LightLink VPN White Paper

Contents

1 Overview 5

1.1 Introduction 5

1.2 Background 5

1.3 Purpose 5

2 Key Technologies 6

2.1 Cloud-Coordinated Access 7

2.1.1 Basic Concepts 7

2.1.2 Benefits 7

2.1.3 Market Demand 8

2.2 NAT Traversal 8

2.2.1 Basic Concepts 8

2.2.2 Benefits 9

2.2.3 Market Demand 9

2.3 WireGuard Encrypted Tunneling 10

2.3.1 Basic Concepts 10

2.3.2 Benefits 10

2.3.3 Market Demand 10

2.4 Resource Access Control 11

2.4.1 Basic Concepts 11

2.4.2 Benefits 11

2.4.3 Market Demand 11

3 Key Technology Principles 12

3.1 Cloud-Coordinated Access 12

3.1.1 Protocol Introduction 12

3.1.2 Principle Analysis 12

3.1.3 Framework Analysis 13

3.1.4 Application Scenario Analysis 13

3.2 NAT Traversal 13

3.2.1 Protocol Introduction 14

3.2.2 Principle Analysis 14

3.2.3 Connectivity Boundaries and Reachability Enhancement Strategies 16
3.2.4 Relay Capability Planning in Future Versions 17
3.2.5 Framework Analysis 18
3.2.6 Application Scenario Analysis 18
3.3 WireGuard Encrypted Tunneling Technology 19
3.3.1 Protocol Introduction 19
3.3.2 Principle Analysis 20
3.3.3 Framework Analysis 21
3.3.4 Application Scenario Analysis 21
3.4 Resource Access Control Technology 21
3.4.1 Protocol Introduction 22
3.4.2 Principle Analysis 22
3.4.3 Framework Analysis 22
3.4.4 Application Scenario Analysis 23
4 Application Scenarios and Solutions 23
4.1 Remote Access for Home Users 23
4.1.1 Scenario Description 23
4.1.2 Requirements and Pain Points 23
4.1.3 LightLink VPN Solutions 24
4.1.4 Network Topology 26
4.2 Remote Access for SMBs / Chain Stores 26
4.2.1 Scenario Description 26
4.2.2 Requirements and Pain Points 27
4.2.3 LightLink VPN Solutions 27
4.2.4 Network Topology 29
4.3 Mobile Work / Remote Work 30
4.3.1 Scenario Description 30
4.3.2 Requirements and Pain Points 30
4.3.3 LightLink VPN Solutions 30
4.3.4 Network Topology 32
4.4 IoT / Edge Device Remote O&M Scenario 32
4.4.1 Scenario Description 32

4.4.2 Requirements and Pain Points 32
4.4.3 LightLink VPN Solutions 33
4.4.4 Network Topology 34
5 Brief Introduction of Representative Models 35
6 Future Outlook 37
6.1 Technology Upgrades 37
6.2 Application Scenario Expansion 38
6.3 Ecosystem and Management Integration 38
6.4 User Experience Improvements 38
6.5 Development Vision 38
7 Appendix 39
7.1 Glossary 39
7.2 Technical Details 40
7.2.1 STUN Messages 40
7.2.2 NAT Types 40
7.2.3 WireGuard Messages 41

1 Overview

Omada LightLink VPN is a lightweight remote-access solution built on the WireGuard protocol. It is designed for prosumer and SMB users and helps remote users securely connect to an Omada gateway over public networks (e.g., hotels, cafés, and airports) to access local devices and resources on home or office networks.

This white paper introduces the background, technical concepts, configuration, main application scenarios, and real-world deployment examples of LightLink VPN to help network administrators understand and use the feature.

1.1 Introduction

Traditional VPN deployments typically rely on public network reachability and manual configuration, which creates a higher barrier to entry.

LightLink VPN follows a "zero-configuration" approach: the Omada gateway (server) can share access through a URL or email, and users can establish a VPN connection with a single tap on a mobile device—even when the gateway is not publicly reachable. This greatly simplifies VPN deployment and use. Users simply complete basic onboarding to gain access, without the need to understand the underlying network topology. Moreover, the system also supports resource-based access control to meet different access requirements.

1.2 Background

In real-world networks, many endpoints are deployed behind NAT or within restricted networks and don't have public IP addresses. As a result, traditional VPN solutions can't establish connections directly and often require complex configuration. Manual setup increases deployment cost and the risk of misconfiguration.

With the growth of remote work and distributed networks, the demand for "zero-configuration" remote access continues to rise. LightLink VPN addresses complex network scenarios without public IP addresses by providing automated access to reduce operational overhead and improve connection availability.

1.3 Purpose

This white paper aims to:

1. Explain the implementation principles of LightLink VPN, including the design and mechanisms for zero-configuration access in no-public-IP scenarios, the interaction between clients and the server, the connection workflow, and baseline access control strategies.

2. Provide configuration guidance and recommended deployment strategies for LightLink VPN.
3. Analyze access capability and stability across different network environments.

After reading this white paper, you should have a solid understanding of how LightLink VPN simplifies access while delivering reliable remote connectivity.

2 Key Technologies

LightLink VPN is a remote-access capability that connects local networks to external endpoints. It is widely used in home networks, enterprise branch networks, remote work, device operations and maintenance, and edge computing. As public IP addresses become harder to obtain, carrier-grade NAT (CGNAT) becomes more common, and endpoints grow increasingly mobile. Traditional remote-access approaches that rely on public IP addresses, port forwarding, or static VPN configuration are becoming less practical to deploy and operate.

In response, the industry is shifting from a traditional model of "public exposure + manual configuration" to a modern model of "cloud coordination + automated connection establishment + centralized management." Users no longer focus only on connectivity, but also care about simple access, controllable resource exposure, central devices management, and reliable connections in complex network environments.

To align with this shift, LightLink VPN is built around four foundational technologies:

- Cloud-coordinated access
- NAT traversal
- WireGuard encrypted tunneling
- Resource access control

These technologies map to four core problems in remote access: connection establishment, path reachability, secure transport, and access boundaries. Together, these form an end-to-end remote-access foundation.

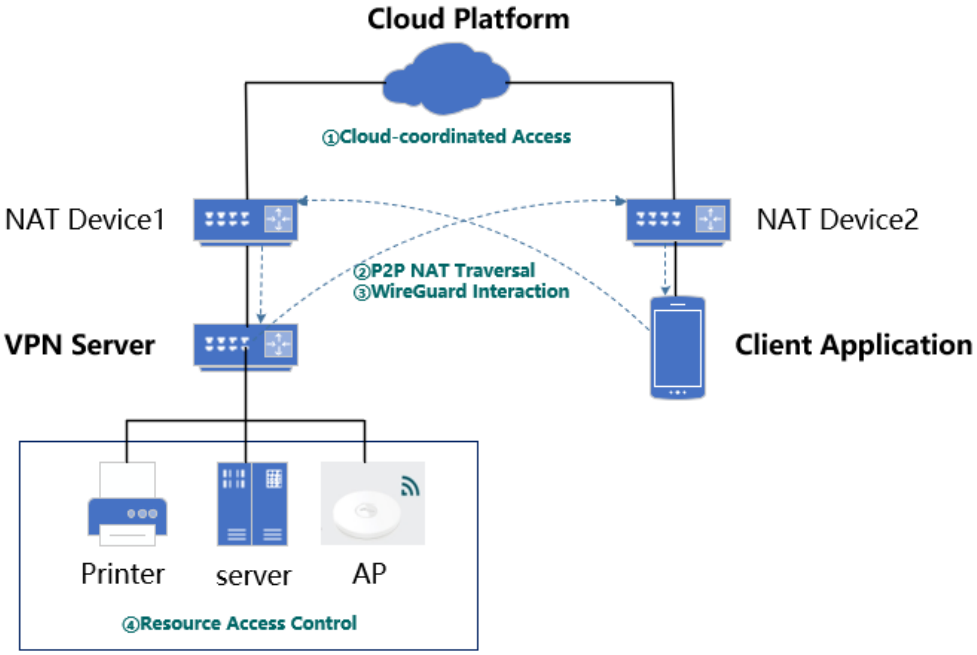


Figure 1. LightLink key technology topology

2.1 Cloud-Coordinated Access

2.1.1 Basic Concepts

Cloud-coordinated access is a mechanism in which the device, client, and cloud work together. The cloud coordinates device association, request forwarding, and the exchange of connection parameters to establish a remote-access relationship.

Key roles are as follows:

- **Client:** Navi app for Android/iOS, Navi Desktop for Windows/Mac
- **Device:** Omada Fusion Gateway
- **Cloud:** TP-Link cloud services

In this model, the client initiates the access workflow and sends a connection request. The device responds and participates in connection establishment. The cloud provides control-plane coordination, enabling devices behind private networks or NAT to be reliably discovered, reached, and brought into a connectable state. The system can then proceed with NAT traversal and encrypted tunnel establishment.

2.1.2 Benefits

Cloud-coordinated access productizes and operationalizes connection establishment in complex network environments, significantly lowering the barrier to remote access.

Compared to approaches that depend on public IP addresses and static configuration, it:

- Turns complex connection setup into a service, reducing manual user effort.
- Enables devices behind NAT or in private networks to be discoverable, reachable, and able to coordinate connections.
- Supports a consistent access workflow and centralized remote-access management.
- Integrates with existing gateways, controllers, and cloud management platforms.

2.1.3 Market Demand

Market demand for remote access has shifted from "can connect" to "easy to access, deploy, and manage." Home and SMB users commonly lack public IP addresses and specialized networking expertise. Vendors and platform providers also want remote access to be easy to integrate into existing product portfolios. As a result, cloud-coordinated access—designed to reduce first-time setup friction, handle complex network conditions, and support standardized workflows—has clear demand and practical value.

2.2 NAT Traversal

2.2.1 Basic Concepts

NAT traversal is a mechanism that attempts to establish an end-to-end reachable path when both the client and the device are behind NAT or in private networks. It typically involves public address discovery, NAT behavior detection, exchange of connection parameters, and peer-to-peer (P2P) connectivity attempts.

