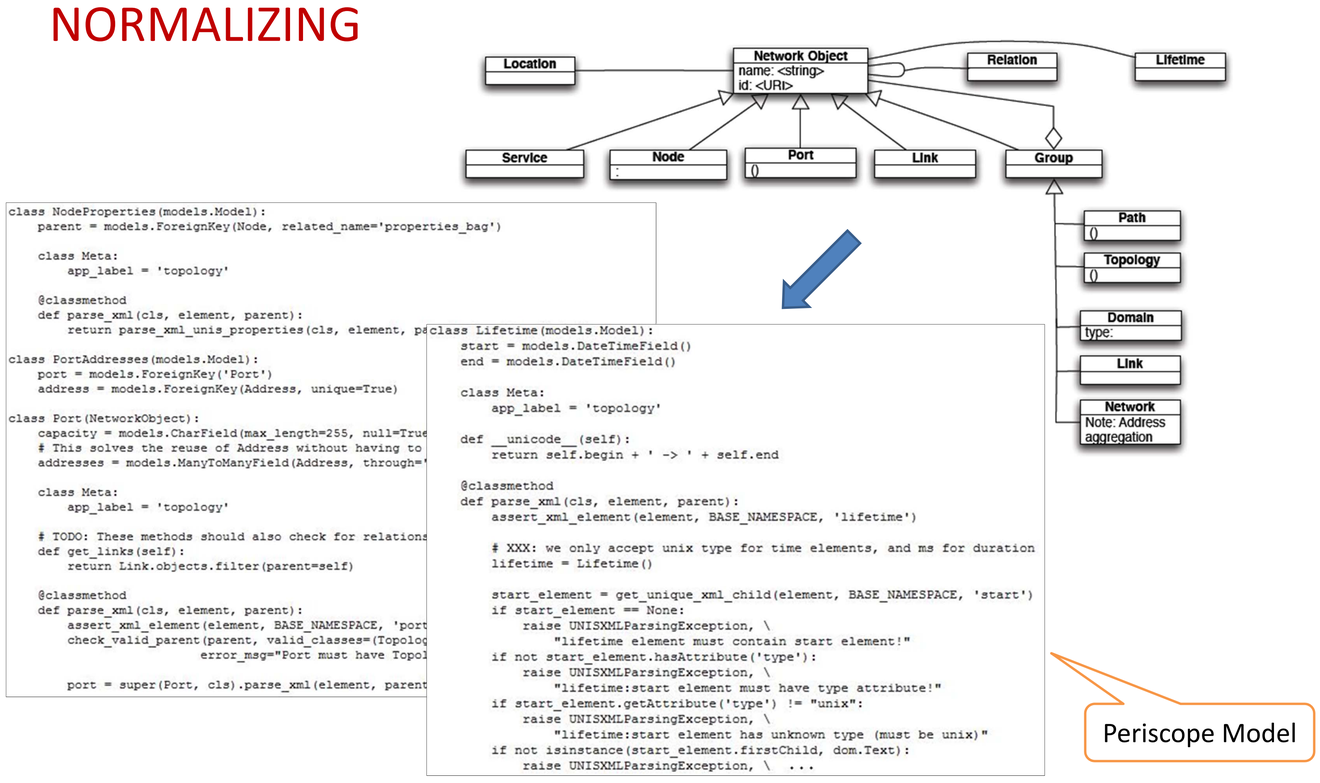
Periscope

Ahmed El-Hassany, Ezra Kissel, Guilherme Fernandes, Omer Arap, Priscilla Moraes, Martin Swany
Department of Computer and Information Sciences, University of Delaware

Periscope is an initiatiave that provides performance data to the user in a friendly and fast manner. Topology data is stored and processed based on UNIS (Unified Network Information Services) Topology Schema - used by perfSONAR, IDC, OSCARS, AutoBAHN and Phoebus. Domain-specific network topologies are represented in UNIS and visualized in an interactive web-interface. Collected measurement data is standardized and cached for analysis and display. The initial Periscope backend has been developed in Python and makes use of the Django MVC framework.

