TCP/IP

شبکه های کامپیوتری ۱

ارائه دهنده

دکتر سید امین حسینی

E.mail: hosseini@um.ac.ir

Home page: http://hosseini.staffcms.um.ac.ir

Time Line

1981. CSNET established.

1983. TCP/IP becomes the official protocol

1983. MILNET was born.

1986. NSFNET established.

1990. ARPANET replaced by NSFNET.

1995. NSFNET became a research network.

1995. **ISPs** started.

Time Line

The following is a list of important Internet events in chronological order:

1969. Four-node ARPANET established.

1970. ARPA hosts implement NCP.

1973. Development of TCP/IP suite begins.

1977. An internet tested using TCP/IP.

1978. UNIX distributed to academic sites.

OSI Model

7 Application

6 Presentation

5 Session

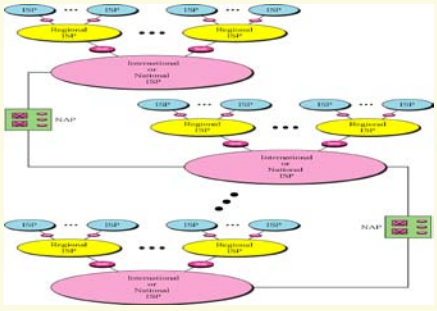
4 Transport

3 Network

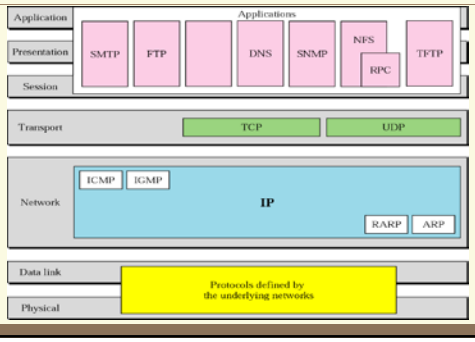
2 Data link

1 Physical

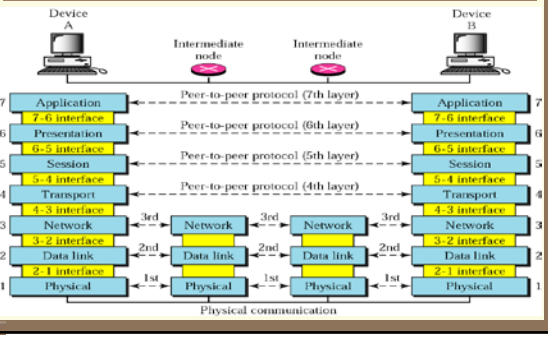
Internet today



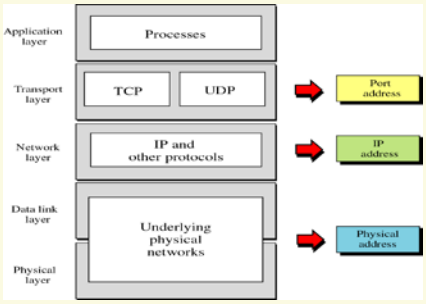
TCP/IP and OSI model



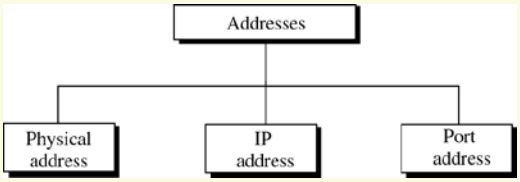
OSI layers



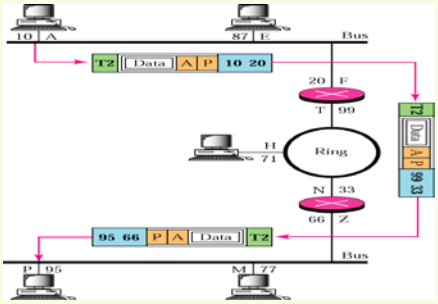
Relation-ship of layers and addresses in TCP/IP



