ping komutu:

Ping komutu ile verilen **IP adresine ait bilgisayarın TCP/IP bakımından çalışıp çalışmadığını öğrenmek ve eğer çalışıyorsa ona ne kadar sürede ulaşıldığını görmek için kullanılır.** Ping komutunda, karşıdaki cihaza 32 baytlık bir **ICMP (Internet Control Message Protocol – İnternet Yönetim Mesajlaşması Protokolü)** paketi gönderilir ve aynı paketin geri gelmesini bekler. Bu paketle karşı cihaza echo komutu yollanmış olur ve karşıdan echoreplay komutu bekler.

Aynı zamanda bu paket yola çıktığında bu pakete **TTL (time to live) adı verilen bir yaşam süresi tanımlanır.** Bu değer 255'ten başlar ve hedef makineye ulaşıncaya kadar her geçtiği yönlendiricide bir azalır. Eğer TTL 0 (sıfır) olursa (destination unreachable) hedef ulaşılamaz mesajı gönderir.

Ping komutu parametrelerini kısaca açıklayalım:

-t: İstemci tarafından karşıdaki makineye istemci durdurana kadar paket yollar ve sonucu ekrana yazar.

-a: ping paketi gönderilen hedef bilgisayarın IP adresinden bilgisayar isminin çözülmesini sağlar.

-n <sayı>: Hedef bilgisayara girdiğimiz değer kadar veri paketi gönderir. Eğer bir sayı girilmezse varsayılan değer 4'tür.

-l : Hedef bilgisayar gönderilen veri paketinin boyutunu değiştirmek için kullanılır. Boyut veri paketinin boyutunu belirler. Varsayılan 32 veya 64'tür.

-f: Gönderilen veri paketinin bölünmeden tek bir paket olarak gitmesini sağlar.

-i TTL: Gönderilen veri paketinin yaşam süresinin (TTL) girilen değerle belirlenmesini sağlar.

-v TOS: Hedef bilgisayardan gönderilen paketlerin başına Hizmet Türü (TOSType of Service) konulmasını sağlar.

-w : Gönderilen paketin geri dönüş süresini zaman aşımı alanına girilen değerle sabitlemeyi sağlar.

