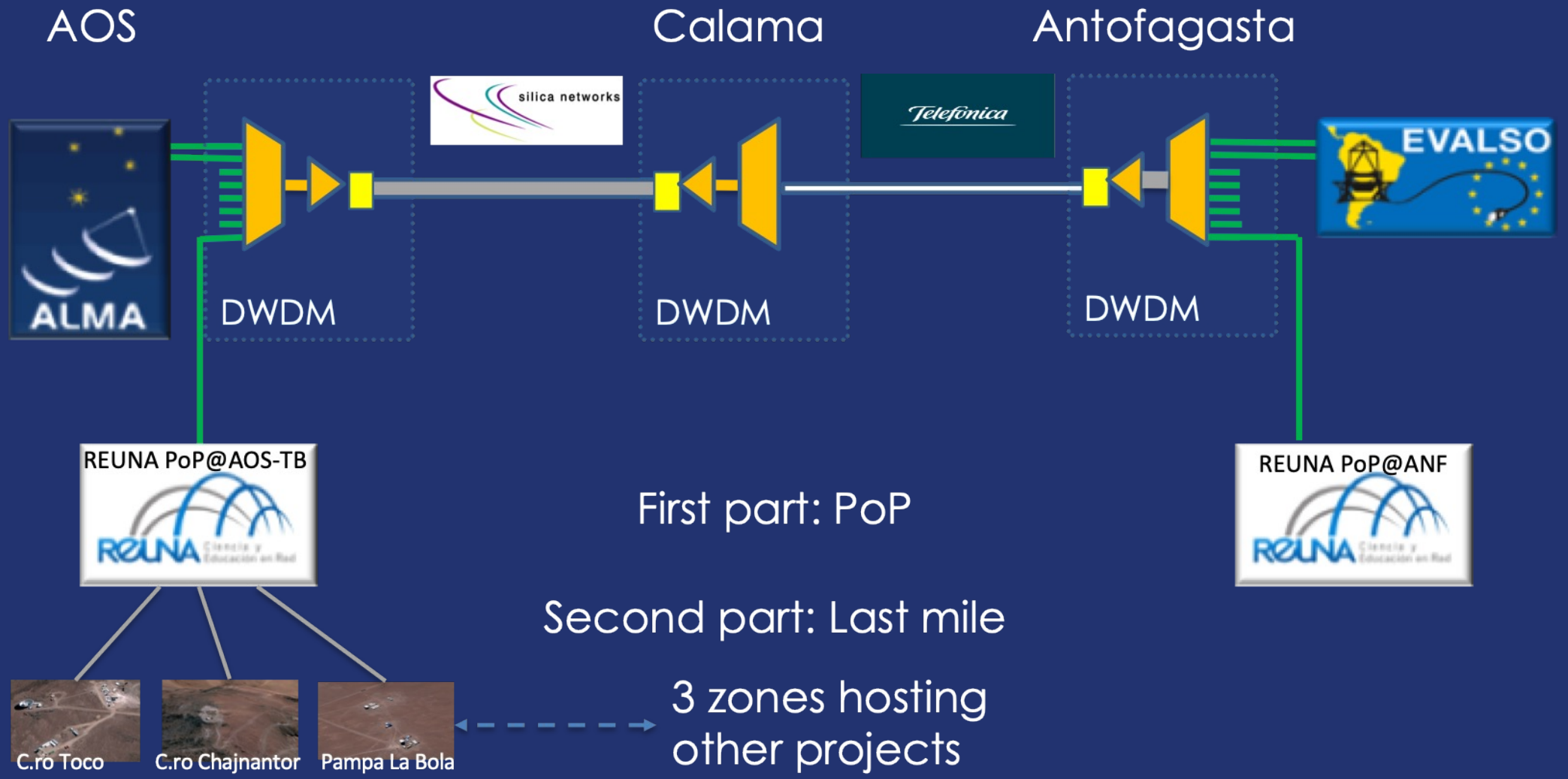
Head of Computing

ALMA Operations

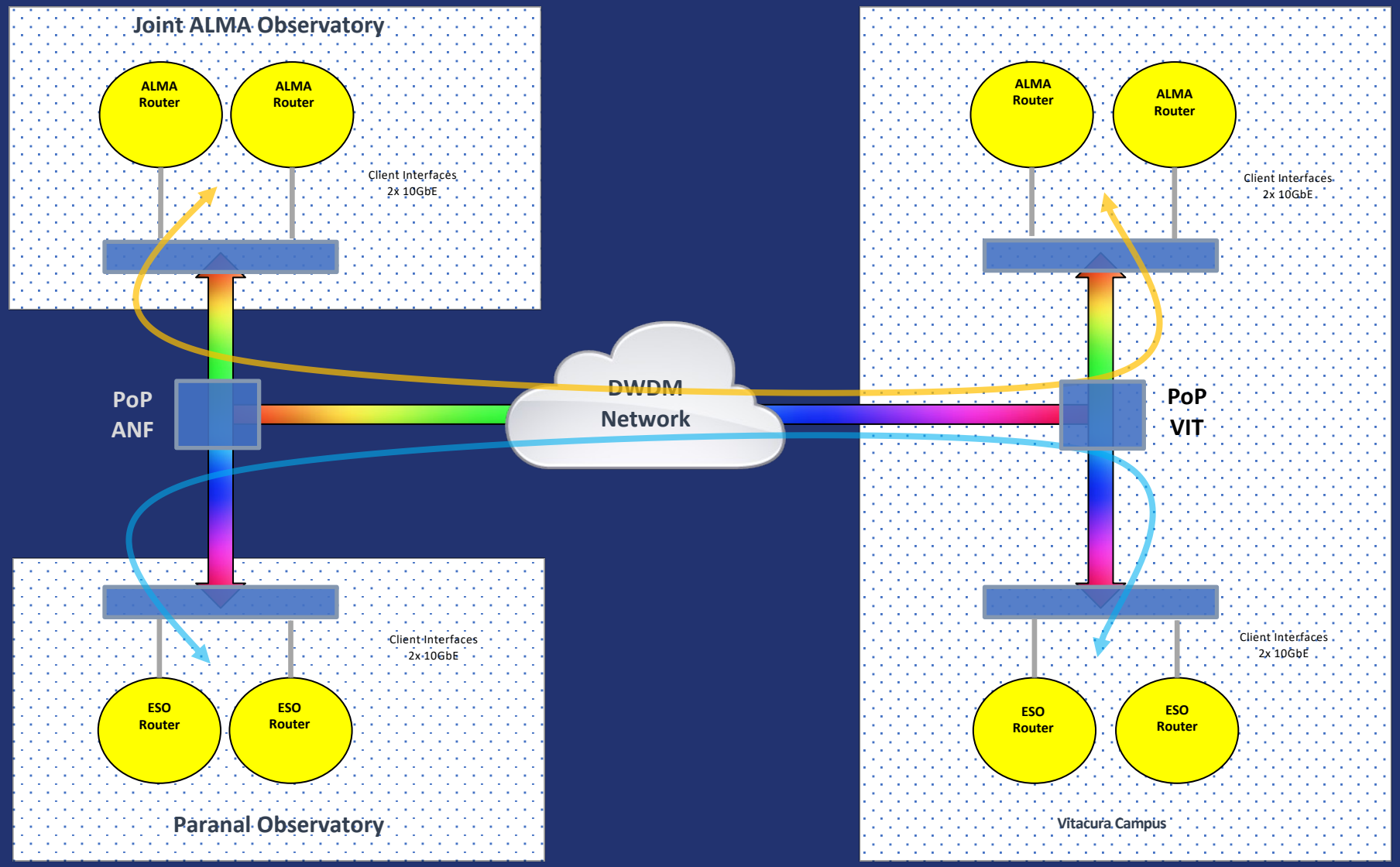

Ecosystem
ASTE
NANTEEN2
CCAT
TAO
APEX
ALMA
Leighton Observatory
ACT/Polar Bear/CLASS/ABS
Simons Observatory
Google Earth
Image © 2018 CNES / Airbus
Image © 2018 DigitalGlobe
ALMA
ESO
NAOJ
National Astronomical Observatory of Japan
NRAO


