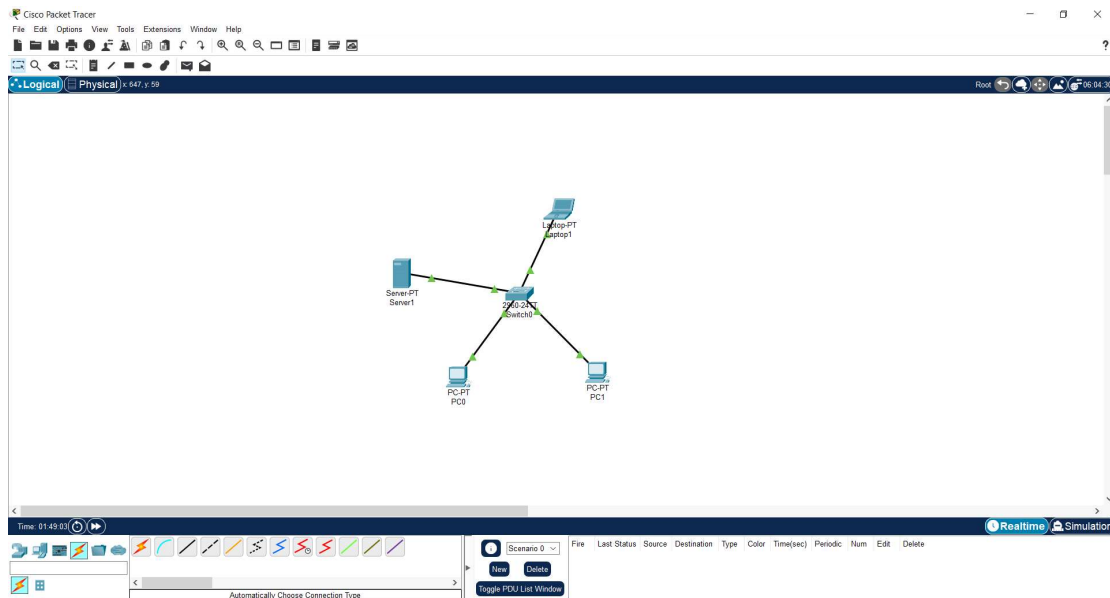


All'interno di una struttura che affitta sale riunioni, e che quindi ha alcuni utenti fissi e la maggior parte mobili, è stato implementato un server DHCP, per rendere più flessibile e ottimizzato l'assegnazione degli indirizzi IP e la configurazione della rete a tutti gli ospiti che necessitano collegarsi alla rete interna.



Il DHCP è un protocollo che assegna in maniera dinamica i parametri di rete di ogni nuovo dispositivo che si collega, configurando nel server DHCP da che indirizzo IP partire, il default gateway e il numero massimo di utenti che possono connettersi.

Server1

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

Interface

FastEthernet0

Service

On

Off

Pool Name

serverPool

Default Gateway

192.168.50.1

DNS Server

192.168.50.6

Start IP Address :

192

168

50

15

Subnet Mask:

255

255

255

0

Maximum Number of Users :

100

TFTP Server:

0.0.0.0

WLC Address:

0.0.0.0

Add

Save

Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.50.1	192.168.50.6	192.168.5...	255.255.2...	100	0.0.0.0	0.0.0.0

Top

Con questo metodo ci sono molti vantaggi a livello gestionale di ogni utente, assegnando in maniera dinamica gli indirizzi IP, azzerando così il rischio di errore o di duplicazione di indirizzi già esistenti.

Laptop1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 192.168.50.15

Subnet Mask 255.255.255.0

Default Gateway 192.168.50.1

DNS Server 192.168.50.6

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:B0FF:FE9C:A142

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

Questo però potrebbe intaccare la sicurezza in quanto, essendo un metodo automatico, una persona malintenzionata potrebbe utilizzare vari metodi per infiltrarsi e indirizzare i vari utenti malcapitati dove si vuole, oppure facendo esaurire gli indirizzi disponibili, ma questi metodi sono tutti prevedibili e risolvibili con delle accortezze e dei controlli approfonditi, implementando il DHCP snooping, e un limite di tempo di richieste per indirizzi IP