DRIfT
Dynamically Rendered Infrastructure Topology

Joseph Maestas, Jimmie Akins

Advanced Network Systems and Technology Development

**Sandia National Laboratories**
Albuquerque, New Mexico
Email address: jhmaest@sandia.gov

LOCKHEED MARTIN

Sandia National Laboratories

What is DRIfT?

DRIfT is a software tool whose primary purpose is to render network diagrams dynamically for rapidly changing networks and to provide an interface from which additional information can be obtained and visualized.
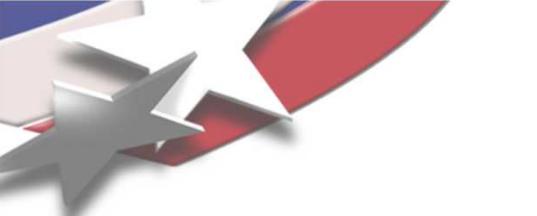
Overview

- **State the problem, the business need, and the solution.**
- **DRIFT Overview.**
- **Future Directions.**
- **Demonstration.**

LOCKHEED MARTIN

Sandia
National
Laboratories
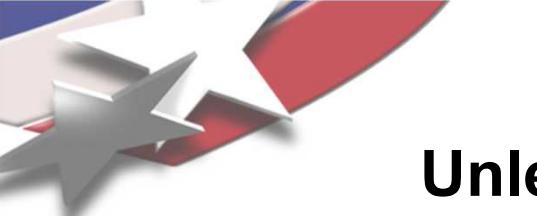
Problem Statement

## Unless a Network Diagram is used for Many Purposes, it's Return is Negligible

- **Accurate network diagrams are needed for many IT disciplines.**

- **It is a recurring need with cumulative costs and little payback.**

- **Typically created and maintained by network engineers.**

- **Data scraping consumes time and is prone to error.**

- **Most data needed for creating a diagram is available only from a privileged account…not just anybody can do it!**

LOCKHEED MARTIN

Sandia National Laboratories

Business Need

Sandia's Large, Rapidly Changing Environment Accentuates Manual Error-Prone Processes

- Switched campus environment at California and New Mexico.

- Supports three security environments.

- Virtual Private Networks interconnect nearly 30 remote sites.

- New Mexico Campus: 1022 network devices, 1014 links, over 1M lines of command code, 30,000 hosts.

- Three-tier architecture.

- 30% of the population moves annually.

- Service provisioning is performed manually via the command line interface.

LOCKHEED MARTIN

Sandia National Laboratories
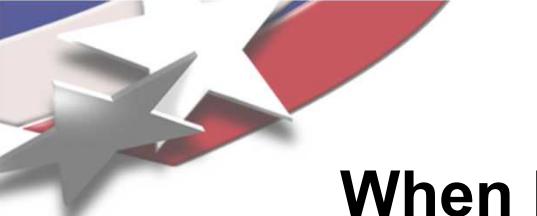
Business Need

When Dealing with Large Networks and Declining Budgets, We Need to Work More Effectively

- Manual creation and maintenance of network diagrams is costly.
- Network engineers spend 70% of their time data scraping.
- Why not have this data available in a versatile form ready to use?
- Why not create a detailed diagram on the fly and use a few key strokes to focus on any portion of the network?
- Why not use this diagram as a way to obtain additional details on the network or on the host systems that connect to it?
- Why not use this diagram to monitor the health of your network?

LOCKHEED MARTIN

Sandia National Laboratories

Solution

Leverage the Rich Data Repository in Your VNE Server to Create Multi-purpose Interactive Network Diagrams

- **Sandia uses OPNET's Virtual Network Environment Server to create a high-fidelity, continuously valid, integrated data model of our networks.**

- **The superior ability of the VNE Server to provide continuously up to date network data allows DRIfT to provide continuously up to date diagrams.**

LOCKHEED MARTIN

Sandia National Laboratories

Conceptual Model of DRIfT
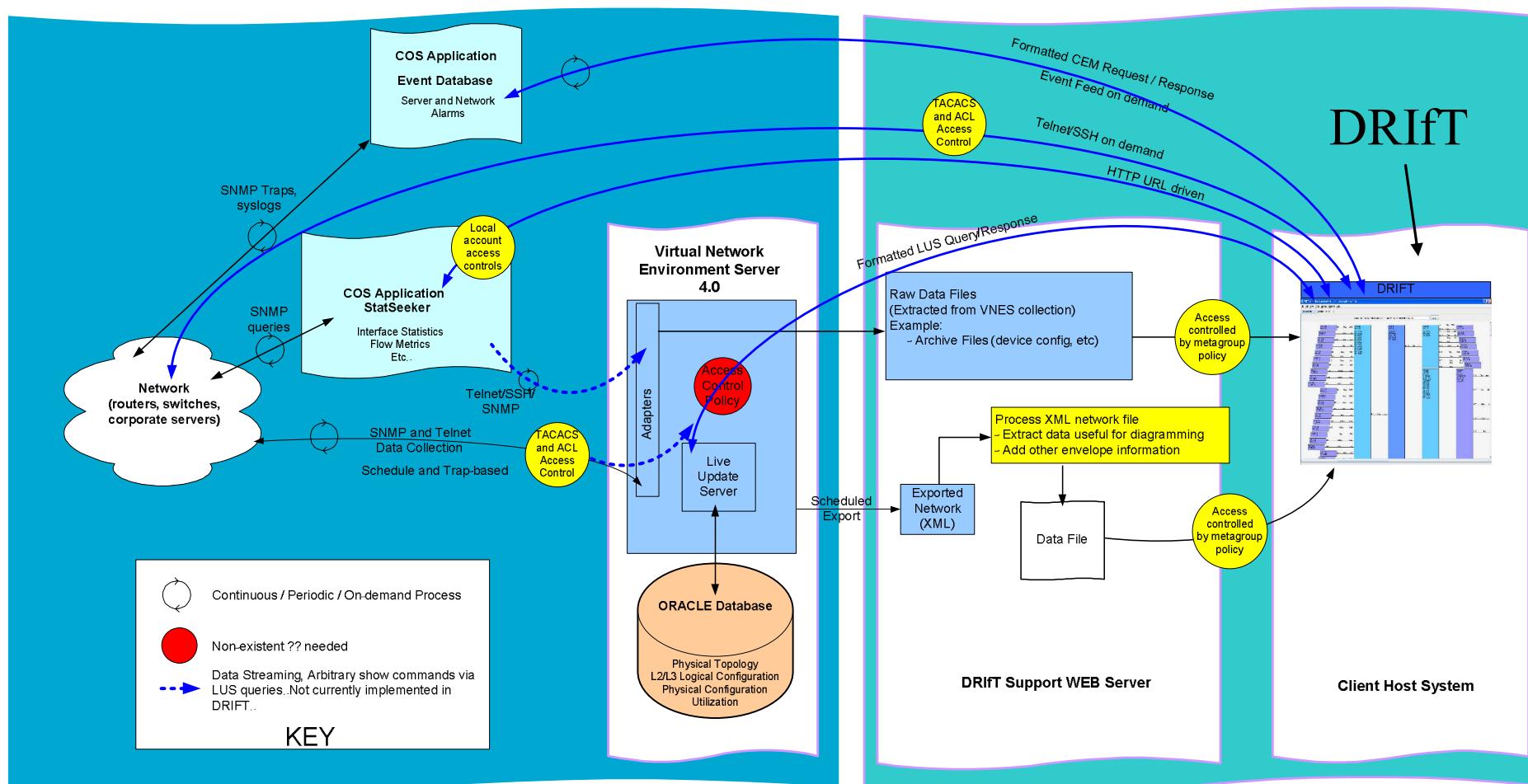
Some VNE Server 4.0 Tweaks Were Necessary to Obtain Correct Routing Table Information in the Exported Network XML File

