ლექცია 11

ქსელური ბრმანებები დისკურ ოპერაციულ სისტემაში. Tracer, nslookup, Net user, ipconfig, Netstat, Getmac, arp, net view, route print, hostname.

ბრძანებების დანიშნულება

შესავალი

MS-DOS (Microsoft Disk Operation System) იყო Microsoft-ის მიერ შექმნილი ოპერაციული სისტემა, რომელიც ფართოდ გამოიყენებოდა 1980-იან და 1990-იან წლებში. ეს იყო ბრძანებების ხაზის ინტერფეისისი ოპერაციული სისტემა, რაც გულისმობს რომ მომხმარებელი ინტერაქციას ახდენდა საჭირო ბრძანებების შეწყანის მეშვეობით.

უშვალოთ ქსელური მიმართულებით, MS-DOS უზრუნველყოფს ბრძანებათა მთელ რიგს ქსელური ამოცანების შესასრულებლად. ქსელური ბრძანებები გვეხმარება: ქსელური კონფიგურაციის შემოწმებაში; დაკავშირების პრობლემის გამოსწორებაში (თრაბელშუთინგი); ქსელური რესურსების მართვაში.

მართალია თვითონ MS-DOS საკმაოდ მოძველებულია, მაგრამ მისმა ზოგიერთმა ბრძანებაბ დღემდე მოაღწია, გაუნჯობესდა და ხელმისაწვდომია თანამედროვე ვინდოუს ოპერაციულ სისტემაში.

ქსელური ბრძანებები

ქსელური ბრძანებები წარმოადგენს აუცილებელ ინსტრუმენტს ქსელური კავშირების მართვისა და თრაბელშუთინგისთვის.

მნიშვბელოვანი ქსელური ბრძანებებია

- Tracer წარმოადგენს ქსელურ უტილიტას, რომელიც აღნუსხავს გზას, რომელასც მონაცემთა პაკეტი გაივლის ინტერნეტში: ჩვენი კომპიუტერიდან დანიშნულების ადგილამდე
- Nslookup არის ბრძანებათა ხაზის ხელსაწყო, რომელიც ახდენს DNS ქუერინგს.
- Net user ბრქანებების ხაზის ხელსაყწო, რომელიც გამოიყენება მომხამრებეთა ანგარიშების სამართავად
- Ipconfig არის ქსელური უტილიტა ვინდოუსში, რომელიც გამოსახავს ყველა მიმდინარე TCP/IP ქსელური/კონფიგურაციის მნიშვნელობას და არეფრეშეფს DHCP და DNS პარამეტრებს
- Netstat /- არის მრავლისმომცველი ქსელური დიაგნოსტირების ხელსაწყო, რომელიც გვაწვდის დეტალურ
 ინფორმაციას: ქსელური კავშირების, მოსასმენი პორტების (listening ports), მარშრუტირების
 ცხრილებისა(routing tables) და მოწყობილობისა თუ კომპიუტერის სხვა ქსელური სტატისტიკის შესახებ
- → Getmac გამოსახავს ყველა ქსელური ადაპტერის MAC მისამართებს
- Arp გამოიყენება კომპიუტერში ARP ქეშის სანახავად და მანიპულირებისთვის; ასევე ქსელური კავშირის პრობლემის მოსაგვარებლად
- net view მიმდინარე დომეინში თუ სამუშაო ჯგუფში კოპიუტერებისა და გაზიარებული რესურსების სიას გამოსახავს
- route print გამოსახავს მიმდინარე კომპიუტერის მარშრუტირების ცხრილს (routing table)
- Hostname მიმდინარე კომპიუტერის ჰოსტს სახელს გამოსახავს

Tracer ბრძანება

Tracert არის ქსელური დიაგნოსტირების ხელსაწყო, რომელიც გამოსახავს გზას, რომელსაც დანიშნულების ადგილამდე მისასველად ამ კომპიუტერიდან გაგზავნილი პაკეტი გაივლის. ამისთვის იგი ICMP ექო მოთხოვნას უგზავნის სამიზნე მოწყობილობას. ამ მოთხოვნებს გააჩნიათ TTL – Time-To-Live მნიშვნელობა, რომელსაც თავდაპიველად აქვს მინიჭებული მაღალი რიცხვი (მაგალითად 128) და ყოველ ჯერზე, როდესაც როუტერი იღებს ამ მოთხოვნას, ერთით ამცირებს TTL მნიშვნელობას და საჭიროებისამებრ ამისამართებს სხვა როუტერთან. თუკი TTL მნიშვნელობა იქამდე გახდება 0-ის ტოლი, სანამ სამიზნე მოწყობილობას მიაღწვს, მაშინ როუტერი უგზავნის ICMP time exceeded (დრის გადაჭარბება) შეტყობინებას თავდაპირველ გამგზავნ კომპიუტერს.

Tracert ბრძანება გამოსახავს თითოეული განვლილი როუტერის IP მისამართს.

ეს ბრძანება გამოყებეას ჰპოვებს ქსელური პრობლემების აღმოსაფხვრელად, როგორიცაა ნელი კავშირის სიჩქარე და პაკეტთა დაკარგვა. როდესაც მოხდება პრობლემის გამომწვევი როუტერების იდენტიფიცირება, შესაძლებლობა გვექნება დავუკავშირდეთ ჩვენ ინტერნეტ სერვის პროვაიდერსა თუ ქსელის ადმინისტრატორს ამ პრობლემის მოსაგავრებლად.

Tracer ბრძანების პარამეტრები

პარამ	მეტრი	აღწერა	
/? -d -h		დეტალური დახმარების გამოტანა ამ ბრძანებასა და მის ოფციებზე	
		ბრძანება აღარ ახდენს IP მისამართისა და ჰოსტის დასახელების მეფინგს, რაც შედეგის უფრო სწრაფ მიღებას უზრუნველყოფს	
		აფიქსირებს ჰოფების მაქსიმალურ რაოდენობას. ნაგულისხმევი მნიშვნელობაა 30	
ب	W	თითოეული როუტერისთვის დალოდების დრო. ნაგულისხმევი მნიშვნელობაა 3000 მილიწამი (3 წამი)	
targe	t_host	სამიზნე ჰოსტი სახელი ან IP მისამართი	

Tracer ბრძანების გამოყენების მაგალითები

Tracert /? გაშვებით ხდება დეტალური დახმარების გამოტანა ამ ბრძანებასა და მის ოფციებზე

```
Command Prompt
C:\Users\Ekaterine>tracert /?
Usage: tracert [-d] [-h maximum hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target name
Options:
                      Do not resolve addresses to hostnames.
    -d
   -h maximum hops
                      Maximum number of hops to search for target.
   -i host-list
                      Loose source route along host-list (IPv4-only).
   -w timeout
                      Wait timeout milliseconds for each reply.
                      Trace round-trip path (IPv6-only).
    -R
   -S srcaddr
                      Source address to use (IPv6-only).
                      Force using IPv4.
                      Force using IPv6.
C:\Users\Ekaterine>
```

