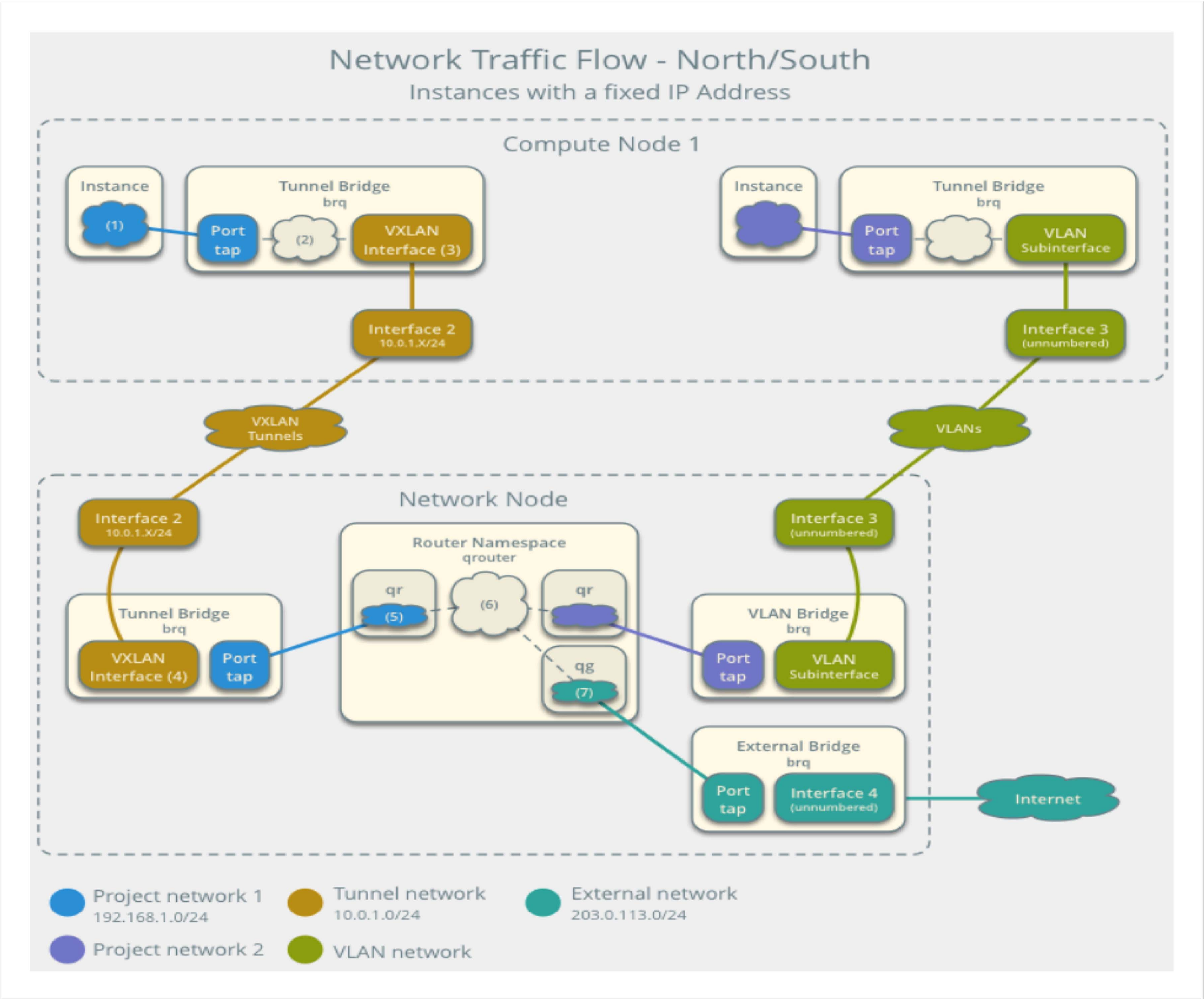
CERIAS

The Center for Education and Research in Information Assurance and Security

Secure Cloud Infrastructure

Nichole McFarland, Justin Salyer, Andrew Thomas, and Connie Justice

Making the cloud more secure



Security Node

•Kali Linux – using primarily for forensic tools, but Kali could also be used to detect any vulnerabilities before an attack could be possible, by using tools to discover any discrepancies.

•Sans Investigative Forensic Toolkit (SIFT) – tools to respond to incidents and digital forensic tools to analyze intrusions in a variety of applications.

•Security Onion

- Suricata – Network IDS, IPS, and Network
  Security Monitoring Engine. Sending logs from the network to the syslog server and then storing them on the security node for further analysis.
- SaltStack – Updating rules universally.
- Bro - network analysis platform, it is very flexible and can used forensically to log any inconsistencies in the network. It includes analyzers to decipher log files from the
  acceptable to the potential disaster.

