

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

Лабораторна робота №6
з дисципліни «Комп'ютерні мережі»

**«Засвоєння принципів перетворення
DNS-імен в IP-адреси»**

Виконала студентка групи: КВ-11

ПІБ: Михайліченко Софія Віталіївна

Перевірив: _____

Мета роботи:

Використовуючи програму моделювання комп'ютерних мереж засвоїти принципи адресації на канальному та мережевому рівнях моделі OSI, принципи динамічного призначення IP-адрес і принципів перетворення DNS-імен в IP-адреси.

План виконання лабораторної роботи:

Завдання №1. Побудова локальної мережі з двома робочими станціями.

Завдання №2. Засвоєння принципів адресації на канальному і мережевому рівнях.

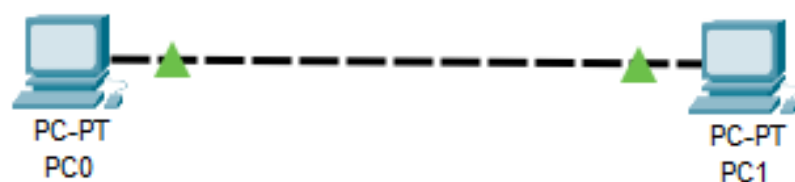
Завдання №3. Засвоєння принципів динамічного призначення IP-адрес.

Завдання №4. Засвоєння принципів перетворення DNS-імен в IP-адреси.

Завдання №5. Ознайомлення з відомостями про структуру перехресного кабеля.

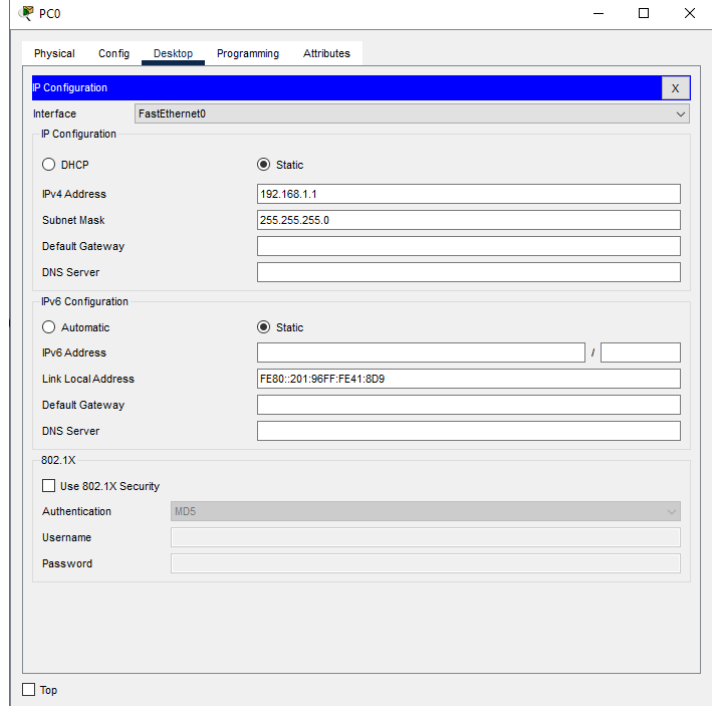
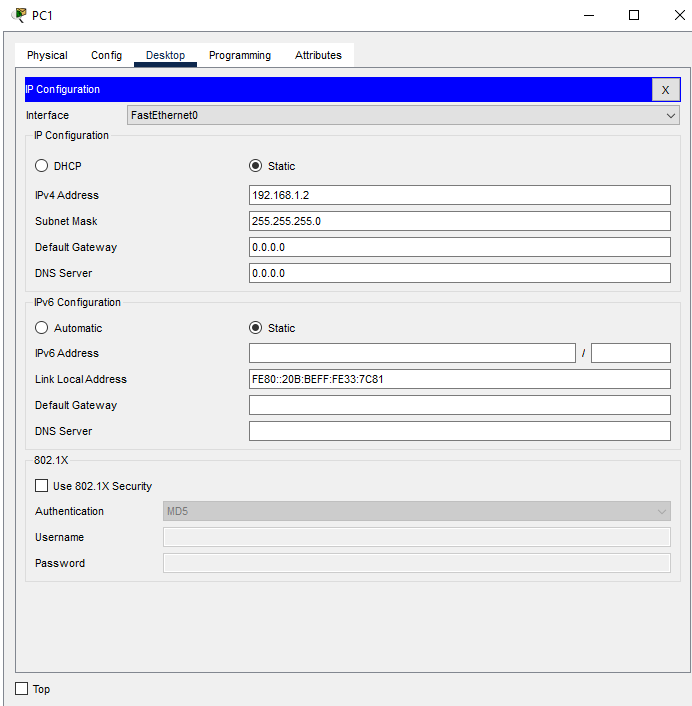
Порядок виконання роботи:

Завдання №1. Побудова локальної мережі з двома робочими станціями



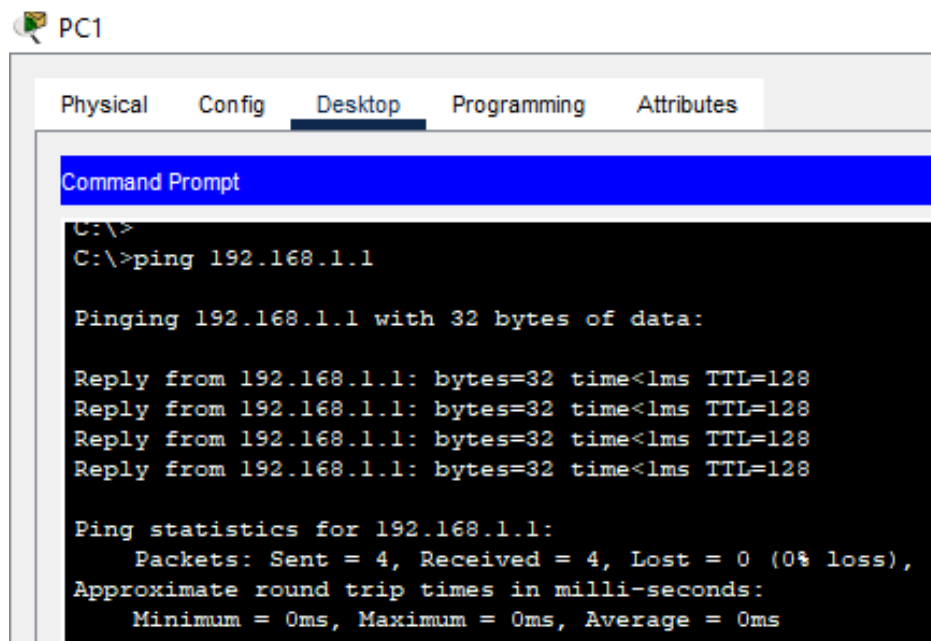
Як ми можемо побачити, що з'єднання між робочими станціями відбулося, адже засвітилися зелені індикатори link.

Тепер потрібно вказати статичну IP-адресу комп'ютера:



Тепер на другій робочій станції вибрати режим Command Prompt:

Виконаємо команду `ping 192.168.1.1`, в результаті виконання якої видно, що зв'язок між робочими станціями встановлений.



В режимі симуляції відслідковуємо протоколи, які надсилаються до PC0 за допомогою команди ping 192.168.1.1:

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	587.180	--	PC1	ICMP
	587.181	PC1	PC0	ICMP
	587.182	PC0	PC1	ICMP
	588.186	--	PC1	ICMP
	588.187	PC1	PC0	ICMP
	588.188	PC0	PC1	ICMP
	589.192	--	PC1	ICMP
	589.193	PC1	PC0	ICMP
	589.194	PC0	PC1	ICMP
	590.194	--	PC1	ICMP
	590.195	PC1	PC0	ICMP
	590.196	PC0	PC1	ICMP

Reset Simulation

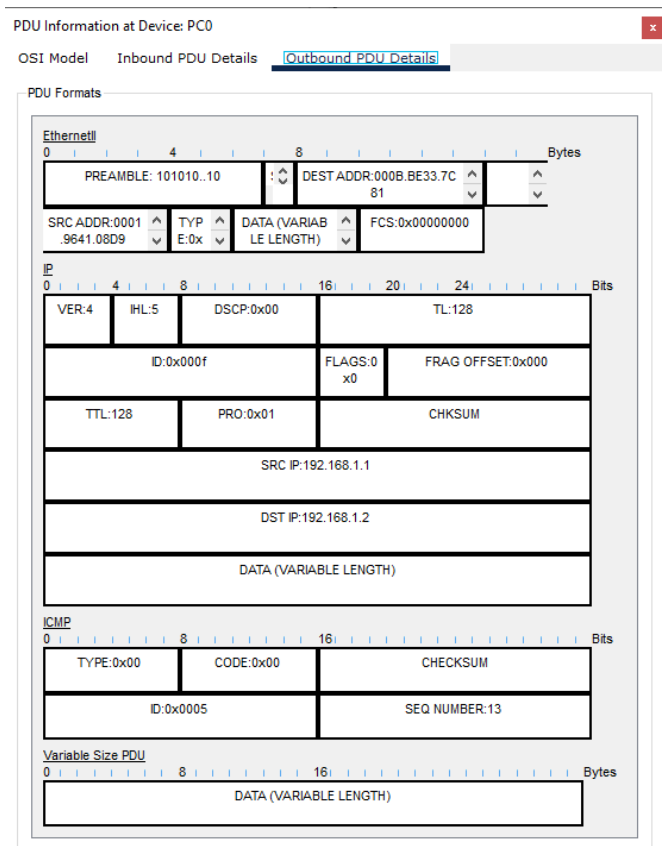
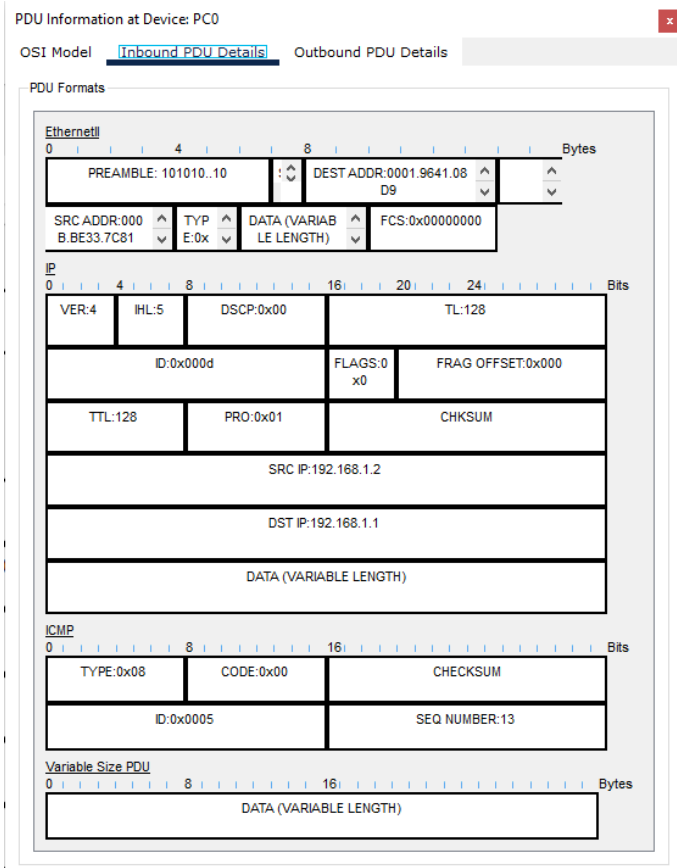
☒ Constant Delay

