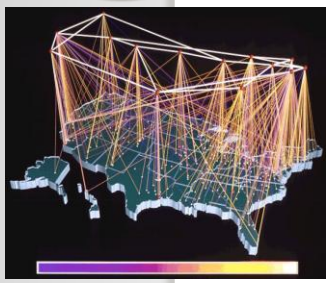
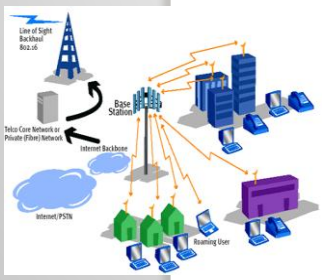




معماری شبکه

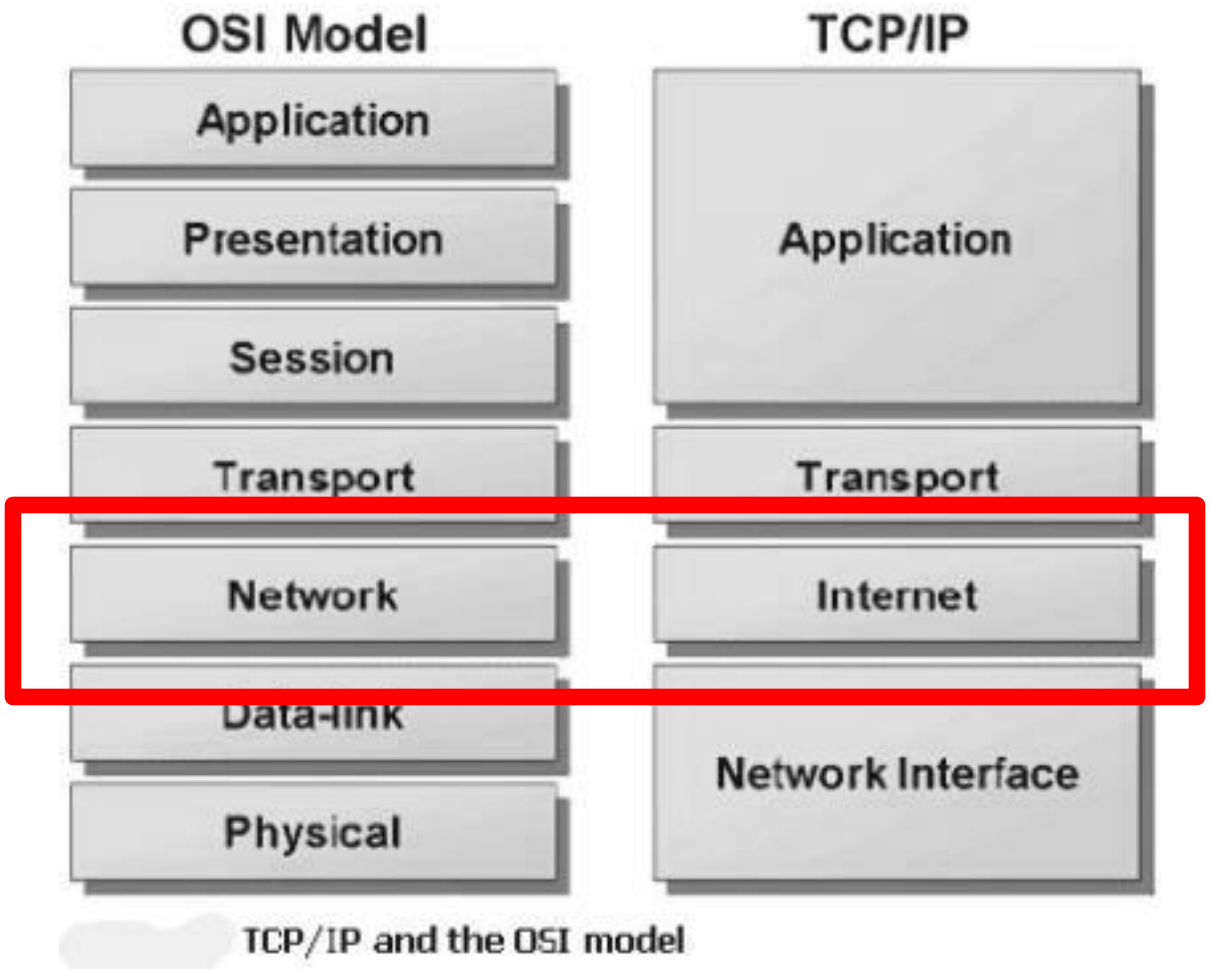
لایه IP در مدل TCP/IP

تهیه و تنظیم:

دکتر سیدرضا کامل

دیدگاه های نرم افزاری شبکه

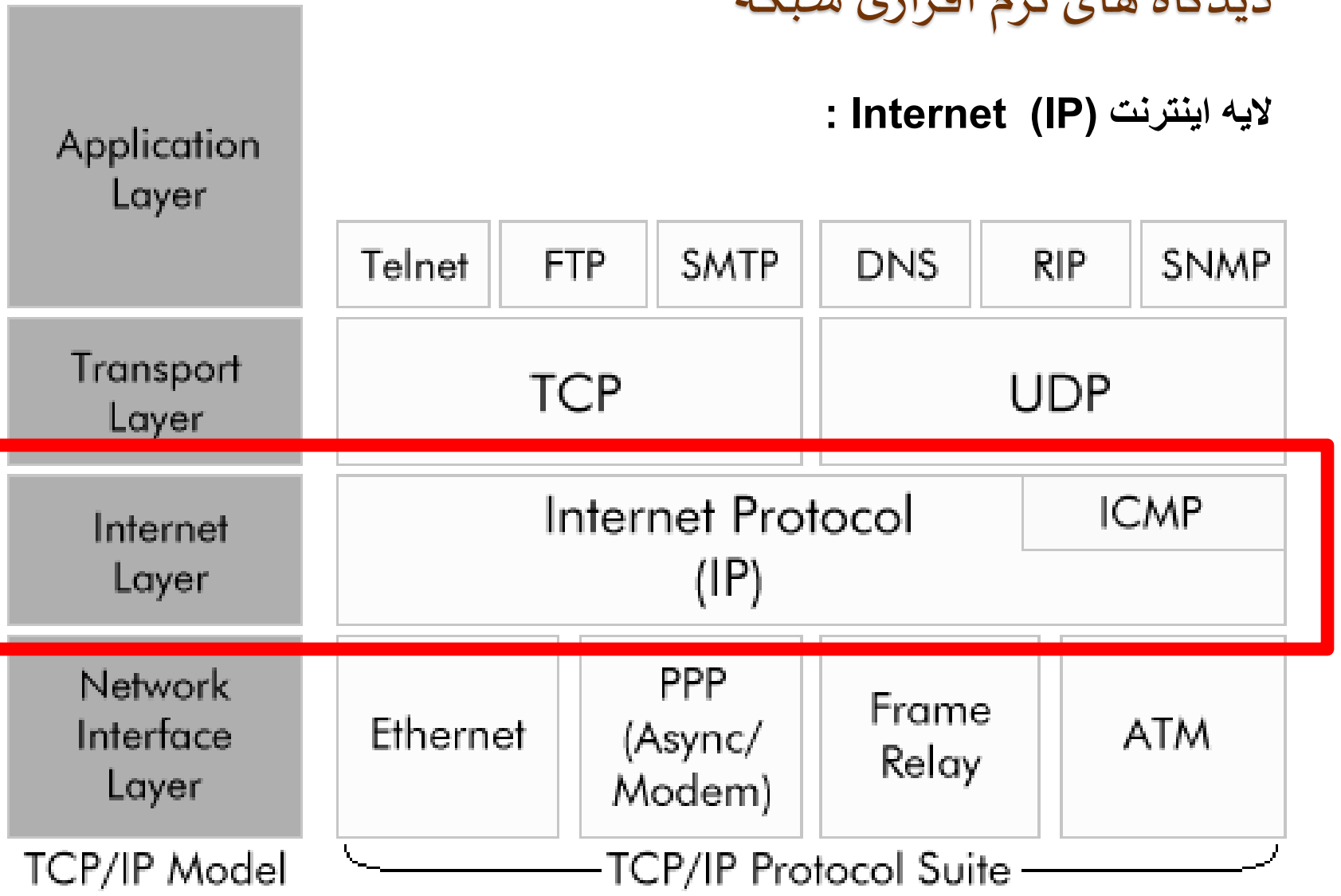
مدل مرجع TCP/IP :



TCP/IP and the OSI model

دیدگاه های نرم افزاری شبکه

لایه اینترنت (IP) Internet :

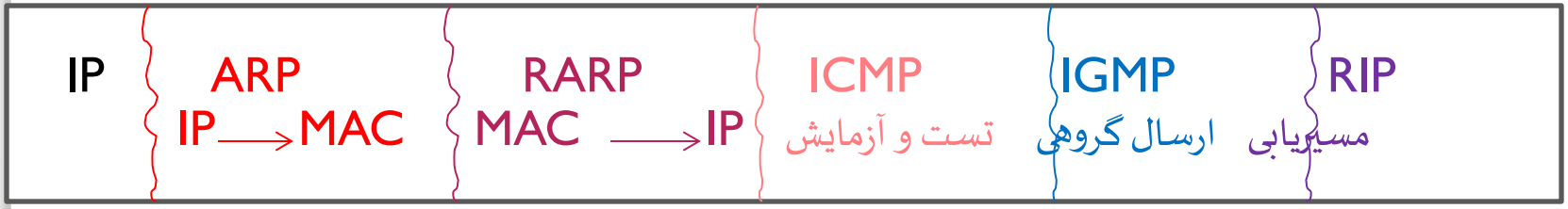


دیدگاه های نرم افزاری شبکه

لایه اینترنت (IP) Internet :

ساختار این لایه در شکل زیر نمایش داده شده که به معرفی پروتکل های مهم این لایه می پردازیم:

ساختار لایه IP در مدل TCP/IP و پروتکل های مهم آن



دیدگاه های نرم افزاری شبکه

سایر مفاهیم مرتبط با آدرس های IP:

- آدرس های معتبر و غیر معتبر
- مفاهیم NAT, Proxy و VPN

دیدگاه های نرم افزاری شبکه

سایر مفاهیم مرتبط با آدرس های IP:

- آدرس های معتبر و غیر معتبر
- مفاهیم NAT, Proxy و VPN

To convert invalid IP addresses to valid IP addresses:

- NAT
- Proxy
- Tunneling
- …

دیدگاه های نرم افزاری شبکه

سایر مفاهیم مرتبط با آدرس های IP:

- آدرس های معتبر و غیر معتبر
- مفاهیم NAT, Proxy و VPN

To convert invalid IP addresses to valid IP addresses:

- NAT
- Proxy
- Tunneling
- …

Non-routable
On the Internet

Routable
On the Internet

دیدگاه های نرم افزاری شبکه

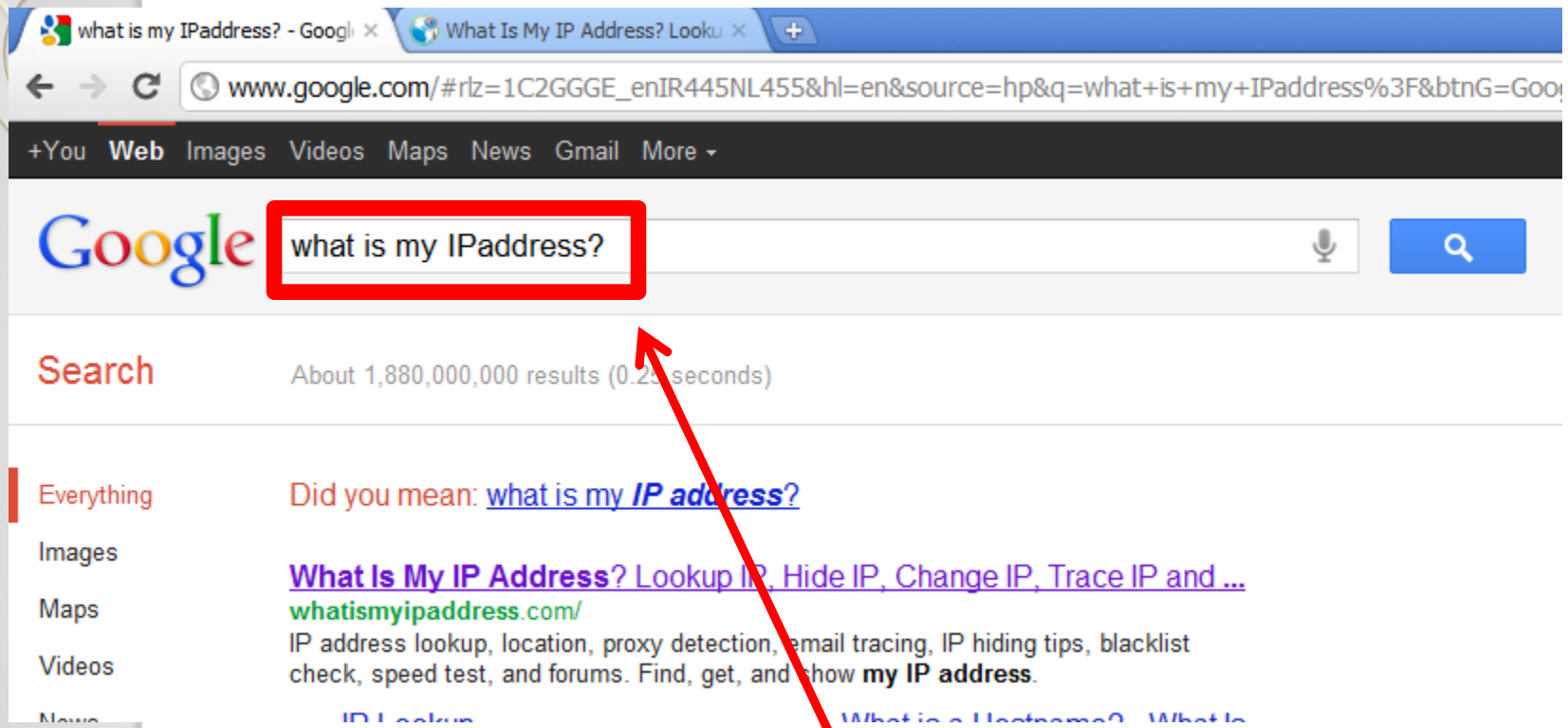
سایر مفاهیم مرتبط با آدرس های IP:

- آدرس های معتبر و غیر معتبر
- مفاهیم NAT, Proxy و VPN

To convert invalid IP addresses to valid IP addresses:

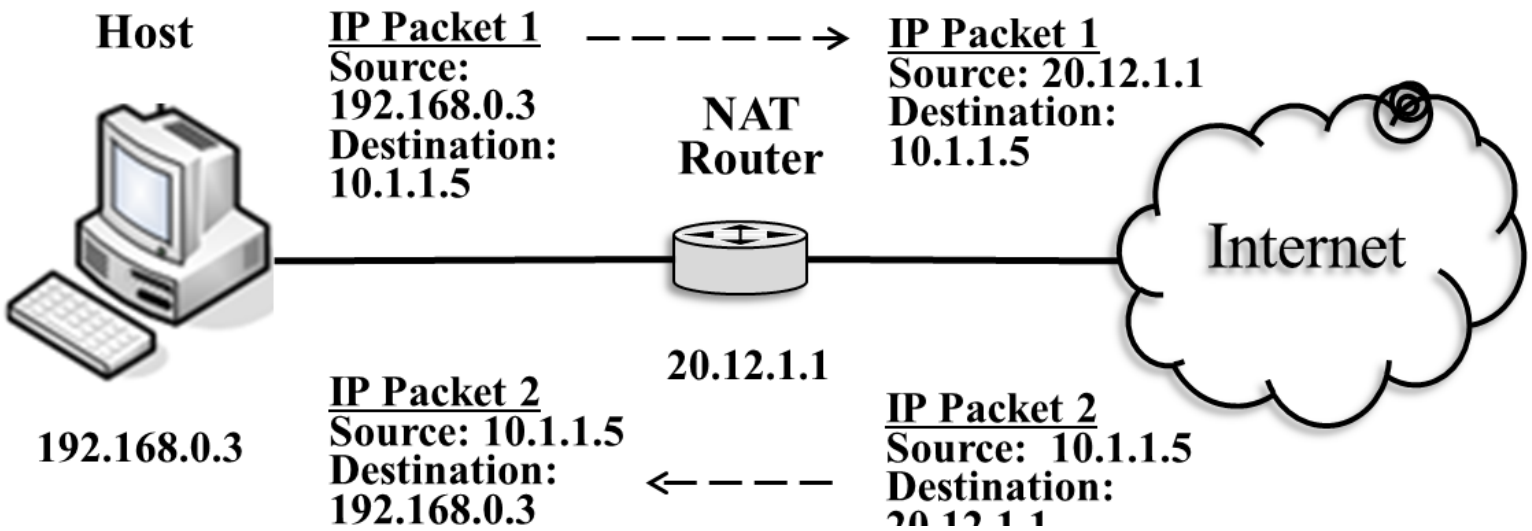
- NAT
- Proxy
- Tunneling
- ...

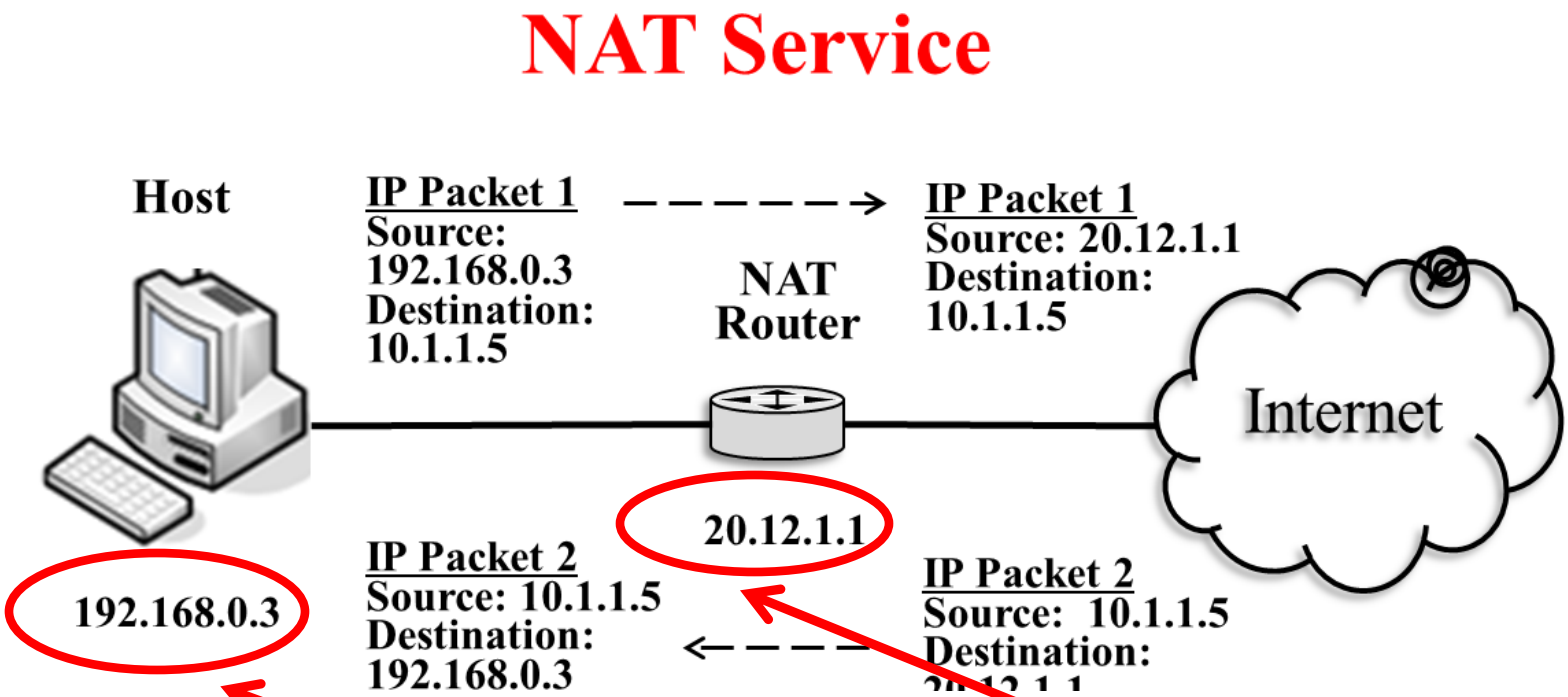
NAT



So, What is my valid IP Address?

