

Realizzazione di un Sistema ad Alta Affidabilità su OpenWrt con Dual WAN e Failover Avanzato

Antonio Francesco Gentile, Davide Macrì, Emilio Greco

RT-ICAR-CS-25-04

Gennaio 2025



Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
– Sede di Cosenza, Via P. Bucci 8-9C, 87036 Rende, Italy, URL: www.icar.cnr.it
– Sezione di Napoli, Via P. Castellino 111, 80131 Napoli, URL: www.icar.cnr.it
– Sezione di Palermo, Via Ugo La Malfa, 153, 90146 Palermo, URL: www.icar.cnr.it

Indice generale

Introduzione	3
Architettura del Sistema.....	3
a) Router OpenWrt dual WAN	4
b) Keepalived per la Gestione del Failover dei VIP.....	4
c) Contrackd per la Sincronizzazione delle Connessioni Attive.....	4
d) MWAN3 per Bilanciamento del Carico e Failover delle WAN.....	4
e) Script di Sincronizzazione delle Leases DHCP.....	4
Configurazione Dettagliata del Sistema	5
A. Configurazione di Base dei Router OpenWrt.....	5
B. Implementazione di Keepalived.....	6
C. Installazione e Configurazione di Contrackd.....	7
D. Configurazione di MWAN3.....	8
E. Gestione delle Leases DHCP.....	10
F. Test e Validazione del Sistema	11
Conclusioni.....	11
Bibliografia.....	12

Introduzione

In ambienti in cui la continuità del servizio e la resilienza della rete rappresentano requisiti critici, l'implementazione di soluzioni ad alta disponibilità (HA) diventa fondamentale. Questa relazione tecnica esplora un approccio pratico per configurare un sistema HA utilizzando router OpenWrt con doppia WAN. La configurazione proposta utilizza esclusivamente software open source, offrendo un'alternativa economica e personalizzabile rispetto alle soluzioni proprietarie.

L'obiettivo è descrivere un'architettura che garantisca la ridondanza sia a livello hardware che software. L'implementazione combina diverse tecnologie per assicurare un funzionamento continuo della rete anche in caso di guasti. Tra gli strumenti principali utilizzati figurano:

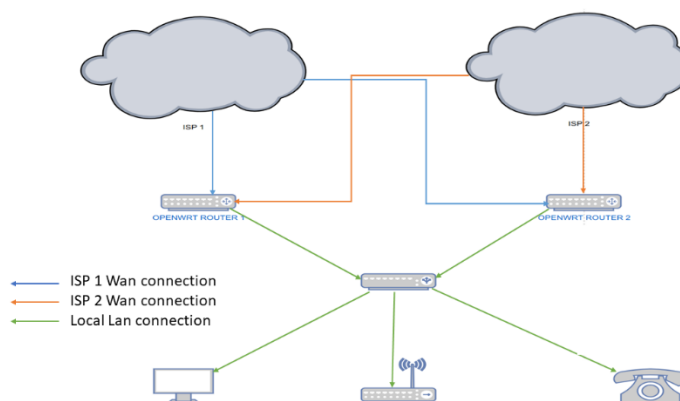
- a) **MWAN3**, per il bilanciamento del carico e il failover automatico delle connessioni WAN.
- b) **Keepalived**, per la gestione dei Virtual IP (VIP) e il failover tra router fisici.
- c) **Conntrackd**, per la sincronizzazione dello stato delle connessioni attive, assicurando la continuità delle sessioni di rete durante un failover.
- d) **Script di sincronizzazione DHCP**, per mantenere la coerenza delle leases DHCP tra i router e prevenire interruzioni nella rete LAN.

L'approccio descritto è particolarmente utile in contesti dove l'affidabilità della rete è cruciale, come in ambienti aziendali, infrastrutture critiche o sistemi di monitoraggio IoT. La soluzione garantisce che il traffico possa essere instradato su percorsi alternativi in caso di guasti di una delle connessioni WAN o di uno dei router, riducendo al minimo i tempi di inattività e l'impatto sull'operatività.

Questo rapporto tecnico si propone di fornire una guida tecnica per l'implementazione della soluzione, analizzando sia i vantaggi sia le sfide connesse all'uso di OpenWrt e di strumenti open source. Verranno inoltre approfonditi aspetti come l'architettura, la configurazione e le procedure di verifica della rete, al fine di garantire una comprensione completa e applicabile al contesto reale.