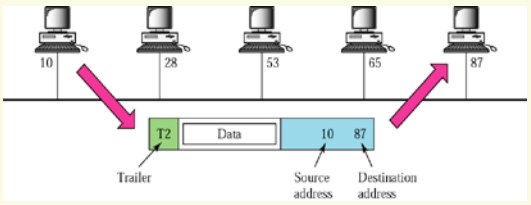
Addresses in TCP/IP



IP addresses



Physical addresses



لایه IP در شبکه اینترنت

لایه IP در شبکه اینترنت

- مفاهیم لایه IP
- تشریح پروتکل و بسته‌های IP
- آدرس‌دهی ماشینها و کلاسهای آدرس
- الگوهای زیر شبکه
- پروتکل ICMP
- پروتکلهای BOOTP,RARP,ARP

۱۴

مقدمه

وظیفه لایه ۲ مدل OSI (پیوند داده ها) آن است که یک فریم اطلاعاتی را بین دو نود که بر روی یک کانال فیزیکی مشترک هستند انتقال دهد و حل و فصل مسایل مربوطه دیگر. آدرسهای قابل تعریف در لایه اول (لایه فیزیکی) جهت انتقال فریمها روی کانال را MAC گویند.

ساختار لایه فیزیکی و پیوند داده ها شدیدا به توپولوژی و سخت افزار شبکه وابسته هست.

۱۵

مقدمه

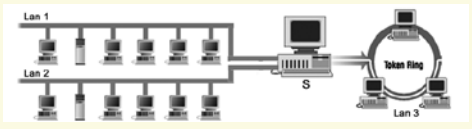
سوال: اگر چند شبکه محلی مستقل و مختلف (بی سیم، اترنت و...) و ارتباط مستقیم فیزیکی بین کانال انتقال در بین آنها نباشد، چگونه انتقال اطلاعات از یک شبکه به شبکه دیگر داشته باشیم؟

باید روی نودهایی که به طریقی روی همه شبکه های محلی حضور داشته باشد بررسی کرد. با این بررسی رسالت لایه سوم از همین جا شروع می شود که هدایت بسته های اطلاعاتی از شبکه ای به شبکه ای دیگر به عهده دارد.

۱۶

مقدمه

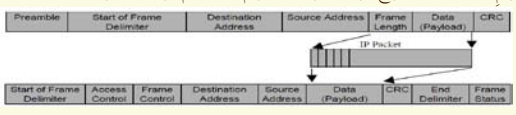
برای ارتباط اطلاعاتی بین دو ایستگاه روی LAN1 و LAN3 نود S بوسیلهٔ سخت افزارِ کارت شبکه، داده ها را از کانال فیزیکی LAN1 دریافت مینماید (این دادهها در فیلد داده از فریم لایهٔ فیزیکی شبکه Ethernet قرار گرفته اند) و پس از استخراج داده ها، مجدداً آنها را درون فیلد داده از فریم شبکهٔ حلقه قرار داده و روی شبکه تزریق میکند.



۱۷

مقدمه

به واحد اطلاعاتی که باید درون فیلد داده از فریم لایه فیزیکی قرار بگیرد بستهٔ IP گفته میشود. این بسته برای عبور از یک شبکه به شبکهٔ دیگر تغییری نخواهد کرد بلکه از فیلد داده در فریم لایهٔ فیزیکی استخراج شده ، در فریم دیگری قرار میگیرد و بدینگونه در شبکه ها طی مسیر میکند. در این شکل فرض شده که یک مسیریاب یک بسته از شبکهٔ Ethernet تحویل گرفته و میخواهد آنرا به شبکهٔ حلقه هدایت نماید؛ برای این کار بسته را از فیلد دادهٔ فریم شبکهٔ اول استخراج کرده و آنرا درون فریم شبکهٔ دوم قرار داده آنرا ارسال مینماید.



آدرس IP

درون یک بسته تعدادی فیلد به منظور تسهیل در هدایت داده ها از یک شبکه به شبکهٔ دیگر درنظر گرفته شده است. دو تا از این فیلدها آدرس مبداء و مقصد هستند که این دو، آدرسهای جهانی محسوب میشوند و دو ماشین را فارغ از ساختار شبکه ای که به آن متصل هستند بصورت یکتا مشخص میکند در شبکهٔ اینترنت به این آدرسها ، آدرسهای IP گفته می شود.

