# Configuration: GL.iNet Opal GL-SFT1200 Repeater Setup

The GL.iNet Opal serves as a versatile intermediate router in VR deployments, handling the complex task of connecting to institutional networks while providing optimized connectivity for your VR equipment. Think of the Opal as your network's diplomatic translator - it speaks the institutional network's language while providing your equipment with the specific network environment it needs.

## Understanding Repeater Mode and WISP Functionality

### What is WISP Mode?

The Opal's repeater mode operates in WISP (Wireless Internet Service Provider) mode. This creates what's called a "double NAT" situation - the Opal creates its own subnet and acts as a firewall between your equipment and the institutional network. While this might sound like it adds complexity, it's actually beneficial for VR deployments because it isolates your equipment from the broader institutional network.

This isolation provides several advantages:

- **Security:** Your VR equipment isn't directly exposed to other devices on the institutional network
- **Control:** You maintain full administrative control over your network segment
- **Stability:** Network changes on the institutional side don't directly affect your equipment
- **Troubleshooting:** Problems can be isolated to either the upstream connection or your local network

### How Double NAT Works in Practice

When your VR headset requests data from the internet, here's what happens:

1. The headset sends the request to the Opal (using addresses like 192.168.8.x)
2. The Opal translates this request and forwards it to the institutional network
3. The institutional network sees the request coming from the Opal, not directly from your VR equipment
4. Responses follow the reverse path, with the Opal handling all the address translation

This process is transparent to your VR applications while providing network isolation and control.

## Device Specifications and Capabilities

**Current Firmware Version:** 4.3.25 (based on OpenWrt 18.06) **Default IP Address:** 192.168.8.1 **WiFi Capabilities:** AC1200 (300Mbps on 2.4GHz + 867Mbps on 5GHz) **Physical Ports:** 3x Gigabit Ethernet (1 WAN + 2 LAN) **Power Requirements:** USB-C 5V/3A (compatible with laptop USB ports for testing) **Physical Size:** Pocket-sized design ideal for discrete institutional deployments

## Initial Setup and Configuration

### First Connection and Access

The Opal uses a simplified setup process designed for travel scenarios:

1. **Wireless Connection Method** Look for the WiFi network named "GL-SFT1200-XXX" where XXX represents the last three characters of the device's MAC address. Connect using the default password

"goodlife". This temporary network allows you to configure the device.

2. **Ethernet Connection Alternative** If wireless setup isn't practical, connect your computer directly to one of the Opal's LAN ports using an ethernet cable. Your computer should automatically receive an IP address via DHCP.
3. **Web Interface Access** Open your web browser and navigate to http://192.168.8.1. The interface will automatically detect your language preferences, though English is recommended for institutional consistency.
4. **Administrator Setup** Create a strong administrator password (minimum 15 characters recommended for institutional use). This password protects all router configuration settings, so choose something secure but memorable for your deployment team.

## Configuring Repeater Mode for VR Deployments

### Basic Repeater Configuration

1. **Network Discovery and Connection** Navigate to **INTERNET → Repeater** in the web administration panel. Click **Connect** to initiate a scan of available wireless networks. The Opal will display all detectable networks with their signal strengths and security types.
2. **Institutional Network Selection** Select your target institutional network from the list. Enter the authentication credentials carefully - incorrect credentials are the most common cause of connection failures. If the network uses enterprise authentication (WPA2-Enterprise), you may need additional configuration parameters from your IT contact.
3. **Portal Authentication Handling** Many institutional networks use captive portals for additional authentication. The Opal automatically detects these situations and enters "Login Mode for Public Hotspots." In this mode, the Opal will redirect your browser to the authentication portal when you first try to access the internet.

### Advanced Repeater Options for Institutional Environments

**MAC Address Management:** Institutional networks often track devices by MAC address. The Opal provides several options:

- **Factory MAC:** Uses the device's original MAC address
- **Clone MAC:** Uses your computer's MAC address (useful if your laptop is already approved on the network)
- **Random MAC:** Generates a random MAC address (useful for privacy but may complicate network management)

**BSSID Locking:** In environments with multiple access points sharing the same network name, BSSID locking forces the Opal to connect to a specific access point. This prevents unwanted roaming but should only be used when connection stability is more important than optimal signal strength.

**Connection Persistence:** Configure the Opal to automatically reconnect if the connection is lost. Set reasonable retry intervals to avoid overwhelming the institutional network with connection attempts.

## Network Optimization for VR Performance

### Wireless Band Configuration

Modern VR systems benefit from dedicated 5GHz connectivity due to the higher bandwidth and typically less congested spectrum:

1. **Dual-Band Strategy** Configure the Opal to connect to the institutional network on 2.4GHz (for range and penetration) while providing VR connectivity on 5GHz (for bandwidth and reduced latency).
2. **Channel Width Optimization** Set the 5GHz channel width to 80MHz when possible for maximum VR throughput. This provides the bandwidth necessary for high-quality VR content while minimizing channel congestion.
3. **Power Management Disable** Disable power-saving features that can introduce latency variations. VR applications prefer consistent performance over power efficiency.

### Quality of Service for VR Traffic

**Device Identification and Prioritization:** Navigate to the **CLIENTS** section to view all connected devices. Identify your VR headsets by MAC address and assign them to high-priority groups. This ensures VR traffic gets preferential treatment during network congestion.

**Bandwidth Allocation:** Allocate minimum bandwidth guarantees for each VR device. A conservative estimate is 100 Mbps per VR headset for high-quality content, though this can vary significantly based on the specific applications being used.

**Gaming Mode Configuration:** Enable gaming/streaming priority profiles if available. These profiles typically reduce buffering and prioritize real-time traffic over background downloads.

## Security Implementation for Institutional Environments

### Wireless Security Configuration

**WPA3/WPA2 Mixed Mode:** Configure mixed WPA3/WPA2 security to ensure compatibility with both modern and legacy VR equipment. Use strong passwords (20+ characters) combining letters, numbers, and symbols.

**Guest Network Isolation:** Enable a separate guest network (typically on 192.168.9.x subnet) for non-VR devices. This provides internet access for administrative devices while keeping them separate from VR equipment.

**MAC Address Filtering:** For high-security environments, implement MAC address filtering to allow only approved devices to connect. Document all approved MAC addresses and maintain this list as equipment changes.

### VPN Integration Considerations

**Institutional VPN Requirements:** Some institutions require all traffic to pass through their VPN infrastructure. The Opal supports OpenVPN and WireGuard clients:

- **OpenVPN:** More compatible but typically slower (30-40 Mbps throughput)

- **WireGuard:** Faster and more efficient (40-50 Mbps throughput) but requires more recent institutional infrastructure

**VPN Performance Impact:** Test VPN compatibility with your VR applications before deployment. VPN encryption adds latency and reduces bandwidth, which can affect VR performance. Monitor performance carefully and consider dedicated VPN hardware if throughput becomes a bottleneck.

### Understanding Network Address Translation (NAT)

When the Opal operates in repeater mode, it creates its own network segment using Network Address Translation. This might seem technical, but understanding NAT helps explain why this configuration works so well for VR deployments:

**Outbound Traffic Translation:** When a VR headset (192.168.8.100) requests data, the Opal translates this to its own address on the institutional network and keeps track of the translation. The institutional network only sees traffic from the Opal, not from individual VR devices.

**Inbound Traffic Handling:** Return traffic comes back to the Opal, which uses its translation table to forward the data to the correct VR device. This process is transparent to both the VR equipment and the institutional network.

**Firewall Benefits:** The NAT process inherently provides firewall protection, as external devices cannot directly initiate connections to your VR equipment. This improves security without requiring additional configuration.