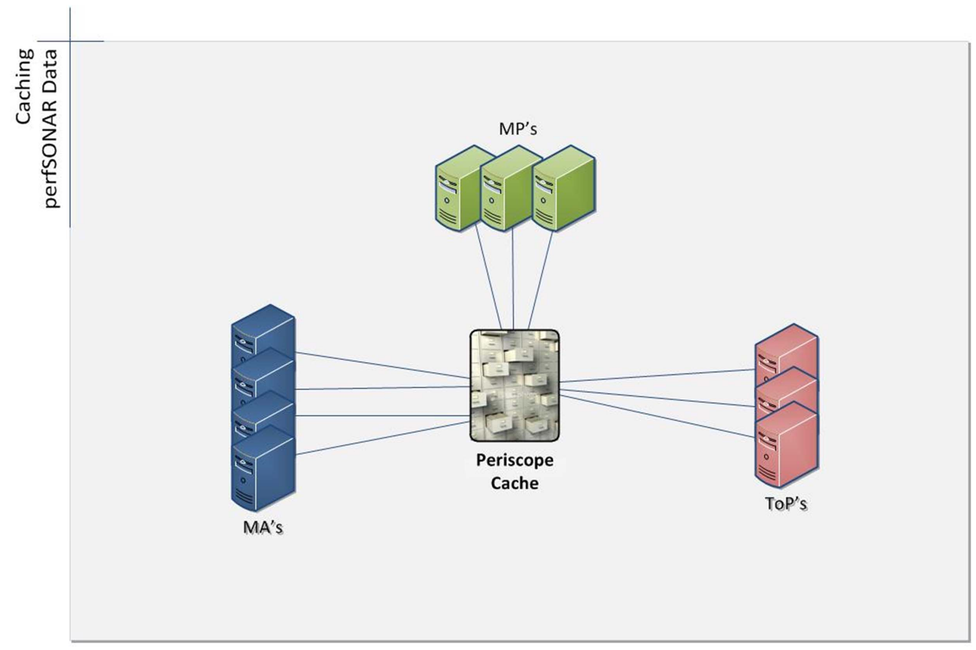
NORMALIZING



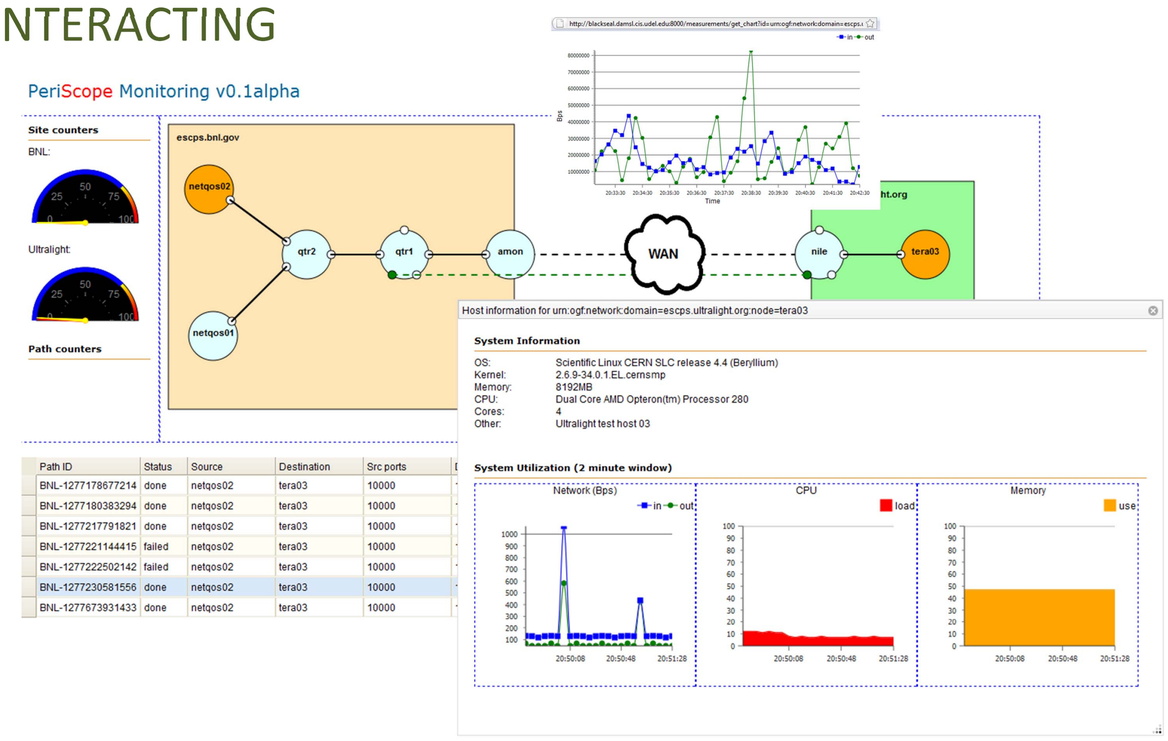
- Schemas based on NML-WG (Network Mark-up Language Working Group) definitions are used to specify XML messages format to interact with perfSONAR services.
- The Django MVC is used to represent UNIS and measurement data within Periscope.
- Periscope may also translate general network models to UNIS.
- Topological elements, from links and ports to domains and networks, are cleanly modeled and mapped to measurement data.

CACHING

- Measurement and Topology data is currently distributed throughout many repositories across perfSONAR domains
- Queries can take a considerable time to return results.
- Obtaining data faster is the main motivation to the caching functionality of Periscope.
- Measurement data from Measurement Archives (MA's) and Measurement Points (MP's), and network data from the Topology Service (ToP's) are cached within Periscope.
- All cached information is available and accessed through a web interface that provides individual link utilization information to the user in a friendly and fast way.



INTERACTING



- Front-end visualized the topology based on cached data acquired from the Topology Service.
- The user can click on a port or link to obtain tooltip information and access updating performance charts.
- Measurement data cached from MA's or MP's – related to the network entity – are shown within a dynamic monitoring pane.
- Information about possible anomalies occurring in the entity are accessed based on an anomaly detection module that will be available.

Poster: Priscilla Moraes, Martin Swany
pmoraes@udel.edu
swany@cis.udel.edu