Towards Robust Trust in Software Defined Networks

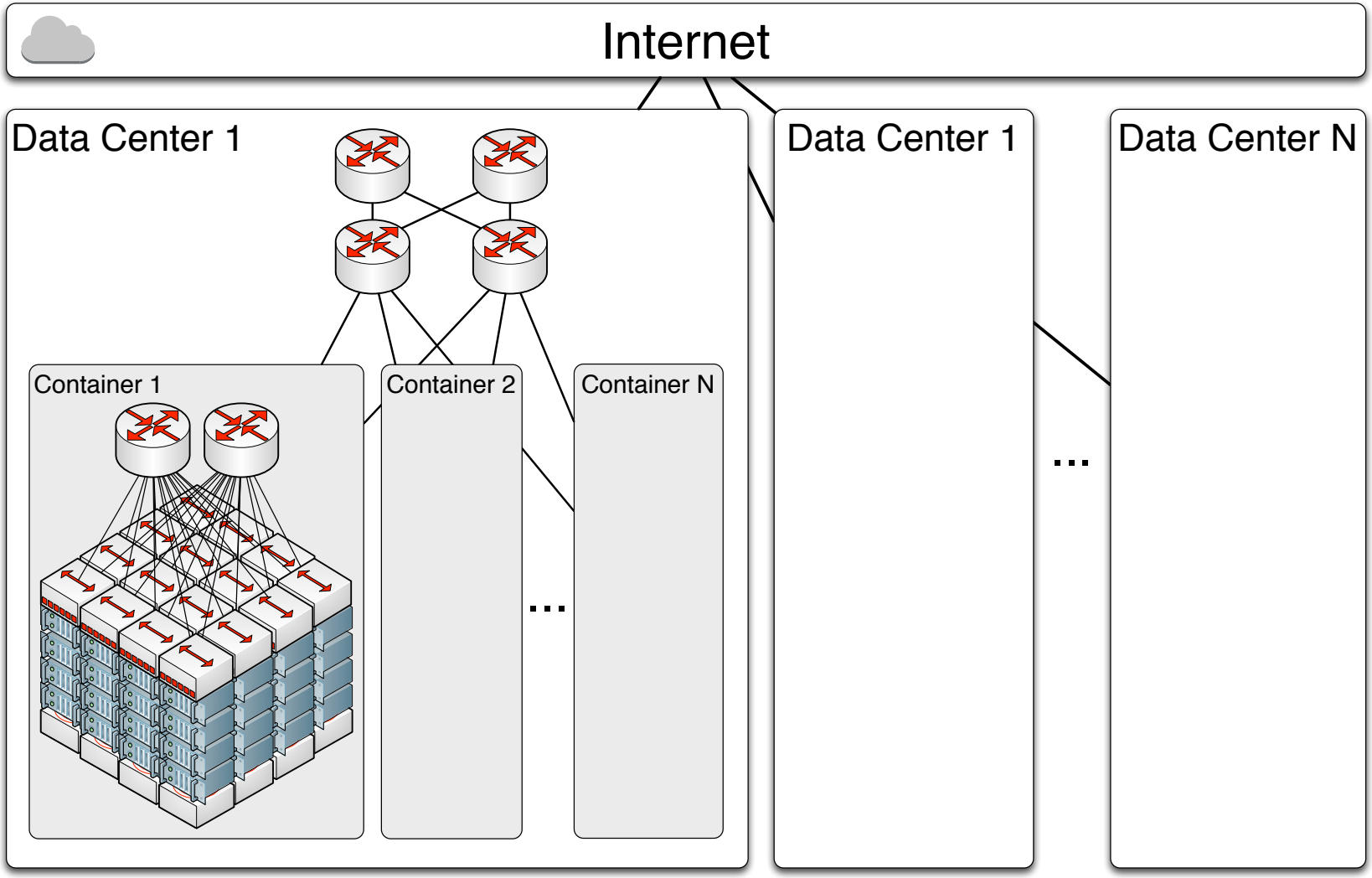
Christopher C. Lamb

Department of Electrical and Computer Engineering
University of New Mexico