ALMA
ESO
NAOJ
National Astronomical Observatory of Japan
NRAO
Calama
San Pedro de Atacama
Antofagasta
Paranal Observatory
ALMA
BOLIVIA
PARAGUAY
BRAZIL
PACIFIC OCEAN
OCÉANO PACÍFICO
ARGENTINA
Calama
BOLIVIA
Telefónica
San Pedro de Atacama
OSF
AOS
RedCLARA
Ciencia y Educación en Red
Antofagasta
ALMA
Paranal Observatory
EVALSO
ARGENTINA
BRAZIL
URUGUAY
KEYS
SIMBOLOGÍA
Academic network (existing)
Red académica (existente)
Commercial network (existing)
Red comercial (existente)
New network segment
Nuevo tramo de red
Redundant link via Argentina (planned)
Conexión de respaldo vía Argentina (planeado)

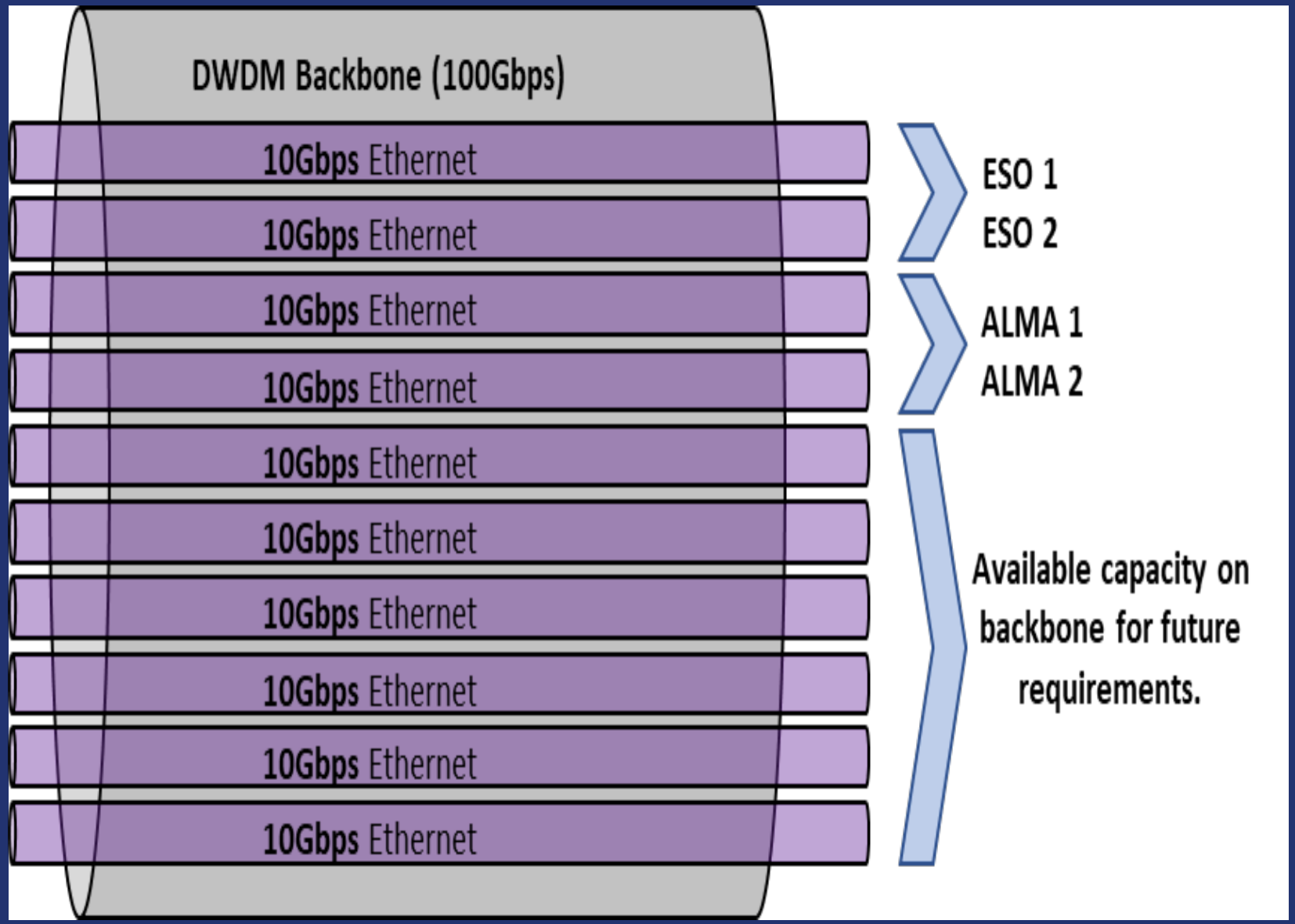
DWDM Equipment Obsolescence



Replacing EVALSO: ESO Call for Tender in Progress



Replacing EVALSO: ESO Call for Tender in Progress



ALMA Operations

Critically based in the interoperability of four separate facilities.

ALMA users worldwide require transparent access to systems and services located within JAO intranet to operate and maintain the observatory

Cyber security incident

What?

- Hive group type ransomware attack performing multiple actions on compromised systems (filesystems encryption, removal of storage volumes, spamming)

When?

- Attack started Oct 29, ~03:00 CLST, first noted by staff ~06:14 CLST, contained within the same day
  - The incident started at the beginning of the first long four days spring weekend after pandemics
- DDoS attack on Nov 1, not conclusively clear if it was related
- Targeted phishing on Nov 4, very likely related

How?

- VPN incoming traffic, most likely attackers got a user/passwd pair
  - Several logs were encrypted or removed during the attack making impossible to know more details about it

Affected physical systems:

- Virtual clusters and associated storages in ALMA facilities, subset of laptops

The attack was blocked before being completed in full.

Recovery

Achieved

- Cycle 9 resumed seven weeks after (Dec 17, 2022)
- Preproduction and testing infrastructure handed over for Cycle 10 testing (Jan 27, 2023)

Priorities

- Encapsulate as much as possible the knock down effect of the cyber attack to Cycle 9 observing window and minimize impact on Cycle 10 milestones and start of observing cycle
- Actively manage and address cybersecurity risks moving forward

Challenges

- Suitable staff levels to work in recovery activities as systems started to became operational
