DHCP

DYNAMIC HOST CONFIGURATION PROTOCOL

Cos’è il DHCP

Il **Dynamic Host Configuration Protocol (DHCP)** è un protocollo di livello applicativo che permette ai dispositivi di una certa rete locale di ricevere automaticamente la configurazione IP necessaria per stabilire una connessione e operare su una rete più ampia basata su protocollo IP.

In una rete basata sul protocollo IP, ogni calcolatore ha bisogno di un indirizzo IP, scelto in modo tale che appartenga all'insieme di indirizzi possibili assegnati all'intera sottorete (cioè al Net_ID) a cui è collegato e che sia univoco, cioè non ci siano altri calcolatori che stiano già utilizzando quell'indirizzo.
Il compito di assegnare manualmente gli indirizzi IP ai calcolatori comporta infatti un rilevante onere per gli amministratori di rete; DHCP supporta questo compito automaticamente e in maniera dinamica, cioè solo quando richiesto dall'host.

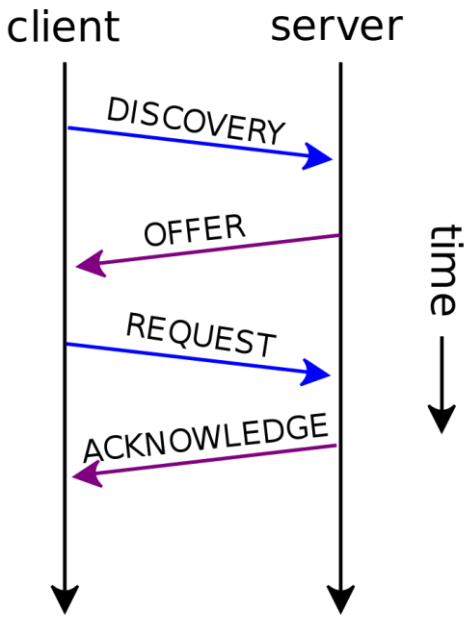
Una volta ricevuta la configurazione di rete il dispositivo della rete locale diventa a tutti gli effetti un host (ospite) della rete Internet e può utilizzare tutti i servizi offerti dalla rete stessa (un servizio DHCP è svolto anche da un semplice router di casa).

Come funziona il DHCP

Si ha bisogno di un **server DHCP** che distribuisca gli indirizzi IP: questo terminale servirà da base per tutte le richieste DHCP, e anch'esso deve avere un indirizzo IP fisso.

DHCP utilizza il protocollo UDP: le porte registrate sono la 67 per il server e la 68 per il client.

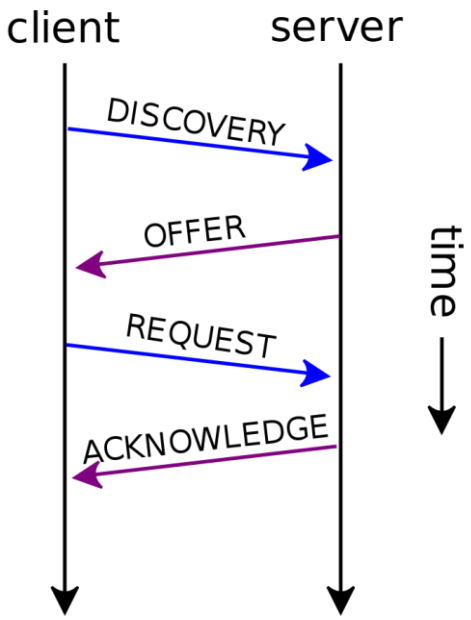
Quando un calcolatore vuole ottenere un indirizzo tramite DHCP, attiva il processo DHCP client: il client invia un pacchetto chiamato **DHCPDISCOVER** in broadcast, con indirizzo IP sorgente messo convenzionalmente a 0.0.0.0, e destinazione 255.255.255.255 (indirizzo di broadcast)



Come funziona il DHCP

Il pacchetto è ricevuto da tutto il dominio di broadcast e in particolare da tutti i server DHCP presenti, i quali possono rispondere (o meno) ciascuno con un pacchetto di **DHCPOFFER** in cui propongono un indirizzo IP e gli altri parametri di configurazione al client. Questo pacchetto di ritorno è indirizzato in broadcast all'indirizzo di livello datalink del client (che non ha ancora un indirizzo IP) cioè in unicast, per cui può essere inviato solo da un server che si trovi sullo stesso dominio di broadcast.

