# Network Capability Discovery for Internet2 Institutions

Henning Schulzrinne
AMSAC

While all nominally connected to the same IP network, end users at different institutions experience very different network capabilities. On some campuses, students and faculty may only be able to access web sites and send email; on other campuses, they can freely use the whole panoply of modern Internet services, from IPv6 to multicast and VoIP. This diversity can make rolling out applications frustrating for users, as they cannot easily predict which applications are likely to work. As an example, the Philadelphia Orchestra found that only a small fraction of institutions could receive their high-bandwidth multicast live performances, and non-technical users had no good way to predict whether they could do so.

We propose to create a system that makes it easy for end users to discover network capabilities, using both campus self-assessments and tool-based approaches.

We envision three broad classifications of capabilities in the self-assessment:

- Production (Supported): The campus network is committed to supporting this capability; if it does not work, local technical support and network operations are willing to help fix the problem.
- Experimental (At your own risk): Applications needing this feature may work, but the support is considered experimental. Campus technical support may or may not be able to remedy problems that occur, and such problems may have lower priority.
- Not available: The capability is not available on campus. If an end user needs that capability, they need to discuss this with policy-making authorities on campus.

The capabilities may differ for a campus wired and wireless network. Certain parts of a campus, such as dormitory networks, may further restrict or enhance the available range of capabilities. The measurement tool would then provide a way to ascertain current functionality.

Applications and services would then also declare the set of capabilities that they need to function, so that end users can match up capabilities and needs.

Longer term, we also hope that external evaluations, e.g., "most wired campus", take this information into account, providing encouragement to increase the network capabilities that are available to students and faculty.

The set of capabilities will be the subject of this discussion as part of this task and is likely to expand over time. The list of capabilities should be reasonably small and

easily describable, so that non-technical users can communicate with local system administrators. It might be useful to define a set of icons that are easily recognizable. An initial set of capabilities could include:

| Capability | Symbol | Description |
|---|---|---|
| Transparency | Checklist | End systems can send data to and from any port. (Some ports that are almost always blocked, such as port 445 (SMB) may need to be excluded, but campuses should list such ports to simplify debugging.) |
| Public IP address | Globe | End systems acquire a public IP address (i.e., not NATed and not an RFC 1918 address) that can be reached from the outside. |
| Multicast | Fan-out symbol | End systems can send and receive multicast traffic. (It may be necessary to distinguish ASM and SSM.) |
| IPv6 | IPv6 | End systems can send and receive IPv6 packets. |
| High bandwidth | Firehose | End systems can send and receive streams of 10 Mb/s. |

The test tool could be developed by a summer intern or short-term supported research project and should be easily downloaded, e.g., as a Flash or Java applet. This may require some NOC support, e.g., to generate a multicast beacon or to report back reception of multicast packets sent.