Management of Broadband Wireless Access networks

Giacomo *"mino"* Bernardi

joint work with
Mahesh Marina and Peter Buneman

Broadband Wireless Access (BWA) networks

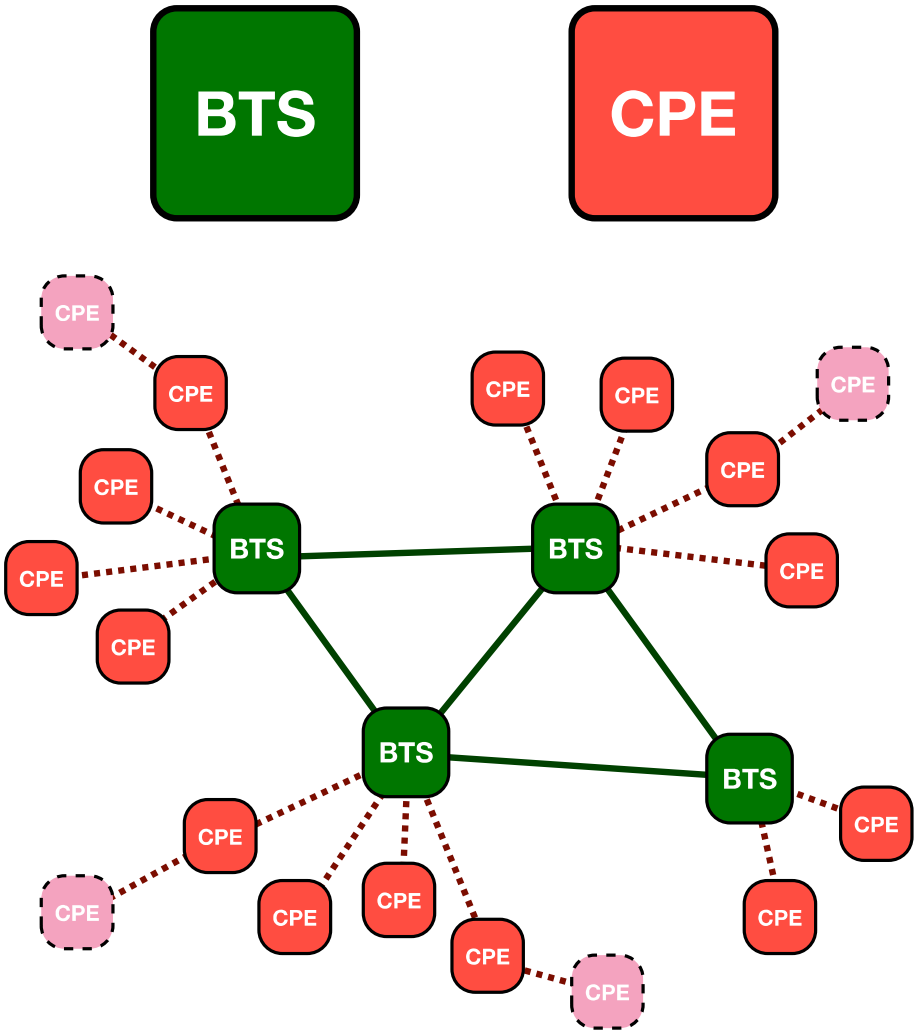
- BWA as effective mean to provide broadband **Internet access to remote subscribers.**

- Many reasons are making wireless **an attractive solution** for the “last mile” coverage:
  - **Lower financial requirements** than copper and fibre
  - **Freedom** from market incumbent
  - Ongoing spectrum “**deregulation**” and licensing of new frequencies
  - Recent developments in **wireless standards**
  - Does not require any existing infrastructure, especially attractive for **rural regions**
  - **Mobile** usage