۱۹

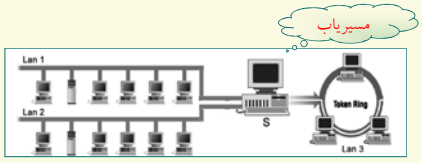
آدرس IP

وقتی یک بستهٔ IP از یک شبکه روی شبکه ای دیگر منتقل میشود آدرسهای MAC یا کلاً (فریم آن) عوض میشود ولیکن ساختار بسته ای که درون فیلد داده قرار گرفته و همچنین آدرسهای IPعوض نخواهد شد.

۲۰

مسیریاب (Router)

- ماشینی با تعدادی ورودی و خروجی
- دریافت بسته‌های اطلاعاتی از ورودی و هدایت و انتخاب کانال خروجی مناسب بر اساس آدرس مقصد



۲۱

لایه اینترنت (Network)

زیرشبکه (**Subnet**) : زیر ساخت ارتباطی شبکه‌ها (مجموعهٔ مسیریابها و کانالهای ارتباطی بین آنها ، توپولوژی زیر شبکه را تشکیل میدهد)

ستون فقرات (**Backbone**) : **خطوط ارتباطی با پهنای باند (نرخ ارسال) بسیار بالا و مسیریابهای بسیار سریع و هوشمند در قسمت زیرشبکه**

۲۲

پروتکل IP:

قراردادی که حمل و تردد بسته های اطلاعاتی و همچنین مسیریابی صحیح آنها را از مبدأ به مقصد ، مدیریّت و سازماندهی مینماید پروتکل IPنام دار.د درحقیقت پروتکل IPکه روی تمامی ماشینهای شبکه اینترنت وجود دارد بسته های اطلاعاتی را از مبداء تا مقصد هدایت مینماید ، فارغ از آنکه آیا ماشینهای مبدأ و مقصد روی یک شبکه هستند یا چندین شبکهٔ دیگر بین آنها واقع شده است.

۲۳

پروتکل IP:

پروتکل IPیک واحد از داده ها را از لایهٔ بالاتر تحویل میگیرد؛ به این واحد اطلاعات معمولاً یک "دیتاگرام "گفته میشود. امکان دارد طول این دیتاگرام بزرگ باشد ، در چنین موردی لایهٔ IPآنرا به واحدهای کوچکتری که هر کدام "قطعه"نام دارد شکسته و با تشکیل یک بستهٔ IPبه ازای هر قطعه ، اطلاعات لازم برای طی مسیر در شبکه را به آنها اضافه میکند و سپس آنها را روی شبکه به جریان میاندازد؛ هر مسیریاب با بررسی و پردازش بسته ها ، آنها را تا مقصد هدایت میکند . هر چند طول یک بسته IPمیتواند حداکثر 64KBSباشد و لیکن در عمل عموماً طول۱۵۰۰ بایت است.

۲۴

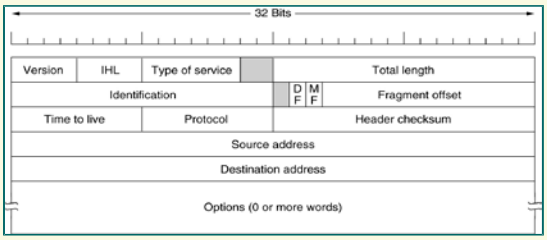
پروتکل IP

دیتاگرام

واحد اطلاعات که به صورت یکجا از لایه IP به لایه انتقال تحویل داده می‌شود یا بالعکس لایه انتقال آنرا جهت ارسال روی شبکه به لایه IP تحویل داده و ممکن است شکسته شود.