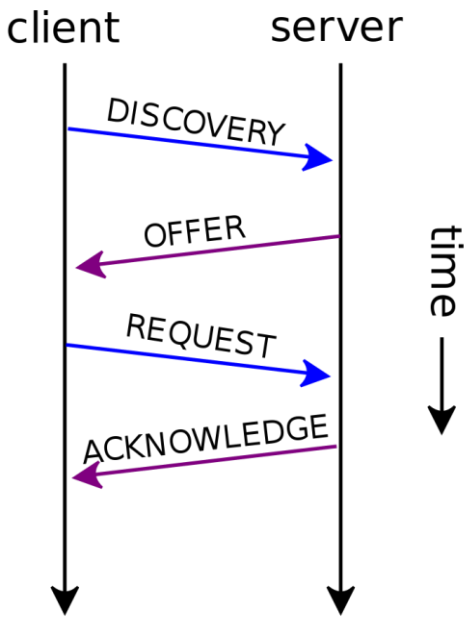
Il client aspetta per un certo tempo di ricevere una o più offerte, dopodiché ne seleziona una, e invia un pacchetto di **DHCPREQUEST** in broadcast, indicando all'interno del pacchetto, con il campo "server identifier", quale server ha selezionato. Anche questo pacchetto raggiunge tutti i server DHCP presenti sulla rete (direttamente o tramite un relay).

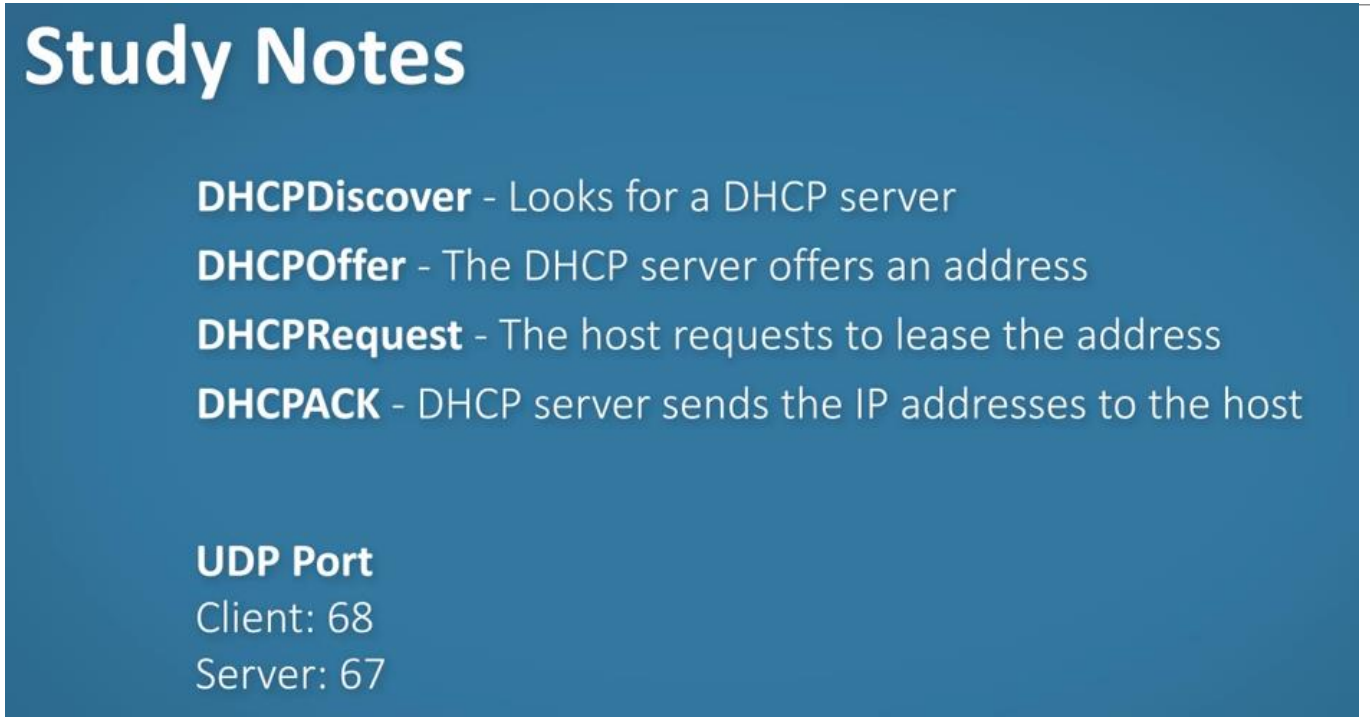


Come funziona il DHCP

Il server che è stato selezionato conferma l'assegnazione dell'indirizzo con un pacchetto di **DHCPACK** (nuovamente indirizzato in broadcast all'indirizzo di livello datalink del client, possibilmente attraverso un relay); gli altri server vengono automaticamente informati che la loro offerta non è stata scelta dal client, e che sulla sottorete è presente un altro server DHCP.

