Model Based Verification of Cyber-Range Event Environment

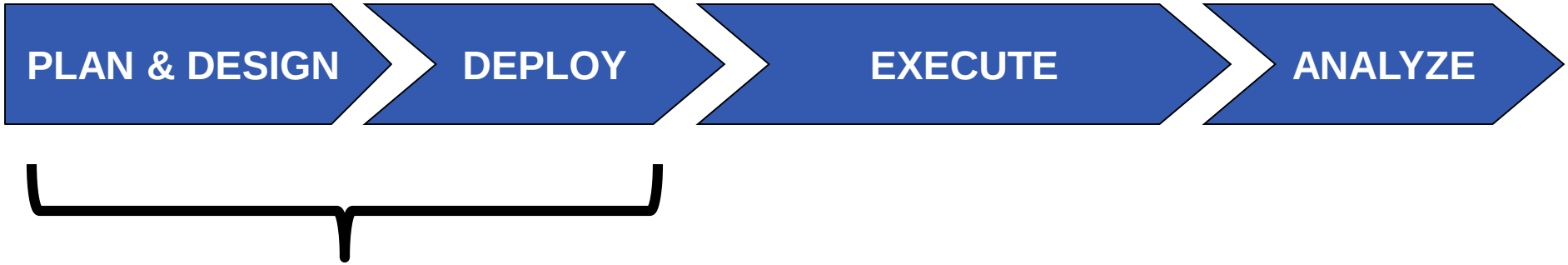
Dr. Suresh Damodaran

November 4, 2015

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

This work is sponsored by the Test Resource Management Center under Air Force Contract FA8721-05-C-0002 Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

Cyber-Range Events



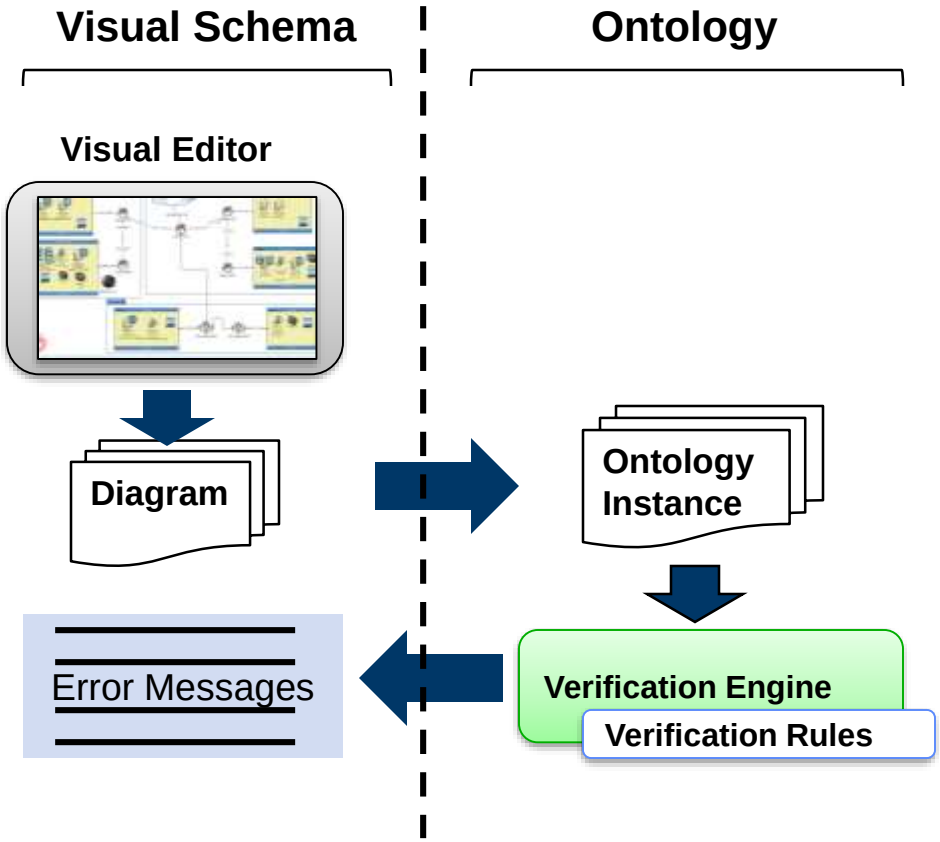
- **Configuration Errors**
  - **Design of event environment**
  - **Deployment of event environment**

Every error adds to the cost and duration of event

Impact of Configuration Errors

- **Configuration Error is a dominant cause of system failures**
  - **Yin et al. (2011)**
- **Configuration errors account for 50% to 80% of the downtime and vulnerabilities in cyber infrastrcuture**
  - **Narain et al. (2011)**

System Overview



What is in the Diagram?

