

Servizio di Connettività d'Ateneo

Network and services provisioning automation

rossella caputo
rossella.caputo@unipi.it

paolo de rosa
paolo.de.rosa@unipi.it

enrico bernardini
enrico.bernardini@unipi.it

WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA

Agenda

- Motivazioni
- Network & Services Infrastructure
- Automated Provisioning
- Criticità e miglioramenti

Motivazioni

ICT @ UniPi in numeri

- ~ 62.000 Studenti
- ~ 2500 Dipendenti
- 110 Edifici da connettere
- ~ 250 Km di canalizzazioni
- ~ 3000 Km di fibra sul territorio
- ~ 280 Access Point
- ~ 700 apparati di accesso
- ~ 5000 dispositivi VOIP
- 15 sedi remote fuori città
- Connettività per enti esterni

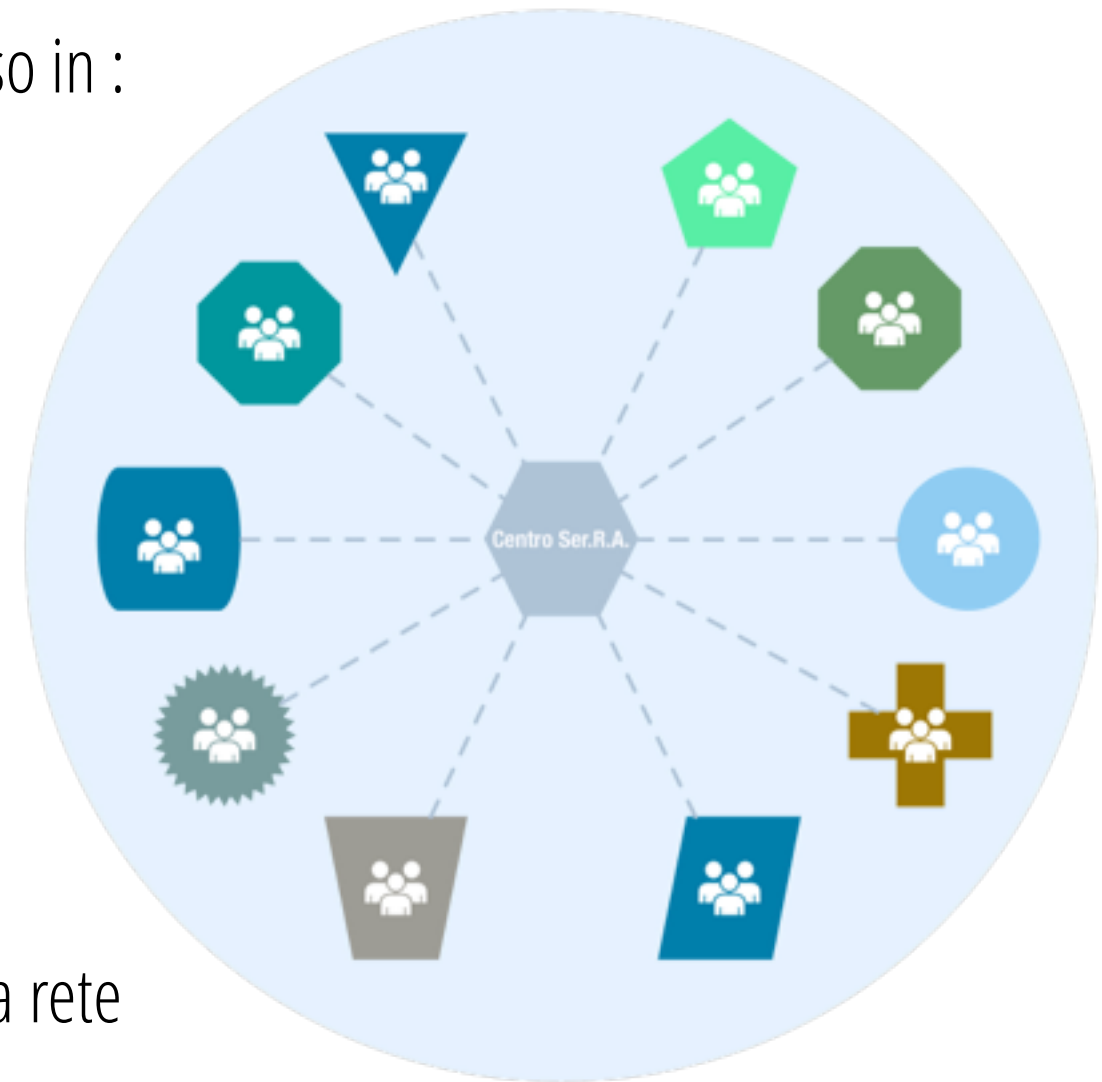
Organizzazione ICT

Prima del 19 Settembre 2012 il settore ICT era suddiviso in :

- 48 Dipartimenti
- 11 Facoltà
- 10 Strutture amministrative

Ogni struttura organizzava la connettività e i servizi ICT in autonomia oppure poteva usufruire di un sistema centralizzato gestito dal centro Ser.R.A.
Ciò ha determinato:

- disomogeneità nella gestione e utilizzo della rete
- maggior carico lavorativo per le piccole strutture
- difficoltà a stabilire buone pratiche per l'uso comune delle risorse