Tracer ბრძანების გამოყენების მაგალითები

Tracert google.com გაშვებით ხდება სახლის კომპიუტერიდან გუგლამდე ჰაკეტის მიერ განვლილი გზის დემონსტრირება.

```
×
Command Prompt
                                                                                    Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Ekaterine>tracert google.com
Tracing route to google.com [142.250.184.142]
over a maximum of 30 hops:
                        <1 ms DeviceDHCP.Home [192.168.1.1]</pre>
               <1 ms
                3 ms
                         3 ms 100.91.0.1
       4 ms
                         4 ms 100.127.255.2
       3 ms
                3 ms
                         3 ms host-213-157-192-125.customer.magticom.ge [213.157.192.125]
       3 ms
                3 ms
                        3 ms host-213-157-192-49.customer.magticom.ge [213.157.192.49]
       3 ms
                3 ms
               30 ms
                        28 ms 84.44.20.157
      29 ms
                        28 ms ae4-17-ucr1.tuz.cw.net [195.2.23.129]
      28 ms
               28 ms
                        29 ms ae2-xcr1.ise.cw.net [195.2.18.213]
      30 ms
               31 ms
      41 ms
               41 ms
                        41 ms ae29-xcr1.sof.cw.net [195.2.18.210]
      41 ms
               41 ms
                        40 ms google-gw.sof.cw.net [195.2.14.106]
11
                        45 ms 108,170,250,177
      45 ms
               45 ms
                        41 ms 142.250.212.23
12
      41 ms
               41 ms
     360 ms
                       151 ms sof02s43-in-f14.1e100.net [142.250.184.142]
              109 ms
Trace complete.
C:\Users\Ekaterine>
```

Tracer გრძანების გამოყენების მაგალითები

Tracert 8.8.8.8 გაშვებითაც ხდება სახლის კომპიუტერიდან გუგლამდე ჰაკეტის მიერ განვლილი გზის დემონსტრირება. წინა მაგალითისგან განსხვავებით აქ ვიყენებთ ლოგიკური მისამართს

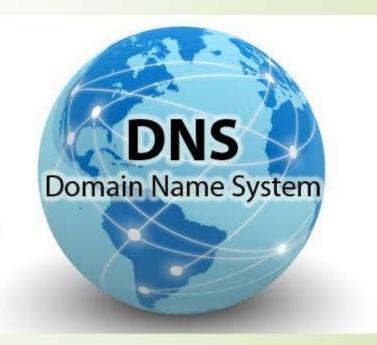
```
Command Prompt
C:\Users\Ekaterine>tracert 8.8.8.8
Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:
                        1 ms DeviceDHCP.Home [192.168.1.1]
                        9 ms 100.91.0.1
       4 ms
                6 ms
                       12 ms 100.127.255.2
       4 ms
                6 ms
                        5 ms host-213-157-192-125.customer.magticom.ge [213.157.192.125]
       4 ms
                3 ms
                        3 ms host-213-157-192-49.customer.magticom.ge [213.157.192.49]
       6 ms
                3 ms
                       29 ms 84.44.20.157
      29 ms
               30 ms
                       28 ms ae4-17-ucr1.tuz.cw.net [195.2.23.129]
      28 ms
               28 ms
               32 ms
                       30 ms ae2-xcr1.ise.cw.net [195.2.18.213]
      30 ms
                       46 ms ae29-xcr1.sof.cw.net [195.2.18.210]
      46 ms
               48 ms
      46 ms
               45 ms
                       46 ms 72.14.218.54
11
      48 ms
               55 ms
                       51 ms 216.239.59.239
12
               45 ms
                       45 ms 142.250.212.21
      46 ms
13
                       45 ms dns.google [8.8.8.8]
      45 ms
               46 ms
Trace complete.
C:\Users\Ekaterine>
```

nslookup ბრძანება

Nslookup არის ბრძანებათა ხაზის ხელსაწყო, რომელიც ახდენს DNS ქუერინგს. მისი მეშვეობით შეგვძლია IP მისამართსითვის შესაბამისი დომეინის გაგება და დომეინის მიხედვით IP-ს გაგება.

DNS – Domain Name System დომენური სახელების სისტემა პასუხისმგებელია ადამიანისთვის გასაგები დომენური სახელის (მაგალითად google.com) მანქანისთვის გასაგებ IP მისამართად(142.250.187.142) გადათარგმნაზე.

როდესაც ბრაუზერში ვკრეფთ დომეინს, ჩვენი კომპიუტერი უგზავნის ქუერის DNS სერვერს.
DNS სერვერს ემებს ამ დომენური სახელისთვის მის შესაბამის IP მისამართს და პასუხად უბრუნებს ჩვენს კომპიუტერს.
ჩვენი კომპიუტერ იყენებს ამ IP მისამართს რათა დაუკავშირდეს ვებსაიტს.



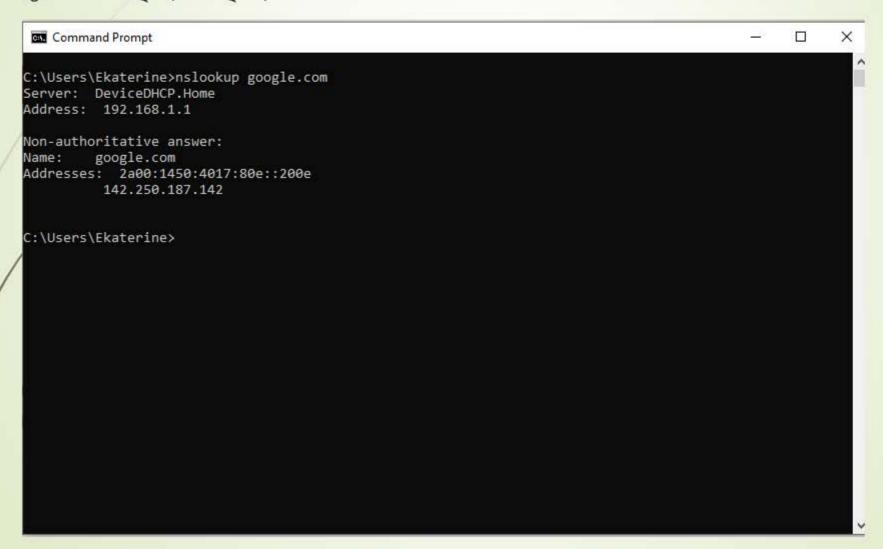
Nslookup ბრძანების გამოყენების მაგალითები

Nslookup 8.8.8.8 გაშვებით მოვახდინეთ IP მისამართი 8,8.8.8-ს დომეინის გაგება

```
×
Command Prompt
C:\Users\Ekaterine>nslookup 8.8.8.8
Server: DeviceDHCP.Home
Address: 192.168.1.1
        dns.google
Address: 8.8.8.8
C:\Users\Ekaterine>_
```

Nslookup ბრძანების გამოყენების მაგალითები

Nslookup google.com გაშვებით მოვახდინეთ google.com-ის IP მისამართის გაგება შესაბამისად: Ipv4 და Ipv6-ში



Net user ბრძანება

Net user არის ბრძანებების ხაზის ხელსაყწო, რომელიც გამოიყენება მომხამრებეთა ანგარიშების სამართავად.