https://www.sordum.net/2272/ping-komutu-nedir-nasil-kullanilir/

```
E:\Projects>ping -i 4 google.com

Pinging google.com [172.217.17.110] with 32 bytes of data:
Reply from 81.212.218.8: TTL expired in transit.
Reply from 81.212.218.8: TTL expired in transit.
Reply from 81.212.218.8: TTL expired in transit.
Reply from 81.212.218.8: TTL expired in transit.

Ping statistics for 172.217.17.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

---

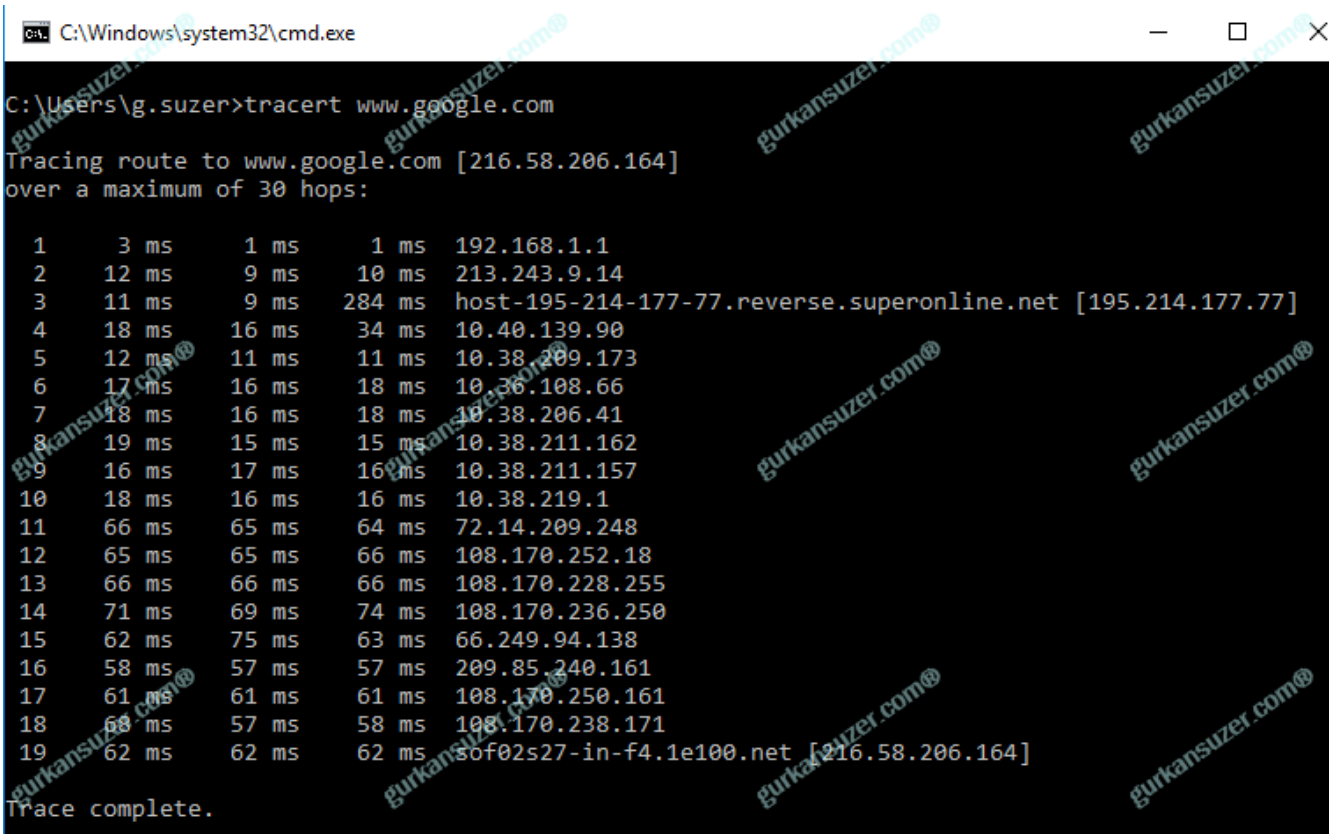
traceroute (tracert) komutu:

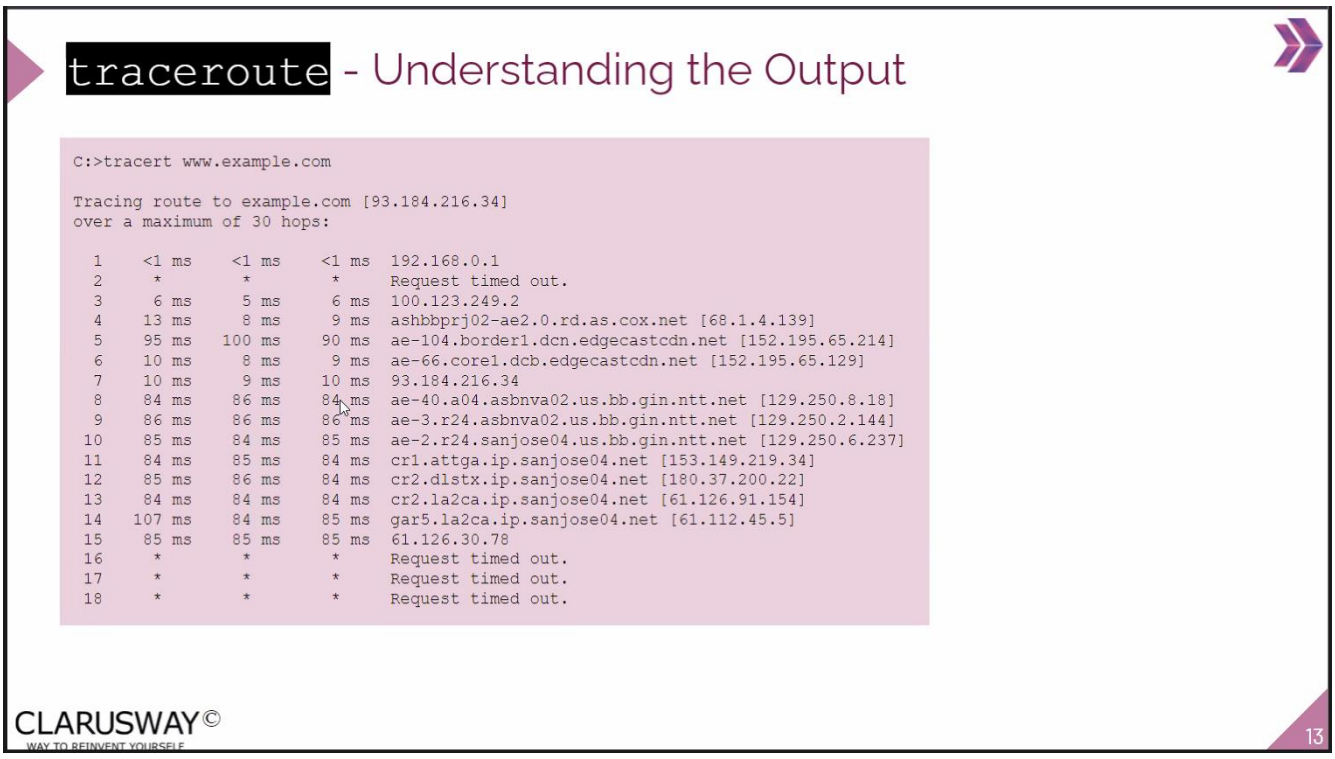
Tracert komutu TCP/IP komutları içerisinde yer alan bir sorgulama komutudur. Hedefe ICMP (Internet Control Message Protocol) paketleri göndererek hedefin yolunun bulunması sağlanır. Tracert komutu Windows işletim sistemlerindeki adıdır. Cisco ve Linux komutları arasındaki ismi traceroute olarak bilinmektedir.

Tracert TTL (Time To Live) değerlerini kullanarak çalışmaktadır. Yol üzerinde bulunan her IP TTL süresini 1 değer düşürerek kaç yönlendiriciden (Router) geçildiğini gösterir.

Komuta Erişmek için sırası ile **Başlat > Çalıştır > CMD** yazıyoruz. Gelen dos ekranının da komutu;

Tracert www.google.com şeklinde kullanabiliriz.





Aradaki yönlendiricilerin bazılarında “Request time out” şeklinde mesaj verebilir. Bu zaman aşımına uğramış TTL paketleridir. Bu yönlendirici (Router) tarafından kendini gizleme olarak düşünebilirsiniz. Sadece ICMP paketlerine cevap vermiyordur.

Tracert komutunun diğer paremetrelerini görmek için tracert /? şeklinde yazabilirsiniz. Ancak bu kısımda benim en çok kullandığım –d parametresidir. Bu her atlamada DNS çözümlemesi yapmayacaktır.

C:\Windows\system32>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]

[-R] [-S srcaddr] [-4] [-6] target_name

Options:

-d Do not resolve addresses to hostnames.

-h maximum_hops Maximum number of hops to search for target.

-j host-list Loose source route along host-list (IPv4-only).

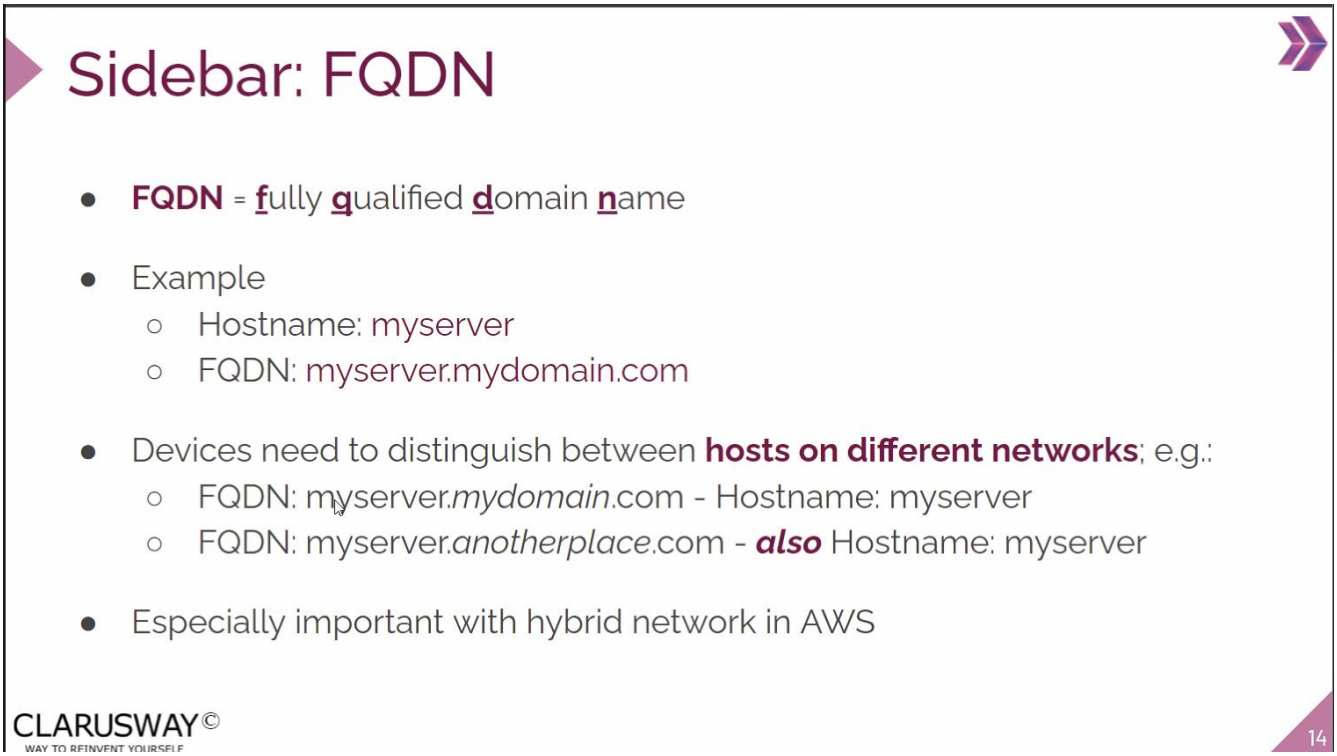
-w timeout Wait timeout milliseconds for each reply.

-R Trace round-trip path (IPv6-only).

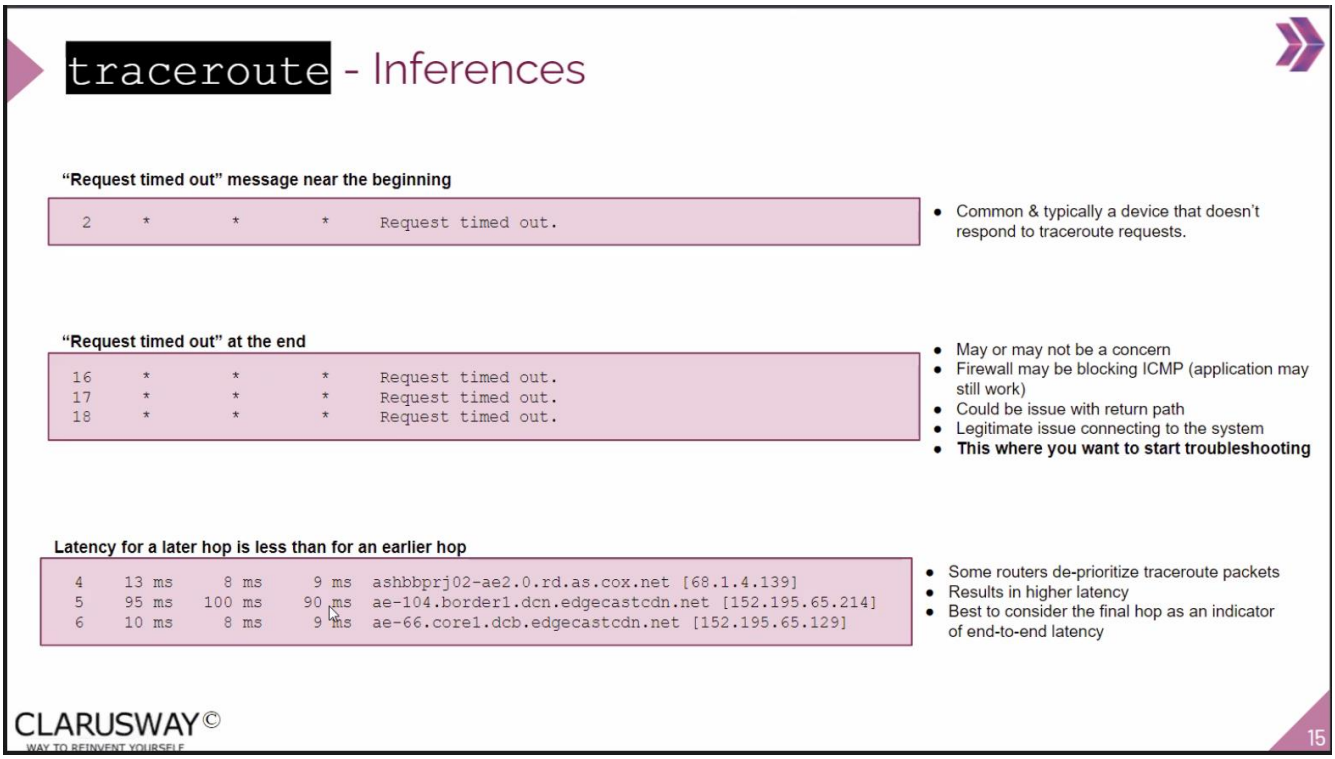
-S srcaddr Source address to use (IPv6-only).

-4 Force using IPv4.

-6 Force using IPv6.



FQDN (Fully Qualified Domain Name) alan adı sisteminde bir alan adının tamamını nitelemek için kullanılır. Örneğin; 'system.microsoft.com' tanımlarken “system” alt alan adı, “microsoft.com.com” alan adıdır. “system.microsoft.com” ise **FQDN** olarak belirtilmektedir.



mtr (patping) komutu:

MTR nedir? Nasıl Kurulur?

MTR, traceroute ve ping araçlarının özelliklerini bir arada bulundurur. Böylece belirlenen hedef adres üzerindeki tüm hop’ların adreslerini tespit eder ve bu cihazlara icmp echo requestler (ping) göndererek her hop'un round-trip time ve packet loss değerlerini tespit ederek ekrana basar.

MTR hem **linux** hemde **windows (WinMTR)** sunucularda kurulabilir.

Centos için aşağıdaki gibi kurulum sağlanabilir.