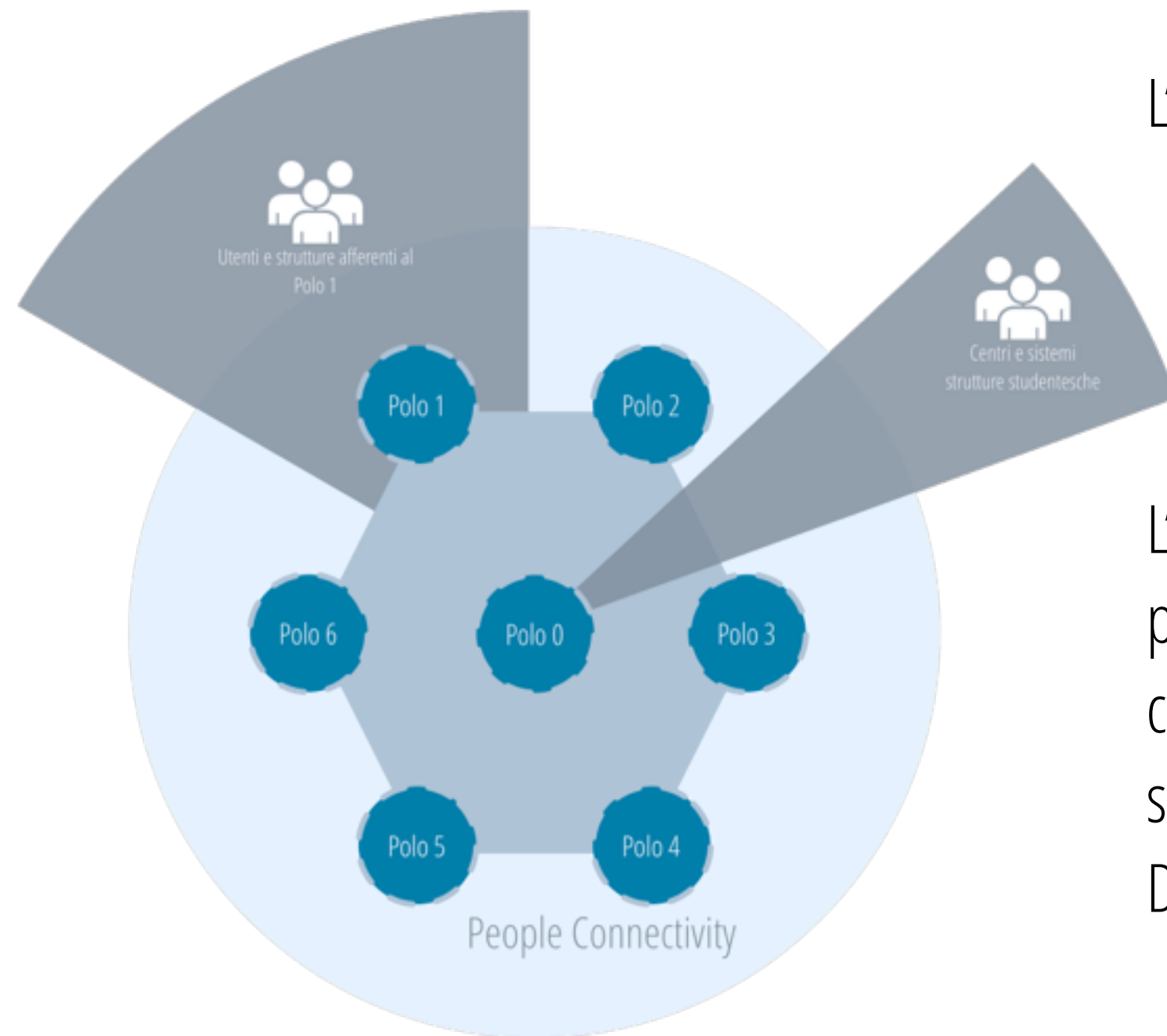


Organizzazione ICT

L'Ateneo è stato riorganizzato in :

- 20 Dipartimenti
- 15 Centri, Sistemi e altre strutture

L'area ICT viene organizzata in 7 poli per la gestione dei servizi informatici, che si spartiscono gli utenti delle 35 strutture dell'Ateneo. Un'unica Direzione ICT



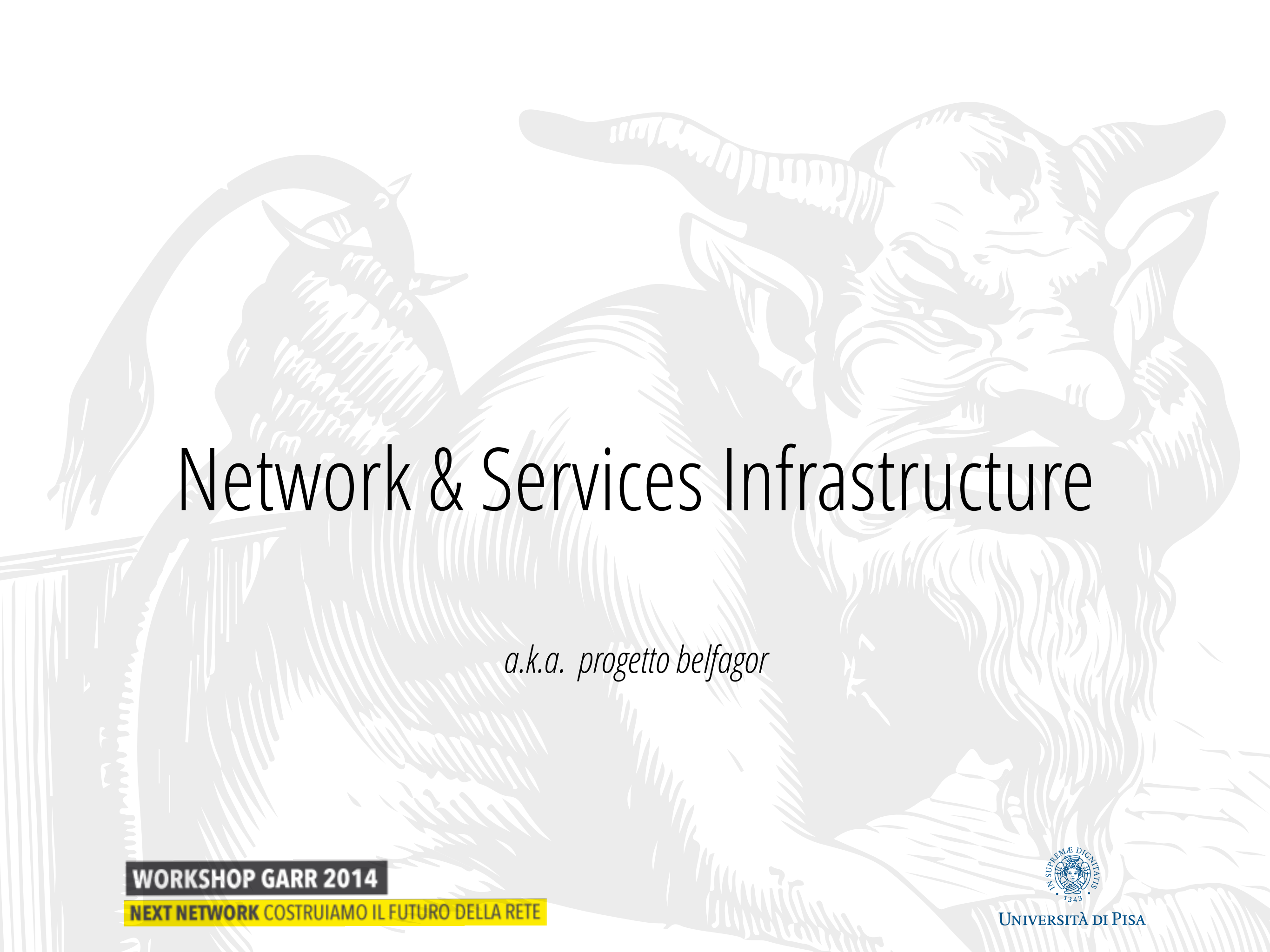
Obiettivo

All'inizio del 2013 viene chiesto di riprogettare la connettività in funzione del nuovo modello organizzativo, semplificando l'infrastruttura esistente e razionalizzando processi e risorse.

