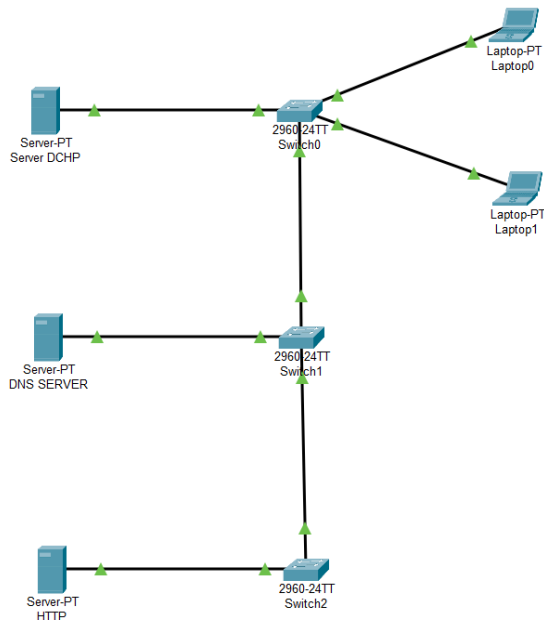


PASSAGGIO 1



La topologia costituita prevede tre Server-PT dedicati ai servizi DHCP, DNS e HTTP, connessi in cascata mediante switch alla quale sono collegati due host client (Laptop0 e Laptop1). Tutti i dispositivi operano sulla medesima rete subnet e le connessioni fisiche tra server, switch e client sono state predisposte per consentire la verifica dei servizi applicativi e delle assegnazioni dinamiche degli indirizzi IP.

PASSAGGIO 2

Cisco Packet Tracer - C:\Users\vikis\OneDrive\Desktop\PROVE CPT\Yes m1w3d1.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x:1382 y:638

DNS SERVER

Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP

☒ Static

IPv4 Address192.168.1.100

Subnet Mask255.255.255.0

Default Gateway0.0.0.0

DNS Server0.0.0.0

Server DHCP

Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP

☒ Static

IPv4 Address192.168.1.3

Subnet Mask255.255.255.0

Default Gateway0.0.0.0

DNS Server0.0.0.0

HTTP

Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP

☒ Static

IPv4 Address192.168.1.90

Subnet Mask255.255.255.0

Default Gateway0.0.0.0

DNS Server0.0.0.0

Time: 00:50:02

Scenario 0

New Delete

Toggle PDU List Window

(Select a Device to Drag and Drop to the Workspace)

