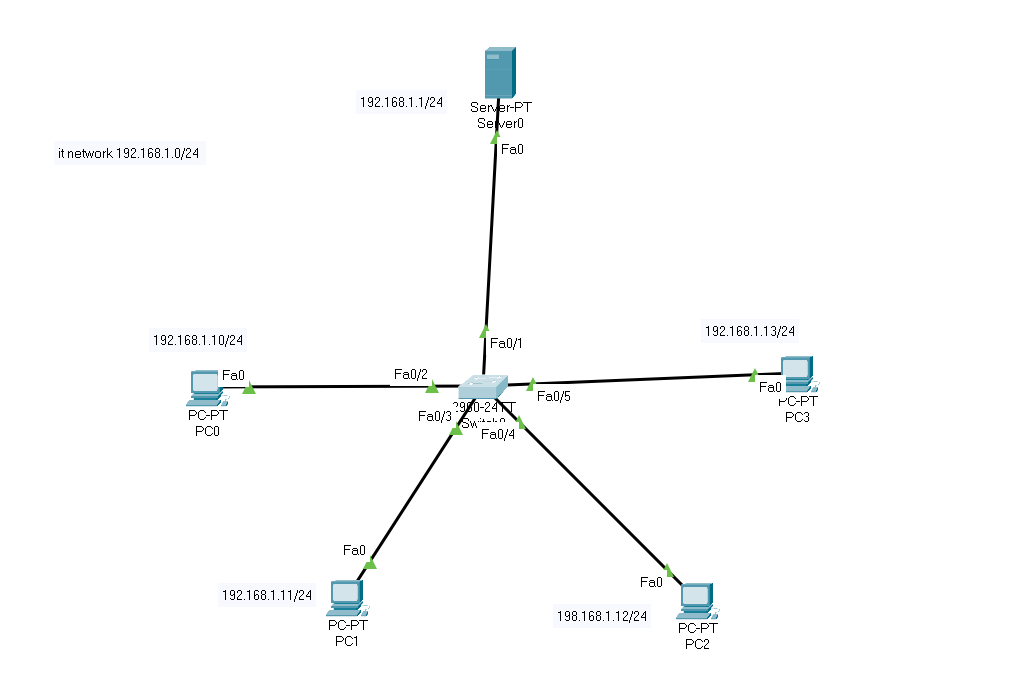
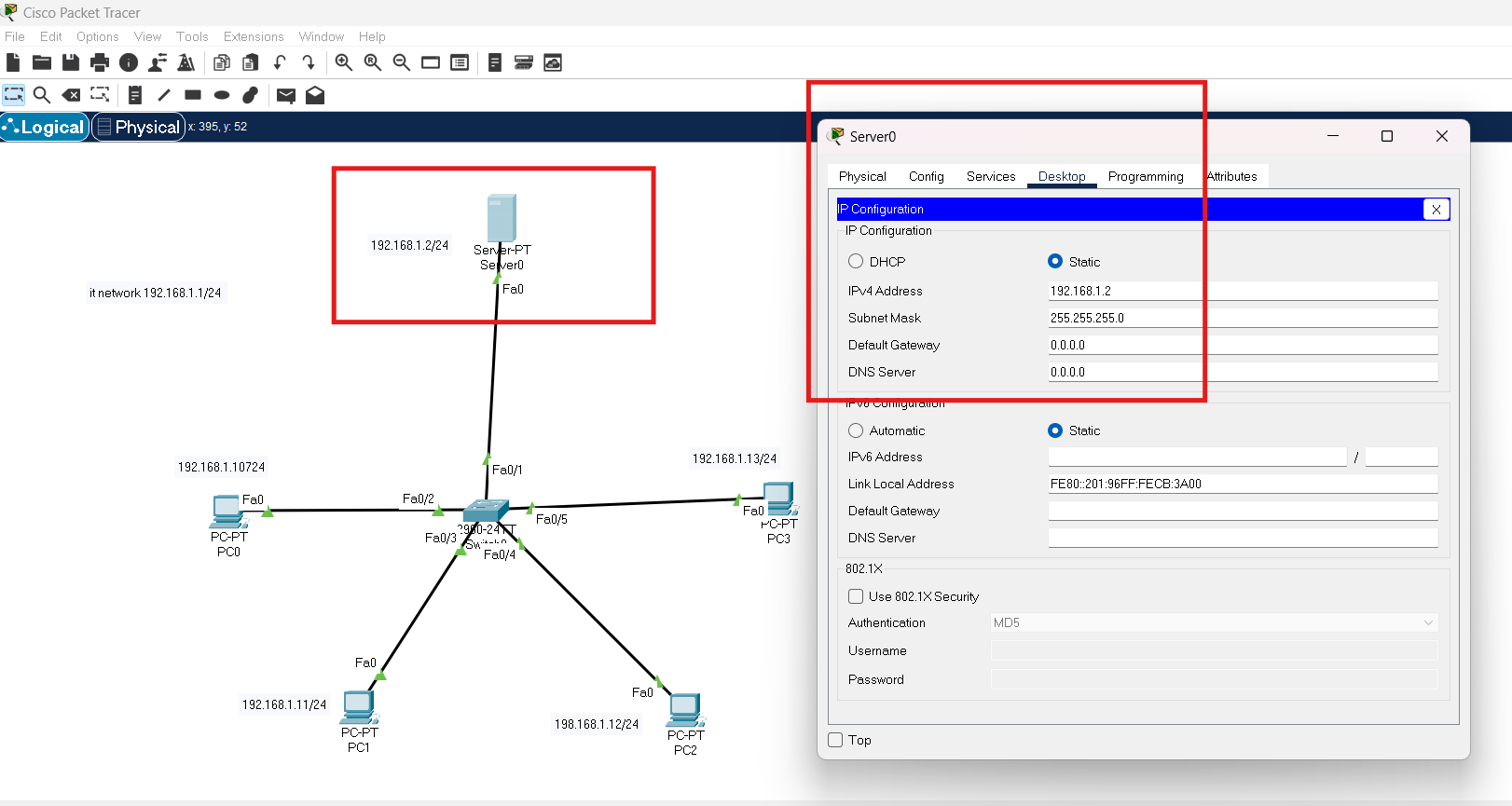
ESERCIZIO S2. L1

