Mesh VPN in a Retail Bank Branch Delivery Platform

Alex Feiszli
Tom Parette
November, 2021

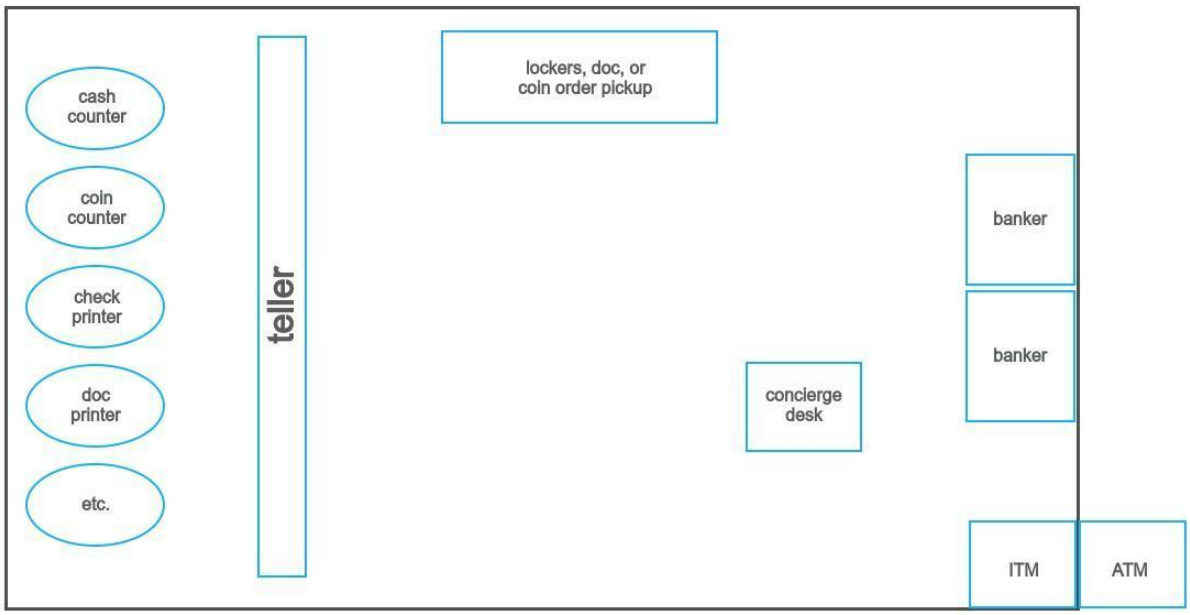
Photo by Christian Wiediger on Unsplash

Table of Contents

Abstract

In this paper, we outline the networking issues faced at bank branches today. We discuss how these network limitations prevent modernization, and how any solution must eliminate these limitations without opening banks to undue risk. Finally, we discuss the mesh VPN as an ideal candidate solution and outline a few example scenarios for how this might look like in practice.

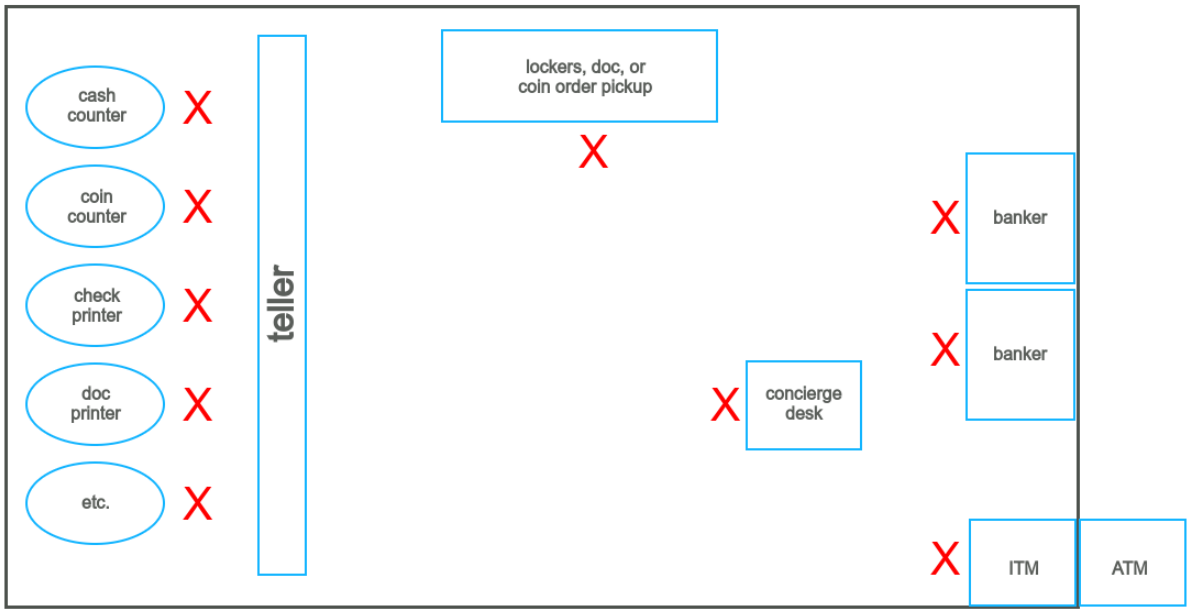
Introduction: The Average Bank Branch is Siloed