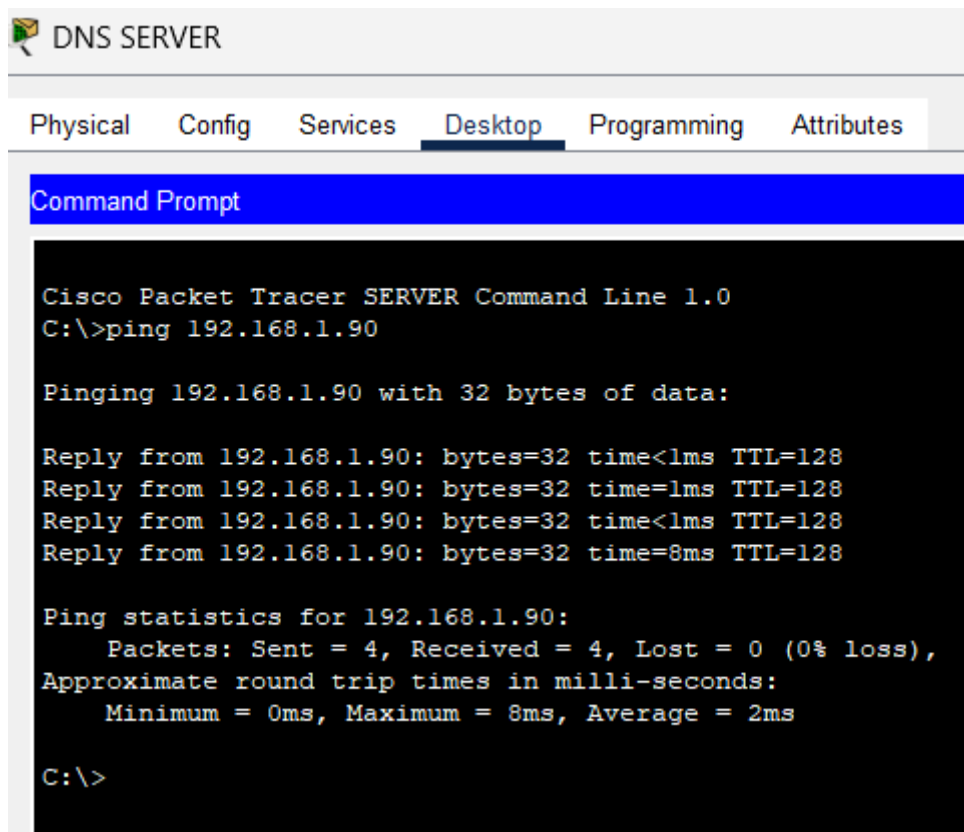
Simulation

Sono stati configurati manualmente gli IP statici ai tre Server impostando i seguenti paramentri:

- DNS avente IP 192.168.1.100 e subnet mask 255.255.255.0
- HTTP avente IP 192.168.1.90 e subnet mask 255.255.255.0
- DHCP avente IP 192.168.1.3 e subnet mask 255.255.255.0

Il gateway della rete è stato definito come 192.168.1.1

Per verificare la connettività di rete ho eseguito un ping dal serve DNS al server HTTP, all'indirizzo 192.158.1.90 ; la prova ha restituito risposte positive dimostrando la corretta instradabilità e raggiungibilità.



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.90

Pinging 192.168.1.90 with 32 bytes of data:

Reply from 192.168.1.90: bytes=32 time<1ms TTL=128
Reply from 192.168.1.90: bytes=32 time=1ms TTL=128
Reply from 192.168.1.90: bytes=32 time<1ms TTL=128
Reply from 192.168.1.90: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.1.90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

PASSAGGIO 3

Server DHCP

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

InterfaceFastEthernet0ServiceOnOff

Pool NameserverPool

Default Gateway192.168.1.1

DNS Server192.168.1.100

Start IP Address : 1921681140

Subnet Mask: 2552552550

Maximum Number of Users : 115

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

AddSaveRemove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1.1	192.168.1....	192.168.1....	255.255.2...	115	0.0.0.0	0.0.0.0