Architettura del Sistema

L'architettura descritta in questa relazione tecnica si basa su un'infrastruttura altamente affidabile, progettata per garantire continuità di servizio anche in caso di guasti di una delle connessioni WAN o di uno dei router. Questa configurazione combina funzionalità avanzate di gestione della rete con tecnologie open source per creare un sistema robusto e flessibile. Di seguito vengono descritti i componenti principali dell'architettura e il loro ruolo all'interno del sistema.



a) Router OpenWrt dual WAN

Il sistema utilizza due router fisici configurati con il firmware OpenWrt, un sistema operativo basato su Linux progettato per router e dispositivi di rete embedded. Entrambi i router sono configurati con doppia WAN, identificata come **WAN1** e **WAN2**, e con interfacce di rete locali (**LAN**) per la gestione del traffico interno. La configurazione con doppia WAN consente di sfruttare due connessioni Internet separate, aumentando la resilienza e la capacità di bilanciamento del carico.

Questi due router operano in modalità attivo/backup: mentre un router gestisce attivamente il traffico di rete, l'altro rimane in standby, pronto a subentrare in caso di guasto. Questa modalità operativa è realizzata attraverso il coordinamento di più strumenti software.

b) Keepalived per la Gestione del Failover dei VIP

Keepalived è il componente chiave utilizzato per gestire i Virtual IP (VIP) associati alle interfacce WAN e LAN. I VIP rappresentano indirizzi IP virtuali condivisi tra i due router, che vengono trasferiti dinamicamente dal router attivo al router di backup in caso di guasto. Keepalived monitora costantemente lo stato dei router e utilizza il protocollo **VRRP (Virtual Router Redundancy Protocol)** per orchestrare il failover. Questa configurazione garantisce che gli host interni possano sempre accedere alla rete attraverso un unico gateway, indipendentemente dal router attualmente attivo.

c) Contrackd per la Sincronizzazione delle Connessioni Attive

La sincronizzazione dello stato delle connessioni attive tra i due router è essenziale per garantire una transizione fluida durante il failover. Questo compito è gestito da **Contrackd**, un demone che replica lo stato delle connessioni tracciate (contrack) dal router attivo al router di backup. Grazie a Contrackd, le connessioni in corso, come download, streaming o sessioni VPN, non vengono interrotte quando il failover si verifica. Questo aumenta significativamente l'esperienza utente e riduce i tempi di ripristino.

d) MWAN3 per Bilanciamento del Carico e Failover delle WAN

MWAN3 è un componente integrato in OpenWrt progettato per gestire il bilanciamento del carico e il failover tra più connessioni WAN. In questa configurazione, MWAN3 assicura che il traffico sia distribuito in modo equilibrato tra WAN1 e WAN2, ottimizzando l'uso delle risorse disponibili. In caso di guasto di una delle connessioni WAN, MWAN3 reindirizza automaticamente tutto il traffico verso la connessione rimanente, garantendo la continuità del servizio. Questo strumento è altamente configurabile, consentendo di definire policy di routing specifiche per determinati tipi di traffico o per indirizzi IP particolari.

e) Script di Sincronizzazione delle Leases DHCP

Un ulteriore elemento di questa architettura è rappresentato dagli script personalizzati per la sincronizzazione delle leases DHCP tra i due router. Questi script assicurano che gli indirizzi IP assegnati dinamicamente ai dispositivi della rete locale siano coerenti su entrambi i router. La sincronizzazione evita conflitti o disconnessioni in caso di failover, poiché il router di backup eredita una mappa aggiornata degli indirizzi IP già assegnati. Questa funzionalità è particolarmente utile in reti con molti dispositivi dinamici, come quelle aziendali o IoT.

L'architettura descritta combina strumenti avanzati per creare un sistema ad alta disponibilità in grado di gestire con efficienza guasti a livello hardware o di connessione. L'integrazione di **OpenWrt**, **Keepalived**, **Conntrackd**, **MWAN3** e script di sincronizzazione DHCP garantisce che la rete rimanga operativa e stabile, fornendo una soluzione scalabile e robusta per scenari critici. Questa configurazione rappresenta un esempio concreto di come il software open source possa essere utilizzato per realizzare infrastrutture di rete altamente affidabili.