- **Problem: Cisco route table entries for directly connected networks were ignored by the VNE route table parser.**
- **Solution: Add VLSM information to Cisco route tables after collection, but prior to import.**
  - **Example: Original**

    198.206.220.0/29 is subnetted, 1 subnets

    C   198.206.220.32 is directly connected, Vlan1000
  - **Example: Modified**

    198.206.220.0/29 is subnetted, 1 subnets

    C   198.206.220.32/29 is directly connected, Vlan1000
- **Translate Foundry routing tables to Cisco format. (Corrected in VNE 6.0 ?)**
- **Enable export of routing tables to the network export XML file**
  - **Example:**

    Modify the ExportAdapter.res file: Change "IP_ROUTING_TABLE" value to "on". Default value is "off"

LOCKHEED MARTIN

Sandia National Laboratories

VNE Server is the Core of Our Data Repository Source, but an Ancillary Support Server Improves Performance.

- **DRIfT 3: Windows Only**
  - * Repository for device configuration archive files.
  - Repository for input data file.

- **LUS_DRIfT 3: Windows Only**
  - No repository is needed. Diagram built entirely using LUS. However, device configuration archive file retrieval is not implemented in DRIfT.

- **DRIfT4: Unix/Windows**
  - Performs SQL query to VNE DB for device access methods
  - * WEB server
    - Repository for device configuration archive files.
    - Repository for input data files.

- **All versions**
  - DRIfT jar files maintained within repository. Is copied into client upon DRIfT startup.
  - Java application derives DRIfT input data file from the VNE Server network export file.

- *** User provided**

LOCKHEED MARTIN

Sandia National Laboratories
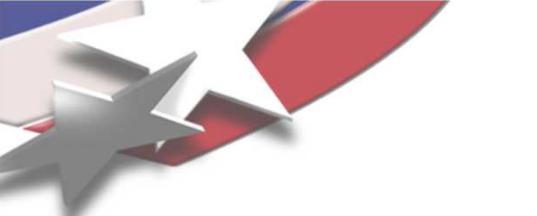
Feature Summary

- **Flat layout for three-tier networks.**
- **Spring layout for arbitrary networks and tab views.**
- **Business Service View Creation.**
- **Situation Awareness.**
- **Root event identification.**
- **Visualize link utilization from Statseeker in near real-time.**
- **Visualize network and server events.**
- **Search device archive configuration files by substring or Regex.**
- **Device locator (SNL specific).**
- **N-way critical path, N-way shortest path.**
- **Version aware.**
- **Network dependencies (what will be affected when this device fails).**
- **Node neighbors.**

LOCKHEED MARTIN

Sandia
National
Laboratories
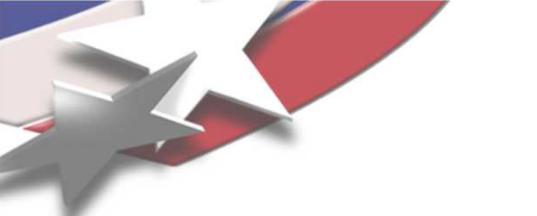
Future Directions

- **Code review: halt feature development, review the DRIfT code to minimize the footprint.**

- **Restructure DRIfT as a server side application.**

- **Leverage the LUS Capabilities**
  - **Understand LUS vulnerabilities.**
  - **Configure multiple VNE accounts for device login.**
  - **Configuration files retrieval.**
  - **Arbitrary show commands and output streaming to support assisted troubleshooting.**

LOCKHEED MARTIN

Sandia National Laboratories
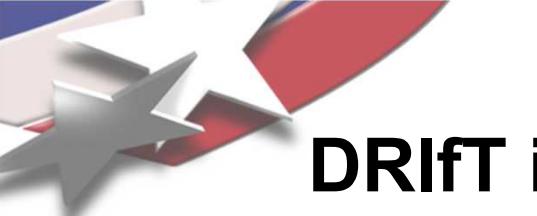
DRIfT is Licensed for Government Use. To Request the Software:

- **Properly registered US Government agencies can use the software at no charge.**
- **Software requests must include:**
  - **Name of contact, name of agency, email address**
  - **Send software requests to: llmcnie@sandia.gov**
- **Requester receives a Participant Data Sheet, completes it.**
- **Requester sends the Participant Data Sheet to Sandia Licensing via email: Nathan Golden (nlgolde@sandia.gov) or Glenn Baird (gtbaird@sandia.gov)**

DRIfT is Licensed for Government Use. The Agreement:

- **Licensing sends the requester an agreement for signature. The agreement in this case, is a Government Use Notice, as this software may be distributed only to Government users.**

- **When the agreement is returned to Licensing, I am notified that the software may be distributed.**

LOCKHEED MARTIN

Sandia National Laboratories
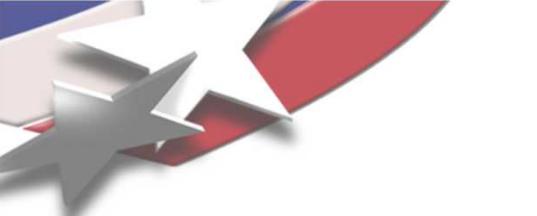
Conclusions

- **The superior ability of the VNE Server to provide continuously up to date network data allows DRIfT to provide continuously up to date diagrams.**

- **By visualizing the VNE network data, DRIfT provides an ideal vehicle for validating the documented topology against the actual topology of the network.**

- **The network data in the VNE Server is useful for many IT disciplines, but proper need to know policies must be applied. An ancillary WEB server helps to apply the policies as needed, but necessitates data duplication.**

- **DRIfT diagrams can be manipulated many different ways with only a few key strokes which translates to lower documentation costs by eliminating data scraping.**

- **DRIfT creates diagrams that are multipurpose including situation awareness, root event analysis, business service view creation, dynamic host mapping and identifying their critical network dependencies, in focus network views of arbitrary network segments, etc.**

LOCKHEED MARTIN

Sandia National Laboratories
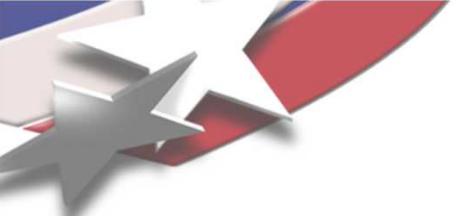
Demonstration

Flat Layout View

- **For three-tier network architectures.**
- **Dynamic object size and map size.**
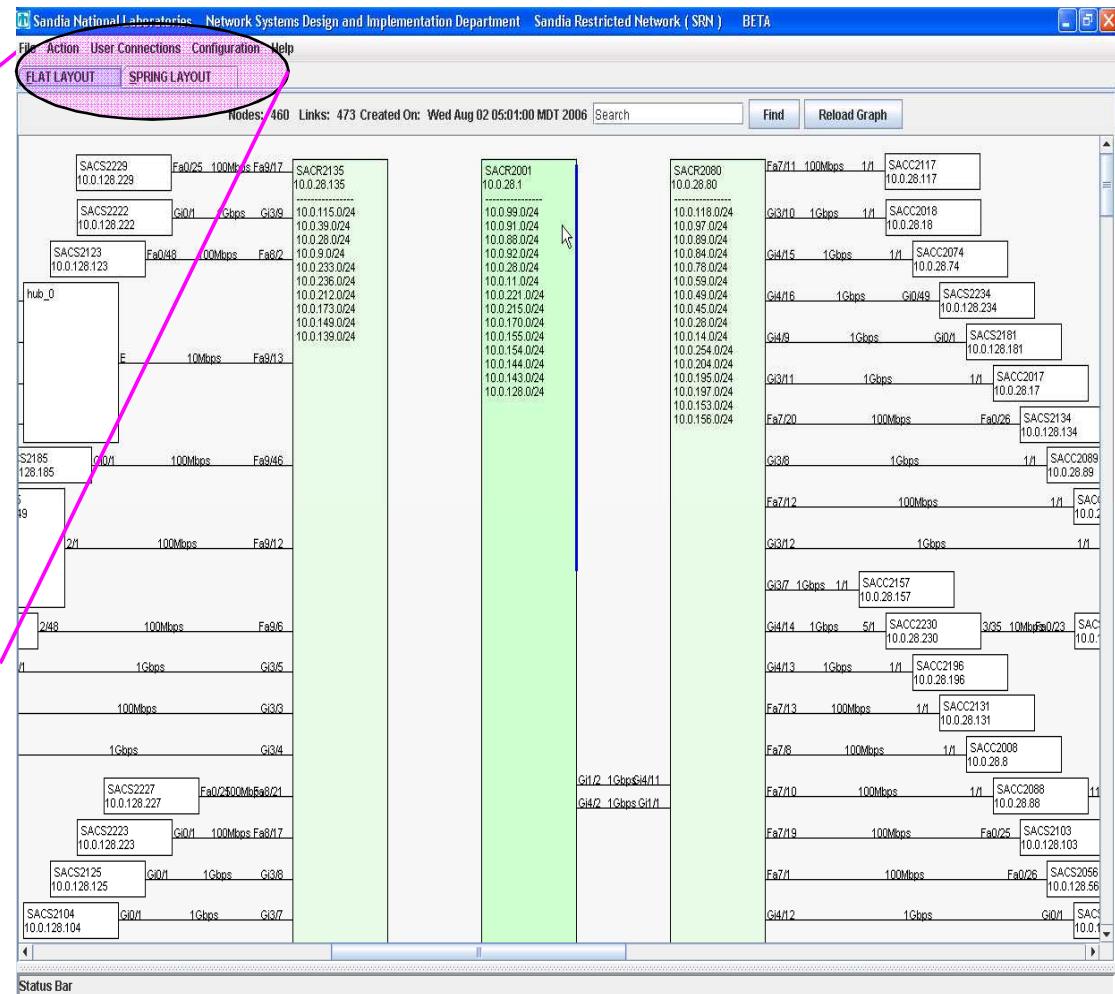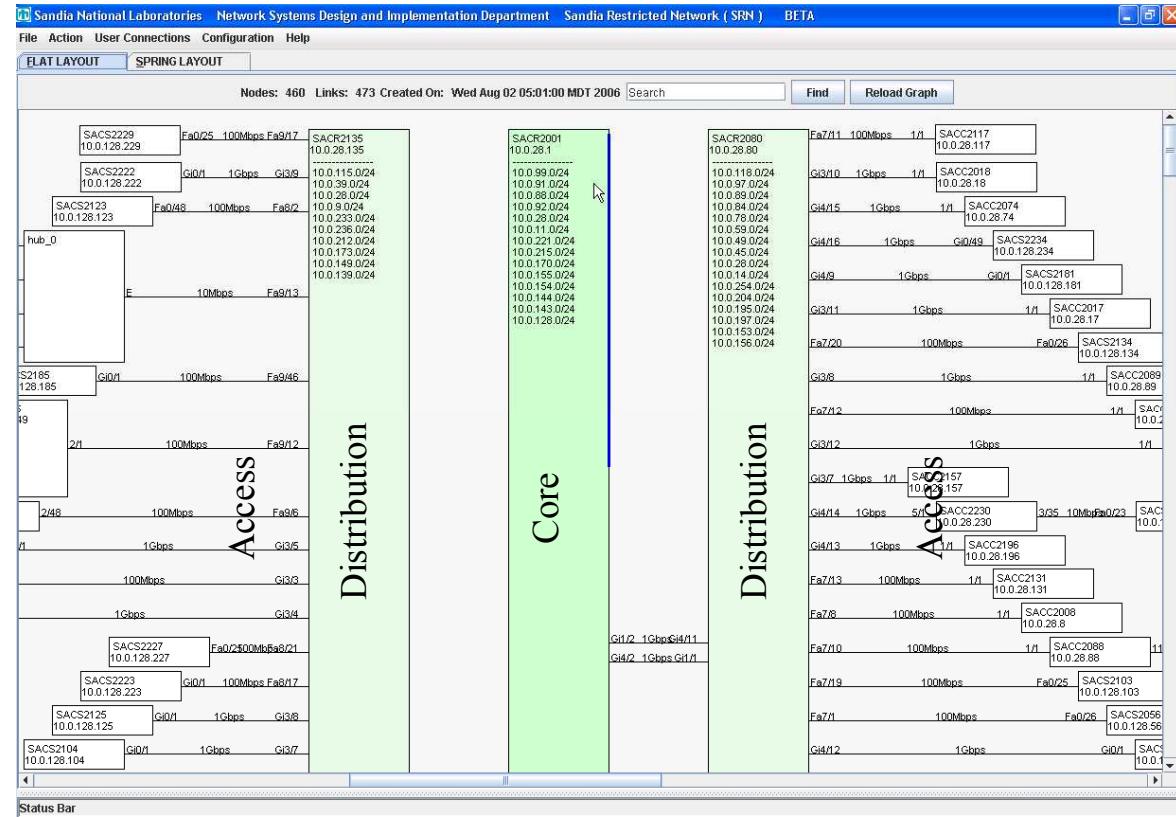- **Renders a 500 node network in approximately 5 seconds.**