Nasce S.C.A.

Servizio di Connettività d'Ateneo

L'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati dell'Università, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna componente dell'Ateneo.



Network & Services Infrastructure

a.k.a. progetto belfagor

WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA

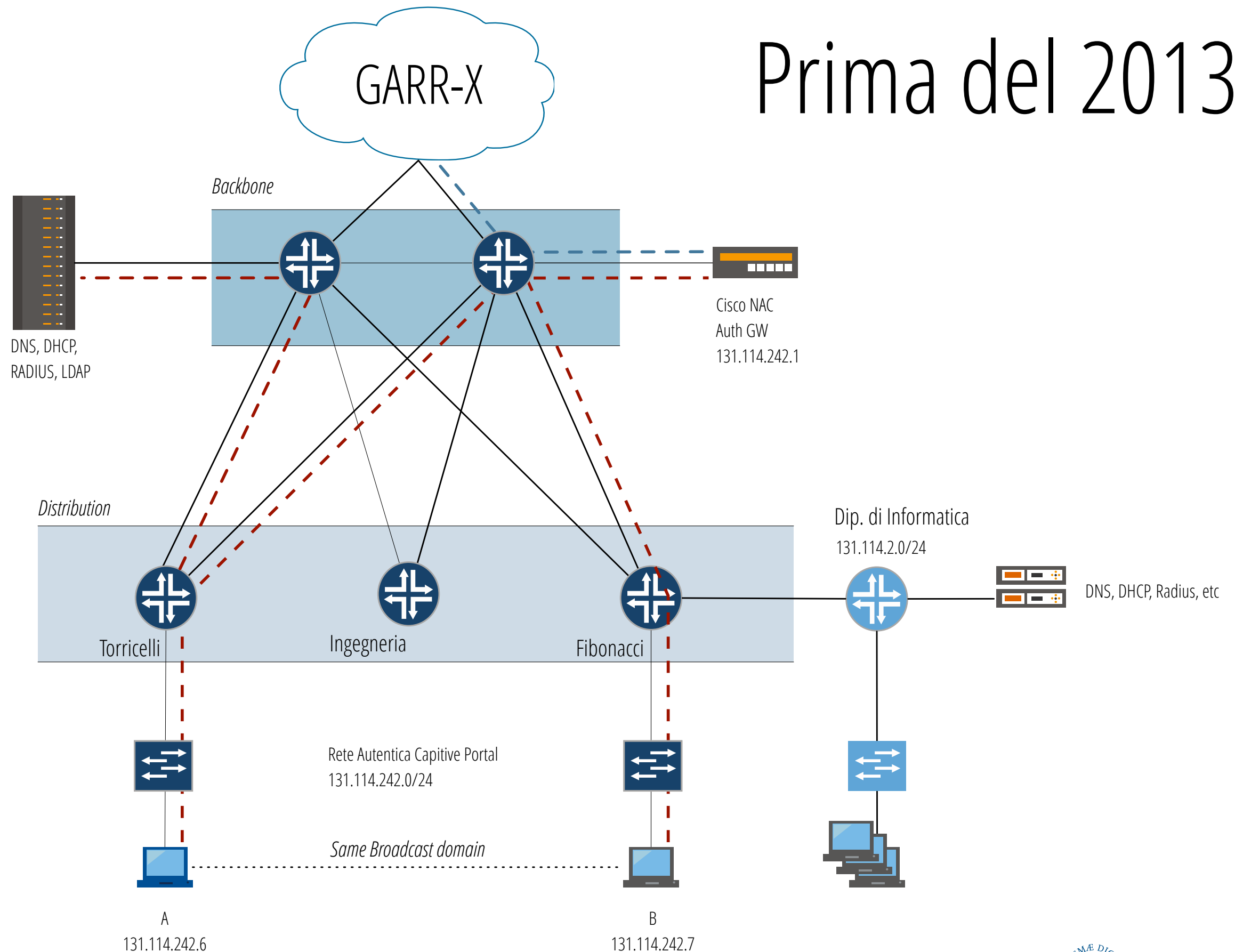
Requisiti I

- Modello organizzativo simile a GARR
- Autonomia nella gestione dei servizi
- Strumenti di gestione condivisi
- Accesso alla rete autenticato

Requisiti II

- Affidabilità del servizio
- Robustezza dell'infrastruttura
- Scalabilità (es. progetto scuole, enti esterni, etc)
- Flessibilità del modello (da afferenza amministrativa a geografica)
- Segregazione (un polo un dominio di routing)