In the current version, LightLink VPN's NAT traversal capability is primarily implemented through P2P hole punching. The goal is to establish a direct P2P channel between two endpoints that can't otherwise reach each other, providing an underlying transport for the encrypted tunnel. Compared to a fully relayed approach, a direct P2P path usually provides a shorter network path, lower latency, and lower bandwidth consumption on the platform side.

P2P hole punching is a best-effort reachability enhancement. Success depends on factors such as NAT type, port mapping behavior, carrier network policies, firewall rules, and link conditions. Not all no-public-IP scenarios can reliably form an end-to-end direct path. In environments such as complex NAT, CGNAT, multi-layer NAT, mobile networks, or restrictive firewalls, direct connections may fail or be unstable.

NAT traversal typically requires cloud coordination. In the current version, key steps include:

1. The client and the device collect local network information, such as public-observed addresses, port mapping, and NAT behavior characteristics.

2. The two sides exchange connection parameters through the cloud to obtain necessary peer network information.
3. The system selects an appropriate hole-punching strategy based on the two sides' network environments and initiates P2P connectivity attempts.
4. After a P2P path is established, the encrypted tunnel is built on top of that underlying path.
5. When direct connectivity isn't possible, the system may rely on retries, path re-probing, or relay capabilities (planned for future versions) to improve overall availability.

2.2.2 Benefits

NAT traversal improves reachability in complex network environments, with an emphasis on establishing end-to-end paths when conditions allow.

Key benefits include:

- Better adaptability for common environments, such as private networks, home broadband, multi-layer NAT, and mobile networks.
- Reduced dependence on long-lived relay forwarding and shortened communication paths when direct connectivity is available.
- Improved latency, user experience, and connection efficiency for remote access.
- Reduced long-lived relay bandwidth and forwarding resource consumption on the platform side.
- More flexible underlying path options for establishing encrypted tunnels.

Since the current version relies mainly on P2P hole punching, its value is mainly in improving direct-connect success rates, reducing dependence on long-lived relay forwarding, and providing a transport foundation for the encrypted tunnel.

For remote-access systems, stronger NAT traversal typically translates to better real-world compatibility, better user experience, and improved platform resource efficiency. Future versions can further enhance availability in difficult environments by adding relay capabilities.

2.2.3 Market Demand

No-public-IP environments, complex NAT, and mobile access have become the mainstream network background for remote access. In home broadband, micro-business networks, remote work, remote operations, and mobile scenarios, both the client and the device are usually behind NAT, and direct inbound reachability is not available.

Without effective NAT traversal and P2P hole punching, remote-access solutions must rely more heavily on relayed paths. While relays can improve connectivity, they can also increase

platform bandwidth cost, lengthen the network path, and increase concurrency pressure. Latency, stability, and platform scalability can all suffer in workloads such as real-time control, remote desktop, device management, and file access.

As a result, NAT traversal is now a baseline capability for remote-access products. In the current version, P2P hole punching is LightLink VPN's primary NAT traversal method, designed to maximize direct-connect success in real-world networks and strengthen overall network adaptability.

2.3 WireGuard Encrypted Tunneling

2.3.1 Basic Concepts

WireGuard is a modern VPN protocol and implementation designed to create secure, encrypted tunnels over untrusted networks such as the internet. With a compact design, lightweight implementation, and strong performance, WireGuard has become an increasingly common choice for remote access—especially where device resource consumption, connection efficiency, and secure transport all matter.

In LightLink VPN, WireGuard encrypted tunneling refers to using the WireGuard protocol to establish a lightweight, efficient encrypted channel between the client and the device to carry application traffic after remote access is established. In this solution, WireGuard doesn't handle device discovery or access coordination. Instead, it serves as the secure transport layer after connectivity is in place, providing consistent encryption and a reliable tunneling mechanism for data in transit.

2.3.2 Benefits

WireGuard combines lightweight deployment with efficient transport and standardized security.

Typical benefits include:

- A lightweight protocol that fits edge devices and resource-constrained platforms.
- Efficient tunnel establishment and data transport for modern remote-access needs.
- A consistent, standardized foundation for secure communications.
- Straightforward integration with dynamic connection-establishment workflows.

For LightLink VPN, WireGuard's value isn't as a complete remote-access system by itself, but as the secure communication infrastructure within a remote-access architecture.

2.3.3 Market Demand

Remote access requirements now go beyond simply establishing a connection, focusing instead on a consistent, stable, and efficient secure transport layer once connected.

Confidentiality, integrity, and connection efficiency are non-negotiable, whether a home user is accessing internal resources or an IT technician is managing devices remotely. Therefore, WireGuard-based encrypted tunneling remains broadly applicable in modern remote-access solutions.

2.4 Resource Access Control

2.4.1 Basic Concepts

Traditional remote-access solutions often focus on joining the remote endpoint to the LAN. This approach works for full network extension, but real-world needs are often narrower. For example, a user may only need access to the gateway itself, a specific host, or a specific set of subnets—not the entire internal network.

With increasing demand for least-privilege assignment, security boundary control, and integrated management of network products, the industry increasingly expects remote access to be not only reachable but also clearly scoped and controllable.

LightLink resource access control enforces and manages what the client can access after the remote-access connection is established, such as specific devices, hosts, subnets, or application resources. The core question it answers isn't "Can I connect?" but "After I connect, what can I access?"

2.4.2 Benefits

Resource access control separates "the ability to connect" from "the scope of access," evolving remote access from "reachable" to "controllable."

Key benefits include:

- Clear remote-access boundaries that support centralized administration.
- The ability to limit access to the gateway itself, specific hosts, or defined subnets, helping reduce the security risk of exposing an entire LAN.
- Better alignment with enterprise networks, remote operations, and multi-role access scenarios by integrating remote access into a broader device policy framework.

2.4.3 Market Demand

In enterprise networks, retail/branch networks, remote operations, and multi-device home environments, users increasingly want to know what they can access. In multi-user, multi-role, and multi-resource environments, solutions without clear access boundaries are difficult to deploy safely and consistently. As a result, remote-access solutions with unified resource access control have strong market demand and product value.

3 Key Technology Principles

This section introduces the core technical principles behind LightLink VPN, using industry-standard fundamentals, standard protocols, and typical architectures. The content below describes general mechanisms only and does not include any product-specific interfaces, private parameter formats, internal algorithms, or other protected implementation details.

3.1 Cloud-Coordinated Access

3.1.1 Protocol Introduction

Cloud-coordinated access is a control-plane capability of LightLink VPN. In practice, it is commonly built on HTTPS, WebSocket, long-lived connections, or other lightweight messaging channels. It is used for device association, request forwarding, status synchronization, and parameter exchange.

These control-plane protocols are not designed to carry long-term business data traffic. Their primary task is to coordinate the client and the device before the connection is established. To ensure the security of control-plane interactions, the communication is typically protected by TLS (e.g., over HTTPS/HTTP2), to ensure the confidentiality and integrity for access requests, device status, and connection parameters during transmission.

3.1.2 Principle Analysis

The core principle of cloud-coordinated access is to establish a unified access mechanism through cloud services, so that clients and devices that cannot directly discover each other can enter a connectable state.

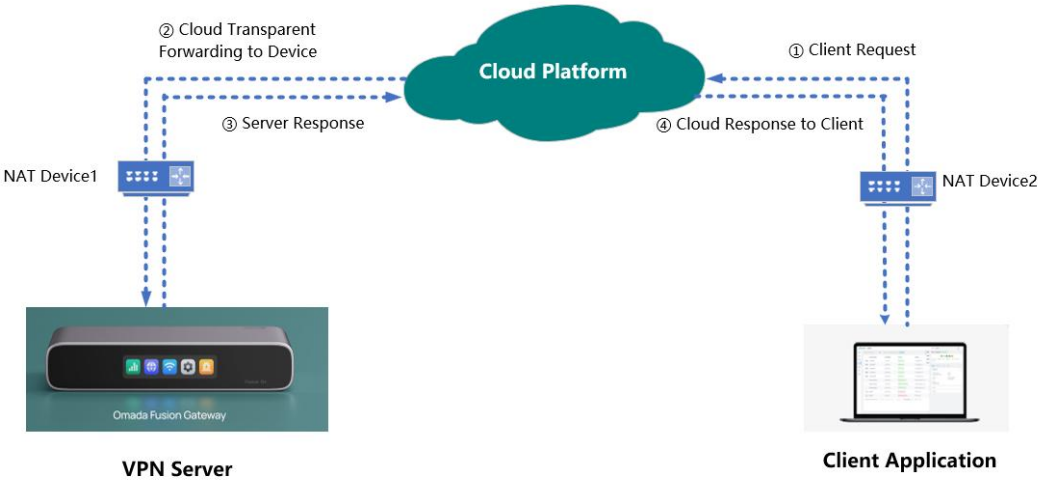


Figure 2 Cloud-Coordinated Access

In complex network environments, the device and the client are usually behind private networks or NAT, and the client cannot locate and reach the target device the way it accesses a public internet service. Cloud-coordinated access completes this discovery and mediation step via the cloud.

Under this model, the client first initiates an association request through an access entry point. The cloud locates the target device based on that entry and forwards the relevant requests and status information to the device. Then, the device processes the request and returns the information required for connection establishment via the cloud, completing the full process from device discovery and access triggering to connection preparation. In this way, two endpoints originally separated by different network boundaries are brought into the same control-plane workflow.

Importantly, cloud-coordinated access does not imply that the cloud must carry business traffic over the long term. Instead, it emphasizes that in modern remote access systems, connection establishment itself benefits from unified cloud coordination. In other words, the cloud solves how to bring both sides into a negotiable state, rather than how to forward business data between them long-term.

3.1.3 Framework Analysis

From a system architecture perspective, cloud-coordinated access consists of three components: the client, the device, and the cloud. The client imports the access entry point, initiates the connection request, and receives connection parameters. The device responds to the access request and participates in subsequent connection establishment. The cloud deals with the message delivery between the client and the device.