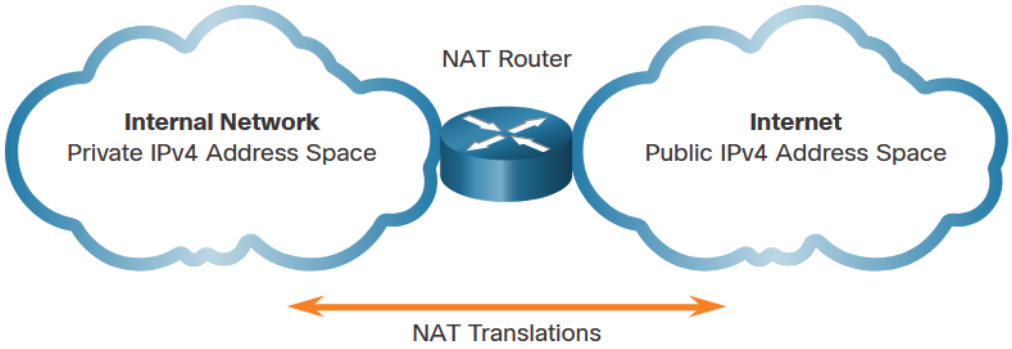
NAT Service


Host
IP Packet 1
Source:
192.168.0.3
Destination:
10.1.1.5
NAT
Router
IP Packet 1
Source: 20.12.1.1
Destination:
10.1.1.5
Internet
20.12.1.1
192.168.0.3
IP Packet 2
Source: 10.1.1.5
Destination:
192.168.0.3
IP Packet 2
Source: 10.1.1.5
Destination:



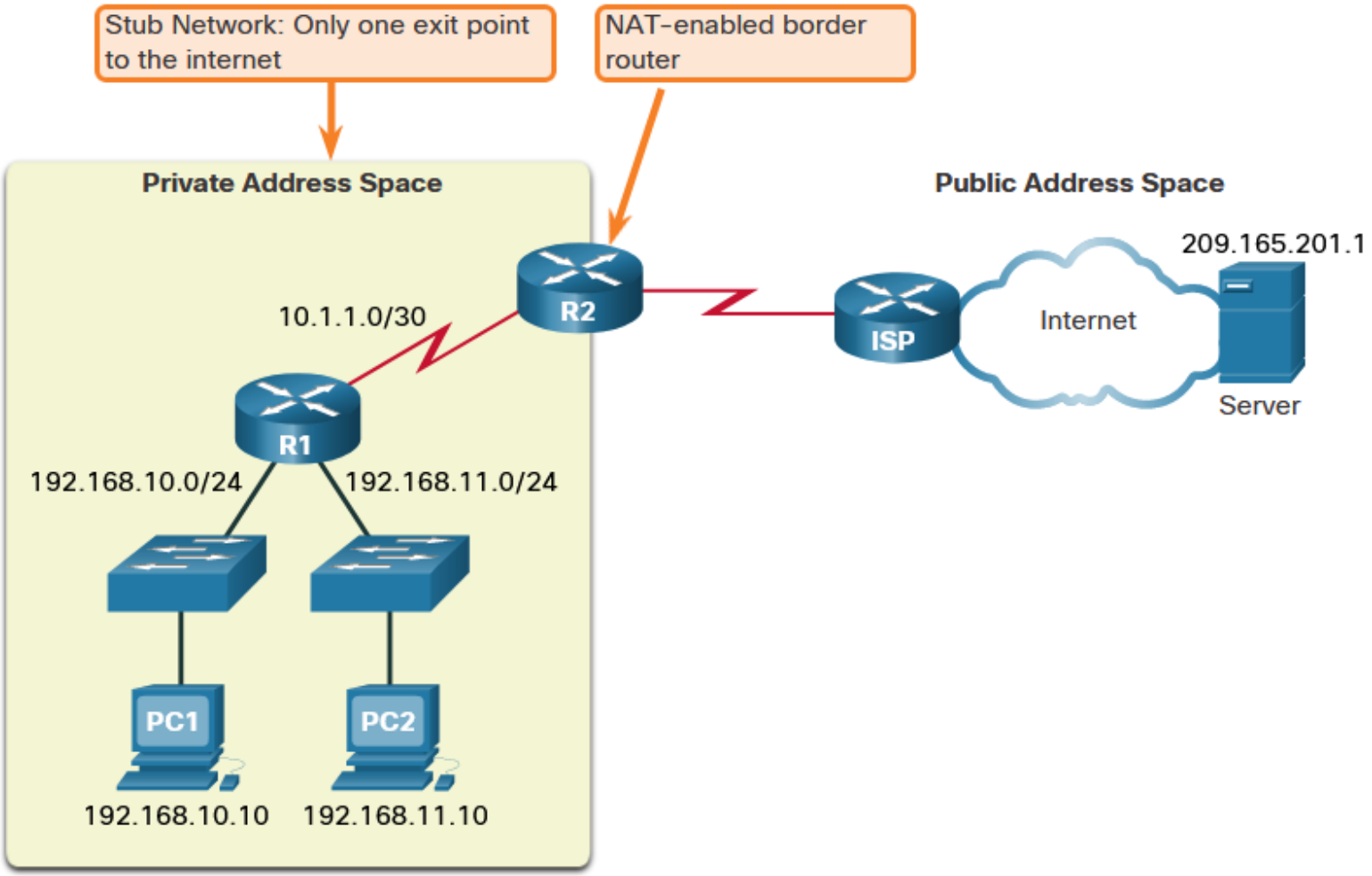
To convert invalid IP addresses to valid IP addresses:

NAT



Class	Private Addresses	Classes
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

NAT


Stub Network: Only one exit point to the internet
NAT-enabled border router
Private Address Space
Public Address Space
209.165.201.1
10.1.1.0/30
R2
ISP
Internet
Server
R1
192.168.10.0/24
192.168.11.0/24
PC1
PC2
192.168.10.10
192.168.11.10

NAT

NAT includes four types of addresses:

- Inside local address
- Inside global address
- Outside local address
- Outside global address

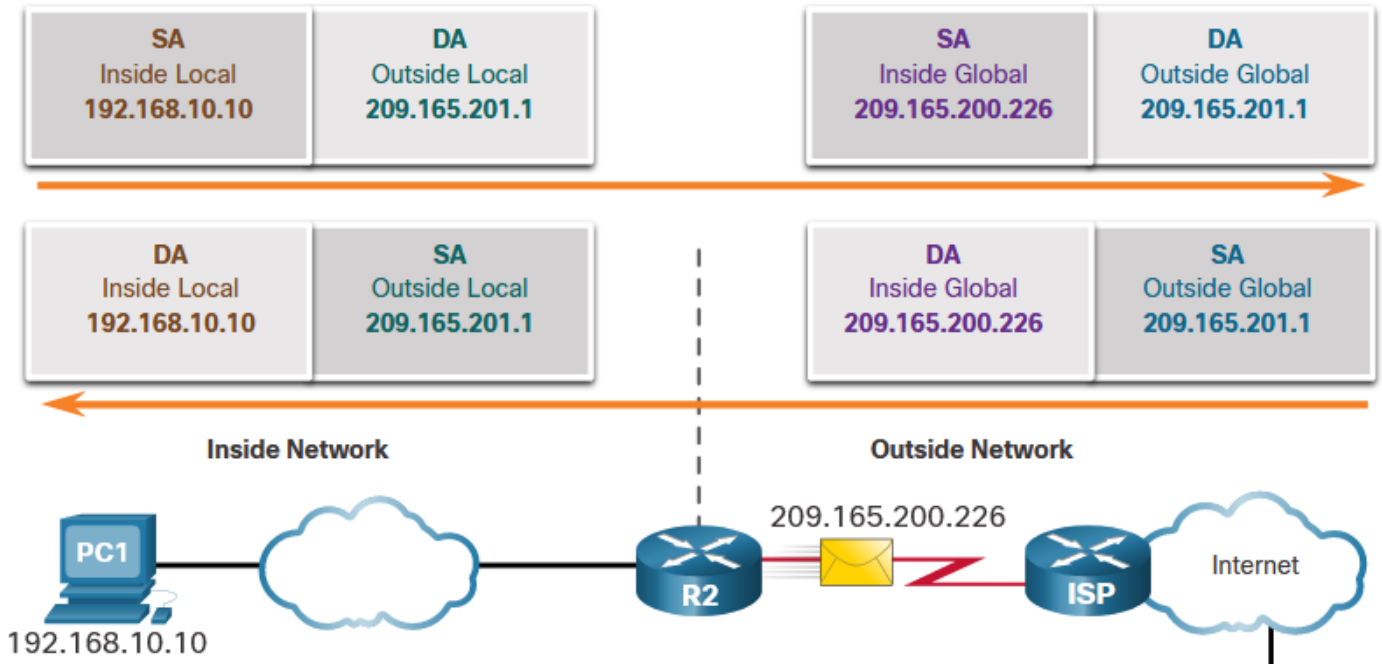
NAT terminology is always applied from the perspective of the device with the translated address:

- **Inside address** - The address of the device which is being translated by NAT.
- **Outside address** - The address of the destination device.
- **Local address** - A local address is any address that appears on the inside portion of the network.
- **Global address** - A global address is any address that appears on the outside portion of the network.

NAT

- **Inside local address**
- The address of the source as seen from inside the network. This is typically a private IPv4 address. The inside local address of PC1 is 192.168.10.10.
- **Inside global addresses**
- The address of source as seen from the outside network. The inside global address of PC1 is 209.165.200.226
- **Outside global address**
- The address of the destination as seen from the outside network. The outside global address of the web server is 209.165.201.1
- **Outside local address**
- The address of the destination as seen from the inside network. PC1 sends traffic to the web server at the IPv4 address 209.165.201.1. While uncommon, this address could be different than the globally routable address of the destination.

NAT



R2 NAT Table			
PC1		**Web Server**	
Inside Global Address	**Inside Local Address**	**Outside Local Address**	**Outside Global Address**
209.165.200.226	**192.168.10.10**	**209.165.201.1**	**209.165.201.1**

دیدگاه های نرم افزاری شبکه

انواع روش های NAT ....

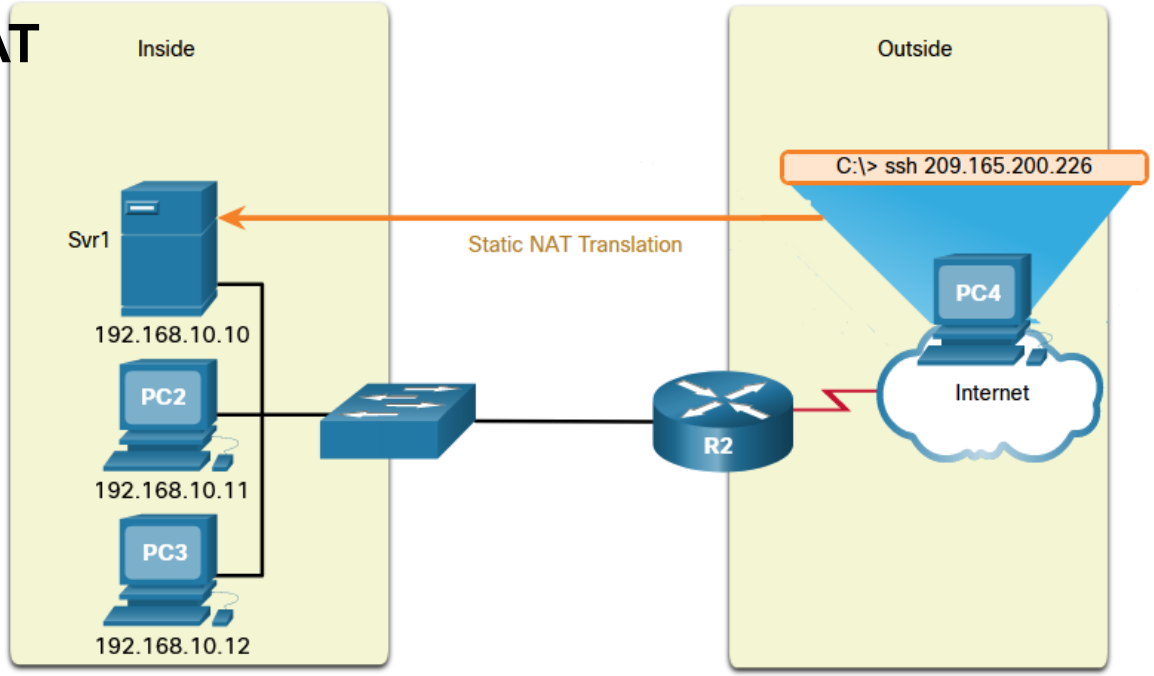
انواع روش های NAT ....

STATIC NAT

- Static NAT uses a one-to-one mapping of local and global addresses configured by the network administrator that remain constant.
- Static NAT is useful for web servers or devices that must have a consistent address that is accessible from the internet, such as a company web server.
- It is also useful for devices that must be accessible by authorized personnel when offsite, but not by the general public on the internet.

انواع روش های NAT ....

STATIC NAT



Static NAT Table	
Inside Local Address	**Inside Global Address - Addresses reachable via R2**
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

انواع روش های NAT ....

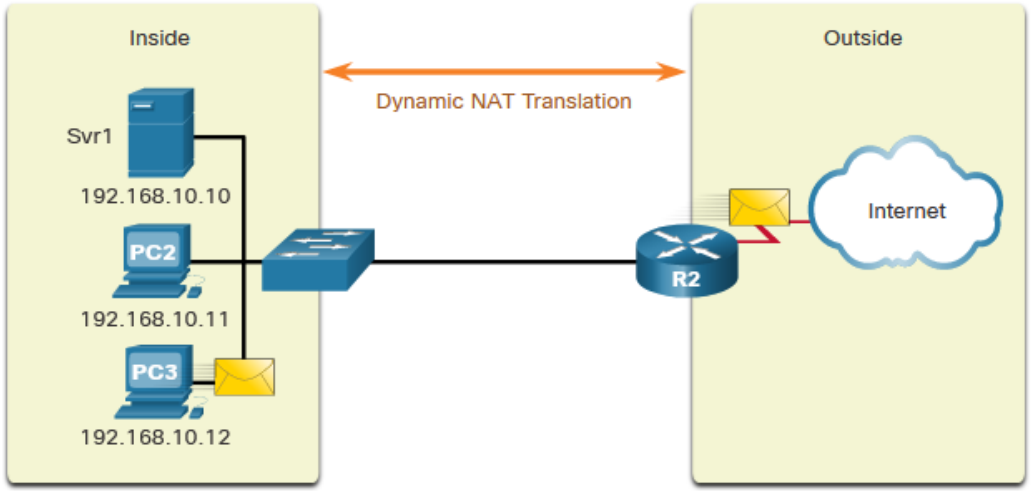
DYNAMIC NAT

- Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis.
- When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool.
- The other addresses in the pool are still available for use.

Note: Dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.

انواع روش های NAT ....

DYNAMIC NAT



IPv4 NAT Pool	
Inside Local Address	**Inside Global Address Pool - Addresses reachable via R2**
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

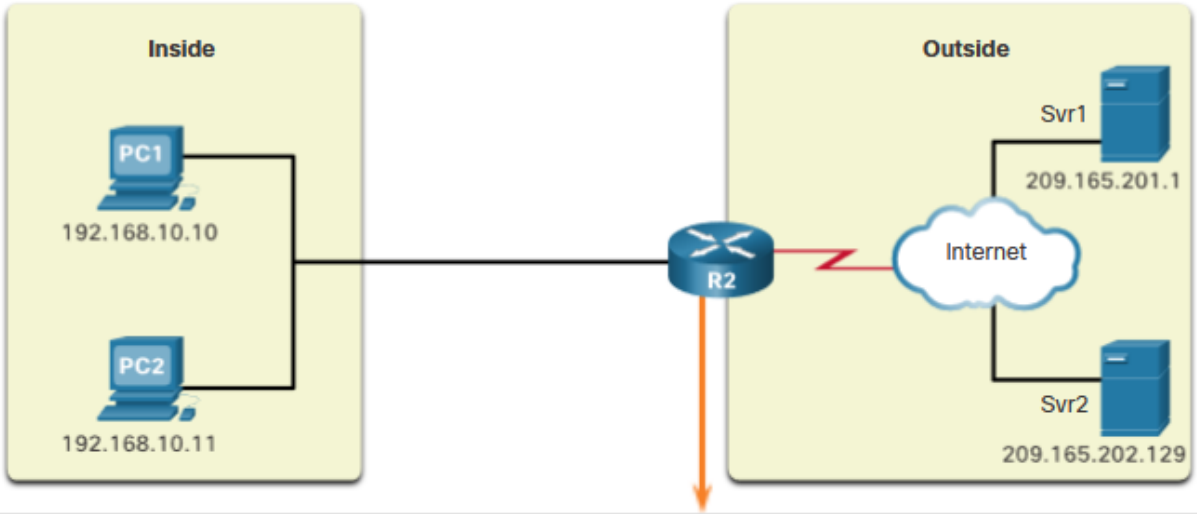
انواع روش های NAT ....

Port Address Translation

- Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses
- With PAT, when the NAT router receives a packet from the client, it uses the source port number to uniquely identify the specific NAT translation
- PAT ensures that devices use a different TCP port number for each session with a server on the internet.

انواع روش های NAT ....

Port Address Translation



NAT Table with Overload

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

انواع روش های NAT ....

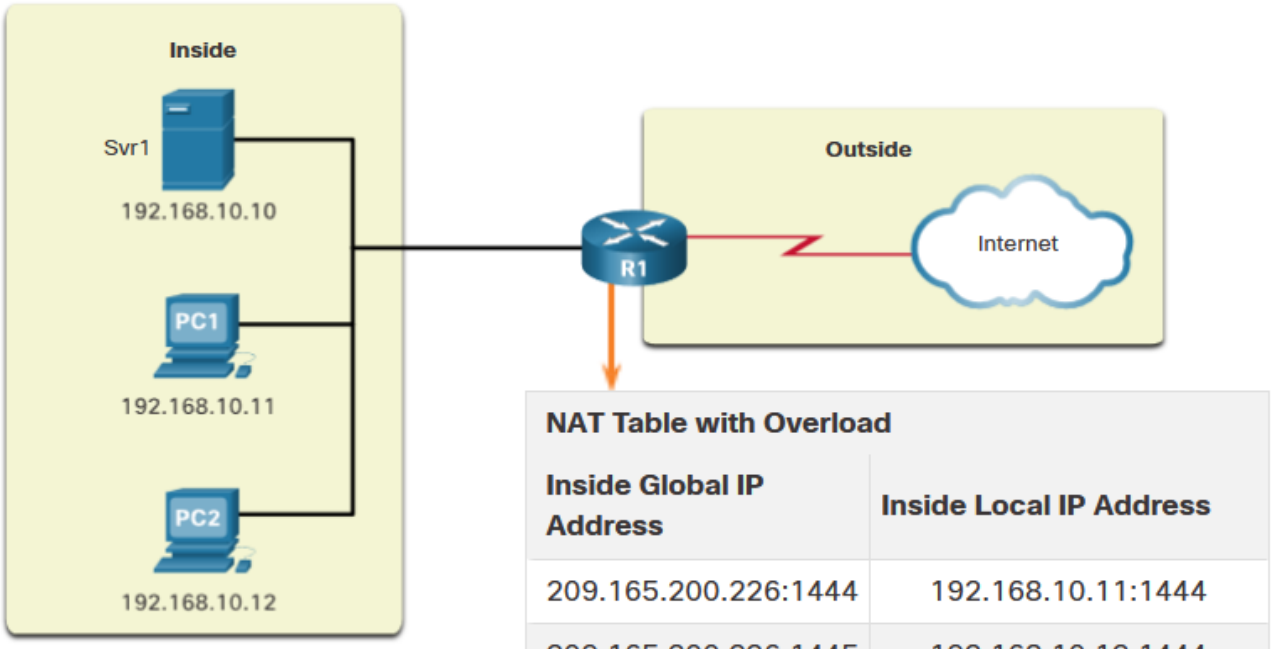
Port Address Translation

- Next Available Port
  - PAT attempts to preserve the original source port. If the original source port is already used, PAT assigns the first available port number starting from the beginning of the appropriate port group 0-511, 512-1,023, or 1,024-65,535.
  - When there are no more ports available and there is more than one external address in the address pool, PAT moves to the next address to try to allocate the original source port.
  - The process continues until there are no more available ports or external IPv4 addresses in the address pool.