Prima del 2013



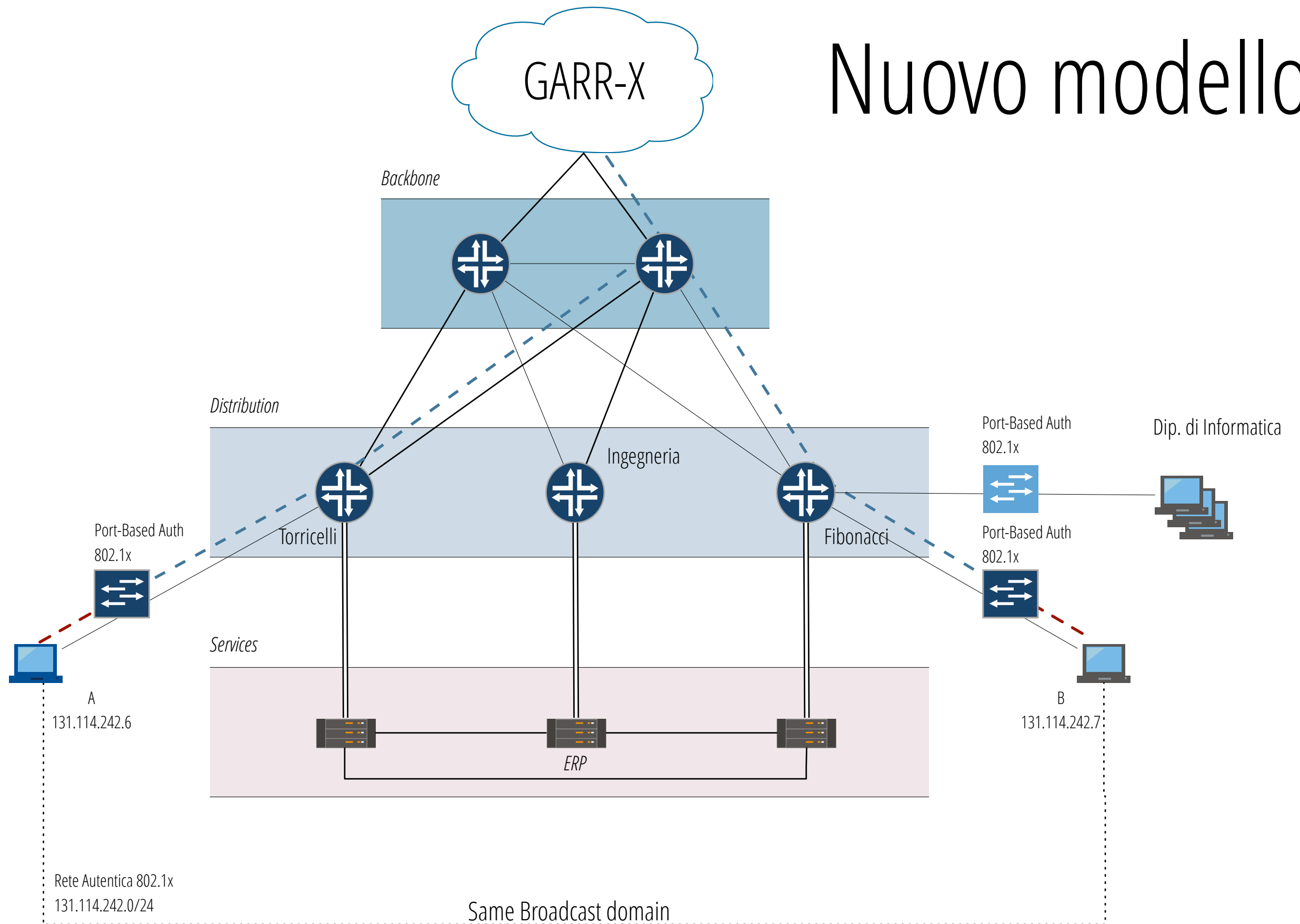
WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA

Nuovo modello



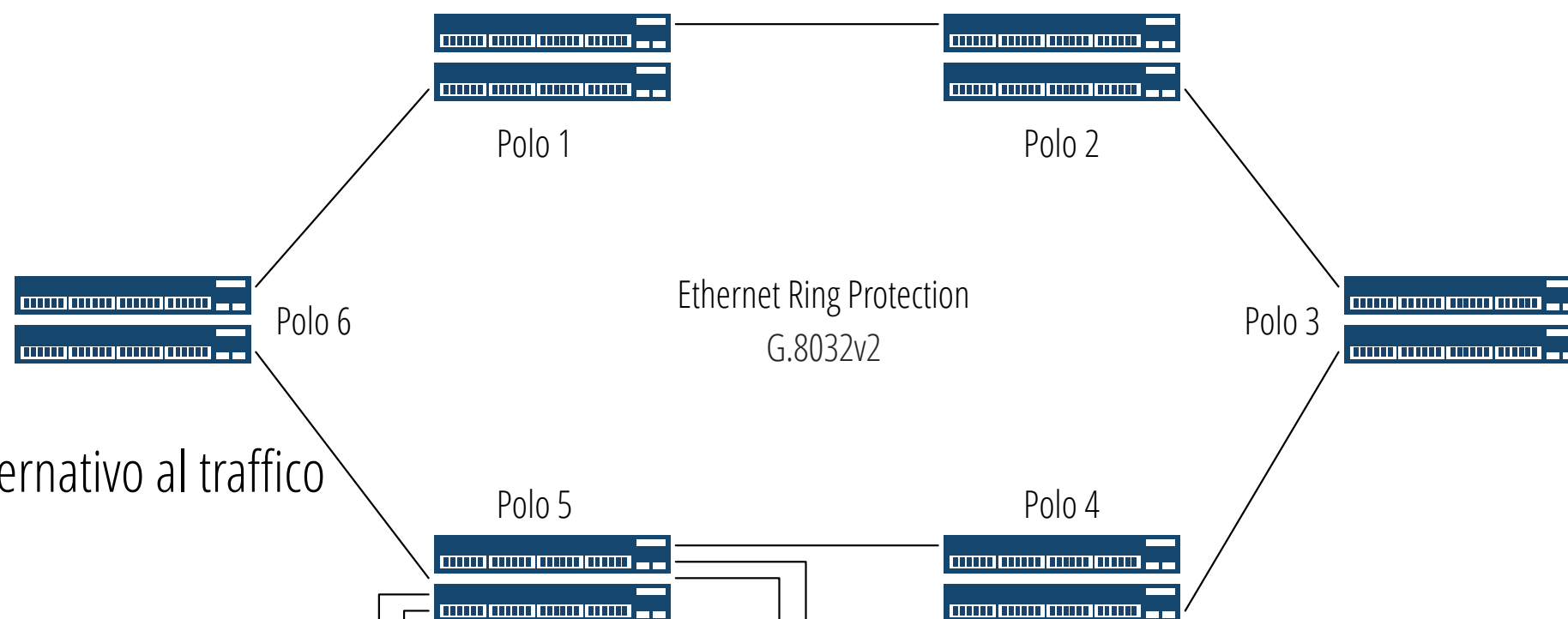
WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA

TORing



Anello in fibra alternativo al traffico di produzione

n.2 EX 4200 24T VC

n.2 Dell R420 (8 Cores, 40GB RAM)

Compute Node 1
ring0: 172.19.0.2
Compute Node 2
ring0: 172.19.0.3



VMs

ringU: 172.19.1.100 (management)

monoid: 131.114.138.100 (services)

VMs

ringU: 172.19.1.101 (management)

monoid: 131.114.138.101 (services)