Flat Layout View – Visualize Important Network Details

- **Node count. Link Count. Creation date.**
- **Substring search.**
- **Quickly identify functional layer (core, distribution, access).**
- **Node name and IP address.**
- **Directly connected networks (route points).**
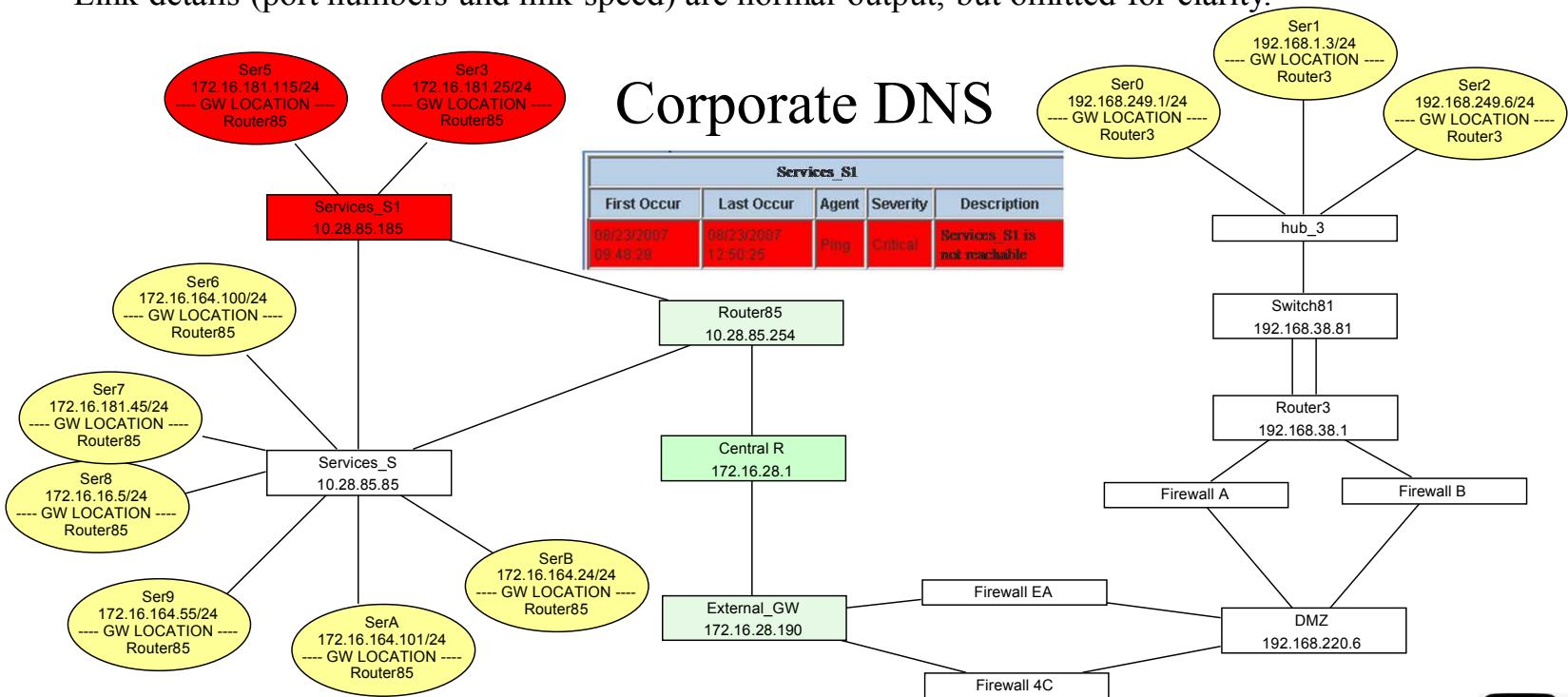- **Link labels.**
- **Link speed.**