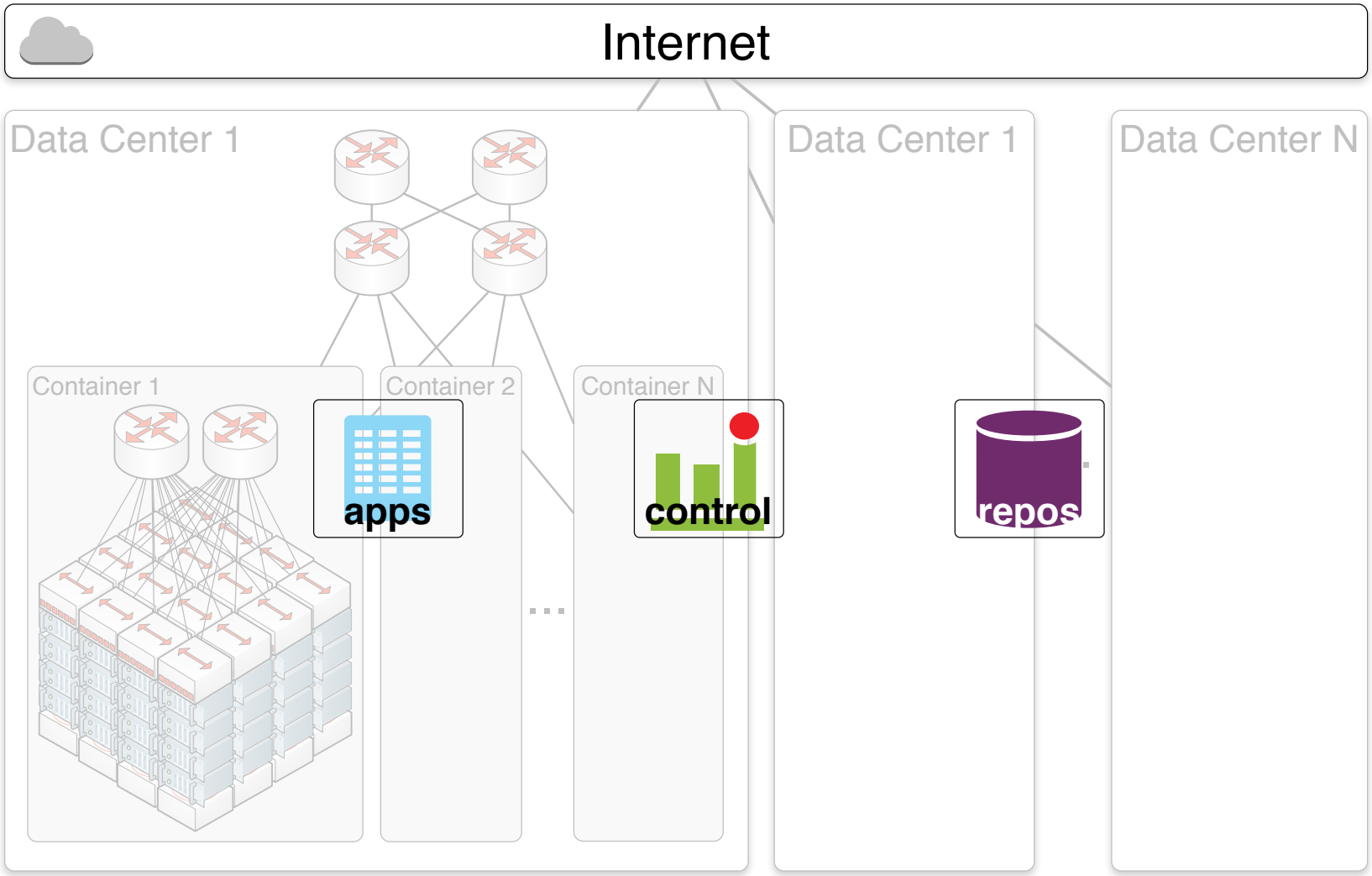
December 7, 2014

THE UNIVERSITY of NEW MEXICO

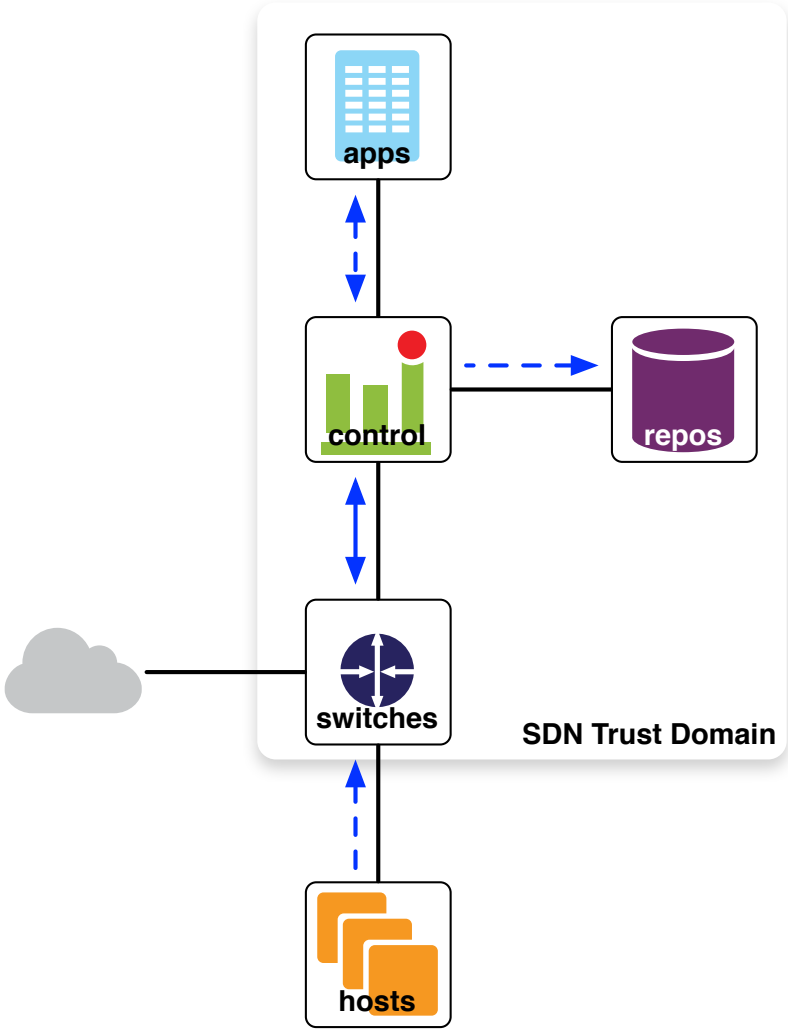
Networks in the Bad Old Days