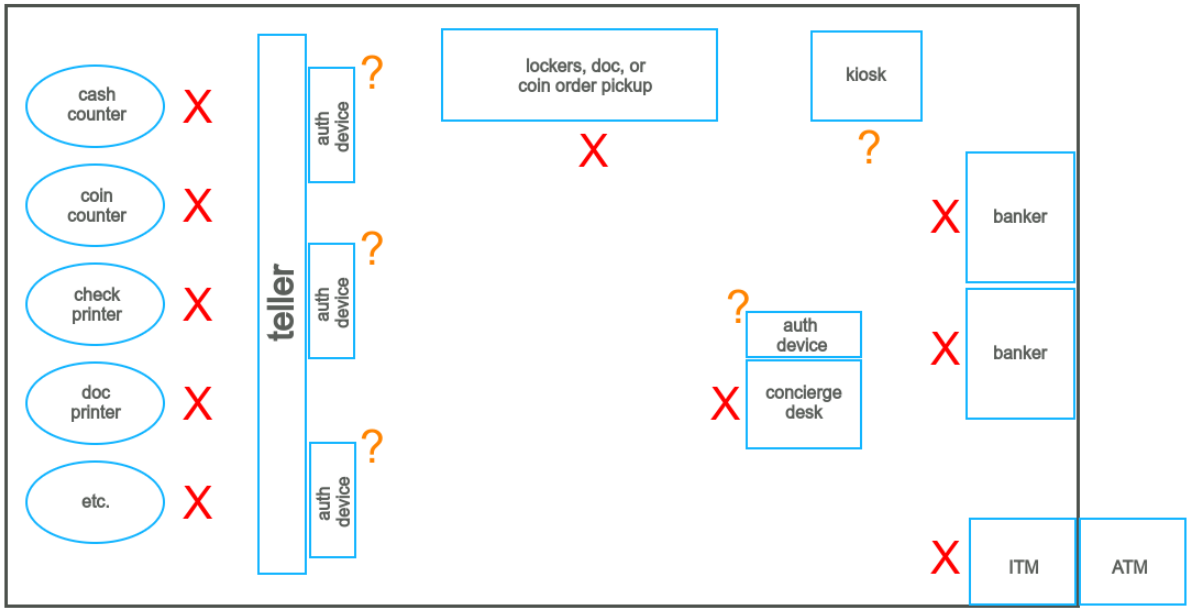
The average person can print documents from any computer in their house, buy goods and services from their phone, and file important documents online. This is not the case at the average bank branch.

The branch consists of many siloed activities, which are not easily performed from different physical locations or devices. Consider a check printer, which can only be accessed directly. If there are many tellers in one branch, they all need to go over to the same machine and queue up the job.

The same goes for the document scanner, the coin counter, the cash counter, and numerous other devices. Each may seem like a small inconvenience, but when taken in aggregate, it leads to hours of additional labor.



These network limitations exist in the current state, but also extend to any next-gen patterns a bank may wish to implement. If a bank wants to adopt Kiosks at all branches, those Kiosks must have direct access to the appropriate services over the network. The same goes for giving tellers tablets or implementing NFC readers and Beacons.