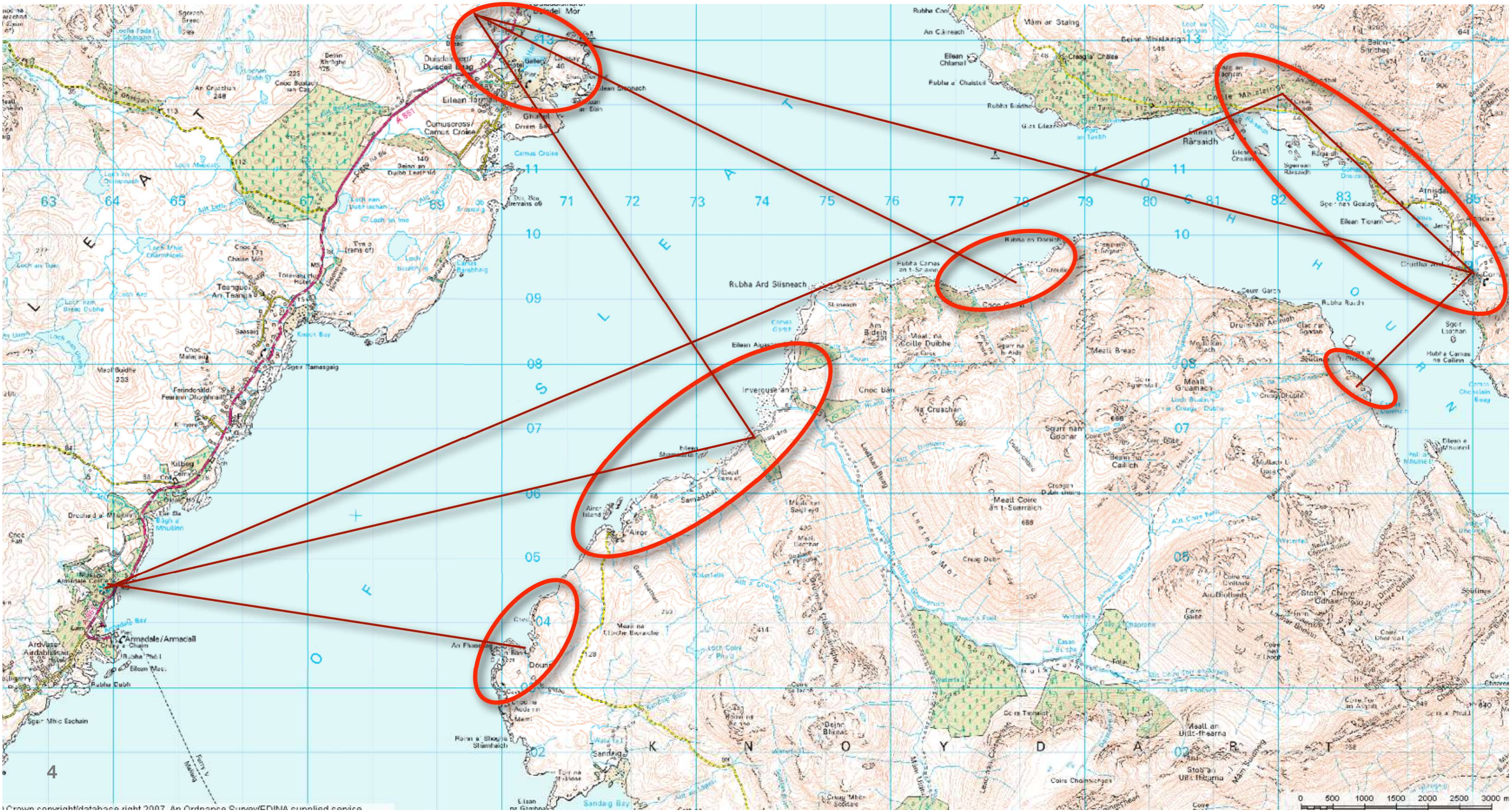
- More and more ISPs are moving to “all wireless” networks:
  - **access tier** is wireless!
  - **backhauling** is wireless!