```
[root@31 ~]# yum install mtr
```

Aşağıdaki komut ile MTR için kullanılabilecek parametreleri görebilirsiniz.

```
[root@31 ~]# mtr --help
mtr [-BfhvrwctglxspQomniuT46] [--help] [--version] [--report]
[--report-wide] [--report-cycles=COUNT] [--curses] [--gtk]
[--csv|-C] [--raw] [--xml] [--split] [--mpls] [--no-dns] [--show-ips]
[--address interface] [--filename=FILE|-F]
[--ipinfo=item_no|-y item_no]
[--aslookup|-z]
```

```
[--psize=bytes/-s bytes] [--order fields]
[--report-wide|-w] [--inet] [--inet6] [--max-ttl=NUM] [--first-ttl=NUM]
[--bitpattern=NUM] [--tos=NUM] [--udp] [--tcp] [--port=PORT] [--timeout=SECONDS]
[--interval=SECONDS] HOSTNAME
```

google.com adresine **MTR** çıktısı alıp yorumlayalım.

```
[root@31 ~]# mtr google.com
```

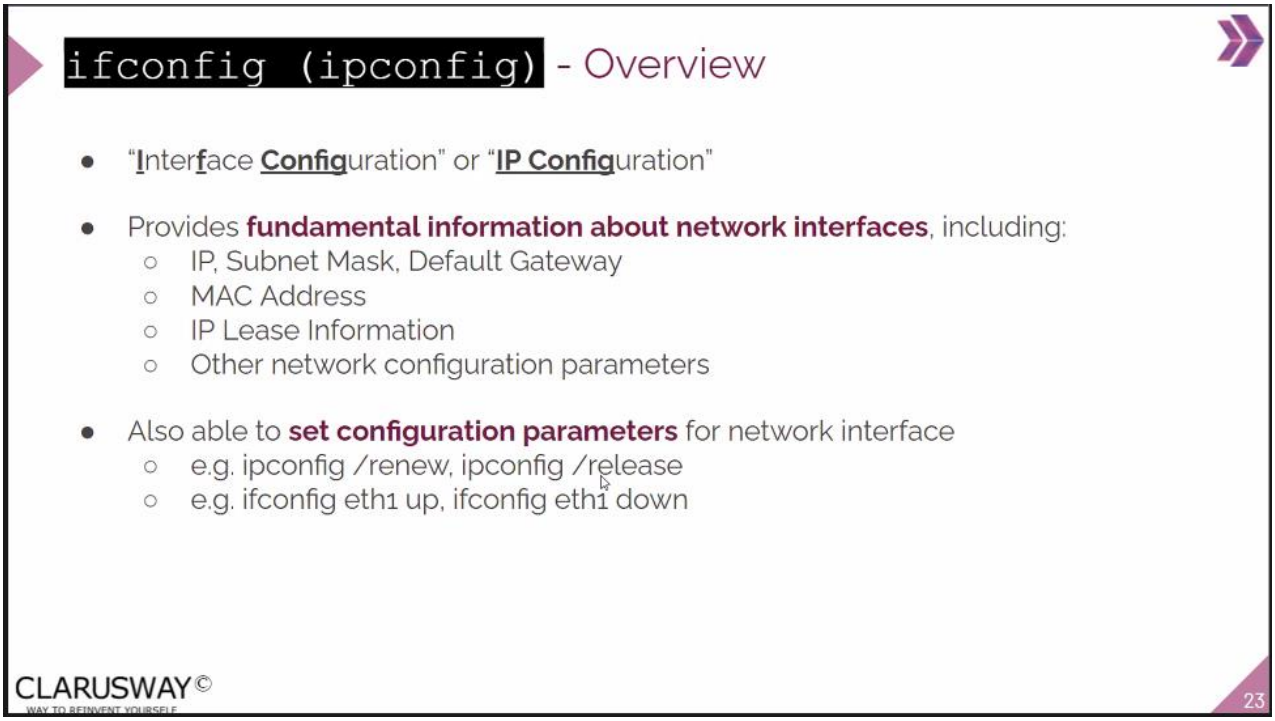
Yukarıda görüldüğü gibi sunucumuzdan google a giderken 4 yerde paket loss görünmektedir.

Ama bu o hoplarda yapılan icmp limitlemesinden kaynaklanıyordur.

Burada dikkat edilmesi gereken nokta "ok" işareti ile gösterilmiş olan ilk paket çıkışındaki loss ve paketin ulaştığı yerdeki loss oranı olmalıdır.

Yani sunucumuzdan çıkan paket kayıpsız şekilde google.com adresine ulaşmıştır.

Ayrıca Windows sunucular içinde **WinMTR** kurulumu yapılabilir.

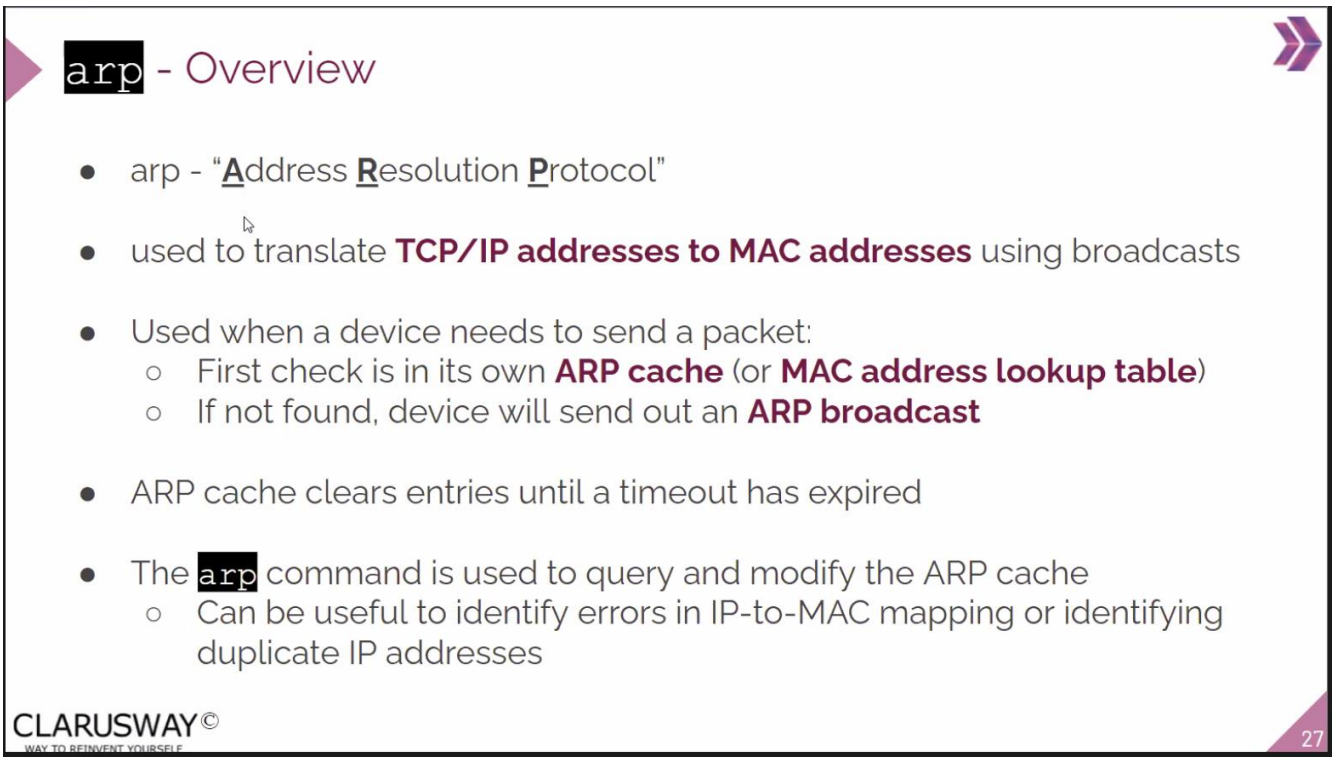


ifconfig (ipconfig) komutu:

Komutum çalıştı 😊

MAC = physical address

arp komutu:

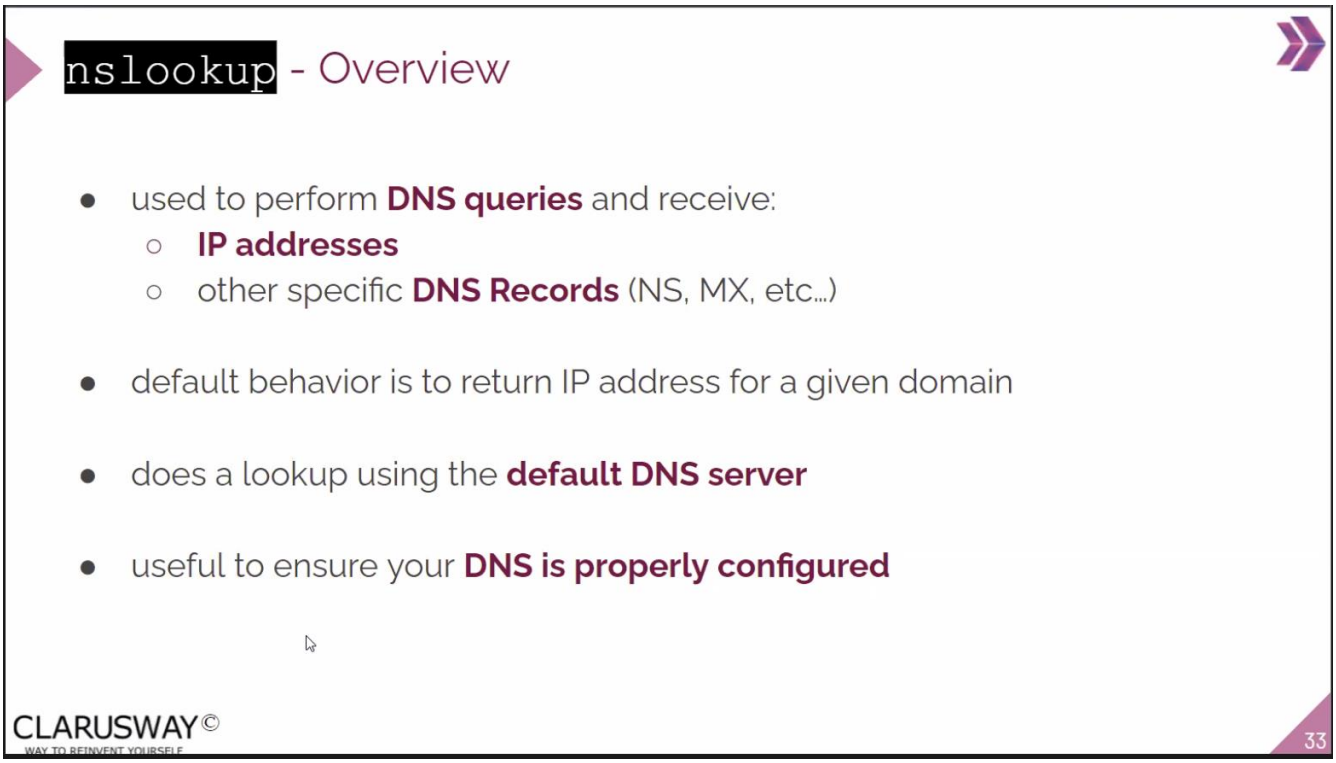