ის გამოიყენება:

- 1) მომხმარებელთა სიის საწახავად net user
- 2) ახალი მომხმარებლის დასამატებლად net user some username mypassword /add
- 3) მომხამრებლის წასაშლელად net user someusername /delete
- 4) მომხამრებლისთვის პაროლის შესაცვლელად net user someusername newpassowrd
- 5) მომხამრებლისთვის პაროლის შესაცვლის ნების დართვა ან არ დართვა შესაბამისად:

net user some username / passwordchg: yes

net user some username /passwordchg:no

ასევე მას აქვს მრავალი სხვა გამოყენება

Net user /? გაშვებით გამოჩნდება ამ ბრძანების სინტაქსი და რამდენიმა ოფცია

```
X
 Command Prompt
C:\Users\Ekaterine>net user /?
The syntax of this command is:
NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]
         username [/ACTIVE: {YES | NO}]
C:\Users\Ekaterine>_
```

Net user გაშვებით გამოჩნდება ამ სისტემაში არსებული მომხმარებლების სია

```
Command Prompt
                                                                                                            ×
C:\Users\student>net user
User accounts for \\BTU407-12
Administrator cthulhu
                                   DefaultAccount
Guest
                       WDAGUtilityAccount
The command completed successfully.
C:\Users\student>net user /?
The syntax of this command is:
NET USER
[username [password | *] [options]] [/DOMAIN]
        username {password | *} /ADD [options] [/DOMAIN]
        username [/DELETE] [/DOMAIN]
        username [/TIMES:{times | ALL}]
        username [/ACTIVE: {YES | NO}]
C:\Users\student>_
```

lpconfig ბრძანება

Ipconfig ბრძანება არის ქსელური უტილიტა ვინდოუსში, რომელიც გამოსახავს ყველა მიმდინარე TCP/IP ქსელური კონფიგურაციის მნიშვნელობას და არეფრეშეფს DHCP და DNS პარამეტრებს

ეს ბრმანება გამოიყენება IP მისამართების, ქვექსელის ნიღაბის (subnet mask)და სხვა ქსელის კარიბჭის სანახავდ (default gateway) ყველა ქსელური ადაპტერისთვის. ასევე გამოიყენება IP მისამართებისა და DNS ქეშის სანახავად.

IP (Internet Protocol) მისამართი - არის მოწყობილობისთვის მინიჭებული ლოგიკური მისამართი. მისი დანიშნულებაა, რომ მოწყობილილობების იდენტიფიცირება მოხდეს ინტერნეტში. ლოგიკური მისამართების მინიჭების 2 გზა არსებობს:

- დინამიური DHCP სერვერის მიერ
- სტატიკური, თუკი მოწყობილობას ხელით გავუწერთ IP-ს

ლოგიკური მისამართები გვეხმარება, რომ სხვადასხვა ქსელებში მყოფმა მოწყობილობება შეძლონ დაკავშირება

lpconfig ბრძანების გამოყენების მაგალითები

```
Command Prompt
C:\Users\student>ipconfig /?
   ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]
where
   adapter
                        Connection name
                       (wildcard characters * and ? allowed, see examples)
   Options:
       13
                        Display this help message
       /a11
                        Display full configuration information.
       /release
                        Release the IPv4 address for the specified adapter.
       /release6
                        Release the IPv6 address for the specified adapter.
       /renew
                        Renew the IPv4 address for the specified adapter.
       /renew6
                        Renew the IPv6 address for the specified adapter.
       /flushdns
                        Purges the DNS Resolver cache.
       /registerdns
                        Refreshes all DHCP leases and re-registers DNS names
       /displaydns
                        Display the contents of the DNS Resolver Cache.
      /showclassid
                        Displays all the dhcp class IDs allowed for adapter.
       /setclassid
                        Modifies the dhcp class id.
       /showclassid6
                        Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6
                        Modifies the IPv6 DHCP class id.
The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.
For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.
For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.
Examples:
   > ipconfig
                                     ... Show information
   > ipconfig /all
                                     ... Show detailed information
   > ipconfig /renew
                                     ... renew all adapters
   > ipconfig /renew EL*
                                     ... renew any connection that has its
                                         name starting with EL
   > ipconfig /release *Con*
                                     ... release all matching connections,
                                         eg. "Wired Ethernet Connection 1" or
                                             "Wired Ethernet Connection 2"
   > ipconfig /allcompartments
                                     ... Show information about all
                                         compartments
   > ipconfig /allcompartments /all ... Show detailed information about all
```

Ipconfig /? გაშვებით გამოგვიჩნდება ამ ბრძანების აღწერა, ოფციები და გამოყენების მაგალითები

lpconfig ბრძანების გამოყენების მაგალითები

```
Command Prompt
                                                                                                          C:\Users\student>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 2:
  Media State . . . . . . . . . . . . Media disconnected
  Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 11:
  Media State . . . . . . . . . . . . Media disconnected
  Connection-specific DNS Suffix .:
Wireless LAN adapter Local Area Connection* 12:
  Media State . . . . . . . . . . . . Media disconnected
  Connection-specific DNS Suffix .:
Wireless LAN adapter Wi-Fi 2:
  Connection-specific DNS Suffix .:
  Link-local IPv6 Address . . . . : fe80::119f:a569:5b55:9292%22
  IPv4 Address. . . . . . . . . . . . . 192.168.30.41
  Default Gateway . . . . . . . . . . . . 192.168.30.1
Ethernet adapter Bluetooth Network Connection 2:
  Media State . . . . . . . . . . . . Media disconnected
  Connection-specific DNS Suffix .:
C:\Users\student>_
```

Ipconfig გაშვებით გამოგვიჩნდება გამოიყენება Ip მისამართები, ქვექსელის ნიღაბი (subnet mask)და სხვა ქსელის კარიბჭე (default gateway) ყველა ქსელური ადაპტერისთვის

lpconfig ზრძანების გამოყენების მაგალითები

```
Command Prompt
C:\Users\student>ipconfig /all
Windows IP Configuration
  Host Name . . . . . . . . . . . . . . . BTU201-1
  Primary Dns Suffix . . . . . . : BTU.local
  IP Routing Enabled. . . . . . . : No
  WINS Proxy Enabled. . . . . . . : No
  DNS Suffix Search List RTU local
Ethernet adapter Ethernet 2:
  Media State . . . . . . . . . . . . . Media disconnected
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . : Realtek PCIe GbE Family Controller #2
  Physical Address. . . . . . . : 00-25-AB-96-81-8B
  DHCP Enabled. . . . . . . . . . . Yes
  Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Local Area Connection* 11:
  Media State . . . . . . . . . . . . Media disconnected
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . . Microsoft Wi-Fi Direct Virtual Adapter #3
  DHCP Enabled. . . . . . . . . . . . Yes
  Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Local Area Connection* 12:
  Media State . . . . . . . . . . . . Media disconnected
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . . Microsoft Wi-Fi Direct Virtual Adapter #4
  DHCP Enabled. . . . . . . . . . . Yes
  Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Wi-Fi 2:
```

```
Description . . . . . . . . . . . . . . Microsoft Wi-Fi Direct Virtual Adapter #4
 DHCP Enabled. . . . . . . . . . Yes
 Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Wi-Fi 2:
 Connection-specific DNS Suffix .:
 Description . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
 Physical Address. . . . . . . : A4-02-B9-68-9D-42
 DHCP Enabled. . . . . . . . . . . Yes
 Autoconfiguration Enabled . . . . : Yes
 Link-local IPv6 Address . . . . : fe80::119f:a569:5b55:9292%22(Preferred)
 IPv4 Address. . . . . . . . . . . . . . . . 192.168.30.41(Preferred)
 Lease Obtained. . . . . . . . . . Tuesday. November 28, 2023 12:51:18
 Lease Expires . . . . . . . . . . Tuesday, November 28, 2023 13:06:18
 Default Gateway . . . . . . . : 192.168.30.1
 DHCPv6 Client DUID. . . . . . . : 00-01-00-01-2A-AD-54-EA-E4-A8-DF-92-02-87
 DNS Servers . . . . . . . . . . . . . . . . 172.20.0.152
 NetBIOS over Tcpip. . . . . . : Enabled
thernet adapter Bluetooth Network Connection 2:
 Media State . . . . . . . . . . . . . Media disconnected
 Connection-specific DNS Suffix .:
 Description . . . . . . . . . . Bluetooth Device (Personal Area Network) #2
 DHCP Enabled. . . . . . . . . . Yes
 Autoconfiguration Enabled . . . . : Yes
:\Users\student>_
```

Ipconfig /all გაშვებით ყველა ქსელურ ადაპტერზე უფრო დეტალური ინფორმაცია გამოგვიჩნდება

netstat ბრძანება

Netstat არის მრავლისმომცველი ქსელური დიაგნოსტირების ხელსაწყო, რომელიც გვაწვდის დეტალურ ინფორმაციას: ქსელური კავშირების, მოსასმენი პორტების (listening ports), მარშრუტირების ცხრილებისა(routing tables) და მოწყობილობისა თუ კომპიუტერის სხვა ქსელური სტატისტიკის შესახებ.