The Brave New World!



Brave New Implications

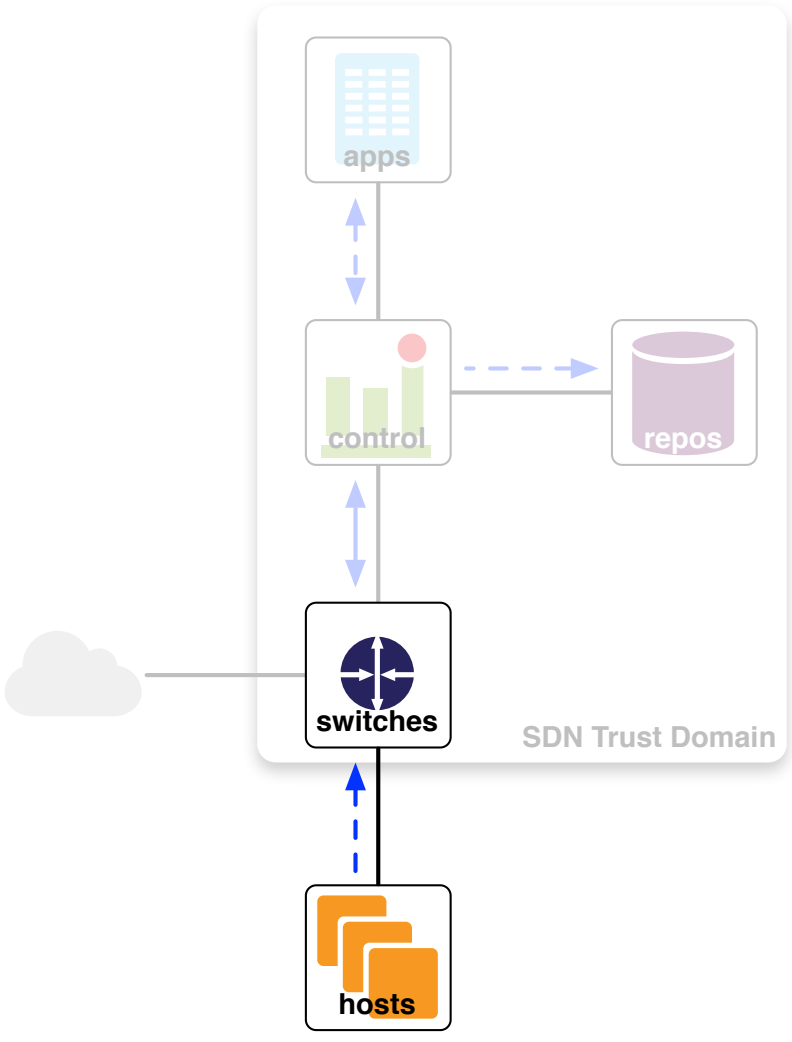


Unintended Results of SDN

Moving to centralized management has profound implications.