```
E:\Projects>arp -a

Interface: 192.168.1.37 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           08-26-97-32-69-2b     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.30.176.1 --- 0x27
  Internet Address      Physical Address      Type
  172.30.191.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Linux / MacOS / Windows	`arp -a` view the ARP cache `arp -s` add an entry to the cache `arp -d` delete an entry from the cache

nslookup komutu:

Nslookup Komutu Nedir?: Dns Serverin Düzgün çalışıp çalışmadığı kontrol etmek için kullanılır. ... Bu **komutu** yazarak Enter'a bastığınızda DNS sunucunuz ve DNS adresinizin hangisi olduğunu göreceksiniz.



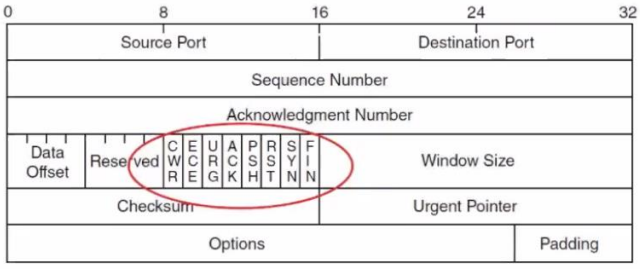
nmap komutu:

Nmap, ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araçtır. İsmini Network Mapper'in kısaltmasından almaktadır. Ağ yöneticileri nmap'i sistemlerinde hangi cihazların çalıştığını belirlemek, mevcut ana makineleri ve sundukları hizmetleri keşfetmek, açık bağlantı noktaları bulmak ve güvenlik risklerini taramak için kullanırlar. Nmap, yüz binlerce cihazı ve alt ağı kapsayan geniş ağların yanı sıra tek ana bilgisayarı izlemek için kullanılabilir.

https://www.beyaz.net/tr/guvenlik/makaleler/nmap_nedir_ve_nasil_kullanilir.html#:~:text=%C4%B0smini%20Network%20Mapper'in%20k%C4%B1saltmas%C4%B1ndan,g%C3%BCvenlik%20risklerini%20taramak%20i%C3%A7in%20kullan%C4%B1rlar.

nmap - Overview

- nmap is a popular port scanning **tool** (i.e. not a command)
- By scanning certain **flags in packets**, security analysts (and hackers) can make certain assumptions
- These flags are used to **control the TCP connection process** and so are present only in TCP packets



CLARUSWAY© WAY TO REINVENT YOURSELF

38

route komutu:

Route komutu adından da anlayabileceğiniz gibi Yönlendirmek amaçlı olarak kullanılır ve bu komut sayesinde iki farklı ağı yönlendirme işlemi yapabiliriz.

Genel Kullanımı –

route [**-f**] [**-p**] [*Command* [*Destination*] [**mask** *Netmask*] [*Gateway*] [**metric** *Metric*]] [**if** *Interface*]]

Parametreleri –

-f = Bu komut yardımı ile route tablosunu silmeniz mümkündür ancak Loopback ipsi olan 127.0.0.0 255.255.255.255, Multicast yönlendirme olan 224.0.0.0 240.0.0.0 netmaskına sahip olan ipler silinmeyecektir. Eğer bu komutu add, change ve delete ile kullanırsanız. İlk önce route talosunu siler daha sonra komutu çalıştırır.

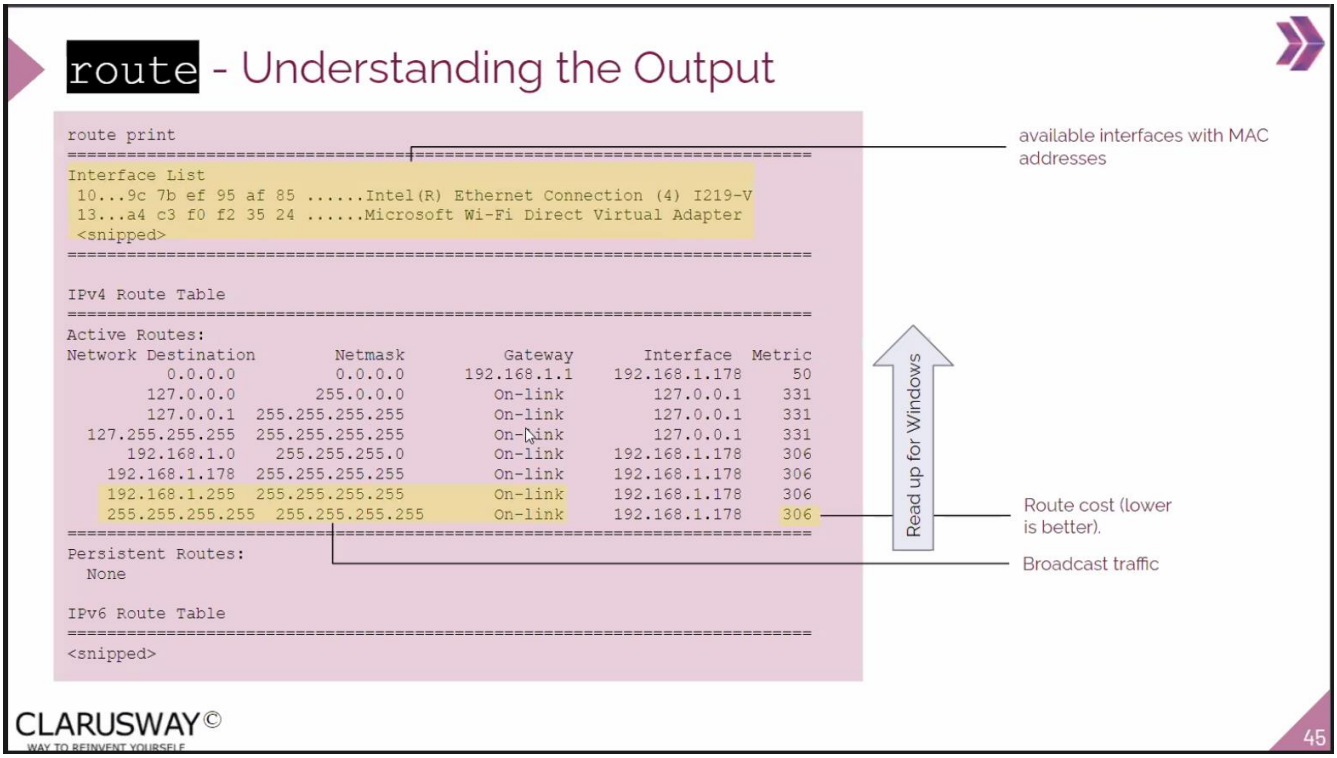
-p = Bu komutu add ile beraber kullanmamız durumunda belirlenen yok persistent olarak belirlenir ve silinmemek üzere kayıt edilir. Print komutu ile kullanılması durumunda sadece persistent olan route bilgileri gözükür ve diğer yönlendirmeler gözükmez.
Persistent Route'ların saklandığı regedit yolu ise :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes.