A questo punto, il client è autorizzato a usare l'indirizzo ricevuto per un tempo limitato, detto **tempo di lease**. Prima della scadenza, dovrà tentare di rinnovarlo inviando un nuovo pacchetto DHCPREQUEST al server, che gli risponderà con un DHCPACK se vuole prolungare l'assegnazione dell'indirizzo. Questi sono normali pacchetti IP unicast scambiati tra due calcolatori che hanno indirizzi validi. Se il client non riesce a rinnovare l'indirizzo, tornerà allo stato iniziale cercando di farsene attribuire un altro.





DCHP study notes

BOOTP

BOOTP (Bootstrap Protocol) è un precursore del DHCP: la differenza sostanziale tra i 2 è che il DHCP introduce l'assegnazione automatica dell'IP; il DHCP mantiene a tutti gli effetti la struttura del messaggio di BOOTP e supera il problema della «lentezza» dell'aggiornamento delle macchine che si spostano da una rete all'altra (specialmente dopo la diffusione del wireless).

Il BOOTP prevedeva che un server comunicasse al client solo tre informazioni:

- il suo indirizzo IP
- il nome del server da cui effettuare il download del file di boot
- il nome del file di boot

Considerata la diffusione di BOOTP, gli sviluppatori del DHCP decisero di non modificare il formato del messaggio e di specificare nel campo Options i campi con le informazioni utili a DHCP: in questo modo un DHCP Server può rispondere alle richieste di client BOOTP.

Assegnazione dinamica

I vantaggi dell'assegnazione dinamica degli indirizzi IP sono da ricercare in:

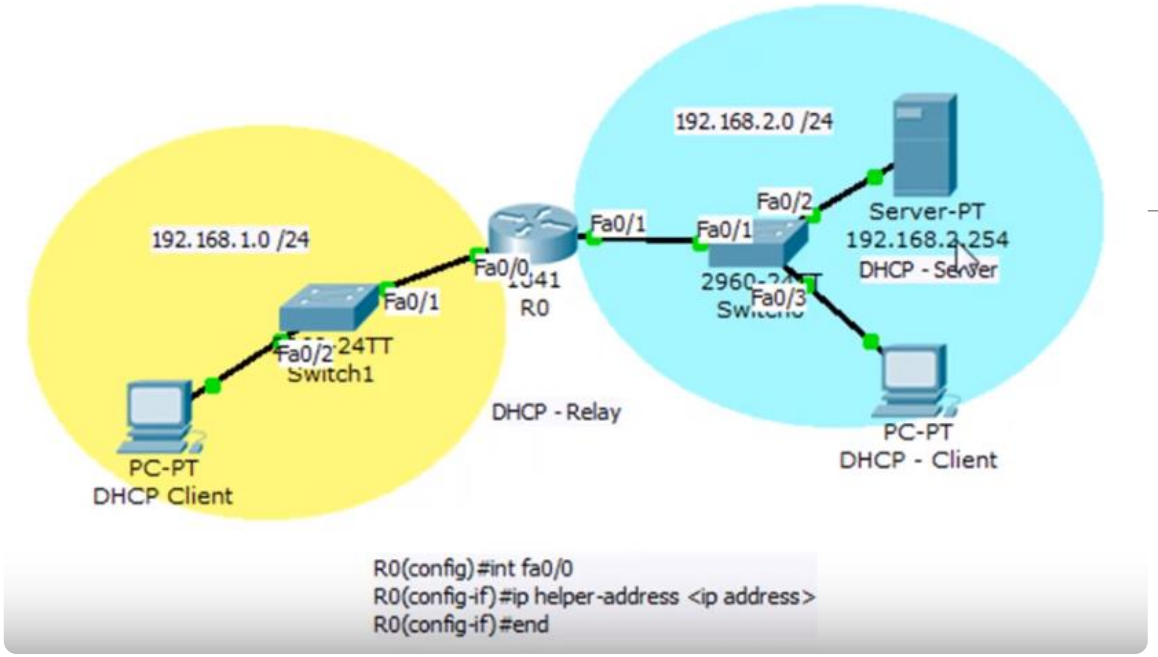
- **Automazione**
- **Gestione centralizzata**: l'amministratore può analizzare lo scenario sempre lavorando su una sola macchina, il DHCP server
- **Condivisione e riutilizzo degli indirizzi**: host di una rete non sempre connessi tutti insieme, quindi la rete può supportare un numero di host superiore al numero di indirizzi disponibili (condivisione); nel momento in cui un host non è più connesso alla rete il suo indirizzo IP torna nel pool a disposizione di altri client (riutilizzo).
- **Portabilità**: non essendoci un assegnamento predefinito host-indirizzoIP, qualunque client che si connetta alla rete può richiedere un indirizzo, supportando così la mobilità degli host.
- **Assenza di conflitti**