User: organizations, teams, and behaviors of users.

Application & OS: applications commonly found on enterprise office computers, such as Microsoft PowerPoint or Outlook, and operating systems.

Service: multiple types of services such as DHCP, DNS, file, firewall, or proxy.

IP Device: devices with IP addresses such as Hosts or devices that support IP-based traffic such as Routers.

Ethernet Device: Ethernet devices, and technologies that support network traffic.

Physical Location: the cyber range and the sites where it is located.

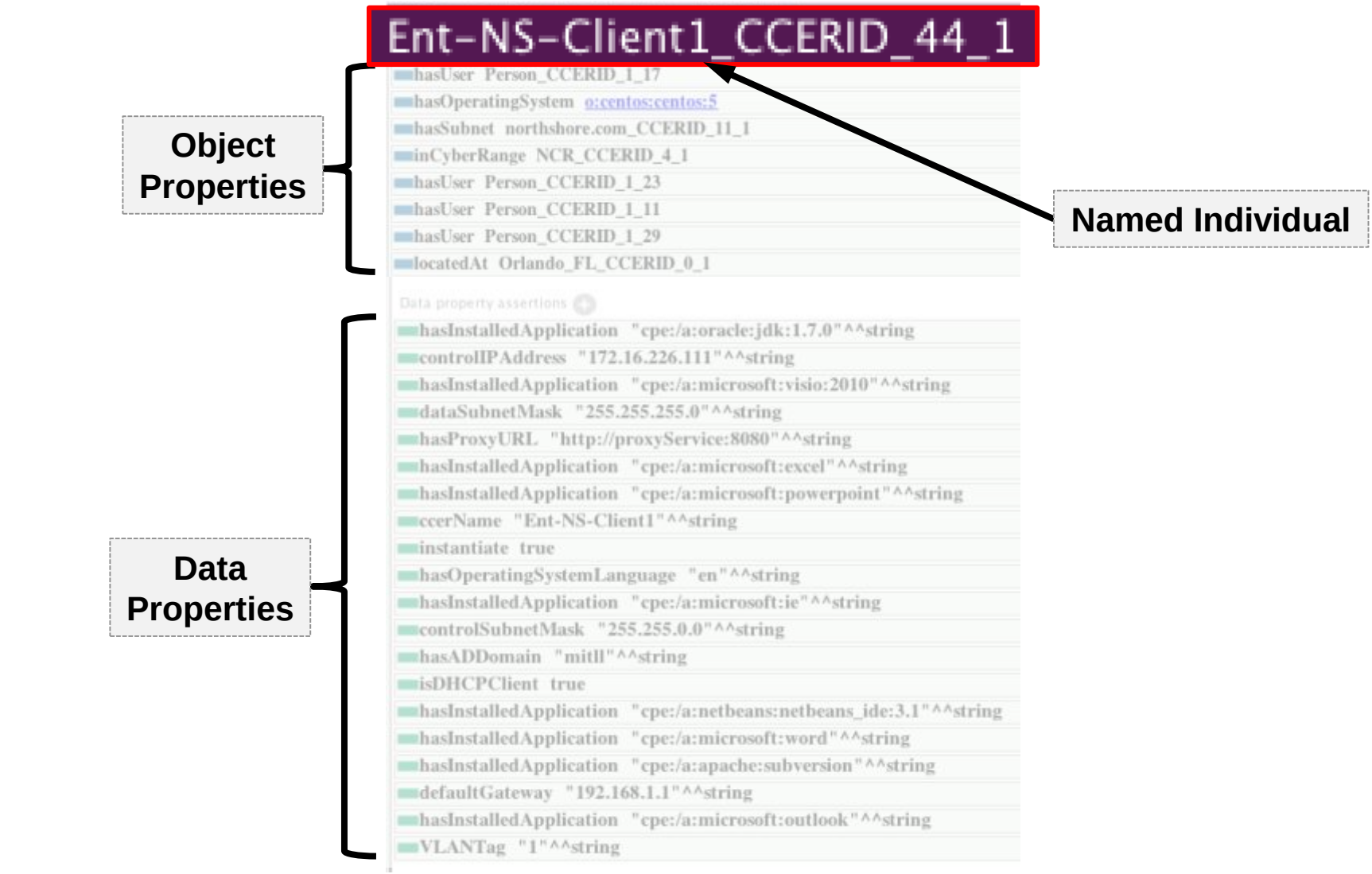
Control Plane: entities such as traffic generators

Instrument Plane: data collection services or probes.