Captured to: 875.013 s

Play Controls

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPv2, RIPv3, RSTP, SLL, STP, TFTP, VRRP, VRRPv6, WPA, WPA2, WPA3, WPA3-Enterprise, WPA3-Enterprise-192-bit, WPA3-Enterprise-256-bit, WPA3-Enterprise-384-bit, WPA3-Enterprise-512-bit, WPA3-Enterprise-768-bit, WPA3-Enterprise-1024-bit, WPA3-Enterprise-1536-bit, WPA3-Enterprise-2048-bit, WPA3-Enterprise-4096-bit, WPA3-Enterprise-8192-bit, WPA3-Enterprise-16384-bit, WPA3-Enterprise-32768-bit, WPA3-Enterprise-65536-bit, WPA3-Enterprise-131072-bit, WPA3-Enterprise-262144-bit, WPA3-Enterprise-524288-bit, WPA3-Enterprise-1048576-bit, WPA3-Enterprise-2097152-bit, WPA3-Enterprise-4194304-bit, WPA3-Enterprise-8388608-bit, WPA3-Enterprise-16777216-bit, WPA3-Enterprise-33554432-bit, WPA3-Enterprise-67108864-bit, WPA3-Enterprise-134217728-bit, WPA3-Enterprise-268435456-bit, WPA3-Enterprise-536870912-bit, WPA3-Enterprise-1073741824-bit, WPA3-Enterprise-2147483648-bit, WPA3-Enterprise-4294967296-bit, WPA3-Enterprise-8589934592-bit, WPA3-Enterprise-17179869184-bit, WPA3-Enterprise-34359738368-bit, WPA3-Enterprise-68719476736-bit, WPA3-Enterprise-137438953472-bit, WPA3-Enterprise-274877906944-bit, WPA3-Enterprise-549755813888-bit, WPA3-Enterprise-1099511627776-bit, WPA3-Enterprise-2199023255552-bit, WPA3-Enterprise-4398046511104-bit, WPA3-Enterprise-8796093022208-bit, WPA3-Enterprise-17592186044416-bit, WPA3-Enterprise-35184372088832-bit, WPA3-Enterprise-70368744177664-bit, WPA3-Enterprise-140737488355328-bit, WPA3-Enterprise-281474976710656-bit, WPA3-Enterprise-562949953421312-bit, WPA3-Enterprise-1125899906842624-bit, WPA3-Enterprise-2251799813685248-bit, WPA3-Enterprise-4503599627370496-bit, WPA3-Enterprise-9007199254740992-bit, WPA3-Enterprise-18014398509481984-bit, WPA3-Enterprise-36028797018963968-bit, WPA3-Enterprise-72057594037927936-bit, WPA3-Enterprise-144115188075855872-bit, WPA3-Enterprise-288230376151711744-bit, WPA3-Enterprise-576460752303423488-bit, WPA3-Enterprise-1152921504606846976-bit, WPA3-Enterprise-2305843009213693952-bit, WPA3-Enterprise-4611686018427387904-bit, WPA3-Enterprise-9223372036854775808-bit, WPA3-Enterprise-18446744073709551616-bit, WPA3-Enterprise-36893488147419103232-bit, WPA3-Enterprise-73786976294838206464-bit, WPA3-Enterprise-147573952589676412928-bit, WPA3-Enterprise-295147905179352825856-bit, WPA3-Enterprise-590295810358705651712-bit, WPA3-Enterprise-1180591620717411303424-bit, WPA3-Enterprise-2361183241434822606848-bit, WPA3-Enterprise-4722366482869645213696-bit, WPA3-Enterprise-9444732965739290427392-bit, WPA3-Enterprise-18889465931478580854784-bit, WPA3-Enterprise-37778931862957161709568-bit, WPA3-Enterprise-75557863725914323419136-bit, WPA3-Enterprise-151115727451828646838272-bit, WPA3-Enterprise-302231454903657293676544-bit, WPA3-Enterprise-604462909807314587353088-bit, WPA3-Enterprise-1208925819614629174706176-bit, WPA3-Enterprise-2417851639229258349412352-bit, WPA3-Enterprise-4835703278458516698824704-bit, WPA3-Enterprise-9671406556917033397649408-bit, WPA3-Enterprise-19342813113834066795298816-bit, WPA3-Enterprise-38685626227668133590597632-bit, WPA3-Enterprise-77371252455336267181195264-bit, WPA3-Enterprise-154742504910672534362390528-bit, WPA3-Enterprise-309485009821345068724781056-bit, WPA3-Enterprise-618970019642690137449562112-bit, WPA3-Enterprise-1237940039285380274899124224-bit, WPA3-Enterprise-2475880078570760549798248448-bit, WPA3-Enterprise-4951760157141521099596496896-bit, WPA3-Enterprise-9903520314283042199192993792-bit, WPA3-Enterprise-19807040628566084398385987584-bit, WPA3-Enterprise-39614081257132168796771975168-bit, WPA3-Enterprise-79228162514264337593543950336-bit, WPA3-Enterprise-158456325028528675187087900672-bit, WPA3-Enterprise-316912650057057350374175801344-bit, WPA3-Enterprise-633825300114114700748351602688-bit, WPA3-Enterprise-1267650600228229401496703205376-bit, WPA3-Enterprise-2535301200456458802993406410752-bit, WPA3-Enterprise-5070602400912917605986812821504-bit, WPA3-Enterprise-10141204801825835211973625643008-bit, WPA3-Enterprise-20282409603651670423947251286016-bit, WPA3-Enterprise-40564819207303340847894502572032-bit, WPA3-Enterprise-81129638414606681695789005144064-bit, WPA3-Enterprise-162259276829213363391578010288128-bit, WPA3-Enterprise-324518553658426726783156020576256-bit, WPA3-Enterprise-649037107316853453566312041152512-bit, WPA3-Enterprise-1298074214633706907132624082305024-bit, WPA3-Enterprise-2596148429267413814265248164610048-bit, WPA3-Enterprise-5192296858534827628530496329220096-bit, WPA3-Enterprise-10384593717069655257060992658440192-bit, WPA3-Enterprise-20769187434139310514121985316880384-bit, WPA3-Enterprise-41538374868278621028243970633760768-bit, WPA3-Enterprise-83076749736557242056487941267521536-bit, WPA3-Enterprise-166153499473114484112975882535043072-bit, WPA3-Enterprise-332306998946228968225951765070086144-bit, WPA3-Enterprise-664613997892457936451903530140172288-bit, WPA3-Enterprise-1329227995784915872903807060280344576-bit, WPA3-Enterprise-2658455991569831745807614120560689152-bit, WPA3-Enterprise-5316911983139663491615228241121378304-bit, WPA3-Enterprise-10633823966279326983230456482242756608-bit, WPA3-Enterprise-21267647932558653966460912964485513216-bit, WPA3-Enterprise-42535295865117307932921825928971026432-bit, WPA3-Enterprise-85070591730234615865843651857942052864-bit, WPA3-Enterprise-170141183460469231731687303715884105728-bit, WPA3-Enterprise-340282366920938463463374607431768211456-bit, WPA3-Enterprise-680564733841876926926749214863536422912-bit, WPA3-Enterprise-1361129467683753853853498429727072845824-bit, WPA3-Enterprise-2722258935367507707706996859454145691648-bit, WPA3-Enterprise-5444517870735015415413993718908291383296-bit, WPA3-Enterprise-10889035741470030830827987437816582766592-bit, WPA3-Enterprise-21778071482940061661655974875633165533184-bit, WPA3-Enterprise-43556142965880123323311949751266331066368-bit, WPA3-Enterprise-87112285931760246646623899502532662132736-bit, WPA3-Enterprise-174224571863520493293247799005065324265472-bit, WPA3-Enterprise-348449143727040986586495598010130648530944-bit, WPA3-Enterprise-696898287454081973172991196020261297061888-bit, WPA3-Enterprise-1393796574908163946345982392040522594123776-bit, WPA3-Enterprise-2787593149816327892691964784081045188247552-bit, WPA3-Enterprise-5575186299632655785383929568162090376495104-bit, WPA3-Enterprise-11150372599265311570767859136324180752990208-bit, WPA3-Enterprise-22300745198530623141535718272648361505980416-bit, WPA3-Enterprise-44601490397061246283071436545296723011960832-bit, WPA3-Enterprise-89202980794122492566142873090593446023921664-bit, WPA3-Enterprise-178405961588244985132285746181186892047843328-bit, WPA3-Enterprise-356811923176489970264571492362373784095686656-bit, WPA3-Enterprise-713623846352979940529142984724747568191373312-bit, WPA3-Enterprise-1427247692705959881058285969449495136382746624-bit, WPA3-Enterprise-2854495385411919762116571938898990272765493248-bit, WPA3-Enterprise-5708990770823839524233143877797980545530986496-bit, WPA3-Enterprise-11417981541647679048466287755595961091061972992-bit, WPA3-Enterprise-22835963083295358096932575511191922182123945984-bit, WPA3-Enterprise-45671926166590716193865151022383844364247891968-bit, WPA3-Enterprise-91343852333181432387730302044767688728495783936-bit, WPA3-Enterprise-182687704666362864775460604089535377456991567872-bit, WPA3-Enterprise-365375409332725729550921208179070754913983135744-bit, WPA3-Enterprise-730750818665451459101842416358141509827966271488-bit, WPA3-Enterprise-1461501637330902918203684832716283019655932542976-bit, WPA3-Enterprise-2923003274661805836407369665432566039311865085952-bit, WPA3-Enterprise-5846006549323611672814739330865132078623730171904-bit, WPA3-Enterprise-11692013098647223345629478661730264157247460343808-bit, WPA3-Enterprise-23384026197294446691258957323460528314494920687616-bit, WPA3-Enterprise-46768052394588893382517914646921056628989841375232-bit, WPA3-Enterprise-93536104789177786765035829293842113257979682750464-bit, WPA3-Enterprise-187072209578355573530071658587684226515959365500928-bit, WPA3-Enterprise-374144419156711147060143317175368453031918731001856-bit, WPA3-Enterprise-748288838313422294120286634350736906063837462003712-bit, WPA3-Enterprise-1496577676626844588240573268701473812127674924007424-bit, WPA3-Enterprise-2993155353253689176481146537402947624255349848014848-bit, WPA3-Enterprise-5986310706507378352962293074805895248510699696029696-bit, WPA3-Enterprise-11972621413014756705924586149611790497021399392059392-bit, WPA3-Enterprise-23945242826029513411849172299223580994042798784118784-bit, WPA3-Enterprise-47890485652059026823698344598447161988085597568237568-bit, WPA3-Enterprise-95780971304118053647396689196894323976171195136475136-bit, WPA3-Enterprise-191561942608236107294793378393788647952342390272950272-bit, WPA3-Enterprise-383123885216472214589586756787577295904684780545900544-bit, WPA3-Enterprise-766247770432944429179173513575154591809369561091801088-bit, WPA3-Enterprise-1532495540865888858358347027150309183618739122183602176-bit, WPA3-Enterprise-3064991081731777716716694054300618367237478244367204352-bit, WPA3-Enterprise-6129982163463555433433388108601236734474956488734408704-bit, WPA3-Enterprise-12259964326927110866866776217202473468949912977468817408-bit, WPA3-Enterprise-24519928653854221733733552434404946937899825954937634816-bit, WPA3-Enterprise-49039857307708443467467104868809893875799651909875269632-bit, WPA3-Enterprise-98079714615416886934934209737619787751599303819750539264-bit, WPA3-Enterprise-196159429228833773869868419475239575503198607639501078528-bit, WPA3-Enterprise-392318858457667547739736838950479151006397215279002157056-bit, WPA3-Enterprise-784637716915335095479473677900958302012794430558004314112-bit, WPA3-Enterprise-1569275433830670190958947355801916604025588861116008628224-bit, WPA3-Enterprise-3138550867661340381917894711603833208051177722232017256448-bit, WPA3-Enterprise-6277101735322680763835789423207666416102355444464034512896-bit, WPA3-Enterprise-12554203470645361527671578846415332832204710888928069025792-bit, WPA3-Enterprise-25108406941290723055343157692830665664409421777856138051584-bit, WPA3-Enterprise-50216813882581446110686315385661331328818843555712276103168-bit, WPA3-Enterprise-100433627765162892221372630771322662657637687111424552206336-bit, WPA3-Enterprise-200867255530325784442745261542645325315275374222849104126672-bit, WPA3-Enterprise-401734511060651568885490523085290650630550748445698208253344-bit, WPA3-Enterprise-803469022121303137770981046170581301261101496891396416506688-bit, WPA3-Enterprise-1606938044242606275541962092341162602522202993782792833013376-bit, WPA3-Enterprise-3213876088485212551083924184682325205044405987565585666026752-bit, WPA3-Enterprise-6427752176970425102167848369364650410088811975131171332053504-bit, WPA3-Enterprise-12855504353940850204335696738729300820177623950262342664107008-bit, WPA3-Enterprise-25711008707881700408671393477458601640355247900524685328214016-bit, WPA3-Enterprise-51422017415763400817342786954917203280710495801049370656428032-bit, WPA3-Enterprise-102844034831526801634685573909834406561420991602098741312856064-bit, WPA3-Enterprise-205688069663053603269371147819668813122841983204197482625712128-bit, WPA3-Enterprise-411376139326107206538742295639337626245683966408394965251424256-bit, WPA3-Enterprise-822752278652214413077484591278675252491367932816789930502848512-bit, WPA3-Enterprise-1645504557304428826154969182557350504982735865633579861005697024-bit, WPA3-Enterprise-3291009114608857652309938365114701009965471731267159722011394048-bit, WPA3-Enterprise-6582018229217715304619876730229402019930943462534319444022788096-bit, WPA3-Enterprise-13164036458435430609239753460458804039861886925068638888045576192-bit, WPA3-Enterprise-26328072916870861218479506920917608079723773850137277776091152384-bit, WPA3-Enterprise-52656145833741722436959013841835216159447547700274555552182304768-bit, WPA3-Enterprise-105312291667483444873918027683670432318895095400549111104364609536-bit, WPA3-Enterprise-210624583334966889747836055367340864637790190801098222208729219072-bit, WPA3-Enterprise-421249166669933779495672110734681729275580381602196444417458438144-bit, WPA3-Enterprise-842498333339867558991344221469363458551160763204392888834916876288-bit, WPA3-Enterprise-1684996666679735117982688442938726917102321526408785777669833752576-bit, WPA3-Enterprise-3369993333359470235965376885877453834204643052817571555339667505152-bit, WPA3-Enterprise-6739986666718940471930753771754907668409286105635143110679335010304-bit, WPA3-Enterprise-13479973333437880943861507543509815336818572211702866221358670020608-bit, WPA3-Enterprise-26959946666875761887723015087019630673637144423405732442717340041216-bit, WPA3-Enterprise-53919893333751523775446030174039261347274288846811464885434680082432-bit, WPA3-Enterprise-107839786667503047550892060348078522694548577693622929770869360164864-bit, WPA3-Enterprise-215679573335006095101784120696157045389097155387245859541738720329728-bit, WPA3-Enterprise-431359146670012190203568241392314090778194310774491719083477440659456-bit, WPA3-Enterprise-862718293340024380407136482784628181556388621548983438166954881318912-bit, WPA3-Enterprise-1725436586680048760814272965569256363112777243097966876333909762637824-bit, WPA3-Enterprise-3450873173360097521628545931138512726225544486195933752667819525275648-bit, WPA3-Enterprise-6901746346720195043257091862277025532451088972391867505335639050551296-bit, WPA3-Enterprise-13803492693440390086514183724554051064902177944783735010671278101102592-bit, WPA3-Enterprise-27606985386880780173028367449108102129804355889567470021342556202205184-bit, WPA3-Enterprise-55213970773761560346056734898216204259608711779134940042685112404410368-bit, WPA3-Enterprise-110427941547523120692113469796432408519217423558269880085370224808820736-bit, WPA3-Enterprise-220855883095046241384226939592864817038434847116539760170740449617641472-bit, WPA3-Enterprise-441711766190092482768453879185729634076869694233079520341480899235282944-bit, WPA3-Enterprise-883423532380184965536907758371459268153739388466159040682961798470565888-bit, WPA3-Enterprise-1766847064760369931073815516742918536307478776932318081365923596941131776-bit, WPA3-Enterprise-3533694129520739862147631033485837072614957553864636162731847193882263552-bit, WPA3-Enterprise-7067388259041479724295262066971674145229915107729272325463694387764527104-bit, WPA3-Enterprise-14134776518082959448590524133943348290459830215458544650927388775529054208-bit, WPA3-Enterprise-28269553036165918897181048267886696580919660430917089301854777551058108416-bit, WPA3-Enterprise-56539106072331837794362096535773393161839320861834178603709555102116216832-bit, WPA3-Enterprise-113078212144663675588724193071546786323678641723668357207419110204232433664-bit, WPA3-Enterprise-226156424289327351177448386143093572647357283447336714414838220408464867328-bit, WPA3-Enterprise-452312848578654702354896772286187145294714566894673428829676440816929734656-bit, WPA3-Enterprise-9046256971573094