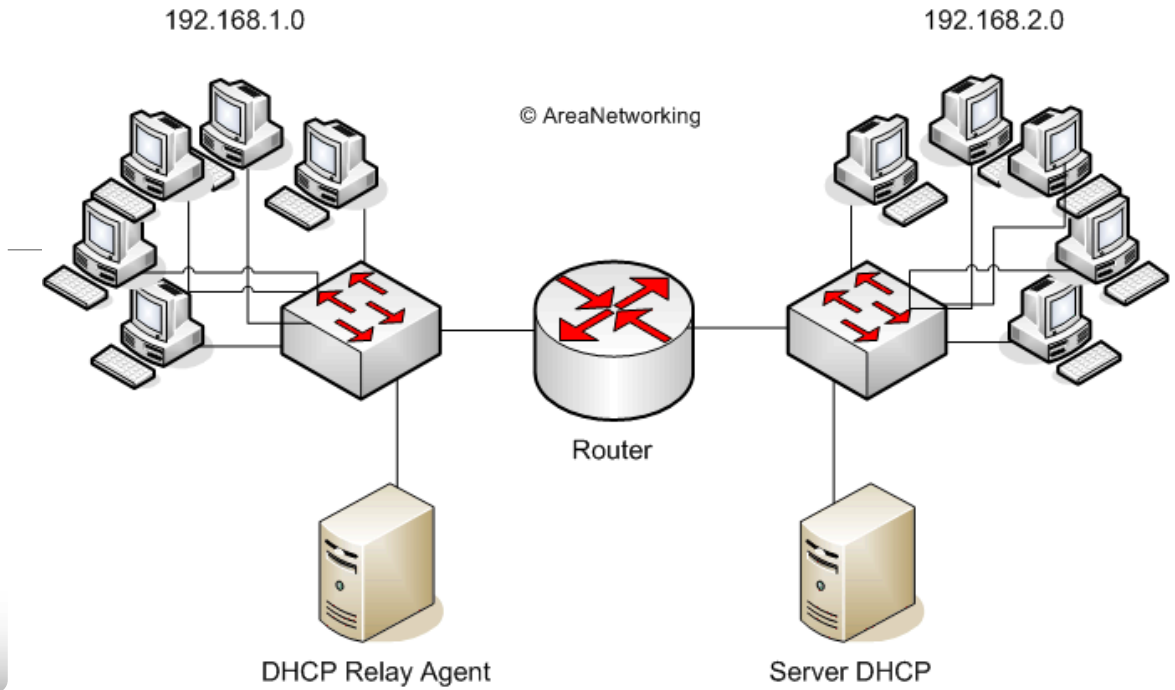
Tipi di assegnazione di indirizzi

DHCP permette 3 tipi di assegnazione degli indirizzi ed è l'amministratore di rete a scegliere il modo in cui il DHCP server risponderà per ogni rete o per ogni host:

- **Configurazione manuale**: solitamente l'amministratore assegna a router o altre macchine che si trovano «stabilmente» nella rete un indirizzo fisso
- **Configurazione automatica**: l'amministratore delega al DHCP server l'assegnazione di un indirizzo permanente all'host
- **Configurazione dinamica**: l'amministratore delega al DHCP server l'assegnazione di un indirizzo in «lease» all'host (cioè per un certo periodo di tempo) tra quelli disponibili nel pool a sua disposizione; al termine del periodo può essere richiesto un indirizzo nuovo o il rinnovo dell'attuale.