CCER is an Ontology

- **CCER ontology is used for representing actual or simulation models of configurations of cyber (range) environment elements**

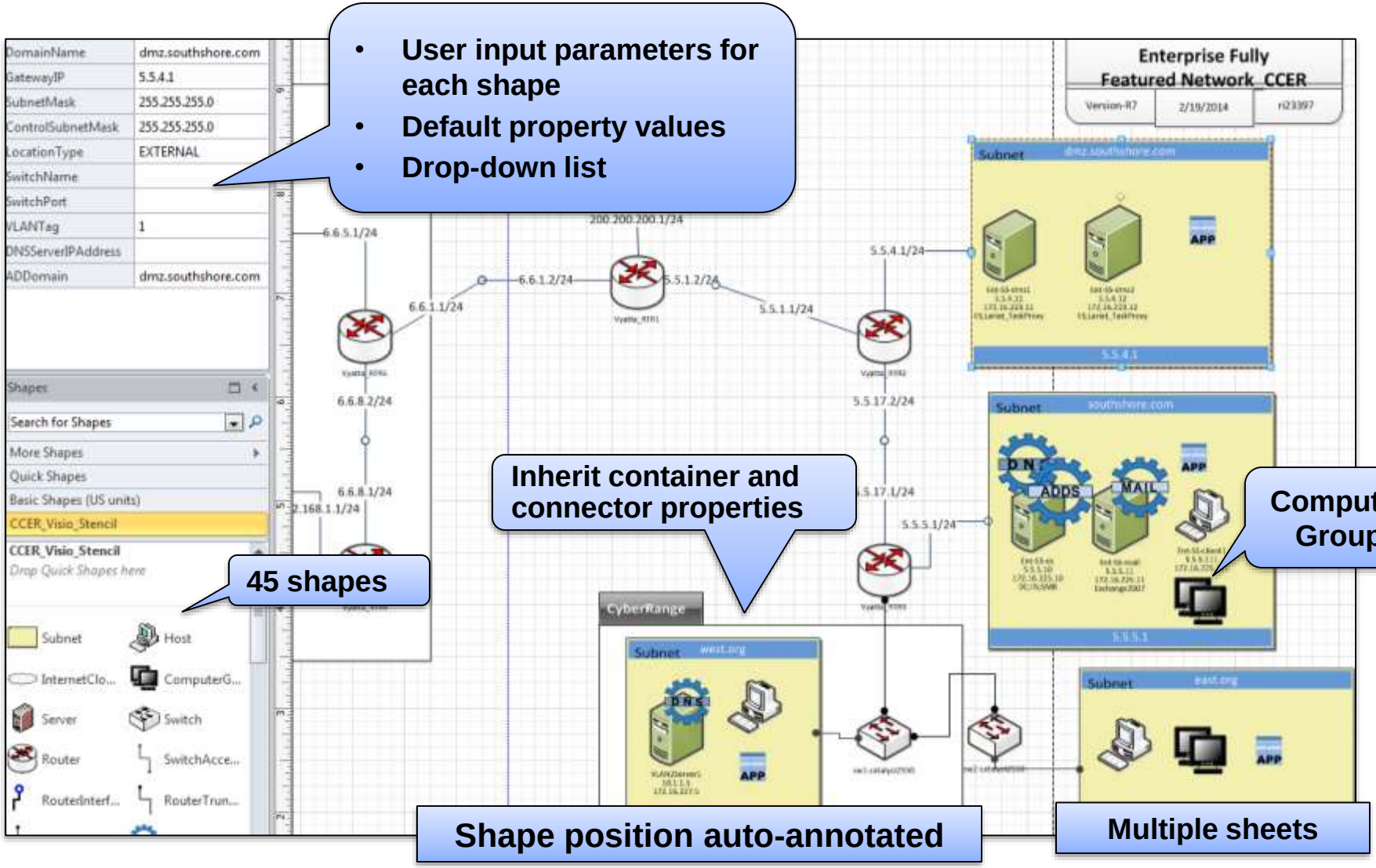
Computer Ontology Instance



Outline

- System Overview
- Visual Schema and Errors
- Methodology for Rules and Errors
- Case Study