Структура вхідного і вихідного пакету:

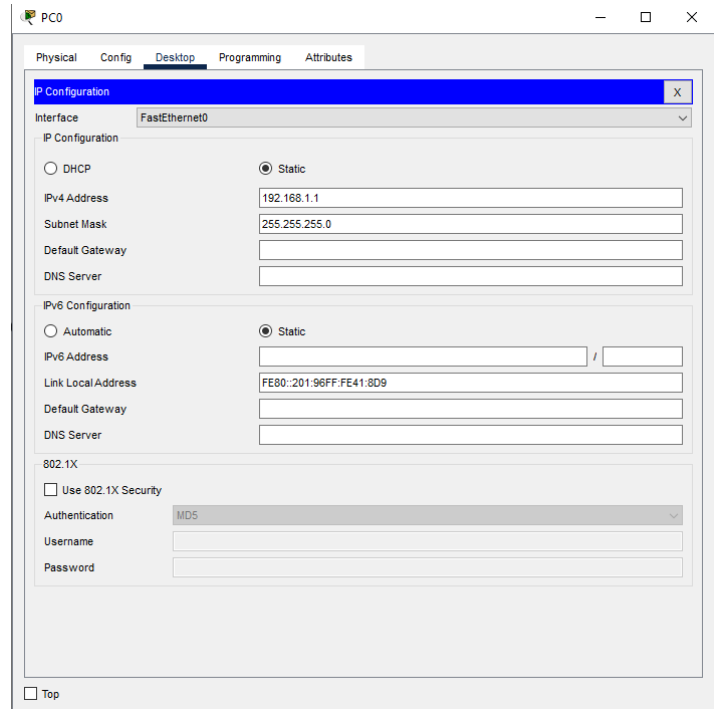
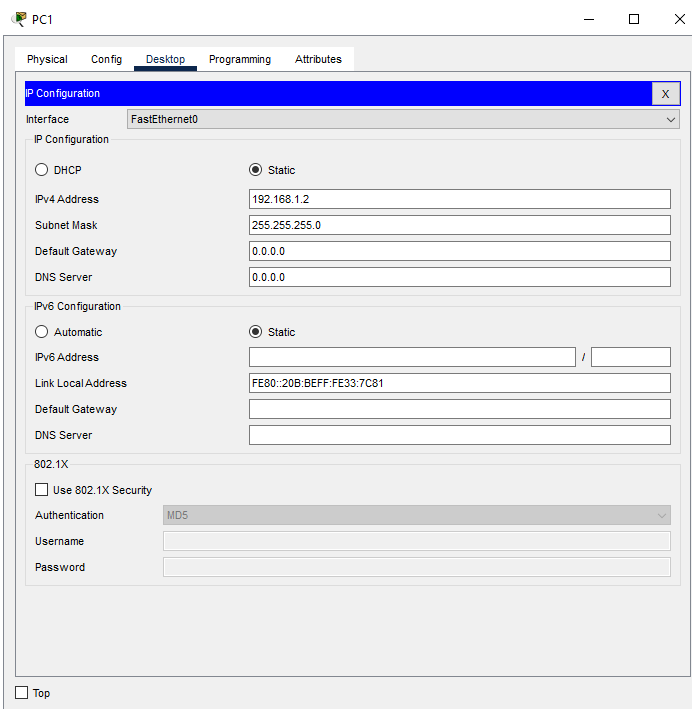


Завдання №2. Засвоєння принципів адресації на каналному і мережевому рівнях.