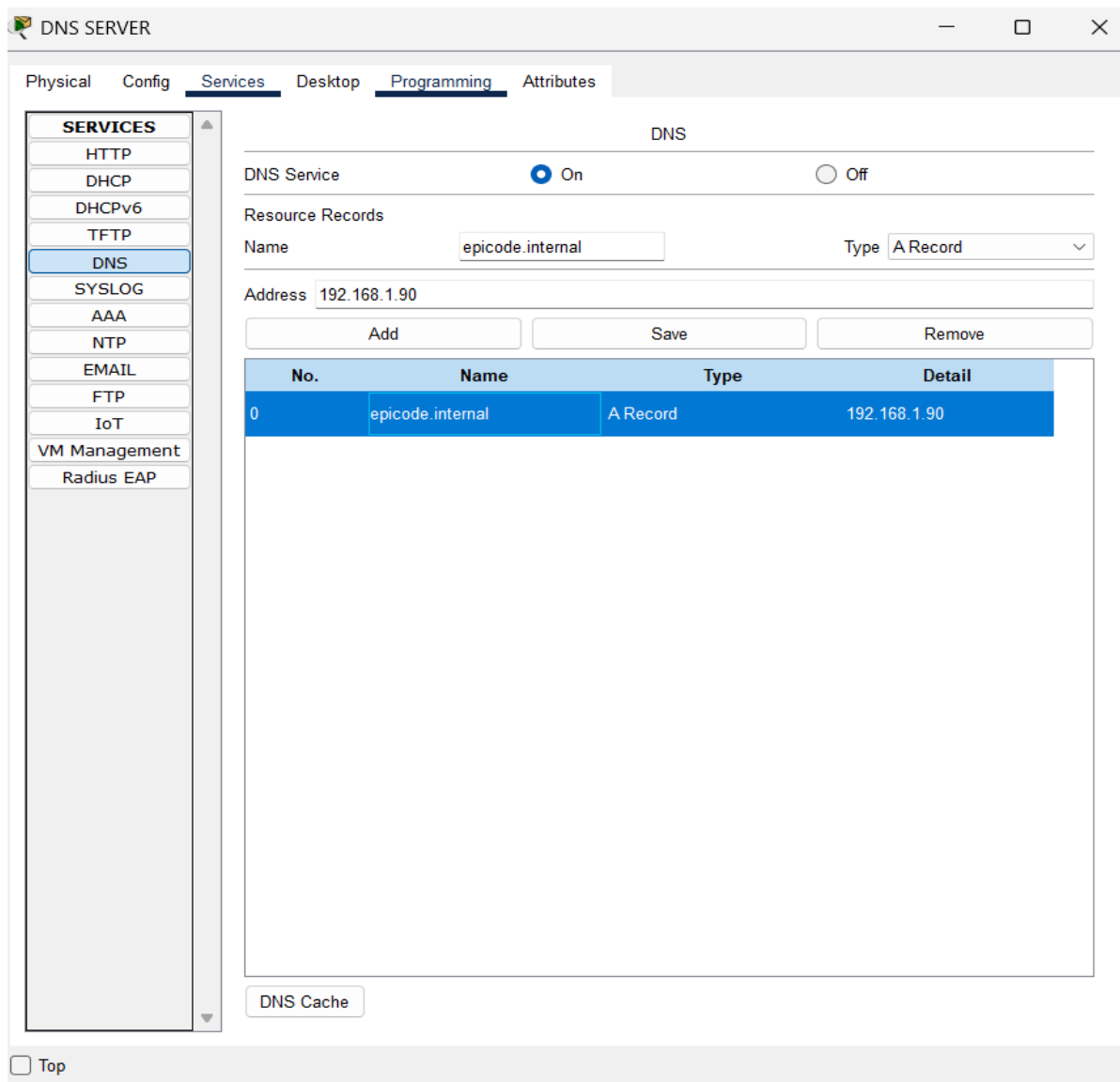
Top

A seguito dell’assegnazione degli indirizzi IP, è stato predisposto sul server DHCP il pool con i seguenti parametri operativi:

- Gateway 192.168.1.1
- DNS 192.168.1.100
- Intervallo indirizzi a partire da 192.168.1.140 fino a 192.168.1.254
- Subnet :255.255.255.0
- capacità max host 115

Questa operazione attiva e configura il server DHCP, ma non assegna manualmente gli indirizzi, il server rimane in ascolto e fornirà gli IP solo quando un client avvierà la normale procedura. Lo scopo è centralizzare la distribuzione automatica degli indirizzi IP e delle impostazioni di rete (gateway, DNS) per evitare conflitti, garantire un instradamento coerente e ridurre l’onere gestionale. In questo modo i client ricevono automaticamente le informazioni necessarie al funzionamento in rete senza configurazioni manuali.

PASSAGGIO 4



È stato attivato e configurato il servizio DNS sul server dedicato. In particolare è stato aggiunto un record di tipo A con nome *epicode.internal* associato all'indirizzo IP 192.168.1.90 ossia l'host che ospita il servizio http.

