Network Configuration Settings

The Network configuration section (**Config > Network**) controls how ESP32-based Meshtastic nodes connect to IP networks - WiFi and Ethernet - and associated services like NTP and remote logging. These settings are only relevant for ESP32 hardware; nRF52-based boards (like the RAK4631) do not support WiFi/Ethernet and these settings have no effect on them.

Access these settings in the Meshtastic app under **Settings > Radio Configuration > Network**, or via the Python CLI with `meshtastic --set network.*`.

Note: Network connectivity unlocks important Meshtastic features: the web interface, MQTT gateway, APRS bridging, NTP time synchronization, and remote syslog. If you are using ESP32-based hardware (T-Beam, T-Lora, Heltec WiFi LoRa, Station G2, etc.), understanding these settings is important for gateway and infrastructure deployments.

WiFi SSID

Config key: `network.wifi_ssid`
Default: Empty (WiFi disabled)

The SSID (network name) of the WiFi network the node should connect to as a client. Case-sensitive. Maximum 32 characters.

To enable WiFi: Set both WiFi SSID and WiFi Password. The node will attempt to join the network on boot and reconnect if the connection drops.

Important considerations:

- WiFi and Bluetooth can operate simultaneously on most ESP32 devices, but enabling WiFi increases power consumption significantly (typical WiFi active current: 80 - 200 mA vs 5 - 10 mA for LoRa+BT only)
- A node with WiFi enabled and a good internet connection can serve as an MQTT gateway, APRS-IS gateway, and NTP time source for the mesh
- On battery-powered mobile nodes, WiFi should generally be disabled to preserve battery life. Enable WiFi on mains-powered infrastructure nodes.

WiFi Password

Config key: `network.wifi_psk`
Default: Empty

The WPA2 password for the WiFi network specified by WiFi SSID. Stored in the device's flash memory. Supports open networks (leave password empty if the network has no password, though this is strongly discouraged for security reasons).

Security note: The WiFi password is stored in plaintext in the device's NVS (Non-Volatile Storage) flash partition. Anyone with physical access to the device and a serial connection can potentially extract it. Do not configure a node with your primary home WiFi password on a device that could be physically compromised; consider using a dedicated IoT VLAN or guest network.

WiFi Mode

Config key: `network.wifi_mode` (indirectly controlled via presence of SSID and AP settings)
Default: Client mode when SSID is set

ESP32-based Meshtastic nodes support three WiFi operating modes:

Client Mode (STA)

The node connects to an existing WiFi network as a client (station). This is the standard mode for gateway nodes that need internet access. In client mode, the node:

- Obtains an IP address via DHCP (or a configured static IP)
- Can reach the internet for MQTT, NTP, APRS-IS, and other services
- Is accessible on the local network at its assigned IP address
- Serves the web interface at `http://<node-ip>/`

Access Point Mode (AP)

The node creates its own WiFi access point instead of connecting to an existing network. Other devices (phones, computers) connect directly to the node's WiFi AP to access the web interface, without needing an external router or internet connection.

AP mode is configured by: Leaving WiFi SSID empty (or setting it to the AP name) and enabling the AP in the app's Network settings. The default AP SSID is typically `meshtastic-XXXX` (where XXXX is derived from the device MAC address). Default AP password: `12345678`.

Use AP mode when:

- In the field with no known WiFi network - AP mode lets you connect your phone directly to the node for configuration without needing Bluetooth
- Setting up a node in an environment where you don't control the WiFi infrastructure
- Demonstrating Meshtastic at an event where local WiFi is unavailable or unreliable

AP mode limitations: No internet access for the node (no MQTT, NTP, APRS), and the phone connected to the AP loses its normal internet access while connected. Not suitable for gateway deployments.

AP + Client Mode (Soft AP + STA)

The node simultaneously connects to an existing WiFi network (client mode) AND creates its own access point. This allows devices to connect directly to the node's AP while the node itself maintains internet connectivity through the upstream network.

Use when: You want both - internet-connected gateway functionality AND the ability to connect phones/laptops directly via WiFi without knowing the upstream network password. Common for demo setups and ARES deployments where field operators need web interface access.

Note: Running both modes simultaneously increases power consumption and can reduce WiFi throughput due to the ESP32 sharing radio time between AP and STA roles.

Ethernet Enabled

Config key: `network.eth_enabled`
Default: `false`

Enables the Ethernet interface on hardware that supports it. Currently, the primary supported Ethernet-capable Meshtastic hardware is the **Meshtastic Station G2** (which uses a W5500 SPI Ethernet module) and some custom RAK WisBlock builds with Ethernet modules.

Advantages of Ethernet over WiFi for infrastructure nodes:

- More reliable and stable connection - no RF interference, no re-association delays
- Lower and more consistent latency
- Lower power consumption than WiFi (typically 10 - 20 mA vs 80 - 200 mA for WiFi active)
- No PSK to manage or expose

Use when: Deploying a fixed infrastructure node (ROUTER or gateway) at a location with Ethernet infrastructure - server room, communications closet, network rack. Ethernet-connected gateway nodes are more reliable than WiFi-connected ones for long-term unattended operation.