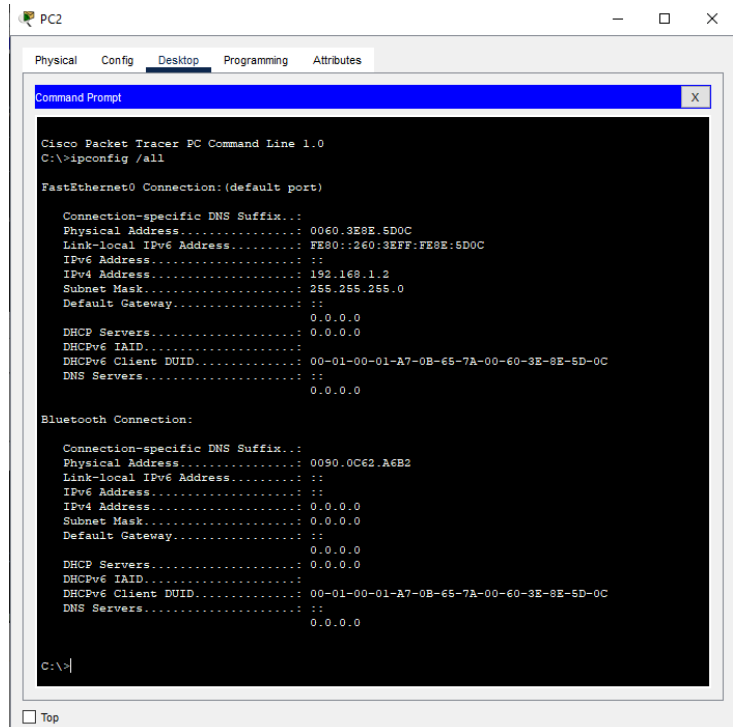
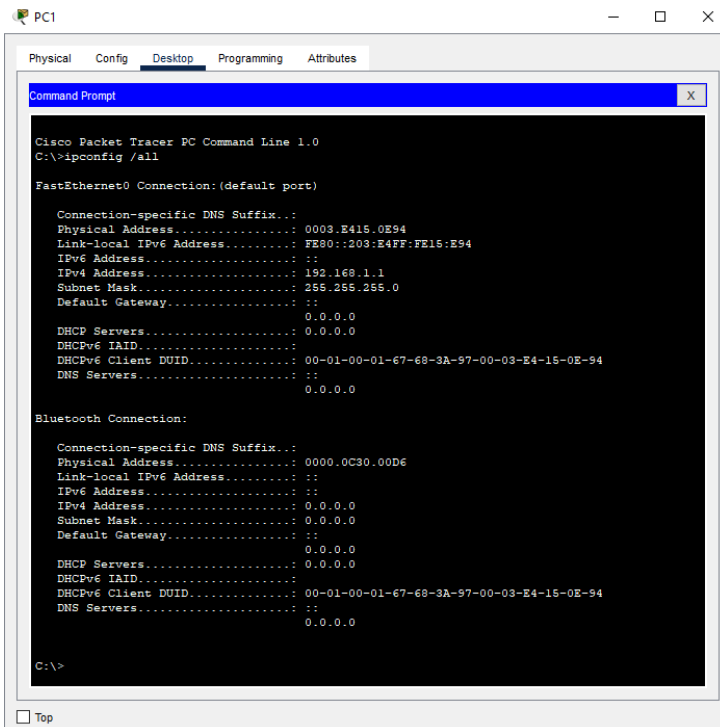
1. Побудова моделі мережі та присвоєння ір-адрес 192.168.1.1 та 192.168.1.2 до приладів PC1 та PC2 відповідно:



2. Призначити робочим станціям IP-адреси та маску. Перші три байти IP-адрес збігаються з адресою мережі, а останній байт дорівнює відповідно 1 та 2:



3. Визначити MAC-адресу кожної робочої станції за допомогою команди **ipconfig /all** з командного рядка:



4. На робочій станції PC1 з командного рядка виконати команду **arp -a**. Зафіксувати отриманий результат:

```
C:\> arp -a
No ARP Entries Found
C:\>
```

5. На робочій станції PC1 з командного рядка виконати команду ping на адресу станції PC2, після чого знову виконати команду arp -a. Пояснити отриманий результат.:

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.2           0060.3e8e.5d0c       dynamic
C:\>
```

Початкова перевірка таблиці ARP командою arp -a показала, що таблиця була порожньою: "No ARP Entries Found". Це очікувано, оскільки ще не надсилалися запити до інших пристроїв у мережі, і відповідно жодних відповідностей між IP- та MAC-адресами не було збережено.

Наступним кроком було надсилання запиту до пристрою з IP-адресою 192.168.1.2 за допомогою команди ping. Результат показав, що пристрій відповів на всі чотири пакети з мінімальною затримкою (<1 мс). Це підтвердило, що пристрій доступний і знаходиться в межах локальної мережі (LAN).

Після успішного виконання ping, було виконано команду arp -a, щоб перевірити зміни у таблиці ARP. Цього разу таблиця містила запис:

- **Internet Address:** 192.168.1.2 (IP-адреса пристрою).
- **Physical Address:** 0060.3e8e.5d0c (MAC-адреса пристрою).
- **Type:** dynamic (запис було створено автоматично).

Цей результат показав, що ARP-запит спрацював, і тепер PC1 "знає", як знайти пристрій 192.168.1.2 у мережі, використовуючи його MAC-адресу.

6. На робочій станції PC1 з командного рядка виконати команду `arp -d`. Пояснити призначення ключа `-d`:

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>arp -a
    Internet Address      Physical Address      Type
    192.168.1.2           0060.3e8e.5d0c       dynamic

C:\>arp -d
C:\>arp -a
No ARP Entries Found
C:\>
```

Ключ `-d` у команді `arp` використовується для видалення записів з таблиці ARP.

7. Перейти в режим Simulation. Із командного рядка робочої станції PC1 виконати команду `ping` на IP-адресу станції PC2. На «Simulation panel» натиснути кнопку «CaptureForward». Пояснити призначення пакетів, що відправляються зі станції PC1. Натиснути кнопкою миші на кожному із створених пакетів і переглянути їх вміст. Звернути увагу на адреси відправника та отримувача. Натискаючи на «CaptureForward» прослідкувати за формуванням та передачею створених пакетів мережею, одночасно спостерігаючи за командним рядком. Пояснити призначення ARP-пакету.

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.000	--	PC1	ARP
	0.001	PC1	PC2	ARP
	0.002	PC2	PC1	ARP
	0.002	--	PC1	ICMP
	0.003	PC1	PC2	ICMP
	0.004	PC2	PC1	ICMP
	1.005	--	PC1	ICMP
	1.006	PC1	PC2	ICMP
	1.007	PC2	PC1	ICMP
	2.009	--	PC1	ICMP
	2.010	PC1	PC2	ICMP
	2.011	PC2	PC1	ICMP
	3.011	--	PC1	ICMP
	3.012	PC1	PC2	ICMP
	3.013	PC2	PC1	ICMP

ARP-пакети

- 0.000 сек: PC1 ініціює ARP-запит, щоб визначити MAC-адресу пристрою PC2, який має відповідну IP-адресу.
- 0.001 сек: ARP-запит передається від PC1 до PC2.
- 0.002 сек: PC2 відповідає на ARP-запит, відправляючи свою MAC-адресу назад до PC1.

Призначення ARP-пакетів:

ARP (Address Resolution Protocol) використовується для встановлення відповідності між IP-адресою (рівень 3, мережевий рівень) та MAC-адресою (рівень 2, канальний рівень). Це необхідно для доставки пакетів у локальній мережі.

ICMP-пакети

- **0.002 сек:** Перший ICMP Echo Request (ping) відправляється з PC1 до PC2. Він перевіряє доступність станції PC2.
- **0.003 сек:** PC2 отримує ICMP Echo Request і відповідає ICMP Echo Reply.
- Наступні серії ICMP-пакетів (1.005, 2.009, 3.011 сек) відповідають додатковим спробам ping і обміну між PC1 та PC2.

Призначення ICMP-пакетів:

ICMP (Internet Control Message Protocol) використовується для діагностики мережеских проблем. Зокрема, ping перевіряє:

1. Доступність вузла (чи отримано відповідь).
2. Час передачі пакета (RTT - round trip time).

ARP-запити відбуваються лише один раз, оскільки інформація кешується в ARP-таблиці.

ICMP-пакети продовжують обмінюватися для кожного запиту ping, відображаючи затримку (RTT) між станціями.

ARP:

PDU Information at Device: PC2

OSI Model Inbound PDU Details Outbound PDU Details

At Device: PC2
Source: PC1
Destination: Broadcast

In Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0003.E415.0E94 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2
Layer 1: Port FastEthernet0

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0060.3E8E.5D0C >> 0003.E415.0E94 ARP Packet Src. IP: 192.168.1.2, Dest. IP: 192.168.1.1
Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

PDU Information at Device: PC2

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

EthernetII

0	4	8	Bytes
PREAMBLE: 101010...10		DEST ADDR: FFFF.FFFF.FFFF	
SRC ADDR: 0003.E415.0E94	TYPE: 0x08	DATA (VARIABLE LENGTH)	FCS: 0x00000000

Arp

0	8	16	Bits
HARDWARE TYPE: 0x0001		PROTOCOL TYPE: 0x0800	
HLEN: 0x06	PLEN: 0x04	OPCODE: 0x0001	
SOURCE MAC: 0003.E415.0E94			
SOURCE IP: 192.168.1.1			
TARGET MAC: 0000.0000.0000			
TARGET IP: 192.168.1.2			

PDU Information at Device: PC2

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

EthernetII

0	4	8	Bytes
PREAMBLE: 101010...10		DEST ADDR: 0003.E415.0E94	
SRC ADDR: 0060.3E8E.5D0C	TYPE: 0x08	DATA (VARIABLE LENGTH)	FCS: 0x00000000

Arp

0	8	16	Bits
HARDWARE TYPE: 0x0001		PROTOCOL TYPE: 0x0800	
HLEN: 0x06	PLEN: 0x04	OPCODE: 0x0002	
SOURCE MAC: 0060.3E8E.5D0C			
SOURCE IP: 192.168.1.2			
TARGET MAC: 0003.E415.0E94			
TARGET IP: 192.168.1.1			

ICMP:

PDU Information at Device: PC2

OSI Model

Inbound PDU Details

Outbound PDU Details

At Device: PC2

Source: PC1

Destination: 192.168.1.2

In Layers

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2 ICMP Message Type: 8

Layer 2: Ethernet II Header 0003.E415.0E94 >> 0060.3E8E.5D0C

Layer 1: Port FastEthernet0

Out Layers

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.1.1 ICMP Message Type: 0

Layer 2: Ethernet II Header 0060.3E8E.5D0C >> 0003.E415.0E94

Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

Challenge Me

<< Previous Layer

Next Layer >>

PDU Information at Device: PC2

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10

DEST ADDR: 0060.3E8E.5D0C

SRC ADDR: 0003.E415.0E94

TYP E: 0x

DATA (VARIABLE LENGTH)

FCS: 0x00000000

IP

0 4 8 16 20 24 Bits

VER: 4

IHL: 5

DSCP: 0x00

TL: 128

ID: 0x0011

FLAGS: 0x0

FRAG OFFSET: 0x000

TTL: 128

PRO: 0x01

CHKSUM

SRC IP: 192.168.1.1

DST IP: 192.168.1.2

DATA (VARIABLE LENGTH)

ICMP

0 8 16 Bits

TYPE: 0x08

CODE: 0x00

CHECKSUM

ID: 0x0006

SEQ NUMBER: 17

Variable Size PDU

0 8 16 Bytes

DATA (VARIABLE LENGTH)

PDU Information at Device: PC2

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10

DEST ADDR: 0003.E415.0E94

SRC ADDR: 0060.3E8E.5D0C

TYP E: 0x

DATA (VARIABLE LENGTH)

FCS: 0x00000000

IP

0 4 8 16 20 24 Bits

VER: 4

IHL: 5

DSCP: 0x00

TL: 128

ID: 0x0011

FLAGS: 0x0

FRAG OFFSET: 0x000

TTL: 128

PRO: 0x01

CHKSUM

SRC IP: 192.168.1.2

DST IP: 192.168.1.1

DATA (VARIABLE LENGTH)

ICMP

0 8 16 Bits

TYPE: 0x00

CODE: 0x00

CHECKSUM

ID: 0x0006

SEQ NUMBER: 17

Variable Size PDU

0 8 16 Bytes

DATA (VARIABLE LENGTH)

Завдання №3. Засвоєння принципів динамічного призначення IP-адрес:

1. За допомогою програми Packet Tracer побудувати мережу, структура якої наведена на рисунку:



2. Перейти до режиму "Simulation".