- JAO computing understaffed (10%-15%) due to turn over and southern summer vacation period (Jan/Feb 2023) also affected staffing availability
- Resume commitments with hard time constrains to comply with (e.g., Atlassian license obsolescence, AEDM project closure, 10y commemoration, …)

Cybersecurity strategy

Prevention

- Assess cyber security risks and enable mitigation actions to reduce the probability of those risks to acceptable levels
- Continue to deploy internal audit solutions to secure systems and increase awareness on staff
- Continue cyber security training for both IT specialist and general users

Containment

- In the event of a successful cyber attack, ensure that the intrusion can be timely contained to minimize negative effects in existing systems

Recovery

- Identify and secure data critical to business continuity to effectively realize disaster recovery plans

Prevention

- Least privilege access – if you don't need it, you don't have it
- Multi-factor authentication – make it harder to impersonate
- Anti-malware monitoring – endpoints and traffic analysis, CSIRT
- Cyber security updates – get them deployed timely
- Data protection – off site vaults for data critical to business continuity, use of cloud commodities when applicable

Containment and Recovery

- Network segmentation to separate administration from user services as well as core and support services domains
- User access rights profiling
- Policies
  - Update on staff obligations and expected behavior toward cyber security: acceptable use, cyber hygiene, password policy,
  - Mandatory yearly awareness trainings becoming a requisite to get access to systems
- Backup structure oriented to integrate cyber attack disaster recovery and acceptable time constrains

Closing thoughts

- The distributed nature of modern operations and the required interoperability between facilities adds additional complexity to cyber security risk management.
  - **Close coordination between interdepending sites is a requisite to be successful in preventive and containment actions**
- Constant active balancing between privileging operational convenience and cyber security considerations is required
- Cyber security actions organized based on a framework.
  - Incorporate best practices through awareness and training
- Incorporating new specific cyber security roles in staffing plans is important to continuously assess risks and updating mitigation actions as well as timely reaction to incidents

Thank you for your time!