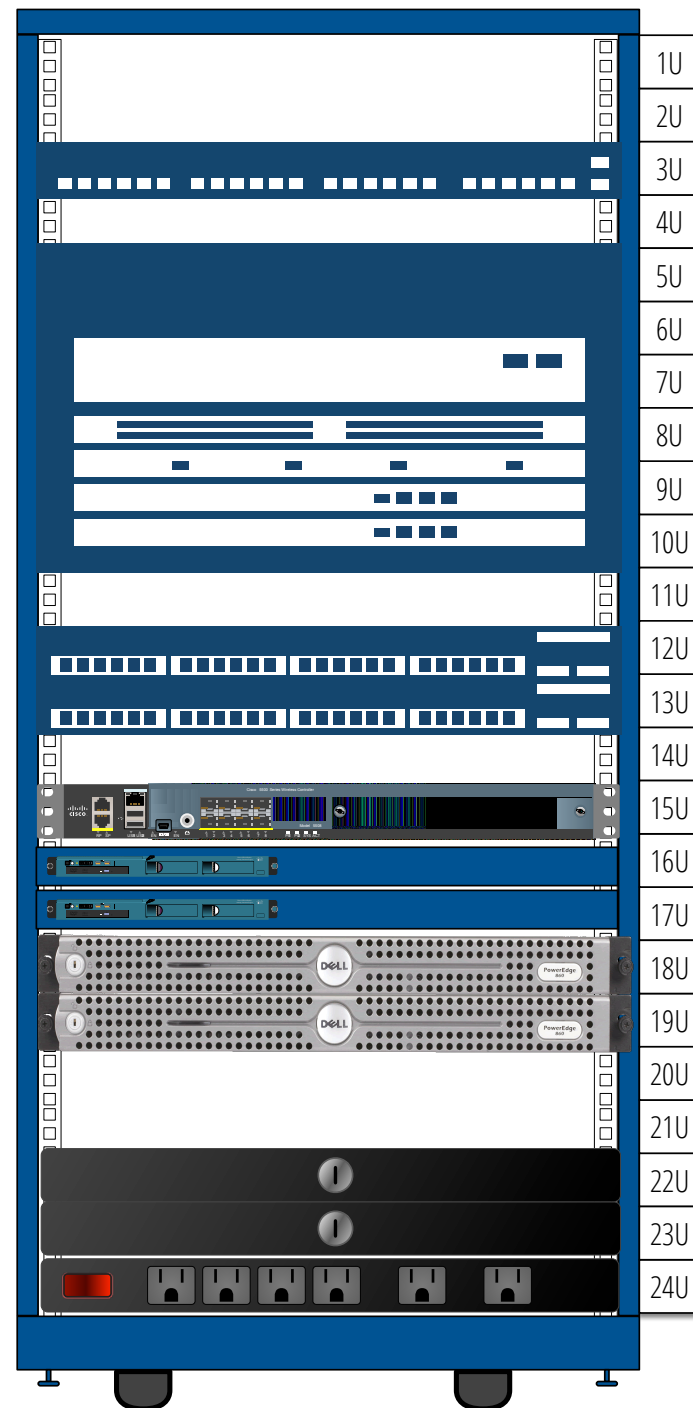
WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA

S.C.A. Rack



~90.000 € una tantum

Out Of Band EX 2200

~3000 € /anno

Router di Polo MX 240

~6000 utenti

TORing EX 4200

24 rack units

WLC 5500

4 kw

NAC Appliance

OpenStack Nodes

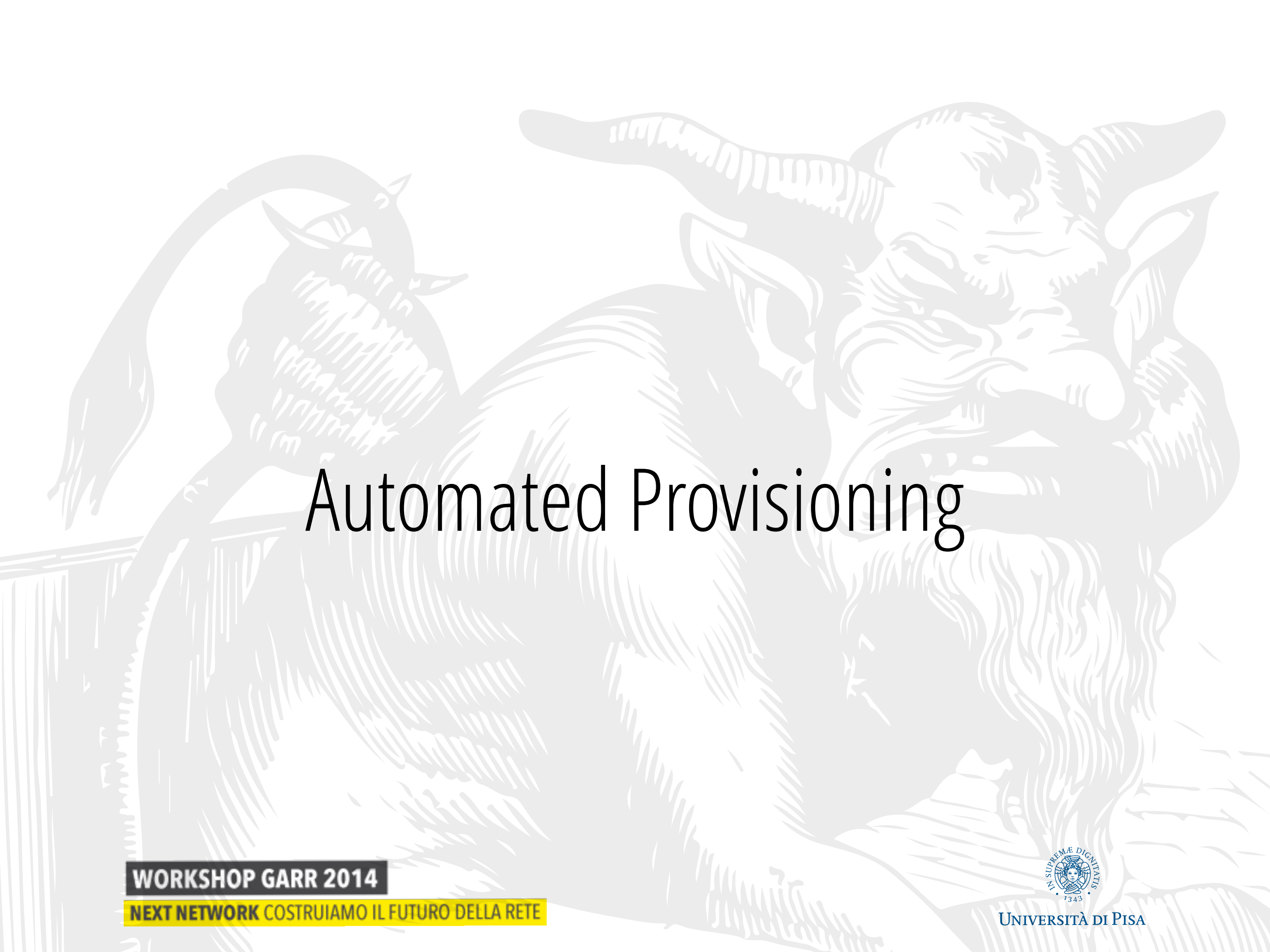
UPS Units

WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA



Automated Provisioning

WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA

Provisioning

Possiamo descrivere i servizi (DNS, DHCP, radius, etc) come delle applicazioni formate da due componenti: la configurazione del servizio che determina il comportamento dell'applicazione e il contesto di esecuzione in cui l'applicazione viene eseguita.