انواع روش های NAT ....

Port Address Translation

- Next Available Port



NAT Table with Overload

Inside Global IP Address	Inside Local IP Address
209.165.200.226:1444	192.168.10.11:1444
209.165.200.226:1445	192.168.10.12:1444

مقایسه روش های NAT و PAT ....

Summary of the differences between NAT and PAT.

NAT - Only modifies the IPv4 addresses

Inside Global Address	Inside Local Address
209.165.200.226	192.168.10.10

PAT - PAT modifies both the IPv4 address and the port number.

Inside Global Address	Inside Local Address
209.165.200.226:2031	192.168.10.10:2031

NAT	PAT
One-to-one mapping between Inside Local and Inside Global addresses.	One Inside Global address can be mapped to many Inside Local addresses.
Uses only IPv4 addresses in translation process.	Uses IPv4 addresses and TCP or UDP source port numbers in translation process.
A unique Inside Global address is required for each inside host accessing the outside network.	A single unique Inside Global address can be shared by many inside hosts accessing the outside network.

دیدگاه های نرم افزاری شبکه

سایر مفاهیم مرتبط با آدرس های IP:

- آدرس های معتبر و غیر معتبر
- مفاهیم NAT, Proxy و VPN

To convert invalid IP addresses to valid IP addresses:

- NAT
- Proxy
- Tunneling
- ...

دیدگاه های نرم افزاری شبکه

سایر مفاهیم مرتبط با آدرس های IP:

- آدرس های معتبر و غیر معتبر
- مفاهیم NAT, Proxy و VPN

To convert invalid IP addresses to valid IP addresses:

- NAT
- Proxy
- Tunneling (VPN)
- ...

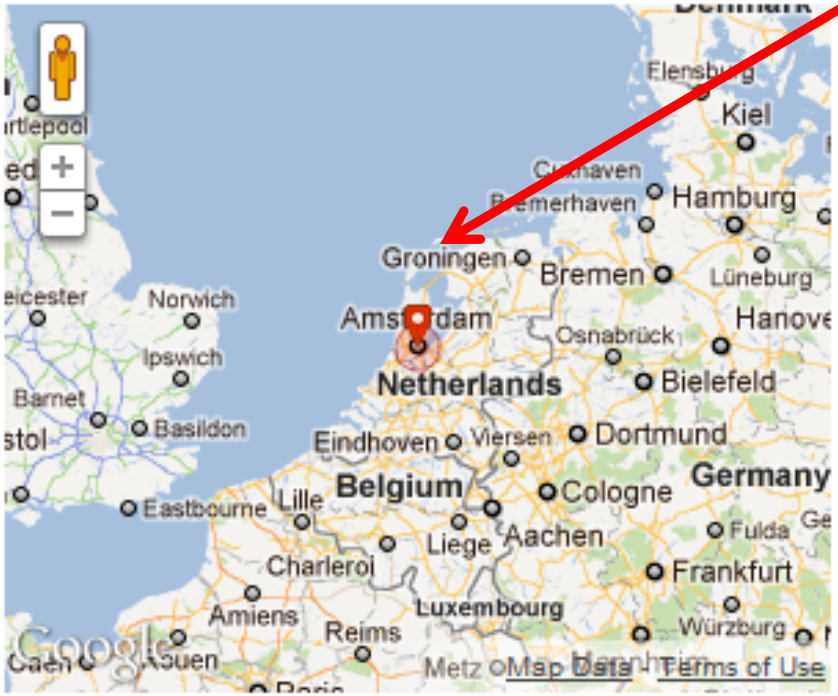
VPN

I am
HERE
In the world

What Is My IP Address? Looku ×

ddress.com

What Is My IP Address? (Now detects many proxy servers)



IP Information: 83.149.126.32

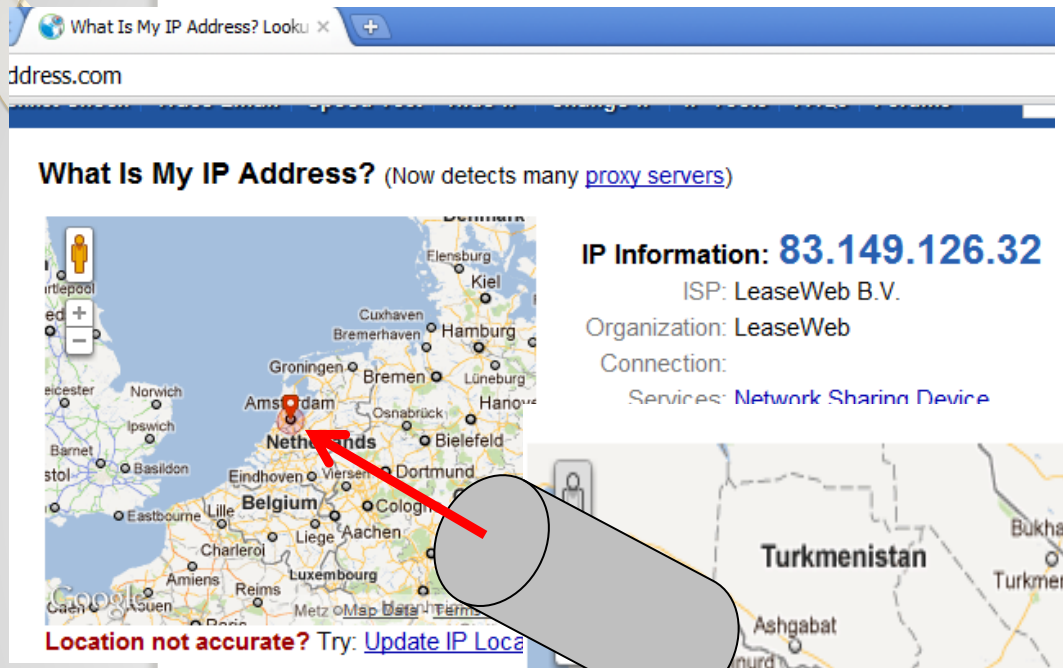
ISP: LeaseWeb B.V.
Organization: LeaseWeb
Connection:
Services: Network Sharing Device
City: Amsterdam
Region: Noord-Holland
Country: Netherlands

83.149.126.32 Additional IP D

Location not accurate? Try: Update IP Location

VPN

دیدگاه های نرم افزاری شبکه



IP Information: 31.25.88.189

ISP: Toos-Ashena Co. Ltd.
Organization: Toos-Ashena Co. Ltd.
Connection:
Services: None Detected
City: Mashhad
Region: Khorasan
Country: Iran, Islamic Republic of

31.25.88.189 Additional I

Tunneling

دیدگاه های نرم افزاری شبکه

پروتکل شفاف سازی آدرس ها

ARP: Address Resolution Protocol

دیدگاه های نرم افزاری شبکه

پروتکل شفاف سازی آدرس ها

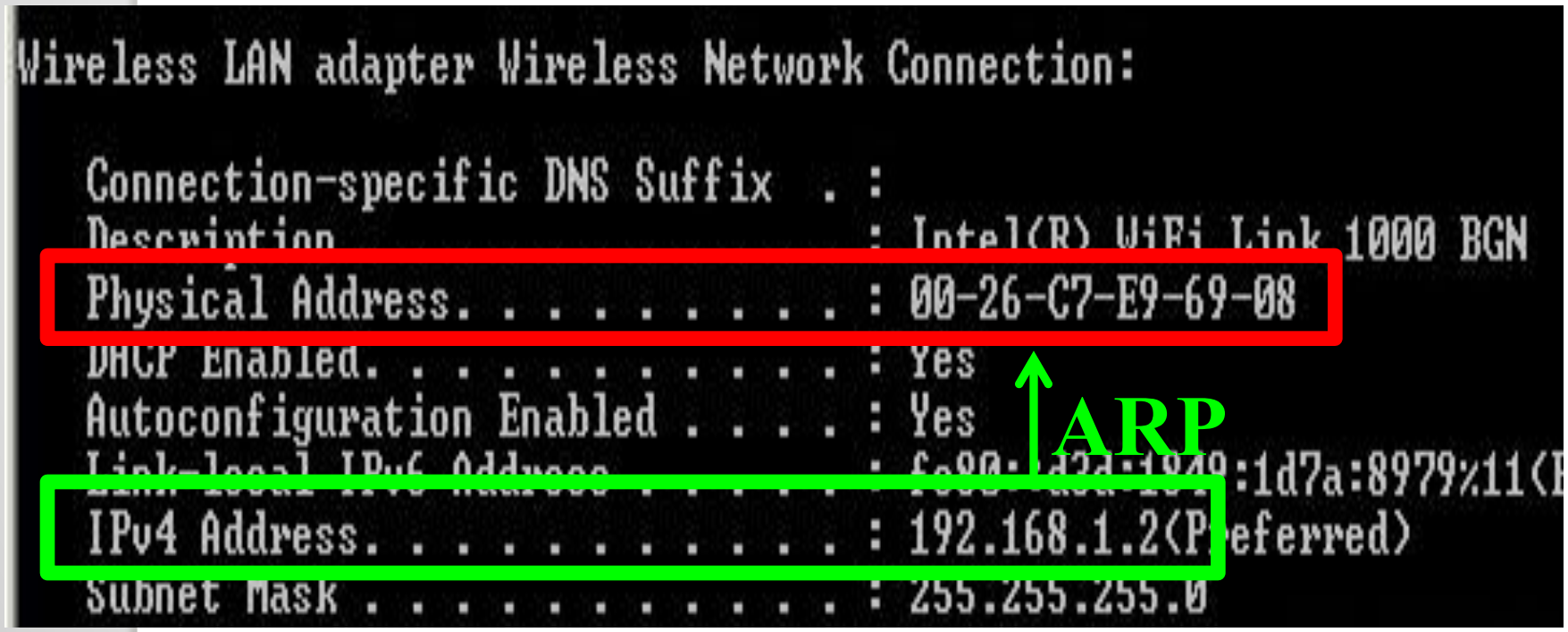
ARP: Address Resolution Protocol

- از این پروتکل برای تحویل بسته های IP به مقصد نهایی استفاده می شود زیرا بسته از مبدأ به مقصد تمام مسیر طولانی را با آدرس IP طی می کند تا به آخرین مسیریاب برسد در این هنگام این مسیریاب باید علاوه بر داشتن آدرس IP ، آدرس سخت افزاری مقصد بسته را نیز بداند. زیرا باید در شبکه نهایی فریمی به آدرس فیزیکی مقصد نهایی ساخته شود و بسته در آن قرار بگیرد تا تحویل تجهیزات لایه دویی شود.
- به کمک این مسیریاب، با داشتن آدرس IP، آدرس MAC مقصد را از شبکه جستجو می کند.

دیدگاه های نرم افزاری شبکه

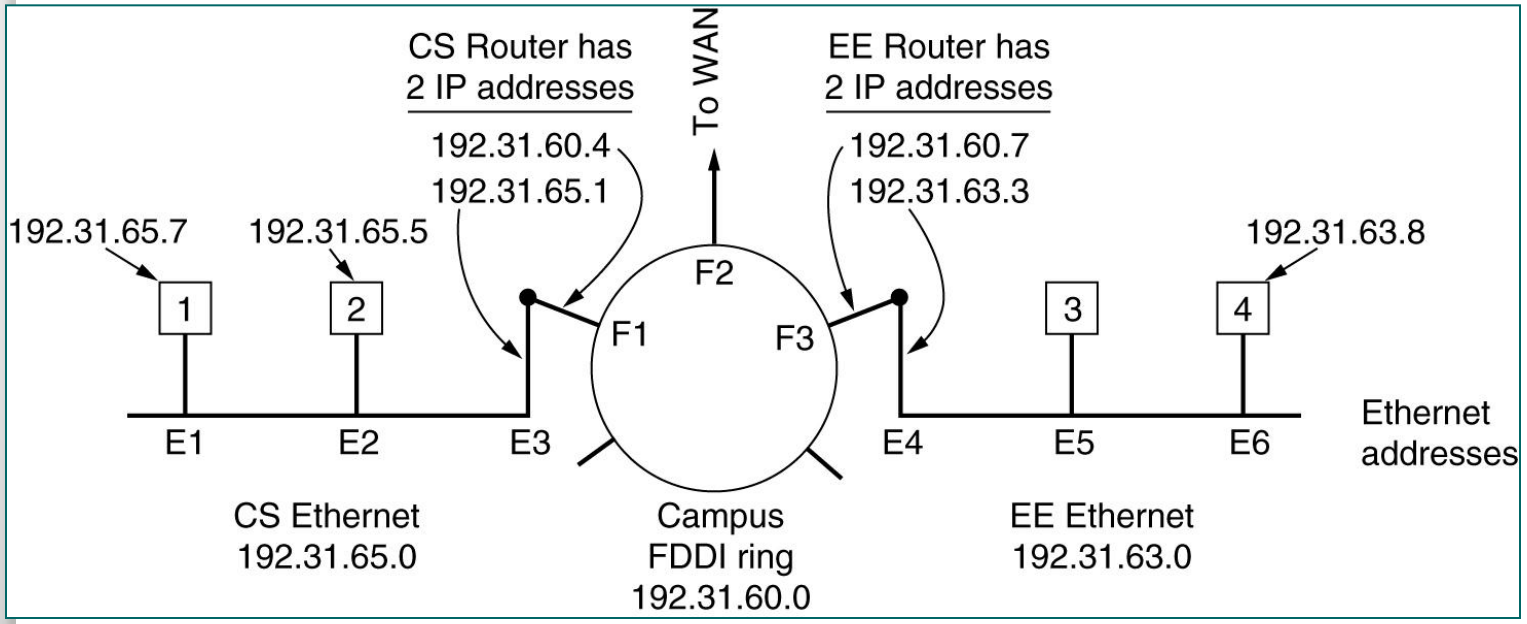
پروتکل شفاف سازی آدرس ها

ARP: Address Resolution Protocol

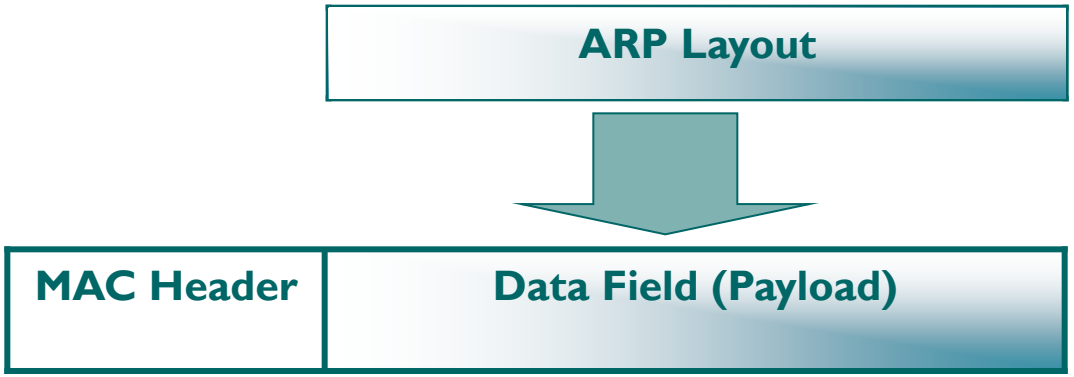


پروتکل ARP : Address Resolution Protocol

- بی‌معنابودن آدرسهای IP روی کانال انتقال
- دانستن آدرس IP ماشین مقصد و نیاز به داشتن آدرس فیزیکی آن جهت ارسال بسته
- وظیفه پروتکل ARP:
- ارسال بسته فراگیر روی کل شبکه محلی که در آن آدرس IP ماشین مورد نظر قرار دارد. پاسخ ماشین با آدرس IP موجود در بسته ارسالی و ارسال آدرس فیزیکی خود برای ارسال‌کننده بسته ARP

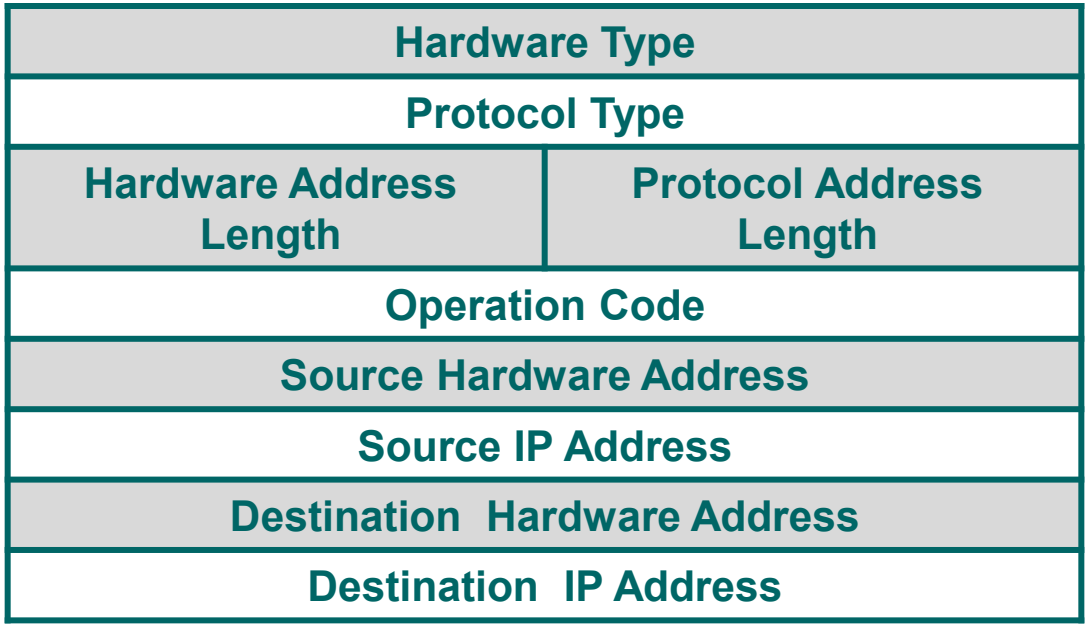


برخلاف پروتکل **ICMP** که روی پروتکل **IP** قرار می‌گیرد ، پروتکل **ARP** مستقیماً بر روی **پروتکل لایهٔ فیزیکی** عمل می‌کند؛ یعنی یک بستهٔ **ARP** ساخته شده و درون فیلد داده از فریم لایهٔ فیزیکی قرار گرفته و روی کانال ارسال می‌شود .