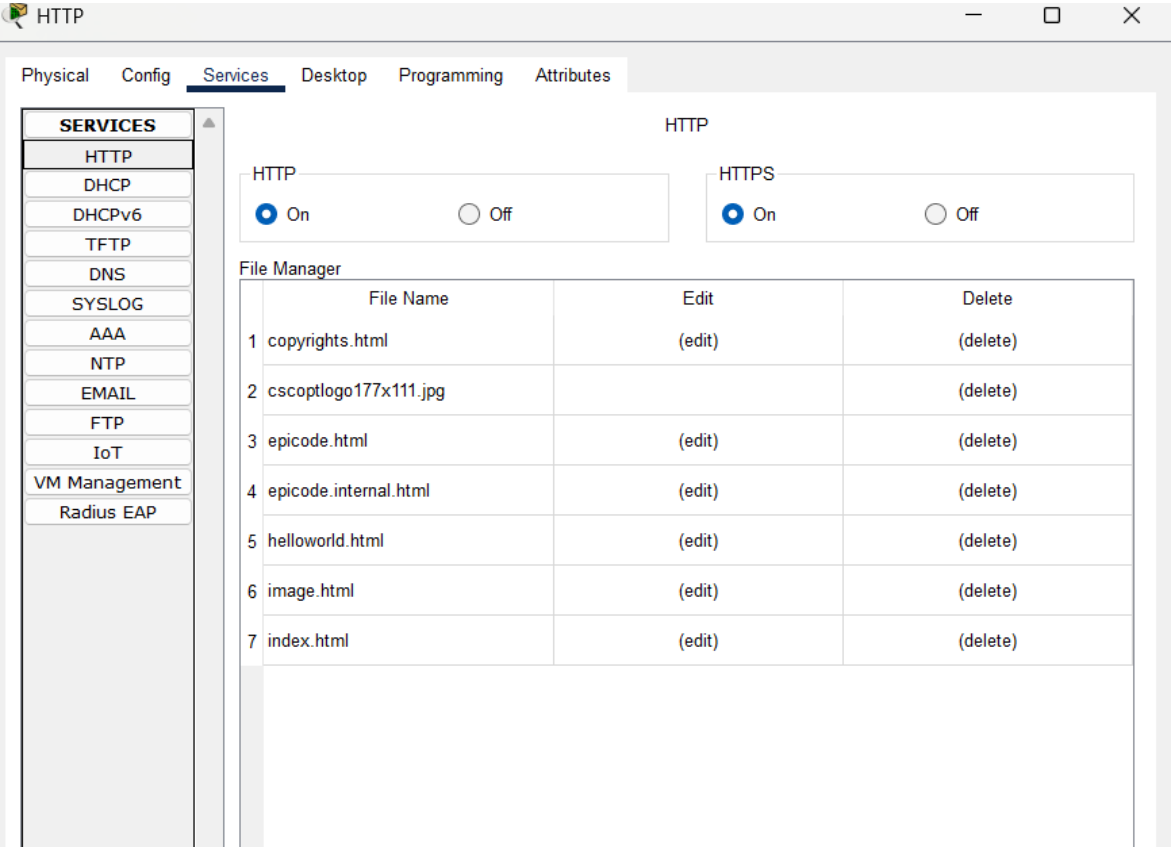
L'obiettivo della configurazione è permettere ai client della LAN di risolvere il nome simbolico *epicode.internal* nel corrispondente indirizzo IPv4 attraverso il servizio DNS , semplificando l'accesso ai servizi e rendendo indipendente l'uso del nome.

La procedura eseguita comprende:

- abilitazione del servizio DNS,
- inserimento del nome e dell'indirizzo nel database dei record (A record)
- salvataggio della voce.

Questa impostazione non impatta direttamente la configurazione IP dei client (che ricevono le informazioni via DHCP) ma fornisce il mapping nome→IP necessario per la risoluzione dei nomi in rete.