Il processo di provisioning si preoccupa di rendere disponibile le *applicazioni* agli amministratori, creando il contesto di esecuzione e applicando la configurazione prevista per quel particolare servizio.

Provisioning Model

- Robusto (comportamento ragionevole in situazioni impreviste)
- Processi asincroni
- Operazioni idempotenti

Provisioning Tools

- Versioning - GIT Repository (OpenSource)
- Virtualizzazione - OpenStack (OpenSource)
- Configuration Management I - Ansible (OpenSource)
- Configuration Management II - IPControl (Commerciale)

Virtualizzare

Perché

- Consolidamento Hardware
- Automazione

Come

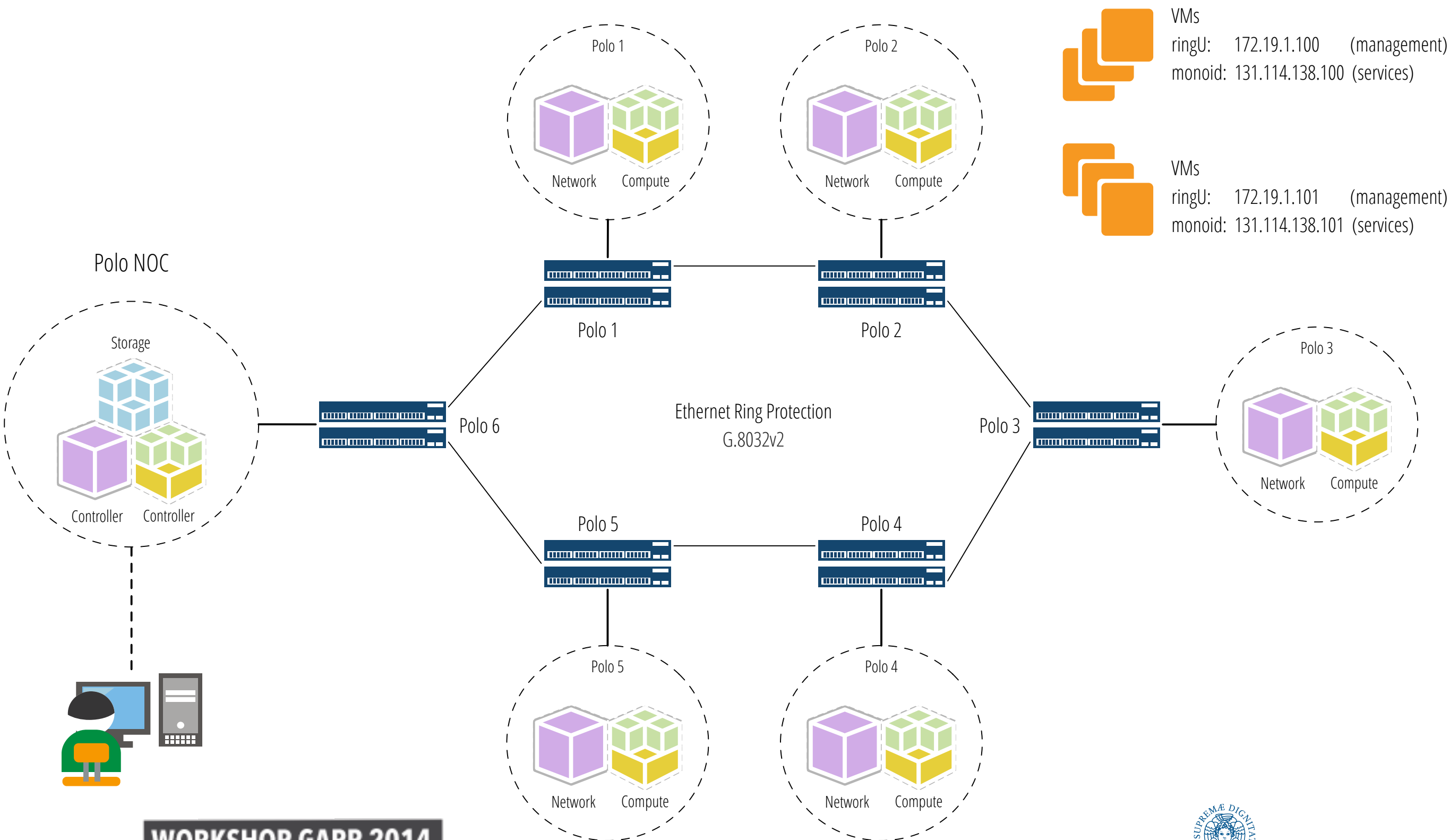
- Technology agnostic
- Multitenant
- Programmable (Api)
- Community based

Virtualizzare

- Debian wheezy
- Virtualizzazione KVM
- Openstack Icehouse



Architettura



WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA

Architettura

- Rete semplice ma centrale
- La virtualizzazione deve garantire la continuità di servizio
- Il contesto di esecuzione localizzato in qualunque nodo, si predilige il nodo locale.

Configuration Management I

- Semplice (YAML, no programming)
- Agentless (solo SSH)
- Una buona comunità di sviluppo
- Network oriented