چگونگی قرار گرفتن یک پیام**ARP** درون فریم لایهٔ فیزیکی

ساختار پیامهای ARP



دیدگاه های نرم افزاری شبکه

معکوس پروتکل شفاف سازی آدرس

RARP: Revers Address Resolution Protocol

دیدگاه های نرم افزاری شبکه

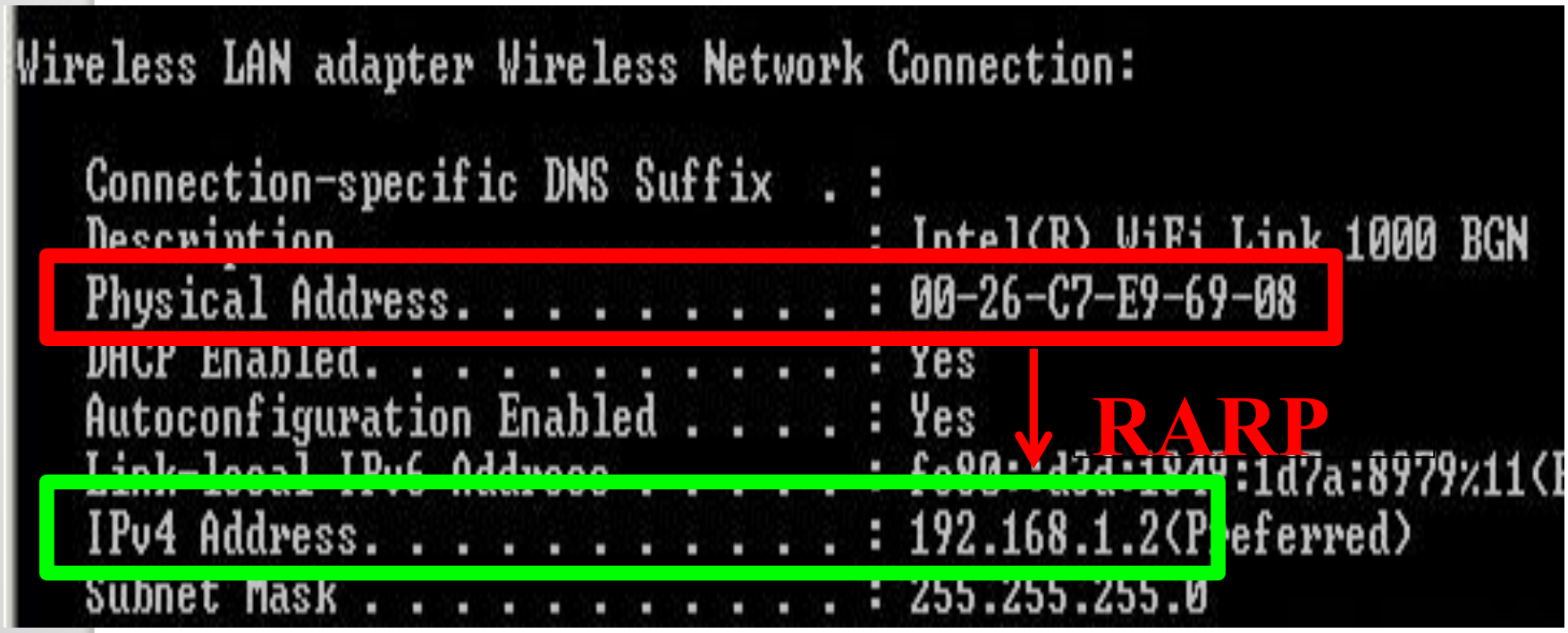
معکوس پروتکل شفاف سازی آدرس
RARP: Revers Address Resolution Protocol

- این پروتکل برعکس پروتکل قبلی عمل می کند بدین معنی که اگر آدرس MACرا داشته باشیم ، می توانیم آدرس IP را از شبکه بپرسیم.

دیدگاه های نرم افزاری شبکه

معکوس پروتکل شفاف سازی آدرس

RARP: Revers Address Resolution Protocol



پروتکل *RARP* : Reverse Address Resolution Protocol

- ایستگاه آدرس فیزیکی مورد نظرش را می‌داند ولیکن آدرس **IP** آن را نمی‌داند
- ارسال یک بسته فراگیر روی خط
- تمامی ایستگاههایی که از پروتکل **RARP** حمایت می‌کنند و بسته‌های مربوطه را تشخیص می‌دهند، در صورتی که آدرس فیزیکی خودشان را درون بسته ببینند در پاسخ به آن، آدرس **IP** خود را در قالب یک بستهٔ **RARP Reply** برمی‌گردانند.

توجه: بسته‌های **RARP, ARP** از نوع فراگیر محلی **Local Broadcast** هستند و بالطبع توسط مسیریابها منتقل نمی‌شوند و فقط در محدوده شبکه محلی عمل می‌کنند.

دیدگاه های نرم افزاری شبکه

پروتکل پروتکل پیغام کنترلی

ICMP: Internet Contorol Message Protocol

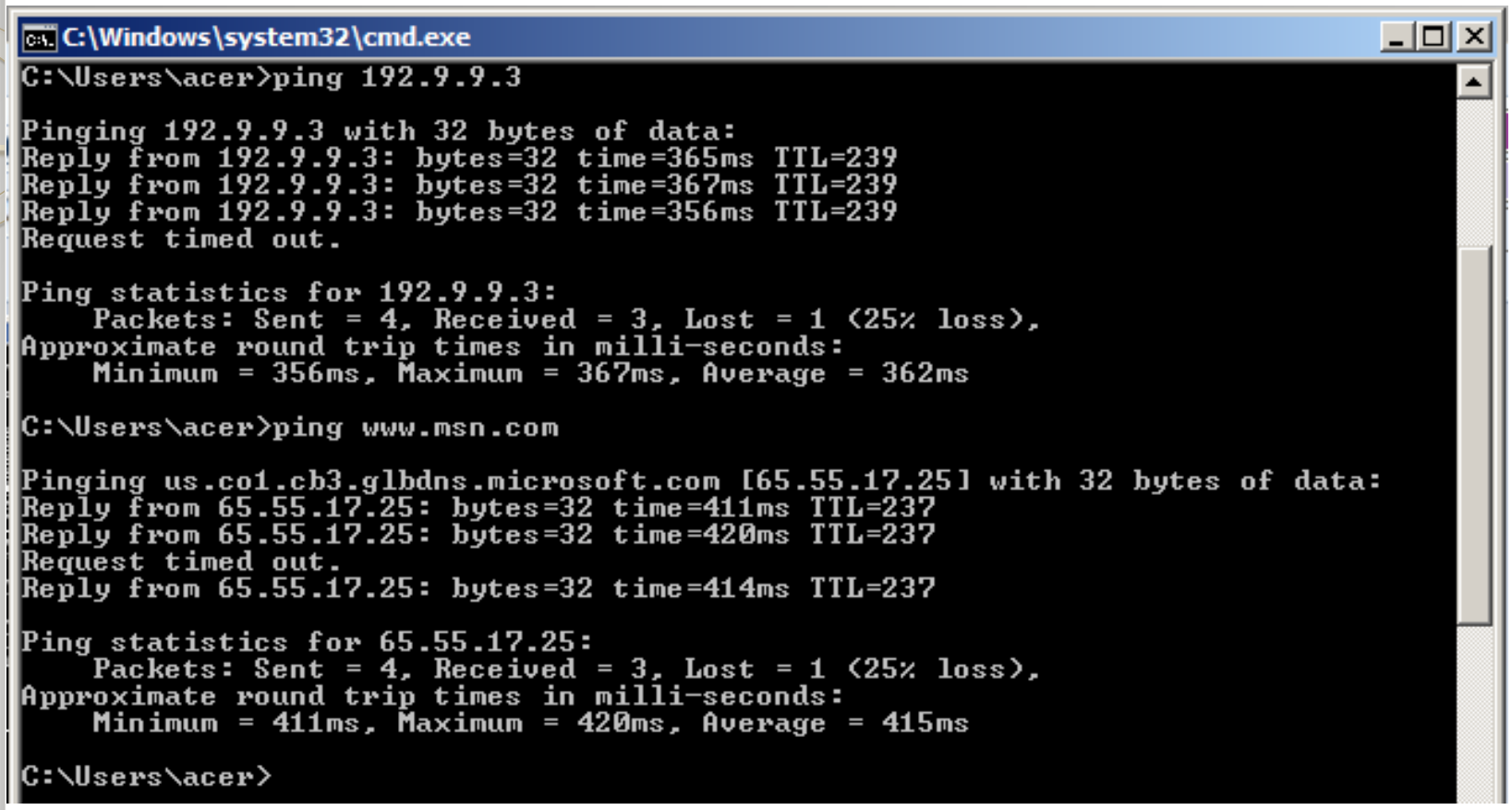
دیدگاه های نرم افزاری شبکه

پروتکل پروتکل پیغام کنترلی
ICMP: Internet Contorol Message Protocol

- از این پروتکل برای تست ارتباط بین میزبان ها استفاده می شود
- با استفاده از این پروتکل می توان وضعیت کیفیت ارتباط دو میزبان را بررسی کرد، شامل:
  - فاصله زمانی به میلی ثانیه (ms)
  - فاصله دو میزبان به تعداد پرش یا تعداد مسیریاب (Number of Hops)
  - نرخ گم شدگی بسته ها (Packet Loss)
  - و خطاهای احتمالی کانال