Configurazione Dettagliata del Sistema

Questo capitolo fornisce una guida pratica per implementare l'architettura ad alta affidabilità descritta in precedenza. Ogni sezione affronta un componente del sistema, spiegando come configurarlo per ottenere le funzionalità di failover, bilanciamento del carico, sincronizzazione delle connessioni e dovrebbe includere:

- A. **Configurazione di Base dei Router OpenWrt:**
- B. **Implementazione di Keepalived:**
- C. **Installazione e Configurazione di Conntrackd:**
- D. **Configurazione di MWAN3**
- E. **Gestione delle Leases DHCP:**
- F. **Test e Validazione del Sistema:**

A. Configurazione di Base dei Router OpenWrt

La configurazione dei router OpenWrt rappresenta il primo passo fondamentale per implementare l'architettura ad alta disponibilità. Ogni router deve essere configurato per gestire due connessioni WAN e una rete locale (LAN). Le interfacce WAN, denominate WAN1 e WAN2, possono essere configurate con indirizzi IP statici o dinamici, a seconda delle specifiche del provider. La rete LAN, invece, dovrebbe utilizzare indirizzi IP statici per garantire la coerenza e facilitare la comunicazione tra i router.

Un elemento essenziale di questa configurazione è l'installazione di MWAN3, un modulo di OpenWrt che gestisce il bilanciamento del carico e il failover tra le connessioni WAN. MWAN3 permette di distribuire il traffico su entrambe le connessioni, ottimizzando le prestazioni della rete, e di reindirizzarlo automaticamente in caso di guasto di una delle due WAN. Per configurarlo, è necessario modificare il file `/etc/config/mwan3`, definendo le regole di bilanciamento e di failover. Questo processo garantisce che la rete rimanga operativa anche in presenza di guasti.

I passaggi da seguire per configurare correttamente le interfacce di rete per gestire doppia WAN e LAN sono pertanto elencati di seguito:

1. **Configurazione delle Interfacce di Rete:**
 - WAN1 e WAN2 devono essere configurate con indirizzi IP statici o dinamici forniti dal provider.
 - La rete LAN deve essere configurata con un indirizzo IP statico, ad esempio 192.168.1.1 per il primo router e 192.168.1.2 per il secondo.
2. **Installazione di MWAN3:**
 - Installare MWAN3 su entrambi i router utilizzando il gestore di pacchetti:

```
opkg update
opkg install mwan3
```

- Configurare le policy di bilanciamento e failover editando il file `/etc/config/mwan3`:
 - Definire le interfacce WAN con priorità.
 - Configurare regole per reindirizzare il traffico in caso di guasto.

3. Abilitazione del Servizio MWAN3:

- Riavviare e abilitare il servizio MWAN3:

```
/etc/init.d/mwan3 restart
/etc/init.d/mwan3 enable
```

B. Implementazione di Keepalived

Keepalived è lo strumento che gestisce il failover dei Virtual IP (VIP), garantendo che gli host nella rete locale possano sempre accedere a un gateway attivo. Questa funzionalità è particolarmente importante nelle architetture di rete ad alta disponibilità, poiché assicura che il traffico interno ed esterno non subisca interruzioni in caso di guasto di uno dei router.

La configurazione di Keepalived prevede la definizione di un file `/etc/keepalived/keepalived.conf`, in cui vengono specificati i parametri per il monitoraggio dello stato dei router e la gestione dei VIP. Ad esempio, un router configurato come MASTER avrà una priorità superiore rispetto al BACKUP, e il protocollo VRRP (Virtual Router Redundancy Protocol) gestirà automaticamente il trasferimento del VIP al router di backup in caso di guasto del master. I passi principali per la configurazione sono:

1. Installazione:

- Installare Keepalived su entrambi i router:

```
opkg install keepalived conntrackd mwan3 ip-full
```