Configuration Management I

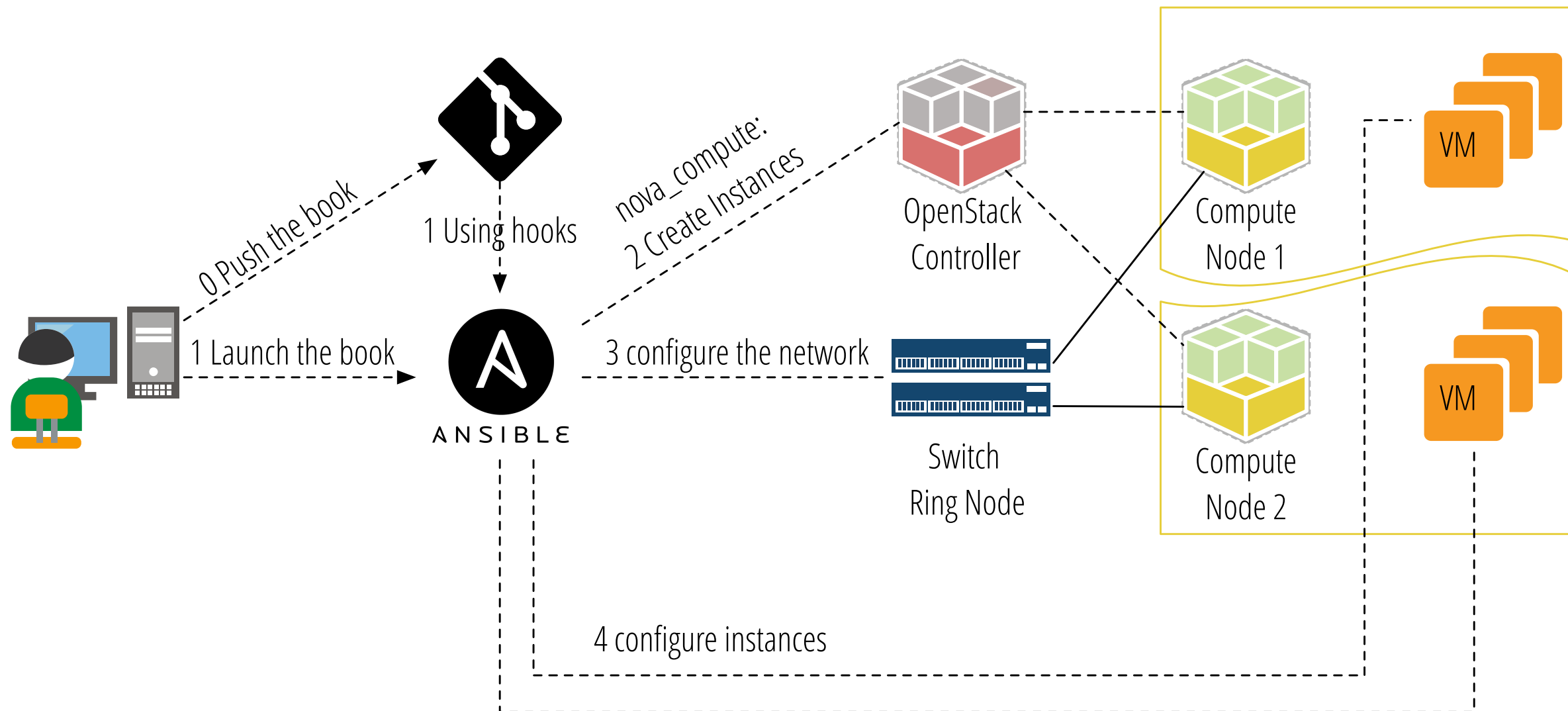
```
- name: create instance
nova_compute:
  auth_url: http://172.19.0.2:35357/v2.0
  state: present
  login_username: ansible
  login_password: XXXXX
  login_tenant_name: sca
  name: {{vm.hostname}}
  image_name: centos-6.5-x86_64
  key_name: admin
  availability_zone: {{vm.avZone}}
  config_drive: yes
  wait_for: 200
  flavor_id: 2
  nics:
    - net-id: f15427c2-2c2a-498b-b8eb-f9cd871ebe89
      v4-fixed-ip: {{vm.MonoidIP}}
    - net-id: 58761159-4f03-458b-9faf-8c452f99c2c3
      v4-fixed-ip: {{vm.RingUIP}}
  security_groups: ringU,default, {{vm.securityGroups}}
  files: [/etc/sysconfig/network-scripts/ifcfg-eth0: {{vm.eth0-srcPath}} ]
  meta:
    hostname: {{vm.hostname}}
    group: {{vm.groups}}
```



Cosa fa Ansible ?

- Configura apparato di accesso dei nodi di computing
- Crea le istanze virtuali utilizzando OpenStack API
- Configura le istanze create (network, syslog, nagios, etc)

Provisioning Workflow



Configuration Management II

- Gestione dello spazio di indirizzamento IPv4 e IPv6
- Configurazioni DNS e DHCP integrata con IPAM
- Logica multi tenant per risorse e funzioni
- Conforme al modello di provisioning e al software utilizzato (ISC DHCP, BIND9, etc)
- Deploy delle configurazioni dei servizi
- Web user interface

Configuration Management II

Prodotto D.D.I Commerciale di BT

The screenshot displays the IPControl web interface. The top navigation bar includes the IPControl logo, a home icon, and tabs for MANAGEMENT, REPORTS, and TOOLS. Below the navigation bar, there are sections for Tasks and Alerts, a search bar, and a tree view of the network hierarchy. The tree view shows a hierarchy starting with UniPi, branching into ict and sid, which further branches into Polo-1, Polo-2, and Polo-3. Each Polo entry has sub-entries for Clients, Devices, Management, and Servers. Polo-2 also includes Auth and NoAuth. A dropdown menu is open under the MANAGEMENT tab, showing three columns of options: IPAM, DNS, and DHCP. The IPAM column includes options like Container View, Subnet/Block View, Pending Approvals, Discovery, Address Space Reclaim, Container Maintenance, Network Elements/Devices, and Server Pairs. The DNS column includes Servers/Services, Configuration/Deployment, Domains, Galaxies, Log Channels, Server Templates, Domain Types, Address Match Lists, Update Policies, Transaction Keys, Option Vendor Dictionary, Option Master Dictionary, and DNS Software Products. The DHCP column includes Servers/Services, Utilization View, Network Links, Configuration/Deployment, Policy Sets, Option Sets, Client Classes, Option Vendor Dictionary, Option Master Dictionary, and DHCP Software Products.

