William Brockelsby

Lead Network Architect, North Carolina State University

SDN Network Admission Control (SDN-NAC)

SDN Network Admission Control (SDN-NAC)

CONTENTS

- About NCSU
- Network Admission Control
- SDN NAC
- Results and Future Plans

About NCSU

- NCSU Metrics
  - Land grant university founded in 1887 – focus on STEM
  - > 34,000 students
  - > 8,000 faculty and staff
  - > 78,000 switch ports
  - > 2,000 switches
  - > 1,900 wireless access points
  - 3 /16 (Class B) IPv4 Networks ; 1 /32 IPv6 Network
  - ~3500 Analog Phones via VoIP Gateways ; ~5800 VoIP Handsets

SDN Initiatives

- SDN Testing and Research
- Traditional Slicing and Dynamic Circuit Provisioning
  - Founding participant of the NCREN regional SDN initiative
  - Campus slicing as part of a virtual Science DMZ (NSF CC-NIE)
- Replacing Proprietary, Complex and Expensive Systems
  - SDN-NAC
  - DNS Load Balancers
  - Data Analysis Network Matrix Switching Systems
  - Perimeter Defense Systems
  - Traffic Manipulation: WAN Optimization, Compression, Encryption, etc

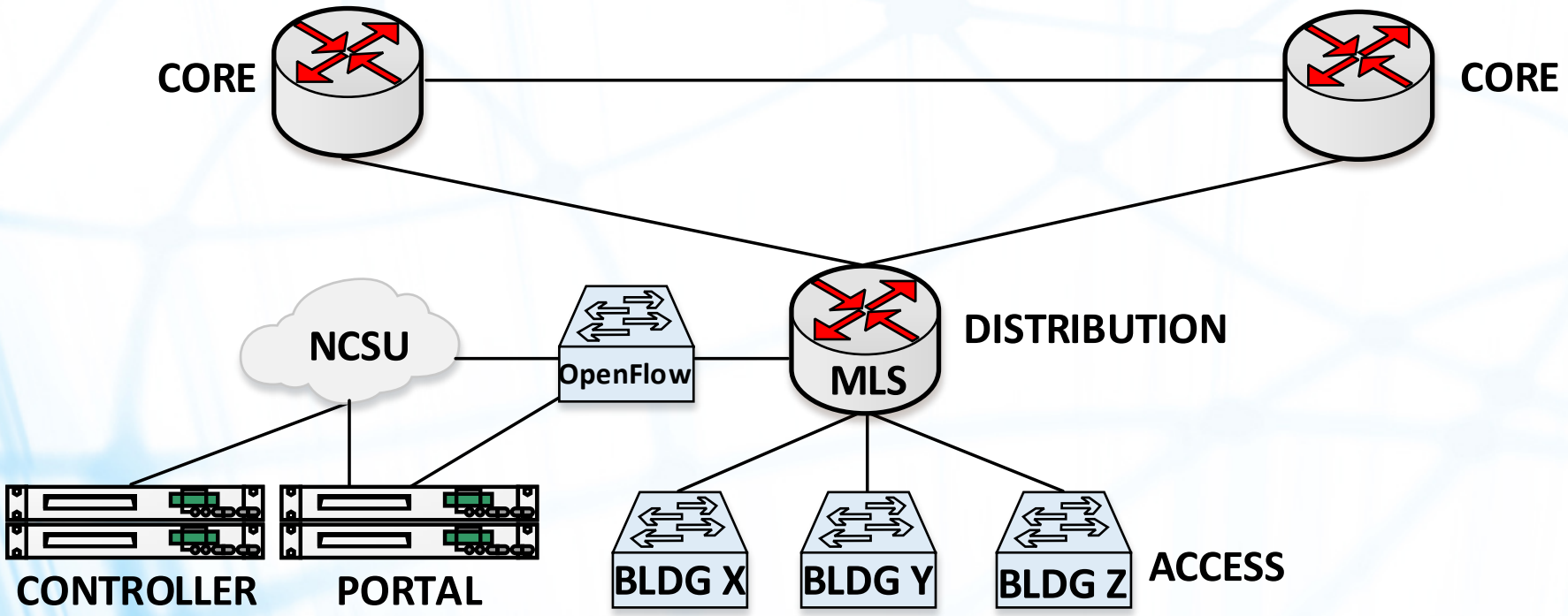
SDN-NAC Traditional Approaches

- The BYOD concept is new in many vertical markets but has always been standard practice in education
- Authenticating users and granting access to resources has many well known approaches
  - 802.1X
  - Functionality natively built into access layer devices by vendors
  - NAC appliances / platforms
    - In-Band vs Out-of-Band
- Traditionally Complicated
  - 802.1X – supplicant configuration
  - Native functionality – changing 1000s of devices
  - NAC appliances
    - Expensive – CAPEX and OPEX
    - In-Band – performance penalty
    - Out-of-Band – changing 1000s of devices (if supported)

SDN-NAC Approach

- In-Band Mechanism
  - Minimal changes to the network
  - Continues to permit the deployment of non-ComTech switches
  - High performance hardware forwarding plane (Thanks to SDN!)
- SDN Algorithm
  - Buildings connect to multi-layer switch/router via VLANs X,Y,Z
  - Remove router interface for VLANs X,Y,Z
  - Create new VLANs X',Y',Z' with the original router interfaces
  - OpenFlow switch maps authenticated users from X -> X', Y -> Y', Z -> Z'
  - OpenFlow switch sends unknown users to web-based captive portal
  - On successful authentication, captive portal installs rules into OpenFlow switch for future mapping to VLAN with router interface