Komutların kullanımı :

add – Yönlendirme eklemek için,
change – Var olan yönlendirmeyi değiştirmek için,
delete – Yönlendirme silmek için,
print – Yönlendirme tablosunu görmek için kullanılır.

Destination – Belirtilecek olan networkun ip adresidir. Ancak o ağın NetId kısmıdır. Örnek olarak 192.168.1.2 numaralı networkumuzun NetId'si 192.168.1.0 olur. Ve burada bütün networklere bir yönlendirme olmasını istiyorsanız 0.0.0.0 ip adresini girmeniz gerekmektedir.

Routing Table Örneği



netstat komutu:

netstat (network statistics) ağ bağlantıları (hem gelen hem giden), yönlendirme tabloları ve ağ arayüzü istatistiklerini görüntüleyen bir komut satırı aracıdır. netstat komutu UNIX, Linux ve Windows NT tabanlı işletim sistemlerinde kullanılabilir.

netstat Komutları

netstat -n: Adresleri ve Bağlantı Noktalarının Numaralarını Sayısal Biçimde Gösterir

netstat -an: Dosya Alırken Karşıdakinin IP adresini Gösterir.(Bu Da Çok İyi Bir Yöntemdir Ama Amacımız IP Bulmak Değil Bu Konuda Tabi)

netstat -a: Tüm Bağlantıları ve Dinleme Bağlantı Noktalarını Gösterir.

netstat -b: Her Bağlantı veya Dinleme Bağlantı Noktası İle İlişkili Çalıştırılabilir Dosyayı Gösterir.

netstat -e: Ethernet İstatistiklerini Gösterir.

netstat -o: Her Bağlantıyla İlişkili Sahip İşlem Kimliğini Gösterir.

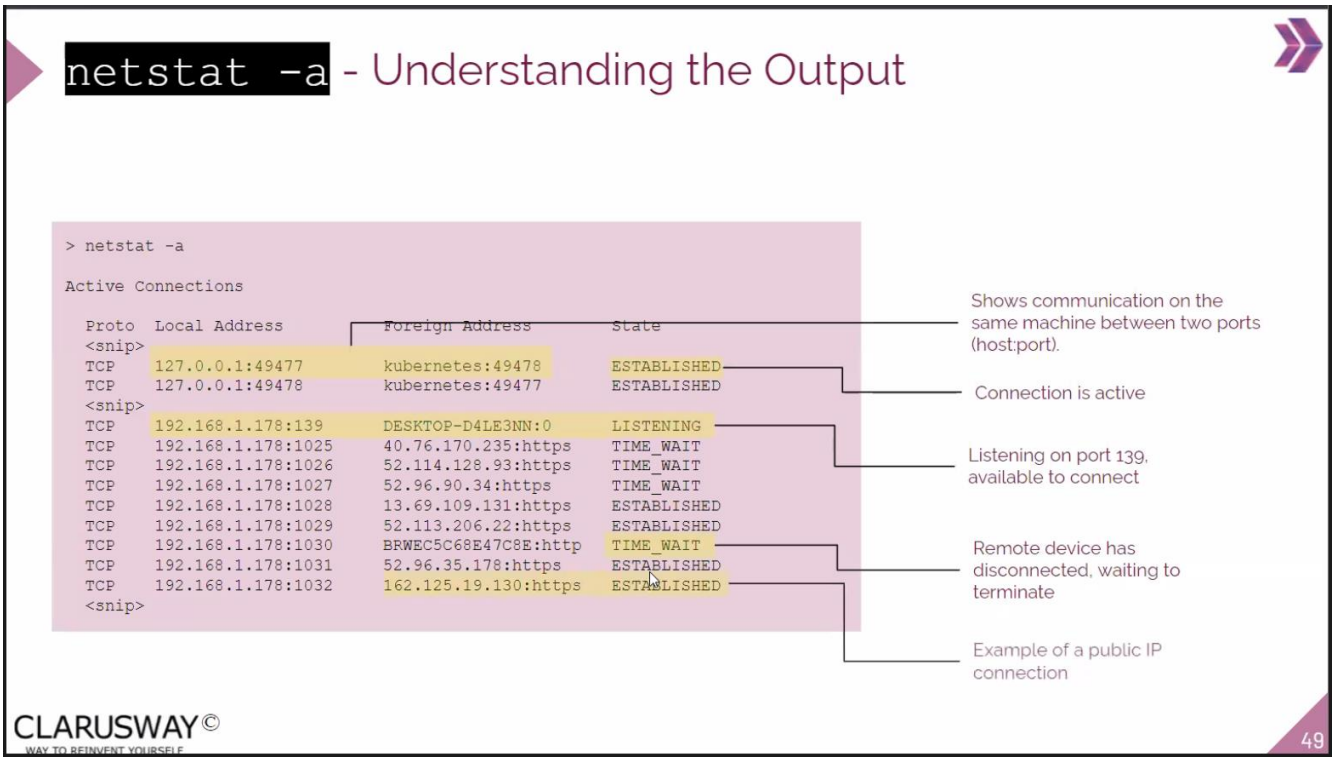
netstat -p: İletişim Kuralının Bağlantılarını Gösterir.

netstat -r: Yönlendirme Tablosunu Gösterir.

netstat -s: her İletişim Kuralları İçin İstatistikleri Gösterir.

netstat -v: En Önemli Netstat Komutu Olan -v, -b İle Birlikte Kullanılırsa Tüm Çalışan Dosyalar İçin Bağlantı ve Bağlantı Noktası Oluşumu İle İlgili Bileşenlerin Sırasını Gösterir.

netstat "aralık" CTRL+C Tuşlarına Basın Atlanırsa Netstat Geçerli Yapılandırma Bilgisini Bir Kez Yazdırır.



tcpdump komutu:

tcpdump	Ağ trafiğini analiz eder.
tcpdump -D	Ağ üzerinde dinlenebilecek bütün arayüzleri listeler.
tcpdump -i "arayüzün adı"	Belirtilen arayüzün dinlenmesini sağlar.
tcpdump -v	Paketin protokol içeriğini de gösteren detaylı bir analiz yapar.
tcpdump -vv	Paketin NFS ve SMB içeriğini de gösteren detaylı bir analiz yapar.
tcpdump -vvv	Paketin Telnet içeriğini de gösteren detaylı bir analiz yapar.
tcpdump -q	Sadece temel bilgilerini içeren bir analiz yapar.
tcpdump –c " sayı"	Belirtilen sayıda paket içeriğini listeler.
tcpdump -n	Analizi yaparken transfer yapılan adresin IP adresi ve port numarasını yazdırır.
tcpdump -n dst "IP adresi"	Belirtilen IP adresine giden paketleri listeler.
tcpdump -n src "IP adresi"	Belirtilen IP adresinden gelen paketleri listeler.
tcpdump -n "IP adresi"	Belirtilen IP adresinden gelen ya da giden bütün paketleri listeler.
tcpdump -n dst net "ağ adresi"	Belirtilen ağ adresine giden paketleri listeler.
tcpdump -n src net "ağ adresi"	Belirtilen ağ adresinden gelen paketleri listeler.
tcpdump -n net "ağ adresi"	Belirtilen ağ adresinden gelen ya da giden paketleri listeler.
tcpdump –n port "port numarası"	Hedef veya kaynak portu belirtilen port olan paketleri listeler.
tcpdump –n dst port "port numarası"	Hedef portu belirtilen port olan paketleri listeler.
tcpdump –n src port "port numarası"	Kaynak portu belirtilen port olan paketleri listeler.
tcpdump –v icmp	ICMP paketlerini listeler.
tcpdump –v arp	ARP paketlerini listeler.
tcpdump –p	Tcpdump ile yalnızca dinleme yapılan arabirime gelen paketleri yakalamak için seçici olmayan moddan çıkılması için kullanılır.
tcpdump –e	Yakalanan paketlerin ikinci katman bilgilerini yani mac adreslerini elde etmek için kullanılır.
tcpdump –w "dosya ismi"	Listelenen paketleri bir dosya halinde kaydeder. Bu kaydettiğimiz dosyayı 'Wireshark' gibi programlarla da açarak inceleyebiliriz.
tcpdump –r "dosya ismi"	Dosya halinde olan bir paket listesini açar.