۲۵

قالب بسته IP



۲۶

قالب بسته IP

فیلد Version

- چهار بیت
- مشخص کننده نسخه پروتکل IP

نسخه شماره ۴ پروتکل IP Version= 0100

نسخه شماره ۶ پروتکل IP

فیلد IHL (IP Header Length)

- چهار بیتی
- مشخص کننده طول کل سرآیند بسته بر مبنای کلمات ۳۲ بیتی
- حداقل مقدار فیلد IHL عدد ۵

۲۷

قالب بسته IP

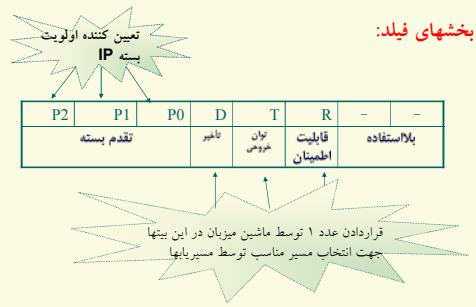
فیلد Type of sevice

- فیلد ۸ بیتی
- مشخص کننده درخواست سرویس ویژه‌ای توسط ماشین میزبان از مجموعه زیرشبکه برای ارسال دیتاگرام

۲۸

قالب بسته IP

بخشهای فیلد:



۲۹

قالب بسته IP

فیلد Total Length

- فیلد ۱۶ بیتی
- مشخص کننده طول کل بسته IP (مجموع اندازه سرآیند و ناحیه داده)
- حداکثر طول کل بسته IP ۶۵۵۳۵ بایت

فیلد Identification

- فیلد ۱۶ بیتی
- مشخص کننده شماره یک دیتاگرام واحد

۳۰

قالب بسته IP

فیلد Fragment Offset

الف) بیت DF (Don't Fragment):

با یک شدن این بیت در یک بسته IP هیچ مسیریابی اجازه قطعه قطعه نمودن بسته را ندارد

ب) بیت MF (More Fragment):

MF=0 : مشخص کننده آخرین قطعه IP از یک دیتاگرام

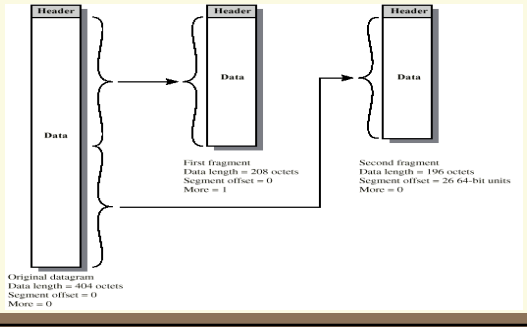
MF=1 : وجود قطعات بعدی از یک دیتاگرام

قالب بسته IP

ج) Fragment offset

- ۱۳ بیتی
- نشان دهنده شماره ترتیب هر قطعه ازیک دیتاگرام شکسته شده
- حداکثرتعداد قطعات یک دیتاگرام ۸۱۹۲

Fragmentation…



قالب بسته IP

فیلد Time To Live

- فیلد ۸ بیتی
- مشخص کننده طول عمر بسته IP
- حداکثر طول عمر بسته IP = ۲۵۵

فیلد پروتکل

- نشان دهنده شماره پروتکل لایه بالاتر متقاضی ارسال دیتاگرام
- فیلد ۸ بیتی

قالب بسته IP

فیلد Header Ckecksum

- فیلد ۱۶ بیتی
- کشف خطاهای احتمالی در سرآیند هر بسته IP

روش محاسبه کد کشف خطا:

جمع کل سرآیند به صورت دو بایت دو بایت

حاصل جمع به روش مکمل یک منفی می گردد

قرارگرفتن عدد منفی حاصله در فیلد Header Ckecksum

قالب بسته IP

فیلد Source Address

- فیلد ۳۲ بیتی
- مشخص کننده آدرس ماشین مبدأ

فیلد Destination Address

- فیلد ۳۲ بیتی
- مشخص کننده آدرس IP ماشین مقصد

قالب بسته IP

فیلد Payload

قرارگرفتن داده های دریافتی از لایه بالاتر دراین فیلد

فیلد اختیاری Option

- حداکثر ٤٠ بایت
- محتوی اطلاعات جهت یافتن مسیر مناسب توسط مسیریابها

۳۷

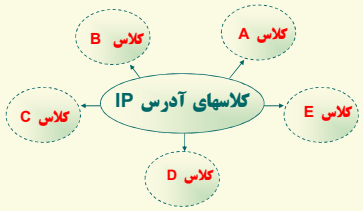
آدرسها در اینترنت و اینترانت

شناسایی تمام ابزار شبکه (ماشینهای میزبان, مسیریابها, چاپگرهای شبکه) در اینترنت با یک آدرس IP