3.1.4 Application Scenario Analysis

Cloud-coordinated access applies to any scenario that requires lowering the onboarding barrier and unifying the access workflow. Examples include remote access to devices in home networks, lightweight access in SMB and retail-store scenarios, triggered access from cloud management platforms, and unified access management in multi-terminal and multi-device environments.

3.2 NAT Traversal

After access preparation is completed, one key problem remains: the client and the device are often still not directly reachable because they sit behind NAT, private networks, or multi-layer network topologies. NAT traversal—coordinated by the cloud—handles public-visible address discovery, connection parameter exchange, and peer-to-peer connectivity attempts, so that an end-to-end reachable path can be established when network

conditions allow. This provides the underlying channel for subsequent secure communication and encrypted tunnel establishment. In essence, NAT traversal does not directly carry business data. It addresses the problem of how to obtain an underlying reachable path in complex private-network environments, and is the key step that moves remote access from “coordinatable” to “connectable.”

This section analyzes NAT traversal from protocol mechanisms, connection establishment process, NAT-type impacts, connectivity boundaries, and future evolution directions.

3.2.1 Protocol Introduction

In remote access, P2P hole punching is an important NAT traversal approach. It is mainly based on UDP communication, public-visible address discovery, address mapping identification, candidate path exchange, and connectivity checks. Typical industry concepts include STUN, TURN, and ICE:

- STUN helps endpoints behind NAT or private networks identify their public-visible address and port information, providing foundational network-environment awareness for subsequent connection establishment.
- ICE defines a more complete mechanism for candidate gathering, exchange, checking, and selection.
- TURN provides relay capability when an end-to-end path is unreachable.

In the current version, LightLink VPN mainly uses STUN-like mechanisms during P2P hole punching. The client and device obtain their public-visible addresses and port mapping information through STUN-like probing, and exchange connection parameters via the cloud to enable subsequent P2P connectivity attempts.

TURN-style relaying is not included in the current version and will be introduced in a future release as a planned relay capability.

3.2.2 Principle Analysis

1. Basic principle of P2P

The basic principle of P2P hole punching is that, under cloud coordination, the client and the device obtain each other’s current public-visible addresses, port mappings, and required connection parameters, and then send UDP packets to the peer’s public-mapped address at an appropriate time. This creates NAT mapping states on both NAT devices that allow bidirectional communication.

Because different NAT types differ in address mapping, port allocation, mapping rules, and inbound traffic filtering, the hole punching process typically requires dynamic handling based on both sides’ current network conditions.

2. P2P connection establishment flow

In the LightLink VPN scenario, P2P hole punching can be understood as the following:

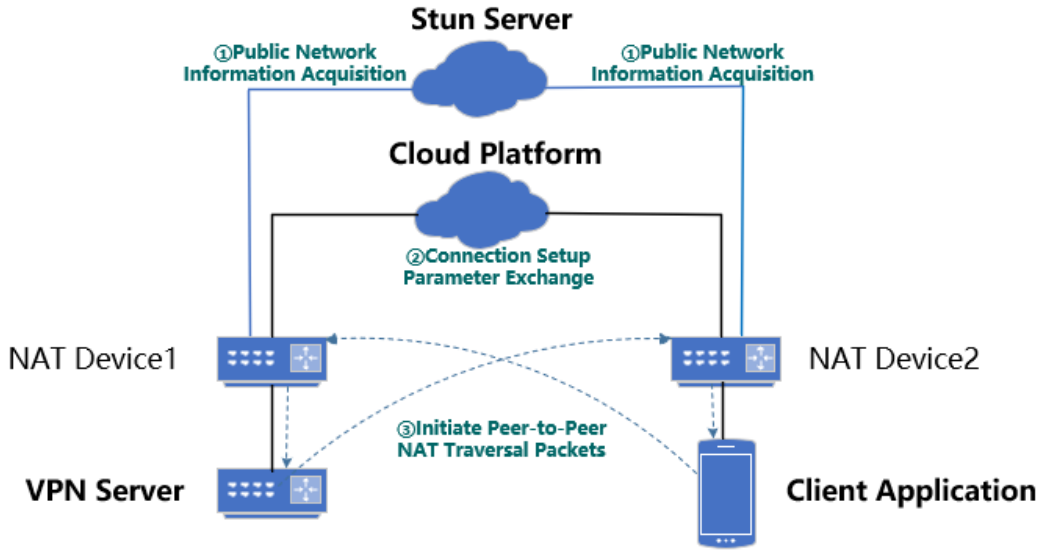


Figure 3 P2P Hole Punching

（1）Obtain public-visible information

The client and the device each obtain their current public-visible address, port mapping, and related network-environment information through STUN-like mechanisms.

（2）Exchange connection parameters

The client and the device exchange public-visible address, port information, session identifiers, authentication information, and other necessary parameters through the cloud.

（3）Prepare for hole punching

Based on peer information, the client and the device enter a preparation state and wait for cloud coordination to trigger peer communication attempts.

（4）Send UDP probe packets

Under coordination, both sides send UDP probe packets to the peer's public-mapped address almost simultaneously. attempting to create returnable NAT mappings on both sides.

（5）Perform connectivity checks

The system determines whether a usable underlying communication path has been formed based on probe packets and responses. If the check passes, the P2P path is considered ready to carry the subsequent tunnel.

（6）Establish the encrypted tunnel

Once the underlying path is available, an encrypted tunnel (e.g., WireGuard) can be established over it to carry application traffic.

(7) Re-probe or retry in exception scenarios

If hole punching fails, the connection is interrupted, or the network environment changes, the system can re-trigger public-visible address discovery, parameter exchange, and P2P hole punching to adapt to dynamic network conditions.

3. Impact of NAT behavior and network policies on hole punching

Whether P2P hole punching succeeds primarily depends on the NAT device's address mapping method, inbound traffic filtering, mapping retention time, and external network policies.

The effect of NAT on P2P hole punching is not simply whether NAT exists, but whether NAT can form stable, predictable mappings that allow return traffic. The stricter the NAT behavior, the more hole punching depends on timing, mapping retention, and connectivity checks—and the more likely the direct-connect success rate is to drop.

Beyond the behavior differences of a single NAT device, actual network environments may also include CGNAT, multi-layer NAT, mobile network switching, and enterprise firewall policies. CGNAT means that public-side mappings are centrally managed by the ISP, making mapping behavior hard to control or predict. Multi-layer NAT increases uncertainty. Strict firewalls may directly restrict inbound UDP traffic or unknown destination ports. Mobile networks may invalidate mappings due to cell handoffs, address changes, or link fluctuations.

Therefore, in symmetric NAT, CGNAT, multi-layer NAT, frequent mobile network switching, or strict firewall environments, P2P hole punching may fail, become unstable, or be interrupted. The system must further improve overall connectivity availability in complex environments through retries, path probing, keepalives, and relay capability planned for future versions.

3.2.3 Connectivity Boundaries and Reachability Enhancement Strategies

As shown above, P2P hole punching success depends not only on public-visible address discovery and parameter exchange, but also on whether both network environments allow stable return paths. NAT mapping behavior, inbound filtering rules, UDP mapping retention time, ISP network policies, and endpoint network-state changes all affect the final result. Therefore, the current version of LightLink VPN introduces multiple reachability enhancement strategies during P2P connection establishment to improve direct-connect success rates and recovery capability.

1. Multiple attempts of hole punching and coordinated connection establishment

Under cloud coordination, the client and the device perform multiple attempts of UDP hole punching. Continuous probing interactions, NAT mapping refresh, and connection-state

synchronization increase the probability of forming a usable communication path. This mechanism improves adaptability in complex NAT environments, but its effectiveness still depends on actual network policies and NAT behavior.

2. Multi-candidate path probing and dynamic retries

In scenarios with complex NAT mapping behavior, unstable link states, or changing public reachability, the system can improve the probability of discovering a valid communication path through multi-candidate path probing, dynamic retries, and connection-state feedback. This mechanism enhances path discovery in complex environments, but does not guarantee direct-connect success under all NAT types or network policies.

3. Keepalive and mapping maintenance

After a P2P path is established, periodic keepalive packets can maintain NAT mappings and reduce the probability of disconnects caused by UDP mapping timeouts. Keepalives should balance reliability and resource cost considering traffic load, endpoint power consumption, and link stability.

4. Path re-probing and reconnection

When the system detects abnormalities, unreachable links, network switching, or connection-state changes, it can re-trigger public-visible address discovery, parameter exchange, and P2P hole punching. This mechanism helps adapt to dynamic environments such as mobile handoffs, multi-WAN changes, and NAT mapping changes, improving recovery capability.

These mechanisms can improve P2P direct-connect success and stability, but cannot fully eliminate the risk of failures in complex NAT, CGNAT, or strict firewall scenarios. Therefore, the NAT traversal capability in the current version should be positioned as a reachability enhancement capability with a "P2P direct-connect first" strategy. For scenarios where direct connectivity still cannot be established, later versions will introduce Relay mechanisms to further improve overall connectivity availability.

3.2.4 Relay Capability Planning in Future Versions

To further improve connectivity availability in complex network environments, future versions of LightLink VPN will introduce a relay mechanism as a complement to P2P direct-connect capability.

Under this mechanism, the system will still prioritize P2P direct connections. When end-to-end direct-connect conditions are not met, the client and the device can establish an indirect communication path through a relay node, which forwards traffic between the two sides. Relay does not depend on direct reachability between the client and the device, and therefore covers more complex network environments.

From a performance perspective, P2P direct paths are usually shorter and lower-latency, and they consume fewer cloud forwarding resources. Relay paths improve availability but introduce an extra forwarding hop and may increase latency, reduce throughput, and raise cloud resource consumption. Future versions will balance success rate, performance, and platform cost by preferring P2P direct connectivity and using Relay as a fallback.

3.2.5 Framework Analysis

Architecturally, NAT traversal and P2P hole punching require coordination among the client, the device, and the cloud. The client and device handle local network probing, parameter processing, probe transmission, connection state maintenance, and tunnel preparation. The cloud coordinates identity, synchronizes state, exchanges parameters, and orchestrates the overall connection process. Together they enable the transition from access preparation to the underlying reachable path establishment.