2. Configurazione dei File:

- Creare il file di configurazione `/etc/keepalived/keepalived.conf` su entrambi i router. Un esempio per il primo router:

```
vrrp_instance VI_WAN1 {
    state MASTER
    interface eth0
    virtual_router_id 51
    priority 100
    advert_int 1

    authentication {
        auth_type PASS
        auth_pass 1234
    }

    virtual_ipaddress {
        192.168.1.100/24
    }

    track_script {
        chk_wan1
    }
}

vrrp_instance VI_WAN2 {
```

```

state BACKUP
interface eth1
virtual_router_id 52
priority 90
advert_int 1

authentication {
    auth_type PASS
    auth_pass 1234
}

virtual_ipaddress {
    192.168.2.100/24
}

track_script {
    chk_wan2
}

}

vrrp_script chk_wan1 {
    script "ping -c 3 8.8.8.8"
    interval 5
}

vrrp_script chk_wan2 {
    script "ping -c 3 8.8.8.8"
    interval 5
}

```

Per il secondo router, cambiare **state** in **BACKUP** e ridurre la priorità.

3. Avvio del Servizio:

- o Avviare e abilitare Keepalived:

```

/etc/init.d/keepalived start
/etc/init.d/keepalived enable

```

C. Installazione e Configurazione di Contrackd

Per garantire che le connessioni in corso non vengano interrotte durante un failover, viene utilizzato Contrackd, un demone che sincronizza lo stato delle connessioni tracciate (contrack) tra i router. Questo strumento è essenziale in scenari di rete critici, come lo streaming in tempo reale o le sessioni VPN, dove la perdita di stato di connessione può causare disservizi significativi.

Contrackd funziona replicando le tabelle di connessione del router attivo al router di backup. La configurazione richiede la creazione di un file `/etc/contrackd/contrackd.conf`, in cui si specificano i parametri di sincronizzazione, inclusi gli indirizzi IP dei router e le porte utilizzate per la comunicazione. Una volta configurato, Contrackd assicura che il router di backup possa assumere immediatamente il ruolo del router attivo senza interrompere le connessioni esistenti.

I passi principali per la configurazione sono:

1. Installazione:

- o Installare Contrackd su entrambi i router:

```
opkg install contrackd
```

2. Configurazione:

- o Creare il file `/etc/contrackd/contrackd.conf` su entrambi Router:

```
Sync {
    Mode FTFW {
        DisableExternalCache On
    }

    UDP {
        IPv4_address 192.168.1.1
        IPv4_Destination_Address 192.168.1.2
        Port 3780
        Interface eth0
        SndSocketBuffer 1249280
        RcvSocketBuffer 1249280
    }

    Timeout {
        generic 30
        tcp 300
        tcp_syn_sent 60
        tcp_syn_recv 60
        tcp_fin_wait 120
        tcp_close_wait 30
        tcp_last_ack 30
        tcp_close 10
        udp 180
        icmp 30
    }
}
Sync {
    Mode FTFW {
        DisableExternalCache Off
    }

    UDP {
        IPv4_address "192.168.1.1"
        IPv4_Destination_Address "192.168.1.2"
        Port 3780
    }
}
```

3. Avvio del Servizio:

- o Avviare Contrackd:

```
/etc/init.d/contrackd start
/etc/init.d/contrackd enable
```

D. Configurazione di MWAN3

MWAN3 è uno strumento fondamentale per gestire il bilanciamento del carico e il failover tra le connessioni WAN in un ambiente ad alta affidabilità. Questo componente di OpenWrt permette di definire regole di routing specifiche, distribuendo il traffico in modo equilibrato tra le connessioni disponibili e reindirizzandolo automaticamente in caso di guasto. Nel contesto dell'architettura descritta, MWAN3 garantisce che la rete rimanga operativa anche quando una delle connessioni WAN non è più disponibile, minimizzando l'impatto per gli utenti.

WAN3 opera monitorando lo stato di ciascuna connessione WAN configurata e utilizzando metriche per determinare quale connessione debba essere utilizzata per instradare il traffico. Ogni connessione WAN viene configurata come un'interfaccia indipendente con parametri specifici, come la frequenza di monitoraggio e i criteri di riattivazione. Questo sistema permette di rilevare rapidamente eventuali problemi con una connessione e di trasferire il traffico sull'altra in modo trasparente.

Il file principale per la configurazione di MWAN3 è `/etc/config/mwan3`. Questo file definisce le interfacce WAN, i membri del bilanciamento del carico, le policy di routing e le regole di instradamento. Di seguito è riportato un esempio di configurazione per due connessioni WAN.