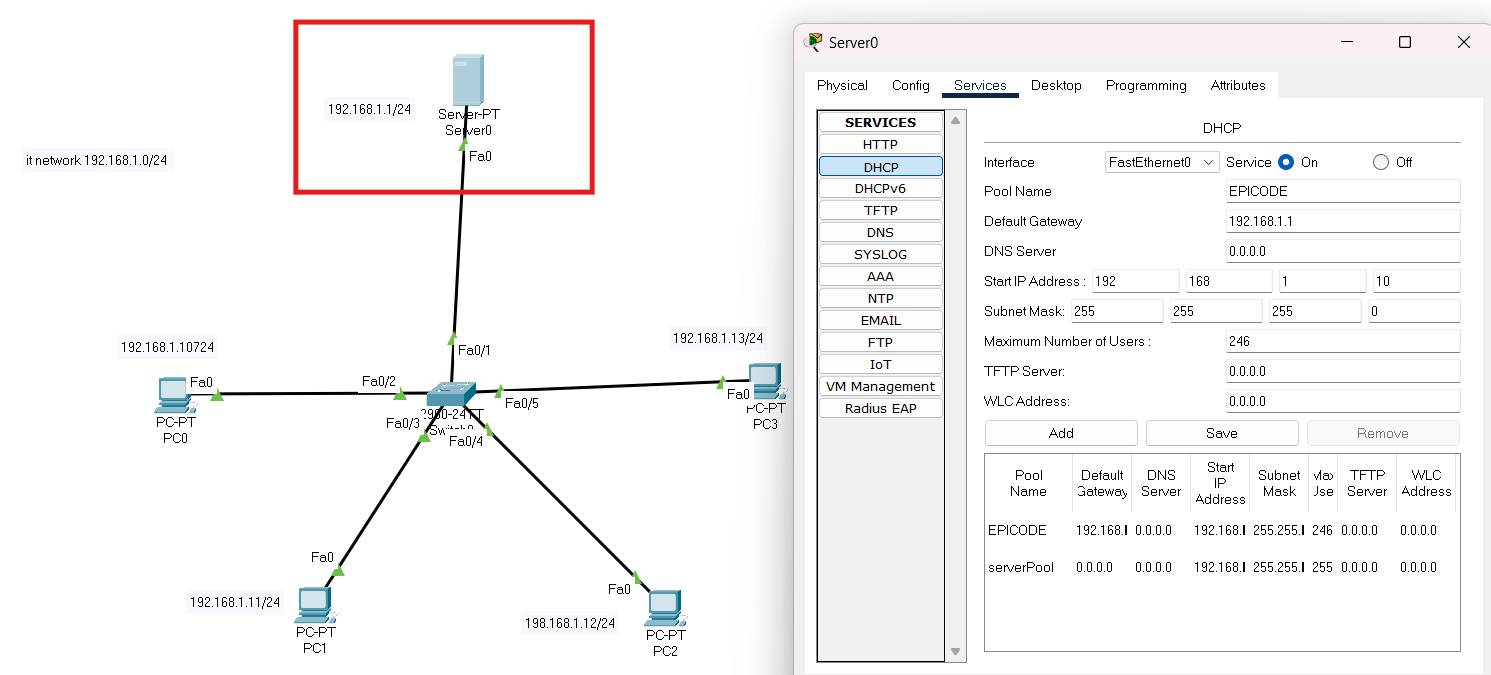
Esercizio di oggi: Configurazione di un Server DHCP su Cisco Packet Tracer Obiettivo: Configurare un server DHCP per la distribuzione automatica degli indirizzi IP. Attività:

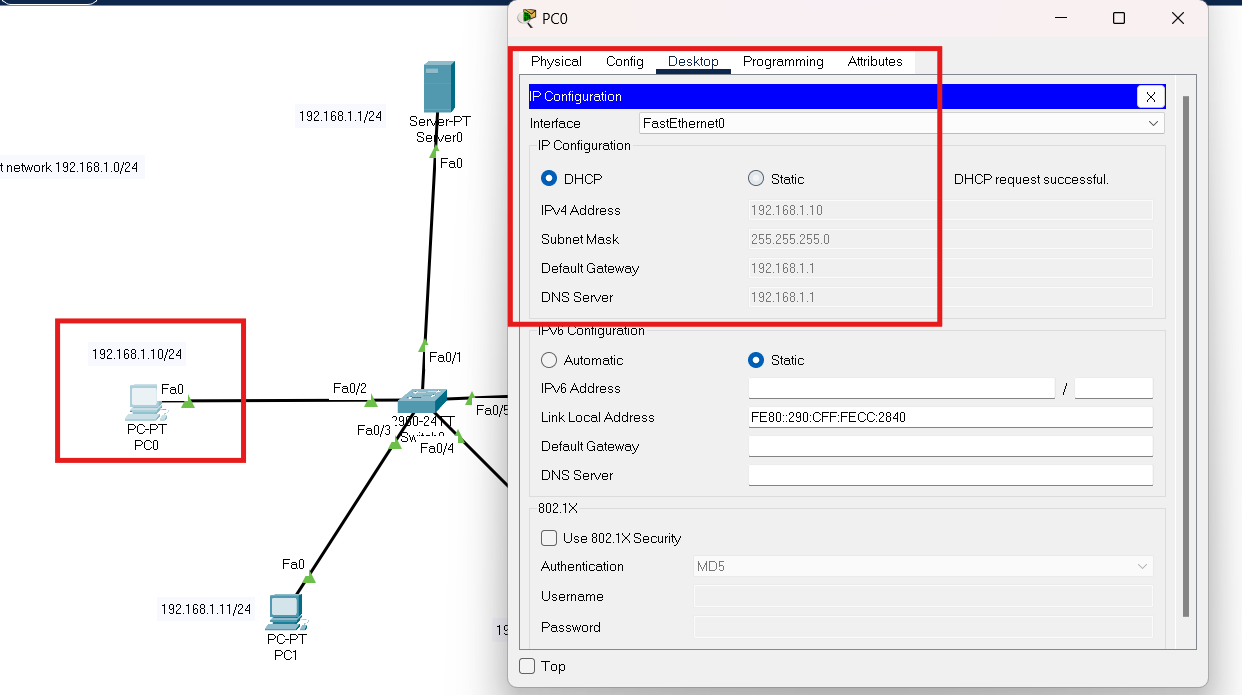
- Installare e configurare un server DHCP Cisco Packet Tracer).

- Configurare il server per assegnare indirizzi IP in un range specifico.









DHCP

Dynamic Host Configuration Protocol

E’ un protocollo di rete utilizzato per assegnare dinamicamente indirizzi IP e altre informazioni di configurazione di rete ai dispositivi client in una rete.

DHCP automatizza il processo di configurazione degli indirizzi IP, riducendo la necessità di configurazione manuale da parte degli amministratori di rete.

E’ il primo protocollo che entra in gioco, ci da alcuni parametri per collegarci alla rete come:

-indirizzo IP

- subnetmasck

- DNS ( associa indirizzo pubblico )

- gateway

UTILIZZO:

Assegnazione di Indirizzi IP

DHCP assegna automaticamente indirizzi IP unici ai dispositivi che si collegano alla rete, evitando conflitti di indirizzi IP.

Configurazione di Parametri di Rete:

DHCP può configurare parametri di rete aggiuntivi come gateway predefinito, server DNS, durata del lease e altre opzioni specifiche.

Facilità di Gestione:

DHCP semplifica la gestione delle reti, riducendo il lavoro manuale necessario per configurare ogni dispositivo.

FUNZIONAMENTO DEL LEASING IP

Lease di Indirizzo IP

Descrizione: Un lease è un periodo di tempo durante il quale un indirizzo IP assegnato a un dispositivo client è valido. Alla scadenza del lease, il client deve rinnovare il lease per continuare a utilizzare l'indirizzo IP.