Within the LightLink VPN remote access system, these capabilities can be viewed as three layers:

1. **Cloud-coordinated access layer**: Device registration, identity authentication, online status maintenance, and connection preparation to bring the client and device into a negotiable state.
2. **Reachability establishment layer**: Public-visible address probing, NAT behavior awareness, parameter exchange, and P2P connectivity attempts to obtain an underlying communication path.
3. **Encrypted tunnel transport layer**: After the underlying path is established, encrypted tunneling mechanisms such as WireGuard carry the actual application traffic.

Therefore, NAT traversal and P2P hole punching serve as the reachability establishment layer in the system, providing underlying network path conditions for subsequent secure communication.

3.2.6 Application Scenario Analysis

NAT traversal is especially suitable for remote access scenarios where both sides are behind private networks, including home broadband, SMB networks, mobile networks, multi-layer NAT, multi-WAN environments, and remote operations and maintenance networks.

Without effective NAT traversal, remote access solutions often rely more on relay forwarding, which imposes clear constraints on latency, bandwidth cost, and platform scalability. P2P hole punching can establish end-to-end direct paths when network

conditions allow, helping reduce latency, improve user experience, and reduce long-term relay resource consumption on the platform side.

However, in complex scenarios such as symmetric NAT, CGNAT, strict firewalls, and frequent mobile network switching, P2P direct-connect may fail or be unstable. Therefore, LightLink VPN's NAT traversal should be positioned as a "direct-connect-first" and reachability enhancement capability, rather than an absolute traversal capability for all private-network environments. The planned relay mechanism in future versions will serve as a complement to further improve remote access success rates in complex network environments.

As a result, NAT traversal directly affects the practicality of a remote access solution in real networks, and is a key foundation for evaluating system reachability, user experience, and platform resource utilization efficiency.

3.3 WireGuard Encrypted Tunneling Technology

3.3.1 Protocol Introduction

WireGuard is a lightweight encrypted tunneling protocol that runs over UDP. It is primarily used to build a secure point-to-point communication channel over untrusted networks. Compared with traditional VPN protocols, WireGuard features a simpler design and a lighter implementation, making it better suited for edge gateways, lightweight devices, and mobile endpoints.

From an interaction-flow perspective, WireGuard requires only one TTL to complete the handshake:

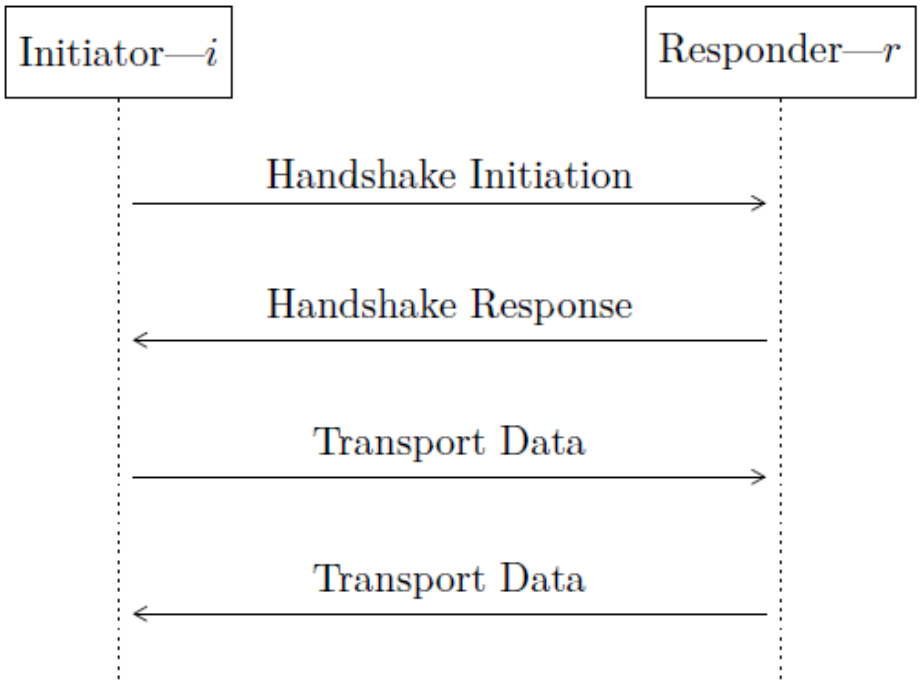


Figure 4 WireGuard Interaction Flow

A WireGuard system typically includes the following basic elements:

(1) **Tunnel Endpoints:** The two entities that participate in communication, such as the client and the device side.

(2) **Key Identity:** Each side uses its own key pair to establish a trusted peer relationship.

(3) **Peer Relationship:** Each side maintains basic communication information and the tunnel relationship for the peer.

(4) **Tunnel Interface:** A logical virtual transport channel for service traffic.

(5) **UDP Transport Path:** WireGuard packets are carried over an underlying UDP path.

Therefore, at the protocol level, WireGuard addresses how to transmit data securely and consistently once connected.

3.3.2 Principle Analysis

The core principle of WireGuard tunnel encryption is to establish a logical encrypted channel between the client and the device side so that subsequent service data is transmitted within that channel.

Conceptually, this process can be understood in the following stages:

1. Establish Tunnel Endpoint Identities

The two parties first exist as tunnel endpoints and form a peer relationship based on their key identities.

2. Form a Tunnel Control Relationship

After the underlying path is reachable, WireGuard establishes a stable peer tunnel relationship between the client and the device side.

3. Send Service Traffic Through the Encrypted Tunnel

Subsequent service data first enters the tunnel interface, and then WireGuard sends it to the peer as encrypted packets over the UDP transport path.

In LightLink VPN, WireGuard is not a complete remote-access solution on its own. It works with access coordination and NAT traversal: once the control plane has coordinated the session and the underlying path is established, WireGuard provides a unified, encrypted tunnel for traffic. In this design, WireGuard functions as the secure transport layer, instead of the discovery or access control layer.

3.3.3 Framework Analysis

In LightLink VPN, WireGuard is not a complete remote-access solution on its own, but playing a role as the secure transport layer. In this structure:

1. The client is on one end of the tunnel and is responsible for initiating and carrying client-side service traffic.
2. The device side is on the other end of the tunnel and is responsible for carrying device-side traffic and traffic for accessing back-end resources.
3. The underlying path is provided by the NAT traversal and P2P hole punching.
4. After the tunnel is established, the cloud generally no longer serves as the primary path for user data traffic.

3.3.4 Application Scenario Analysis

WireGuard encrypted tunneling technology is suitable for scenarios such as home network access, enterprise device connectivity, remote management of edge gateways, and secure communication between mobile endpoints and local devices. Especially in scenarios that require low resource usage, efficient communication, and easy deployment, WireGuard's combination of lightweight design and strong security makes it a representative tunneling transport technology in remote-access solutions.

3.4 Resource Access Control Technology

Resource access control determines whether remote access has clear boundaries and whether it can evolve from simply "connecting" to "controlled access."

3.4.1 Protocol Introduction

Resource access control does not rely on a single standard protocol. Instead, it is built on common mechanisms such as access control, resource boundary enforcement, policy constraints, and network path control.

3.4.2 Principle Analysis

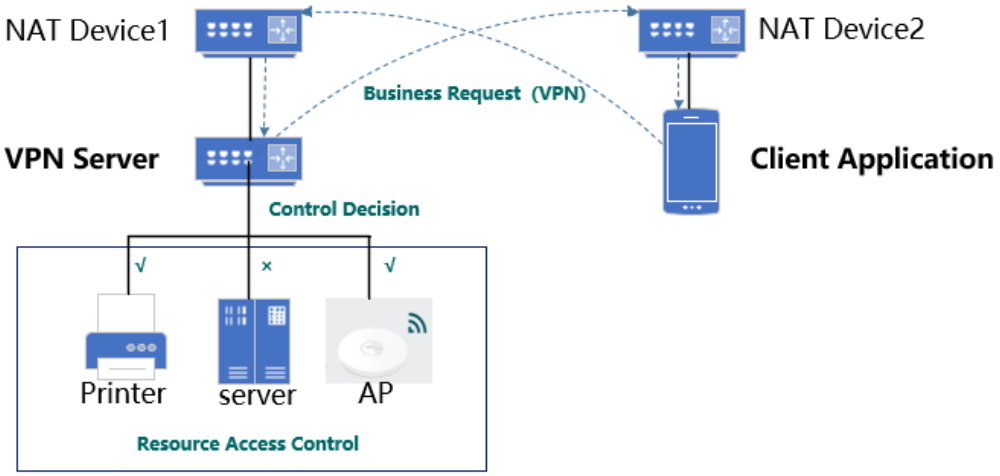


Figure 5 Resource Access Control Diagram

Resource access control separates establishing a remote connection from defining accessible resources. A remote-access connection does not inherently mean exposing the entire local network. With resource access control, you can restrict access to the device itself, specific hosts, specific subnets, or other service resources. This shifts remote access from basic network reachability to controlled access.

At its core, this approach changes remote access from “open everything” to “open only within defined boundaries,” which better matches modern network security and management requirements.

3.4.3 Framework Analysis

From an architectural perspective, resource access control is implemented primarily on the device. The device defines the allowed resource scope and enforces it for the remote-access session, so clients can access only permitted targets after the connection is established. In the overall architecture, resource access control sits between established connection and resource access, essentially acting as a policy enforcement layer.

3.4.4 Application Scenario Analysis

Resource access control applies to the following typical scenarios:

1. Remote operations and maintenance where access is required only to the device itself.
2. Home and retail deployments where access is required only to specific LAN hosts or services.
3. Enterprise deployments where remote endpoints should not have full access to the LAN.
4. Product scenarios where remote access must align with device-management boundaries.

As least-privilege principles and fine-grained access requirements continue to grow, resource access control has become a key capability for moving remote access from "reachable" to "controlled."

4 Application Scenarios and Solutions

With zero-configuration onboarding, powerful NAT traversal, and granular resource access control, LightLink VPN is well-suited to a wide range of network environments—from individual homes to small and medium-sized businesses. This section describes typical application scenarios and their corresponding solutions.