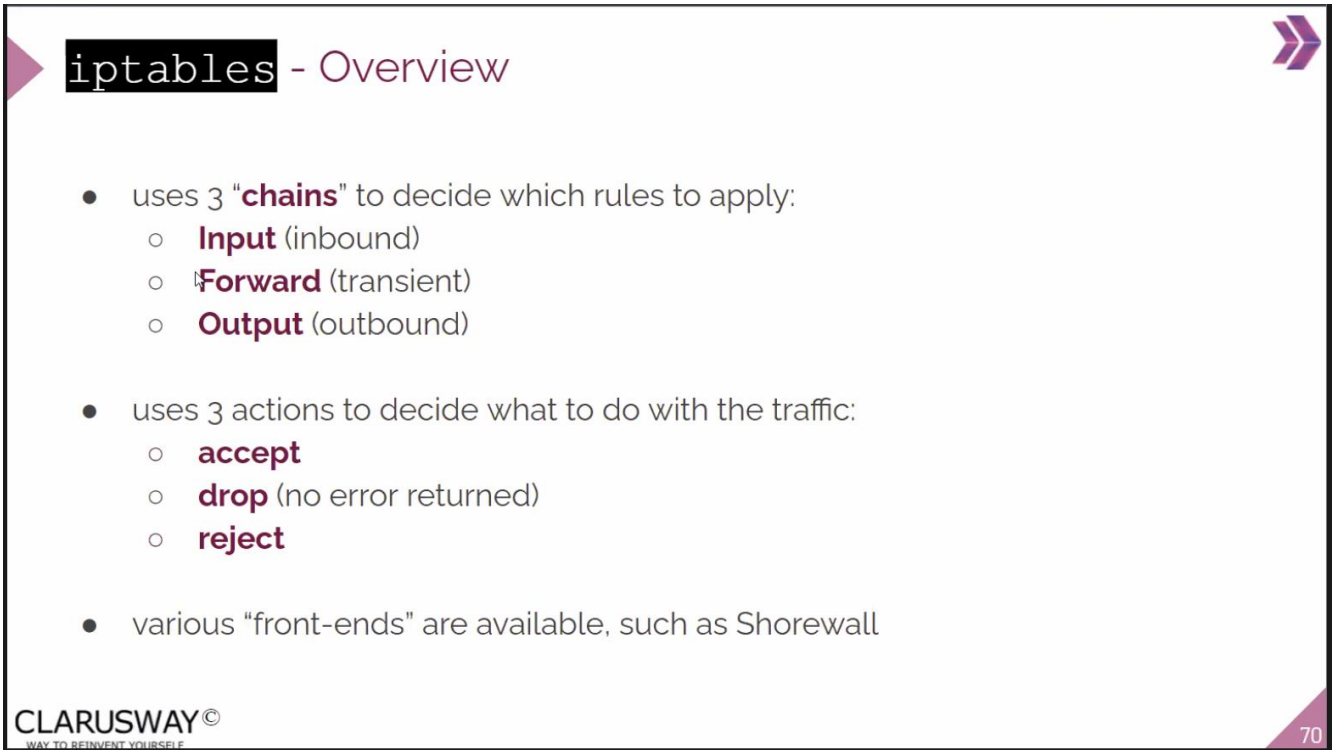
telnet komutu:

https://kodlayarakhayat.com/yazilim-muhendisligi/telnet-nasil-calisir/

curl komutu:

https://www.hostixo.com/blog/curl-nedir-curl-komutlarinin-kullanimi/

host-based
firewalls



Summary of Tools & Commands - Part 1

Tool/Command	What it Does	How it Helps	Notes
`ping`	Sends an ICMP "are you there?" request	Can determine definitively if a host is running	Cannot say for certain a host is down if it fails
`traceroute/tracert`	Sends ICMP requests to all routers on the path from source to destination	Identifies the number of hops from end-to-end and indicates latency	
`mtr/pathping`	Combines ping and tracert with continuous refresh	Identifies if a host is up and any potential latency issues	
`ifconfig/ipconfig`	Enables you to view or modify properties of network interfaces	Helps ensure interfaces are properly configured	
`arp`	Allows you to view or edit the ARP cache (IP-MAC address lookup)	Troubleshoot any outbound packet drops	Be wary of making changes to the ARP cache
`nslookup`	Provides DNS information about a particular domain	Debug to make sure source-to-destination connections are going where expected	

Summary of Tools & Commands - Part 2

Tool/Command	What it Does	How it Helps	Notes
`nmap`	A tool that allows you to discover open ports and map a network topology	Provides a birds-eye view of a network to identify which devices have which ports open	This is a 3rd party tool and may or may not be approved by an organization to use
`route`	View and edit the network route table	Troubleshoot any issues for any inbound or outbound packet loss	Be wary of changing a route table
`netstat`	View TCP connections and packet statistics by protocol	Validate existing connections and identify issues with packet errors	
`tcpdump`	View live network traffic	Trace traffic from a particular host and/or ensure it is arriving	
`telnet`	Connect to a remote host on any port	Ensure remote ports are listening and a path exists from source to target	Telnet is insecure and not installed by default usually
`curl`	Receive or send information to a remote host using a range of protocols	Ensures that the remote application is connected and able to respond	Particularly useful when no UI is available, especially for http & https

Summary of Tools & Commands - Part 3

Tool/Command	What it Does	How it Helps	Notes
Linux network configuration files	View and modify host aliases and resolver addresses	Look here to determine if the host is misconfigured with the wrong DNS server or aliases	
`iptables/` Windows Firewall	View and edit host-based firewall rules	Determine if any rules are blocking traffic you are expecting	There are layers of FWs in any network that cause operational headaches

I use ping against a remote device and there is no response.

Which of the following is definitely true?

A. The remote server is down

B. ICMP is not enabled on the remote device

C. A firewall along the way is blocking ICMP traffic

D. There is nothing for certain based on this ping result

1.Sorunun Cevabı: **D**

2

I use traceroute and get the output below. Approximately what is the latency from source to target?

```
Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     6 ms     5 ms     6 ms  100.123.249.2
  4    13 ms     8 ms     9 ms  ashbbprj02-ae2.0.rd.as.cox.net [68.1.4.139]
  5    95 ms   100 ms    90 ms  ae-104.border1.dcn.edgecastcdn.net [152.195.65.214]
  6    10 ms     8 ms     9 ms  ae-66.core1.dcb.edgecastcdn.net [152.195.65.129]
  7    10 ms     9 ms    10 ms  93.184.216.34
```

A. Approximately 125ms (the sum of the 3rd column)

B. Approximately 10ms (one value in the 3rd row)

C. Approximately 22ms (the average of all the columns)

D. Approximately 391ms (the sum of all the columns)

CLARUSWAY©
WAY TO REINVENT YOURSELF

85

2. Sorunun Cevabı: **B**

3

I use traceroute and get the output below. My manager tells me that there is an issue with the network at the 5th hop. Is she correct?

```
Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     6 ms     5 ms     6 ms  100.123.249.2
  4    13 ms     8 ms     9 ms  ashbbprj02-ae2.0.rd.as.cox.net [68.1.4.139]
  5    95 ms   100 ms    90 ms  ae-104.border1.dcn.edgecastcdn.net [152.195.65.214]
  6    10 ms     8 ms     9 ms  ae-66.core1.dcb.edgecastcdn.net [152.195.65.129]
  7    10 ms     9 ms    10 ms  93.184.216.34
```

A. No, chances are that router is de-prioritizing ICMP packets

B. No, chances are that router is dropping ICMP packets

C. No, my computer probably glitched when it sent that request

D. Yes, she's right

CLARUSWAY©
WAY TO REINVENT YOURSELF

86

3. Sorunun Cevabı: **A**

4

I use traceroute and get the output below. An application engineer looks at it and tells me traffic is being blocked at hop #2. Is it correct?

```
Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     6 ms     5 ms     6 ms  100.123.249.2
  4    13 ms     8 ms     9 ms  ashbbprj02-ae2.0.rd.as.cox.net [68.1.4.139]
  5    95 ms   100 ms    90 ms  ae-104.border1.dcn.edgecastcdn.net [152.195.65.214]
  6    10 ms     8 ms     9 ms  ae-66.core1.dcb.edgecastcdn.net [152.195.65.129]
  7    10 ms     9 ms    10 ms  93.184.216.34
```

A. Yes, the request definitely timed out

B. Yes, since every attempted ping resulted in a *

C. No, that router is most likely dropping netstat requests

D. No, the previous result is <1ms and it's too fast for hop #2 to respond

CLARUSWAY©
WAY TO REINVENT YOURSELF

87

4. Sorunun Cevabı: **C**

5

You're on a Linux server within a secure company network which is not connected to the Internet. How do you find out what your IP is?