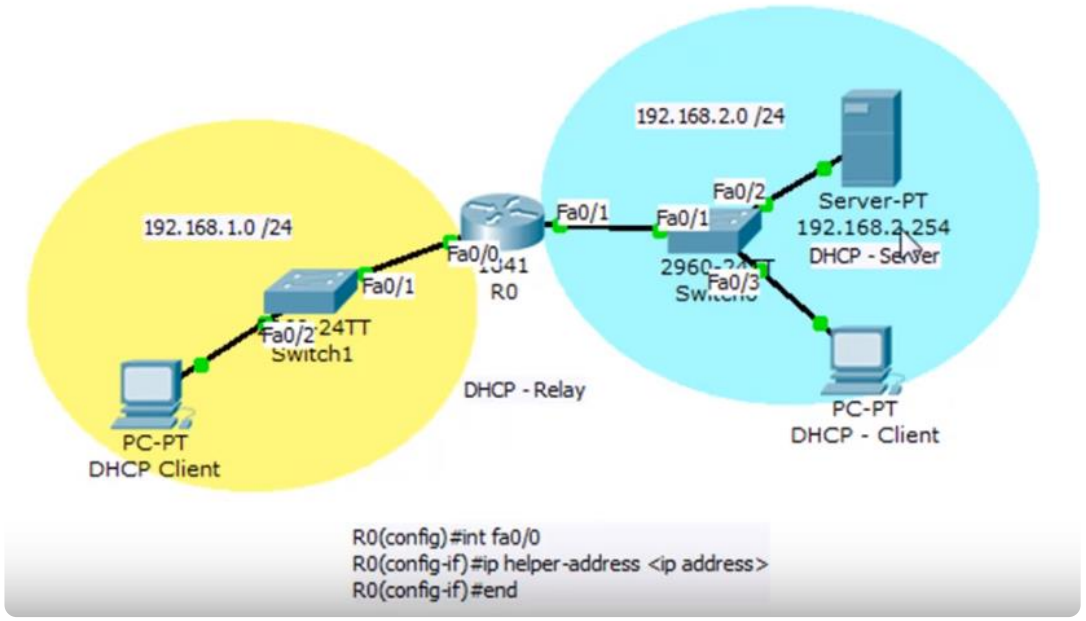
Uno dei compiti più delicati dell'amministratore è impostare la durata del lease (**lease length policy**); il periodo ottimale dipende dal tipo di rete e dalle necessità dell'host: un periodo lungo, offre agli host una certa stabilità (utile in caso si attendano risposte dalla rete, che farà riferimento all'indirizzo indicato nella richiesta); un periodo breve, risolve il problema del mantenere assegnato un indirizzo a un computer non più in rete. Costringe, però, un host attivo a richiedere continuamente il suo rinnovo. Appena "libero", l'indirizzo torna a disposizione degli altri host e, quindi nel pool.





DHCP Server multipli e relay agent

Helper Address



Nello scenario in figura R0 ha le seguenti configurazioni:

- `Fa0/0 → 192.168.1.1 /24`
- `Fa0/1 → 192.168.2.1 /24`

Il server DHCP è configurato con 2 pool:

- `serverPool1 → DHCP per la rete 192.168.2.0 /24`
- `serverPool2 → DHCP per la rete 192.168.1.0 /24`

Il router deve avere sull'interfaccia Fa0/0 un «helper-address» che consente ai pacchetti di broadcast (in particolare il DHCP discover) di poter raggiungere il DHCP server, altrimenti non potrebbero uscire dalla rete segmentata dal router:

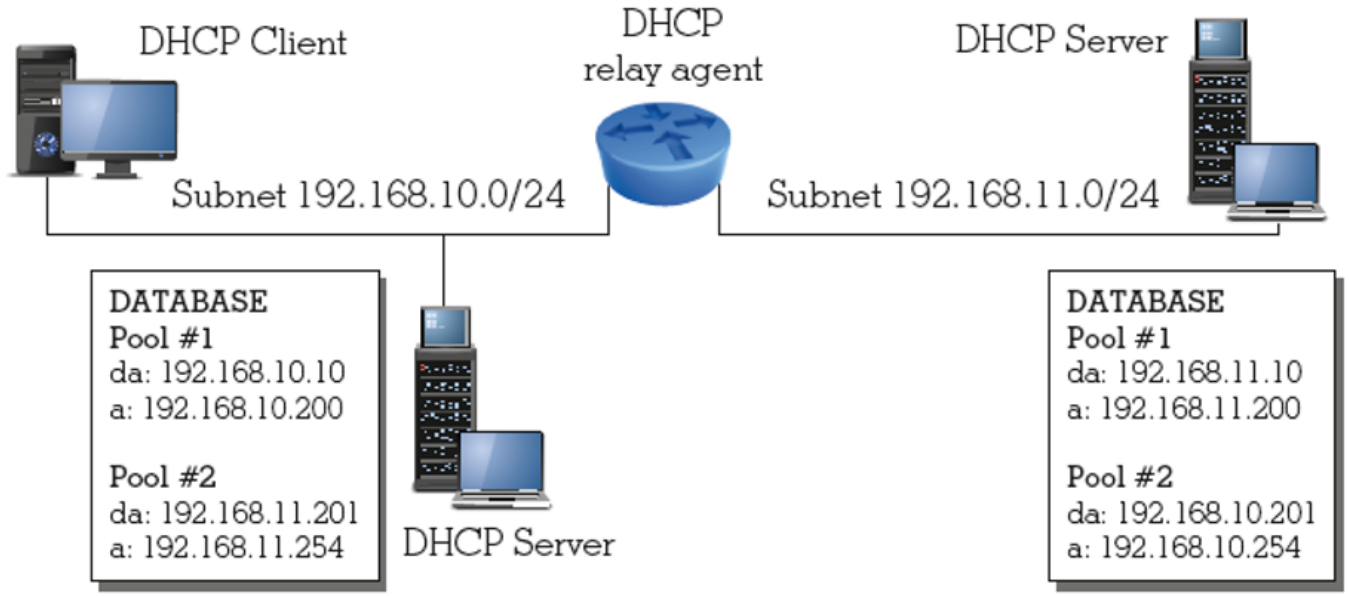
```
int Fa0/0
ip helper-address 192.168.2.254
```