- Trust loci provides greater spoofing opportunities
- Smaller number of involved systems refines target space
- Trust concentration leads to larger attack surface
- Single compromise can have outsized effects

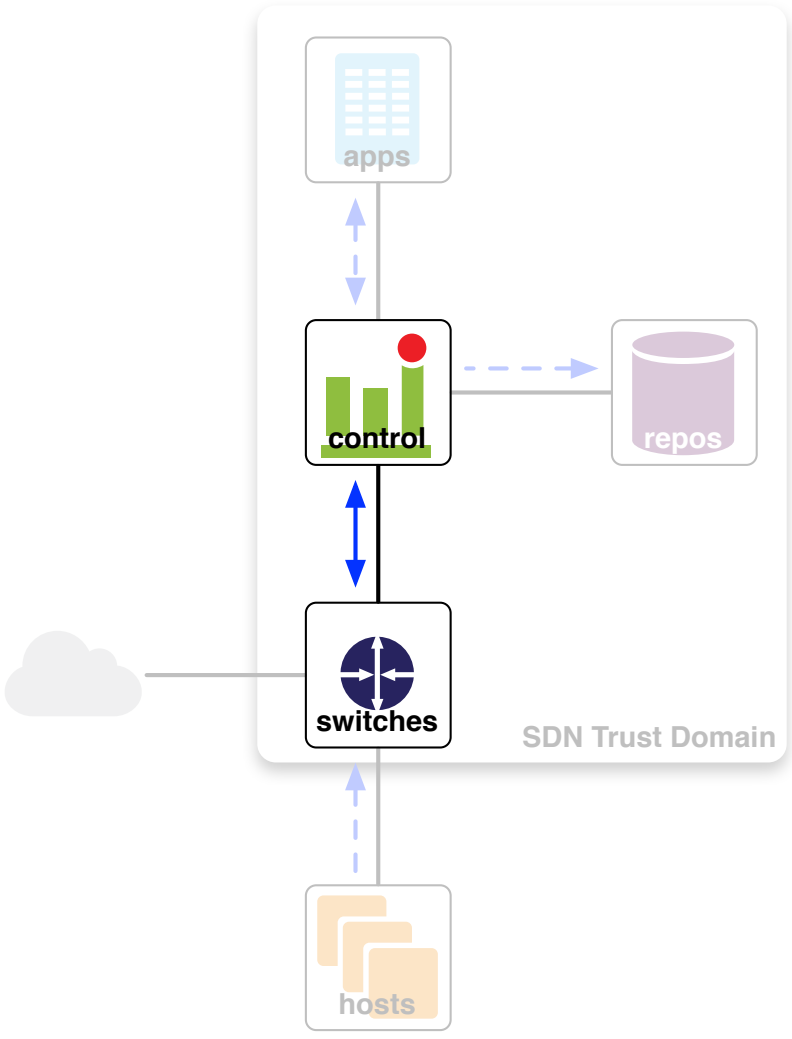
host $\Longleftrightarrow$ switch



(In the following slides, red is very important, orange less so, and green even less).