CCER Visual Schema Summary

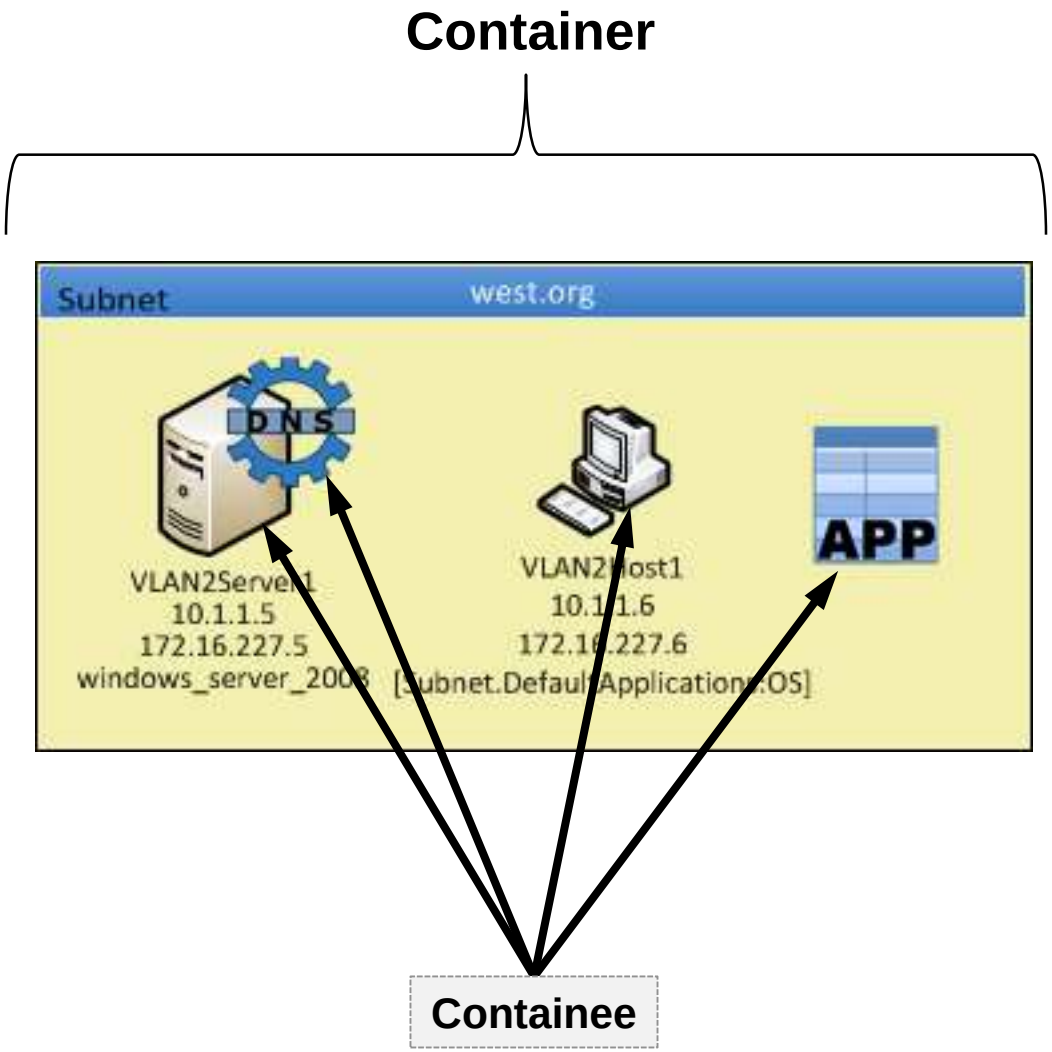


Visual Schema: Aggregation

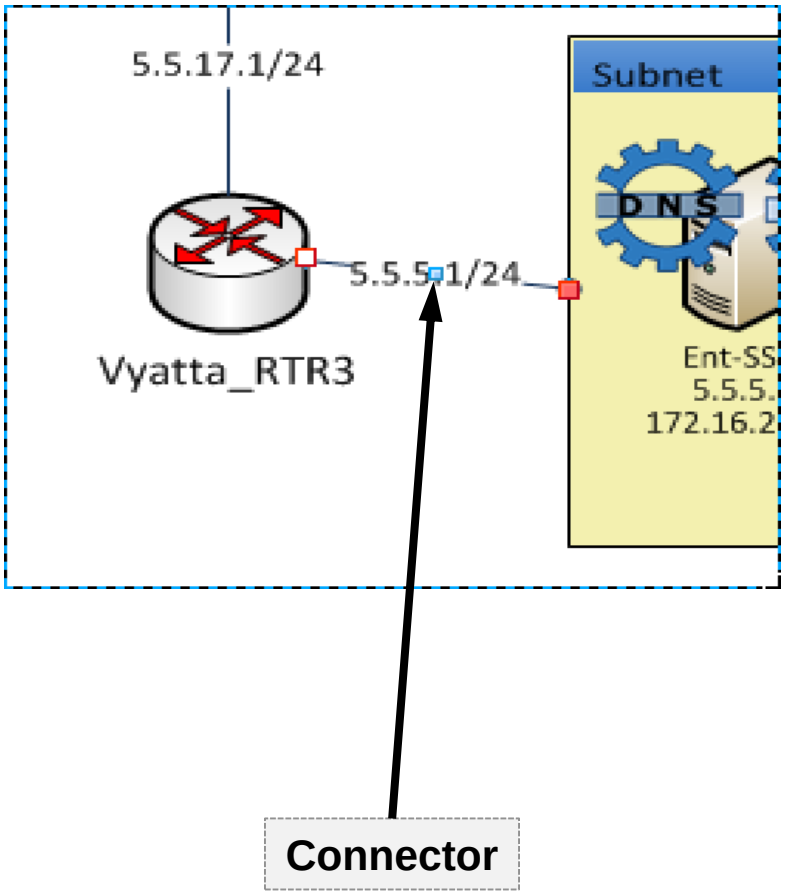
Shape Data - ComputerGroup.414

ComputerNameGenerationPattern	V3CG{i3}.{s}
MaximumNameLength	20
HostCount	5
DHCPClient	NO
StartingIPAddress	10.1.2.6
StartingControlIPAddress	172.16.228.6
OS	windows_8
OSLanguage	burmese (my)
Applications	[Subnet.DefaultApplicatio
AddedApplications	
ADDomain	[Subnet:ADDomain]
ProxyURL	[Subnet:ProxyURL]
Instantiate	TRUE

Visual Schema: Container

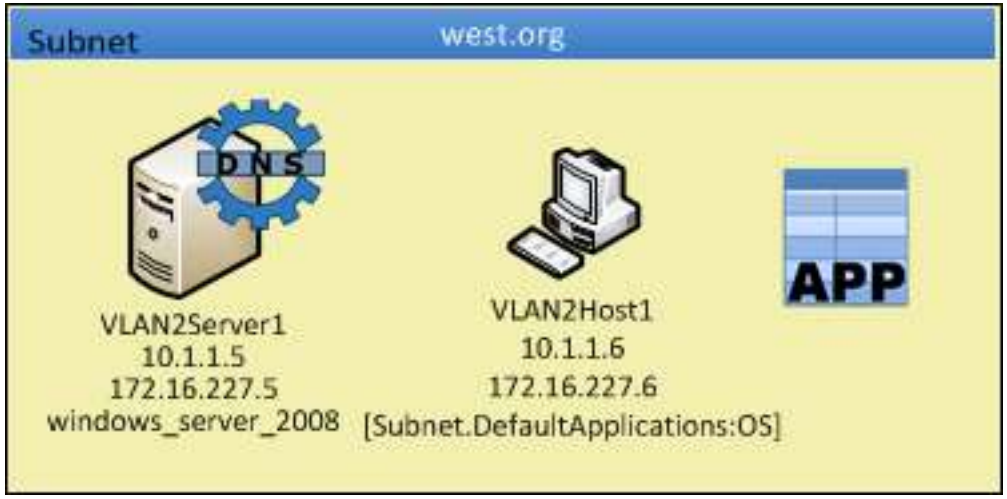


Visual Schema: Connection



Visual Schema: Scope

- **VLAN2Host1 is scoped within Subnet (west.org), if the processing of VLAN2Host1's fields is done by analyzing west.org, and all other shape instances that are scoped within west.org.**



Diagrams and Errors

- **Errors on diagram but processing with Ontology**
  - **Generating intuitive error messages is hard**
  - **1:1 relationship between shapes and OWL Classes may not exist**
- **Examples**
  - **Errors for Container Relationship**
  - **Errors for Aggregation Relationship**
- **CCER Tool suite needs to process error-free as well as erroneous diagrams (and should not crash!)**