A. Use ipconfig

B. Use ifconfig

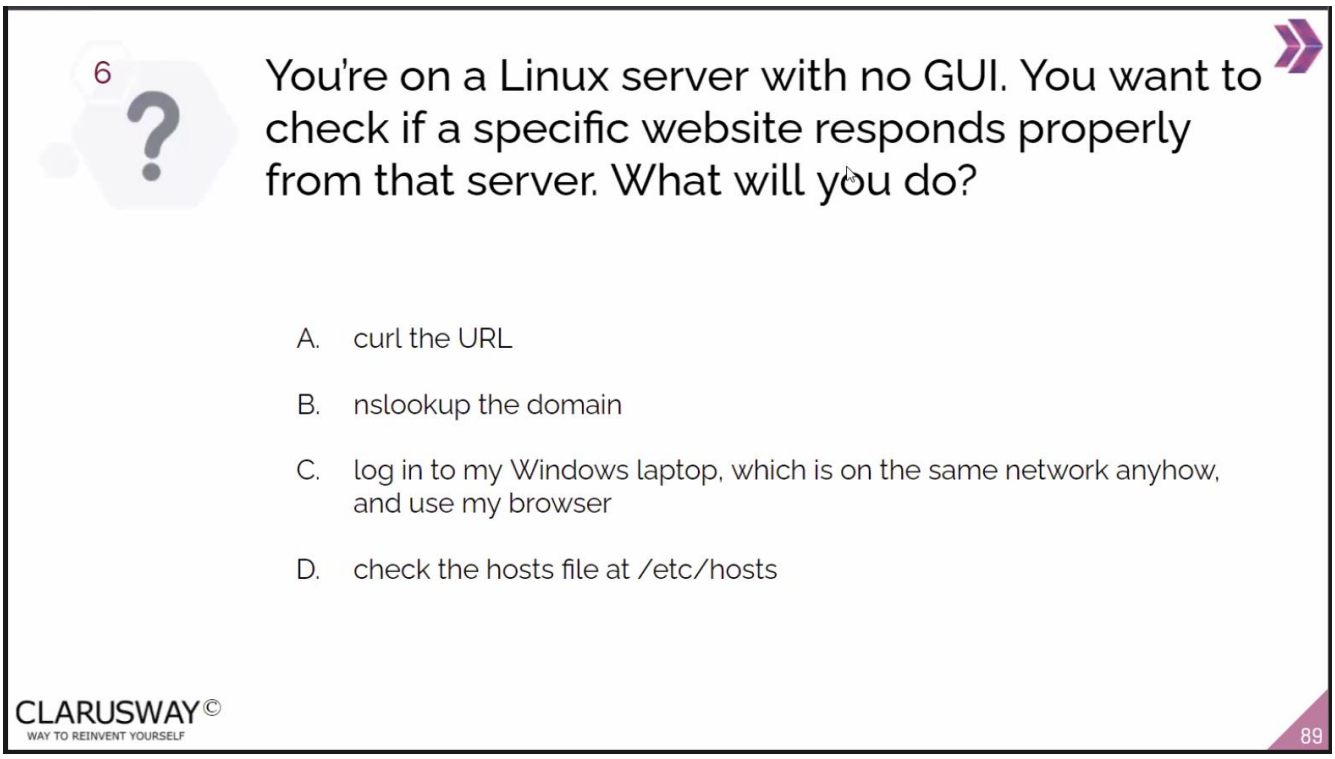
C. Use my browser to go to whatismyip.com