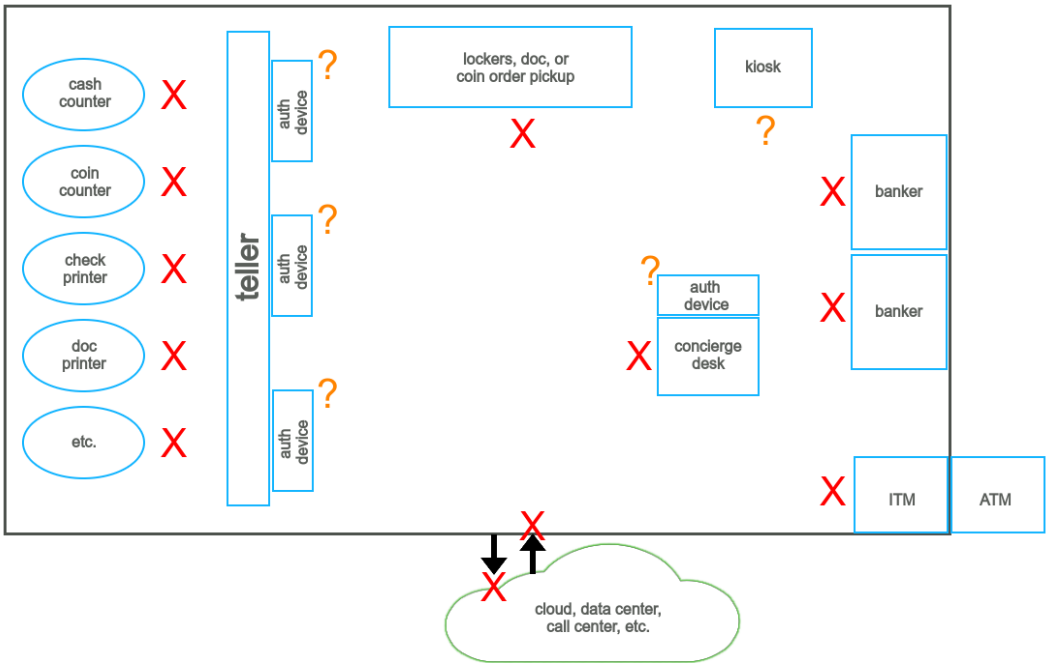
In addition to intra-bank networking, many of these next-gen devices also require communication with out-of-bank services. For instance, a Kiosk might need to connect with a contact center for enhanced services.

All these practices are common in retail, but almost unheard of in banking, and in large part, the network presents the severe limitation.

Even further, as large businesses move many of their services into the cloud, it becomes necessary to connect bank branches with these cloud services. This can happen in two directions:

Central access to branch services (Edge Computing): In this case, a support center might need to reach a bank, or perhaps some cloud application must process data that is held only at a bank location. In these cases, you must have a machine running at the branch that is accessible from outside.

Branch access to central services (Cloud Computing): In this case, a teller, Kiosk, or someone/something else at the branch must use an application that the bank (or a vendor) hosts in the cloud. In these cases, you need a secure way to access to that external service.



In all these cases, the fundamental problem is restricted network access.

Tellers cannot reach printers from their computers, Kiosks have no way of connecting to central services, and call centers can't reach into a bank branch. If we want to remove these silos, we must first remove the network silos.

Why Can't Banks Have Integrated Networking Today?

While bank devices must have network connectivity to enable modern patterns, there are good reasons this has not been commonly implemented up to this point.

#1: Networks can be unreliable

If you have direct connectivity to a required service (printer, scanner), then you are never reliant on the network. If you make these services available over the network, your router might go down, and then you lose the ability to perform these services at the branch. Bank branches cannot lose access to the services they need, so they cannot rely on a network that might go down.

#2: Open networking is dangerous

Allowing access to devices and services over the network opens a branch to many new vulnerabilities. In a year of renewed focus on cybersecurity, this is a larger concern than ever before. If a bad actor gains access to a trusted device inside the branch, with the wrong setup, this enables all sorts of malicious activity. Bank branches cannot allow malicious activity to occur.

#3: Proper networking is hard

It is possible to implement networking that is both reliable and secure. When networking is absolutely required (e.x: ATM's), banks make sure there are layers of redundancy in place to avoid outages. They also configure the network so that only trusted parties have access. This requires a big investment of time and resources.

A network engineer must implement a proper network configuration, and this can take weeks, months, or in some cases even years. Worse still, these designs tend to be inflexible, meaning if a device such as a tablet is added to, or removed from the network, the administrator must make sure all the security rules and firewalls are appropriately configured.