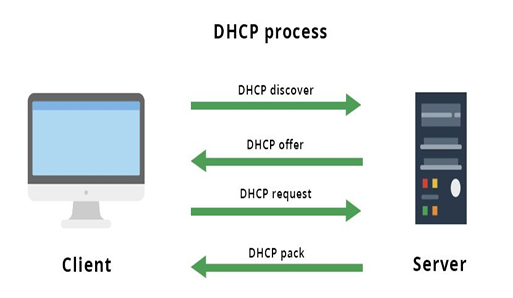
Durata del Lease: La durata del lease è configurabile e può variare da pochi minuti a diversi giorni, a seconda delle esigenze della rete.

Rinnovo del Lease: I client DHCP tentano di rinnovare il loro lease a metà del periodo di validità del lease per garantire la continuità della connessione di rete.

Liberazione del Lease:

Descrizione: Quando un client DHCP non ha più bisogno dell'indirizzo IP, può inviare un messaggio DHCPRELEASE al server DHCP per liberare l'indirizzo IP, rendendolo disponibile per altri dispositivi.

PROCESSI DI SCOPERTA E OFFERTA ( PROCESSO “ DORA” )



1.DHCP Discovery ( SCOPERTA ): Quando un dispositivo client si collega a una rete e ha bisogno di un indirizzo IP, invia un messaggio DHCPDISCOVER in broadcast alla rete locale per trovare un server DHCP disponibile.

Messaggio: Il messaggio DHCPDISCOVER contiene l'indirizzo MAC del client e altre informazioni di identificazione.

2. DHCP Offer (OFFERTA ): Un server DHCP che riceve il messaggio DHCPDISCOVER risponde con un messaggio DHCPOFFER, offrendo un indirizzo IP al client.

Messaggio: Il messaggio DHCPOFFER contiene l'indirizzo IP offerto, la durata del lease e altre informazioni di configurazione di rete.

NOTA: in questa fase di offerta il nostro dispositivo manderà “ un ping “ per fare la prova che veramente l’indirizzo ip sia già stato assegnato

3. DHCP Request ( RICHIESTA ): Il client riceve una o più offerte DHCP e sceglie un'offerta specifica, inviando un messaggio DHCPREQUEST in broadcast per accettare l'offerta selezionata.

Messaggio: Il messaggio DHCPREQUEST include l'indirizzo IP scelto e l'identificativo del server DHCP che ha fatto l'offerta.

4. DHCP Acknowledgment ( CONFERMA ): ○ Descrizione: Il server DHCP che ha fatto l'offerta selezionata dal client risponde con un messaggio DHCPACK per confermare che il client può utilizzare l'indirizzo IP assegnato.

NOTA: questo indirizzo ip NON E’ PERMANETE, viene assegnato l’indirizzo ip solo per un determinato lasso di tempo, che dipenderà da come è stato configurato.

Es. in un bar, sarà molto breve ( come per esempio 15 minuti ) perché un cliente quando entra nel bar e si collega alla rete se fosse permanente questo indirizzo andremo ad esaurire gli indirizzi ip e non ce ne saranno altri per altri clienti ( essendo univoci ).

Invece dandogli un tempo, si potra riutilizzare lo stesso ip scaduto per un altro cliente che lo richiederà ( sempre per altri 15 minuti ).

Messaggio: Il messaggio DHCPACK contiene la conferma dell'indirizzo IP, la durata del lease e le altre configurazioni di rete.

CONSIDERAZIONI DI SICUREZZA

1. Spoofing di Server DHCP

- Descrizione: Un attaccante può configurare un falso server DHCP per rispondere ai messaggi DHCPDISCOVER, assegnando indirizzi IP e configurazioni di rete malevoli ai client. - - Contromisure: Utilizzare tecnologie come DHCP Snooping sui switch di rete per filtrare i messaggi DHCP non autorizzati.

2. DHCP Starvation ( Esaurimento):

- Descrizione: Un attaccante può inviare una grande quantità di richieste DHCP, esaurendo il pool di indirizzi IP disponibili sul server DHCP.

- Contromisure: Implementare rate limiting e autenticazione per le richieste DHCP per prevenire attacchi di esaurimento.

3. Assegnazione di Configurazioni di Rete Malevole:

- Descrizione: Un server DHCP compromesso può assegnare configurazioni di rete che indirizzano il traffico attraverso un attaccante, permettendo attacchi man-in-the-middle.

- Contromisure: Utilizzare server DHCP sicuri e monitorare le configurazioni di rete assegnate per rilevare eventuali anomalie.

CONCLUSIONE

DHCP è un protocollo fondamentale per la gestione automatica degli indirizzi IP e delle configurazioni di rete. Tuttavia, la sua natura automatica e in chiaro lo rende vulnerabile a vari attacchi. Implementare misure di sicurezza adeguate, come DHCP Snooping e autenticazione, è essenziale per proteggere la rete da potenziali minacce.