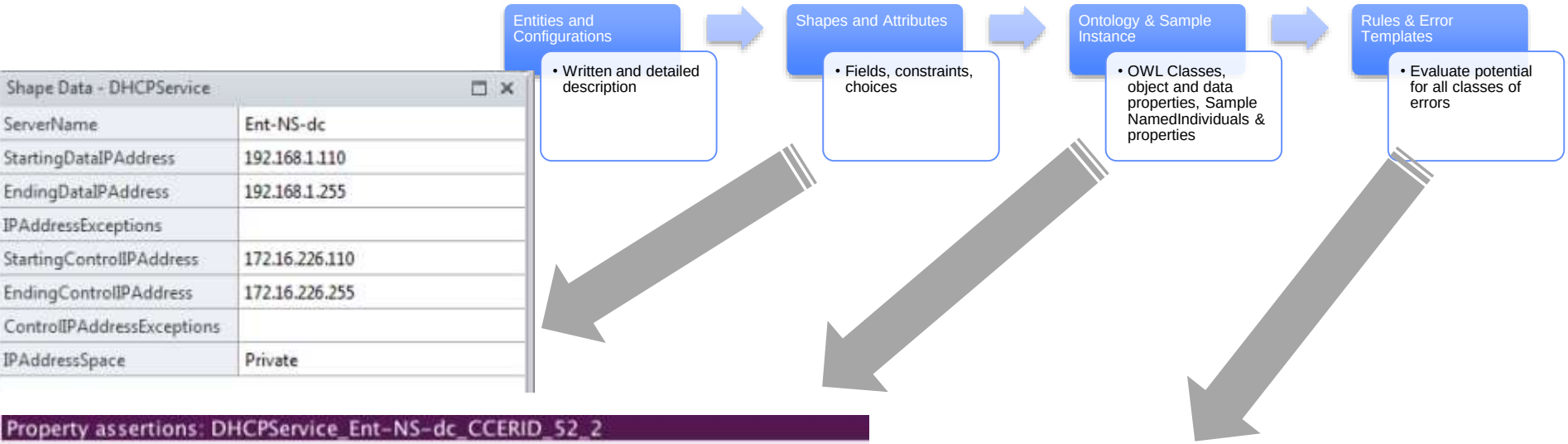
Outline

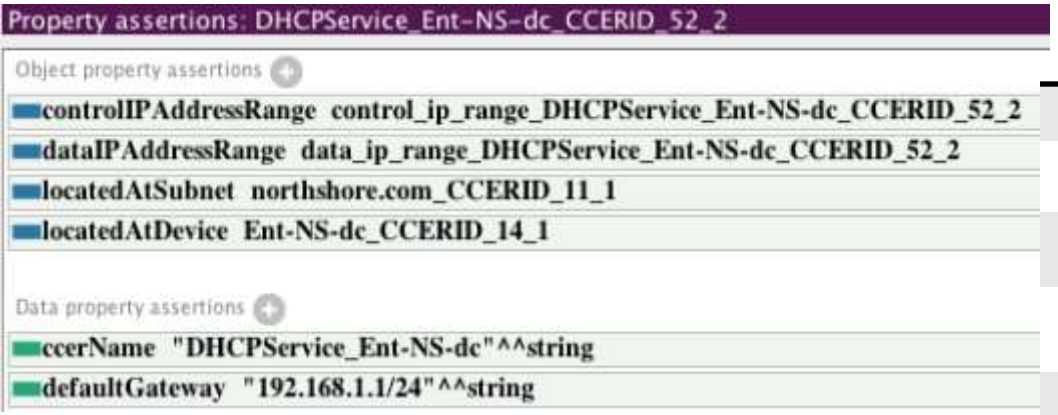
- System Overview
- Visual Schema and Errors
- Methodology for Rules and Errors
- Case Study

Verification Error Classification

1. Invalid Format
2. Unspecified Value
3. Inconsistent Value
4. Out-of-range Value
5. Uniqueness Violation
6. Non-existent Reference (Direct)
7. Non-existent Reference (Indirect)
8. Unspecified Reference
9. Inconsistent Reference
10. Singleton Violation
11. Generational Insufficiency
12. Abnormal Specification