ეს არის ბრმანებათა ხაზის უტილიტა, რომელიც ხელმისაწვდომია უმეტეს ოპერაციულ სისტემებში, მათ შორის: Windows, Linux და MacOS.

/ამ ბრძანებას აქვს პრაქტიკაში ხშირად გამოყენებადი ბევრი მნიშვნელოვანი ოფცია. განვიხილოთ რამდენიმე მათგანი

netstat გრმანების გამოყენების მაგალითები

```
Command Prompt
C:\Users\student>netstat /?
Displays protocol statistics and current TCP/IP network connections.
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]
               Displays all connections and listening ports.
 -b
               Displays the executable involved in creating each connection or
               listening port. In some cases well-known executables host
               multiple independent components, and in these cases the
               sequence of components involved in creating the connection
               or listening port is displayed. In this case the executable
               name is in [] at the bottom, on top is the component it called.
               and so forth until TCP/IP was reached. Note that this option
               can be time-consuming and will fail unless you have sufficient
               permissions.
               Displays Ethernet statistics. This may be combined with the -s
               option.
  -f
               Displays Fully Qualified Domain Names (FODN) for foreign
               addresses.
               Displays addresses and port numbers in numerical form.
  -n
               Displays the owning process ID associated with each connection.
  -0
               Shows connections for the protocol specified by proto; proto
  -p proto
               may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
               option to display per-protocol statistics, proto may be any of:
               IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
               Displays all connections, listening ports, and bound
  -q
               nonlistening TCP ports. Bound nonlistening ports may or may not
               be associated with an active connection.
               Displays the routing table.
               Displays per-protocol statistics. By default, statistics are
               shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
               the -p option may be used to specify a subset of the default.
               Displays the current connection offload state.
  -t
               Displays NetworkDirect connections, listeners, and shared
               endpoints.
  -y
               Displays the TCP connection template for all connections.
               Cannot be combined with the other options.
 interval
               Redisplays selected statistics, pausing interval seconds
               between each display. Press CTRL+C to stop redisplaying
               statistics. If omitted, netstat will print the current
               configuration information once.
```

C:\Users\student>

netstat /?
გაშვებით
გამოგვიჩნდება
ამ
ბრძანების
აღწერა და
ოფციები

netstat ზრმანების გამოყენების მაგალითები

Command Prompt

C:\Users\student>netstat

Active Connections

C:\Users\student>

Proto	Local Address	Foreign Address	State
TCP	192.168.30.41:53695	20.199.120.85:https	ESTABLISHED
TCP	192.168.30.41:53872	wl-in-f188:5228	ESTABLISHED
TCP	192.168.30.41:54560	bud02s35-in-f5:https	ESTABLISHED
TCP	192.168.30.41:54569	bud02s38-in-f10:https	TIME_WAIT
TCP	192.168.30.41:54572	eh-in-f102:https	ESTABLISHED
TCP	192.168.30.41:54576	bud02s39-in-f1:https	ESTABLISHED
TCP	192.168.30.41:54577	bud02s39-in-f1:https	ESTABLISHED
TCP	192.168.30.41:54578	bud02s39-in-f1:https	ESTABLISHED
TCP	192.168.30.41:54579	bud02s39-in-f1:https	ESTABLISHED
TCP	192.168.30.41:54580	bud02s33-in-f14:https	ESTABLISHED

netstat გაშვებით გამოგვიჩნდება აქტიური TCP კავშირების სია. ამ სიის თითოეული ჩანაწერი მოიცავს: Proto - ამ კავშირის ტრანსპორტირების პროტოკოლი; Local Address კავშირის ლიკალური IP მისმამართი და პროტი; Foreign Address - კავშირის მოშორებული IP მისმამართი და პროტი; State - მიმდინარე კავშირის სტატუსი/მდგომარეობა.

netstat ბრძანების გამოყენების მაგალითები

Netstat -a გაშვებით სიის სახით გამოგვიჩნდება ყველა აქტიური TCP კავშირი და UDP მომსმენი