آدرس IP

- ۳۲ بیتی
- پرارزشترین بایت آدرس IP مشخص کننده کلاس آدرس
- نوشتن آدرسهای IP به صورت چهار عدد دهدهی که با نقطه از هم جدا شده اند جهت سادگی نمایش

۳۸



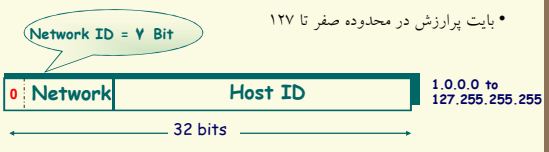
تقسیم ۳۲ بیت آدرس IP به قسمتهای :

آدرس ماشین/ آدرس زیرشبکه/ آدرس شبکه

۳۹

آدرسهای کلاسA

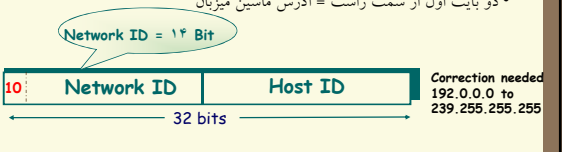
- مقدرا پرارزشترین بیت = ۰
- ۷ بیت از یک بایت اول = مشخصه آدرس IP
- ۳ بایت باقیمانده مشخص‌کننده آدرس ماشین میزبان
- بایت پرارزش در محدوده صفر تا ۱۲۷



۴۰

کلاسB

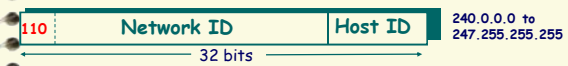
- مقدار دو بیت پرارزش = ۱۰
- ١٤ بیت از دو بایت سمت چپ = آدرس شبکه
- دو بایت اول از سمت راست = آدرس ماشین میزبان



۴۱

کلاسC

- مناسب‌ترین و پرکاربردترین کلاس از آدرسهای IP
- مقدار سه بیت پرارزش = ۱۱۰
- ۲۱ بیت از سه بایت سمت چپ = مشخص‌کننده آدرس شبکه
- ۸ بیت سمت چپ = آدرس ماشین میزبان



۴۲

کلاس D

- مقدار چهار بیت پرارزش = ۱۱۱۰
- ۲۸ بیت = تعیین آدرسهای چند مقصده (آدرسهای گروهی)
- کاربرد = عملیات رسانه‌ای و چند پخشی

۴۳

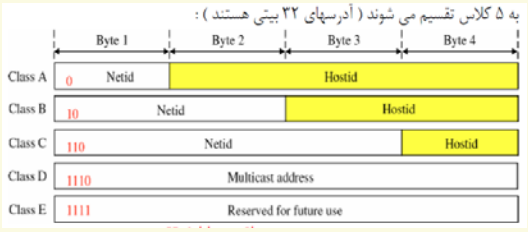
کلاس E

- مقدار پنج بیت پرارزش = ۱۱۱۱۰

۴۴

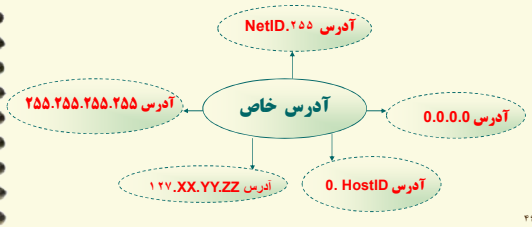
کلاس های آدرس در یک نگاه

به ۵ کلاس تقسیم می شوند (آدرسهای ۳۲ بیتی هستند) :



آدرسهای خاص

در بین تمام کلاسهای آدرس IP با پنج گروه از آدرسها نمی توان یک شبکه خاص را تعریف و آدرس‌دهی نمود.