Flexible systems require flexible networks, but banks cannot afford to have a network engineer as the bottleneck for each of its thousands of branches.

So, what is the solution to these issues?

The Solution must be Reliable, Secure, and Painless

We require a solution that can automatically configure secure connections between devices while being highly available. This solution should be virtual and remotely configurable to avoid local bottlenecks. The network must be properly secured, and ideally should be “zero trust”, meaning only the minimal network permission is ever granted to any service.

We must also consider some additional limitations:

Handle many protocols, ports, and device types: Many solutions are focused on the application layer, or only work for certain devices. We need a general solution that will work across many device types (Printers, Tablets, Kiosks) and many protocols (database, https, ssh).

Handle many topologies: We need to forge 1-N, N-1, 1-1, and N-N connections in different scenarios, as needed. A cloud service may need to access all the bank branches. A teller may only need to access a check printer. Tablets may all need access to each other. The solution must be flexible enough to handle these connections as needed.

Our overall checklist for a solution looks like this:

- Secure
- Virtual
- Remote operations
- Flexible / Dynamic
- Highly available
- Zero Trust

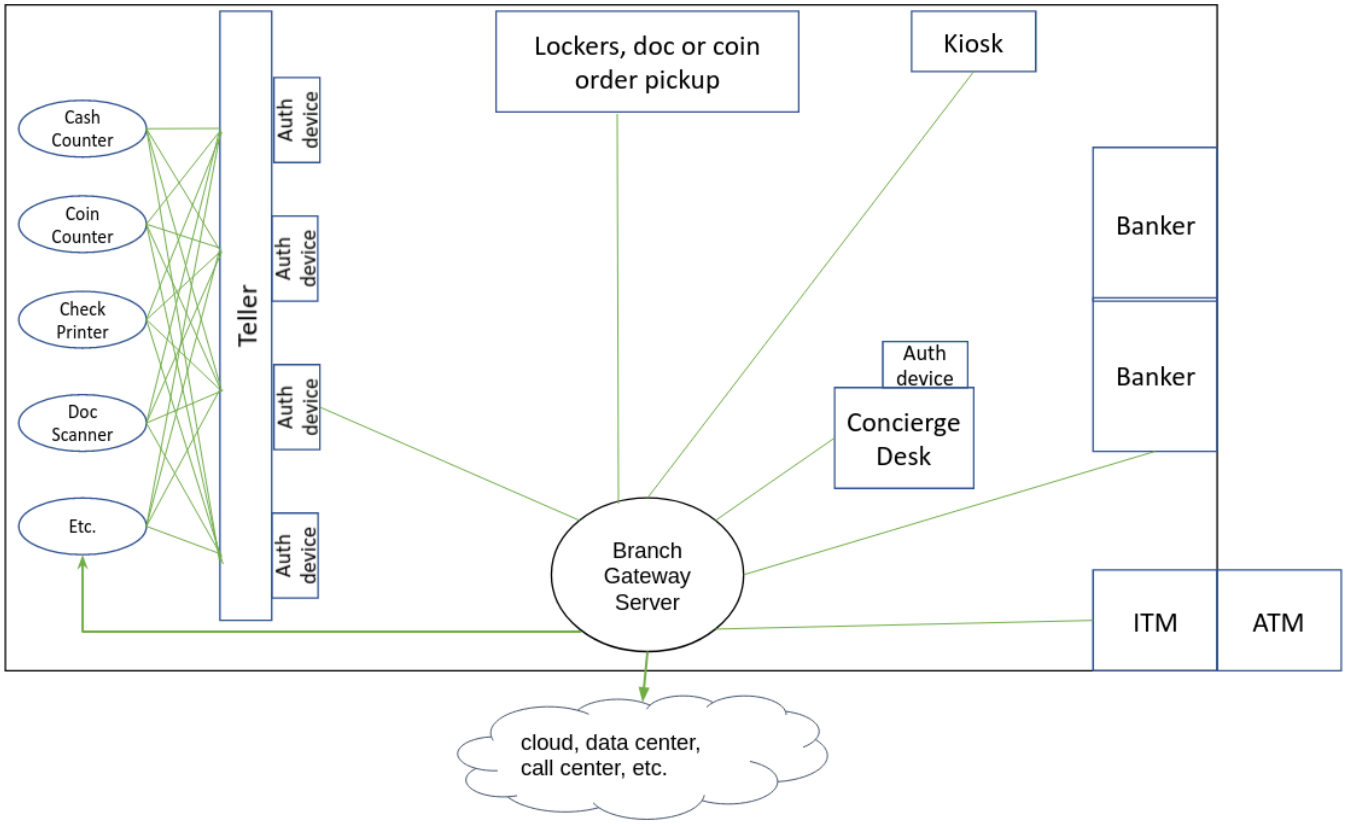
Mesh VPN’s Provide the Answer

What is a mesh VPN? In simple terms, think of it as a regular network, but virtualized, and encrypted. If a bank branch has a regular router-based local network, the mesh VPN sits on top of it and controls access to both resources on the network and on different networks.
Because it is virtual, it is highly configurable and dynamic. It can be managed remotely, and because it is virtual, it can be built with layers of redundancy such as relays.

Because it is encrypted, it is highly secure, and depending on the solution, you can provide fine-grained controls on what machine can access which other machine, providing a zero-trust network.

A mesh VPN enables branches to create “groups” of devices that have access to each other, any of which can be booted out at any time. This creates a sort of “walled garden” for applications and services.

For instance, only a teller should be able to access a check printer in the branch. The mesh VPN can group together the “printer” devices with the “teller” devices and leave out everything else. Simultaneously, maybe a Kiosk and a Teller should both be able to reach a cloud service, but only via some other “router” machine. This can be a separate group. The topologies are entirely arbitrary and can be configured remotely and on the fly.



Real World Scenarios

Let us consider a few examples of a mesh VPN in a next-gen banking scenario.

#1: NFC

NFC readers have many use cases that may be applicable to a next-gen bank branch. The NFC reader is local, physical device located at the branch, however, it may need access to a cloud-based authentication service, to identify the user. A common pattern would be to have only **one device** with access to the external, cloud-based services. Call it an “edge router”. This could be any device: a Windows computer, a raspberry pi, or a real, physical router.