PASSAGGIO 5



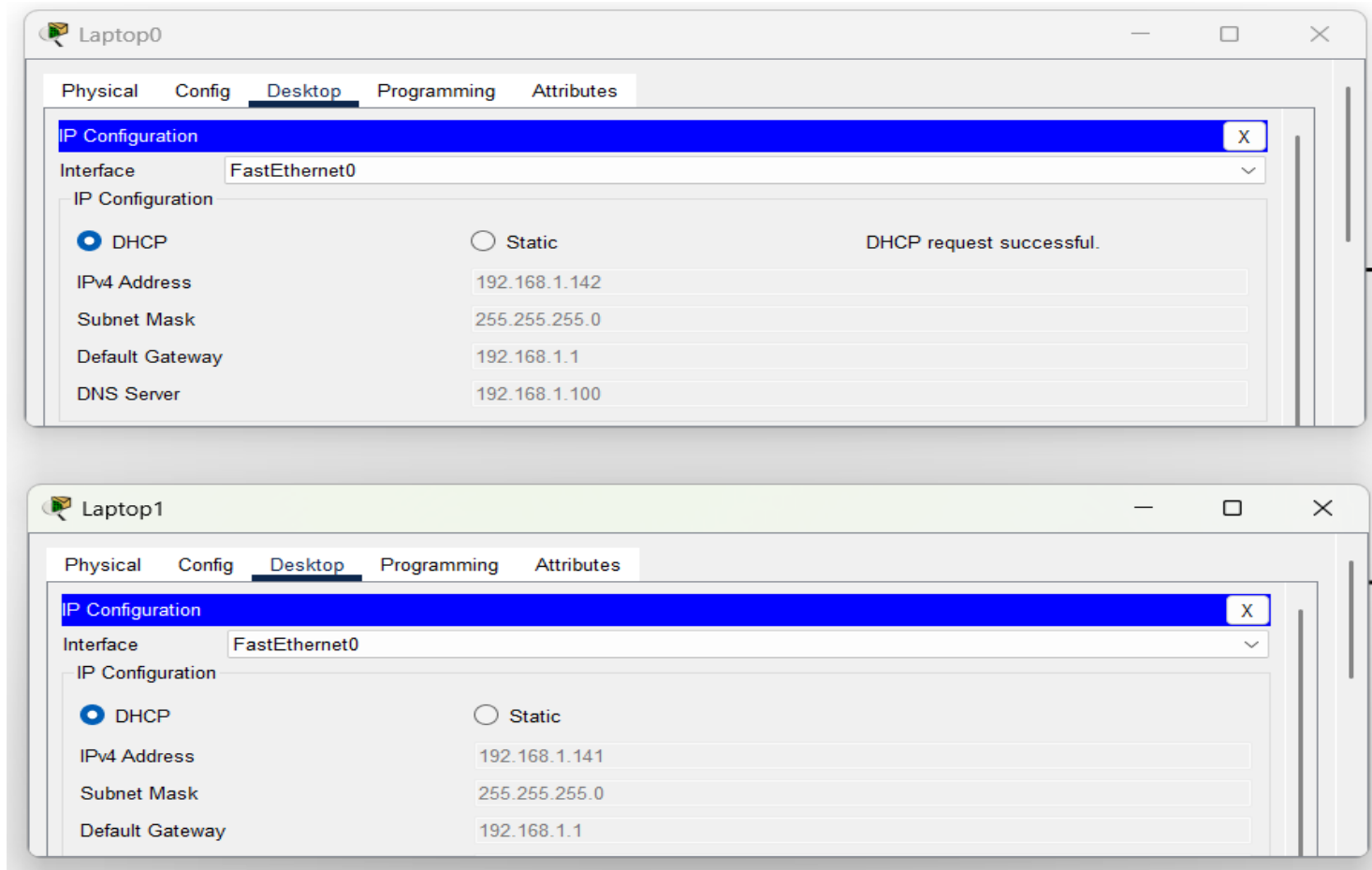
È stato attivato il servizio HTTP/HTTPS sul server dedicato e sono state predisposte le risorse web necessarie per l'erogazione dei contenuti ai client della LAN.