Methodology for Rule Development



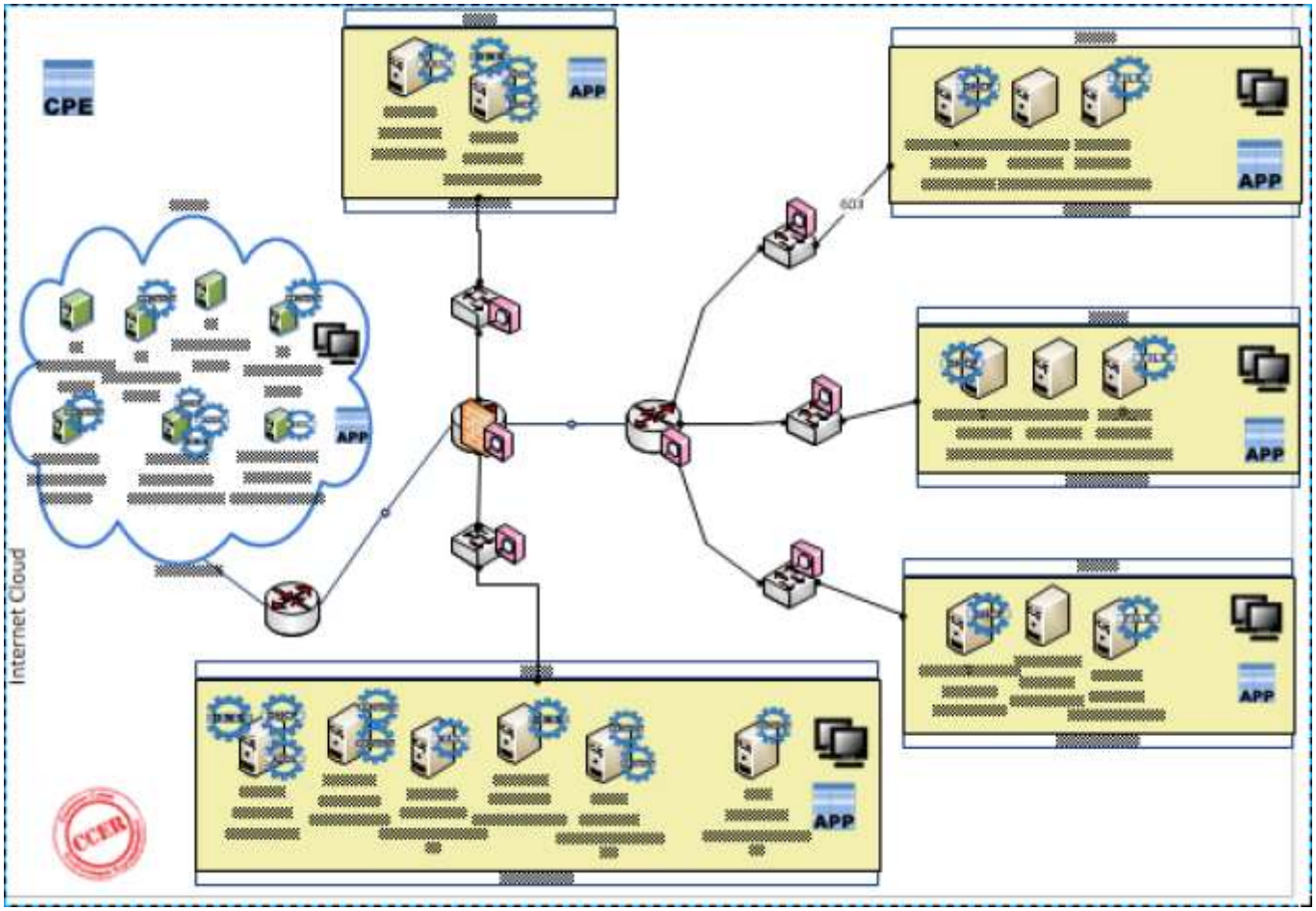


Rule ID	DHCP3
Error Category	Invalid Format
Shape	DHCP Service
Rule	DHCP Service Exception IP Addresses are specified in correct format
Error Message	DHCP Service: $DHCPService Exception IP Addresses have incorrect format

Outline

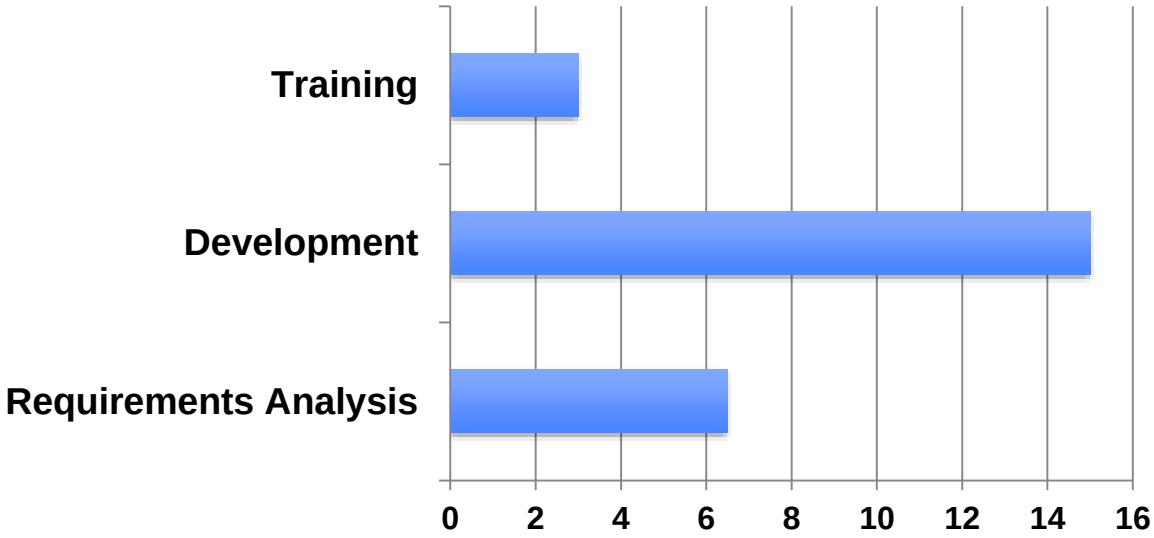
- System Overview
- Visual Schema and Errors
- Methodology for Rules and Errors
- Case Study