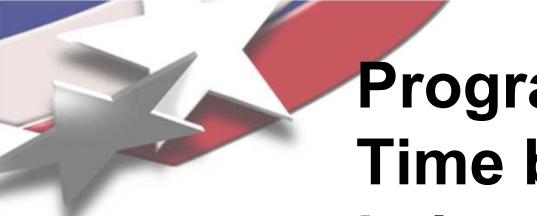# Spring Layout – Visualize Arbitrary Network

- **For an arbitrary network architecture.**
- **Uses a system of springs and magnetic forces. Converges when the total energy in the system is minimized.**
- **Convergence time is several minutes for 500 nodes.**
- **Supports same features as flat layout.**

LOCKHEED MARTIN

Sandia National Laboratories
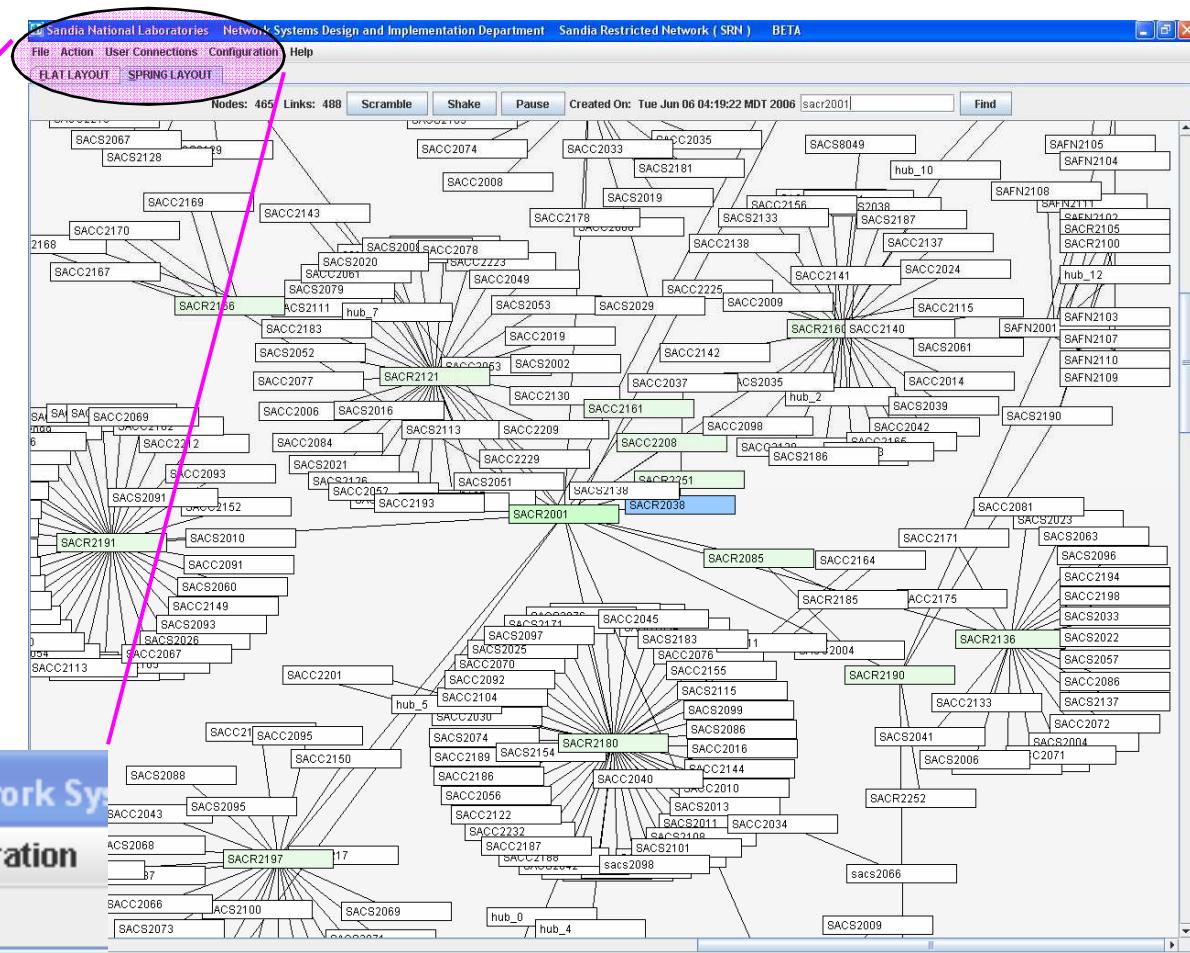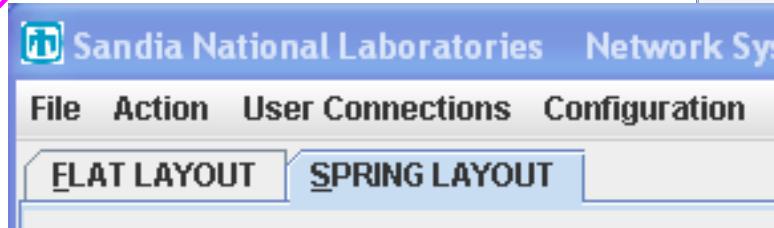
# Business Service Views Help Isolate Faults During Service Outages

- A service view represent the critical elements that go into supporting a service.

- At Sandia, many services are monitored at the application layer via synthetic transactions as well as through SNMP queries, pings and by monitoring system syslogs and traps.

- Eliminates laborious data scraping via the CLI.

- Link details (port numbers and link speed) are normal output, but omitted for clarity.

Corporate DNS

Ser5
172.16.181.115/24
---- GW LOCATION ----
Router85

Ser3
172.16.181.25/24
---- GW LOCATION ----
Router85

Services_S1
10.28.85.185

Ser6
172.16.164.100/24
---- GW LOCATION ----
Router85

Ser7
172.16.181.45/24
---- GW LOCATION ----
Router85

Ser8
172.16.16.5/24
---- GW LOCATION ----
Router85

Services_S
10.28.85.85

Ser9
172.16.164.55/24
---- GW LOCATION ----
Router85

SerA
172.16.164.101/24
---- GW LOCATION ----
Router85

SerB
172.16.164.24/24
---- GW LOCATION ----
Router85

Router85
10.28.85.254

Central R
172.16.28.1

External_GW
172.16.28.190

Ser1
192.168.1.3/24
---- GW LOCATION ----
Router3

Ser0
192.168.249.1/24
---- GW LOCATION ----
Router3

Ser2
192.168.249.6/24
---- GW LOCATION ----
Router3

hub_3

Switch81
192.168.38.81

Router3
192.168.38.1

Firewall A

Firewall B

Firewall EA

DMZ
192.168.220.6

Firewall 4C

Services_S1				
First Occur	Last Occur	Agent	Severity	Description
08/23/2007 09:48:29	08/23/2007 12:50:25	Ping	Critical	Services_S1 is not reachable

Sandia National Laboratories

Programmatic Creation of Service Views Saves Time by Automating What Once Used to Be a Laborious Error-prone Process

- **Service Views are created via the GUI or via asynchronous requests directed to DRIfT.**
  - **-n** *<comma separated host list>*
  - **-p 8767 -s** *<name or IP of DRIFT Server>*
  - **Example: Obtain the business service view with hosts h1 and h2**
    - **java -jar Client.jar -s drift-server -p 8567 -n h1, h2**
  - **DRIfT responds with the topology that includes:**
    - **segment by segment XML description of the path(s) between the host(s) and their default gateways.**
    - **segment by segment XML description of the path(s) between the gateways and core router.**

LOCKHEED MARTIN

Sandia National Laboratories
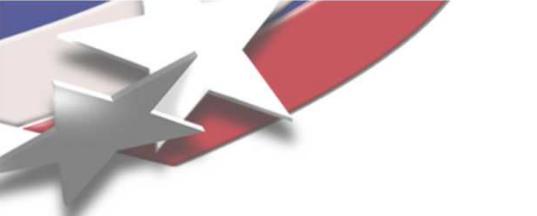
Node Neighbors

- **Display directly connected nodes only**
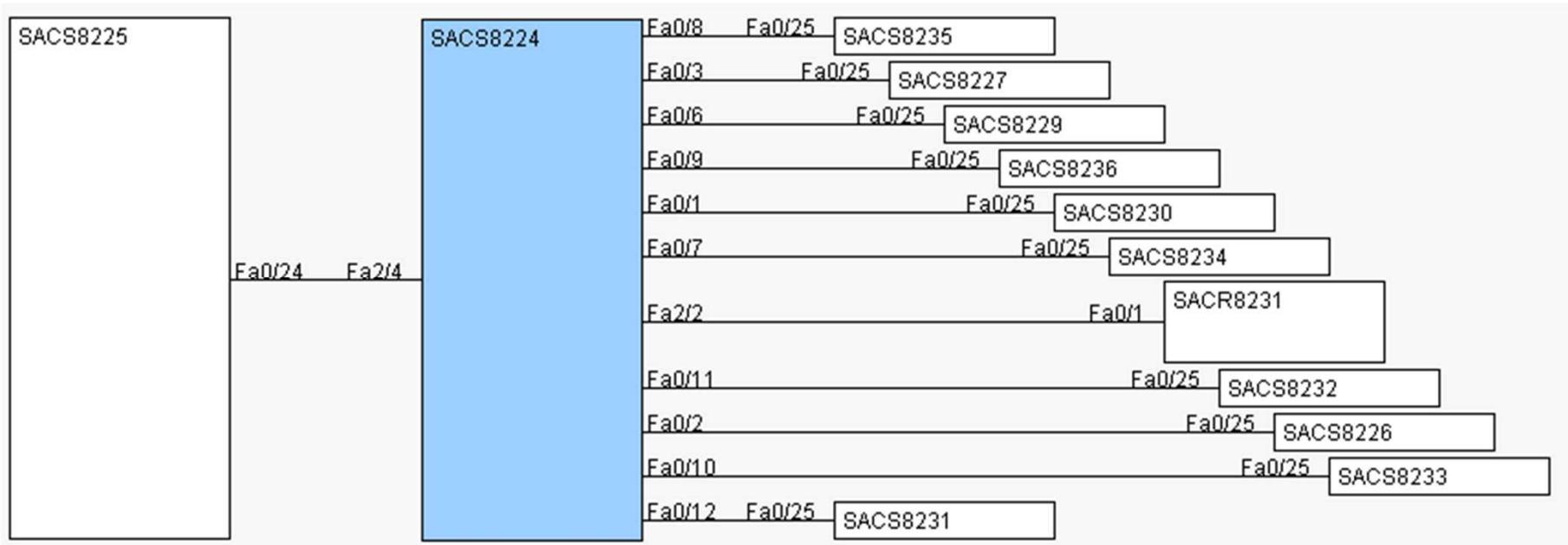
Network Dependencies

