K20 End to End Performance Initiative

Leveraging the Internet 2 Tools and Partnership
Overview

- About MCNC
- End to End Performance Initiative
- K12 End to End Performance Pilot
- Lessons Learned from Pilot
- Revised Approach
- Proposed Architecture
About MCNC

– We own and operate the North Carolina Research and Education Network (NCREN)

– Our customers include public and private universities, community colleges, K12 school systems, state government and other non-profit institutions

– Our mission is to provide K20 connectivity to North Carolina’s educational systems as requested by the state
The K12 Part of the K20 Vision

– Today, 27 Local Education Agencies (LEAs) or Public School Systems are connected to the NCREN backbone

– We plan to connect 115 out of 115 LEAs by the end of the year

– MCNC is a member of the School Connectivity Initiative, a partnership between key institutions in the state focused on:
  • 21st Century Student Outcomes
  • Equity of access for students
  • Implementing a statewide education backbone to keep local traffic local
Layer-2 Metro Ethernet between NCREN and NCREN Managed Router at LEA; LEA maintains control of WAN connectivity to schools behind LEA firewall; NCREN managed routing policy via BGP such that local NCREN, ITS, and DPI traffic, along with Internet2/NLR related traffic flows to NCREN.
MCNC’s End to End Performance Initiative

– Goals of the initiative:
  • Provide network performance data to customers including availability, latency, traffic levels and utilization
  • Provide customers and NOC engineers ability to diagnose performance issues

– Some of our available tools:
  • Latency Matrix
  • Weather Maps
  • Cacti Utilization Graphs
  • Smoke Ping (one way latency and loss)
  • NDT servers (end to end throughput testing)
End to End Performance Initiative: (The K12 Part)

– Continue to provide network performance data to customers

– Continue to provide tools to diagnose network performance problems

– Expand our scope and ability to assess application readiness of school systems’ network infrastructure
1. We identified a few school systems that were extremely excited about joining the pilot and offered to do anything that was needed to be a pilot site.

2. These districts had distinctly different network architectures that are representative of the vast majority of LEAs.

3. Tools would measure network utilization and latency/loss at LEA and each school.

4. Tools architecture was centralized in RTP and would poll remote LEA infrastructure.
What We Learned

1. We found this was not a simple architecture to implement. Someone at the LEA or a contractor had to make various changes on equipment. The types of changes needed vary from LEA to LEA depending on local equipment installed.

2. Firewall case - One LEA did not have enough public IP space to implement static NAT to reach devices. We think this will be an issue that affects the majority of systems.

3. Another LEA had publicly accessible “routers” but were not a “standard” CPE device.

4. Tech Directors at School Systems are busy! When onsite they are eager to participate, but once we leave it was extremely difficult motivating them to make changes (or even getting them on the phone!)

5. Yet another LEA had already implemented Cacti.
Revised Approach

- Pilot model had a centralized architecture that polled LEAs or school systems

- New approach would collect and analyze latency and utilization data between two end points:
  1. Somewhere on the statewide backbone
  2. Somewhere in the LEA or school system network
Visualization of Proposed Architecture
Proposed Architecture

CD image that can be distributed to LEA
✓ Can be easily installed on any server or computer
✓ Simple installation that only requires user to boot from CD
✓ Will work on almost any server hardware
✓ Support remote configuration and management

Tools in the toolkit
✓ Measures latency/loss/(jitter) from each endpoint
✓ Measures available bandwidth on LEA connection
✓ Provides real-time network analysis, both internal and external
✓ Extensibility desired. Possibly expand to capture flow data in the future.

Centralized Data Repository
✓ Summarized data is sent northbound to a collection server
✓ Collection server provides GUI access to performance data
✓ Support for Federated Identity Management
How would it work?

— CD installs operating system and tools /or/ CD runs from memory in virtual OS

— Once installed, server automatically creates northbound connection to central server

— To get through NDD’s, server establishes IPSEC tunnel to central reporting server

— Centralized server starts collecting network performance metrics immediately

— Centralized server has a GUI interface and a “Dashboard” to see overall network health
How would it work (cont’d)

—Centralized server acts as a VPN concentrator and gives out private IP addresses to endpoints

—By using IPSEC tunnels, we get through firewalls and create a statewide private IP network overlay for network performance measurements

—Toolkit endpoints store detailed data. When user wants more information than Central GUI has it is pulled from endpoint
Next Steps…

1. Leverage Internet2 toolkit for endpoint at school systems

2. Leverage PerfSonar for centralized server with GUI interface
Special Thanks to the Network Performance Working Group

Andrew Mabe, Duke Medicine
Carla Hunt, MCNC
Dave Furiness, MCNC
Ed Winstead, MCNC
John Bass, NCSU Centennial Networking Lab
John Moore, MCNC
Mark Johnson, MCNC