3. Вибрати режим конфігурування сервера. Призначити IP-адресу, перші три байти якої збігаються з адресою мережі, а останній байт дорівнює 100:

The screenshot shows the configuration window for "Server0" in Packet Tracer. The "Desktop" tab is selected. Within this tab, the "IP Configuration" sub-tab is active. The "Static" radio button is selected for IP configuration. The IPv4 Address is set to "192.168.1.100", the Subnet Mask is "255.255.255.0", the Default Gateway is "0.0.0.0", and the DNS Server is "0.0.0.0". The IPv6 Configuration section shows "Static" selected, with an empty IPv6 Address field, a Link Local Address of "FE80::2D0:97FF:FE6C:86BB", and empty fields for Default Gateway and DNS Server. The 802.1X section has "Use 802.1X Security" unchecked, with "MD5" selected for Authentication and empty fields for Username and Password. A "Top" button is at the bottom left.

4. У режимі конфігурування перейти до вкладки DHCP і налаштувати таким чином: у полях Default Gateway та DNS Server ввести адреси, перші три байти

яких збігаються з адресою мережі, а останній байт відповідно дорівнює 254 та 253. У полі Start IP Address ввести адресу, перші три байти якої збігаються з адресою мережі, а останній дорівнює 10. Значення поля Maximum number of Users встановити рівним 15:

Server0

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: 192.168.1.254

DNS Server: 192.168.1.253

Start IP Address: 192 168 1 10

Subnet Mask: 255 255 255 0

Maximum Number of Users: 15

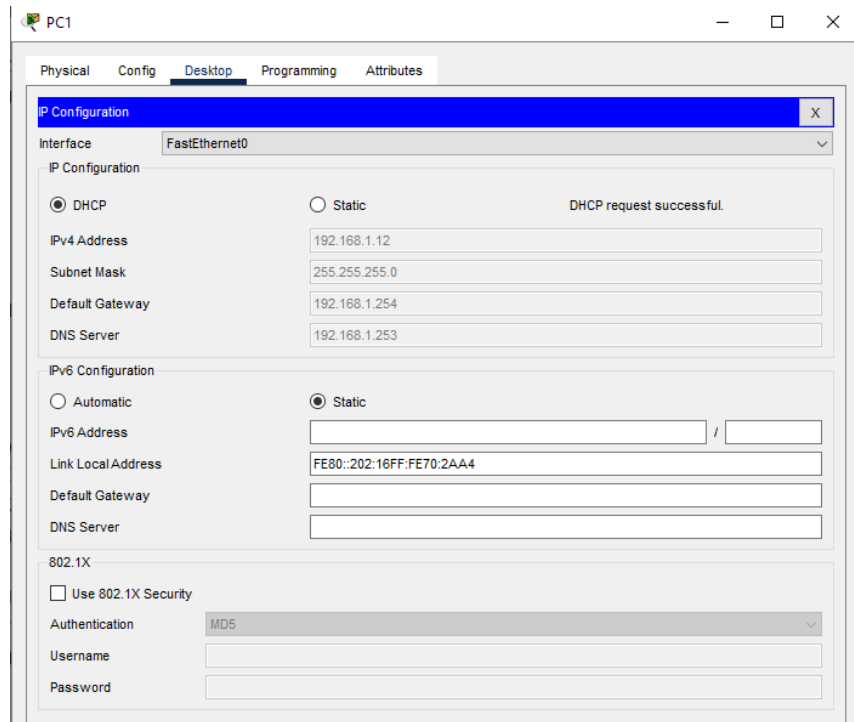
TFTP Server: 0.0.0.0

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....	192.168....	192.168....	255.255....	15	0.0.0.0	0.0.0.0

5. На PC1 включити динамічний режим конфігурування адрес (DHCP). Впевнитись, що поле IP-адреси, маска підмережі, шлюз за замовчуванням та DNS-сервер порожні. Не закриваючи вікна конфігурування PC1 натиснути кнопку «CaptureForward»:



Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Server1	ARP
	0.000	--	PC5	DHCP
	0.001	Server1	PC5	ARP
	0.002	PC5	Server1	DHCP
	0.002	--	Server1	ICMP
	0.002	--	Server1	ARP
	0.004	Server1	PC5	ARP
	1.003	--	Server1	ICMP
	1.003	--	Server1	ARP
	1.505	Server1	PC5	DHCP
	1.507	PC5	Server1	DHCP
	1.509	Server1	PC5	DHCP
	1.509	--	PC5	ARP
	1.511	PC5	Server1	ARP
	2.005	--	Server1	ICMP
	2.005	--	Server1	ICMP

6. Переглянути вміст пакета, що передав PC1, звернути увагу, що вказано в полі адреси отримувача, порівняти вміст пакетів «Inbound PDU» та «Outbound PDU». Визначити, яку інформацію передав DHCP-сервер станції:

Клієнт DHCP підключається до мережі і починає пошук DHCP-сервера, для чого відправляє запит DHCPDISCOVER на широкомовну адресу 255.255.255.255. Адреса клієнта в цьому запиті 0.0.0.0, оскільки своєї адреси у

клієнта ще немає. Також в запиті клієнт вказує свою MAC-адресу.

PDU Information at Device: Server1

OSI Model Inbound PDU Details

At Device: Server1
Source: PC5
Destination: 255.255.255.255

In Layers
Layer 7: DHCP Packet Server: 0.0.0.0, Client: 0.0.0.0
Layer6
Layer5
Layer 4: UDP Src Port: 68, Dst Port: 67
Layer 3: IP Header Src. IP: 0.0.0.0, Dest. IP: 255.255.255.255
Layer 2: Ethernet II Header 0002.4A4A.C690 >> FFFF.FFFF.FFFF
Layer 1: Port FastEthernet0

Out Layers
Layer 7:
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

1. FastEthernet0 receives the frame.

Запит надходить всім модулям, які знаходяться в даному сегменті мережі, але відповідають на нього тільки DHCP-сервери:

PDU Information at Device: Server1

OSI Model Outbound PDU Details

At Device: Server1
Source: Server1
Destination: 192.168.1.19

In Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.100, Dest. IP: 192.168.1.19 ICMP Message Type: 8
Layer 2:
Layer1

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The destination IP address is in the same subnet. The device sets the next-hop to destination.

Challenge Me

<< Previous Layer

Next Layer >>

PDU Information at Device: Server1

OSI Model Outbound PDU Details

At Device: Server1
Source: Server1
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer2	Layer 2: Ethernet II Header 00D0.BAB5.5992 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.100, Dest. IP: 192.168.1.19
Layer1	Layer 1: Port(s): FastEthernet0

1. The ARP process constructs a request for the target IP address.
2. The device encapsulates the PDU into an Ethernet frame.

Challenge Me << Previous Layer Next Layer >>

Запит надходить всім модулям, які знаходяться в даному сегменті мережі, але відповідають на нього тільки DHCP-сервери.

PDU Information at Device: PC5

OSI Model Inbound PDU Details Outbound PDU Details

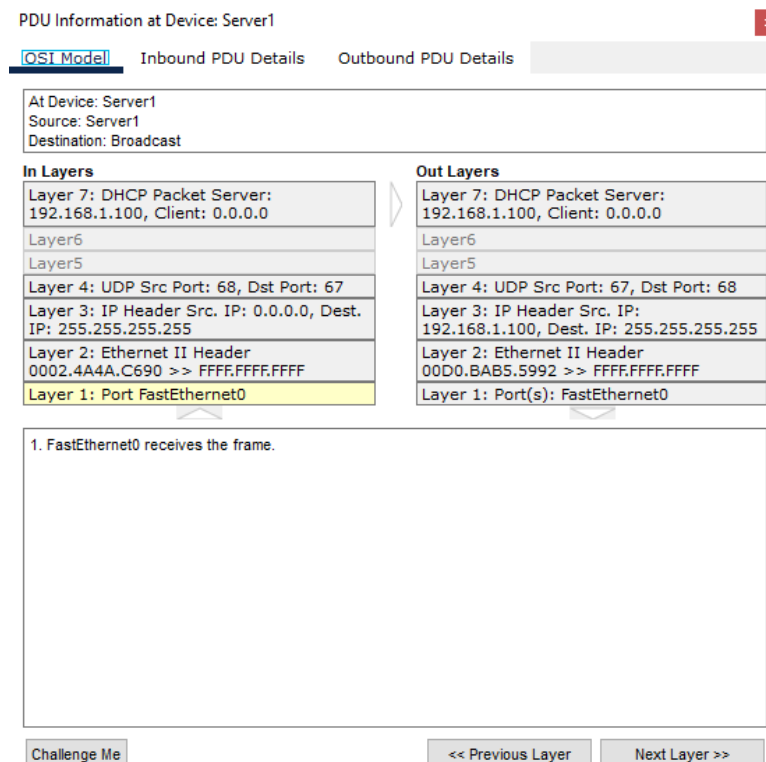
At Device: PC5
Source: Server1
Destination: Broadcast

In Layers	Out Layers
Layer 7: DHCP Packet Server: 192.168.1.100, Client: 0.0.0.0	Layer 7: DHCP Packet Server: 192.168.1.100, Client: 0.0.0.0
Layer6	Layer6
Layer5	Layer5
Layer 4: UDP Src Port: 67, Dst Port: 68	Layer 4: UDP Src Port: 68, Dst Port: 67
Layer 3: IP Header Src. IP: 192.168.1.100, Dest. IP: 255.255.255.255	Layer 3: IP Header Src. IP: 0.0.0.0, Dest. IP: 255.255.255.255
Layer 2: Ethernet II Header 00D0.BAB5.5992 >> FFFF.FFFF.FFFF	Layer 2: Ethernet II Header 0002.4A4A.C690 >> FFFF.FFFF.FFFF
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

Challenge Me << Previous Layer Next Layer >>

DHCP-сервер, який отримав запит **DHCPDISCOVER**, аналізує його зміст, вибирає підходящу конфігурацію мережі та відправляє її в повідомленні **DHCPOFFER**. **DHCPOFFER** відправляється на широкомовне розсилання. Якщо в мережі знаходиться кілька DHCP-серверів, то клієнт отримує кілька відповідей **DHCPOFFER** і вибирає з них одну, як правило, отриману першою.



Отримавши відповідь сервера, клієнт відповідає повідомленням **DHCPREQUEST**, в якому «офіційно» запитує у сервера надані йому налаштування. В повідомленні **DHCPREQUEST** міститься та ж інформація, що і в **DHCPDISCOVER**, а також IP-адреса вибраного DHCP-сервера. **DHCPREQUEST** надсилається на широкомовну адресу і ті DHCP-сервери, адреса яких відсутня в повідомленні, розуміють, що їхня пропозиція відкинута.