პორტები.

```
Command Prompt
:\Users\student>netstat -a
Active Connections
 Proto Local Address
                                Foreign Address
                                                        State
        0.0.0.0:135
                                BTU201-1:0
                                                        LISTENING
 TCP
        0.0.0.0:445
                                BTU201-1:0
                                                        LISTENING
 TCP
        0.0.0.0:5040
                                BTU201-1:0
                                                        LISTENING
 TCP
        0.0.0.0:7680
                                RTU201-1:0
                                                        LISTENING
 TCP
        0.0.0.0:49664
                                BTU201-1:0
                                                        LISTENING
 TCP
        0.0.0.0:49665
                                                        LISTENING
                                BTU201-1:0
 TCP
        0.0.0.0:49666
                                BTU201-1:0
                                                        LISTENING
 TCP
        0.0.0.0:49667
                                BTU201-1:0
                                                        LISTENING
 TCP
        0.0.0.0:49668
                                BTU201-1:0
                                                        LISTENING
 TCP
                                                        LISTENING
        0.0.0.0:49669
                                BTU201-1:0
 TCP
        0.0.0.0:53691
                                BTU201-1:0
                                                        LISTENING
 TCP
        192.168.30.41:139
                                BTU201-1:0
                                                        LISTENING
 TCP
        192.168.30.41:53695
                                20.199.120.85:https
                                                        ESTABLISHED
 TCP
        192.168.30.41:53872
                                wl-in-f188:5228
                                                        ESTABLISHED
                                                        ESTABLISHED
 TCP
        192,168,30,41:54560
                                bud@2s35-in-f5:https
 TCP
        192,168,30,41:54572
                                eh-in-f102:https
                                                        TIME WAIT
 TCP
        192.168.30.41:54576
                                bud@2s39-in-f1:https
                                                        ESTABLISHED
 TCP
        192.168.30.41:54577
                                bud@2s39-in-f1:https
                                                        ESTABLISHED
 TCP
        192.168.30.41:54578
                                bud@2s39-in-f1:https
                                                        ESTABLISHED
 TCP
        192.168.30.41:54579
                                bud02s39-in-f1:https
                                                        ESTABLISHED
 TCP
        192.168.30.41:54580
                                bud02s33-in-f14:https
                                                        ESTABLISHED
 TCP
        192.168.30.41:54581
                                bud@2s38-in-f10:https
                                                       ESTABLISHED
 TCP
        192.168.30.41:64404
                                172.20.0.41:domain
                                                        TIME WAIT
 TCP
        192.168.30.41:64405
                                40.78.107.253:https
                                                        TIME WAIT
 TCP
        192.168.30.41:64406
                                104.46.162.226:https
                                                        TIME WAIT
 TCP
        192.168.30.41:64407
                                13.95.31.18:https
                                                        TIME WAIT
 TCP
        [::]:135
                                BTU201-1:0
                                                        LISTENING
         [::]:445
 TCP
                                                        LISTENING
                                BTU201-1:0
 TCP
         [::]:7680
                                BTU201-1:0
                                                        LISTENING
 TCP
         ::1:49664
                                BTU201-1:0
                                                        LISTENING
 TCP
         ::1:49665
                                BTU201-1:0
                                                        LISTENING
 TCP
         ::1:49666
                                BTU201-1:0
                                                        LISTENING
 TCP
         1::1:49667
                                BTU201-1:0
                                                        LISTENING
 TCP
         ::1:49668
                                BTU201-1:0
                                                        LISTENING
 TCP
         ::1:49669
                                BTU201-1:0
                                                        LISTENING
 TCP
         ::]:53691
                                                        LISTENING
                                BTU201-1:0
 TCP
         ::1]:42050
                                BTU201-1:0
                                                        LISTENING
 TCP
         [::1]:49670
                                BTU201-1:0
                                                        LISTENING
 UDP
        0.0.0.0:123
 UDP
        0.0.0.0:5050
        0.0.0.0:5353
```

```
Command Prompt
         192.168.30.41:64406
                                                            TIME WATT
 TCP
                                   104.46.162.226:https
 TCP
         192.168.30.41:64407
                                   13.95.31.18:https
                                                            TIME WAIT
 TCP
         [::1:135
                                  BTU201-1:0
                                                            LISTENING
 TCP
          1::1:445
                                  BTU201-1:0
                                                            LISTENING
 TCP
          ::1:7680
                                  BTU201-1:0
                                                            LISTENING
 TCP
          ::1:49664
                                  BTU201-1:0
                                                            LISTENING
 TCP
          ::1:49665
                                  BTU201-1:0
                                                            LISTENING
 TCP
          ::1:49666
                                  BTU201-1:0
                                                            LISTENING
 TCP
          ::1:49667
                                  BTU201-1:0
                                                            LISTENING
 TCP
          ::1:49668
                                  BTU201-1:0
                                                            LISTENING
 TCP
          ::1:49669
                                  BTU201-1:0
                                                            LISTENING
 TCP
          ::1:53691
                                  BTU201-1:0
                                                            LISTENING
 TCP
          [::1]:42050
                                  BTU201-1:0
                                                            LISTENING
 TCP
         [::1]:49670
                                  BTU201-1:0
                                                            LISTENING
                                   *:*
 UDP
         0.0.0.0:123
                                   *.*
 UDP
         0.0.0.0:5050
 UDP
         0.0.0.0:5353
                                   * . *
                                   * . *
 UDP
         0.0.0.0:5353
 UDP
         0.0.0.0:5353
 UDP
         0.0.0.0:5355
                                   * . *
 UDP
         0.0.0.0:49899
                                   *:*
 UDP
         0.0.0.0:53206
                                   * . *
 UDP
         0.0.0.0:53679
                                   *: *
 UDP
         0.0.0.0:55900
 UDP
         0.0.0.0:61045
                                   * - *
                                   *:*
 UDP
         127.0.0.1:1900
 UDP
         127.0.0.1:49664
                                   * : *
 UDP
         127.0.0.1:56057
                                   * * *
 UDP
         127.0.0.1:56060
                                   * * *
         127.0.0.1:58643
 UDP
                                   * *
 UDP
         127.0.0.1:60634
                                   * . *
 UDP
         192.168.30.41:137
                                   *:*
 UDP
         192.168.30.41:138
                                   * . *
 UDP
         192.168.30.41:1900
                                   * *
 UDP
                                   * . *
         192.168.30.41:60633
 UDP
         192.168.30.41:64391
 UDP
         [::1:123
                                   * . *
 UDP
          [::1:5353
 UDP
          1::1:5353
 UDP
          ::1:5355
 UDP
          ::11:1900
                                   * . *
 UDP
          ::11:60632
          fe80::119f:a569:5b55:9292%221:1900
 UDP
 UDP
          fe80::119f:a569:5b55:9292%22]:60631
C:\Users\student>_
```

netstat გრმანების გამოყენების მაგალითები

Netstat -e გაშვებით გამოისხება Ethernet სტატისტიკა, როგორიცაა გაგზავნილი და მიღებული ბაიტებისა და პაკეტების რაოდენობები.

Command Prompt				×
C:\Users\student>netsta Interface Statistics	at -e			
Interrace Statistics				
	Received	Sent		
Bytes	159097938	80856102		
Unicast packets	169716	152364		
Non-unicast packets	22266	2268		
Discards	0	0		
Errors	0	0		
Unknown protocols	0			
C:\Users\student>_				

getmac ბრძანება

ეს ბრძანება გამოსახავს ყველა ქსელური ადაპტერის MAC მისამართებს

MAC (Media Access Control) მისამართი წარმოადგენს ქსელური ინტერფეისის კონტროლერის (NIC) ან ქსელური ადაპტერის უნიკალურ იდენტიფიკატორს, რომელიც მინიჭებული აქვს მწარრმოებლის მიერ. მას ასევე მოიხსენიებენ როგორც ფიზიკურ მისამართს და მისი ცვლილება შეუძლებელია. გამოიყენება ლოკალურ ქსელში (მაგალითად სახლი ან ოფისი) მოწყობილობების იდენტიფიცირებისთვის.

ფიზიკური მისამართი ჩაიწრება შემდეგი სახით 4A:8C:5E:00:40:85



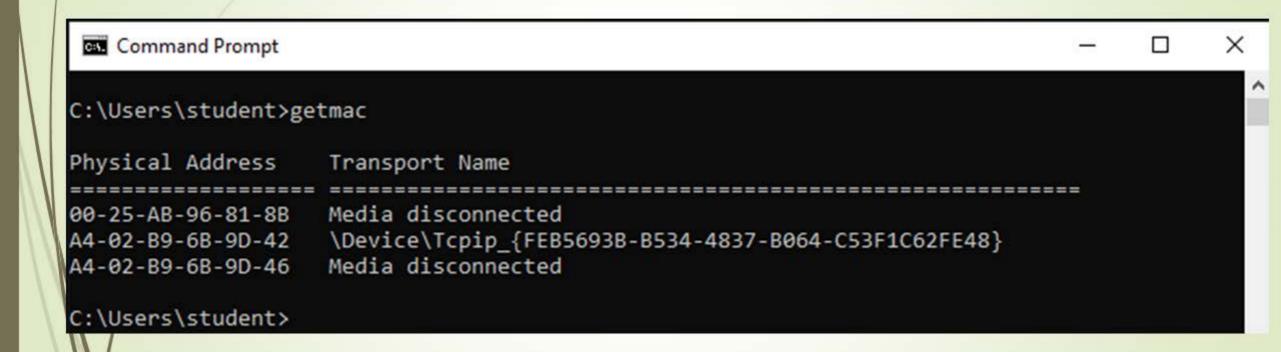
getmac გრძანების გამოყენების მაგალითები

getmac /? გაშვებით გამოგვიჩნდება ამ ბრძანების აღწერა, ოფციები და გამოყენების მაგალითები

```
×
Command Prompt
C:\Users\student>getmac /?
GETMAC [/S system [/U username [/P [password]]]] [/FO format] [/NH] [/V]
Description:
   This tool enables an administrator to display the MAC address
    for network adapters on a system.
Parameter List:
                             Specifies the remote system to connect to.
    15
           system
    /U
           [domain\]user
                             Specifies the user context under
                             which the command should execute.
           [password]
                             Specifies the password for the given
    /P
                             user context. Prompts for input if omitted.
    /FO
           format
                             Specifies the format in which the output
                             is to be displayed.
                             Valid values: "TABLE", "LIST", "CSV".
    /NH
                             Specifies that the "Column Header" should
                             not be displayed in the output.
                             Valid only for TABLE and CSV formats.
                             Specifies that verbose output is displayed.
    /V
    12
                             Displays this help message.
Examples:
   GETMAC /?
   GETMAC /FO CSV
   GETMAC /S system /NH /V
   GETMAC /S system /U user
   GETMAC /S system /U domain\user /P password /FO list /V
   GETMAC /S system /U domain\user /P password /FO table /NH
C:\Users\student>_
```

getmac გრძანების გამოყენების მაგალითები

getmac გაშვებით გამოგვიჩნდება ქსელური ადაპტერების ფიზიკური მდგომარეობის სია (Transport Name სვეტში) და მათი შესაბამისი MAC მისამართები (Physical Address სვეტში)