Nel pannello File-Manager sono visibili i file di servizio (tra cui index.html ed epicode.internal.html) a conferma che la homepage e le pagine correlate sono state create/aggiunte ed erano pronte per essere servite. Contestualmente è stato effettuato un intervento di editing sul file index.html per personalizzare il contenuto della pagina principale e il file è stato salvato all'interno del File Manager.

A valle di tutto ciò sono state eseguite delle verifiche funzionali , ossia dal client è stata controllata la risoluzione del nome tramite nslookup epicode.internal , è stata verificata la raggiungibilità IP del web server con ping 192.168.1.90 ed infine il browser del client ha effettuato la richiesta <http://epicode.internal>.

I risultati positivi di questi test confermano l'integrazione corretta tra DNS e servizio HTTP e attestano la piena disponibilità dei contenuti web per gli utenti della LAN.

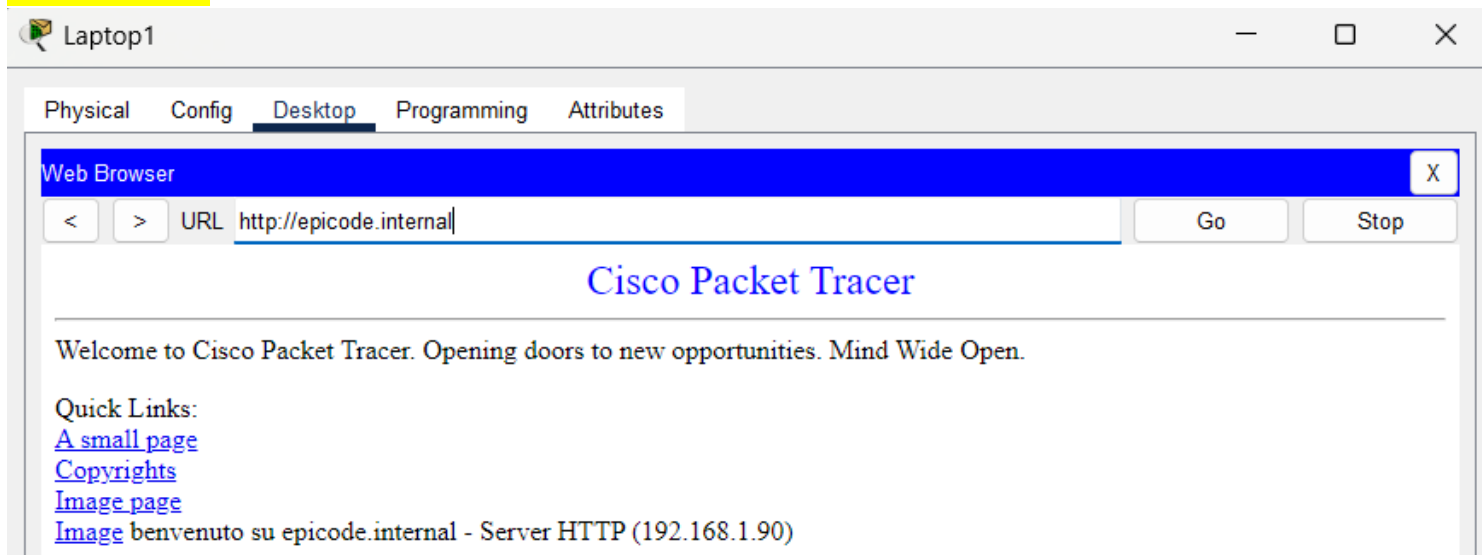
PASSAGGIO 6



A seguito della predisposizione del server DHCP è stata verificata la corretta distribuzione automatica delle configurazioni di rete ai client Laptop0 e Laptop1. Come riportato entrambi i laptop riportano “DHCP request successful”.