4.1 Remote Access for Home Users

4.1.1 Scenario Description

A home user has deployed an Omada Fusion Gateway and a NAS at home to store photos, work documents, and home security camera recordings. When traveling or working off-site, the user wants to securely access the home NAS from a laptop or smartphone to view or upload files, while also being able to remotely view smart camera feeds or use the home printer.

4.1.2 Requirements and Pain Points

- Most home broadband connections are behind CGNAT (Carrier-Grade NAT) and/or multi-layer NAT, with no public IPv4 address, making traditional VPN access impractical.
- Home users typically lack professional networking knowledge and cannot complete complex operations such as port forwarding and static configuration. Exposing service ports to the public internet also introduces security risks.

- The user only needs access to specific devices on the home LAN (NAS, cameras, printer, or smart home devices) rather than opening up the entire internal network.
- Family members use devices running different operating systems (smartphones and laptops), requiring cross-platform support.

4.1.3 LightLink VPN Solutions

➢ **Technical Solution Overview**

1. **Zero-configuration, one-click onboarding:** The Omada Fusion Gateway generates a LightLink access link with one click. The link can be shared with family members via app, SMS, or email. On a phone or PC, simply tap the link on the client (Navi app) to automatically complete configuration and connect—no need to manually set a public IP address, ports, or keys.
2. **P2P direct connection first:** The system automatically detects NAT types and performs hole punching, prioritizing an end-to-end direct tunnel between the client and the home gateway. This significantly reduces latency when accessing NAS videos or camera feeds and makes full use of the home broadband uplink.
3. **Granular resource control:** Limit the client to access only designated devices such as the home NAS and security cameras, while blocking access to other endpoints on the home LAN to protect home network security.
4. **Multi-device compatibility:** Supports clients on iOS/Android/Windows/macOS to meet remote access needs from smartphones and laptops.

➢ **Configuration Steps**

1. Complete the basic initial setup of Fusion. Log in to the management page with your account and password, enable Cloud Access, and confirm its status shows **Online**.
2. On the left navigation pane, go to **Configuration** > **Network Config** > **LightLink VPN** to open the configuration page.
3. On the configuration page, confirm the service is enabled. If it is not, toggle the switch at the top to enable it.
4. The Invite method supports **By Link** or **By Email**:
   - **By Link:** Click **Generate** to create a unique access URL. Copy the link and share it with family members via app, SMS, email, etc.

- **By Email:** Enter a family member's email address in **Email 1**. You can add multiple email addresses. Click **Send Invites**, and the system will email the access link to the specified addresses.

5. **Client (Navi app) onboarding:** Family members install the Navi app on their phone or computer. Tap the link to open the app, choose to join LightLink VPN, and the app will automatically parse the link and establish a VPN connection to the Fusion Gateway. After a successful connection, the gateway management page's **LightLink Clients** list will display the connected client's name, IP address, online time, and other information.
6. **Configure resource access control:** On the Fusion Gateway's LightLink VPN configuration page, use **Access Control** to define which internal resources the VPN client can access—restrict subnets via **Allowed Networks** and restrict specific devices via **Allowed Devices**. If **Advertise Accessible Resources** is enabled, the client can view the list of resources it is allowed to access, making the permission scope clear to the user.

➢ **Operations and Management**

1. **Authorize and revoke access:** Family members can self-authorize by clicking the shared link. The administrator can select a client in the **LightLink Clients** list on the gateway web management page and click **Disable** or **Delete** at any time to revoke access immediately.
2. **View tunnel status:** In the **LightLink Clients** list, you can easily see each online/offline client's name, IP address, online duration, and transmitted/received traffic.
3. **Log-based troubleshooting:** If a connection fails, go to the gateway's **Logs** page and filter by keywords to view detailed handshake, authentication, and NAT hole-punching logs for faster troubleshooting.

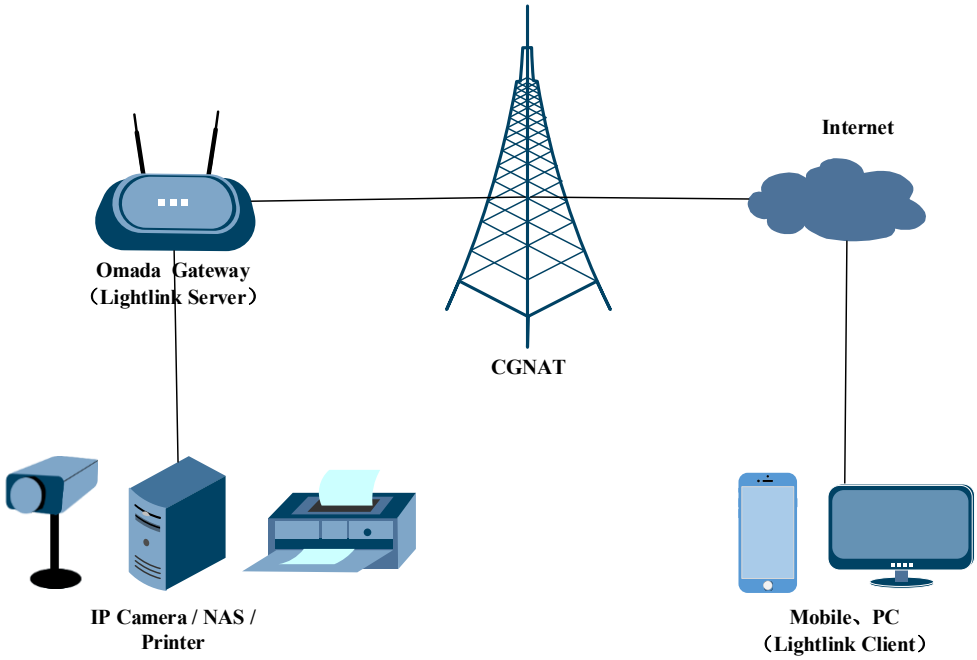
➢ **Comparison with Traditional Solutions**

Item	Traditional WireGuard / IPsec Remote Access	LightLink VPN
Server-side deployment	Requires a public IP, port forwarding configuration, and manual key-pair generation	One-click enable on the gateway; no public IP required; access credentials are generated automatically
Client configuration	Manually import a configuration file or enter the endpoint, public key, and allowed IPs	Tap a link; the app completes configuration automatically

NAT traversal	Relies on user-configured DDNS or port forwarding; cannot traverse CGNAT	Cloud-assisted coordination + automatic STUN hole punching; works in CGNAT environments
Access control	Typically exposes the entire LAN subnet; cannot restrict by device	Precise restrictions by IP / subnet / device; can allow access only to the NAS and cameras
Target users	Requires basic networking knowledge	No technical knowledge needed for typical family members; sharing and onboarding can be completed in about 1 minute

4.1.4 Network Topology

Home devices (phone/laptop, LightLink client) → Internet → ISP NAT network → Home Omada gateway (LightLink server) → LAN resources (NAS / cameras / printer)



4.2 Remote Access for SMBs / Chain Stores

4.2.1 Scenario Description

A small chain coffee shop has five branches and one headquarters. Each branch deploys a Fusion Gateway. Headquarters needs to regularly collect data from each branch's POS system, surveillance system, and inventory server. Meanwhile, IT staff must be able to

remotely log in to branch gateways for maintenance and troubleshooting. Due to high employee turnover, remote access permissions need to be granted and revoked quickly.

4.2.2 Requirements and Pain Points

- The enterprise/branches do not have public IP addresses, and the network environment is complex (multi-layer routing and firewall restrictions).
- High employee turnover requires fast provisioning and deprovisioning of remote access.
- Role-based permissions are required: only business subnets (POS systems and office servers) should be accessible, while core internal networks must be blocked.
- Using traditional VPNs (e.g., IPsec) to build site-to-site VPNs requires complex IKE policies, routing, and NAT traversal configuration on every branch gateway, resulting in high maintenance costs and a higher risk of misconfiguration.
- Low deployment cost is required, with no need to purchase additional VPN servers or leased lines.

4.2.3 LightLink VPN Solutions

➢ **Technical Solution Overview**

1. **Batch deployment and management:** Omada Cloud centrally manages all gateways, generates LightLink onboarding credentials in bulk, and distributes them to branches/employees with one click.
2. **Reliable cross-NAT connectivity:** Works with multi-layer NAT and firewall-restricted environments at branches; P2P direct connections reduce relay bandwidth consumption.
3. **Role-based access control:**
   a) General staff: Access only office subnets and shared printers.
   b) Operations/IT staff: Access branch gateways and POS servers.
   c) Administrators: Full control (customizable policy-based permissions).
4. **Lightweight and cost-effective:** Built on native Omada gateway capabilities—no additional hardware/software deployment required, reducing IT investment.
5. **Temporary access and auditing:** Generate time-bound onboarding credentials for short-term staff or external auditors; access expires automatically. All access logs can be recorded for post-event auditing.

➢ **Configuration Steps**

1. **Onboard all branch gateways to Omada Cloud:** Each Fusion Gateway completes initial setup and is bound to the same Omada Cloud account so that all online gateways are visible in the cloud platform. Enable LightLink VPN on each branch gateway.
2. **Generate onboarding credentials for staff/IT:** Go to the Omada Cloud LightLink VPN configuration page, choose **Invite via By Link** or **By Email**. For different roles, generate separate links and bind them to different permissions through access control policies later.
3. **Configure role-based access control:** On each gateway's LightLink VPN page, use **Access Control** to define policies for general staff, IT/ops staff, and administrators.
4. **Distribute links and monitor connections:** Send the generated links to the relevant employees via email or corporate IM. After installing the Navi app, employees can tap the link to connect. In **LightLink Clients** (on the cloud platform or on each gateway), view connected clients, time online, traffic, and revoke a client's access at any time.