In any case, the NFC reader will need to access the “edge” device, which needs to have access to the cloud service. Your mesh VPN will automatically configure a direct, encrypted link to the edge machine, and tell the NFC reader that any request to the cloud service needs to go through this machine. Any attempt to access the cloud service over the public network would fail.

#2 Mortgage fulfillment

Although loan origination is a centralized business process supporting multiple banking channels, the fulfillment portion of the loan will be a hybrid local and centralized business process. Many of the steps in the fulfillment process will access external (non-branch) capabilities in conjunction with local functions such as document prep.

In this case, you might configure a direct link between the cloud service and one of your local machines. It could be an “edge router” as in the above case, or a direct connection to the machine with the data. The same goes for the “cloud” side of the equation. There might be many of such cloud software stacks, all of which must route through a given machine. In any of these cases, the mesh VPN can be configured to decide which machines can connect to which other machines, and which machines they must route through to reach them. This connectivity can even be automated on the fly, so that the cloud software only has access to the local data when needed.

#3: Teller Device

Let’s say that we want to enable all tellers at a branch with tablets. They should be able to use these tablets to do many things, whether it’s processing some data, or accessing a printer, scanner, or counter. The mesh VPN can provide direct peer-to-peer connections for all these devices. From the teller’s perspective, it’s just a simple connection. But under the hood, all the traffic is being encrypted and direct links are configured.

Even better, redundancy can be set up. Let's say the bank relies on a single router. Some backup internet connection can be configured, and if the primary router is having issues, the connections can fall back to a secondary method of communication.

Recommendation: Use a Mesh VPN

Bank branches can achieve flexible, secure, and dynamic networking using a mesh VPN.

In the previous section, we outlined a few examples, but ultimately, think of the Mesh VPN as a way to do regular networking, but virtually, remotely, and encrypted. It opens a lot of freedom for the bank to implement new patterns, while minimizing the impact at the bank branches.

No one likes to think about networking. Ultimately, it should be an afterthought. Unfortunately, with concerns around safety and reliability, it cannot be ignored. A mesh VPN allows banks to implement next-gen banking patterns with best practices, while incurring the minimal toll on their existing infrastructure.

While this paper outlines the "what" and the "why", it does not prescribe a "how". In part two of this discussion, we will walk through how to implement such a design in practice at retail bank branch locations, in a way that is automated and highly available.