The network model: *a ring of stars...*

- **Two types of devices**
  - Base transmitting stations (BTS)
  - Customer premises equipment (CPE)
- **Two types of links**
  - Point-to-point (PTP) for backhauling
  - Point-to-multipoint (PMP) for local access
- A common topology is thus **a ring of stars**:
  - easy to connect remote users
  - robust backbone



Our *tegola* testbed



Our *tegola* testbed

Our *tegola* testbed

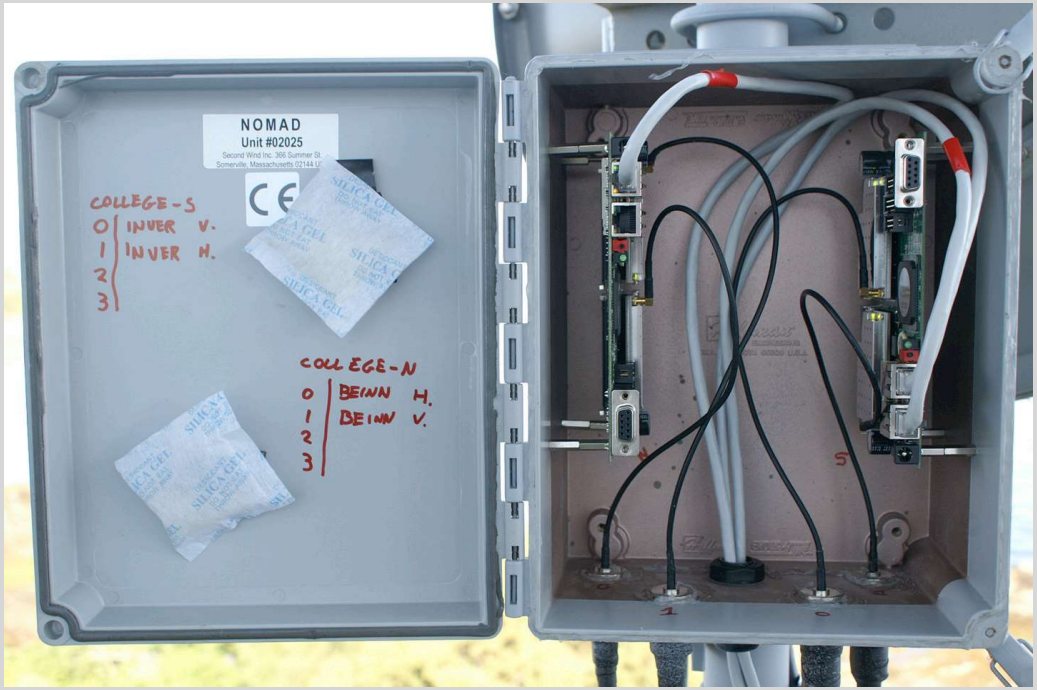
Our *tegola* testbed

Our *tegola* testbed

The BTS platform

- BTS devices:
  - are **core components** of the backbone network
  - **act as master** in point-to-multipoint links
  - can handle **IP routing** and QoS

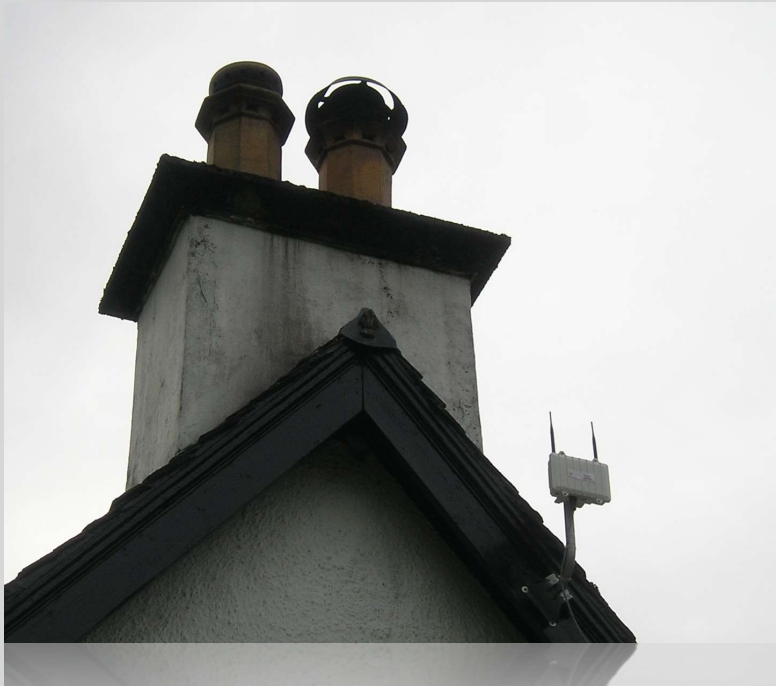
- **Our BTS platform** is based on Gateworks Avila boards running Linux, equipped 4 indipendent radios and two ethernet interfaces.