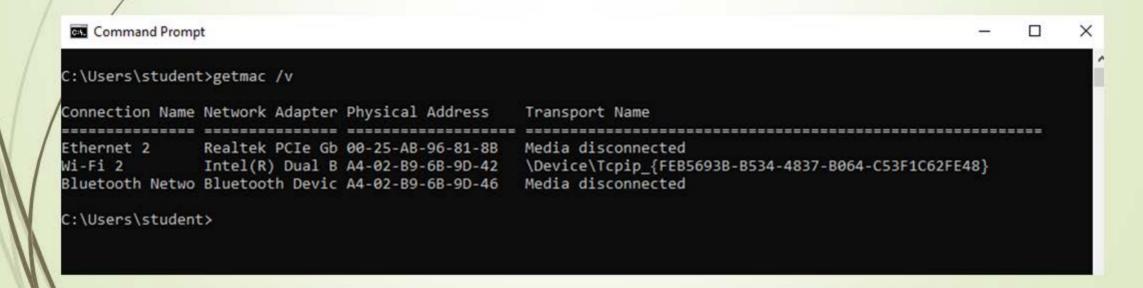


getmac ბრძანების გამოყენების მაგალითები

Getmac -v გაშვებით გამოგვიჩნდება:

- Connection Name კავშირის სახელი
- Network Adapter ქსელური ადაპტერი
- Physical Address შესაბამისი MAC მისამართები
- Transport Name ქსელური ადაპტერის ფიზიკური მდგომარეობა

 - / ოფციის გამოყენებით, წინა მაგალითთან შედარებით უფრო დეტალური ინფორაციის გამოტანაა შესაძლებელი



arp ბრძანება

ARP – Address Resolution Protocol არის ქსელური პროტოკოლი, რომელიც გამოიყენება IP მისამართებისა და MAC მისამართების მეფინგისთვის. ეს არის მწიშვნელოვანი კომპონენტი Ethernet და LAN ტექნოლოგიებში.

ARP ბრძანება არის ხელსაწყო, რომელიც გამოიყენება ARP ქეშის სამართავად. ARP ქეში არის ცხრილი, რომელიც ინახავს კავშირებს IP და MAC მისამართებს შორის. ეს ცხრილი ეფექტური ქსელური კომუნიკაციისთვის არის უაღრესად მნიშვნელოვანი, რადგანაც მოწყობილობებს საშუალებას აძლევს სწრაფად დაადგინონ ქსელში სხვა მოწყობილობის ფიზიკური მისამართი მთელ ქსელში broadcast ARP request-ის გაგზავნის გარეშე.

arp ბრძანების გამოყენების მაგალითები

```
C:\Users\student>arp /?
Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).
ARP -s inet addr eth addr [if addr]
ARP -d inet addr [if addr]
ARP -a [inet addr] [-N if addr] [-v]
               Displays current ARP entries by interrogating the current
  -a
               protocol data. If inet addr is specified, the IP and Physical
               addresses for only the specified computer are displayed. If
               more than one network interface uses ARP, entries for each ARP
               table are displayed.
               Same as -a.
  -g
               Displays current ARP entries in verbose mode. All invalid
               entries and entries on the loop-back interface will be shown.
  inet addr
               Specifies an internet address.
               Displays the ARP entries for the network interface specified
  -N if addr
               by if addr.
  -d
               Deletes the host specified by inet addr. inet addr may be
               wildcarded with * to delete all hosts.
               Adds the host and associates the Internet address inet addr
  -5
               with the Physical address eth addr. The Physical address is
               given as 6 hexadecimal bytes separated by hyphens. The entry
               is permanent.
               Specifies a physical address.
  eth addr
               If present, this specifies the Internet address of the
  if addr
               interface whose address translation table should be modified.
               If not present, the first applicable interface will be used.
Example:
  .... Displays the arp table.
  > arp -a
```

ამ ბრძანების აღწერილობის, ოფციებისა და მაგალითების ნახვა

arp ბრძანების გამოყენების მაგალითები

Command Prompt C:\Users\student>arp -a Interface: 192.168.30.41 --- 0x16 Internet Address Physical Address Type e8-1c-ba-ee-20-02 dynamic 192,168,30,1 192.168.30.255 ff-ff-ff-ff-ff static static 224.0.0.22 01-00-5e-00-00-16 01-00-5e-00-00-fb static 224.0.0.251 01-00-5e-00-00-fc 224.0.0.252 static static 239.255.255.250 01-00-5e-7f-ff-fa 255.255.255.255 ff-ff-ff-ff-ff static

C:\Users\student>_

Arp –a გაშვებით ხდება ARP ქეშის გამოტანა

აწალოგიურ შედეგს იძლევა ეს ბრძანება -g ოფციით

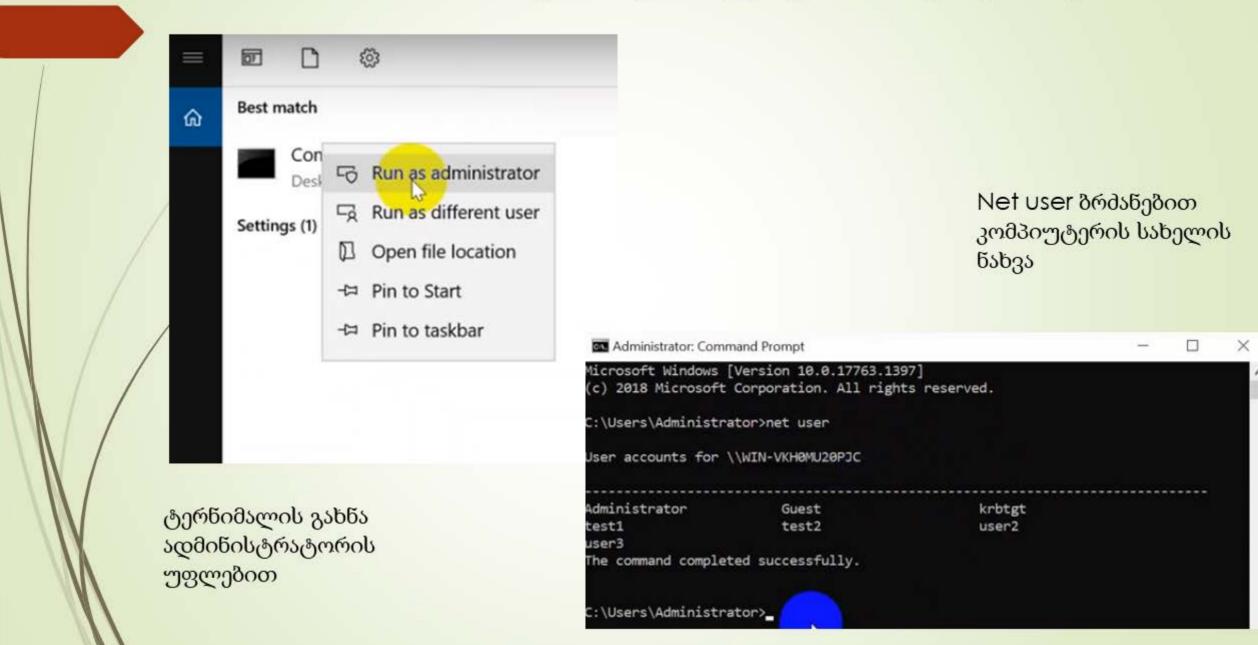
```
C:\Users\student>arp -g
Interface: 192.168.30.41 --- 0x16
 Internet Address
                      Physical Address
                                            Type
                       e8-1c-ba-ee-20-02
 192.168.30.1
                                            dynamic
                      ff-ff-ff-ff-ff
 192.168.30.255
                                            static
 224.0.0.22
                       01-00-5e-00-00-16
                                            static
 224.0.0.251
                       01-00-5e-00-00-fb
                                            static
                                            static
 224.0.0.252
                       01-00-5e-00-00-fc
 239.255.255.250
                       01-00-5e-7f-ff-fa
                                            static
                      ff-ff-ff-ff-ff
 255.255.255.255
                                            static
:\Users\student>_
```