- **Network dependencies include all neighbor devices plus all connected devices downstream (away from the core) from the selected node.**

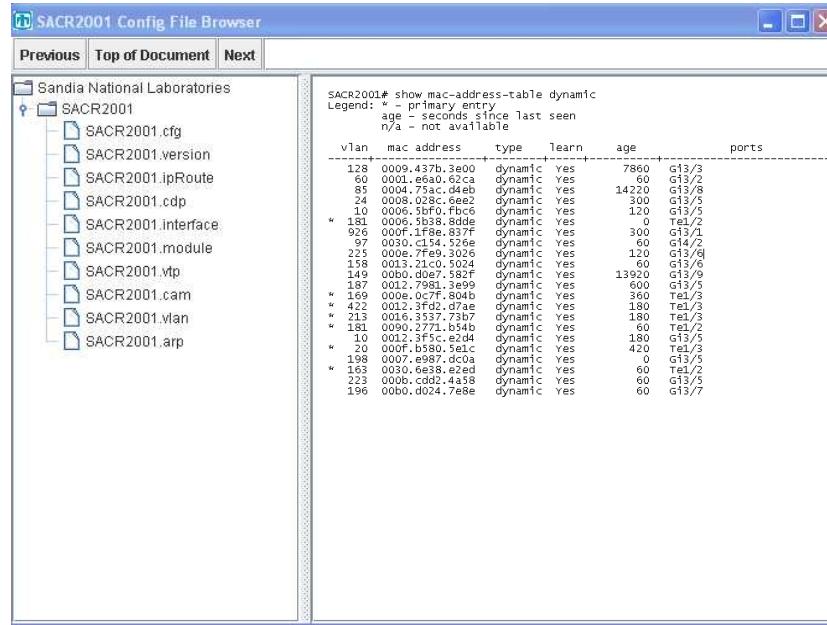- **Answers the question: What will be affected when this device fails?**
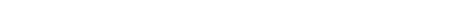
Upstream ⟵―――――――――――⟶ Downstream
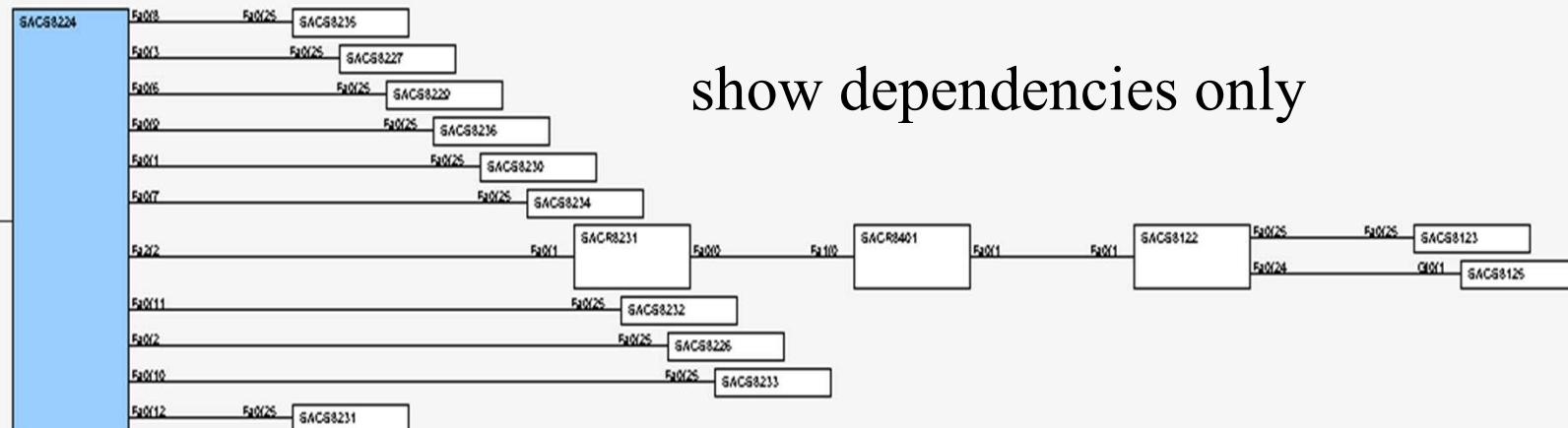
show dependencies only