The CPE platform

- The **CPE device** is housed by the subscriber.
- It **marks the border** between the ISP cloud and the subscriber local network.
- Typically it **provides** DHCP, NAT, authentication and basic firewalling.

- **Our CPE platform** is composed by an x86 embedded board from PCengines equipped with **two 802.11abg radios** and an ethernet interface.



Advancements in BWA hardware

- Carrier-grade wireless hardware market is in **costant growth** (+37.5% in the last 12 months in the US).
- Higher competition generates **compromises.**
  - Even mid-sized ISPs use devices from **several vendors** and on **different wireless technologies.**
- Some vendors are specialized in PTP products, others in PMP, but all try to impose **their own infrastructure.**
- Devices are controlled over **SNMP** (private MIBs) or via proprietary protocols.
- CPEs are getting smarter (i.e.: **femtocells**).

What is management?

- Managing equipment for a WISP is worth **as the equipment itself.**
- **FCAPS** model: **F**ault management, **C**onfiguration, **A**ccounting, **P**erformance and **S**ecurity:

F	C	A	P	S
Fault detection	Resource initialization	Track service / resource usage	Utilization & error rates	Selective resource access
Fault correction	Network provisioning	Cost for services	Consistent performance level	Enable NE functions
Fault isolation	Auto-discovery	Accounting limit	Performance data collection	Access logs
Network recovery	Backup and restore	Combine costs for multiple resources	Performance report generation	Security alarm / event reporting
Alarm handling	Resource shut down	Set quotas for usage	Performance data analysis	Data privacy
Alarm filtering	Change management	Audits	Problem reporting	User access rights checking
Alarm generation	Pre-provisioning	Fraud reporting	Capacity planning	Take care of security breaches & attempts
Clear correlation	Inventory/asset management	Support for different modes of accounting	Performance data & statistics collection	Security audit trail log
Diagnostic test	Copy configuration		Maintaining & examining historical logs	Security related information distributions
Error logging	Remote configuration			
Error handling	Job initiation, tracking & execution			
Error statistics	Automated software distribution			

SNMP, a “de facto” standard

- **Simple Network Management Protocol**, standardized by IETF in the 80s.
- It’s **minimalist**, **lightweight**, **inexpensive** for a manufacturer to adopt.
- **Flaws**:
  - It specifies only the syntax of data
  - Since it works “in band”, it generates an intrinsic disturbance (heisenberg uncertainty)
  - Polling frequency is determined by the client
  - It lacks transactionality
  - Commands cannot have a flexible number of parameters
  - No queries based on object value or type
  - The “private MIB space” has degenerated (e.g.: Cisco has hundreds of thousands OIDs!)

- ...so basically it is an **end-to-end** data-moving protocol!

