Design Project FAQ

6.033 2018
Last update: 4/24/2018, 11:30am

As we receive more questions about the DP, we may change the structure of this document, to make it easier to find information.

If there is a conflict between technical realities and the DP spec, which is the authoritative source?

The DP spec. In this project, we've simplified some protocols, and made changes to others to highlight particular trade-offs that we want you to deal with (for example, our version of the BLE Communications Protocol is not exactly how BLE devices communicate, and is capable of higher speeds than the actual protocol is).

Project Scope

Can we have a map of where smart devices are located?

You are welcome to look at the floor plans of different buildings on campus, but we aren't providing a map of smart device locations. Remember that, while you're designing for MIT's campus, you should think about whether your system could be used elsewhere (e.g., on other campuses). If your design depends heavily on the precise location of smart devices, it's not very extensible.

What is defined as "main campus"?

Assume that it's roughly the office/classroom buildings at MIT, not the dorms/living groups/sororities/etc. Our intent here is just for you to not have to think about whether living spaces should be handled differently than working spaces.

Also remember that if your design depends heavily on the precise location of smart devices, or on the precise size of what constitutes the main campus, it will not be particularly extensible.

Networking

Repeaters don't advertise themselves with beacons. How would a gateway learn of the repeater's existence?

We haven't set the repeaters up for you as beaconing devices. But you could choose to do that; you just have to explain how frequently/what they broadcast. (You could also choose some other method. Basically, we want you to design and describe this process.)

Are we allowed to modify beacon formats in any way?

For smart devices, no; they're set to beacon out only their IDs. For repeaters/gateways, sure; you are in control of the node-discovery protocol there. You could set them to beacon out some additional information.

Is bandwidth shared between uploading and downloading for gateways, repeaters?

Assume that the bandwidth is a total. E.g., 16Mbit/s upload/download combined for gateways.

Can the smart devices send a message of its own volition to the FCS through our routing framework? What about repeaters?

Yes, you can have the smart devices initiate the sending of a message. You'll need to provide all of the details (message format, how that message is routed through the network to the FCS, etc.).

Repeaters are also able to send packets of their own creation (again, you describe the entire process, this is allowed.)

(Note that this means they're technically capable of more than just repeating information.)

What is the total network bandwidth going into the FCS?

You can assume there's a total of 1GB/s into the FCS. (Gateways have a wired connection to FCS, but it's not a direct wired connection. There's a wired network between the gateways and the FCS.)

Since we are transmitting over the air for the BLE protocol do we have to deal with interference at the receiving device?

Don't worry about that for this project. You can assume that there is a protocol in place to mitigate that type of interference.

Miscellaneous

Can the motion detectors turn lights on or off without talking to the FCS, or does the FCS have to initiate any request to turn lights on or off?

As long as you describe the entire process by which this happens (what messages need to be sent where, e.g.), yes, this is possible. Your system still has to support devices receiving commands from FCS, though.

Is 1KB 1000 bytes, or 1024 bytes?

There is actually a standard in systems: for networking speeds, 1KB = 1000 bytes. For storage, 1KB = 1024 bytes.

Does facilities need all 5 FPS when in crisis mode?

No, it's okay to still have just 1 frame/sec. The primary difference is that that frame has to be delivered in real time.

What happens when there are power outages?

For now, we've asked you deal with a few different types of failures: the FCS being down for maintenance (one of the use cases), and BLE+ repeaters and gateways failing (that's a property of those components). You should design your system with those failures in mind, but you don't need to design a system to handle a full power failure (or, say, power failure in a large area of campus like an entire building).

Should we be concerned with malicious users logging into the FCS and issuing commands?

In terms of your actual design, no; the main reason being that we have not taught you any techniques to deal with those problems yet (and so can't expect you to design a system that uses them).

In terms of the security thought experiment, yes; you should consider how you might prevent this (but you do not have to specify a full design of your system to support it).

In the real world, malicious users would certainly be a concern. If you want to think about how to handle that, and include some solution in your design, that's fine so long as your design still meets all of the other requirements.

Will the smart device ID on the device be same as the one stored in the database?

It's okay to assume that the smart device ID and the ID stored in the database will be the same (just perhaps not the ID you wanted that device to be set to).

Our intent is this: since humans are needed to set the smart device ID, it's reasonable to imagine that there might be some error in that process. We'd like your schemes to be able to handle that error, and somehow recover. I.e., if your routing scheme relies on each smart-device ID being constructed in a very specific way, what happens when that setting process is incorrect?

Given that context, it's certainly reasonable to *also* imagine that there would be errors in the database, and that smart devices might not reflect the IDs in the database. However, that adds an additional problem for you to solve (recovering from an incorrectly recorded ID). If your system can handle both of these types of errors, that's certainly nice, but we're also happy to limit you to just the first error.

MIT OpenCourseWare
https://ocw.mit.edu

6.033 Computer System Engineering
Spring 2018

For information about citing these materials or our Terms of Use, visit: https://ocw.mit.edu/terms