Configurazione delle Interfacce WAN Ogni connessione WAN è definita con parametri di monitoraggio che ne determinano l'affidabilità. In questo esempio, entrambe le interfacce WAN1 e WAN2 sono configurate per monitorare la connessione a intervalli regolari:

```
config interface 'wan1'
    option enabled '1'
    option reliability '1'
    option count '1'
    option timeout '2'
    option interval '5'
    option down '3'
    option up '8'

config interface 'wan2'
    option enabled '1'
    option reliability '1'
    option count '1'
    option timeout '2'
    option interval '5'
    option down '3'
    option up '8'
```

Questi parametri specificano che:

- La connessione viene verificata ogni 5 secondi.
- La connessione è considerata inattiva dopo 3 tentativi falliti e riattivata dopo 8 tentativi riusciti.

Definizione dei Membri del Bilanciamento del Carico I membri rappresentano le interfacce WAN utilizzate per il bilanciamento del carico, assegnando a ciascuna una metrica e un peso:

```
config member 'wan1_m1_w3'
    option interface 'wan1'
    option metric '1'
    option weight '3'

config member 'wan2_m2_w3'
    option interface 'wan2'
    option metric '2'
    option weight '3'
```

In questo esempio, entrambe le connessioni WAN hanno lo stesso peso, il che significa che il traffico sarà distribuito equamente tra loro. Le metriche definiscono la priorità di utilizzo: un valore più basso indica una priorità più alta.

Creazione delle Policy di Routing Le policy definiscono come i membri del bilanciamento devono essere utilizzati per gestire il traffico:

```
config policy 'balanced'  
  list use_member 'wan1_m1_w3'  
  list use_member 'wan2_m2_w3'  
  option last_resort 'unreachable'
```

In questa configurazione, il traffico viene bilanciato tra WAN1 e WAN2. Se entrambe le connessioni non sono disponibili, il traffico sarà contrassegnato come non raggiungibile.

Regole di Instradamento Le regole determinano quali policy devono essere applicate a specifici tipi di traffico:

```
config rule 'default_rule'  
  option dest_ip '0.0.0.0/0'  
  option use_policy 'balanced'
```

Questa regola applica la policy di bilanciamento "balanced" a tutto il traffico in uscita verso qualsiasi destinazione.

Una volta configurato, è necessario avviare e abilitare MWAN3 sul router. Questo può essere fatto con i seguenti comandi:

```
/etc/init.d/mwan3 restart  
/etc/init.d/mwan3 enable
```

Per verificare il funzionamento di MWAN3 e monitorare lo stato delle connessioni WAN, è possibile utilizzare il comando:

```
mwan3 status
```

Questo comando fornisce informazioni dettagliate sullo stato delle connessioni, inclusi i membri attivi e le regole applicate.

E. Gestione delle Leases DHCP

La sincronizzazione delle leases DHCP è un aspetto critico per garantire la continuità del servizio nella rete locale. Quando un router subentra al posto dell'altro, è fondamentale che il router di backup abbia una mappa aggiornata degli indirizzi IP già assegnati nella rete. Per ottenere questo risultato, è possibile utilizzare script personalizzati che copiano il file delle leases DHCP tra i due router.

Uno script tipico può utilizzare il protocollo SCP (Secure Copy Protocol) per trasferire il file `/tmp/dhcp.leases` dal router attivo al router di backup. Questo processo può essere automatizzato con cron, impostando un intervallo di sincronizzazione regolare. Questo approccio garantisce che i dispositivi nella rete non perdano la connessione durante un failover. I passi principali per la configurazione sono:

1. Creazione degli Script:

- Creare uno script per sincronizzare le leases tra i router, ad esempio:

```
#!/bin/sh  
scp /tmp/dhcp.leases root@192.168.1.2:/tmp/dhcp.leases
```

- Salvare lo script in `/usr/local/bin/sync-dhcp.sh` e renderlo eseguibile:

```
chmod +x /usr/local/bin/sync-dhcp.sh
```

2. Esecuzione Automatica:

- Utilizzare cron per eseguire lo script periodicamente:

```
crontab -e
```

Aggiungere la seguente riga per eseguire lo script ogni minuto:

```
* * * * * /usr/local/bin/sync-dhcp.sh
```

F. Test e Validazione del Sistema

Una volta completata la configurazione, è essenziale testare il sistema per verificare che funzioni come previsto. Il failover WAN può essere testato disabilitando manualmente una delle connessioni e verificando che MWAN3 reindirizzi il traffico all'altra WAN. Il failover dei router può essere simulato spegnendo uno dei dispositivi, mentre Contrackd può essere verificato monitorando le connessioni durante il processo di failover. Questi test garantiscono che il sistema sia pronto per affrontare scenari reali di guasto.

1. Test del Failover WAN:

- Disabilitare manualmente una delle connessioni WAN e verificare che MWAN3 reindirizzi il traffico all'altra connessione.

2. Test del Failover dei Router:

- Spegnere uno dei router e assicurarsi che Keepalived trasferisca i VIP al router di backup senza interruzioni.

3. Validazione delle Connessioni Attive:

- Durante un failover, verificare che le connessioni attive non vengano interrotte, grazie a Contrackd.

Conclusioni

La realizzazione di un sistema ad alta affidabilità utilizzando router OpenWrt con doppia WAN rappresenta una soluzione versatile e robusta per garantire la continuità del servizio in ambienti critici. L'architettura proposta combina strumenti open source avanzati, come Keepalived, Contrackd, MWAN3 e script di sincronizzazione delle leases DHCP, offrendo un'alternativa flessibile ed economicamente vantaggiosa rispetto alle soluzioni proprietarie.

Il sistema descritto in questo rapporto si distingue per la sua capacità di gestire il failover a livello sia di connessione WAN sia di hardware del router. Attraverso Keepalived e il protocollo VRRP, il traffico di rete viene reindirizzato dinamicamente tra i router fisici, garantendo un'unica configurazione gateway visibile agli host della rete locale. La sincronizzazione dello stato delle connessioni attive, gestita da Contrackd, aggiunge un ulteriore livello di resilienza, permettendo alle connessioni in corso di continuare senza interruzioni durante un failover.

Il bilanciamento del carico e il failover delle connessioni WAN sono gestiti da MWAN3, che ottimizza l'utilizzo delle risorse disponibili e offre una gestione flessibile del traffico in base a policy

personalizzate. Inoltre, la sincronizzazione delle leases DHCP mediante script garantisce la continuità del servizio nella rete locale, evitando conflitti IP e interruzioni di connettività.

Nonostante la complessità della configurazione, l'adozione di strumenti open source permette di ottenere un elevato livello di controllo e personalizzazione, rendendo questa soluzione particolarmente adatta per contesti aziendali, infrastrutture critiche e ambienti IoT. I test di validazione del sistema hanno confermato la sua affidabilità, dimostrando che il sistema è in grado di rispondere efficacemente a scenari di guasto e di mantenere la continuità operativa con tempi di inattività minimi.

In conclusione, questo rapporto tecnico fornisce una guida pratica per l'implementazione di un sistema ad alta affidabilità utilizzando tecnologie open source. La flessibilità e la scalabilità offerte da questa configurazione la rendono ideale per affrontare le sfide delle moderne infrastrutture di rete.

Bibliografia

1. OpenWrt Official Documentation. *User Guide and Tutorials*. Disponibile online: <https://openwrt.org/docs/start>, ultima consultazione il 11 Gennaio 2025.
2. Keepalived Official Website. *Keepalived Documentation and Tutorials*. Disponibile online: <https://keepalived.org/>, ultima consultazione il 11 Gennaio 2025.
3. Contrackd Official Documentation. *Contrackd Tools and Resources*. Disponibile online: <https://contrack-tools.netfilter.org/>, ultima consultazione il 11 Gennaio 2025.
4. MWAN3 Documentation in OpenWrt. *MWAN3 User Guide*. Disponibile online: <https://openwrt.org/docs/guide-user/network/wan/multiwan/mwan3>, ultima consultazione il 11 Gennaio 2025.
5. RFC 5798 - Internet Engineering Task Force (IETF). *Virtual Router Redundancy Protocol (VRRP)*. Disponibile online: <https://www.rfc-editor.org/rfc/rfc5798>, ultima consultazione il 11 Gennaio 2025.