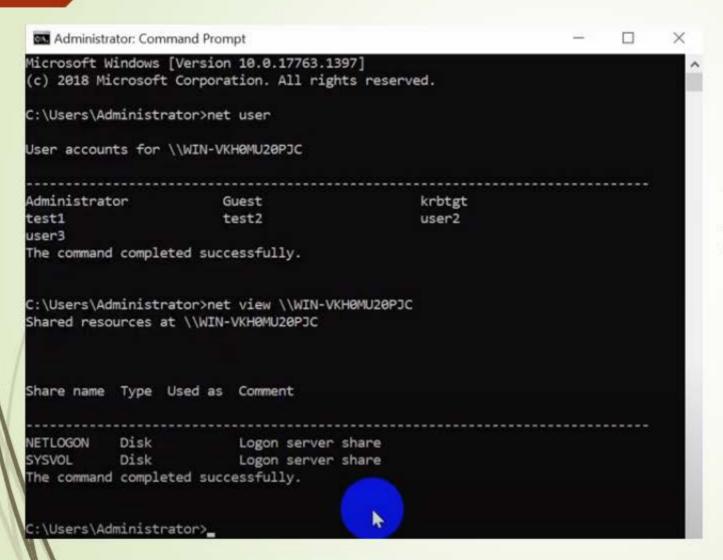
Net view ბრძანება

მიმდინარე დომეინში თუ სამუშაო ჯგუფში კოპიუტერებისა და გაზიარებული რესურსების სიას გამოსახავს

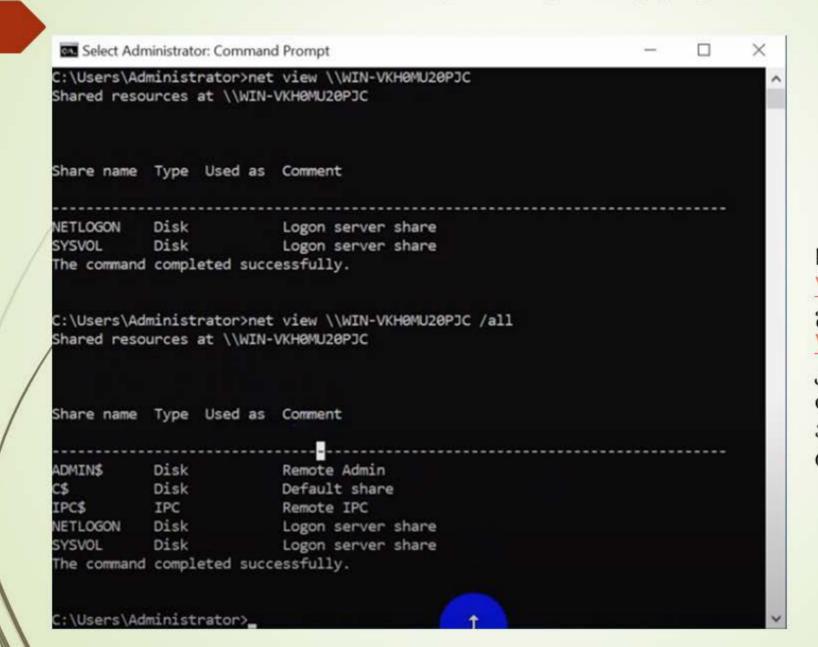
მის გამოსაყენებლად აუცილებელია:

- 1) გავხსნათ ტერმინალი ადმინისტრატორის უფლებით: დავაწკაპუნოთ start-ს, შემდეგ Command Prompt-ს დავაწკაპოთ მარჯვენა კლიკით და ავირჩიოთ Run as administrator
- 2) გავუშვათ net user ბრძანება რათა ვნახოთ ჩვენი კომპიუტერის სახელი
- 3) ახლა უკვე შეგვიძლია net view ბრძანება გავუშვათ ჩვენი კომპიუტერის მითითებით
- 4) უფრო დეტალური ინფორმაციისთვის გავუშვათ net view ბრმანება /all ოფციით





Net view \\WIN-VKH0MU20PJC
გაშვებით \\WIN-VKH0MU20PJC
კომპიუტერისთვის გაზიარებული
რესურსების ხილვა



Net view /? გაშვებით ამ ბრძანების შაბლონი გამოჩნდება

```
C:\Users\student>net view /?
The syntax of this command is:

NET VIEW
[\\computername [/CACHE] | [/ALL] | /DOMAIN[:domainname]]

C:\Users\student>_
```

route print ბრძანება

გამოსახავს მიმდიწარე კომპიუტერის მარშრუტირების ცხრილს (routing table).

routing table არის ცხრილი რომელიც ინახება როუტერში ან ჰოსტში და წარმოადგენს კონკრეტულ დანიშნულების ადგილამდე მარშრუტებს.

Router - როუტერი, იგივე მარშრუტიზატორი გამოიყენება ქსელების ერთმანეთთან დასაკავშირებლად. მისი ფუნქცინალიადან აღსანიშნავია:

- მონაცემთა პაკეტების სამიზნე IP-სთან გადაცემის გზით ქსელთა შორისი ტრეფიკის მართვა;
- რამდენიმე მოწყობილობისთვის ერთი ინტერნეტ კავშირის გამოყენების
 საშყალების უზრუნვეკყოფა



route print ბრძანების გამოყენების მაგალითები

Route print /? ამ ბრძანების აღწერის, ოფციებისა და მაგალითების ნახვა

```
Command Prompt
 :\Users\student>route print /?
Manipulates network routing tables.
ROUTE [-f] [-p] [-4|-6] command [destination]
                 [MASK netmask] [gateway] [METRIC metric] [IF interface]
              Clears the routing tables of all gateway entries. If this is
              used in conjunction with one of the commands, the tables are
              cleared prior to running the command.
              When used with the ADD command, makes a route persistent across
              boots of the system. By default, routes are not preserved
              when the system is restarted. Ignored for all other commands,
              which always affect the appropriate persistent routes.
              Force using IPv4.
              Force using IPv6.
 command
              One of these:
                          Prints a route
                          Adds a route
                DELETE Deletes a route
                CHANGE
                         Modifies an existing route
 destination Specifies the host.
              Specifies that the next parameter is the 'netmask' value.
              Specifies a subnet mask value for this route entry.
              If not specified, it defaults to 255.255.255.255.
              Specifies gateway.
 gateway
              the interface number for the specified route.
  interface
              specifies the metric, ie. cost for the destination.
All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.
If the command is PRINT or DELETE, Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.
If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string.
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.
Pattern match is only allowed in PRINT command.
Diagnostic Notes:
```

```
Command Prompt
              Specifies that the next parameter is the 'netmask' value.
 netmask
              Specifies a subnet mask value for this route entry.
              If not specified, it defaults to 255,255,255,255.
              Specifies gateway.
 gateway
              the interface number for the specified route.
 interface
 METRIC
              specifies the metric, ie, cost for the destination.
All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.
f the command is PRINT or DELETE. Destination or gateway can be a wildcard.
(wildcard is specified as a star '*'), or the gateway argument may be omitted.
If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string.
and '?' matches any one char. Examples: 157. 1, 157. 127. 224.
Pattern match is only allowed in PRINT command.
Diagnostic Notes:
   Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
   Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
            The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.
Examples:
   > route PRINT
   > route PRINT -4
   > route PRINT -6
   > route PRINT 157*
                               .... Only prints those matching 157*
   > route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
            destination^
                                         ^gateway
                                                      metric^ ^
                                                        Interface*
     If IF is not given, it tries to find the best interface for a given
     gateway.
   > route ADD 3ffe::/32 3ffe::1
   > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2
     CHANGE is used to modify gateway and/or metric only.
   > route DELETE 157.0.0.0
   > route DELETE 3ffe::/32
```