Gli indirizzi IPv4 assegnati (ad es. 192.168.1.141 e 192.168.1.142) rientrano nell’intervallo 192.168.1.140–192.168.1.254 definito nel pool, la subnet mask visualizzata è 255.255.255.0 e le opzioni di rete critiche (Default Gateway 192.168.1.1 e DNS Server 192.168.1.100) sono state effettivamente fornite dal server; questi elementi confermano il completamento del processo di negoziazione DHCP e attestano che il servizio DHCP è operativo, che la distribuzione centralizzata delle impostazioni funziona correttamente e che i client possono ora ottenere automaticamente tutte le informazioni necessarie per comunicare nella LAN.

PASSAGGIO 7



Il client (Laptop0) è riuscito a caricare la homepage tramite `http://epicode.internal`, quindi il nome **epicode.internal** viene risolto correttamente in **192.168.1.90**; il server HTTP risponde e consegna il file `index.html`. In pratica: il client ha preso via DHCP l'indirizzo del DNS, il DNS ha restituito il mapping nome→IP, il traffico ha raggiunto la macchina corretta e il servizio web ha risposto alla richiesta.

Questo conferma che tutto funziona come previsto e programmato.

CONCLUSIONE

Al termine delle attività è stata predisposta e verificata l'infrastruttura di rete prevista: i server sono stati configurati con indirizzi statici.

- sul server DHCP è stato creato il pool 192.168.1.140–192.168.1.254 (gateway 192.168.1.1, DNS 192.168.1.100) e il servizio è risultato positivo poiché fornisce indirizzi ai client.

- il server DNS tiene il record A `epicode.internal`

- il server HTTP espone la pagina `index.html` e risponde correttamente alle richieste dei client.

Le verifiche effettuate confermano che i servizi DHCP, DNS e HTTP sono integrati e funzionanti nella LAN secondo le specifiche dell'esercizio.

ESERCIZIO FACOLTATIVO

Attraverso l'analisi guidata con il modello ISO/OSI ho scritto i passaggi funzionali (dal trasporto fisico al livello applicazione) mettendo in evidenza protocolli, dispositivi e meccanismi che consentono la corretta trasmissione e conservazione delle immagini.

LIVELLO 1 FISICO

Al livello fisico avviene la trasmissione dei bit tra telecamera e rete mediante i cavi di trasporto. In un contesto di sistema di sorveglianza è fondamentale scegliere un cablaggio e ricetrasmittenti adeguati alla larghezza di banda e alla distanza richieste. Una solida progettazione del livello fisico riduce errori di trasmissione ed influiscono sull'efficienza.

LIVELLO 2 DATA-LINK

Al livello Data-link avviene la gestione dei frame ETHERNET ed utilizza gli indirizzi MAC per consegnare i dati nella stessa rete.

Si crea una VLAN separata per il traffico video così da isolare le telecamere dal resto della rete e ridurre broadcast.

LIVELLO 3 RETE

In questo livello avviene l'instradamento dei pacchetti in sottoreti mediante l'utilizzo degli indirizzi IP. Sostanzialmente vengono assegnati indirizzi IP statici alle telecamere e al server di registrazione. Se le telecamere e i server stanno in subnet diverse serve un router per instradare il traffico.

LIVELLO 4 TRASPORTO

Questo livello ha il compito di garantire una trasmissione affidabile tra dati ed i sistemi.

LIVELLO 5 SESSIONE

In questo livello si controlla l'apertura/chiusura della conversazione tra camera e server. Si controlla la sessione video (pausa, play, stop) ed il server mantiene lo stato per ogni sessione della camera.

LIVELLO 6 PRESENTAZIONE

Questo livello si occupa di formato, compressione, cifratura dei dati.

Le telecamere codificano il video in MJPEG(?) , il server decodifica .

LIVELLO 7 APPLICAZIONE

Questo livello interagisce con le applicazioni utilizzate dall'utente fornendo servizi di interfaccia e supporto alle reti.

Il server riceve il flusso, lo registra, indicizza gli orari e mostra le immagini attraverso l'interfaccia web o il player. È il punto in cui puoi cercare una registrazione, riprodurla o scaricarla; qui si svolge tutta la logica di gestione, monitoraggio e accesso alle riprese.