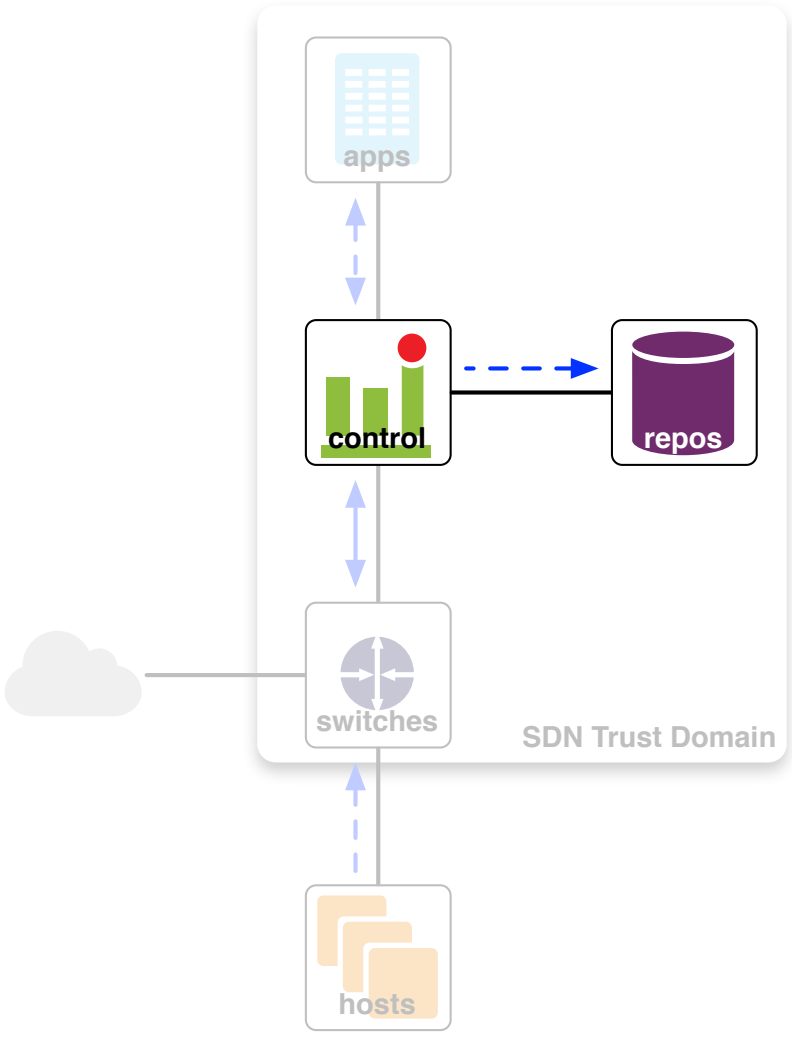
- Confidentiality not critical
- Integrity vital
- Availability expected
- Non-repudiation nice under certain circumstances
- Authentication likewise handy at times

switch $\Longleftrightarrow$ controller



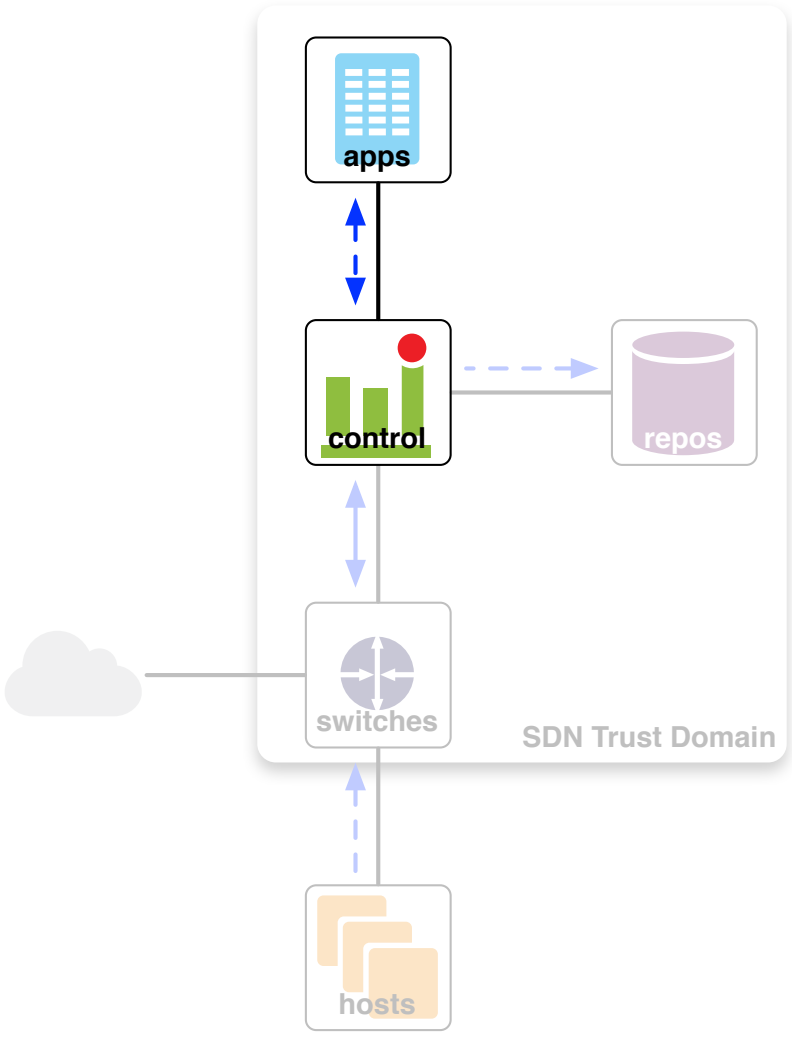
- Confidentiality only important in some edge cases
- Integrity again vital
- Availability paramount
- Non-repudiation perhaps more important
- Authentication of controllers important