Il router si comporta da «relay agent» (agente di ritrasmissione). Da notare che in questo scenario il DHCP server gestisce più subnet

DHCP Server multipli e relay agent

Tipicamente un solo server è sufficiente a soddisfare le esigenze legate all'operatività DHCP. Il motivo per cui si configurano più DHCP Server su un rete è legato alla **fault** tollerance: se l'unico server si guastasse gli utenti non avrebbero la possibilità di connettersi alla rete.

Il relay agent ha come scopo non soltanto quello di consentire la comunicazione tra subnet differenti (il caso del DHCP analizzato in precedenza), ma anche consentire il forward di tutti i frame UDP



Sicurezza

DHCP utilizza i protocolli UDP e IP che sono intrinsecamente insicuri e nelle sue specifiche non si fa riferimento a possibili misure per la sicurezza. Attualmente le problematiche di sicurezza sono le più critiche, soprattutto per un protocollo come DHCP che tratta informazioni di configurazione.

Possiamo dividere i problemi di sicurezza tra quelli riguardanti il server e quelli riguardanti il client in:

- ✓ **DHCP Server non autorizzati**: si potrebbe inserire un DHCP Server "abusivo" che risponda alle richieste del *client* fornendo informazioni false in modo da rendere inusabili host, oppure si forniscono informazioni di configurazioni tali da renderli utilizzabili per azioni fraudolente
- ✓ **DHCP Client non autorizzati**: un host potrebbe essere predisposto per sembrare un certo client e ottenere le informazioni di configurazione a esso destinate ed essere poi usato per creare danni alla rete, oppure si potrebbe usare un software che genera moltissime richieste DHCP così da esaurire gli indirizzi a disposizione del server e bloccare la rete in quanto nessun altro host in seguito riuscirebbe a ottenere un nuovo indirizzo

Appendix – DHCP router

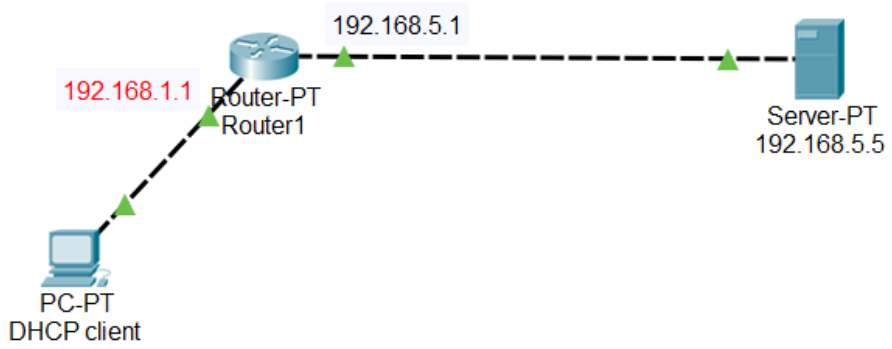
Configurazione DHCP router

```
ip dhcp pool MYPOOL
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
ip dhcp excluded-address 192.168.1.1 192.168.1.99
```

Per forzare il refresh dell'IP sul PC usare i comandi:

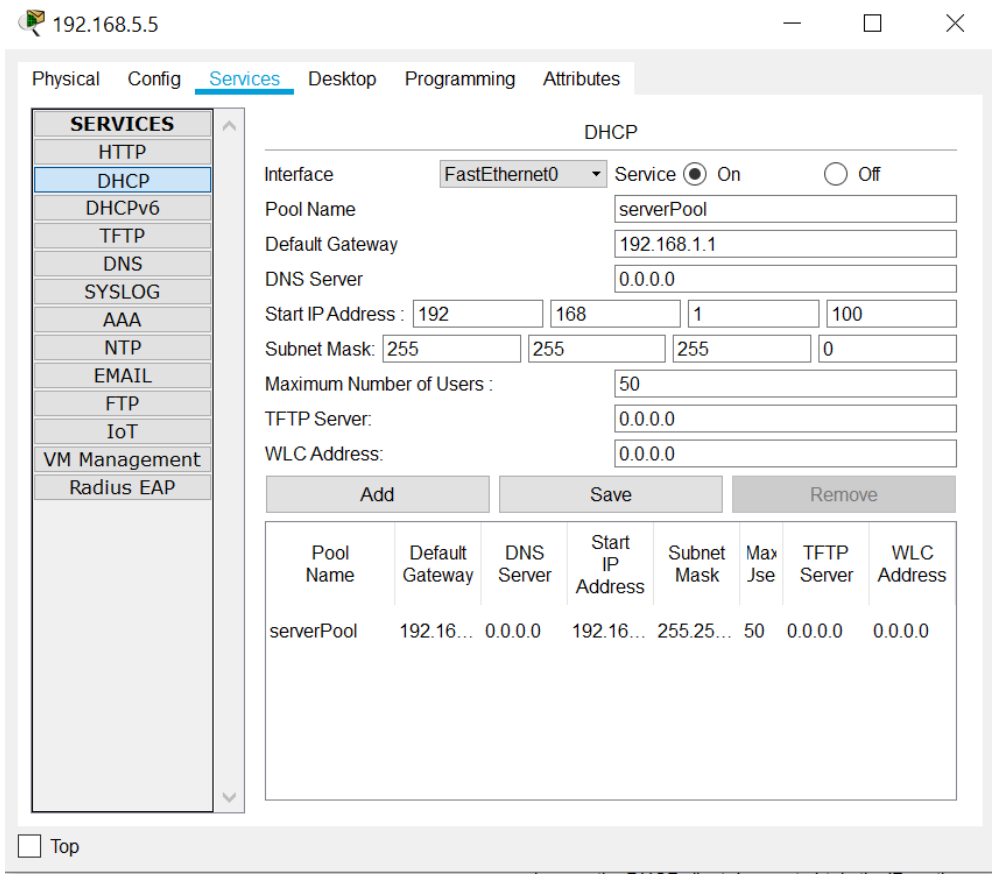
```
ipconfig /release
ipconfig /renew
```

Appendix – DHCP server



Configurazione router

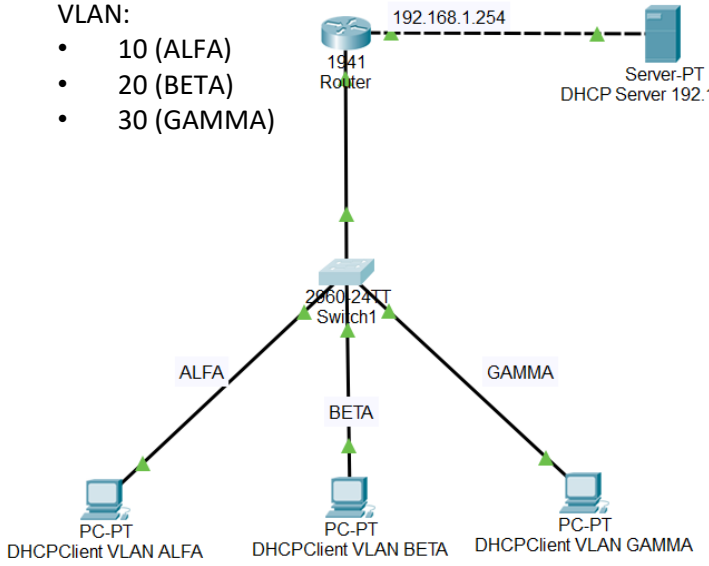
```
int fa0/0
ip helper-address 192.168.5.5
```



