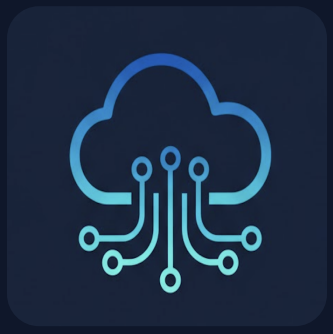

Penn Tech Solutions

Your Local IT Partner for Small Businesses

TECHNICAL REFERENCE

Small Business Network Configuration Plan

Security & Infrastructure Standards for Retail, Restaurant & Service Businesses

Greater Philadelphia Area
Montgomery, Bucks, Chester & Delaware Counties

info@penntechsolutions.com | (215) 555-1234

January 2026

Executive Summary

This document outlines the recommended network infrastructure configuration for small businesses such as pet shops, barber shops, salons, restaurants, and retail stores. It serves as a benchmark to assess your current network against industry best practices and identify critical security gaps.

Why This Matters

Small businesses are the #1 target for cyber attacks. 43% of all data breaches involve small businesses, and 60% of small businesses close within 6 months of a cyber attack. A properly configured network is your first line of defense.

Who This Document Is For

Retail Stores

Pet shops, boutiques, gift shops, convenience stores

Food Service

Restaurants, cafes, bakeries, food trucks with fixed locations

Service Businesses

Barber shops, salons, spas, auto shops, dry cleaners

Professional Offices

Small medical/dental, law offices, accountants, real estate

Network Complexity Levels

Basic (1-5 Employees)

Single location, basic internet needs, 1-2 POS terminals

Standard (5-15 Employees)

Advanced (15-50 Employees)

+ Business firewall
+ Single managed switch
+ 1-2 access points
+ Basic VLAN separation

Multiple workstations, security cameras, moderate traffic

+ UTM firewall with subscriptions
+ PoE managed switch
+ 2-4 access points
+ Full VLAN segmentation

Multiple departments, high availability needs, complex security

+ High-availability firewall
+ Stacked/redundant switches
+ Controller-based WiFi
+ Backup internet failover

01 Internet Connection

Your internet connection is the foundation of your network. Business operations increasingly depend on reliable connectivity for POS systems, cloud services, and customer WiFi.

Primary Connection Requirements

Type	Business-class fiber or cable (not residential)
Speed (Minimum)	100 Mbps download / 20 Mbps upload
Speed (Recommended)	250+ Mbps download / 50+ Mbps upload
SLA	Business SLA with guaranteed uptime
Static IP	At least 1 static IP address

Why Business-Class Internet?

Business connections include SLAs (Service Level Agreements) guaranteeing uptime and faster repair times. Residential service has no guarantees and repairs can take days. The cost difference is often only $20-50/month.

Backup Connection (Recommended)

For businesses where downtime means lost revenue, a backup internet connection provides automatic failover when your primary connection goes down.

- Different provider than primary (different infrastructure)
- Can be lower speed (50 Mbps sufficient for failover)
- 4G/5G cellular backup as alternative
- Automatic failover configured in firewall

02 Firewall / Router

The firewall is the most critical security device in your network. It controls all traffic entering and leaving your business. Consumer routers are NOT adequate for business use.

Feature	Consumer Router	Business Firewall
Stateful Packet Inspection	Basic	Advanced
Intrusion Prevention (IPS)	No	Yes
Content Filtering	No	Yes
Malware Protection	No	Yes
VPN Server	Limited	Full
VLAN Support	No	Yes
Threat Intelligence	No	Yes
Reporting/Logging	Minimal	Comprehensive

Recommended Firewall Brands

- SonicWall TZ Series
- Fortinet FortiGate
- Cisco Meraki MX
- Ubiquiti Dream Machine Pro
- WatchGuard Firebox

03 Network Switch

The network switch connects all wired devices in your business. A managed switch is essential for proper network segmentation and security.

Managed Switch Requirements

- Managed switch with VLAN support
- Gigabit ports (minimum)
- PoE+ for access points and cameras
- Port security and 802.1X support
- Link aggregation capability
- Remote management interface

Port Planning Guide

POS Terminals	1 port each
Workstations	1 port each
Printers	1 port each (wired preferred)
Access Points	1 PoE port each
Security Cameras	1 PoE port each
DVR/NVR	1 port
Spare Ports	20% headroom recommended

04 Structured Cabling

Proper cabling infrastructure ensures reliable connectivity and makes future changes easier. Poor cabling is a common source of intermittent network issues.

Cable Standards

- Cat6 minimum (Cat6a preferred)
- Plenum-rated for ceiling runs
- Terminated at patch panel
- Labeled at both ends
- Tested and certified

Best Practices

- Separate from electrical runs
- No sharp bends (minimum radius)
- Properly supported in ceiling
- Avoid running near fluorescents
- Document all cable paths

Common Cabling Mistakes

Running network cables alongside electrical wiring causes interference. Using Cat5 instead of Cat6 limits speeds. Loose connections at patch panels cause intermittent issues that are hard to diagnose. Invest in proper cabling installation upfront.

Recommended Switch Brands

Cisco CBS Series | Ubiquiti UniFi | Netgear Pro | Aruba Instant On | Juniper EX Series

05 WiFi Infrastructure

Business WiFi requires more than a consumer router. Proper coverage, security, and network separation are essential for protecting your business while serving customers.

Business WiFi Requirements

- Business-grade access points (not consumer routers)
- WPA3 encryption (WPA2 minimum)
- Separate SSIDs for business and guest
- Band steering (2.4GHz/5GHz)
- Client isolation on guest network
- Centralized management

Required Wireless Networks (SSIDs)

BusinessName-Private

Employee Only

For employee devices, POS tablets, back-office computers. WPA3-Enterprise or WPA2-PSK with strong password (20+ characters). Connected to business VLAN.

BusinessName-Guest

Customer Access

For customer internet access. Client isolation enabled (guests can't see each other). Bandwidth limited. Captive portal optional. Connected to guest VLAN with internet-only access.

BusinessName-IoT

Hidden SSID

For smart devices, thermostats, smart displays. Hidden SSID (not broadcast). Isolated VLAN with restricted internet access. No access to business network.

Access Point Placement

Small Retail (1,000-2,000 sq ft)	1-2 access points
Medium Retail (2,000-4,000 sq ft)	2-3 access points
Restaurant (2,000-5,000 sq ft)	2-4 access points
Warehouse/Open Space	1 AP per 2,500-3,000 sq ft
Multi-Floor Building	At least 1 AP per floor

Recommended Access Point Brands

Ubiquiti UniFi | Cisco Meraki | Aruba Instant On | Ruckus | TP-Link Omada

06 Network Segmentation (VLANs)

Network segmentation using VLANs (Virtual Local Area Networks) is critical for security. It prevents a breach in one area from spreading to the entire network—especially important for PCI compliance if you accept credit cards.

PCI-DSS Requirement

If your business processes credit cards, PCI-DSS requires that payment systems be isolated from the rest of your network. Running POS on the same network as guest WiFi is a compliance violation that can result in fines and loss of card processing ability.

VLAN	Name	Purpose	Security
VLAN 10	Management	Network equipment management	Highly Restricted
VLAN 20	Business Operations	Employee workstations, printers	Standard
VLAN 30	Point of Sale	POS terminals, payment processing	PCI Isolated
VLAN 40	Security Systems	Cameras, access control, DVR/NVR	Restricted
VLAN 50	IoT Devices	Smart devices, sensors, thermostats	Isolated
VLAN 100	Guest WiFi	Customer internet access	Internet Only

Inter-VLAN Access Rules

Guest WiFi	→	Internet Only	No access to any internal network
POS Systems	→	Payment Processor	Internet access to payment gateway only
Business Ops	→	Printers, Internet	Normal business internet access
Security Cams	→	NVR + Cloud (optional)	Limited to recording and remote view
IoT Devices	→	Specific Cloud Services	Restricted to manufacturer services only

07 Security Configuration

Beyond network segmentation, proper security configuration ensures your business is protected against common threats.

