Router & Switch Setup Guide: The PureIoT Configuration Standard

Introduction

Routers and switches are the core devices that enable communication within your local network and with the outside world. Proper configuration is essential for security, performance, and reliability. This guide outlines the key steps for setting up these critical network components.

1. Router Setup: Connecting to the World

The router acts as the gateway between your Local Area Network (LAN) and the Wide Area Network (WAN - the Internet).

- **Initial Access:** Connect a computer directly to the router's management port and access the configuration interface via a web browser (usually at a default IP like `192.168.1.1`).
- **Change Default Credentials: Immediately change the default username and password.** This is the most critical security step.
- **WAN Configuration:** Configure the WAN (Internet) port with the settings provided by your Internet Service Provider (ISP) (e.g., PPPoE, Static IP, or DHCP).
- **Firewall Configuration:** Enable the router's built-in firewall. Configure **Port Forwarding** only for services that absolutely require external access (e.g., a public web server), following the principle of least privilege.
- **VPN Setup:** Configure the router to support a secure VPN connection for remote users, ensuring all remote traffic is encrypted.

2. Switch Setup: Managing Local Traffic

Switches manage the flow of data between devices on your local network.

- **Managed vs. Unmanaged:** For business use, **Managed Switches** are recommended as they allow for advanced configuration like VLANs and Quality of Service (QoS).

- **VLAN Configuration (Virtual Local Area Networks):** Create separate VLANs to segment traffic. This is a critical security measure.
    - **VLAN 10:** Data (Employee PCs, Servers)
    - **VLAN 20:** Voice (VoIP Phones)
    - **VLAN 30:** Guest Wi-Fi (Isolated from the main network)
    - **VLAN 40:** Management (For IT staff to manage devices)
- **Quality of Service (QoS):** Prioritize critical traffic, such as VoIP (Voice over IP) and video conferencing, to ensure clear communication even during high network usage.
- **Spanning Tree Protocol (STP):** Enable STP to prevent network loops, which can cause broadcast storms and bring the network down.

3. Wireless Access Point (WAP) Setup

WAPs extend your network wirelessly.

- **Separate SSIDs:** Create at least two separate Wi-Fi networks (SSIDs): one for **Employees** (connected to the Data VLAN) and one for **Guests** (connected to the Guest VLAN).
- **Security:** Use **WPA3** encryption. If WPA3 is not supported by all devices, use WPA2-Enterprise. **Never use WEP or WPA.**
- **Power and Channel Management:** Use a centralized controller to manage WAP power levels and automatically assign non-overlapping channels to prevent interference.

Router & Switch Configuration Checklist

Item	Status	Notes
Default Credentials Changed	[ ]	**Critical Security Step**
Firewall Enabled and Configured	[ ]	
VLANs Configured for Segmentation	[ ]	
QoS Prioritizing Voice/Video	[ ]	
WPA3/WPA2-Enterprise Enabled	[ ]	
Guest Wi-Fi Isolated (VLAN)	[ ]	

Conclusion

A well-configured router and switch setup is the key to a secure and high-performing network. PureIoT provides expert configuration and ongoing management to ensure your network operates at peak efficiency.