# Conceptual Overview (Networking Side)

### Describing a dual-subnet/VLAN setup:

* **10.1.x.x (or 1.1.x.x)** = *public-facing* VLAN (accessible to students + internal school network)
* **10.2.x.x (or 1.2.x.x)** = *private, isolated Host Node network* for 3D printing (not internet-facing)

### The goal:

* Students **submit jobs from the public side (1.1.x.x)**
* **Host Nodes stay shielded** from external access (no internet, reduced attack surface)
* Only **controlled internal routing or proxy access** allows communication across these subnets

### This Setup Is:

|  |  |  |
| --- | --- | --- |
| **Goal** | **Achievable in Your Plan?** | **Explanation** |
| Isolate Host Nodes from Internet | ✅ Yes | VLANs + no routing out from 10.2.x.x will enforce this |
| Allow Students to Submit Prints | ✅ Yes | Done via reverse proxy (e.g., NGINX on school network side) |
| Assign Static IPs to Host Nodes | ✅ Yes | Either via switch-side DHCP, MAC reservation, or static config |
| Let Admins SSH into Host Nodes | ✅ Yes | If routed via firewall/proxy, or via a jumpbox on 10.1.x.x |
| Keep Students from accessing Host OS | ✅ Yes | Use VLAN separation, reverse proxy rules, and firewall ACLs |

# How This Is Typically Implemented

## 1. VLANs on the Switch

You divide your ports:

* **Ports 1–24** → VLAN 10 (10.2.x.x) → Host Nodes
* **Ports 25–48** → VLAN 20 (10.1.x.x) → School network / student uploads

On the Cisco 2960-X, this might look like:

vlan 10

name PRIVATE\_PRINT\_NET

vlan 20

name STUDENT\_ACCESS

interface range gigabitEthernet1/0/1 - 24

switchport mode access

switchport access vlan 10

interface range gigabitEthernet1/0/25 - 48

switchport mode access

switchport access vlan 20

## 2. Reverse Proxy Bridging the VLANs

A system (possibly a Raspberry Pi or VM) **connected to both VLANs** will:

* Serve as a **reverse proxy (NGINX or Apache)**
* Let students at 10.1.x.x access OctoPrint UIs located at 10.2.x.x

Nginx:

# On the proxy at 10.1.1.100

location /printer1/ {

proxy\_pass http://10.2.1.4:5000/;

}

Perl:

# On the proxy at 10.1.1.100

location /printer1/ {

proxy\_pass http://10.2.1.4:5000/;

}

This allows:

http://10.1.1.100/printer1/ → proxies → http://10.2.1.4:5000/

So students never even “see” the private Ips.

## 3. Firewall and Routing Rules

To secure this:

* The **switch or upstream router** enforces:
  + No internet access from 10.2.x.x
  + No inbound SSH/web access *to* 10.2.x.x from 10.1.x.x (except from proxy/admin machines)

### Alternate Names for This Topology:

* "DMZ-Style" subnet separation
* Reverse-proxy shielded subnet
* Air-gapped service VLAN with upstream gateway

### Bonus: Integration with Static IP Binding

If you assign each Host Node a known static IP (e.g., via port-based DHCP or MAC reservation), then:

* Your reverse proxy can always point to the right IP
* Your print farm will be more robust and scalable
* You won’t need mDNS or service discovery

## Pitfalls to Watch Out For

|  |  |  |
| --- | --- | --- |
| **Issue** | **Risk** | **Fix** |
| **Misconfigured VLANs** | **Hosts can't talk** | **Confirm correct switchport mapping** |
| **Proxy server is single point of failure** | **No web UI access** | **Consider HA or a failover proxy** |
| **Exposing internal IPs** | **Security concern** | **Use proxy rules and ACLs carefully** |
| **Time sync issues** | **Breaks HTTPS/SSL or logs** | **Ensure NTP is working on both VLANs** |