Session Abstract:
Today the Internet2 network doesn't offer QoS, all traffic via AL2S, AL3S, etc. is provided via a best effort service. As we more tightly couple both on and off campus services (e.g., extending local workloads so they are both in the cloud and local), what QoS capabilities are required, and how are they stitched together from campus to RON to Internet2, and beyond.
This session will provide a survey of the current state of QoS within our community, and seek input on potential future states.
Current State of community QoS deployment

59% of campus network use some form of QoS (n = 12)

89% of RONs use some form of QoS (n = 9)

Note: inconsistency in responses. Some answer “none” to “What QoS is in use today”, but then say “only VoIP” in response to “what applications does the QoS support?”
QoS is used to...

- **Enforce policy** for low capacity access circuits (e.g., K12 connections)
- **Protect** VoIP & Video sessions
- **Protect** control plane
Since its beginning, the Internet2 network’s QoS has been over provisioning. With the exception of experiential services such as ION, Internet2’s headroom, alone, has provided a loss-free, relatively low jitter network service.

The **Policy** has to been to over provision. Does the community perceive a need for bandwidth **Protection**?
In the beginning...

- The Internet2 connection was operationally optional
- For the most part, the compute and storage backends critical for the day to day operation of the university were at the university
- Loss of off-campus connectivity wasn’t a snow day
At some point we crossed the Rubicon.

As our critical education systems increasingly rely on cloud connectivity, do we need bandwidth protection mechanisms to ensure access to these systems when there’s a network fault?

Is that require end-to-end coordination?

If desired, how should the community provide input to Internet2?
Potential Backbone Contention Scenarios

• Single elephant flows don’t hash evenly over LAG
• Unexpected traffic
  • Hidden research project that pops up one day
  • Fiber cut with traffic re-route
  • A combination of the two!
• “Expected” traffic
  • Supercomputing
  • Sometimes no one knows the effect until it happens
• IXP and Peering traffic
  • Large peer shifts traffic to another IXP
  • New services are turned up rapidly
  • Large scale events (e.g. iOS release)
• Most of the time the above is controlled via overprovisioning and traffic engineering- if we know about it ahead of time