PDU Information at Device: PC5

OSI Model Inbound PDU Details

At Device: PC5
Source: Server1
Destination: Broadcast

In Layers	Out Layers
Layer 7: DHCP Packet Server: 192.168.1.100, Client: 0.0.0.0	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: UDP Src Port: 67, Dst Port: 68	Layer4
Layer 3: IP Header Src. IP: 192.168.1.100, Dest. IP: 255.255.255.255	Layer3
Layer 2: Ethernet II Header 00D0.BAB5.5992 >> FFFF.FFFF.FFFF	Layer2
Layer 1: Port FastEthernet0	Layer1

1. FastEthernet0 receives the frame.

Challenge Me << Previous Layer Next Layer >>

PDU Information at Device: PC5

OSI Model Outbound PDU Details

At Device: PC5
Source: PC5
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer2	Layer 2: Ethernet II Header 0002.4A4A.C690 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.19, Dest. IP: 192.168.1.19
Layer1	Layer 1: Port(s): FastEthernet0

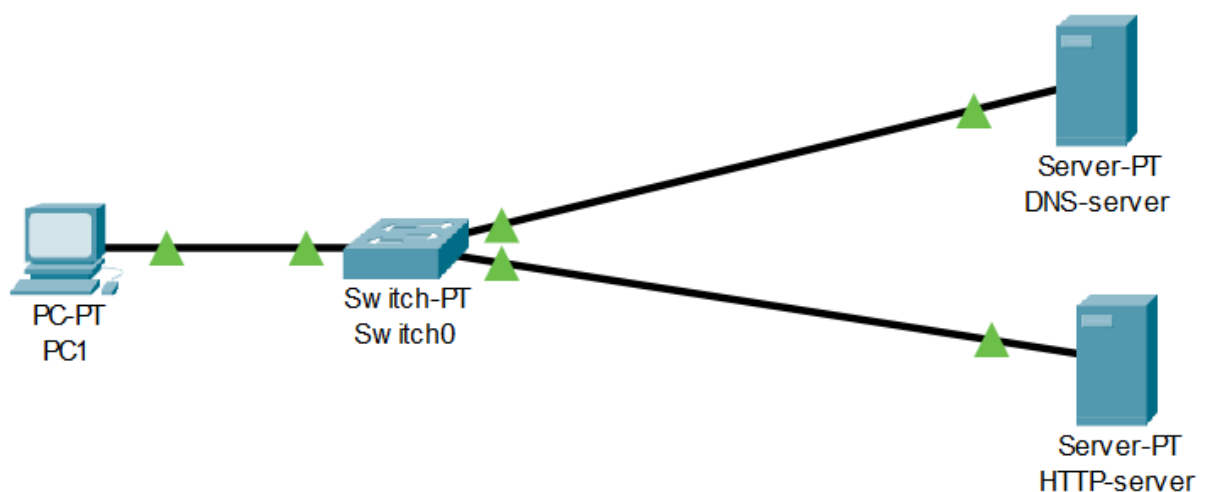
1. The ARP frame is a gratuitous ARP Request.
2. The device encapsulates the PDU into an Ethernet frame.

Перш ніж зрозуміти процес призначення IP-адреси, важливо знати деякі ключові технічні терміни, які використовуються в контексті сервера DHCP. Пул адрес DHCP – це віртуальний контейнер, який містить усі IP-адреси, які були налаштовані в діапазоні DHCP, щоб зробити їх доступними для клієнтських комп'ютерів. Як тільки будь-яка IP-адреса з пулу адрес

призначається клієнтському комп'ютеру, адреса тимчасово видаляється з пулу. Коли сервер DHCP призначає IP-адресу клієнтському комп'ютеру DHCP, адреса призначається на певний час. Тривалість часу, протягом якого сервер DHCP призначає IP адресу клієнтському комп'ютеру DHCP, технічно називається орендою DHCP. Коли термін оренди DHCP закінчується, IP-адреса відкликається з комп'ютера-клієнта DHCP і повертається до пулу адрес DHCP. Оскільки DHCP-сервер відіграє важливу роль у мережі, коли кількість клієнтських комп'ютерів велика, DHCP-сервер діє дуже розумно та точно, щоб уникнути будь-яких конфліктів або погіршення продуктивності. Покроковий процес, за допомогою якого DHCP-сервер призначає IP-адресу клієнтському комп'ютеру DHCP, коротко називається DORA. Після завершення всього процесу DORA сервер DHCP позначає IP-адресу як призначену в його базі даних, і клієнтський комп'ютер DHCP починає використовувати призначену IP-адресу для зв'язку з іншими комп'ютерами в мережі.

Завдання №4. Засвоєння принципів перетворення DNS-імен в IP-адреси.

1. За допомогою програми Packet Tracer побудувати мережу, структуру якої наведено на рисунку 6.18. Призначити такі IP-адреси: перші три байти всіх адрес відповідають адресі мережі, останній байт PC1 – 1; DNS- сервера – 253; HTTP-сервера – 252.



PC1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:B0FF:FE79:5B52

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

DNS-server

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.253

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::202:4AFF:FE9A:2B73

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

HTTP-server

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.252

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:8FFF:FE74:878B

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

2. На PC1 в полі DNS вказати відповідну адресу.

PC1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 192.168.1.253

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:B0FF:FE79:5B52

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

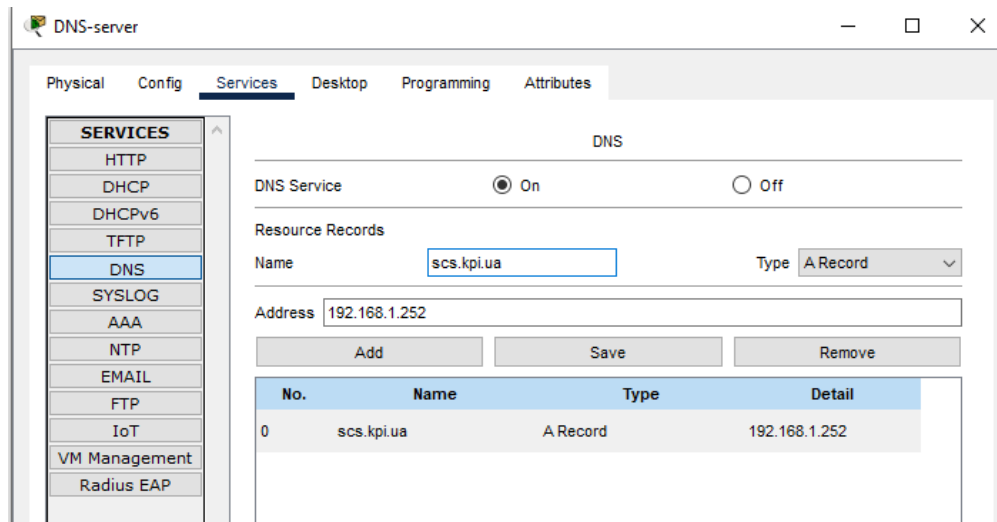
Authentication MD5

Username

Password

☐ Top

3. На DNS-сервері в вкладці DNS додати запис, в якому в полі Domain Name вказати ім'я scs.kpi.ua, а в полі IP-Address – адресу HTTP-сервера.



4. Перейти до режиму “Simulation”.

5. На PC1 в командному рядку виконати команду ping, вказавши доменне ім'я scs.kpi.ua та натиснути кнопку «Capture/Forward».

6. Натискати кнопку «Capture/Forward», поки на PC1 не буде сформований DNS-запит. Пояснити призначення ARP-пакетів, які були сформовані на попередніх кроках:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping scs.kpi.ua

Pinging 192.168.1.252 with 32 bytes of data:

Reply from 192.168.1.252: bytes=32 time=17ms TTL=128
Reply from 192.168.1.252: bytes=32 time=9ms TTL=128
Reply from 192.168.1.252: bytes=32 time=6ms TTL=128
Reply from 192.168.1.252: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.1.252:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 17ms, Average = 10ms