DRIfT Visualizes Five-Minute Link Utilization Metrics from Statseeker as They Change
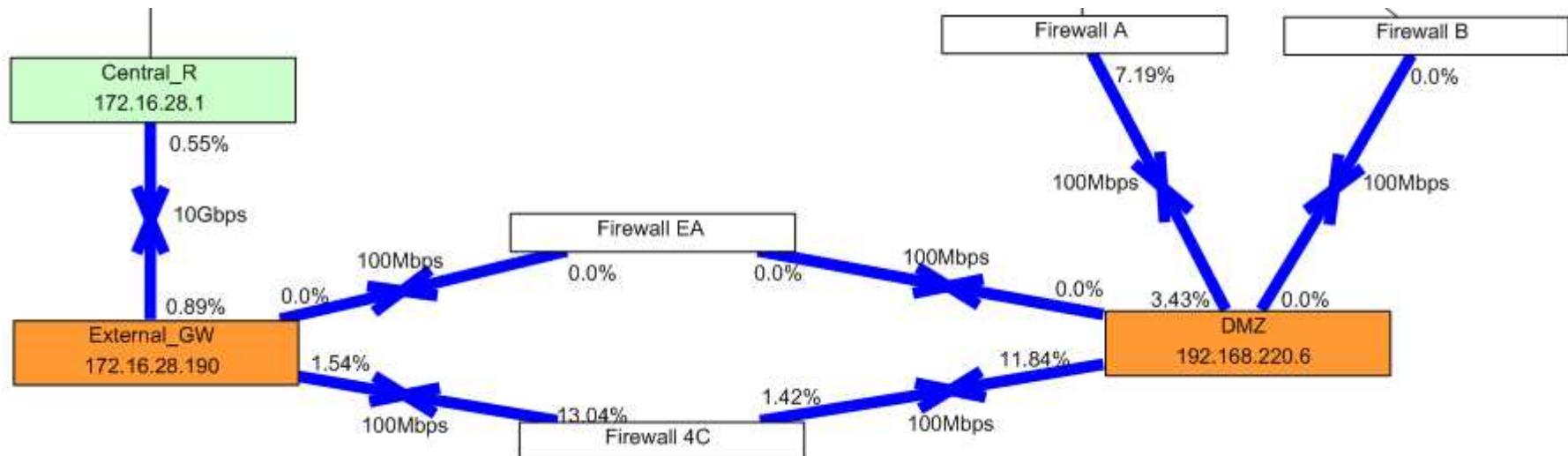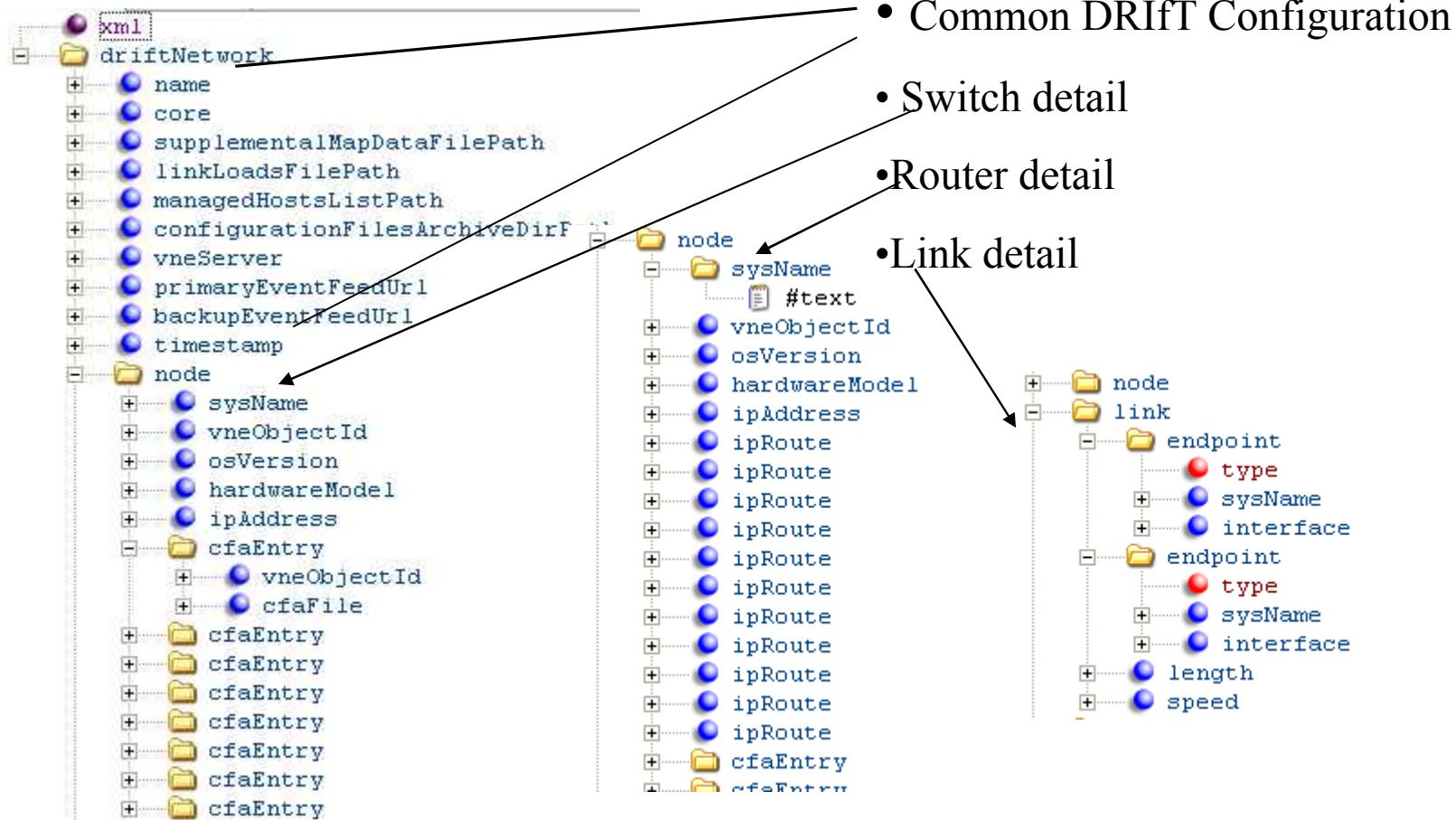
Retrieve Device Configurations

- **Device archive files are collected by VNE Server, and are retrievable by LUS starting in VNES 4.0.**

- **Archive file retrieval via LUS is not currently implemented in DRIfT.**

- **Archive files are stored in the ancillary server.**

DRIfT Input File Data Format.

- Common DRIfT Configuration

- Switch detail

- Router detail

- Link detail

DRIfT Event Feed Supports a Simple XML Structure

```
events
    xmlns:xlink = "http://www.w3.org/1999/xlink"
    event
        serial = "84087749"
        xlink:href = "URL FOR EVENT FEED "
        node
        severity
        firstoccurrence
        lastoccurrence
        summary
        agent
        snlarsticketnum
    event
```