Controller Node

✧ Database handling,

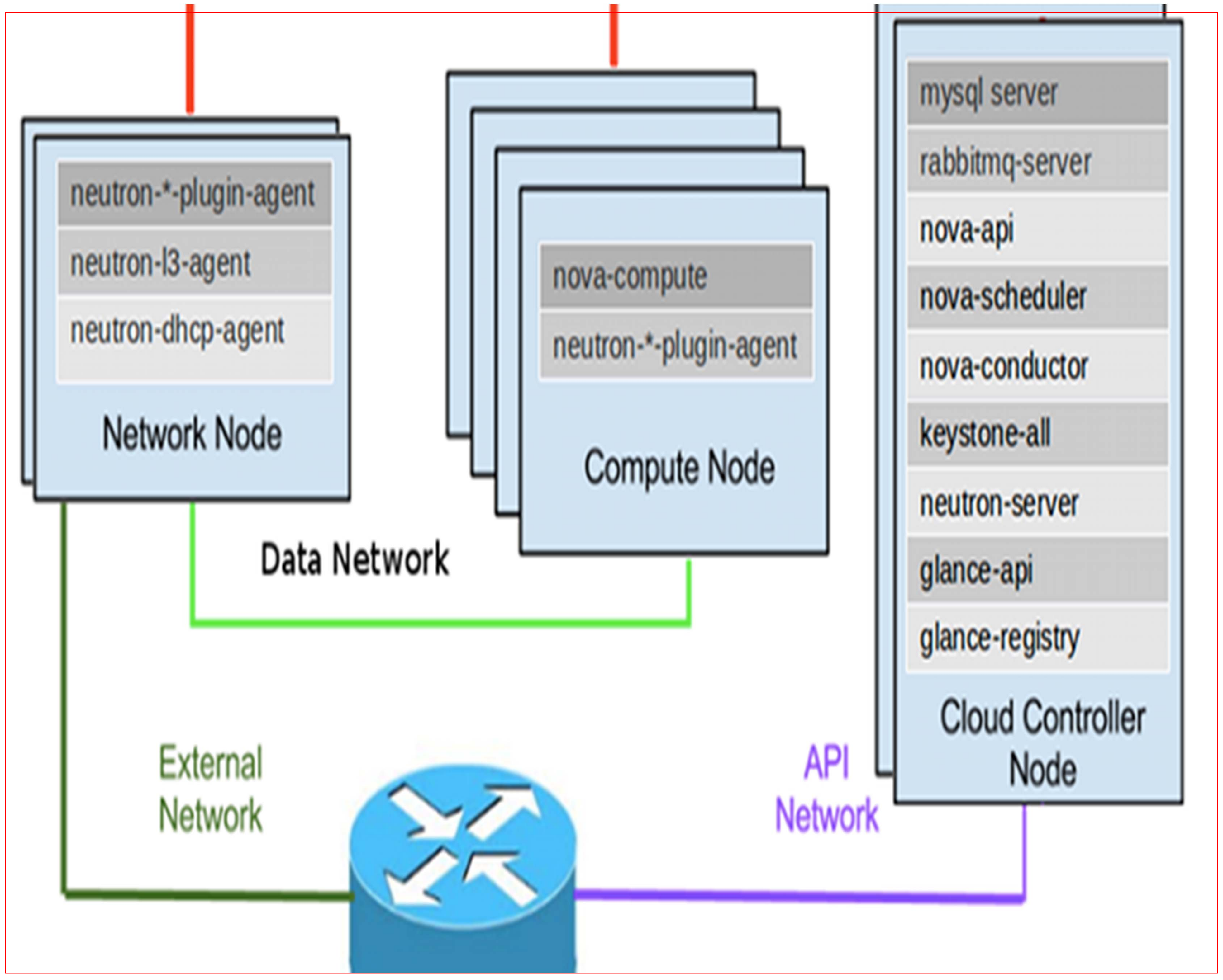
- ✧ Keystone – Identity Service
- ✧ Glance – Imaging Service
- ✧ Nova – Compute Service
- ✧ Neutron – Networking Service

Compute Node

- ✧ Open vSwitch
- ✧ KVM Hypervisor
- ✧ Compute

Network Node

- ✧ Networking ML2 Plugin
- ✧ Open vSwitch
- ✧ Network L3 Agent
- ✧ Networking DHCP Agent



Problem:

K – 12 Schools have a lack of IT resources, thus creating a great security weakness. Additionally there is great pressure on school systems to provide access to their networks.