

CASE STUDY • NETWORK

Visitors on the network, *never on your systems.*

A representative build: how a multi-building facility went from one flat, fragile network to a documented one where guests never touch staff systems.

Representative case study. Details are generalized; specifics vary by site.

Campus stabilized

Result

Fully isolated

Guests

Documented

Handover

THE SITUATION

One flat network doing too much

Several buildings, staff, visitors, and equipment all sharing one flat network and consumer wi-fi.

Coverage was patchy, with dead zones between buildings and drops at busy times. Worse, there was no separation. A visitor's laptop and the machine holding sensitive records sat on the same network, one hop apart. Nobody could say what was connected, and when something broke there was nothing to work from but trial and error.

What was at stake

- **Security** — guest devices able to reach internal systems.
- **Reliability** — dead zones and drops interrupting the work.
- **Accountability** — no map, no fast way to fix anything.

THE BUILD

Separated, and documented

One dashboard, clean separation, and a diagram they keep.

We deployed a full Cisco Meraki stack across the buildings, managed from one place, so the whole facility is visible and controllable at a glance.

PIECE	ROLE
Security appliance	Firewall, routing between buildings, and site-to-site links
Switches	Wired backbone with power for the access points
Access points	Wi-fi that holds up across the whole campus
Segmentation	Separate networks for staff, guests, and equipment

The separation that mattered

Guests now get internet and nothing else. They cannot see or reach a single staff device or internal system. Staff, shared equipment, and building systems each sit on their own segment, so a problem in one place stays there.

THE OUTCOME

Stabilized, and finally mapped

How it went in

- Building by building, out of hours where we could
- Cut over with staff barely noticing
- Tuned coverage after go-live on real usage

What changed

- Wi-fi that holds across the campus
- Visitors fully isolated from staff systems
- One dashboard showing everything connected
- A documented network, not a mystery

Every deployment ships with documentation. The layout, the rules, and a diagram, in editable form and yours to keep. You are never tied to one provider to understand your own network.

Talk to us

If your network grew faster than anyone documented it, email info@makingitworc.ca.