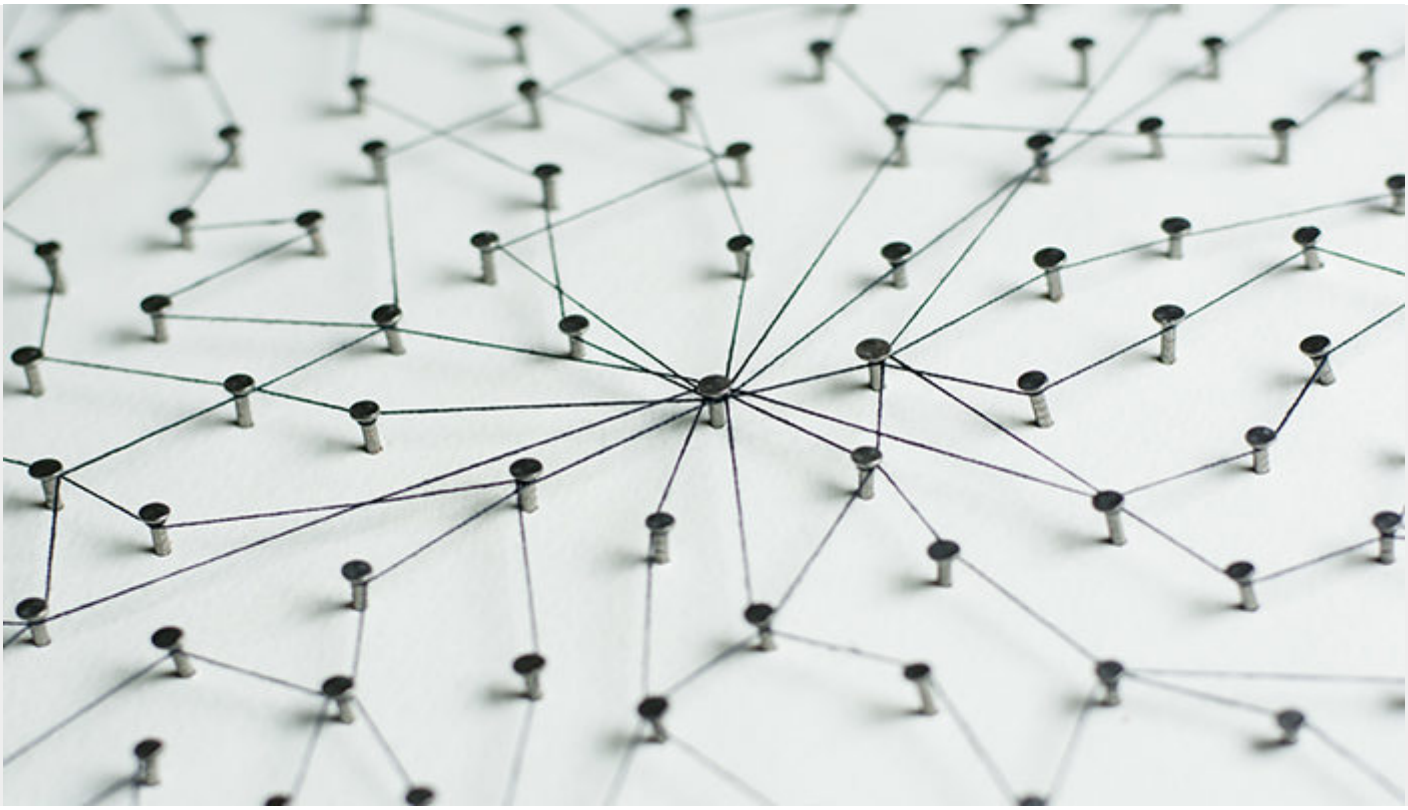
BUILDING AN IT NETWORK FOR A REMOTE FACILITY



Let's assume your organization is expanding. It's adding a new processing facility or distribution center. As the IT Operations (IT Ops) group, your job is to add this new location to your corporate network, so they can enter, process, and ship orders, as well as communicate with headquarters vendors, and customers.

Where do you start, and how soon can you get that new location on the network?

In today's post, let's look at some of the challenges and issues you'll need to consider when adding a new location to your network.

The checklist

Figure 1 shows my basic checklist for what's usually needed to create an IT network for a remote facility (not headquarters). This network runs VMWare virtual machines (VMs) for Windows domain controllers, file and print serving, and other special purpose servers. It also accesses production and email servers either in the cloud or at another facility. This checklist shows the basic requirements to form the nucleus for the simple network described here. The rest of this post describes each item in the network checklist in more detail.

Figure 1: A basic checklist for creating an IT network in a remote facility

Equipment or service needed	Needed (yes/no) and notes

Secured equipment room

Electrical service with redundant circuits, as needed

Universal Power Supplies (UPSes)

Generator

Computer racks with shelves

Fireproof backing board for one or more walls

Air conditioning

Patch panels

Switches and routers

Fire suppression equipment

Telecommunications lines

Ethernet cabling to equipment room for all office and warehouse locations

Firewall setups

IDF (Intermediate Distribution Frame), patch panels, and switches in the warehouse or manufacturing space for warehouse equipment beyond the maximum Ethernet transmission distance

Ethernet cabling for connecting all equipment

Cable or Internet modems for telecom lines (usually vendor provided)

Wireless modems for wireless network

Production servers hosted at facility (application, domain authentication, file and print serving, email, special purpose servers)

Telephone systems, if not using VoIP

Phones

Computing devices (desktop, laptops, tablets, terminals, other devices)

Wireless scanning for inventory and production activities

Time clocks

Office printers and copiers

Warehouse printers for multi-part forms and older green-bar printing

Internet of Things (IoT) devices

Vendor-supplied devices

Beginning pieces

The first thing you'll need is a secured equipment room within your location. For a remote facility, the equipment room doesn't have to be big. It just needs to house all the equipment you'll need to host your local network. The basic requirements of a remote location equipment room include:

- *Locked door* with a keyed, card reader, push button, or a biometric entry system, to prevent unauthorized access and to provide for climate control.
- *Electrical service* for powering all the equipment. Be sure to install redundant circuits for servicing all equipment with redundant power supplies or power distribution units (PDUs). Inventory all your equipment to insure everything requiring special plugs or voltages can be powered with the service you're ordering. Redundant circuits should be on different electrical boxes and if available, different services.
- *Universal Power Systems (UPSes)*¸ to provide for continued operation in the event of a brown-out or short power outages. For a small remote setup, two UPSes may be enough. Be sure that redundant power supplies on the same machine are plugged into two different UPS systems (one plug in each UPS to protect against a UPS failure).
- *Generator (if called for)* to power the computer room, in the event of a long-term power outage.
- *Fireproof backing boards for one or more walls*, to allow for the installation of telecommunication modems, jacks, punch-down blocks, telephone systems, or other network inputs.
- *Computer racks with shelves* to mount all the equipment. Servers, UPSes, switches and some other basic network equipment can be mounted in the rack. Equipment that can't be rack mounted can be stored on the shelves or attached to the fireproof backing boards.
- *Air conditioning*, for climate control outside of the normal office heating and cooling system
- *Patch panels* for connecting all your infrastructure and client equipment into the equipment room.
- *Any necessary fire suppression equipment*. This could range from a simple fire extinguisher all the way up to a full-blown fire suppression system.

Telecommunication lines

Regardless of where you host your servers (locally or in the cloud), you'll still need telecom lines for production server access, Internet access, telephone, and other special service lines. Be sure to spec out and order your telecom lines early in the process, as installation can take many weeks. Telecom installation can consist of one or two phases: 1) Delivery to the Demarcation Point (DMARC) into the building, which may or may not be in the equipment room; and 2) DMARC extension to the equipment room. Either phase can consist of additional cabling through your new location to the Computer Room. If you're renting a location, you may also have to get permission from your landlord to run the new lines.

Once the telecom lines are in your equipment room, you'll want to mount modems from your telecom provider on either the fireproof backing board or in the rack.

Basic networking equipment and cabling

For a new location, you'll also need the following basic networking equipment.

- *Ethernet cabling and network jacks for all office and warehouse locations*, to connect your facility locations (offices, printer rooms, warehouse locations) to the patch panel in the equipment room. Be sure each cable drop at user locations has at least two Ethernet jacks to accommodate one or more wired devices and one phone. Don't forget that warehouse lines need to be run through the warehouse ceiling (which can be 20 feet or higher) and dropped at their locations, which will increase their maximum Ethernet transmission distance.
- *One or more firewall setups (depending on how many Internet lines you're running)*, for protecting your network from unauthorized access.
- *Switches and routers for connecting workstations, servers, network equipment, and telecommunications lines together*. Switches allow the different devices and servers on your network to reach each other (or isolate different devices and servers from each other). Routers and gateways provide the basic policies and rules that route traffic to servers, Internet lines, and other locations inside and outside your network. Devices outside the equipment room will reach the equipment room through a port on the patch panel, which can be connected to a switch via a short Ethernet cable, while devices inside the rack are connected directly into switch. The router is also connected to a switch, and the router regulates and directs network traffic to its destination. If you're also setting up a wireless network that feeds into your switches, make sure the switches have as many power over Ethernet (Poe) ports as you need, so that you won't have to run electrical to power your wireless modems, wherever they are installed (usually in or on the ceiling).
- *An Intermediate Distribution Frame (IDF) in the warehouse*. An IDF is generally a locked cabinet in the warehouse that houses at least two components: 1) a patch panel where other warehouse equipment can connect to the IDF; and 2) a switch that can route equipment from the warehouse patch panel to the main switch in the equipment room. Since warehouse Ethernet connections may not be able to connect to the equipment room patch panel (because they are out of the maximum transmission distance for Ethernet cable, 100 meters or 328 feet), they can connect to the patch panel in the IDF and then be routed to the equipment room through the IDF switch, which is usually hardwired to the equipment room patch pane. An IDF isn't needed for all warehouses, but it's useful in larger warehouse that can't reach the equipment room in one Ethernet run.
- *Lots of Ethernet cables*. You'll need short and medium Ethernet cables for attaching all devices, servers, network equipment, etc., to their local Ethernet jacks. Since patch panels and switches are generally in the same rack or IDF, you'll need plenty of short Ethernet cables (2-3 feet) to attach each patch panel port to the nearest switch.
- *Cable or Internet modems for attaching your incoming telecom lines to your network*. Your telecom service provider generally provides the modem to attach to their incoming service line.
- *Wireless modems for your warehouse and office*. Your wireless modems should have Power over Ethernet (PoE) ports for powering the modem using its Ethernet line rather than an electrical outlet. People generally use a single wireless modem (or a clustered wireless setup) for four purposes: 1) Connectivity movable wireless warehouse equipment (such as scanners and telephones) to the network: 2) Allowing visiting employees with laptops to access the company network; 3) Setting up a guest network to provide Internet access to your vendors,

guests, and business partners, without allowing their devices to access your domain; and 4) Providing a network bridge between two wireless modems to extend your network to another location that' s impossible or impractical to wire. Wireless modem placement can be an art form in a warehouse or production facility, where racks can be stuffed with product from floor to ceiling (blocking signal reception). Plan carefully for wireless modem placement in a warehouse environment.

And now the stuff you want to connect

At this point, you'll have all the basic infrastructure and equipment you need to start setting up your remote location's network. Now it's time to start filling it with the servers and devices that connect over the network. Here's a starter list of items you'll want to install in your equipment room, office, or warehouse for servicing your customers.

- *Servers for domain authentication, file and print serving, or special purpose servers, such as time clock servers, email servers, backup servers, etc*. Using a product such as VMWare on a large Intel server, for example, one server can be partitioned into several VM to accommodate most of your server needs.
- *Telephone systems and phones*, either a physical phone system or a Voice over IP (VoIP) system.
- *Special purpose appliances, such as Web filtering servers, security appliances, etc.*
- *User devices, such as PCs, laptops, tablets, and cell phones*
- *Wireless scanners for order processing, warehouse inventory, item tracking, and other barcode processing.*
- *Time clocks*
- *Office printers and copiers for printing plain paper documents and reports, and for scanning and emailing documents.*
- *Warehouse printers for printing multi-part forms and older large green-screen format reports*
- *Internet of Things (IoT) devices for collecting and analyzing data*.
- *Vendor-supplied devices that allow vendors access to machines in your facility*

Cloud, and MSP considerations

This checklist changes somewhat depending on whether the services and applications your users need to access are in the cloud. For cloud access, you'll still need most of the items described in the ***Beginning Pieces, Telecommunications lines,*** and ***Basic networking equipment and cabling*** sections. You will also need any item in the ***And now for the stuff you actually want to connect*** section that requires local installation (printers, scanners, time clocks, users, PCs, IoT devices, etc.). Even when every application your facility needs is hosted in the cloud, you will still need to set up a local infrastructure that allows your users and devices to access the cloud. So, the task of setting up a remote facility network gets a little easier with the cloud, but you'll still need most of the things listed in this checklist.

I hope this checklist helps you with any remote facility planning you need to do.