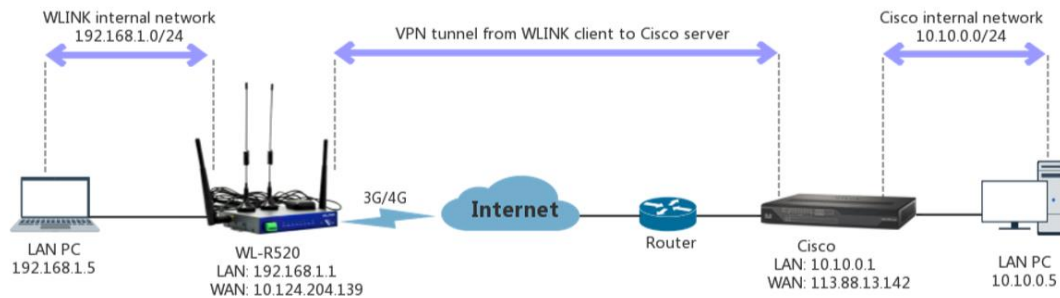


IPSec between WL-R520 and Cisco Router



(Network diagram)

1. Cisco Config (main mode)

```
!  
crypto isakmp policy 10  
  encr 3des  
  hash md5  
  authentication pre-share  
  group 2  
crypto isakmp key test1234 address 0.0.0.0 0.0.0.0  
!  
!  
crypto ipsec transform-set Tran-set esp-3des esp-sha-hmac  
crypto ipsec nat-transparency spi-matching  
!
```

2. WLINK Config

2.1 Navigate to **VPN Tunnel > IPSec > Group Setup**

WLINK

Cellular Router

| Status | IPSEC |
|------------------|--|
| Basic Network | IPSEC 1 IPSEC 2 SCHEDULE |
| WLAN | Group Setup Basic Setup Advanced Setup |
| Advanced Network | |
| Firewall | |
| VPN Tunnel | |
| GRE | |
| OpenVPN Client | |
| PPTP/L2TP Client | |
| IPSec | |
| Administration | |
| Debugging | |
| Logout | |

| IPSEC | |
|--------------------------------------|-------------------------------------|
| Enable IPsec | <input checked="" type="checkbox"/> |
| IPsec Extensions | Normal |
| Local Security Gateway Interface | 3G Cellular |
| Local Security Group Subnet/Netmask | 192.168.1.0/24 ex. 192.168.1.0/24 |
| Local Security Firewalling | <input checked="" type="checkbox"/> |
| Remote Security Gateway IP/Domain | 113.88.13.142 |
| Remote Security Group Subnet/Netmask | 10.10.0.0/24 ex. 192.168.88.0/24 |
| Remote Security Firewalling | <input checked="" type="checkbox"/> |

Save Cancel

2.2 Navigate to VPN Tunnel > IPsec > Basic Setup



IPSEC Router

IPSEC 1 | IPSEC 2 | SCHEDULE

Group Setup | **Basic Setup** | Advanced Setup

Keying Mode IKE with Preshared Key

Phase 1 DH Group Group 2 - modp1024

Phase 1 Encryption 3DES (168-bit)

Phase 1 Authentication MD5 HMAC (96-bit)

Phase 1 SA Life Time 28800 seconds

Phase 2 DH Group Group 2 - modp1024

Phase 2 Encryption 3DES (168-bit)

Phase 2 Authentication SHA1 HMAC (96-bit)

Phase 2 SA Life Time 3600 seconds

Preshared Key

Save Cancel

2.3 Navigate to VPN Tunnel > IPsec > Advanced Setup



IPSEC Router

IPSEC 1 | IPSEC 2 | SCHEDULE

Group Setup | Basic Setup | **Advanced Setup**

Aggressive Mode

Compress(IP Payload Compression)

Dead Peer Detection(DPD)

ICMP Check

Check Period Time Interval 10 seconds

Check Timeout Count 3 Times

Check IP 10.10.0.1

IPsec Custom Options 1 rightid=%any

IPsec Custom Options 2

IPsec Custom Options 3

IPsec Custom Options 4

2.4 Status

VPN Status

| | |
|----------------|---|
| IPSec 1 | Enable |
| Phase 1 Status | 73 seconds |
| Phase 1 IKE | 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024 |
| Phase 2 Status | TUNNEL |
| Phase 2 ESP | 3DES_CBC/HMAC_SHA1_96 |
| IPSec Recv. | 420 Bytes |
| IPSec Send. | 680 Bytes |