



www.internet2.edu

What is E2Epi? E2Epi is Internet2's End-to-End Performance Initiative. For more information about us, see our website at: <http://e2epi.internet2.edu/>. There you'll find links to recent projects (like **E2E piPEs**) and presentations, as well as other information related to end-to-end performance issues, measurement tools, upcoming events, and related activities.

Too Much Is Never Enough

Wireless Problems Affect Network Planning

A Case Study for E2Epi

When planning a wireless network for a recent conference, the networking team thought they had all their ducks in a row. A year before the event, they opened lines of communication with the telecommunications staff at the conference hotel, began bi-weekly team conversations, and regularly exchanged email with the hotel staff. ***What could possibly go wrong?***

Several things, actually, could and did, despite the planning and hard work of the team. Wireless networks routinely cause headaches and this meeting was no exception. Three challenges that often confront meeting planners were faced and solved by the team.

1. Have a well-tested plan for a cohesive, functioning network.

A few of the campus engineers were interested in a new wireless system and wanted to use this opportunity to test its efficacy in an indoor environment. Some members of the team were very concerned; the system being considered was very effective in outdoor situations (for which it was originally designed), but the technology it used seemed incompatible with such indoor environments as the hotel.

To ensure against system failure, the team agreed to have another, well-understood (*and* well-tested) backup system in place to take over at a moments notice.

During the meeting, wireless problems caused the team to switch to the backup system – they discovered that, although

the secondary wireless system was physically onsite:

- The access points were pre-configured and functionally tested but not deployed (still in boxes).
- The power levels were not adjustable (which is unusual and caused problems in deployment).
- The access points hadn't been tested as a cohesive, functioning network.

As a result of these three issues, the backup system was even *less effective* than the initial wireless system. The backup system was up for only half a day. The original system had been running and undergoing modifications for 3 days; the backup system would require 2-3 days to fine-tune it by which time the meeting would be over. The team switched back to the initial system and continued working around the known problems.

2. Know who is using the network and where they can be found.

The campus wanted to use a wireless registration system that was adapted from the authentication system they used successfully in residence halls. To get a DHCP address, the user has to provide a name and email address so that, if a problem occurs, the user can be located quickly.

This system caused some concern for two reasons: first, there is a 5-minute delay in the registration process, which could prove to be a grumbling point amongst a

group used to fast, easy access to the Internet. Second, because attendees were largely computer professionals and researchers, privacy issues were raised that do not usually affect students.

To avoid the negative public reaction that may occur with the registration request, the team agreed to inform the attendees: 1) that this is a one-time registration (not daily during the conference), 2) that the data would be kept for the period of the conference only and then deleted, and 3) *why* the information was being collected and what the expected delay would be. To avoid possible delays with late-arriving speakers, all speakers would be pre-registered. These measures proved very effective in managing user expectations; the registration was also very useful in quickly contacting owners of machines with problems.

3. Provide “adequate” support. The team’s goals for the network at this meeting were to provide a quality wireless service and identify and fix problems created by “ad hoc” access points. To meet these goals, they:

- Staffed the support desk with 3-4 people from 7 am to 7 pm throughout the week.
- Dedicated 4-6 people walking around the hotel with wireless analyzers to find rogues.
- Arranged for a trained engineer from the wireless company that was being used to be on-site, full-time, during the meeting.
- Maintained several campus network engineers full-time throughout the meeting to assist with configuring and running various servers.

In the end, this team was able to solve many problems quickly because of the extra support.

Recommendations

The team learned quite a few lessons during this period, including:

1. Lots of support reduced the time in locating and resolving problems.
2. Wireless inside buildings is very difficult because of barriers; thoroughly testing both primary and contingency plans is necessary.
3. Test, test, test. The backup wireless system was, equipment-wise, tried and true but the actual location of access points must be tested for each new meeting site.
4. Wireless registration is *very useful* if registrants provide accurate information.
5. There are inherent limitations to wireless technology in large, closely-spaced groups of concurrent users. Don’t expect perfection! Instead, try to tune to the best of your abilities.
6. Don’t be afraid to experiment with new technologies and approaches to wireless – but be sure to have a well-understood backup system or contingency plan in place, first!