ICMP: Internet Contorol Message Protocol

دیدگاه های نرم افزاری شبکه

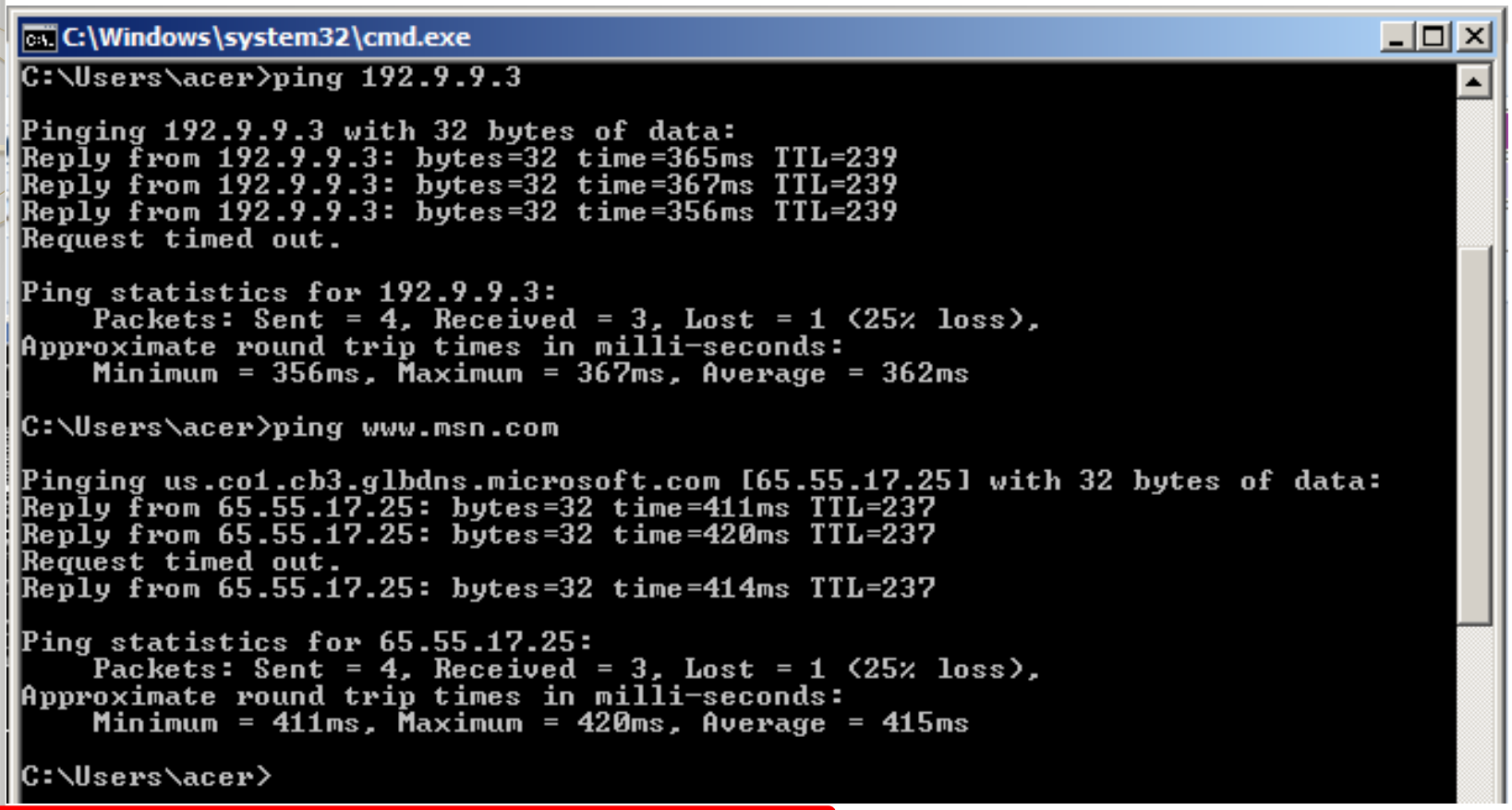


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

دیدگاه های نرم افزاری شبکه

ICMP: Internet Contorol Message Protocol

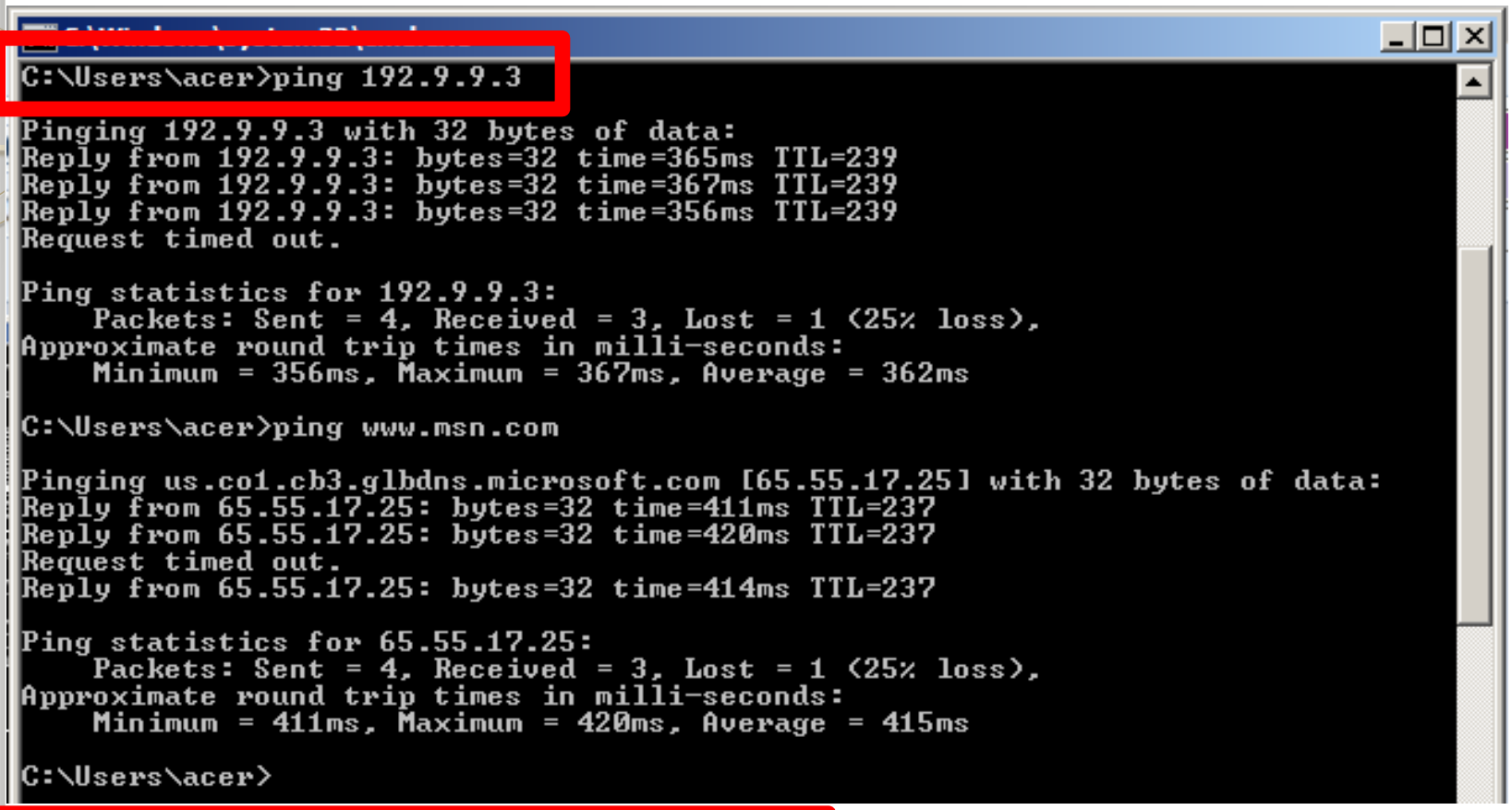


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

ICMP: Internet Contorol Message Protocol

دیدگاه های نرم افزاری شبکه

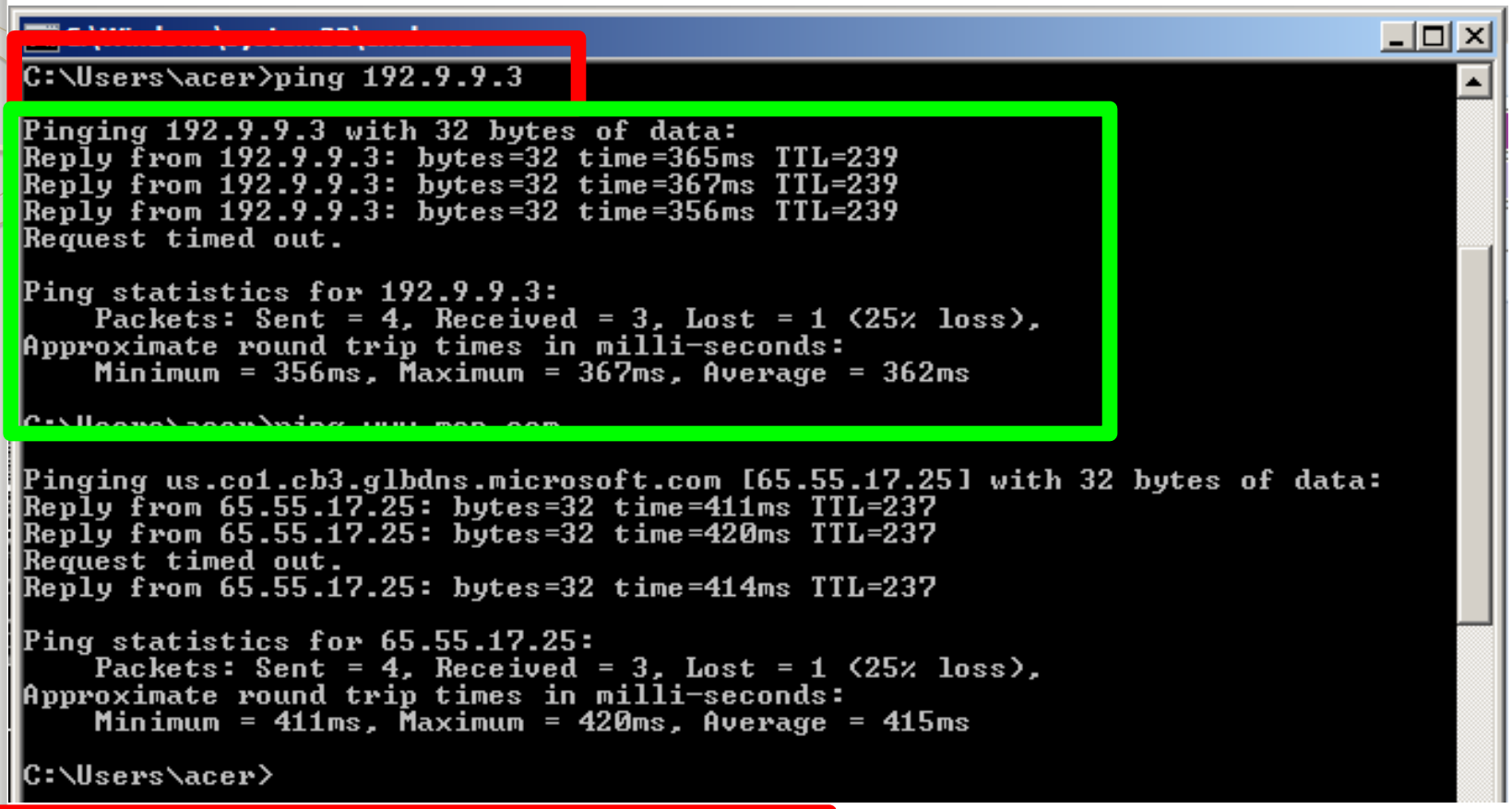


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

ICMP: Internet Contorol Message Protocol

دیدگاه های نرم افزاری شبکه

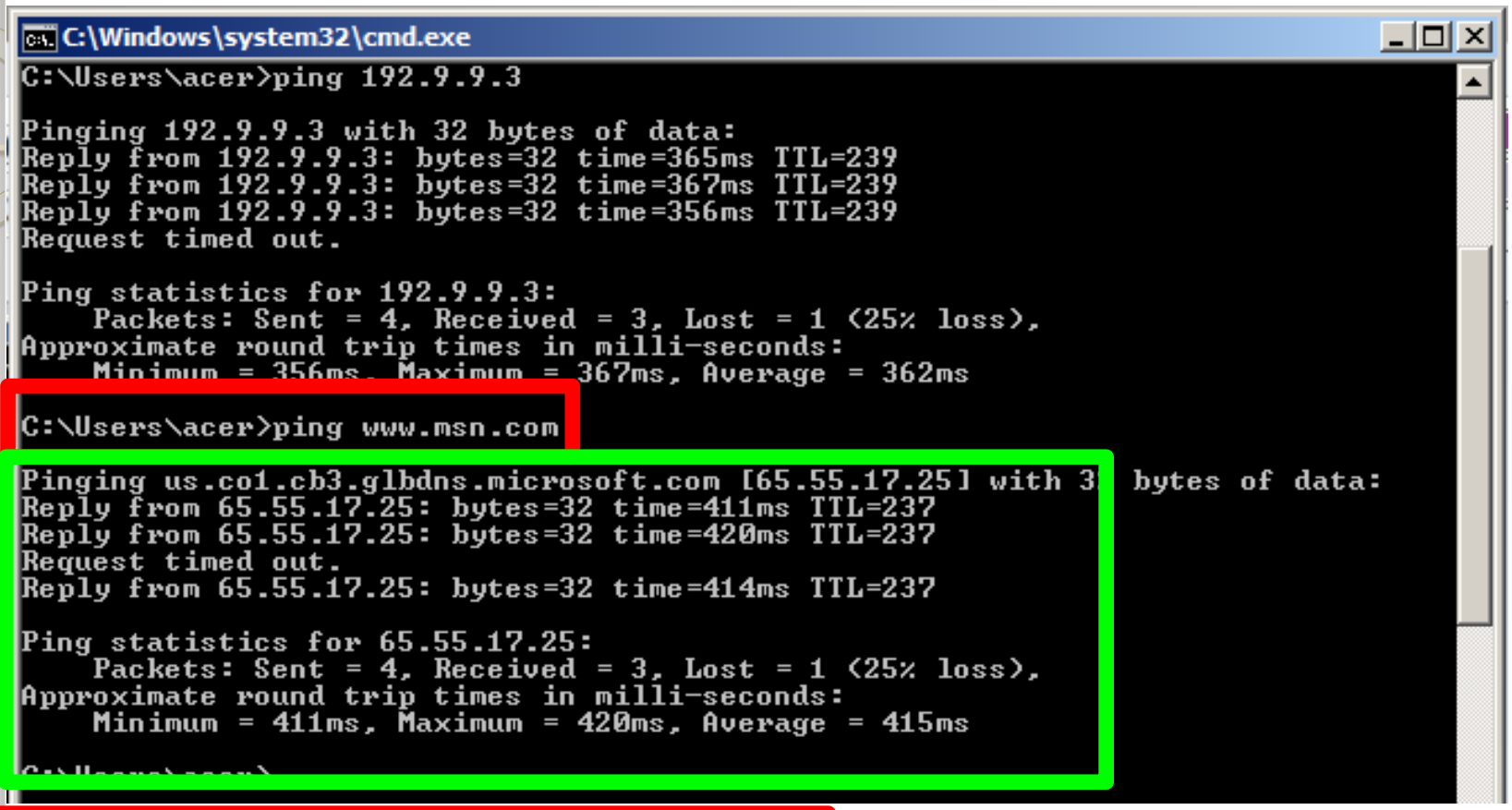


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

ICMP: Internet Contorol Message Protocol

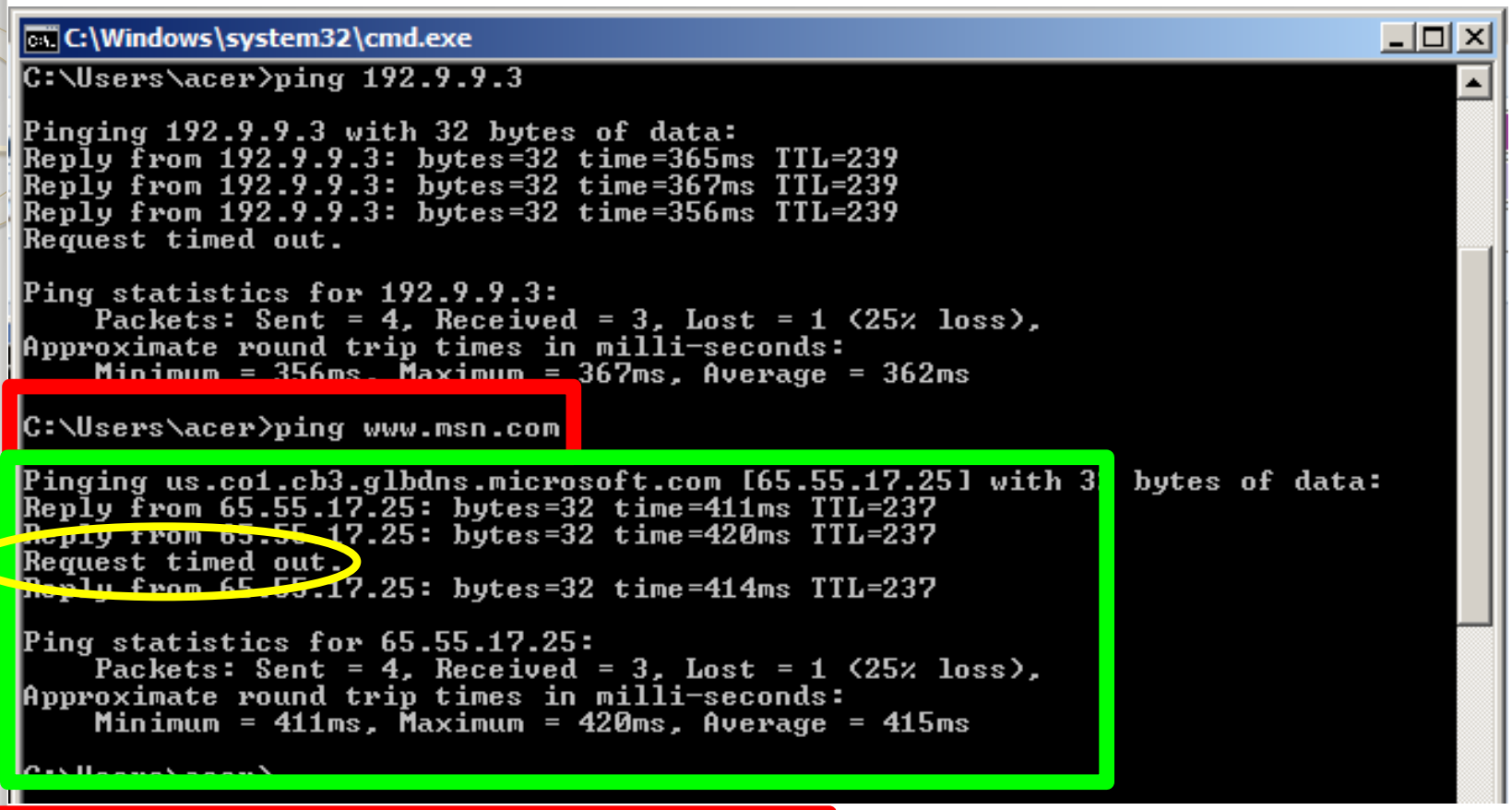
دیدگاه های نرم افزاری شبکه



C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

دیدگاه های نرم افزاری شبکه

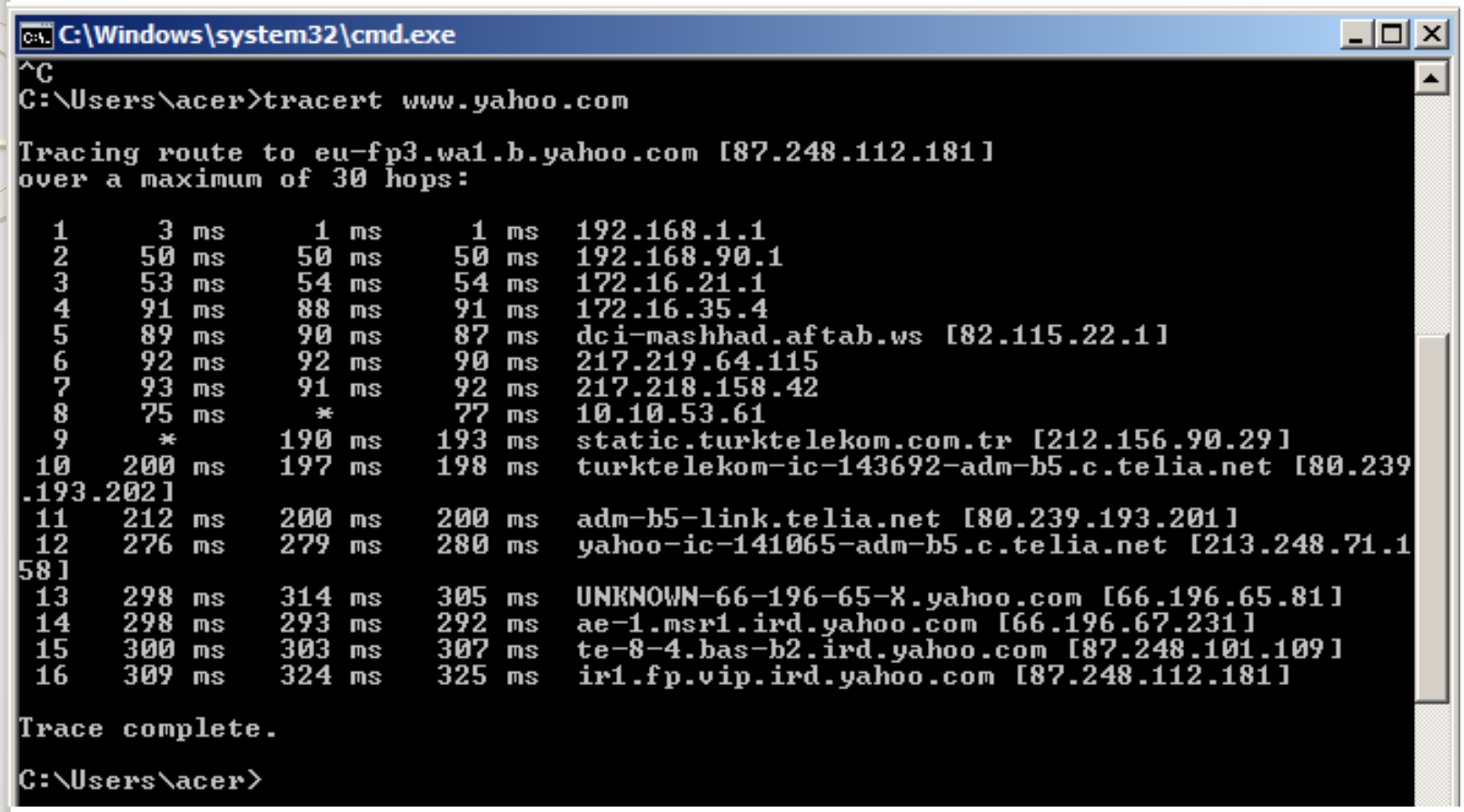


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

دیدگاه های نرم افزاری شبکه

ICMP: Internet Contorol Message Protocol

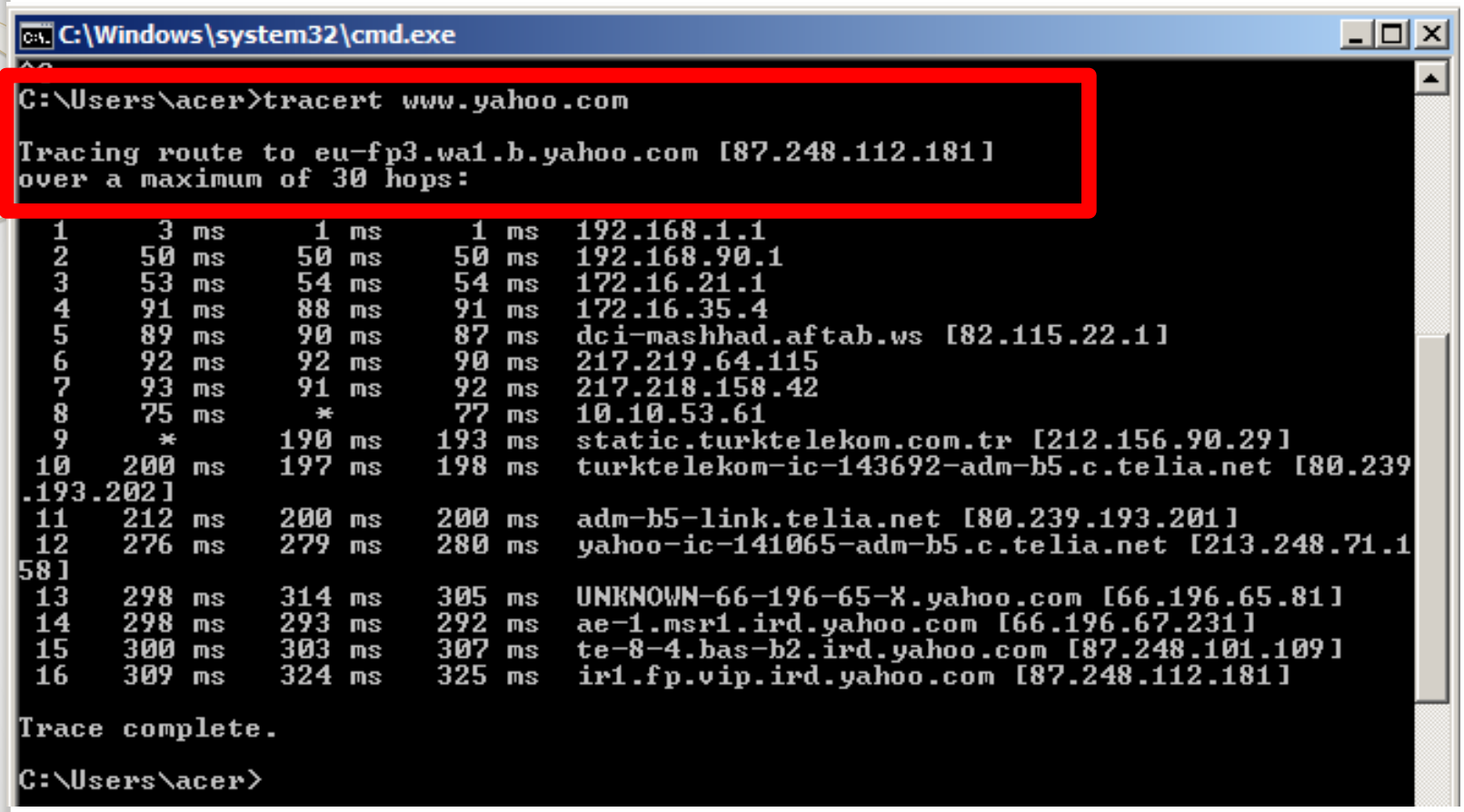


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