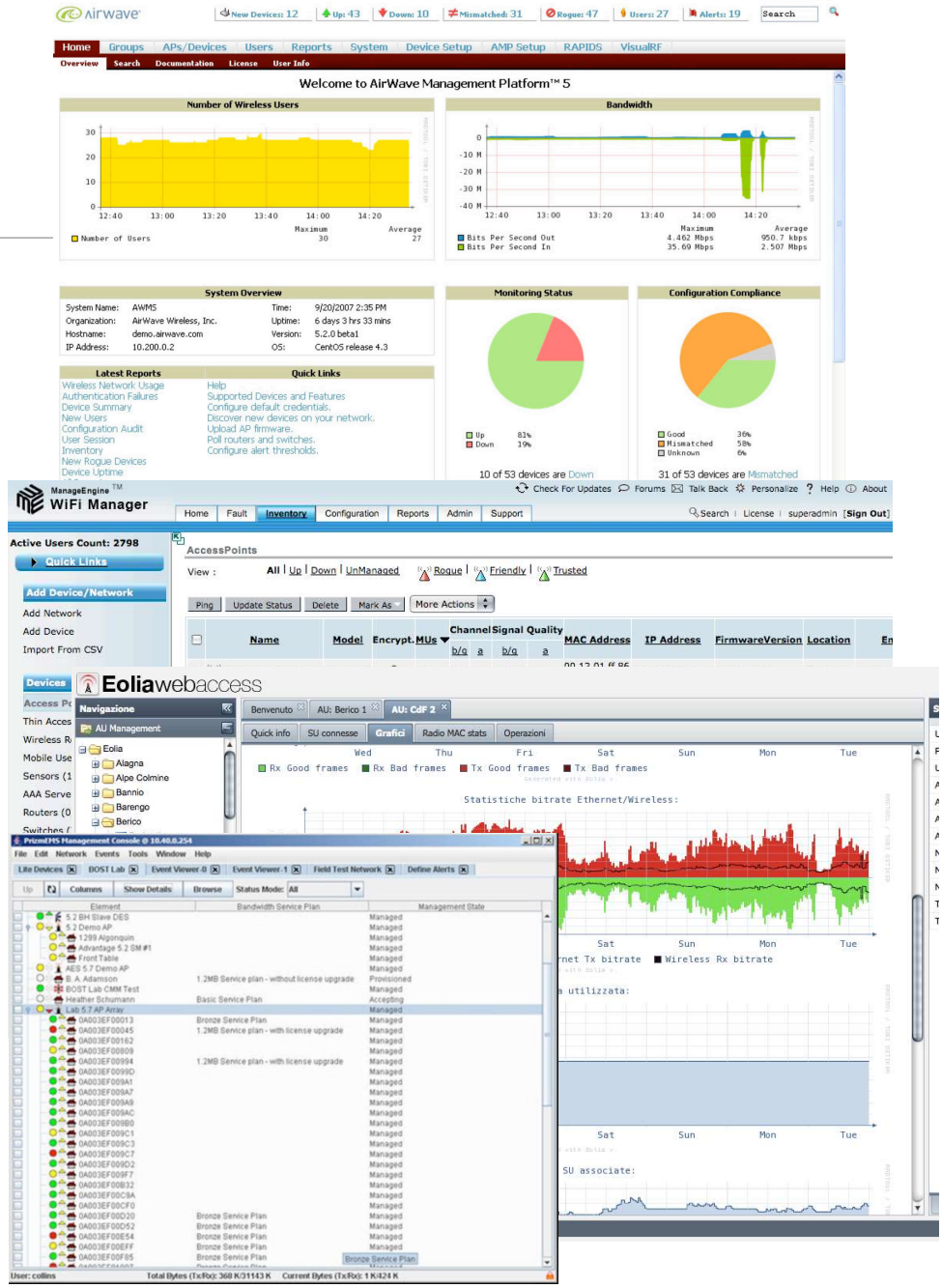
A bunch of use cases

- **Firmware upgrades:**
  remotely modifying the operating system of a horde of critical devices.
- **Bulk configuration changes:**
  e.g.: set the ESSID to all BTSs, change frequency of devices in an area.
- **Deployment of new devices:**
  how to prepare and configure CPEs before shipping them to subscribers.
- **Historical performances query:**
  “how has that link performed over the last month?”
- **Verify frequency planning:**
  check than a CPE cannot see more than a BTS on the same freq.
- **Triggered actions:**
  have a device perform an action without manual intervention.

The “state of the art”