- **Operations and Management**

1. **Role-based authorization:** In Omada Cloud, generate different access links for different roles (e.g., store manager, IT/ops, and finance), and bind each link to the corresponding LAN resource access policy in the gateway's **Access Control**.
2. **Permission management:** Generate links for short-term employees or external consultants, and revoke access upon expiration from the **LightLink Clients** list.
3. **Centralized monitoring:** In Omada Cloud, view the number of LightLink sessions and online status for all branch gateways. Go down to a specific gateway for a detailed client list.
4. **Audit logs:** Omada Cloud provides complete access logs that record who, when, from which IP, and which resource was accessed, meeting compliance audit requirements.

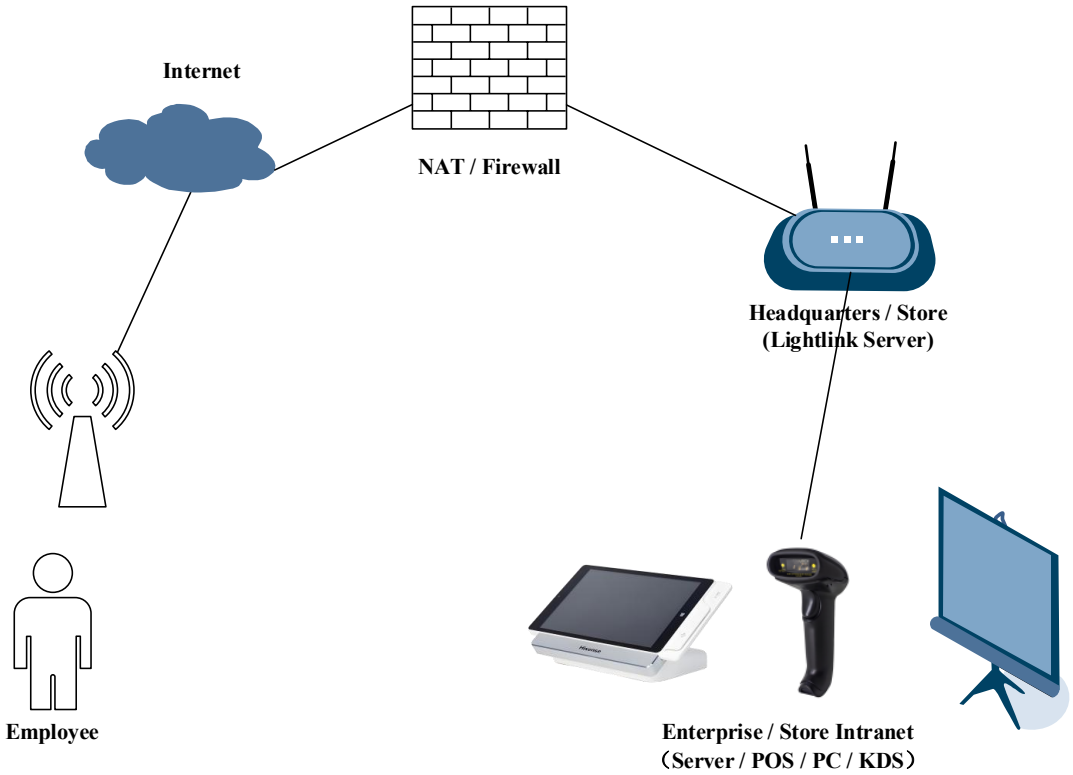
- **Comparison with Traditional Solutions**

Item	Traditional IPsec Site-to-Site / Remote Access	LightLink VPN
Branch deployment	Requires configuring IKE policies, routing, and NAT traversal; each store must be configured individually	Enabled centrally via the cloud on gateways;

		onboarding links can be generated in bulk
Employee onboarding	Requires installing a VPN client and manually entering the gateway address and certificates	One-tap onboarding via link; permissions are preconfigured by the administrator
Permission management	Typically subnet-based access; difficult to refine by role	Supports role-based restrictions (staff / IT ops / admin) on accessible resources
Temporary access	Manual user account add/remove; expirations are easy to miss	Time-limited links can be issued; access expires automatically; audit logs are supported
O&M cost	Requires skilled personnel; troubleshooting is difficult when errors occur	Cloud-based visual management; one-click revocation of access

4.2.4 Network Topology

Employee device (LightLink client) → Internet → NAT / firewall → HQ/branch Omada gateway → corporate/branch LAN → specified business resources (POS systems / office servers)



4.3 Mobile Work / Remote Work

4.3.1 Scenario Description

The company allows employees to use personal laptops or smartphones to work remotely from any public location such as home, cafés, or hotels. Employees need secure access to internal corporate resources, including the OA system, file servers, and code repositories. However, public Wi-Fi networks pose risks such as eavesdropping and phishing. The company also has temporary contractors and visitors who require time-limited, scope-limited access to enterprise resources.

4.3.2 Requirements and Pain Points

- Employees must securely access the corporate intranet when using public Wi-Fi in hotels, cafés, airports, and similar environments.
- Public networks may be subject to eavesdropping and phishing; data transmission must be protected with encryption.
- Temporary contractors and visitors require time-limited and limited-scope access to enterprise resources.
- With a large number of employees, traditional VPN client configuration is complex and can easily conflict with corporate firewall policies.

4.3.3 LightLink VPN Solutions

- **Technical Solution Overview**
  1. **Secure encryption over public networks:** Built on WireGuard encryption to protect data transmission on public networks against eavesdropping and tampering.
  2. **Fast access anytime, anywhere:** One-click connection as long as internet access is available; works across 4G/5G and public Wi-Fi.
  3. **Temporary access control:** Issue time-bound onboarding credentials for contractors/visitors; access expires automatically and only specified business systems are exposed.
  4. **Seamless network switching:** The client supports automatic reconnection when the network changes, ensuring continuity for work sessions.
- **Configuration Steps**
  1. **Enable LightLink VPN on the corporate HQ Fusion Gateway:** Log in to the HQ gateway management page, go to **Configuration** > **Network Config** > **LightLink VPN**, and enable it.

2. **Generate access links for different roles:** Email links to full-time employees via corporate email; send invitation links to temporary staff/visitors.
3. **Configure access control policies:** In **Access Control**, set allowed resources based on the employee's department or role.
4. **Employee client onboarding:** Employees install the TP-Link Navi app on their devices and tap the received link. The app automatically configures and connects. Once connected, employees can securely access the authorized enterprise resources.
5. **Monitoring and auditing:** In **LightLink Clients**, view connection status, time online, and traffic for all remote-work clients. For temporary staff, delete the client entry from the list after the engagement ends to revoke access.

- **Operations and Management**

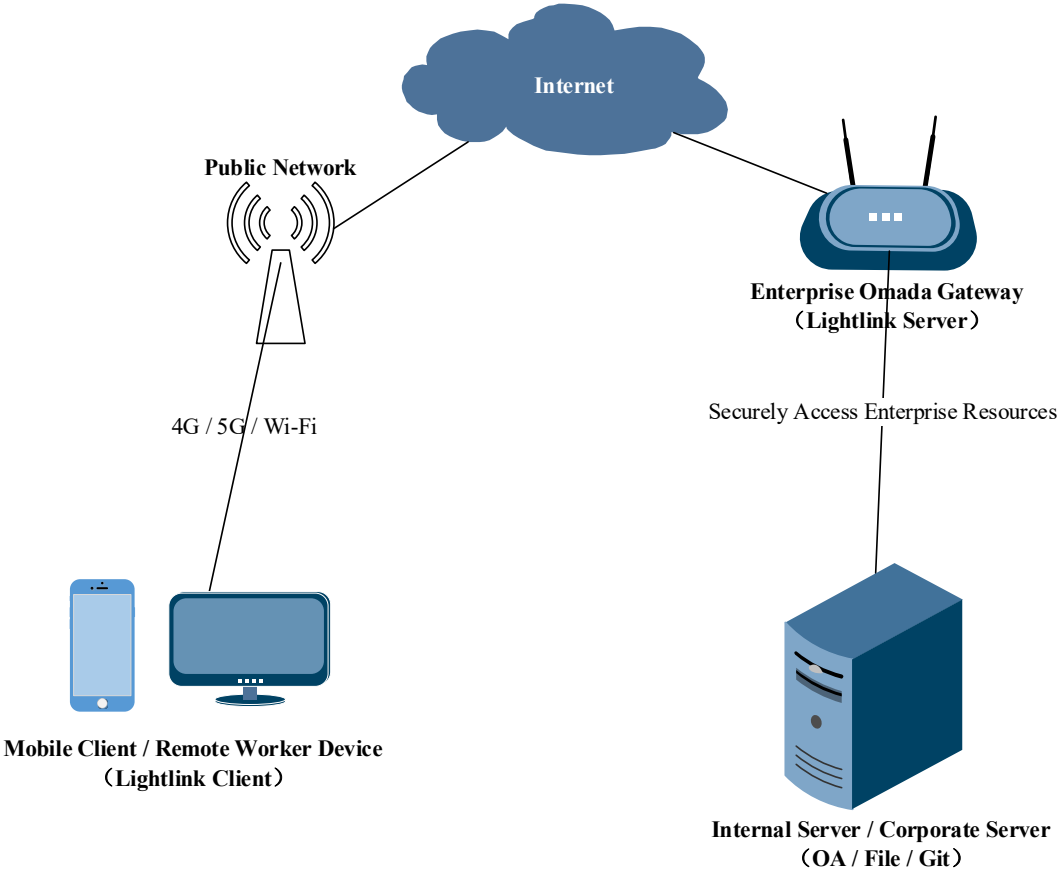
1. **Device access control:** On the gateway, administrators can enable MAC address verification or client certificates so that only company-issued and registered devices are allowed to connect, preventing account/link sharing.
2. **Connection diagnostics:** The Navi app includes built-in diagnostics. Users can run one-click tests for reachability to the gateway and view real-time tunnel throughput, packet loss, and latency to assess network quality.
3. **Link switching:** When switching from Wi-Fi to 5G, WireGuard tunnels can be re-established within seconds thanks to the resilience of underlying UDP sessions—keeping services uninterrupted and requiring no user intervention.