C:\>
```

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	DNS
	0.000	--	PC1	ARP
	0.003	PC1	Switch0	ARP
	0.005	Switch0	HTTP-server	ARP
	0.005	Switch0	DNS-server	ARP
	0.007	DNS-server	Switch0	ARP
	0.009	Switch0	PC1	ARP
	0.009	--	PC1	DNS
	0.011	PC1	Switch0	DNS
	0.013	Switch0	DNS-server	DNS
	0.014	DNS-server	Switch0	DNS
	0.016	Switch0	PC1	DNS
	0.016	--	PC1	ICMP
	0.016	--	PC1	ARP
	0.020	PC1	Switch0	ARP
	0.022	Switch0	HTTP-server	ARP
	0.022	Switch0	DNS-server	ARP
	0.024	HTTP-server	Switch0	ARP
	0.026	Switch0	PC1	ARP
	0.026	--	PC1	ICMP
	0.027	PC1	Switch0	ICMP
	0.029	Switch0	HTTP-server	ICMP
	0.031	HTTP-server	Switch0	ICMP
	0.033	Switch0	PC1	ICMP
	1.033	--	PC1	ICMP

ARP (Address Resolution Protocol) використовується для визначення MAC-адрес пристроїв у локальній мережі. Оскільки DNS-запит передається від PC1 до DNS-сервера, а в подальшому — від PC1 до HTTP-сервера, комп'ютер PC1 спочатку має отримати MAC-адреси обох серверів. Саме для цього і використовуються ARP-запити.

На початку симуляції ми спостерігали декілька етапів формування ARP-пакетів:

1. Визначення MAC-адреси DNS-сервера

- **0.000 сек:** PC1 формує ARP-запит для визначення MAC-адреси DNS-сервера. Цей запит передається через Switch0 до всіх підключених пристроїв.
- **0.007 сек:** DNS-сервер відповідає на запит, повідомляючи свою MAC-адресу.
- **0.009 сек:** PC1 отримує відповідь і зберігає MAC-адресу DNS-сервера у своїй таблиці ARP.

2. Формування DNS-запиту

Після отримання MAC-адреси DNS-сервера PC1 формує DNS-запит і передає його до DNS-сервера. Цей запит є ключовим для отримання IP-адреси HTTP-сервера.

3. Визначення MAC-адреси HTTP-сервера

- **0.016 сек:** Після отримання відповіді від DNS-сервера PC1 дізнається IP-адресу HTTP-сервера (192.168.1.252).
- **0.020 сек:** PC1 формує новий ARP-запит, щоб визначити MAC-адресу HTTP-сервера.
- **0.024 сек:** HTTP-сервер відповідає на ARP-запит, після чого його MAC-адреса зберігається у таблиці ARP на PC1.

4. Передача ICMP-запиту (ping)

Після завершення ARP-взаємодії PC1 починає надсилати ICMP-пакети до HTTP-сервера. На цьому етапі ARP більше не використовується, оскільки всі необхідні MAC-адреси вже визначено.

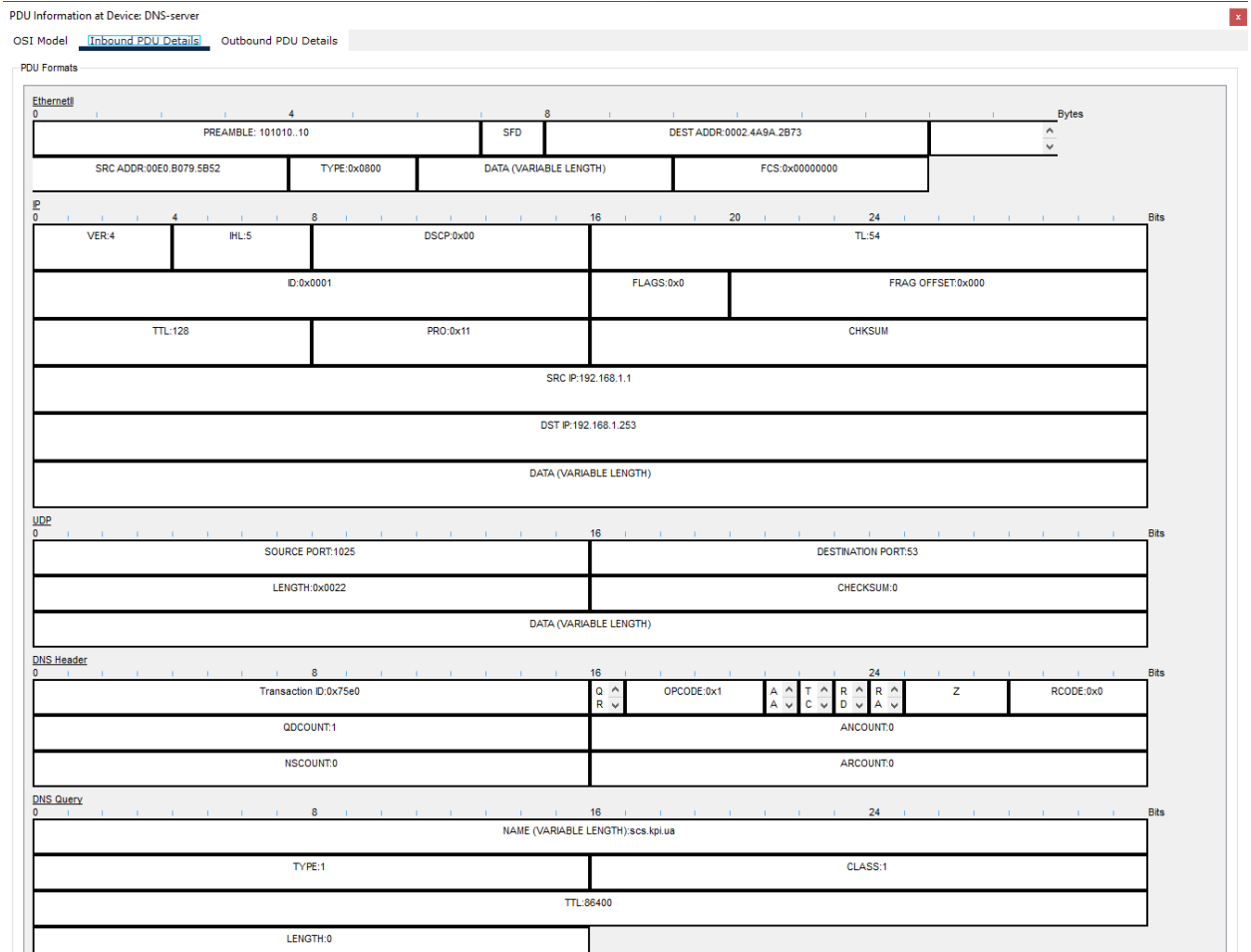
7. Коли DNS-запит надійде на сервер, переглянути його вміст (Inbound PDU) та вміст відповіді (Outbound PDU). Пояснити інформацію, що міститься в цих пакетах.

PDU Information at Device: DNS-server

OSI Model Inbound PDU Details Outbound PDU Details

At Device: DNS-server Source: PC1 Destination: 192.168.1.253	
In Layers	Out Layers
Layer 7: DNS	Layer 7: DNS
Layer 6	Layer 6
Layer 5	Layer 5
Layer 4: UDP Src Port: 1025, Dst Port: 53	Layer 4: UDP Src Port: 53, Dst Port: 1025
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.253	Layer 3: IP Header Src. IP: 192.168.1.253, Dest. IP: 192.168.1.1
Layer 2: Ethernet II Header 00E0.B079.5B52 >> 0002.4A9A.2B73	Layer 2: Ethernet II Header 0002.4A9A.2B73 >> 00E0.B079.5B52
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.



Аналіз структури DNS-запиту

1. Ethernet Header

- SRC ADDR: 00E0.B079.5852 — MAC-адреса відправника (робочої станції PC1).
- DEST ADDR: 0002.4A9A.2B73 — MAC-адреса одержувача (DNS-сервера).
- TYPE: 0x0800 — Позначає, що передається IP-пакет.

2. IP Header

- VER: 4 — Версія протоколу IP (IPv4).
- SRC IP: 192.168.1.1 — IP-адреса відправника (PC1).
- DST IP: 192.168.1.253 — IP-адреса отримувача (DNS-сервера).
- PRO: 0x11 — Протокол UDP (User Datagram Protocol), який використовується для DNS-запитів.

3. UDP Header

- Source Port: 1025 — Випадковий порт відправника (PC1),

використаний для зв'язку.

- Destination Port: 53 — Порт DNS, стандартний для отримання запитів.
- Length: 0x0022 — Довжина UDP-пакета.

4. DNS Header

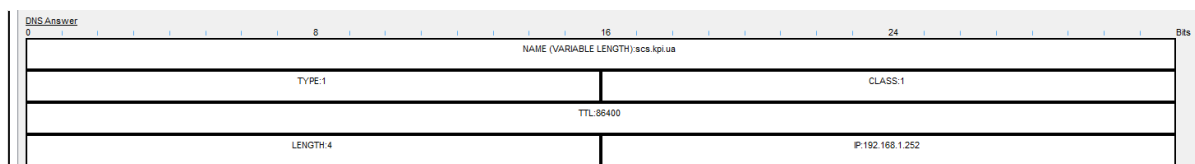
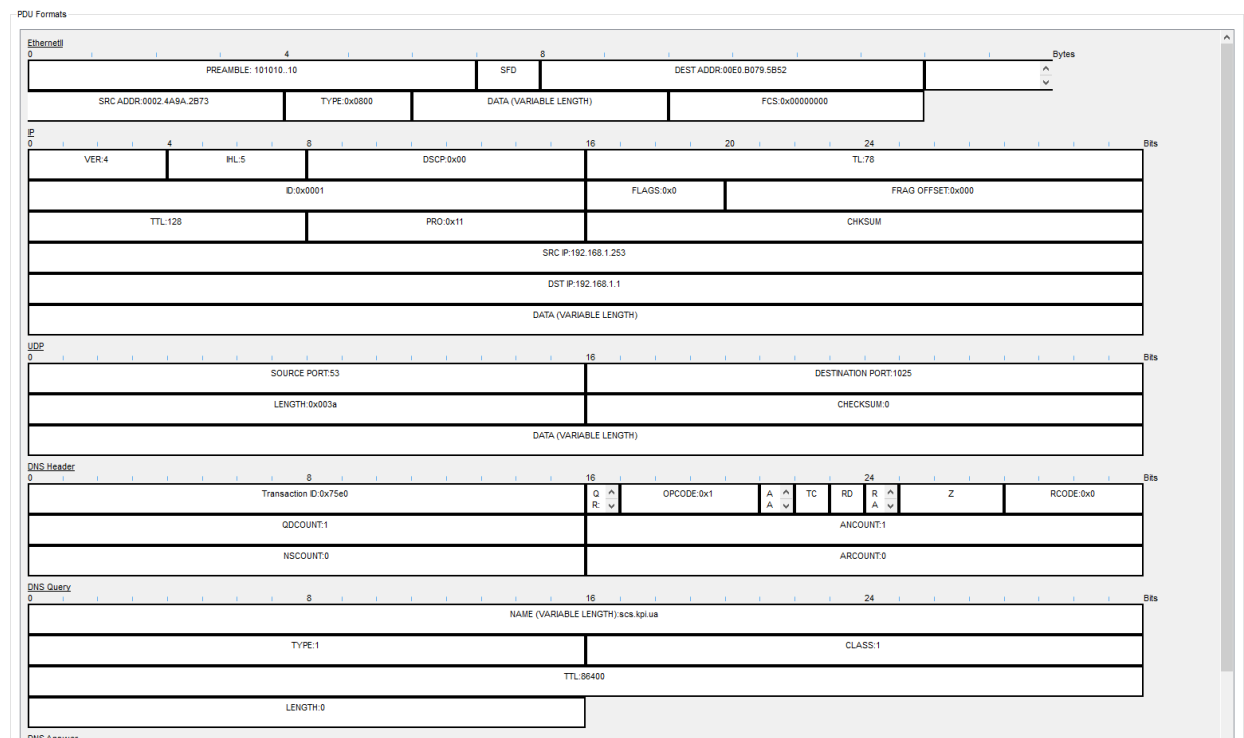
- Transaction ID: 0x75E0 — Унікальний ідентифікатор для зіставлення запиту та відповіді.
- Opcode: 0x1 — Вказує на стандартний запит (Query).
- QCOUNT: 1 — Кількість запитуваних доменних імен (одне доменне ім'я).

5. DNS Query

- Name: scs.kpi.ua — Доменне ім'я, яке необхідно перетворити в IP-адресу.
- Type: 1 — Запит для IPv4-адреси (A-запис).
- Class: 1 — Інтернет (IN).
- TTL: 86400 — Час життя запису в секундах (24 години).

PDU Information at Device: DNS-server

OSI Model Inbound PDU Details [Outbound PDU Details](#)



Аналіз структури DNS-відповіді

1. Ethernet Header

- SRC ADDR: 0002.4A9A.2B73 — MAC-адреса відправника (DNS-сервера).
- DEST ADDR: 00E0.B079.5852 — MAC-адреса одержувача (робочої станції PC1).
- TYPE: 0x0800 — Вказує на те, що передається IP-пакет.

2. IP Header

- VER: 4 — Версія протоколу IP (IPv4).
- SRC IP: 192.168.1.253 — IP-адреса відправника (DNS-сервера).
- DST IP: 192.168.1.1 — IP-адреса одержувача (PC1).
- PRO: 0x11 — Протокол UDP (User Datagram Protocol).

3. UDP Header

- Source Port: 53 — Порт DNS-сервера, стандартний для відповіді на DNS-запити.
- Destination Port: 1025 — Порт клієнта (PC1), через який був зроблений запит.
- Length: 0x003a — Довжина UDP-пакета.

4. DNS Header

- Transaction ID: 0x75E0 — Ідентифікатор транзакції, що відповідає запиту. Це дозволяє клієнту зрозуміти, на який запит прийшла відповідь.
- Opcode: 0x1 — Стандартна відповідь на запит.
- QR: 1 — Позначає, що це відповідь, а не запит.
- RD: 1 — Встановлений біт рекурсії, що підтверджує виконання рекурсивного пошуку.
- RA: 1 — Сервер підтримує рекурсивний пошук.
- RCode: 0x0 — Відповідь успішна, без помилок.

5. DNS Query

- Name: scs.kpi.ua — Доменне ім'я, запитане клієнтом.

- Type: 1 — Вказує на те, що клієнт запитував IPv4-адресу (А-запис).
- Class: 1 — Інтернет (IN).

6. DNS Answer

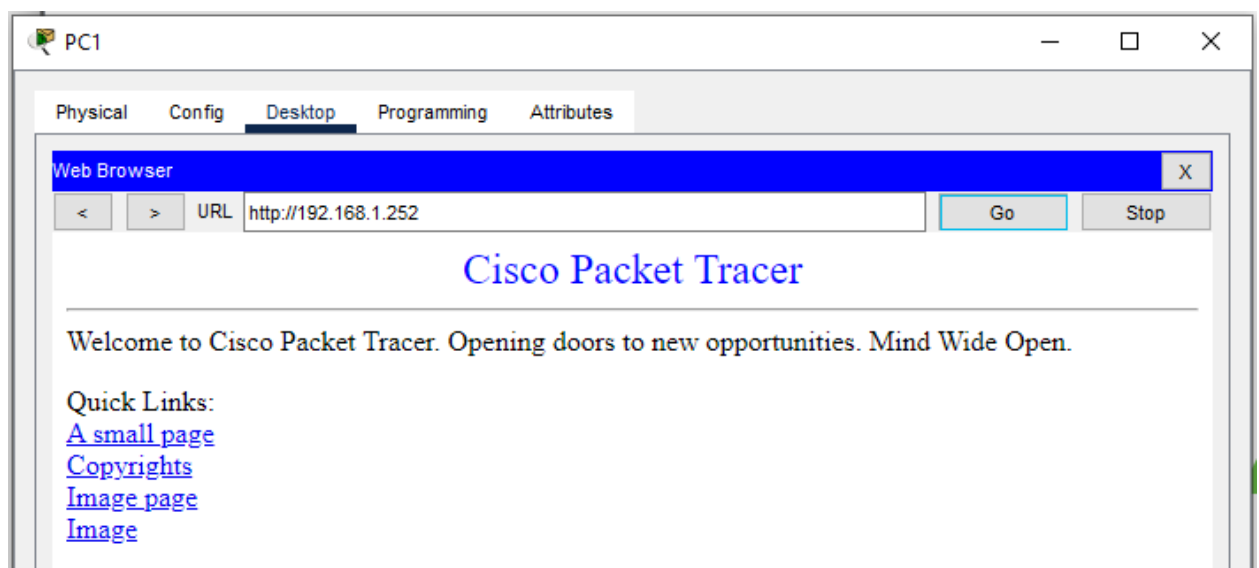
- Name: scs.kpi.ua — Доменне ім'я, на яке дається відповідь.
- Type: 1 — Відповідь для IPv4-адреси (А-запис).