ICMP: Internet Contorol Message Protocol

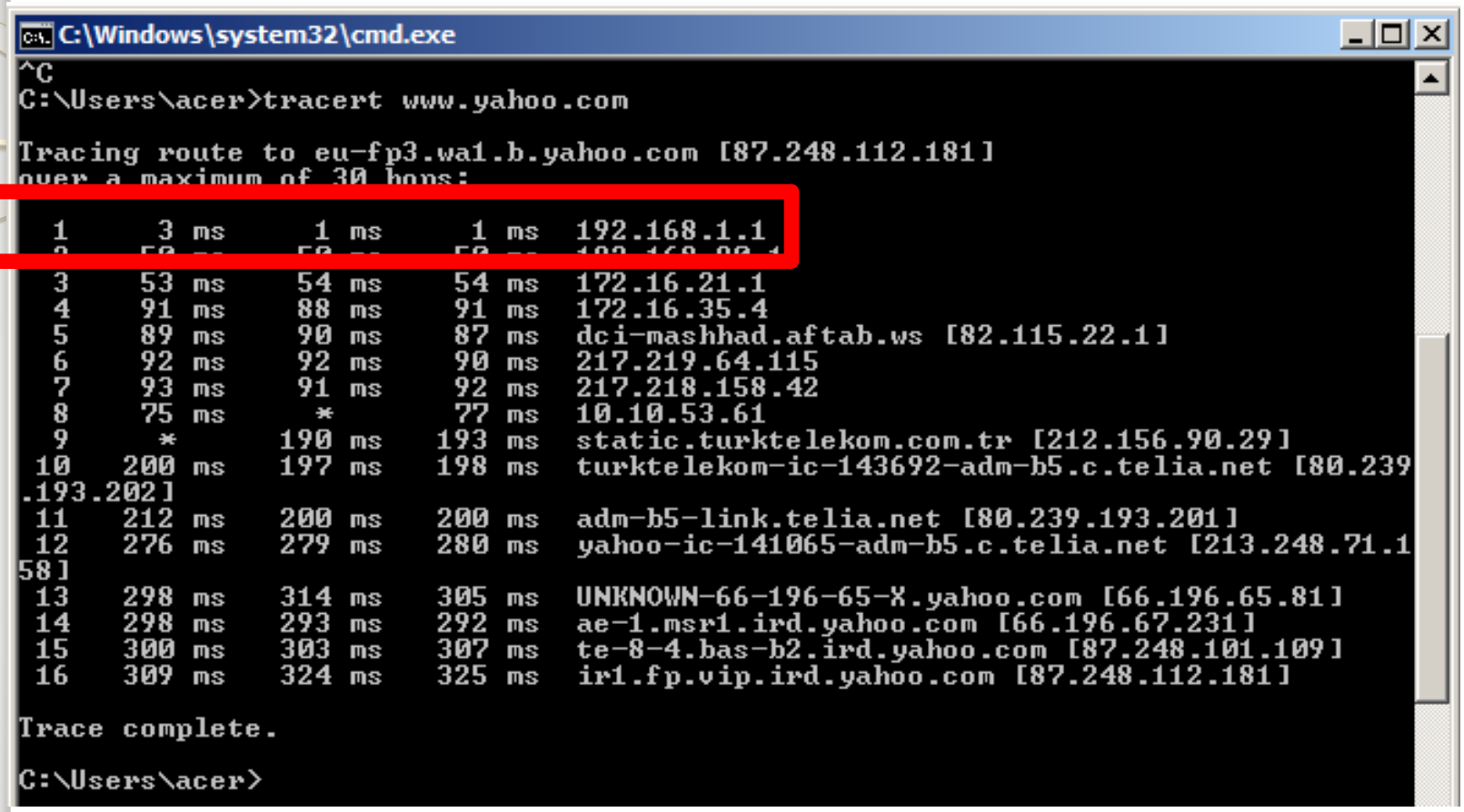
دیدگاه های نرم افزاری شبکه



C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

دیدگاه های نرم افزاری شبکه

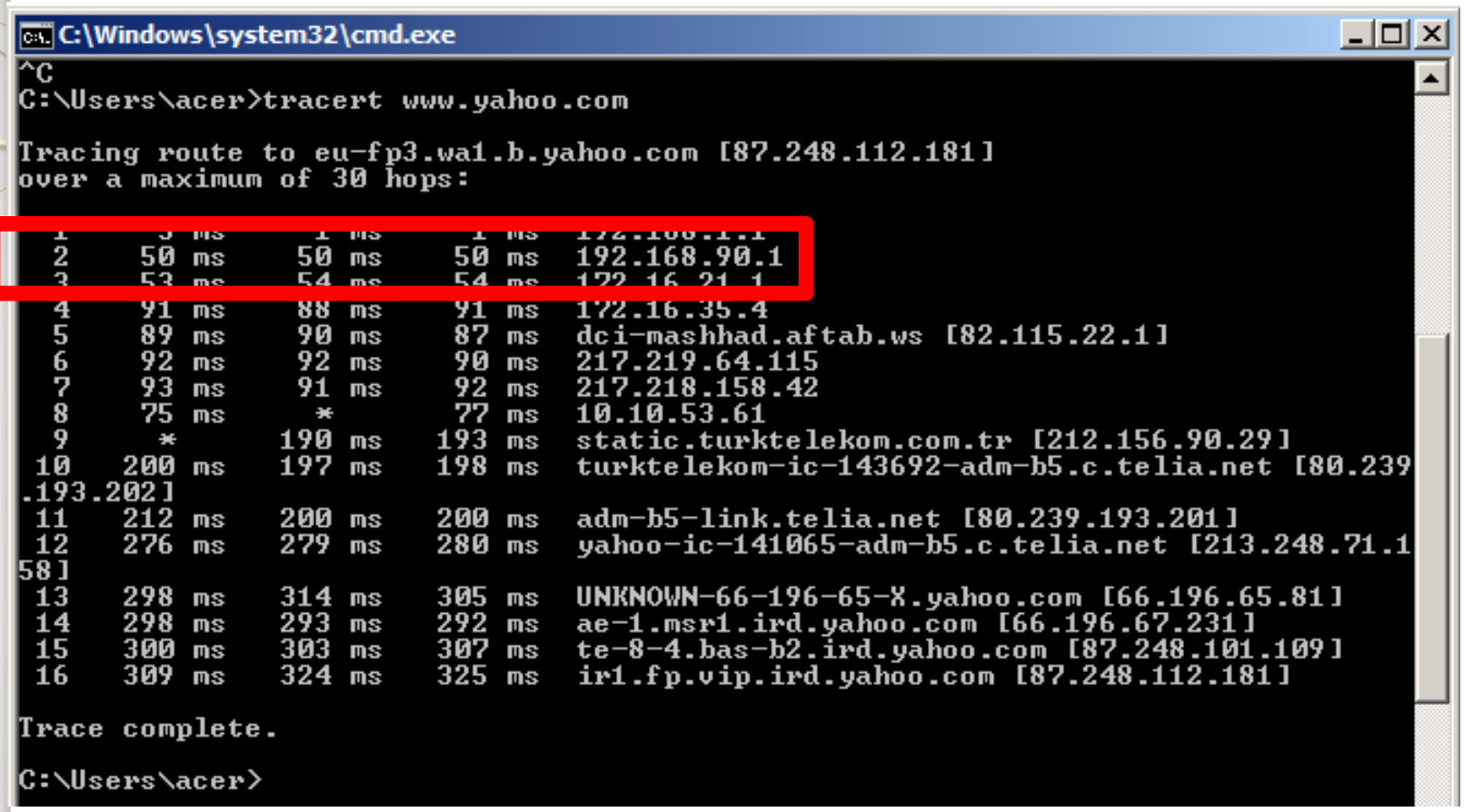


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

ICMP: Internet Contorol Message Protocol

دیدگاه های نرم افزاری شبکه

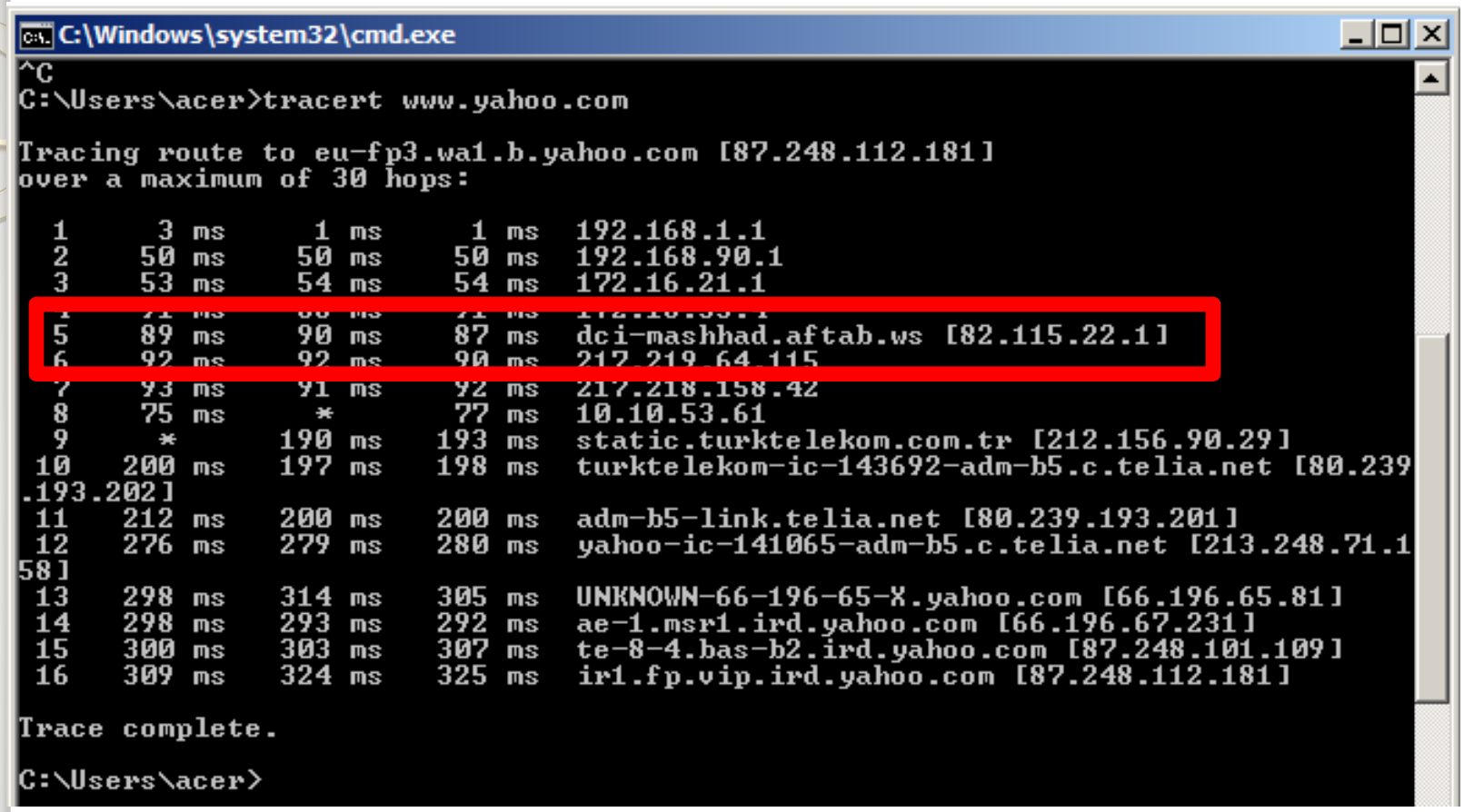


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

ICMP: Internet Contorol Message Protocol

دیدگاه های نرم افزاری شبکه

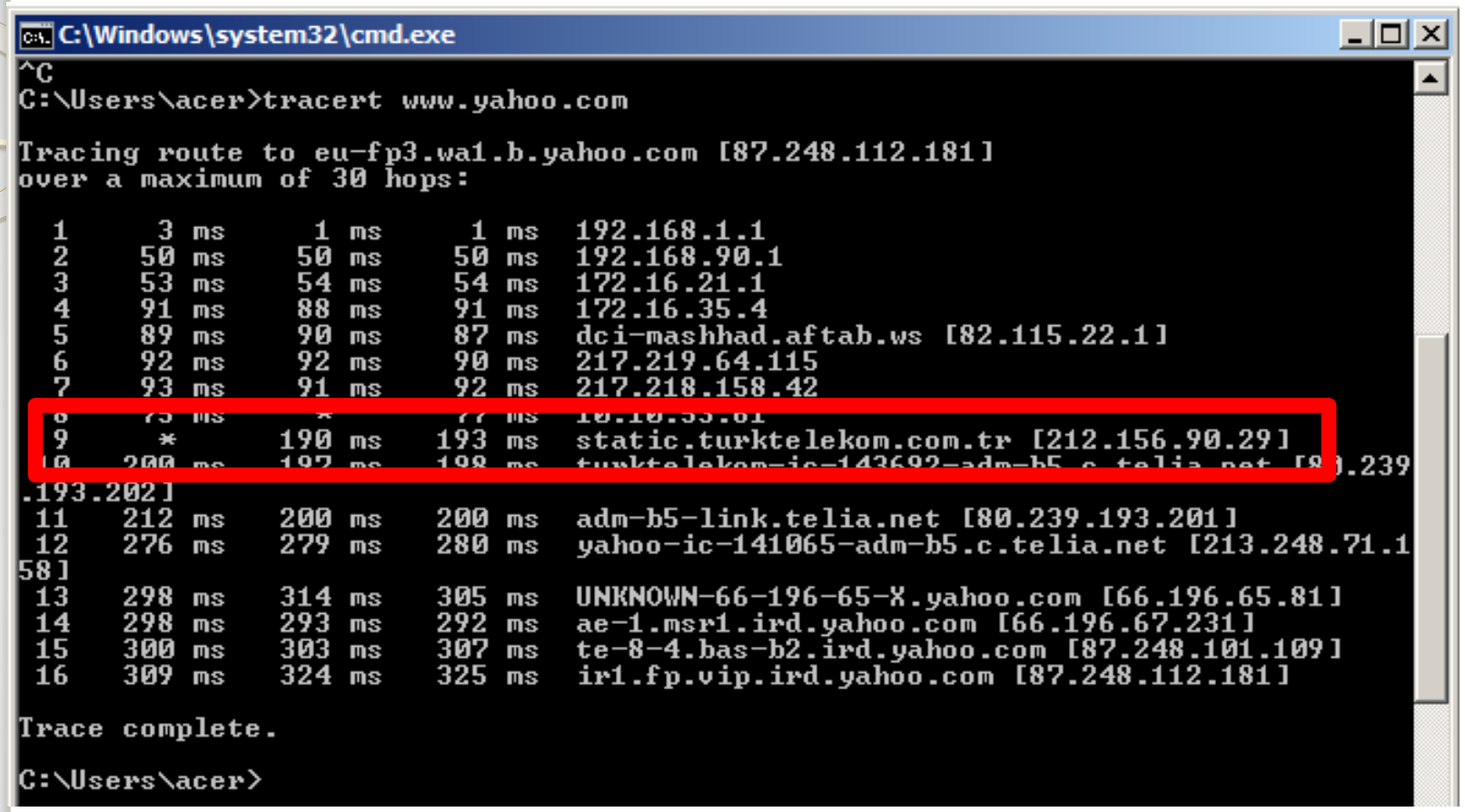


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

ICMP: Internet Contorol Message Protocol

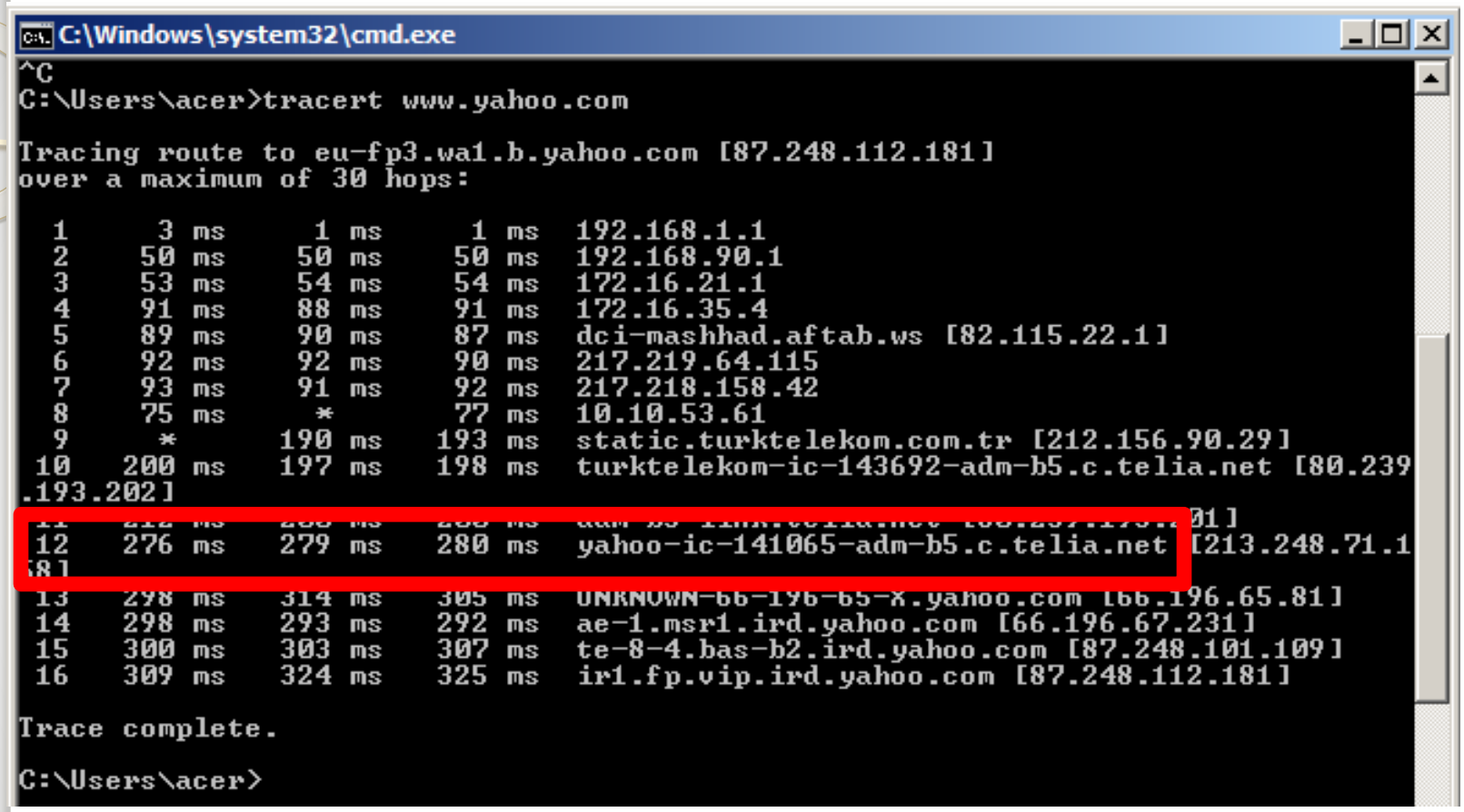
دیدگاه های نرم افزاری شبکه



C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

دیدگاه های نرم افزاری شبکه

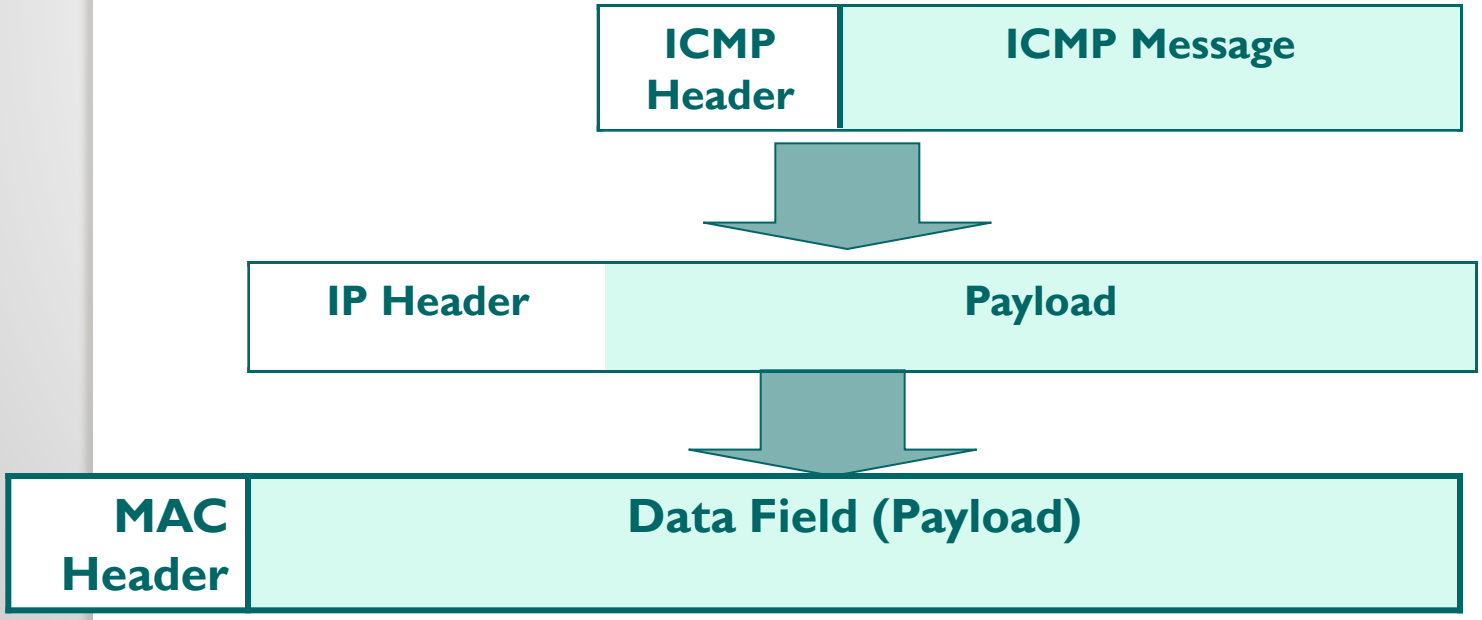


C:\>Ping <IP Address> or <url>

C:\>tracert <IP Address> or <url>

پروتکل ICMP: Internet Control Message Protocol

- بررسی انواع خطا و ارسال پیام برای مبدأ بسته در صورت بروز خطا و اعلام نوع خطا
- یک سیستم گزارش خطا
- قرارگرفتن پیام ICMP درون بسته IP