SDN-NAC Architecture



SDN-NAC Example

- Visiting Faculty/Staff/Student Connects Host
- DNS+DHCP is permitted through SDN NAC switch
- DHCP server responds and provides valid IP lease
- Browser opened on host: www.internet2.edu
- No specific OpenFlow match for this users SRC MAC and IP combo
  - Traffic is sent to the captive portal (VLAN rewrite, DST MAC rewrite)
- Destination NAT is running on Linux captive portal via IPTABLES
- Apache is running to present captive portal web page
- User authenticates via Shibboleth/WRAP or other web authentication

SDN-NAC Example

- Captive portal sends flow mod to controller and logs transaction in DB:
  - Match SRC MAC M+ SRC IP S
  - Action: Rewrite VLAN X to X'
  - An inactivity timeout is specified
- X' traffic always rewritten to X (to permit return traffic flow)
- Host traffic is now on the network with line rate performance
- After inactivity, flow times out and controller updates database
- Role based access: Can be implemented with additional flow mods

SDN-NAC Goals

- SDN NAC Goals
  - Minimize changes in the network topology (low cost)
  - Minimize dependence on SDN (maximize vendor compatibility)
  - Minimize flow mod / sec (proactive = high performance)
  - Leverage Layer2 and Layer 3 matches
  - Do not rely on DNS tricks for captive portal
  - Minimize number of flows

SDN-NAC Where We Are

- SDN Status
  - Lab Tested
    - Juniper, Brocade, Cisco, Dell/Force10, etc
  - Waiting on vendor hardware support for OpenFlow 1.3
    - To provide IPv6 match capabilities, etc
  - Looking at high availability options
    - Redundant NAC switches
    - High availability controllers (i.e. 100% solid state, fanless, DC, etc)
  - Planning deployment in our conference rooms this calendar year
  - Depending on results, potential replacement of our existing residence hall network (RESNET) NAC environment

Funding Results

- 10K Innovative Application Award Plans
  - Develop “Internet of Things/Everything” lab
  - Develop embedded systems for a variety of application use cases
  - Integrate these systems onto the network by leveraging SDN
  - Continue to publish projects to the community

William Brockelsby

Lead Network Architect, North Carolina State University

QUESTIONS?

SDN Network Admission Control (SDN-NAC)

wjbrocke@ncsu.edu
919-515-0114