- **Comparison with Traditional Solutions**

Item	Traditional SSL VPN / IPsec IKEv2	LightLink VPN
Public Wi-Fi security	Tunnel encryption is available, but client configuration is complex	WireGuard-encrypted tunnel with one-click connection
Network switching adaptability	Often requires reconnecting or re-authentication after switching networks	Automatic reconnection, seamless to the user
Temporary contractor management	Requires creating temporary accounts on the VPN gateway and manually revoking them	Issues time-limited links that expire automatically
Client compatibility	Different devices often require different configuration profiles	One Navi app across platforms; a unified link-based onboarding experience

4.3.4 Network Topology

Mobile client device initiates connection → public network (4G/5G/Wi-Fi) → Internet → enterprise Omada gateway → enterprise LAN servers → LightLink encrypted tunnel → secure access to enterprise resources



4.4 IoT / Edge Device Remote O&M Scenario

4.4.1 Scenario Description

An industrial automation company has deployed thousands of edge computing devices based on Fusion Gateways across substations and factories in different regions. Engineers need to remotely log in from headquarters to perform firmware upgrades, configuration changes, and fault diagnostics. These devices are behind 4G/5G networks, have no public IP addresses, and are unattended.

4.4.2 Requirements and Pain Points

- IoT gateways and edge nodes are deployed across plants, construction sites, and outdoor environments with no public IP and no on-site personnel.
- O&M teams must remotely debug, upgrade, and troubleshoot without on-site access.

- O&M permissions must be strictly controlled: only the device itself should be accessible, and access to downstream IoT device clusters must be prohibited.

4.4.3 LightLink VPN Solutions

➢ **Technical Solution Overview**

1. **O&M without public IP:** The edge Fusion Gateway includes a built-in LightLink server. After powering on, it registers with the cloud platform and maintains a lightweight control channel. Engineers can initiate connection requests from the cloud at any time; the cloud coordinates NAT traversal, eliminating the need to configure a public IP or port forwarding per device.
2. **Device-level access restriction:** Configure resource access policies on the edge gateway to allow the remote O&M client to access only the gateway's own management IP and specified ports (e.g., 22 for SSH, 443 for HTTPS). No downstream IoT subnets are exposed, enforcing the principle of least privilege.
3. **Stable long-lived sessions and auto-reconnect:** A persistent heartbeat channel is maintained between the edge gateway and the cloud platform, with auto-reconnecting supported. If the network briefly drops during O&M, the tunnel can be rebuilt quickly, preventing long-running operations (firmware upgrades and configuration pushes) from being interrupted.
4. **Bulk O&M and unified cloud management:** Through Omada Cloud, administrators can view all online edge devices and initiate O&M connections with one click, without tracking device addresses one by one.

➢ **Configuration Steps**

1. **Initial setup and cloud binding:** Power on the edge Fusion Gateway and bring it online. Bind it to the enterprise cloud account via the Omada app or the web UI.
2. **Enable LightLink VPN:** Log in to Omada Cloud, open the device list, select the target edge gateway → **Remote Configuration** → enable **LightLink VPN**.
3. **Configure device-level access control**.
4. **Generate onboarding links for O&M engineers**.
5. **Remote connection:** Engineers install the Navi app on their computers and tap the link to connect to the VPN. Once connected, they can perform remote debugging, upgrades, and log viewing via SSH or HTTPS.
6. **Revoke access after O&M is complete**.

- **Operations and Management**

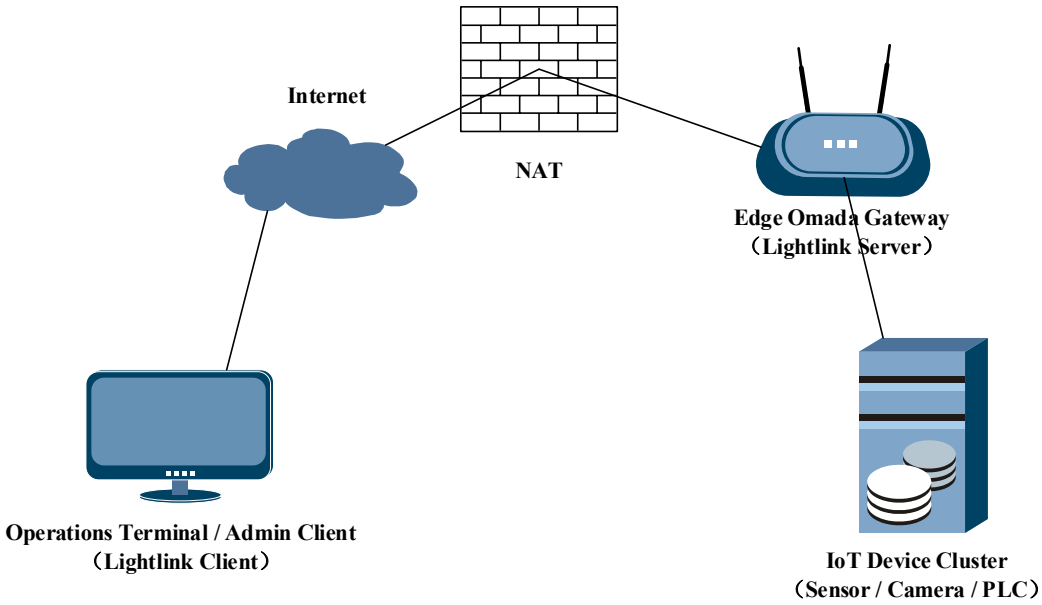
1. **Site adding/removal:** When a new edge device is powered on and bound to the cloud account, it automatically joins the enterprise network and can receive LightLink configurations in bulk via cloud policies. When a device is not needed or taken offline, remove it from the cloud to immediately block all access.
2. **Deep tunnel status monitoring:** In Omada Cloud, view each edge gateway's Underlay status (physical network, such as 4G signal strength and public IP) and Overlay status (WireGuard tunnel, such as latest handshake time and tunnel throughput).
3. **Proactive alerts:** When tunnels drop, devices go offline, or traffic anomalies occur, the system automatically sends alerts to the O&M team via email or corporate IM.

- **Comparison with Traditional Solutions**

Item	Traditional Port Forwarding / SSH Gateway	LightLink VPN
Devices without public IP	Cannot be mapped directly	Devices register to the cloud automatically; NAT traversal is performed on demand
Least privilege	Once a port is forwarded, it can be scanned from the entire internet	Only authorized clients can access, and access is restricted to the device itself
Bulk O&M	Requires recording the public address of each device	Unified device inventory in the cloud; one-click connection initiation
Reconnection	Highly dependent on network stability; long operations may be interrupted	Heartbeat + auto-reconnect keeps firmware upgrades from dropping

4.4.4 Network Topology

O&M terminal → Internet → NAT network → edge Omada gateway → IoT device cluster → remote debugging / upgrades



5 Brief Introduction of Representative Models

Network Scale	Series	Target Scenario	Product Name	Industrial Design	Hardware Specification
Medium to Large Scale 200+ Devices 1000+ Clients 50xCameras	Fusion Max (Network+ Controller+ Physical Security)	Medium Offices	Fusion Max 10G PoE		- CPU Info: 4 Core Armv8 1.6/2.2GHz - RAM & eMMC: 8GB DDR4 32GB eMMC - Video Storage (Only Tray): 2xHDD - Port: 2x10G + 5x2.5G + 4xGE 8xPoE+, 200W
		Chains Stores / Restaurants	Fusion Max 10G		- CPU Info: 4 Core Armv8 1.6/2.2GHz - RAM & eMMC: 8GB DDR4 32GB eMMC - Video Storage (Only Tray): 2xHDD - Port: 2x10G + 5x2.5G + 4xGE

Small Scale 40 Devices 300+ Clients 24xCameras	Fusion Pro (Network+ Controller+ Physical Security)	Small Offices (Unified Communication)	Fusion Pro 2.5G PoE		- CPU Info: 4 Core CA73 1.8GHz - RAM & eMMC: 4GB DDR4 32GB eMMC - Video Storage (Only Tray): SSD - Port: 9x2.5G 8xPoE+, 180W
			Fusion Pro 2.5G		- CPU Info: 4 Core CA73 1.8GHz - RAM & eMMC: 4GB DDR4 32GB eMMC - Video Storage (Only Tray): SSD - Port: 5x2.5G
			Fusion Pro Wi-Fi 7		- CPU Info: 4 Core CA53 1.8GHz - RAM & eMMC: 4GB DDR4 32GB eMMC - Video Storage (Only Tray): SD - Wi-Fi7 : 2 + 2 + 2 - Port: 2x10G + 4x2.5G 2xPoE+, 30W
	Fusion (Network + Controller)	Small Restaurants / Cafes (POS)	Fusion 2.5G PoE		- CPU Info: 4 Core CA73 1.8GHz - RAM & eMMC: 2GB DDR4 16GB eMMC - Port: 9x2.5G 8xPoE+, 110W
			Fusion 2.5G		- CPU Info: 4 Core CA53 / CA73 2.0GHz / 1.8GHz - RAM & eMMC: 2GB DDR4 16GB eMMC - Port: 5x2.5G

			Fusion G+		- CPU Info: 4 Core CA53 / CA73 2.0GHz / 1.8GHz - RAM & eMMC: 2GB DDR4 16GB eMMC - Port: 1x2.5G+4xGE
			Fusion Wi-Fi 7		- CPU Info: 4 Core CA53 1.5GHz - RAM & eMMC: 4GB DDR4 16GB eMMC - Wi-Fi 7: 2 + 2 - Port: 2x2.5G

6 Future Outlook

6.1 Technology Upgrades

1. **NAT Traversal Performance Optimization:** We will evaluate an AI-based intelligent port prediction approach as part of the R&D roadmap and explore ways to improve hole-punching success rates for symmetric NAT.
2. **Enhanced Encryption Protocols:** We will build upon WireGuard and add support for additional encryption algorithms to meet compliance requirements in government, enterprise, and financial sectors.
3. **Intelligent Path Selection:** Future releases will automatically detect network quality and switch intelligently between P2P direct connections and cloud relay to keep connections stable in poor network conditions.
4. **Intelligent QoS:** Future releases will integrate intelligent QoS to identify traffic types such as remote desktop, file transfer, and video conferencing, and dynamically assign in-tunnel bandwidth priority to keep critical applications running smoothly.
5. **Multipath Aggregation:** When a client (such as a phone) has both Wi-Fi and 5G available, we will explore virtualizing the two physical links into a single, more reliable, higher-bandwidth WireGuard tunnel to enable seamless handoff and bandwidth aggregation.