route print ბრძანების გამოყენების მაგალითები

მიმდინარე კომპიუტერის მარშრუტირების ცხრილს (routing table) გამოსახავა

```
Command Prompt
                                                                              - 0 X
:\Users\student>route print
 ______
Interface List
 2...00 25 ab 96 81 8b .....Realtek PCIe GbE Family Controller #2
14...a4 02 b9 6b 9d 43 .....Microsoft Wi-Fi Direct Virtual Adapter #3
15...a6 02 b9 6b 9d 42 .....Microsoft Wi-Fi Direct Virtual Adapter #4
22...a4 02 b9 6b 9d 42 .....Intel(R) Dual Band Wireless-AC 7265
17. a4 02 b9 6b 9d 46 ..... Bluetooth Device (Personal Area Network) #2
 1.....Software Loopback Interface 1
......
IPv4 Route Table
Active Routes:
                                            Interface Metric
Network Destination
                    Netmask
                                 Gateway
       0.0.0.0
                    0.0.0.0
                             192.168.30.1
                                         192,168,30,41
     127.0.0.0
                   255.0.0.0
                                On-link
                                             127.0.0.1
                                                       331
     127.0.0.1 255.255.255.255
                                On-link
                                             127.0.0.1
 127.255.255.255 255.255.255.255
                                On-link
                                            127.0.0.1
                                                       331
   192,168,30.0 255,255,255.0
                                On-link
                                         192.168.30.41
  192,168,38,41 255,255,255,255
                                On-link
                                         192,168,30,41
  192.168.30.255 255.255.255.255
                                On-link
                                         192,168,30,41
     224.0.0.0
                   240.0.0.0
                                On-link
                                             127.0.0.1
                                                       331
     224.0.0.0
                  240.0.0.0
                                On-link
                                         192.168.30.41
                                                       306
 255.255.255.255 255.255.255.255
                                On-link
                                             127.0.0.1
 255.255.255.255 255.255.255.255
                                On-link
                                         192.168.30.41
Persistent Routes:
 None
IPv6 Route Table
If Metric Network Destination
                           Gateway
                           On-link
     331 ::1/128
     306 fe80::/64
                           On-link
     306 fe80::119f:a569:5b55:9292/128
                           On-link
     331 ff@0::/8
                           On-link
     306 ff00::/8
                           On-link
Persistent Routes:
 None
```

route print ბრძანების გამოყენების მაგალითები

C.\ Ucanc\ ctudant\

მიმდინარე კომპიუტერის IPV4 მარშრუტირების ცხრილს (IPV4 routing table) გამოსახვა

```
C:\Users\student>route print -4
Interface List
  2...00 25 ab 96 81 8b .....Realtek PCIe GbE Family Controller #2
 14...a4 02 b9 6b 9d 43 .....Microsoft Wi-Fi Direct Virtual Adapter #3
 15...a6 02 b9 6b 9d 42 .....Microsoft Wi-Fi Direct Virtual Adapter #4
 22...a4 02 b9 6b 9d 42 .....Intel(R) Dual Band Wireless-AC 7265
 17...a4 02 b9 6b 9d 46 .....Bluetooth Device (Personal Area Network) #2
  1.....Software Loopback Interface 1
TPv4 Route Table
Active Routes:
Network Destination
                                                         Interface Metric
                          Netmask
                                           Gateway
                          0.0.0.0
                                      192.168.30.1
                                                      192.168.30.41
                                                                        45
          0.0.0.0
        127.0.0.0
                         255.0.0.0
                                          On-link
                                                          127.0.0.1
                                                                       331
        127.0.0.1 255.255.255.255
                                          On-link
                                                          127.0.0.1
                                                                       331
                                          On-link
  127.255.255.255 255.255.255.255
                                                          127.0.0.1
                                                                       331
     192.168.30.0
                     255.255.255.0
                                          On-link
                                                      192,168,30,41
                                                                       301
    192.168.30.41 255.255.255.255
                                          On-link
                                                      192.168.30.41
                                                                       301
                                          On-link
   192.168.30.255 255.255.255.255
                                                      192.168.30.41
                                                                       301
                                          On-link
        224.0.0.0
                         240.0.0.0
                                                          127.0.0.1
                                                                       331
        224.0.0.0
                        240.0.0.0
                                          On-link
                                                      192.168.30.41
                                                                       301
  255.255.255.255 255.255.255.255
                                          On-link
                                                                       331
                                                          127.0.0.1
                                          On-link
  255.255.255.255 255.255.255.255
                                                      192.168.30.41
                                                                       301
Persistent Routes:
  None
C:\Users\student>_
```

მიმდინარე კომპიუტერის IPv6 მარშრუტირების ცხრილს (IPv6 routing table) გამოსახვა

```
C:\Users\student>route print -6
Interface List
 2...00 25 ab 96 81 8b .....Realtek PCIe GbE Family Controller #2
14...a4 02 b9 6b 9d 43 .....Microsoft Wi-Fi Direct Virtual Adapter #3
15...a6 02 b9 6b 9d 42 .....Microsoft Wi-Fi Direct Virtual Adapter #4
22...a4 02 b9 6b 9d 42 .....Intel(R) Dual Band Wireless-AC 7265
17...a4 02 b9 6b 9d 46 .....Bluetooth Device (Personal Area Network) #2
 1.....Software Loopback Interface 1
TPv6 Route Table
Active Routes:
If Metric Network Destination
                                   Gateway
      331 ::1/128
                                   On-link
22
      301 fe80::/64
                                   On-link
      301 fe80::119f:a569:5b55:9292/128
                                   On-link
 1
      331 ff00::/8
                                   On-link
       301 ff00::/8
                                   On-link
Persistent Routes:
  None
```

Hostname ბრძანება

Hostname ბეჭდავს მიმდიწარე ჰოსტის დასახელებას

ჰოსტი (კვანძი) ეწოდება ქსელში ჩართულ ნებისმიერ მოწყობილობას



Hostname ბრძანების გამოყენება

Hostname მიმდინარე ჰოსტის დასახელების დაბეჭდვა

Command Prompt

C:\Users\student>hostname BTU201-1

Hostname /? ამ ბრძანების აღწერის გამობეჭდვა. როგორც აღბეჭდილია, ამ ბრძენბას არ გააჩნია ოფციები

C:\Users\student>hostname /?

Prints the name of the current host.

hostname

C:\Users\student>

შეჯამება

ქსელური ბრმანებები ასრულებს მნიშვნელოვან როლს ქსელის მართვის, შეცდმოების აღმოფხვრისა და გაუნჯობესებისთვის.

ქსელური ბრძანებების მეშვეობით ხორციელდება:

- ქსელური კავშირების ვერიფიცირება
- ქსელური ინფორმაციის მოგროვება
- ქსელური პარამეტრების მართვა
- ქსელური შეცდომების აღმოფხვრა
- უსაფრთხოების გაძლიერება
- ქსელის ადმინისტრირება