Appendix – DHCP server + VLAN

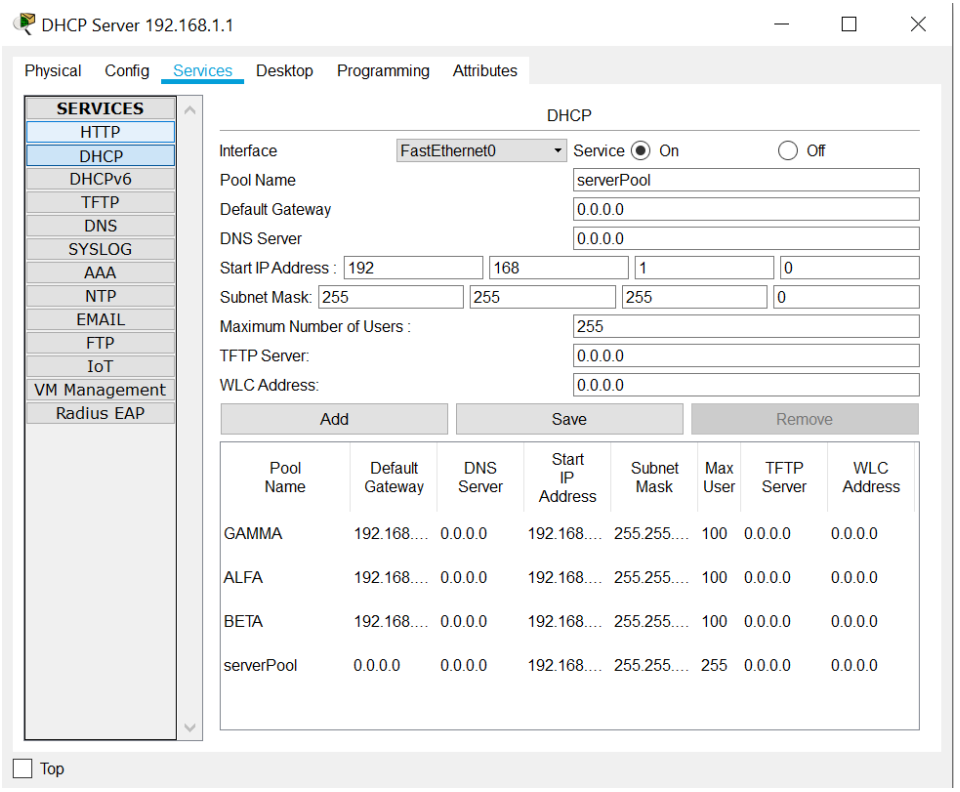
VLAN:

- 10 (ALFA)
- 20 (BETA)
- 30 (GAMMA)



Configurazione router – virtual interface

```
Router(config)#interface GigabitEthernet 0/0.1
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#ip helper-address 192.168.1.1
Router(config-subif)#exit
Router(config)#interface GigabitEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#ip helper-address 192.168.1.1
Router(config-subif)#exit
Router(config)#interface GigabitEthernet 0/0.3
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#ip helper-address 192.168.1.1
Router(config-subif)#exit
```



Appendix – VLAN

SWITCH COMMAND CONFIGURATION

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per
line.  End with CNTL/Z.
```

SHOW

```
Switch#show vlan
Switch#show run
```

VLAN CONFIGURATION COMMAND

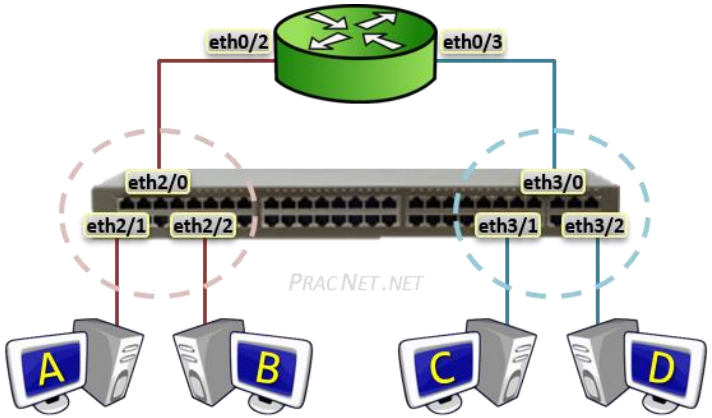
```
Switch(config)#vlan 10
Switch(config-vlan)#name ten
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name twenty
Switch(config-vlan)#exit
Switch(config)#exit
Switch#show vlan
```

ASSOCIATE ACCESS VLAN TO PORT

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

ASSOCIATE TRUNK VLAN TO PORT

```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,20
```



SWITCH: IP ASSOCIATION TO VLAN

```
Switch(config)#interface vlan 30
Switch(config-if)#ip address 192.168.30.2 255.255.255.0
```

Appendix – VLAN

ROUTER COMMAND CONFIGURATION

```
Router>enable
Router#configure terminal
Enter configuration commands, one per
line.  End with CNTL/Z.
```

SHOW

```
Router#show run
```

ROUTER IP ADDRESS CONFIGURATION

```
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.100.1 255.255.255.0
```

ASSOCIATE MULTIPLE IPS ON SAME PORT (One IP per VLAN)

```
Router(config-subif)#interface gigabitEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#interface gigabitEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#interface gigabitEthernet 0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
```