6.2 Application Scenario Expansion

1. **Industrial IoT Support:** We plan to support remote access for industrial gateways and PLC devices to meet remote operation and maintenance needs in industrial internet and smart factory deployments.
2. **Whole-Home Smart Integration:** We plan to integrate with the Omada smart home ecosystem to enable secure remote control of whole-home smart devices without exposing the internal network.
3. **Cross-Border Networking Optimization:** We will optimize global node deployment to support LightLink networking for cross-border enterprise branches and reduce cross-border access latency.

6.3 Ecosystem and Management Integration

1. **Seamless Multi-Platform Integration:** We plan to integrate more deeply with the Omada cloud management platform and office tools such as Teams to unify account and permission management.
2. **Open APIs:** We plan to provide third-party developers with LightLink access APIs to support custom remote-access solutions.
3. **SD-WAN Integration:** We plan to combine LightLink's lightweight access capabilities with SD-WAN technology to deliver an enterprise-level, low-cost WAN networking solution.

6.4 User Experience Improvements

1. **Frictionless Access:** We will enable devices to come online automatically after powering on and clients to connect automatically, with no manual action required.
2. **Visualized Operation and Maintenance:** We will display LightLink connection status, access logs, and traffic statistics on the Omada Controller to make monitoring easier for administrators.
3. **Simplified Deployment:** We will support one-scan enablement for LightLink, with zero configuration and no specialized expertise required.
4. **Continuous Authentication:** We will add multi-factor authentication based on device fingerprinting, geolocation, and behavioral analysis, and continuously assess trust after the connection is established—not only at login.

6.5 Development Vision

LightLink VPN will continue to focus on low barrier-to-entry access, strong security, and broad compatibility. It aims to become the preferred remote-access solution for homes,

small and medium-sized businesses, and edge computing scenarios. By shifting remote access from complex configuration to frictionless use, LightLink VPN will provide simpler, more secure, and more stable network connectivity services.

7 Appendix

7.1 Glossary

Term	Description
CGNAT	Carrier-Grade NAT. Large-scale NAT deployed by ISPs to mitigate IPv4 address exhaustion, which prevents users from obtaining a public IPv4 address.
Hub	Central node. In a Hub-Spoke topology, the headquarters gateway acts as the Hub and establishes VPN tunnels with all branch gateways.
Spoke	Branch node. In a Hub-Spoke topology, each branch gateway acts as a Spoke and establishes a VPN tunnel only with the headquarters Hub. Branches do not connect directly to each other.
ICE	Interactive Connectivity Establishment. A comprehensive NAT traversal framework that integrates multiple techniques such as STUN and TURN.
STUN	Session Traversal Utilities for NAT. A lightweight protocol that helps an endpoint learn its public-facing address and port.
TURN	Traversal Using Relays around NAT. A fallback approach that relays data through a relay server when P2P hole punching fails.
NAT	Network Address Translation. A technology that maps private IP addresses to public IP addresses, commonly used in home and enterprise networks.
NAT Penetration / Hole Punching	In networks where both sides are behind NAT, peers exchange public mapped addresses and send UDP packets to establish an end-to-end direct path.
P2P	Peer-to-peer. A communication model where two peers connect directly without relaying data through an intermediate server.

7.2 Technical Details

7.2.1 STUN Messages

The core STUN mechanisms include binding requests, binding responses, mapped-address discovery, and message-integrity protection. STUN's primary value is discovery and awareness. It helps an endpoint understand its current network environment and how it is mapped on the public internet.

It is important to note that STUN does not forward user traffic by itself, and it does not guarantee an end-to-end connection in every NAT environment. In real-world remote-access systems, STUN typically works with cloud-based parameter exchange, P2P hole-punching attempts, connectivity checks, keepalives, and the subsequent encrypted-tunnel setup process to establish connectivity in complex networks.

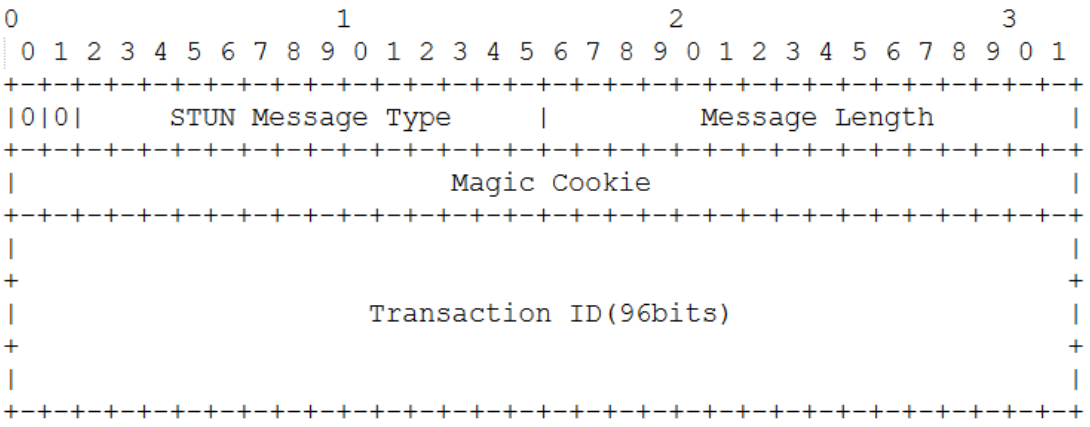


Figure 6 STUN Message Format

7.2.2 NAT Types

Common NAT behaviors can be summarized into the following types, from more permissive to more restrictive:

(1) Full-Cone NAT

Full-cone NAT is relatively permissive. After an internal host initiates traffic, the NAT maps the internal address and port to a public-facing address and port. As long as the mapping remains valid, any external host that knows the public address and port can try to send data to the internal host. As a result, this NAT type is generally more favorable for establishing P2P paths.

(2) Restricted-Cone NAT

Restricted-cone NAT limits which external sources can send inbound traffic. An internal host must first send traffic to a given external IP address before the NAT allows that external IP

address to send traffic back. Compared with full-cone NAT, this type places stricter requirements on hole-punching timing and peer address matching.

(3) Port-Restricted-Cone NAT

Port-restricted-cone NAT further restricts inbound sources on the basis of restricted-cone NAT. The external host must match not only the IP address but also the port number. In other words, only an external IP address and port that the internal host has previously reached may be allowed to send traffic back. As a result, P2P hole punching under this NAT type is more sensitive to probe-packet timing and port matching.

(4) Symmetric NAT

Symmetric NAT is the least friendly to P2P hole punching. It typically creates a different public mapping for different external destinations. The public mapping discovered via a STUN server may not work for subsequent communication with the real peer. In other words, the public address and port that the endpoint observes may differ from the mapping the peer must actually use, significantly increasing the hole-punching failure rate.

7.2.3 WireGuard Messages

WireGuard messages include the following fields:

- Type: 1 byte. Identifies the message type (handshake or data).
- Reserved: 3 bytes. Set to 0.
- Sender Index: 4 bytes. Identifies the tunnel endpoint.
- Encrypted Payload: Variable length. Contains the actual IP packet being carried or handshake data.

The message format is shown below:

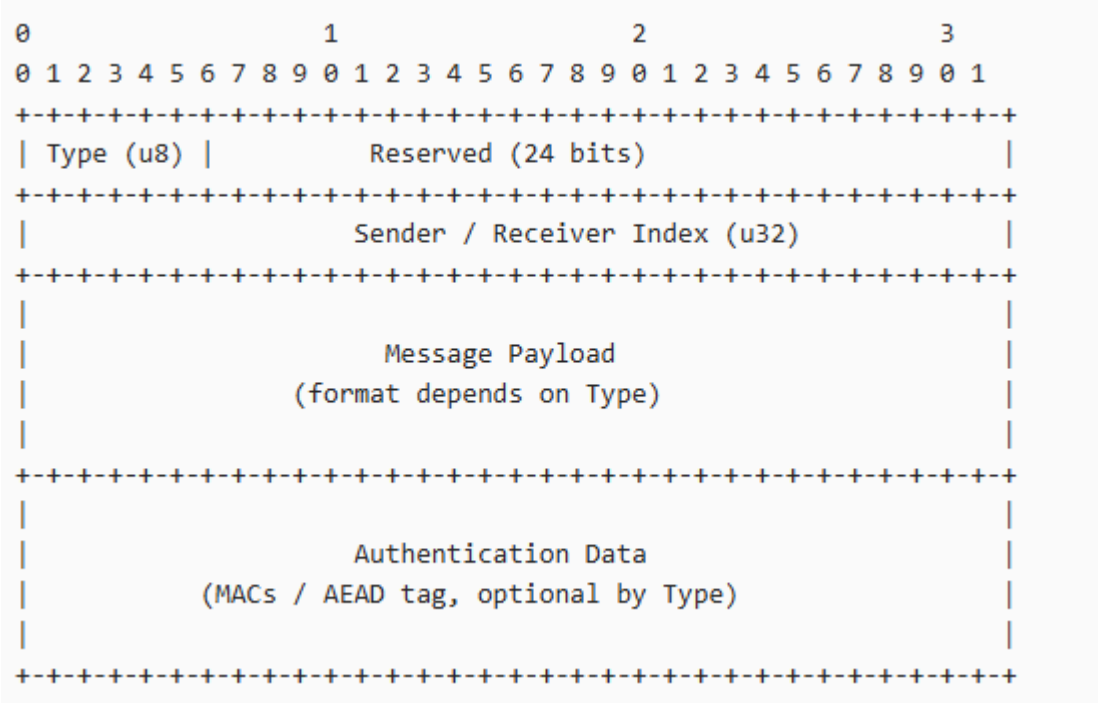


Figure 7 WireGuard Message Format