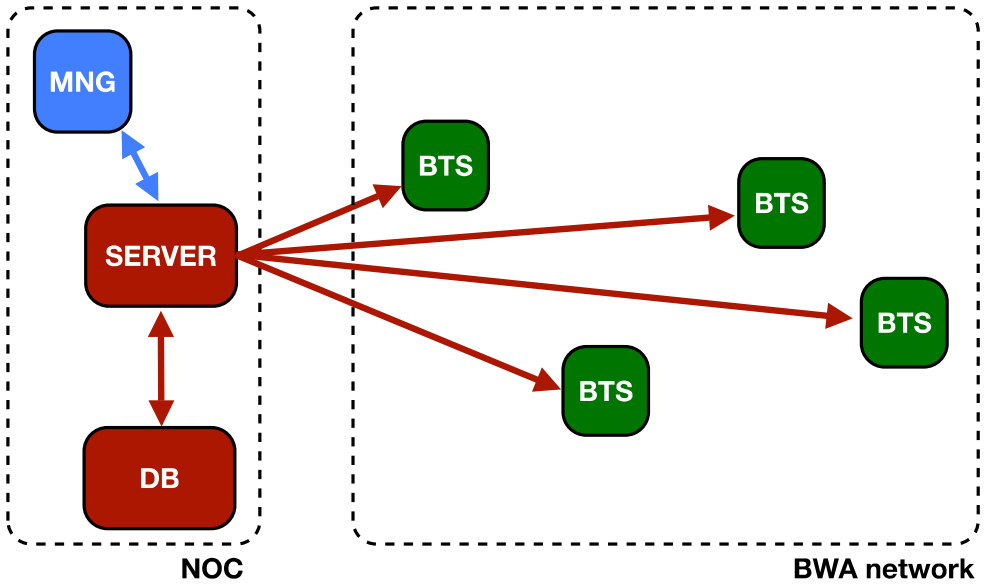
- On the market there is a myriad of network management software platforms:
  - **Products developed by hardware vendors** typically work only with devices of the same brand.
  - **Third parties solutions** often rely on standard SNMP MIBs.

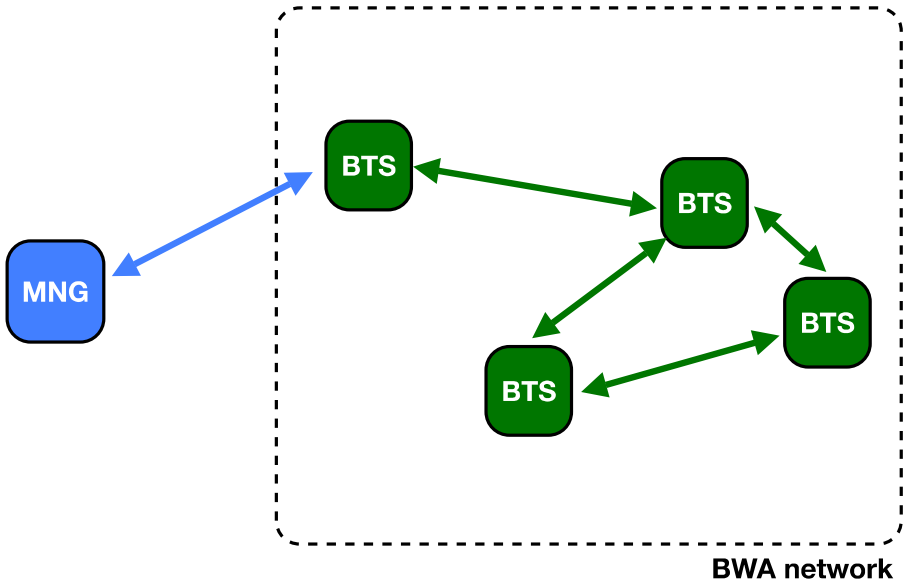
- They all bank on:
  - **remote servers** they run on
  - the existence of a **database**
  - **always-on links**



The network is the datacenter

- Traditional management software follows an **“end-to-end” paradigm**: it runs on a remote server at the ISP datacenter and connects to each remote device.
- Modern network equipment **not very different** from a datacenter.





Ideas from the academic community

- The IETF "**Remote Network Monitoring**" (RMON) to manage remote sites from a central location. It gives a certain level of decentralization over SNMP.
- **Active Networks** (early 90s) and **Smart Packets**: create more intelligent networks by introducing dynamic network programming, allowing routers to execute binary code received in packets.
- **Management by Delegation** (1995): server send applications to clients, the software is run where the data is.
- **Netscript** (1998): developed by IBM to provide a generic runtime environment on the nodes
- Real adoption of these ideas **?**

Proposed approach

- **Key concepts:**
  - **Device indipendence:** even in mid-sized WISP networks it is common to find devices from different vendors. Do not assume every device can be managed.
  - **Delegation:** as we authorize someone else to perform tasks on our behalf, a similar behavior can be applied to network devices.
  - **Local responsability:** it sould be possible to elect a device as responsible for a particular region.
  - **Scattered knowledge:** facts about the network should be stored in the network itself, the network *is* the database.

Thank you

www.tegola.org.uk