IPAM	DNS	DHCP
Container View	Servers/Services	Servers/Services
Subnet/Block View	Configuration/Deployment	Utilization View
Pending Approvals	Domains	Network Links
Discovery	Galaxies	Configuration/Deployment
Address Space Reclaim	Log Channels	Policy Sets
Container Maintenance	Server Templates	Option Sets
Network Elements/Devices	Domain Types	Client Classes
Server Pairs	Address Match Lists	Option Vendor Dictionary
	Update Policies	Option Master Dictionary
	Transaction Keys	DHCP Software Products
	Option Vendor Dictionary	
	Option Master Dictionary	
	DNS Software Products	

WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA

Services

Modello Active/Active

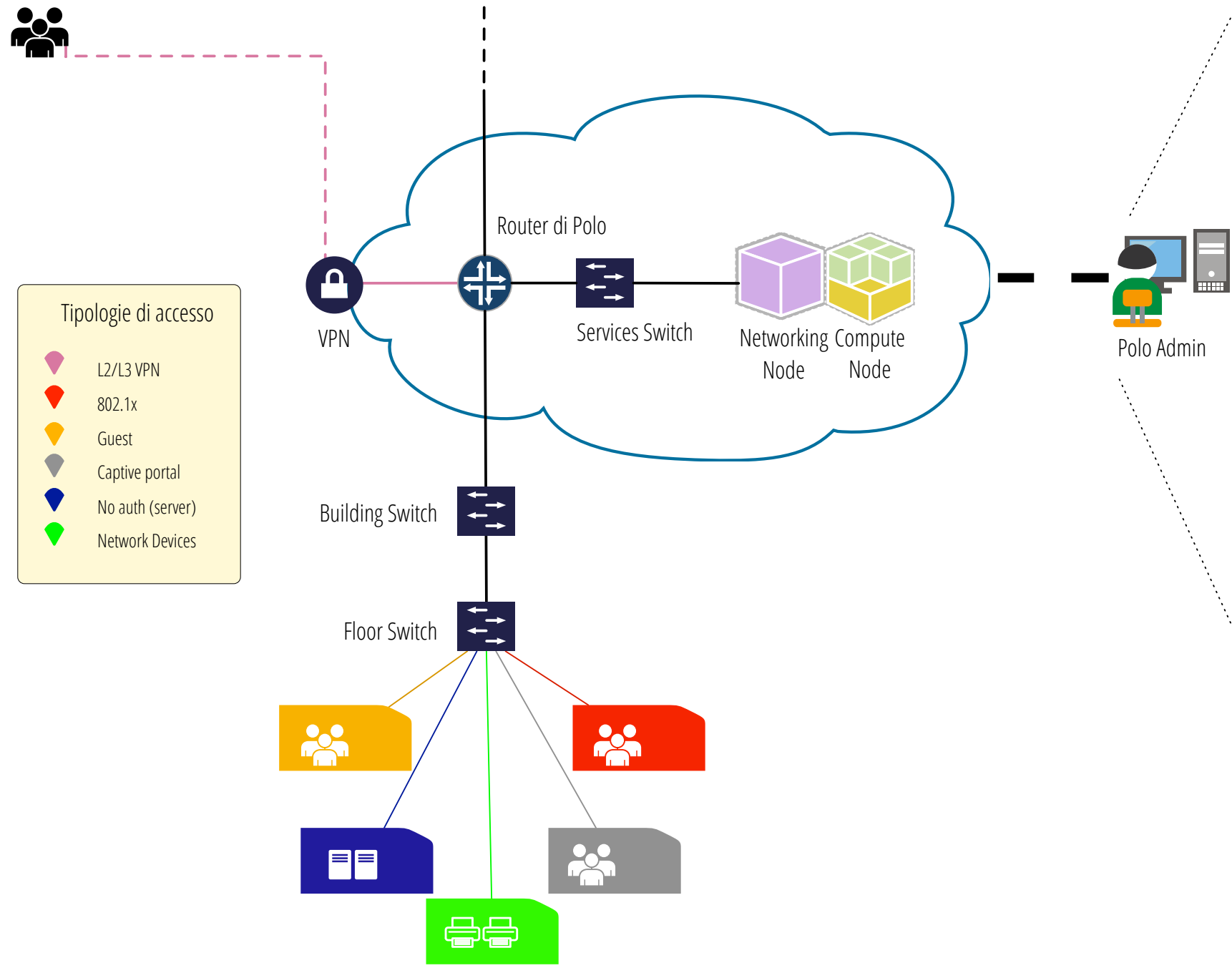
Per ogni polo:

- n.2 Ldap Replicas
- n.2 Radius
- n.2 DHCP (internal failover)
- n.2 DNS Cache
- n.2 LOG Rounting

Admin Side

- Interfaccia web D.D.I. da cui gestire le configurazioni ed effettuare il deploy
- Interfaccia OpenStack per la gestione delle regole di firewall e per riavviare o ricreare le istanze
- Accesso in console alle istanze virtuali ed apparati
- Strumenti di monitoring

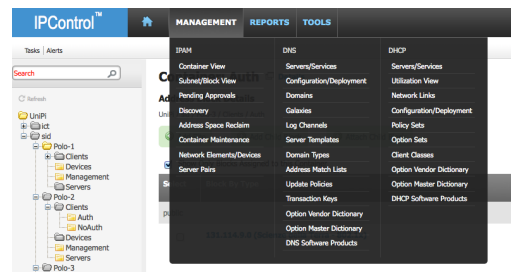
Admin side



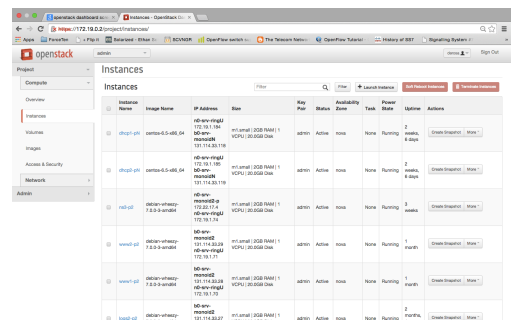
Tipologie di accesso

- L2/L3 VPN
- 802.1x
- Guest
- Captive portal
- No auth (server)
- Network Devices

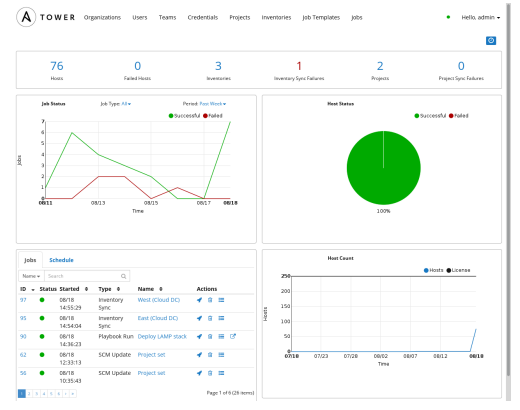
IPControl Dashboard



OpenStack Dashboard



Ansible Dashboard





Criticità e sviluppo

WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA

Criticità

- Single Point of Failure (Router)
- Formazione del personale
- Complessità

Miglioramenti

- Automazione del livello di distribuzione (SDN)
- Automazione del processo di installazione di Openstack
- Utilizzo dei container (Dockers) al posto di KVM
- Meccanismi di High Availability per i servizi



Fine

WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA



Domande ?

WORKSHOP GARR 2014

NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE



UNIVERSITÀ DI PISA