Bash: rilevare gli host di una subnet senza usare nmap

Se desideri uno script Bash che rilevi gli host sulla tua rete locale senza utilizzare nmap, possiamo utilizzare altri strumenti come ping per il rilevamento degli host. Tuttavia, senza nmap, sarà più difficile e meno affidabile rilevare le porte aperte su ciascun host.

La soluzione potrebbe essere la seguente:

```
#!/bin/bash

# Definisci la subnet base e il range di indirizzi IP
da controllare
subnet="192.168.1"
start=1
end=254

echo "Scanning for active hosts in the subnet
$subnet.0/24..."

# Funzione per testare la connettività con ping
ping_host() {
    if ping -c 1 -W 1 $1 &> /dev/null; then
        echo "$1 is up"
    fi
}

# Esegue il ping a tutti gli indirizzi IP nel range
definito
for i in $(seq $start $end); do
```

```
    ip="$subnet.$i"
    # Esegui ping in background per velocizzare il
processo
    ping_host $ip &
done

# Aspetta che tutti i processi in background
terminino
wait

echo "Scan complete."
```

In dettaglio:

1. **Definizione della subnet e del range di IP**: Modifica la variabile `subnet` per riflettere i primi tre ottetti della tua rete locale e adatta `start` e `end` per coprire il range di IP che vuoi scansionare.
2. **Funzione di ping**: La funzione `ping_host` usa `ping` per verificare la disponibilità di un host. Se l'host risponde al ping, viene stampato un messaggio.
3. **Esecuzione parallela**: Per ogni IP nel range definito, il ping viene eseguito in background per velocizzare la scansione.
4. **Sincronizzazione**: `wait` è usato per assicurarsi che tutti i processi in background terminino prima di dichiarare completata la scansione.

Questo metodo è meno invasivo e non richiede strumenti aggiuntivi, ma è anche meno dettagliato e potrebbe non rilevare gli host configurati per ignorare i pacchetti ICMP (ping). Inoltre, non effettua la scansione delle porte, poiché farlo senza `nmap` richiederebbe un approccio molto più complesso e meno affidabile.