Case Study: Environment Diagram



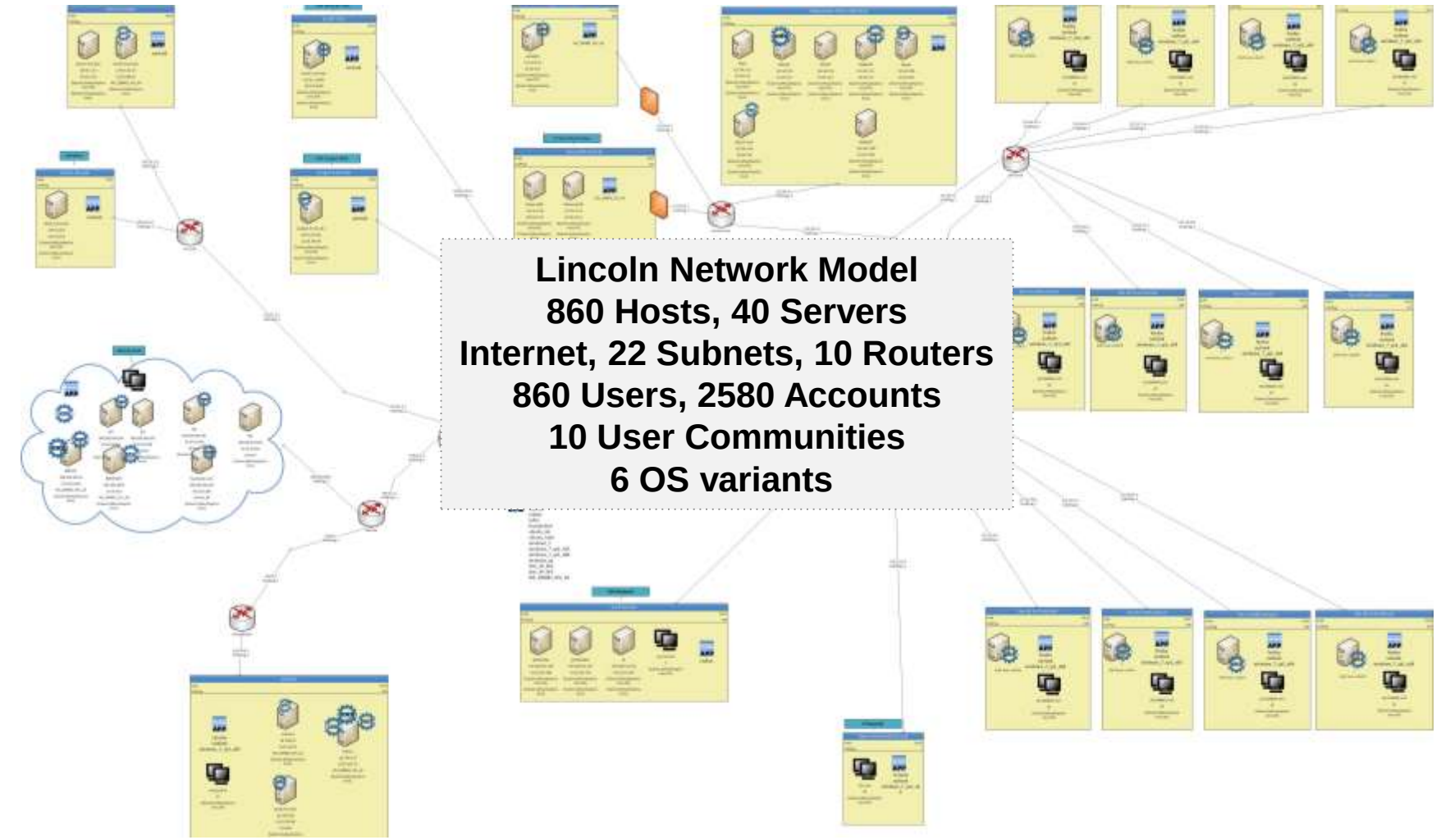
- 5 subnets
- 1 simulated Internet
- 3 routers
- 5 switches, and approximately 100 computers, users and 25 services

Case Study: Time Allocation



- **The X-axis is the actual time spent in hours on the activities shown on the Y-axis.**

Another Diagram



Conclusion

- **Model-based verification approach is demonstrably useful in reducing configuration errors in cyber-range event environments**
  - **Visual Schema for relationships**
  - **Classification of verification errors**
  - **Methodology for developing new verification rules and errors for new domains**
- **Future Directions**
  - **Reducing the number of error messages**
  - **Making errors more intuitive**
  - **Expanding CCER to include more domains**
  - **Performance analysis**
  - **Dynamic visual schema**

Questions?

suresh.damodaran@ll.mit.edu

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY