Understanding Network Architecture for VR Systems

Before diving into specific router configurations, it's important to understand what you're building and why each component matters for VR deployments. Think of your network setup as a bridge system connecting the institution's existing WiFi to your VR equipment, with each router serving a specific purpose in ensuring reliable, high-performance connectivity.

The Challenge of VR Networking

VR systems have demanding network requirements that differ significantly from typical web browsing or even video streaming. A single VR headset can require **25-400+ Mbps of bandwidth** depending on the content quality, and perhaps more critically, VR applications need **sub-20ms latency** to prevent motion sickness and maintain immersion. Unlike streaming video where a few seconds of buffering is acceptable, VR systems need consistent, real-time data flow.

Why Multiple Routers Make Sense

You might wonder why we use multiple routers instead of just connecting directly to the institution's network. There are several important reasons:

Network Isolation: Institutions often have security policies that limit what devices can connect directly to their networks. By creating your own network segment, you maintain control over your VR equipment while respecting their security requirements.

Performance Control: Institutional networks are shared resources with unpredictable traffic patterns. Your own network segment allows you to prioritize VR traffic and ensure consistent performance.

Flexibility: Different routers excel at different tasks. A compact travel router like the Opal is perfect for capturing WiFi signals, while a more powerful router like the ASUS provides the advanced features needed for VR optimization.

Redundancy: Multiple connection points mean that if one component fails, you often have alternatives to maintain connectivity.

Understanding IP Addressing for VR Network Deployments

Network addressing might seem like a dry technical topic, but understanding it is crucial for creating a network that works reliably and doesn't conflict with existing institutional systems. Think of IP addresses like postal addresses for your network - each device needs a unique address, and related devices should be grouped in the same "neighborhood."

The Basics of Network Subnets

An IP address like 192.168.1.100 has two parts: the network portion (192.168.1) and the host portion (100). All devices with the same network portion can communicate directly with each other, like houses on the same street. When you see "/24" after an IP address, it means the first 24 bits (roughly the first three numbers) define the network, leaving the last number for individual devices.

Why We Use Private IP Ranges

You'll notice all our configurations use addresses starting with 192.168. These are "private" IP addresses, meaning they're not routed over the internet and can be safely used in internal networks without conflicts. There are three private ranges available:

- 10.0.0.0 to 10.255.255.255 (used by many large institutions)
- 172.16.0.0 to 172.31.255.255 (less common, sometimes used by businesses)
- 192.168.0.0 to 192.168.255.255 (most common for small networks)

We use the 192.168 range because it's familiar to most people and unlikely to conflict with personal devices that staff might bring.

Our Strategic IP Allocation Plan

Here's how we organize IP addresses across different network functions, with explanations for why each range serves its purpose:

192.168.1.x - Infrastructure Management This range is reserved for the routers themselves and network management. Think of this as the "administrative district" of your network. Keeping management separate from user devices makes troubleshooting much easier.

192.168.8.x - GL.iNet Opal Networks The Opal router defaults to this range, and we often keep it to maintain consistency. This becomes your "intermediate processing zone" where the Opal handles tasks like VPN connections or initial traffic filtering.

192.168.10.x - Primary VR Systems This is your main VR device network. We use .10 because it's easy to remember and clearly different from common defaults like .1. VR headsets, VR computers, and VR-specific equipment get addresses in this range.

192.168.20.x - General Computing Equipment Laptops, tablets, and other general computing devices that aren't specifically VR equipment use this range. This separation helps with traffic management and troubleshooting.

192.168.100.x - Guest and Temporary Devices Using .100 makes it obvious these are temporary connections. This range often has more restrictive access policies and bandwidth limitations.

Avoiding IP Address Conflicts

The most common networking problem in multi-router setups is IP address conflicts - when two devices try to use the same address. Our addressing strategy prevents this by ensuring each router manages a completely different range. When Router A uses 192.168.8.x and Router B uses 192.168.10.x, they can coexist without conflicts because they're managing different "neighborhoods."