Firewall Security Services

- Gateway Anti-Virus scanning
- Intrusion Prevention (IPS)
- Content filtering (block malicious sites)
- Geo-IP blocking (block foreign countries)
- Botnet filtering

Access Control

- Strong, unique passwords on all devices
- Change all default credentials
- Disable unused switch ports
- MAC filtering where appropriate
- 802.1X authentication (advanced)

08 Remote Access

Business owners and IT support need secure remote access to the network. This must be done securely to prevent unauthorized access.

Recommended: VPN

Encrypted tunnel to your network. Requires authentication. Industry standard for remote access.

- Site-to-site or client VPN
- Strong authentication
- All traffic encrypted

Avoid: Port Forwarding

Exposes services directly to internet. Common attack vector. Should only be used when absolutely necessary.

- Direct exposure risk
- No encryption unless service provides it
- Brute force target

09 Monitoring & Maintenance

A properly configured network requires ongoing monitoring and maintenance to remain secure and reliable.

Daily	Automated threat log review	**Weekly**	Check for firmware updates
Monthly	Review firewall rules and access logs	**Monthly**	Backup firewall configuration
Quarterly	Security subscription renewals check	**Quarterly**	Password rotation for network devices
Annually	Full network security audit	**Annually**	Disaster recovery test

10 Common Issues We Find

These are the most common network problems we encounter in small business environments. Use this to identify potential issues in your current setup.

Issue	Risk	Impact
Consumer-grade router as primary firewall	High	No threat protection, easy to compromise
Flat network (no VLANs)	High	POS breach = total network breach
Default passwords on equipment	Critical	Trivial unauthorized access
POS on same network as guest WiFi	Critical	PCI compliance violation, card theft risk
Outdated firmware	High	Known vulnerabilities exploitable
No backup internet connection	Medium	Business stops when internet goes down
No network monitoring	Medium	Issues discovered only when things break

11 Network Assessment Checklist

Use this checklist to evaluate your current network configuration. Items marked with a star are critical security requirements.

- [ ] **Business-grade firewall with active subscriptions**
- [ ] **Unique, strong passwords on all network equipment**
- [ ] **Default credentials changed on all devices**
- [ ] **Firmware up to date on all network equipment**

- [ ] **POS systems on isolated VLAN**
- [ ] **Guest WiFi separated from business network**
- [ ] **WPA3/WPA2 encryption on all wireless networks**
- [ ] Remote management disabled or secured via VPN
- [ ] Unused switch ports disabled
- [ ] Network monitoring/alerting configured
- [ ] Automatic backup of firewall configuration
- [ ] Documented network diagram

How Does Your Network Compare?

After reviewing this document, you likely have a better understanding of what a properly configured small business network should look like. The question now is: how does your current setup compare?

Free Network Assessment

Penn Tech Solutions offers a complimentary network assessment for small businesses in the Greater Philadelphia area. We'll evaluate your current setup against these standards and provide a detailed report of findings and recommendations.

+ On-site evaluation of your network infrastructure
+ Security vulnerability identification
+ Compliance gap analysis (PCI if applicable)
+ Written report with prioritized recommendations
+ No obligation, no pressure

Schedule Your Free Assessment

Takes about 1-2 hours depending on network size

Email
info@penntechsolutions.com

Phone
(215) 555-1234

Service Area
Greater Philadelphia Area

Website
penntechsolutions.com

Your network is the backbone of your business operations. Don't wait for a breach or outage to find out your infrastructure wasn't up to the task.