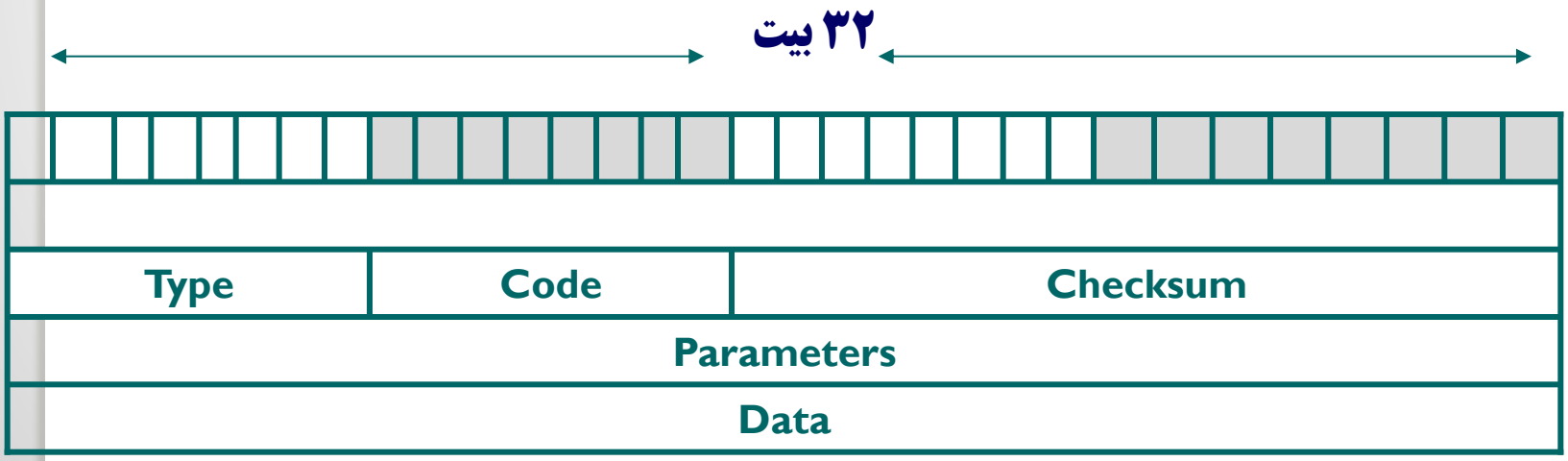


قالب پیام ICMP

فیلد **Type**: مشخص کننده نوع پیام

فیلد **Code**: مشخص کننده کد زیرنوع

فیلد **Checksum**: جهت سنجش اعتبار و درستی بسته **ICMP**



انواع پیامهای ICMP

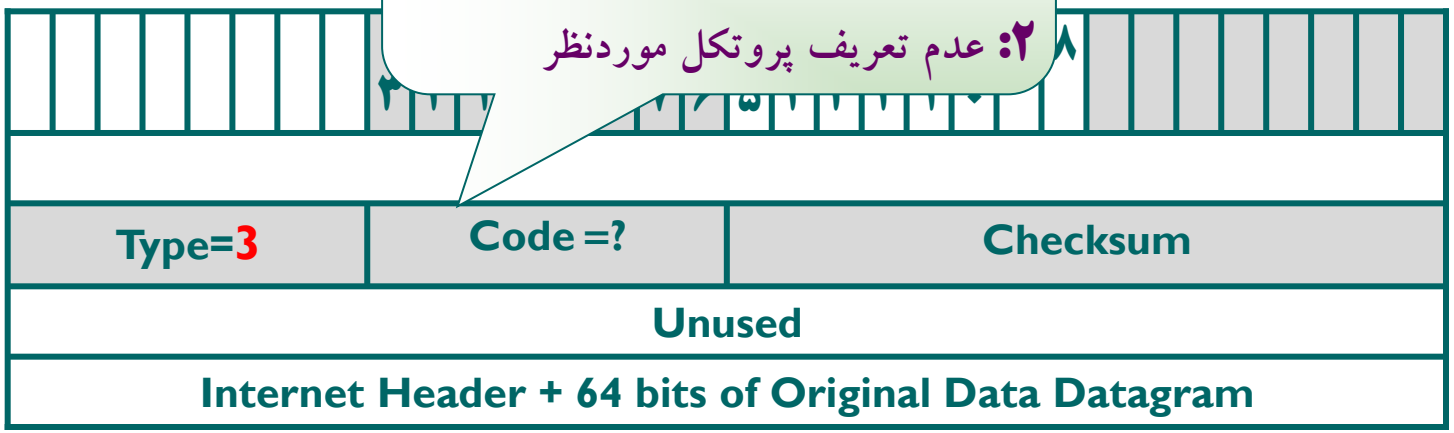
1) پیام Destination Unreachable

- عدم تشخیص آدرس توسط مسیریاب و یا زیر شبکه
- نرسیدن بسته به مقصد به هر علت

۰: در دسترس‌نبودن شبکه مورد نظر

۱: در دسترس‌نبودن ماشین میزبان

۲: عدم تعریف پروتکل موردنظر

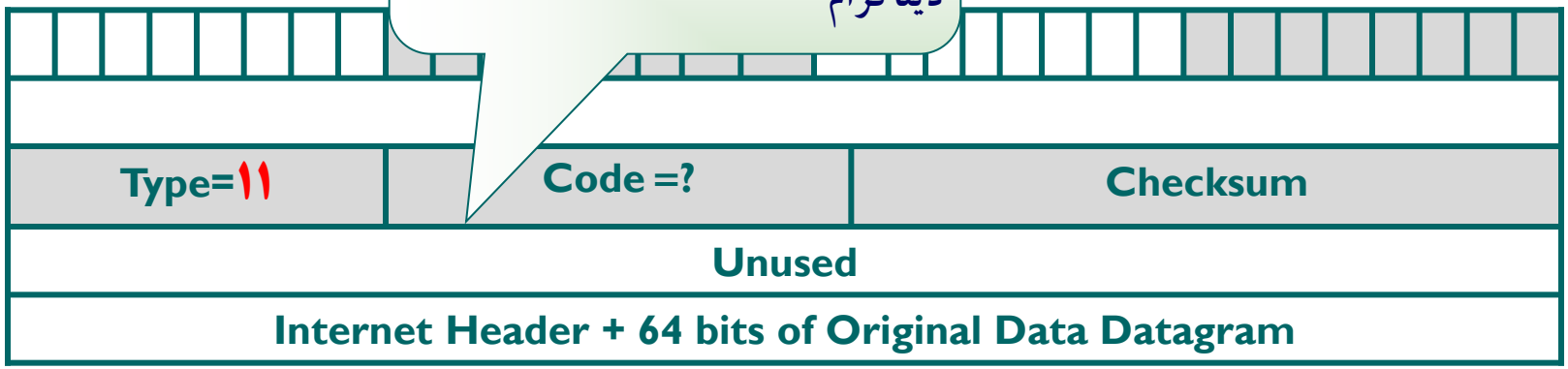


۲) پیام Time Exceeded

ارسال پیام به فرستنده بسته جهت آگاهی از اتمام طول عمر بسته و حذف آن توسط مسیریاب

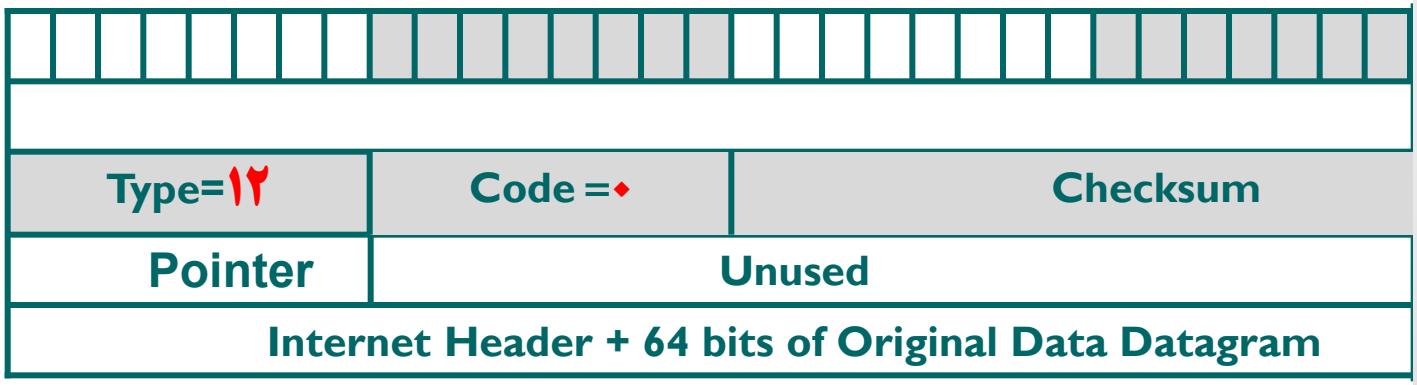
۰ = اتمام زمان حیات بسته

۱= اتمام زمان بازسازی قطعات یک دیتاگرام



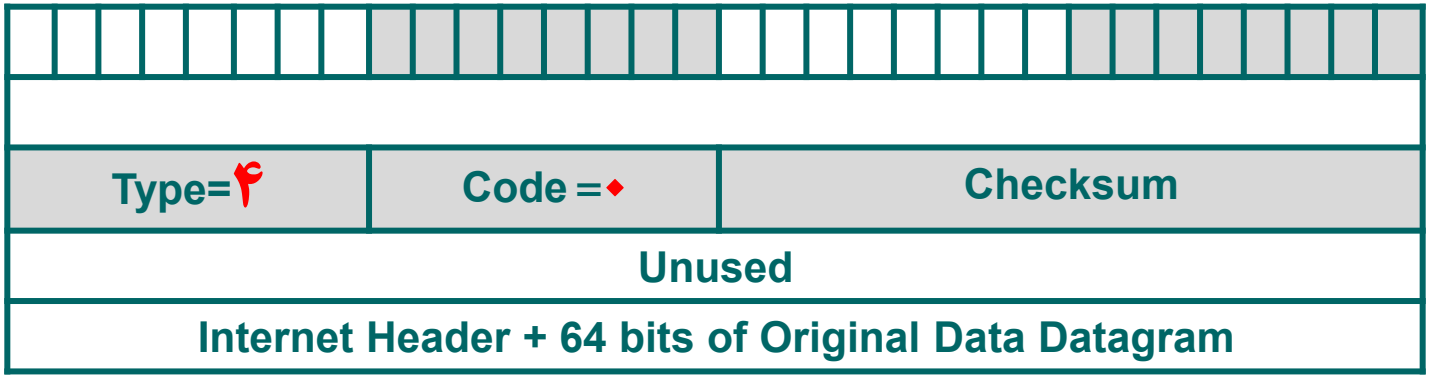
۳) پیام Parameter Problem

نشان‌دهنده وجود مقدار نامعتبر در یکی از فیلدهای سرآیند بسته IP



۴) پیام Source Quench

تقاضای کاهش نرخ تولید و ارسال بسته‌های IP از ماشین میزبان



۵) پیام Redirect

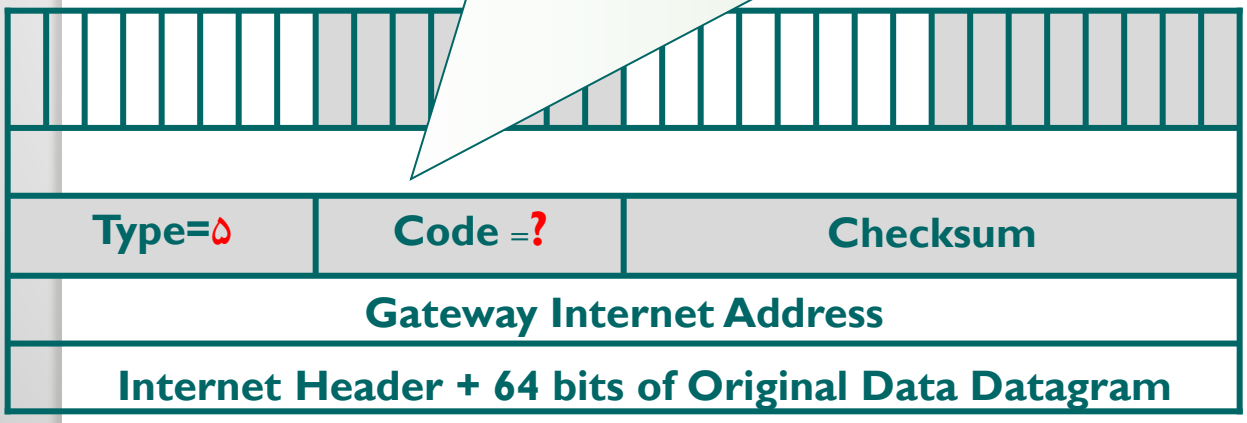
وجود اشکال در مسیریابی

۰ = تغییر مسیر به شبکه‌ای که آدرس آن مشخص شده است.

۱ = تغییر مسیر به ماشینی که آدرس آن مشخص شده است.

۲ = تغییر مسیر به شبکه‌ای که آدرس آن مشخص شده است جهت تأمین سرویس ویژهٔ درخواستی مشخص شده در فیلد **Type of service**

۳ = تغییر مسیر به ماشینی که آدرس آن مشخص شده است جهت تأمین سرویس ویژهٔ **Type of service** درخواستی مشخص شده در فیلد



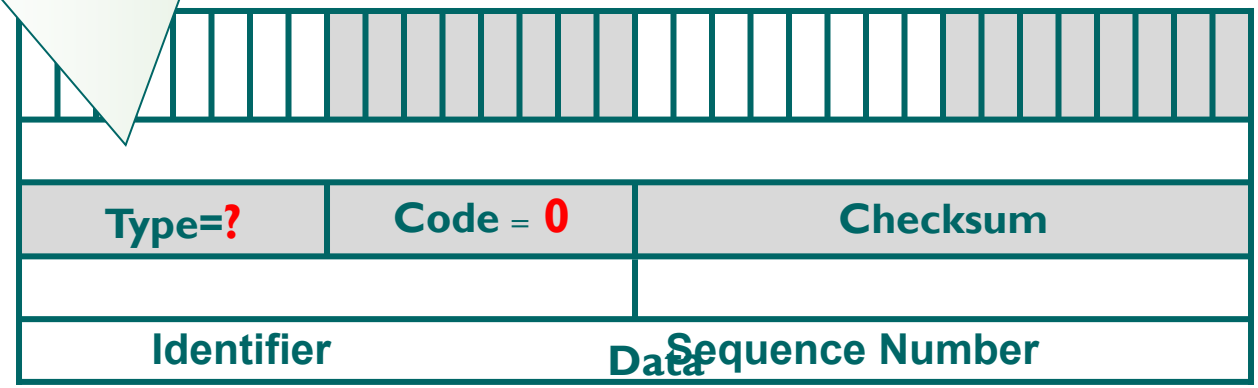
۶) پیامهای Echo Request , Echo Reply

پیام **Echo Request** : موجود و قابل دسترس بودن یک ماشین خاص در شبکه توسط مسیریاب

پیام **Echo Reply**: پاسخ مقصد مبنی بر دریافت پیام **Echo Request**

Echo Request برای مشخص کردن پیام : **8**

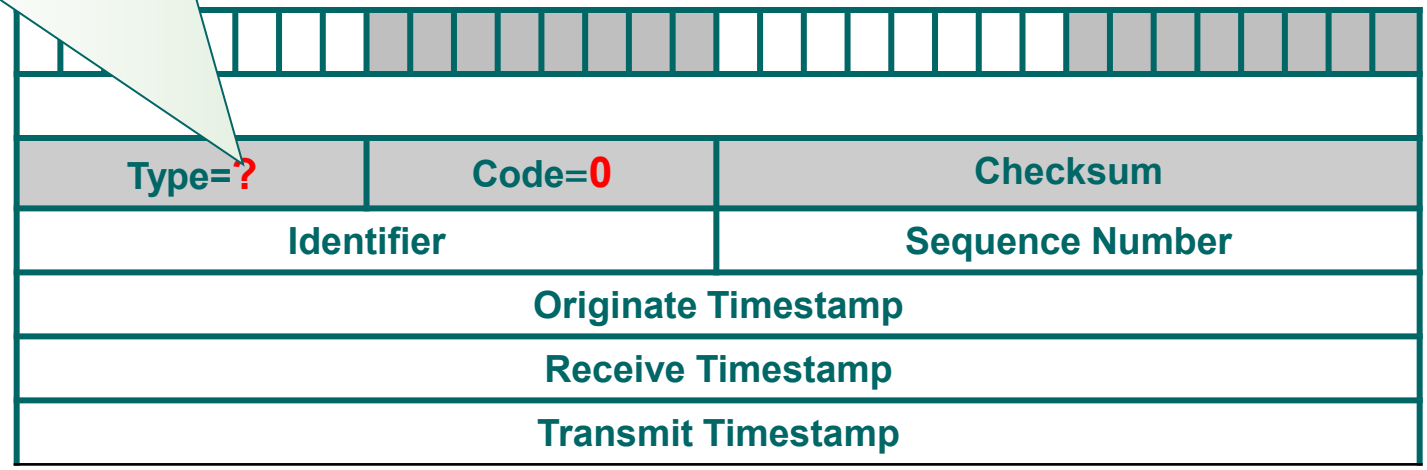
Echo Reply برای مشخص کردن پیام : **0**



۷) پیامهای Timestamp Reply و Timestamp Request

دریافت‌کننده پیام **Timestamp Request** زمان دریافت و زمان ارسال بسته را نیز مشخص می‌کند.

Timestamp Request برای مشخص کردن پیام : **13**
Timestamp Reply برای مشخص کردن پیام : **14**



پروتکل تخصیص آدرس به میزبان ها ...

Dynamic Host Configuration Protocol (DHCP)

دیدگاه های نرم افزاری شبکه

پروتکل تخصیص آدرس به میزبان ها ...

- Dynamic Host Configuration Protocol v4 (DHCPv4) assigns IPv4 addresses and other network configuration information dynamically
- The DHCPv4 server dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address
- Clients lease the information from the server for an administratively defined period.
- Administrators configure DHCPv4 servers to set the leases to time out at different intervals.
- The lease is typically anywhere from 24 hours to a week or more. When the lease expires, the client must ask for another address, although the client is typically reassigned the same address.

DHCPv4 Operation

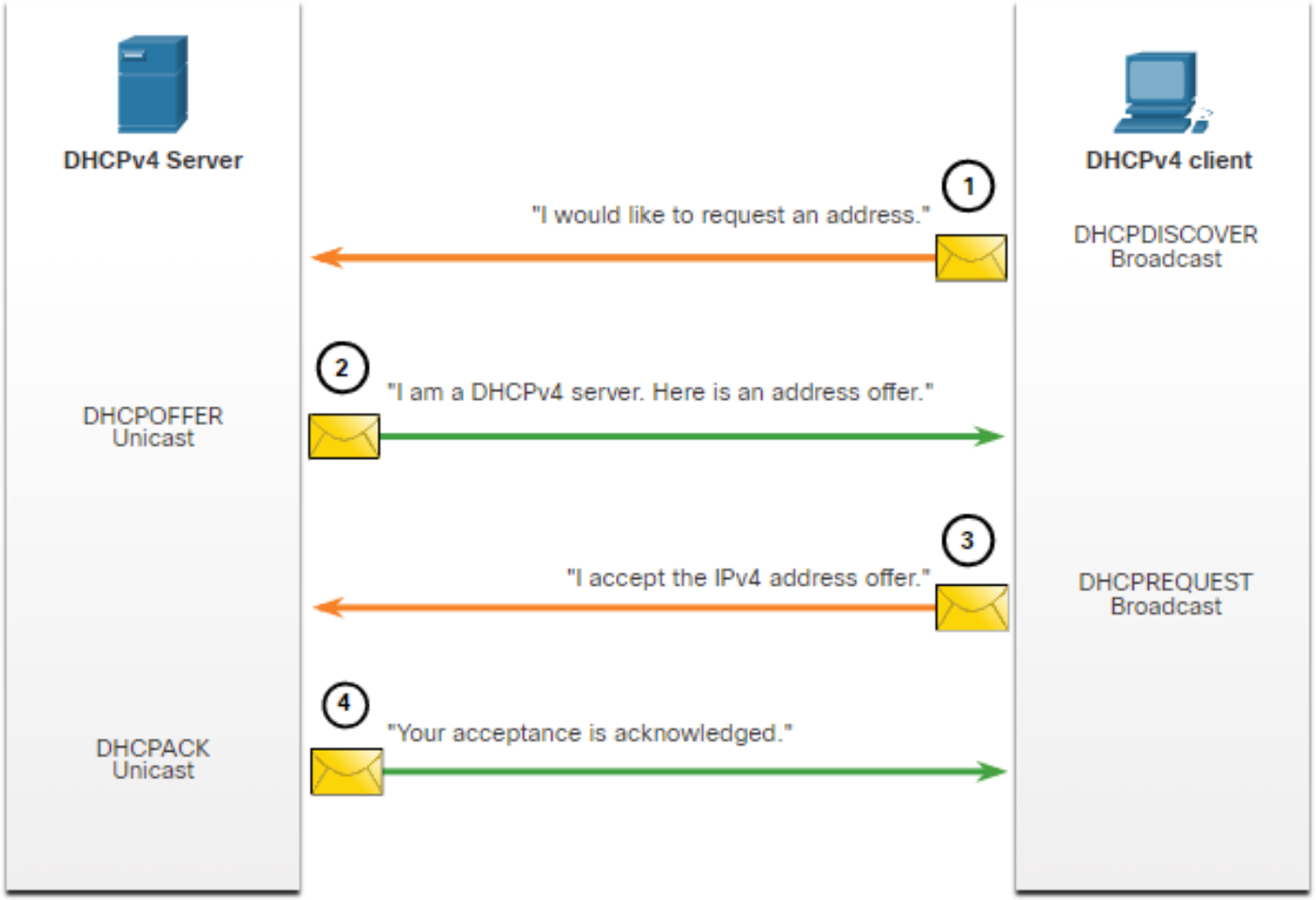
پروتکل تخصیص آدرس به میزبان ها ...

DHCPv4 works in a client/server mode. When a client communicates with a DHCPv4 server, the server assigns or leases an IPv4 address to that client

- The client connects to the network with that leased IPv4 address until the lease expires. The client must contact the DHCP server periodically to extend the lease
- This lease mechanism ensures that clients that move or power off do not keep addresses that they no longer need
- When a lease expires, the DHCP server returns the address to the pool where it can be reallocated as necessary

DHCPv4 Operation

پروتکل تخصیص آدرس به میزبان ها ...



DHCPv4 Operation

پروتکل تخصیص آدرس به میزبان ها ...

When the client boots (or otherwise wants to join a network), it begins a four-step process to obtain a lease:

1. DHCP Discover (DHCPDISCOVER)

2. DHCP Offer (DHCPOFFER)

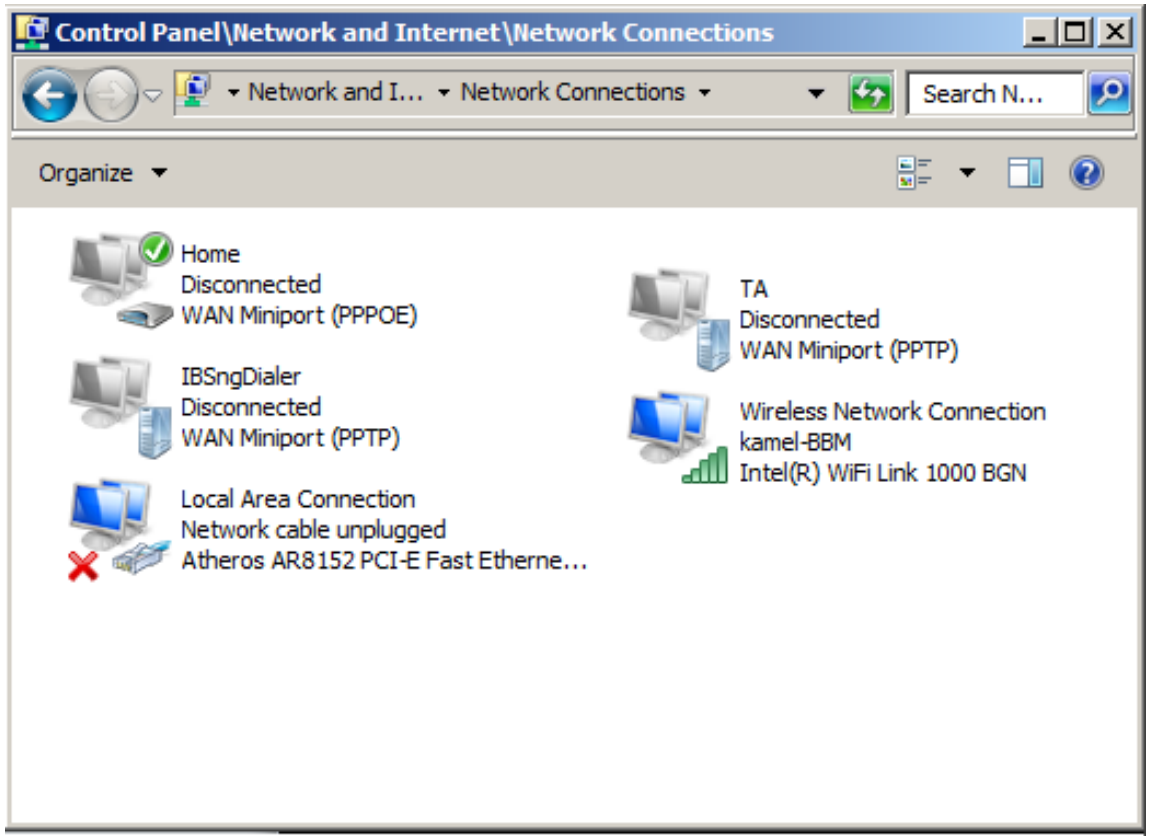
3. DHCP Request (DHCPREQUEST)

4. DHCP Acknowledgment (DHCPACK)

دیدگاه های نرم افزاری شبکه

Internet Protocol (IP) پروتکل

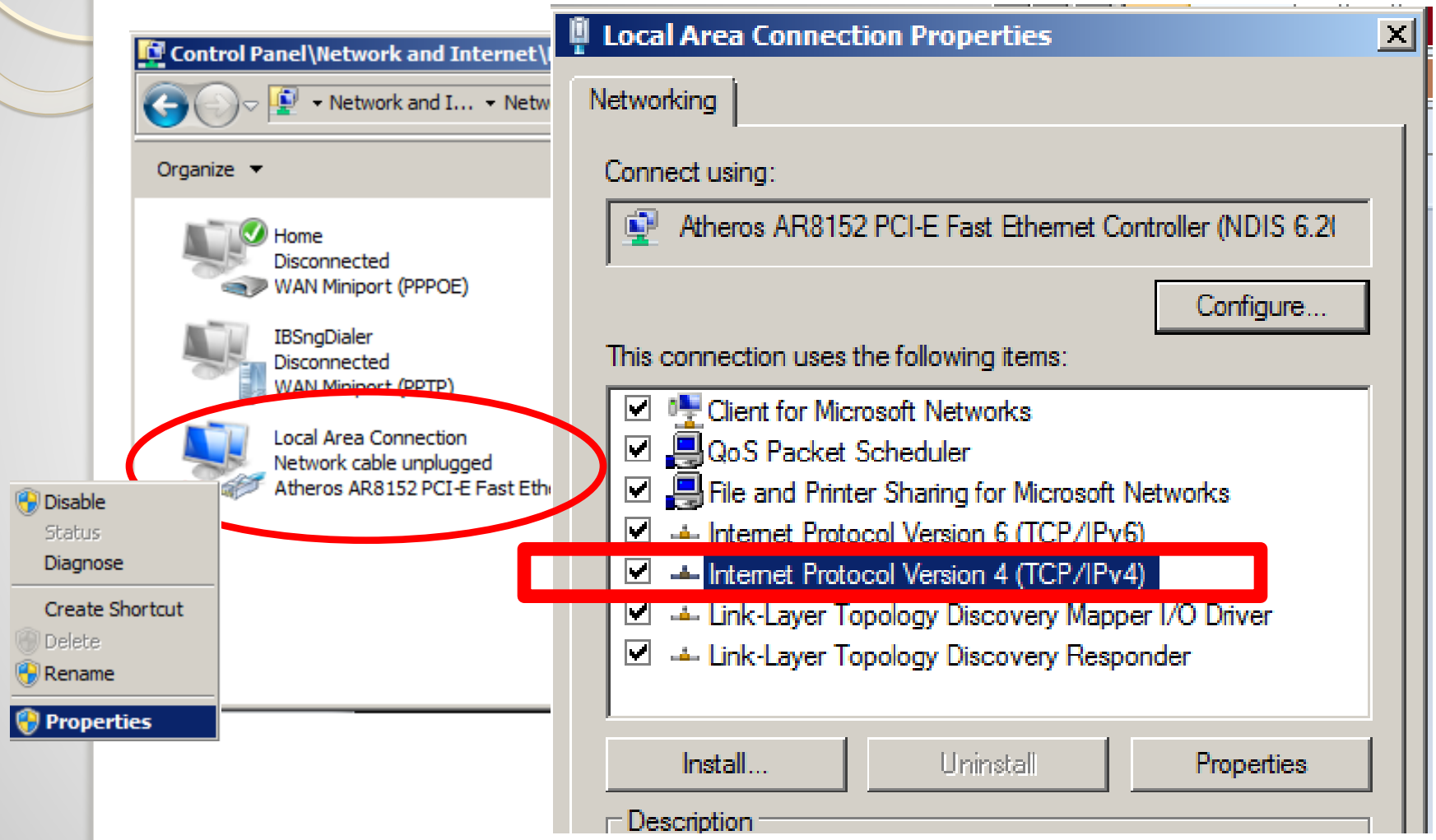
تنظیم میزبان ها برای دریافت آدرس خودکار ...



Internet Protocol (IP) پروتکل

دیدگاه های نرم افزاری شبکه

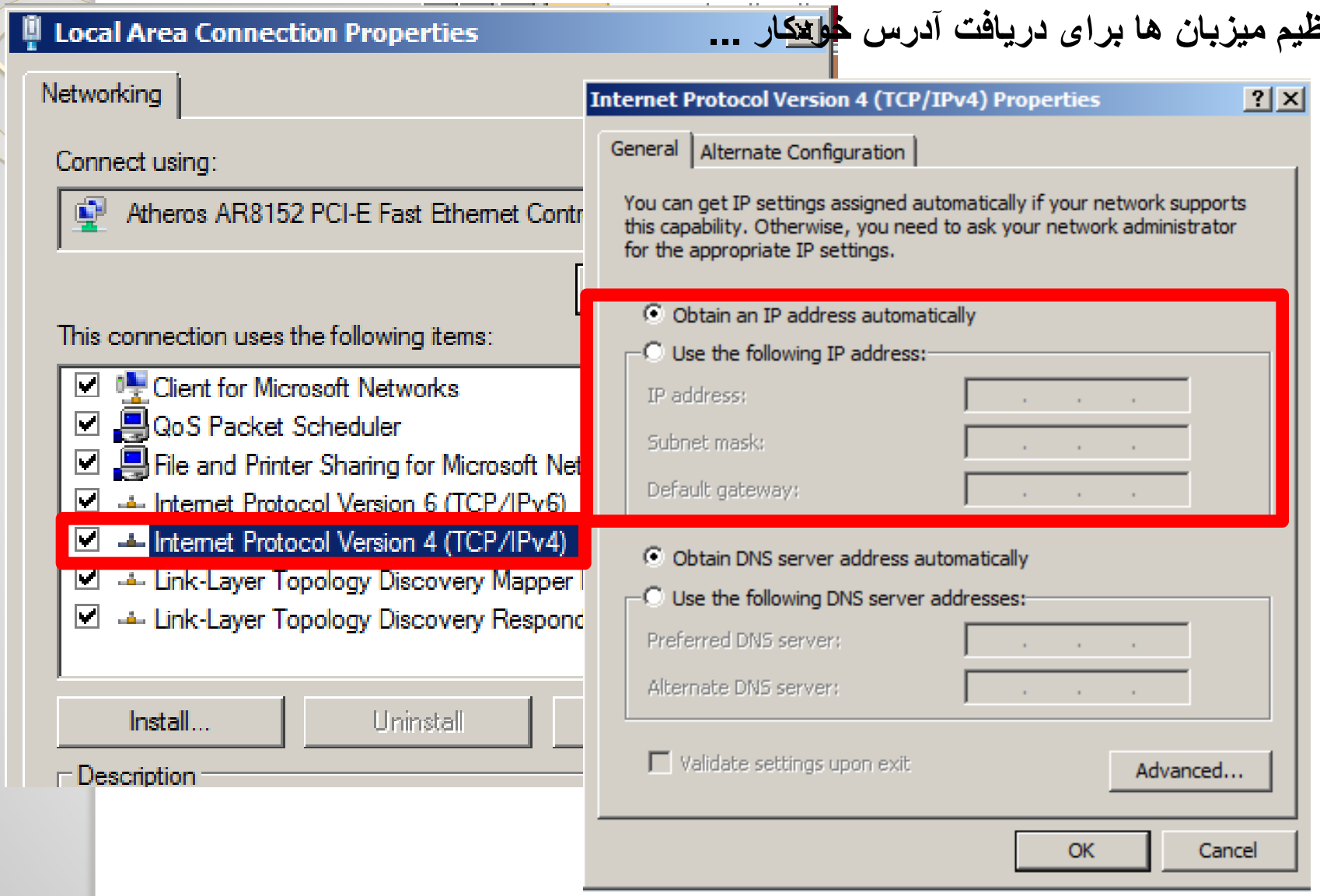
تنظیم میزبان ها برای دریافت آدرس خودکار ...



دیدگاه های نرم افزاری شبکه

Internet Protocol (IP) پروتکل

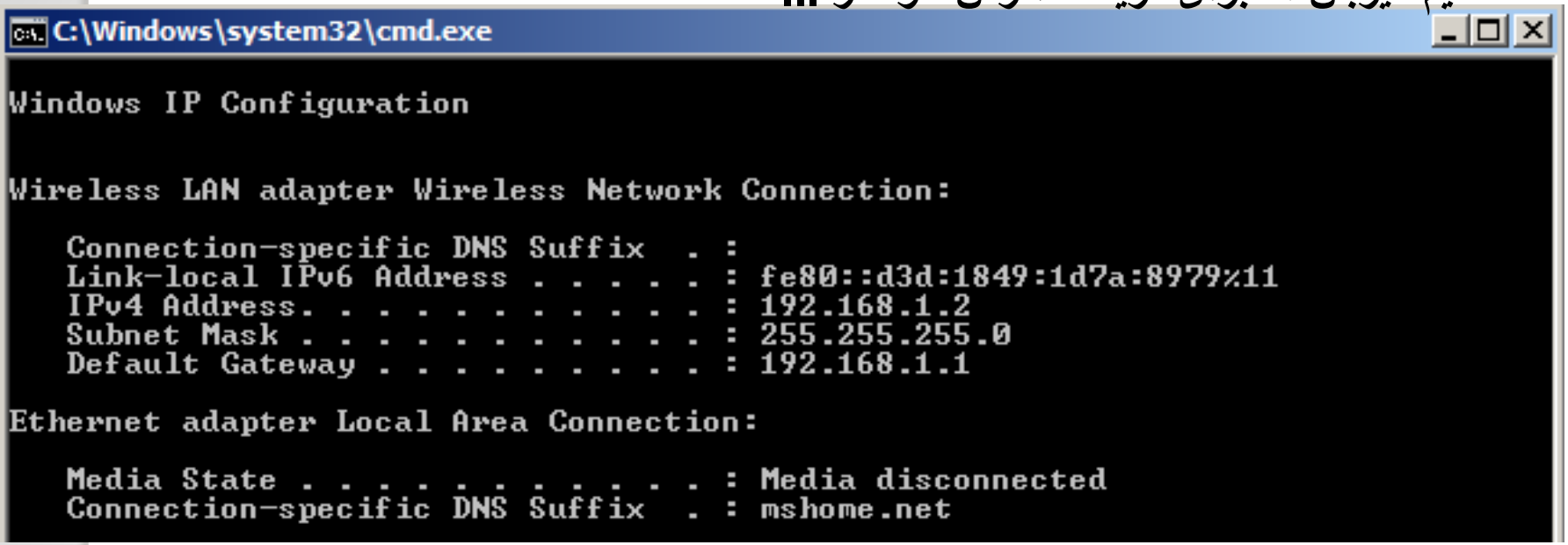
تنظیم میزبان ها برای دریافت آدرس خودکار ...



دیدگاه های نرم افزاری شبکه

Internet Protocol (IP) پروتکل

تنظیم میزبان ها برای دریافت آدرس خودکار ...



C:\>ipconfig

C:\>ipconfig /all

پروتکل زمان ...

Network Time Protocol (NTP)

Network Time Protocol (NTP)

- Network Time Protocol (NTP) synchronizes clocks of hosts and routers in the Internet
- Over 100,000 NTP peers deployed in the Internet and its tributaries all over the world
- Provides nominal accuracies of low tens of milliseconds on WANs, submilliseconds on LANs, and submicroseconds using a precision time source such as a cesium oscillator or GPS receiver

Network Time Protocol (NTP)

Application of NTP …

- Stock market sale and buy orders and confirmation timestamps
- Network fault isolation, reporting and restoral
- Network monitoring, measurement and control
- Distributed multimedia stream synchronization
- RPC at-most-once transactions; replay defenses; sequence-number disambiguation
- Research experiment setup, measurement and control
- Cryptographic key management and lifetime control

Network Time Protocol (NTP)

Application of NTP …

- Stock market sale and buy orders and confirmation timestamps
- Network fault isolation, reporting and restoral
- Network monitoring, measurement and control
- Distributed multimedia stream synchronization
- RPC at-most-once transactions; replay defenses; sequence-number disambiguation
- Research experiment setup, measurement and control
- Cryptographic key management and lifetime control

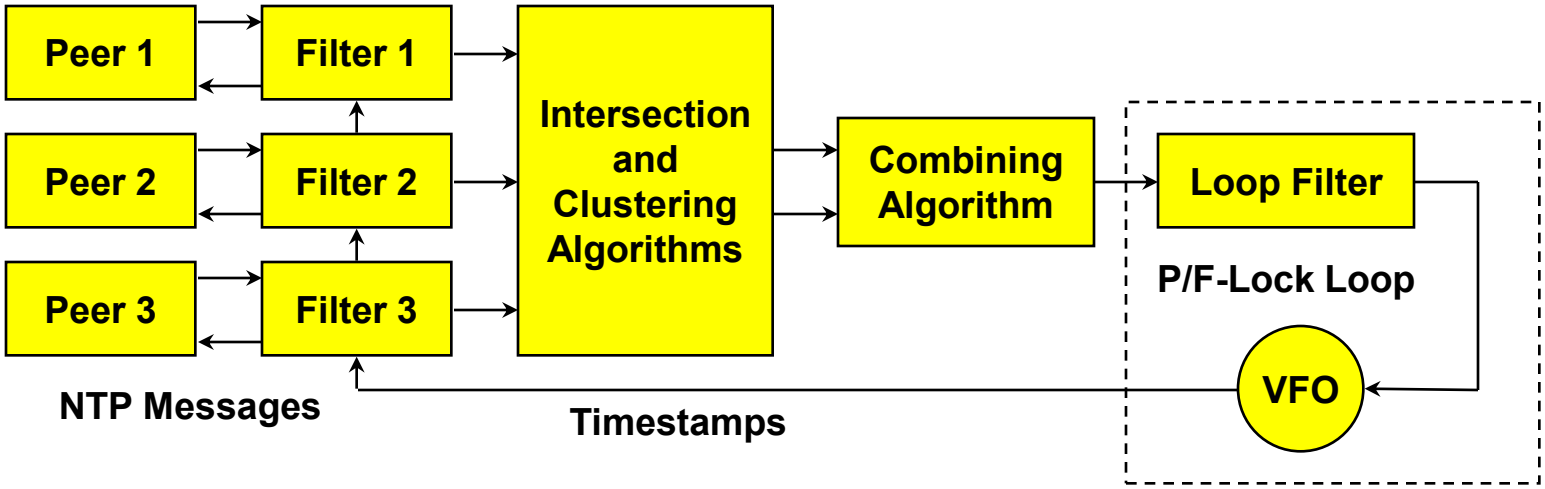
Network Time Protocol (NTP)

How it works …

- Primary (stratum 1) servers synchronize to national time standards via radio, satellite and modem
- Secondary (stratum 2, ...) servers and clients synchronize to primary servers via hierarchical subnet
- Clients and servers operate in master/slave, symmetric or multicast modes with or without cryptographic authentication
- Reliability assured by redundant servers and diverse network paths
- Engineered algorithms reduce jitter, mitigate multiple sources and avoid improperly operating servers
- System clock is disciplined in time and frequency using an adaptive algorithm responsive to network time jitter and clock oscillator frequency wander

Network Time Protocol (NTP)

How it works …



- Multiple synchronization peers provide redundancy and diversity
- Clock filters select best from a window of eight clock offset samples
- Intersection and clustering algorithms pick best subset of servers believed to be accurate and fault-free
- Combining algorithm computes weighted average of offsets for best accuracy
- Phase/frequency-lock feedback loop disciplines local clock time and frequency to maximize accuracy and stability

Other common protocols in LANs

- Port 37: Time
- Port 49: TACACS
- Port 53: DNS
- Port 67: DHCP/BOOTP server
- Port 68: DHCP/BOOTP client
- Port 69: TFTP
- Port 137: NetBIOS name service
- Port 138: NetBIOS datagram service