controller $\Longleftrightarrow$ repository



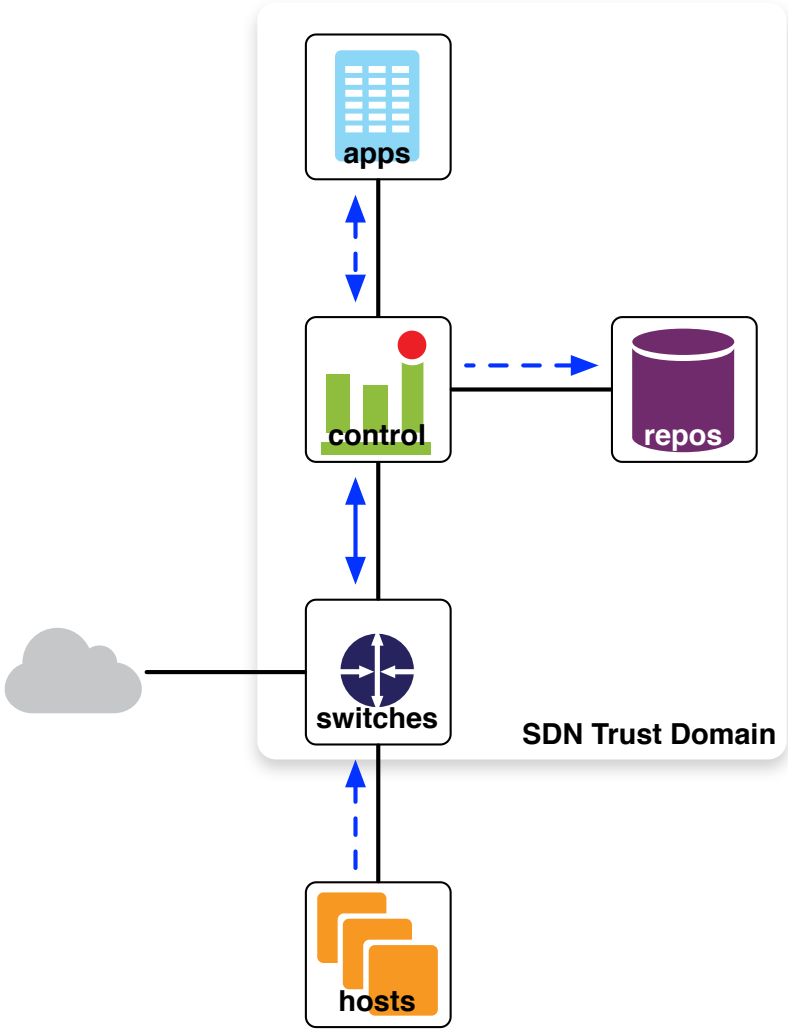
- Confidentiality not always vital
- Integrity important, as usual
- Availability not vital
- Non-repudiation less important for core control plane functions
- Authentication of repositories important

controller $\Longleftrightarrow$ application



- Confidentiality based on application
- Integrity important, as usual
- Availability not vital
- Non-repudiation needs again based on application
- Authentication of certain applications important

Attribute Commonality



So overall, how important are our typical cyber-security attributes?

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Authentication

Differentiating Attributes of SDN

Compared to other more agent-centric systems, SDN control systems have some advantages:

- Limited control-plane volatility
  - MANETs and agent-based systems are much more chaotic with respect to functional distribution (many devices wear multiple commmunication hats) and suffer from frequent attach / detach issues
- Centralized High-Availability
  - Any high-availability requirements are constrained to specific functional areas (e.g. controllers)
- Clearly Defined Roles
  - SDN entities have clear roles; systems in MANETs or agent-based systems frequently do not
- Predicable Expected Behavior
  - Clear roles should lead to more predicable behavior and correspondingly easier behavioral outlier detection

Questions? Comments?