NTP Server

Config key: `network.ntp_server`
Default: `0.pool.ntp.org`

The hostname or IP address of the NTP (Network Time Protocol) server the node uses to synchronize its real-time clock. Accurate time is important for:

- Correct message timestamps displayed in the app
- Log entries with accurate timestamps for troubleshooting
- MQTT message timestamps
- Coordinating time-dependent operations across the mesh

Meshtastic nodes without internet connectivity rely on time received from other nodes on the mesh (nodes share timestamps in packets). A node with NTP access becomes a time source for the entire mesh, improving timestamp accuracy for all nodes.

Recommended NTP Servers

Server	Description	Use When
`0.pool.ntp.org`	Default NTP pool (global)	General use, internet-connected nodes
`time.cloudflare.com`	Cloudflare NTP (anycast, fast)	Reliable alternative with good global coverage
`time.google.com`	Google Public NTP	Reliable alternative
`time.nist.gov`	NIST time server	When US government standard time is needed
`192.168.x.x` (local)	Your own local NTP server	Isolated networks, high-accuracy requirements, no internet

Local NTP server: If your deployment has a local NTP server (common in enterprise and government networks, and in some emergency operations centers), set this to that server's address. This reduces internet dependency and may improve synchronization accuracy.

NTP without internet: If the node has no internet access but is on a local network with a router that provides NTP (most home routers do), using the router's IP address as the NTP server works well: `192.168.1.1` or similar.

---

rsyslog Server

Config key: `network.rsyslog_server`
Default: Empty (disabled)

Configures remote syslog logging. When set to a hostname or IP address (with optional port, e.g., `192.168.1.100:514`), the node sends its log output to a remote syslog server over UDP using the standard syslog protocol (RFC 3164/5424).

Why use remote logging:

- Centralized log collection from multiple nodes - see all infrastructure logs in one place
- Persistent log storage - node logs that would otherwise be lost on reboot are captured on the server
- Real-time alerting - syslog servers can trigger alerts on specific log messages (errors, reconnections, etc.)
- Troubleshooting unattended nodes - diagnose issues without physically connecting a serial cable

Setup requirements:

- A syslog server running on the local network (rsyslog, syslog-ng, Graylog, or any standard syslog receiver)
- The node and syslog server must be on the same network (or routable to each other)
- UDP port 514 must be accessible (default syslog port)

Recommended syslog servers for small deployments:

- **rsyslog** on Linux (Raspberry Pi, server): Simple, lightweight, standard
- **Graylog**: Full log management with search and dashboards - good for larger deployments
- **Loki + Grafana**: Modern log aggregation with excellent visualization

Example rsyslog configuration to receive Meshtastic logs on a Linux server:

```
# /etc/rsyslog.d/meshtastic.conf
module(load="imudp")
input(type="imudp" port="514")

# Save Meshtastic logs to a dedicated file
if $fromhost-ip == '192.168.1.50' then /var/log/meshtastic/node1.log
```

IPv6

Config key: `network.ipv6_enabled` (handled automatically in current firmware)
Default: Enabled when available

Meshtastic's ESP32 networking stack (based on ESP-IDF and lwIP) supports IPv6. The node will request an IPv6 address via SLAAC (Stateless Address Autoconfiguration) if the connected network provides IPv6 router advertisements.

For most users, IPv6 is transparent - the node simply has both an IPv4 and IPv6 address, and connections work over whichever is available. No explicit configuration is typically needed.

When IPv6 matters:

- Networks that are IPv6-only (rare but increasingly common in enterprise environments)
- When you want to access the node's web interface over IPv6 (useful on networks where IPv4 DHCP is restricted)
- Future MQTT and NTP configurations that specify IPv6 server addresses

---

Practical Configuration Guidance

Standard Home Gateway Node

For a mains-powered T-Beam or Station G2 acting as a gateway and router at home:

- WiFi SSID: your home network SSID (or use IoT VLAN if available)
- WiFi Password: your network password
- WiFi Mode: Client
- NTP Server: `0.pool.ntp.org` (default is fine)
- rsyslog Server: empty unless you have a log server

Field Deployment - No Internet

For a node deployed at an event or emergency operation without internet access:

- WiFi Mode: AP (create your own access point for phone/laptop connection)
- AP SSID: something recognizable, e.g., "ARES-Mesh-Node1"
- NTP Server: empty or your EOC's local network NTP if available
- Time will sync from other mesh nodes that have NTP access

Ethernet-Connected Infrastructure

For a fixed ROUTER node on a rack or network closet:

- Ethernet Enabled: true
- WiFi: disabled (leave SSID empty)

- NTP Server: your organization's NTP server or `time.cloudflare.com`
- rsyslog Server: your organization's syslog collector
- Managed Mode: true (with admin channel configured)

Direct Phone Connection Without Bluetooth

When Bluetooth is unavailable or problematic (interference, pairing issues):

- WiFi Mode: AP (or AP+Client if the node also needs internet)
- Connect your phone to the node's AP network
- Open `http://meshtastic.local` in a browser or use the Meshtastic app with HTTP transport
- Full configuration and messaging capability without Bluetooth

Revision #5
Created 2026-05-03 05:55:56 UTC by Mesh America Admin
Updated 2026-05-03 13:58:01 UTC by Mesh America Admin