- Class: 1 — Інтернет (IN).
- TTL: 86400 — Час життя запису (24 години).
- IP: 192.168.1.252 — Відповідна IP-адреса для доменного імені.

Роль DNS-відповіді

Ця відповідь дозволяє клієнту використовувати отриману IP-адресу (192.168.1.252) для доступу до ресурсу scs.kpi.ua. Це ключовий етап у механізмі DNS, який забезпечує перетворення доменних імен в IP-адреси для подальшого встановлення з'єднань.

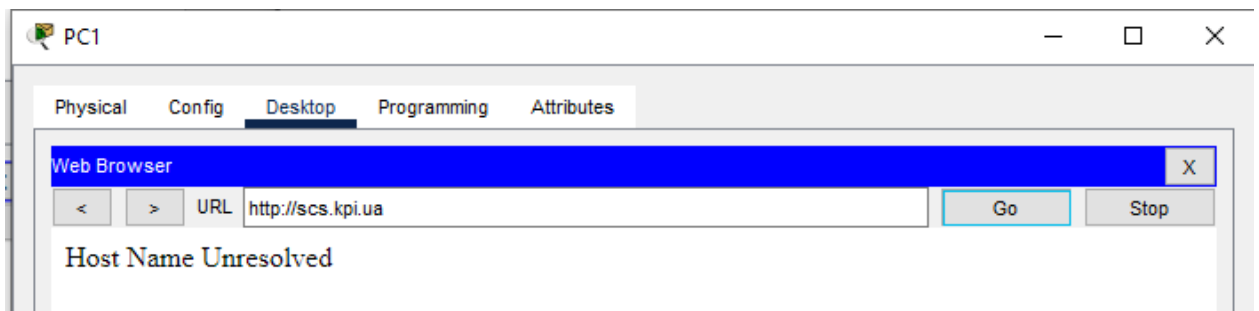
9. Перейти в режим «Real Time».

10. У налаштуваннях DNS-сервера відключити DNS-сервіс. У полі URL веб-браузера на PC1 набрати IP-адресу HTTP-сервера. Зафіксувати результат. Замість IP-адреси HTTP-сервера набрати його DNS-ім'я. Пояснити отриманий результат. Не закриваючи вікна веб-браузера включити DNS-сервіс. Зафіксувати зміни, що відбулися.

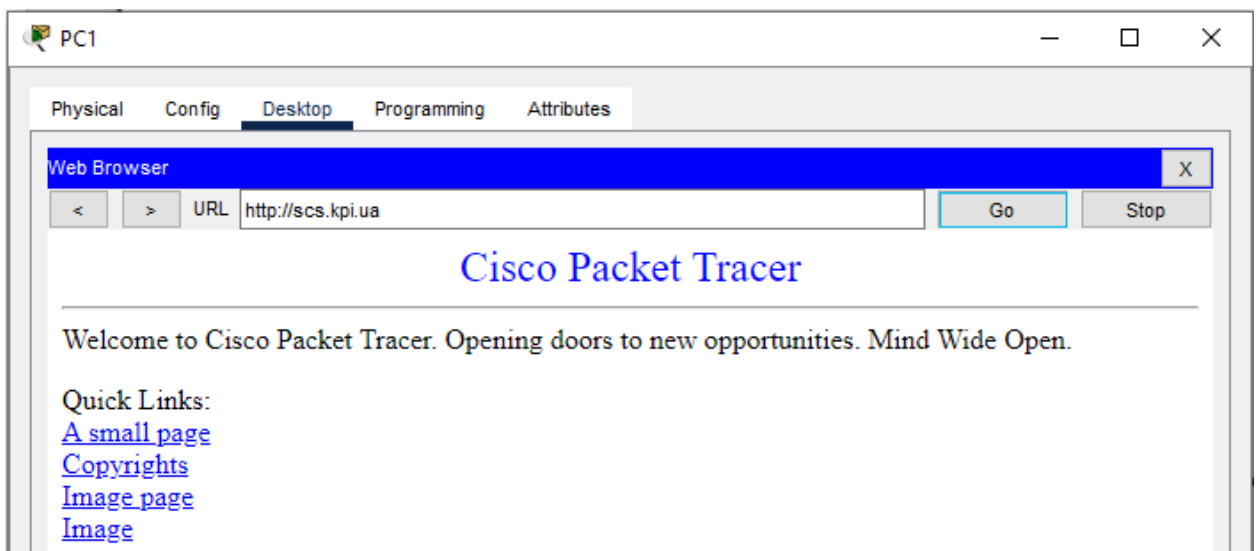


Браузер відкриє веб-сторінку HTTP-сервера, оскільки IP-адреса не потребує DNS-розв'язання. Це демонструє, що DNS є необов'язковим, якщо клієнт

знає IP-адресу.



Веб-сторінка не відкриється, оскільки відсутній DNS-сервіс для перетворення доменного імені на IP-адресу.



Веб-сторінка завантажиться успішно, оскільки DNS-сервіс тепер працює й клієнт отримує правильну IP-адресу для доменного імені.

Завдання №5. Ознайомлення з відомостями про структуру перехресного кабеля.

Кабель типу «вита пара» є основою для побудови Ethernet-мереж, які використовуються для з'єднання різних мережевих пристроїв. Його популярність пояснюється простотою використання, доступністю та ефективністю в передачі даних. У цьому есе ми розглянемо особливості використання перехресного кабелю, його роль у мережевих технологіях і принципи створення.

Вита пара складається з кількох ізольованих провідників, які скручені

попарно для зменшення електромагнітних завад. Це рішення дозволяє забезпечити надійну передачу сигналів, навіть у середовищах з високим рівнем завад. Кабелі поділяються на екрановані (STP, FTP) та неекрановані (UTP). Екрановані кабелі використовуються у складних умовах, тоді як неекрановані, через їхню гнучкість і простоту використання, підходять для офісних приміщень.

Однією з ключових характеристик кабелю є його обтискання, тобто порядок з'єднання проводів у роз'ємах RJ-45. Існує два основні стандарти обтискання – T568A та T568B, які визначають послідовність кольорових проводів. Ці стандарти дозволяють створювати два типи кабелів: прямий і перехресний.

Прямий і перехресний кабель

Прямий кабель має однаковий порядок обтискання на обох кінцях (T568A–T568A або T568B–T568B) і використовується для з'єднання пристроїв різних рівнів моделі OSI, наприклад, комп'ютера з комутатором. У перехресному кабелі один кінець обтиснутий за стандартом T568A, а інший — за T568B. Цей кабель дозволяє з'єднувати пристрої одного рівня моделі OSI, наприклад, дві робочі станції або два комутатори.

Головна мета перехресного кабелю — забезпечити передачу сигналів з контактів TX (передача) одного пристрою на контакти RX (прийом) іншого. Це досягається через «перехрещення» провідників, яке синхронізує логічні сигнали між пристроями.

Автоматизація з Auto MDI/MDI-X

Із розвитком технологій більшість сучасного мережевого обладнання підтримує функцію **Auto MDI/MDI-X**. Вона дозволяє пристроям автоматично налаштовуватися під пряме чи перехресне з'єднання, незалежно від типу кабелю. Це зменшує необхідність використання перехресного кабелю в реальних мережах. Однак у навчальних цілях, зокрема в програмі **Cisco Packet Tracer**, традиція використання перехресного кабелю для однотипного обладнання залишається актуальною.

Процес створення перехресного кабелю

Для виготовлення перехресного кабелю потрібно:

1. Один кінець кабелю обтиснути за стандартом **T568A**.
2. Інший кінець обтиснути за стандартом **T568B**. Це забезпечить правильне «перехрещення» сигналів для передачі та прийому.

На практиці кабель використовується для з'єднання двох комп'ютерів або комутаторів. У програмі Cisco Packet Tracer це дозволяє симулювати роботу однотипного обладнання.

Висновок:

Лабораторна робота №6 дала змогу не лише закріпити теоретичні знання, а й отримати практичний досвід роботи з основними механізмами функціонування комп'ютерних мереж, зокрема принципами перетворення DNS-імен в IP-адреси.

У ході виконання роботи я наочно побачила, як базові протоколи взаємодіють між собою в рамках моделі OSI, а саме на мережевому та канальному рівнях. Особливо цікавим було спостерігати, як за допомогою протоколу ARP відбувається визначення MAC-адрес для встановлення з'єднання між пристроями. Цей процес, що на перший погляд здається непомітним для кінцевого користувача, є фундаментально важливим для функціонування локальних мереж.

Динамічне призначення IP-адрес за допомогою DHCP-сервера продемонструвало ефективність автоматизації управління мережевими ресурсами. Це ще раз підкреслило важливість грамотного налаштування мережі, що дозволяє уникати конфліктів адрес та зменшувати кількість ручної роботи адміністратора. Спостерігаючи за взаємодією DHCP-сервера і клієнта, вдалося зрозуміти чотири основні етапи DORA (Discover, Offer, Request, Acknowledge), які забезпечують процес оренди адреси.

Окремим відкриттям стало розуміння ролі DNS у повсякденному житті користувачів. Виконання DNS-запиту продемонструвало, як доменні імена, що є зручними для людини, перетворюються на IP-адреси, зрозумілі

комп'ютерам. Процес перетворення є швидким і непомітним, але водночас базується на складній і багаторівневій взаємодії серверів та клієнтів.

Ця робота допомогла усвідомити, наскільки важливою є синергія між різними рівнями та протоколами мережі. Простий процес передачі даних, як-от ping або доступ до веб-сайту, є результатом злагодженої роботи десятків механізмів, від фізичного з'єднання до абстрактних протоколів.