D. Check the resolver file at /etc/resolv.conf

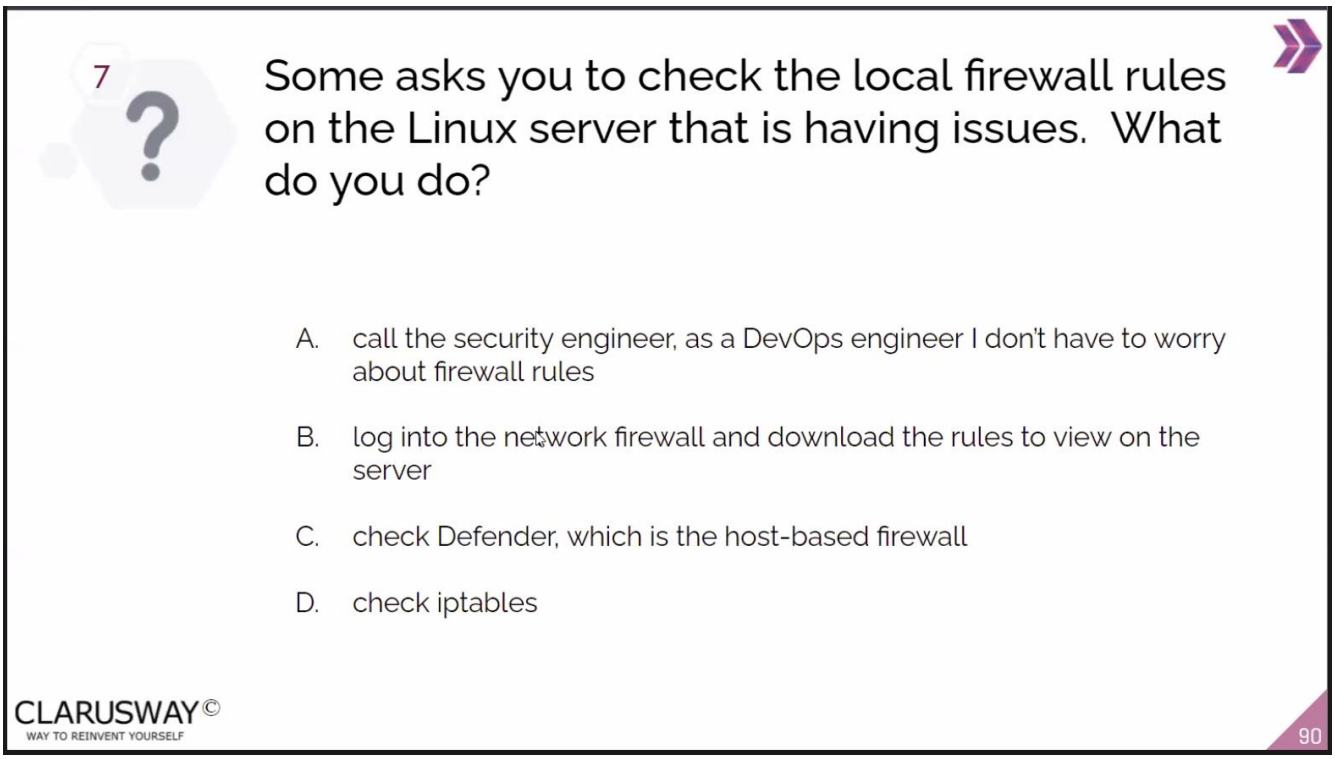
CLARUSWAY©
WAY TO REINVENT YOURSELF

88

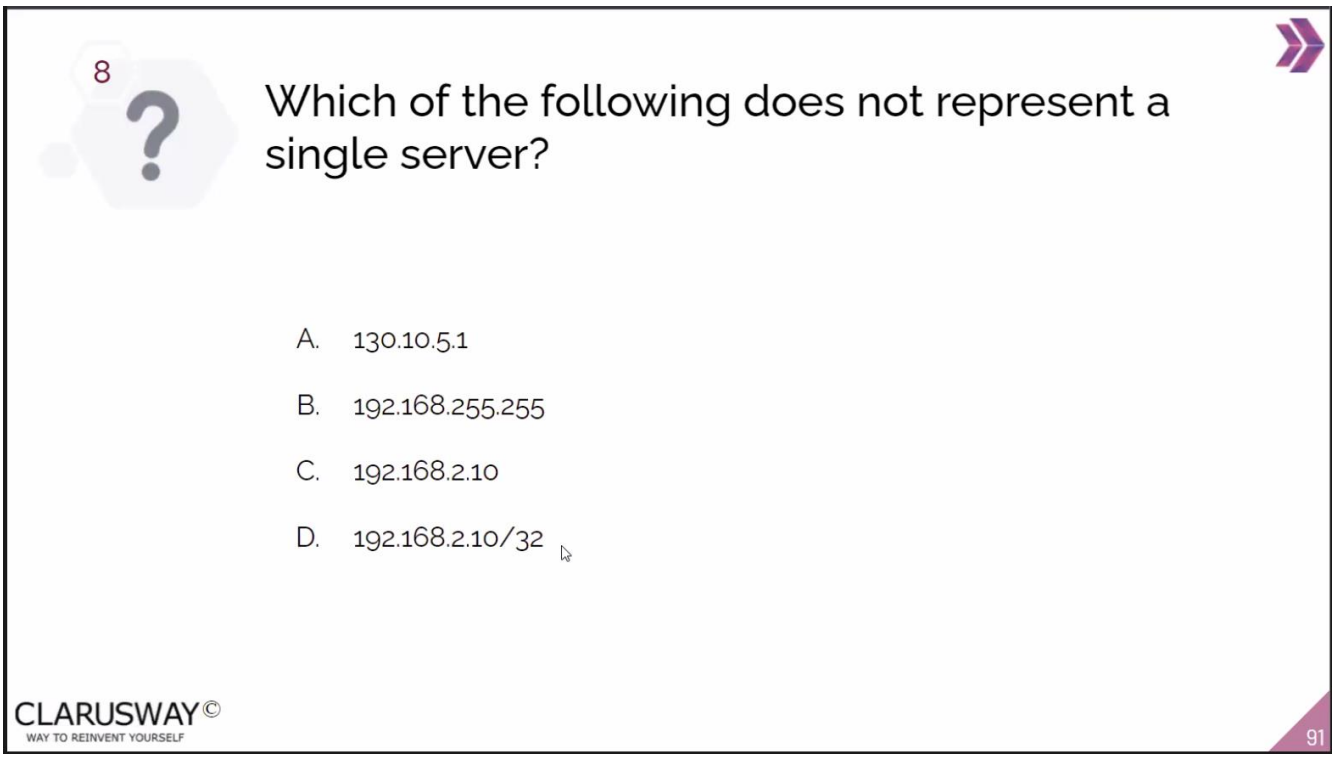
5. Sorunun Cevabı: **B**



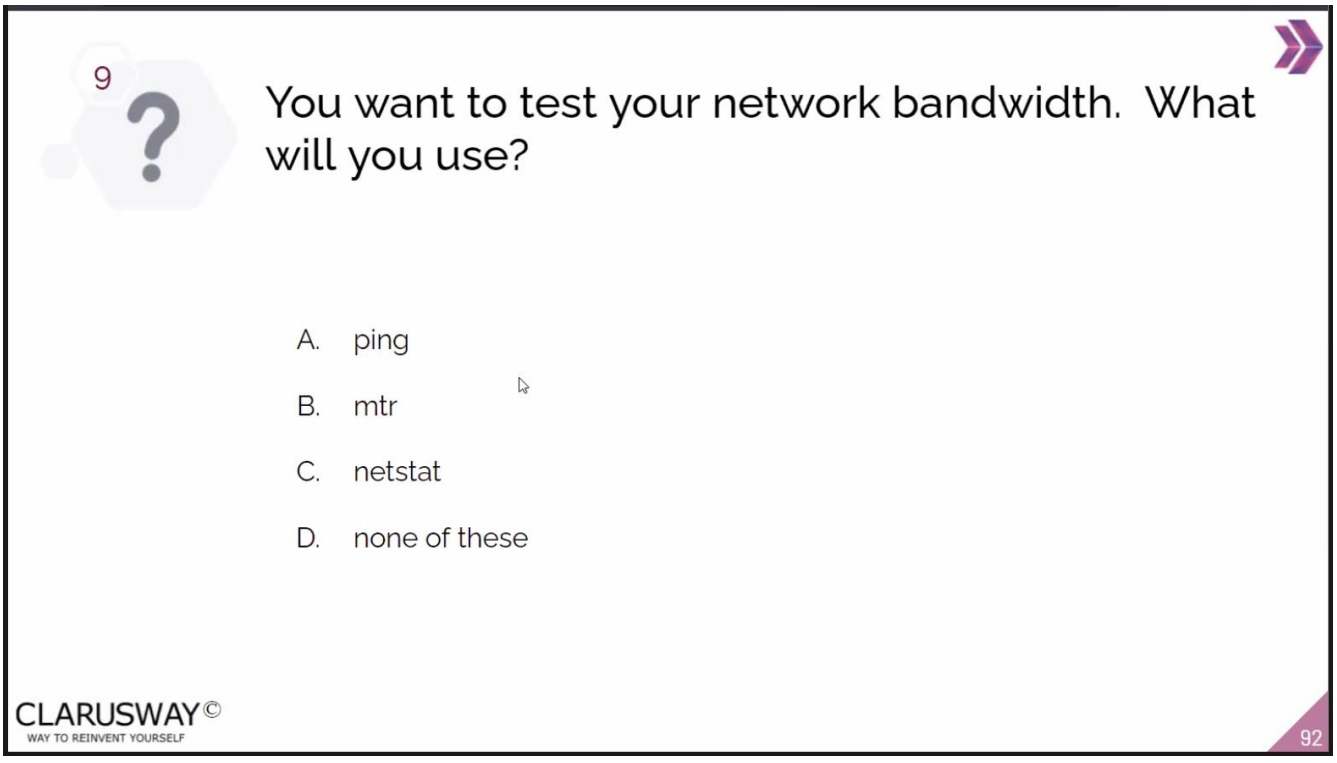
6. Sorunun Cevabı: **A**



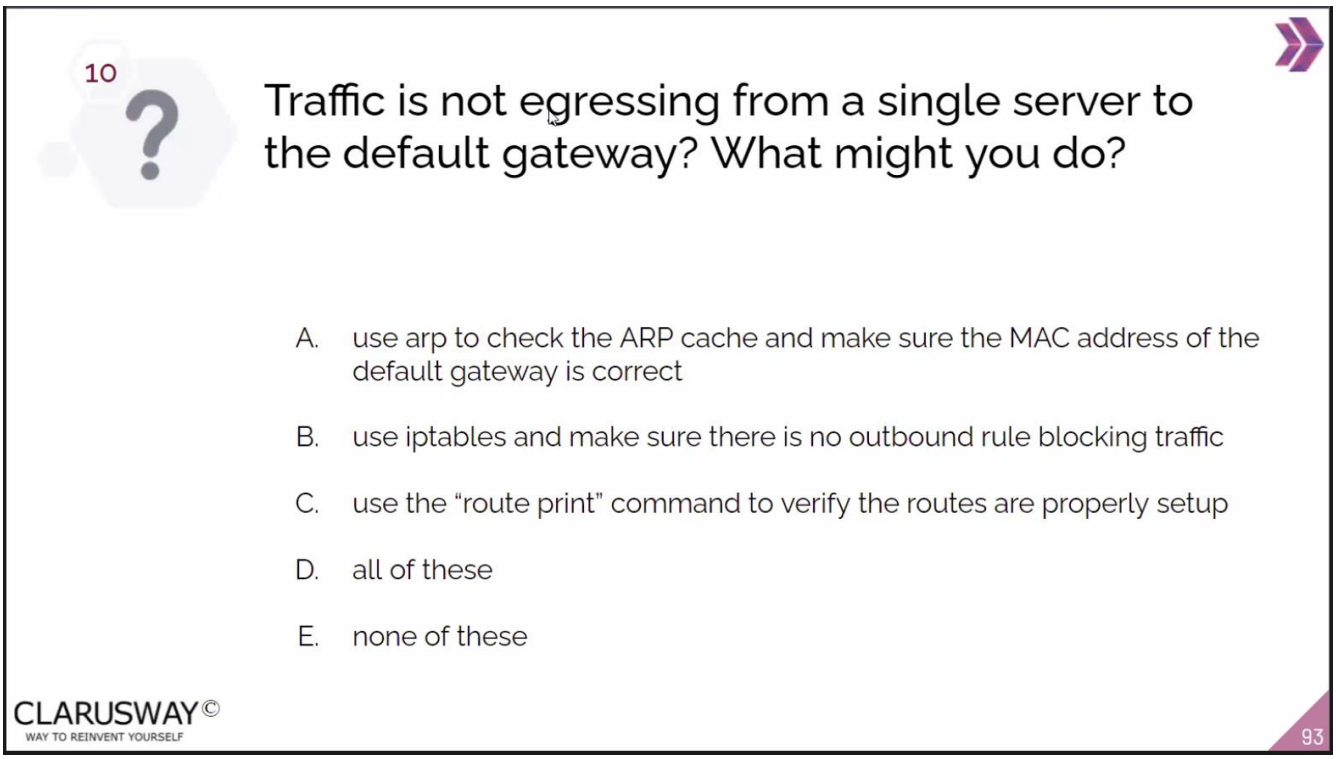
7. Sorunun Cevabı: **D**



8. Sorunun Cevabı: **D**



9. Sorunun Cevabı: **A**



10. Sorunun Cevabı: **D**