۴۶

آدرسهای خاص

آدرس 0.0.0.0:

هر ماشین میزبان که از آدرس IP خودش مطلع نیست این آدرس را بعنوان آدرس خودش فرض می‌کند.

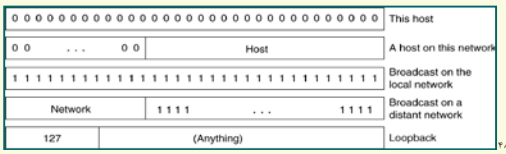
.

۴۷

آدرسهای خاص

آدرس 0. HostID :

این آدرس زمانی به کار می‌رود که ماشین میزبان ، آدرس مشخصهٔ شبکه‌ای که بدان متعلق است را نداند. در این حالت در قسمت NetID مقدار صفر و در قسمت HostID شمارهٔ مشخصهٔ ماشین خود را قرار می‌دهد.



۴۸

آدرسهای خاص

آدرس ۲۵۵.۲۵۵.۲۵۵.۲۵۵:

جهت ارسال پیامهای فراگیر برای تمامی ماشینهای میزبان بر روی شبکهٔ محلی که ماشین ارسال‌کننده به آن متعلق است .

آدرس NetID.۲۵۵ :

جهت ارسال پیامهای فراگیر برای تمامی ماشینهای یک شبکهٔ راه دور که ماشین میزبان فعلی متعلق به آن نیست .

۴۹

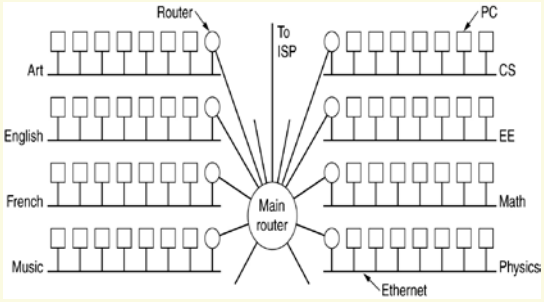
آدرسهای خاص

آدرس 127.xx.yy.zz:

این آدرس بعنوان "آدرس بازگشت" شناخته می‌شود و آدرس بسیار مفیدی برای اشکالزدایی از نرم افزار می‌باشد .

۵۰

زیر شبکه سازی

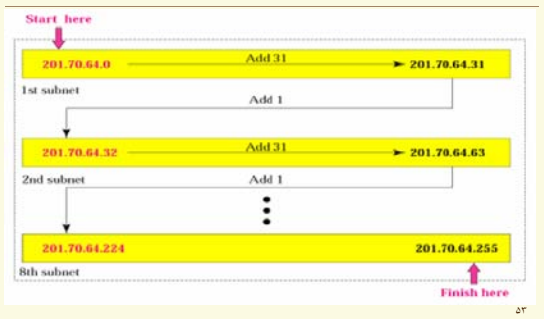


زیر شبکه سازی

مثال: یک شرکت فضای آدرس ۲۰۱.۷۰.۶۴.۰ را دارد (کلاس c) و درخواست subnet6 دارد. از آنجاییکه ۶ توانی از ۲ نیست ,کوچکترین عدد توان ۲ که عد ۸ است را در نظر می گیریم .تعداد یکهای Mask پیش فرض ۲۴ می باشد. بنابراین تعداد یکهای Subnet Mask ۲۷=۳+۲۴ می باشد و تعداد صفرها ۵=۲۷-۳۲ می باشد. بنابراین Subnet 8 هر کدام با $۲^{۵}$=۳۲ آدرس خواهیم داشت .Subnet Mask در این حالت برابر است با: ۱۱۱۰۰۰۰۰ ۱۱۱۱۱۱۱۱ ۱۱۱۱۱۱۱۱ ۱۱۱۱۱۱۱۱یا ۲۵۵.۲۵۵.۲۵۵.۲۲۴

۵۲

زیر شبکه سازی



۵۳

زیر شبکه سازی

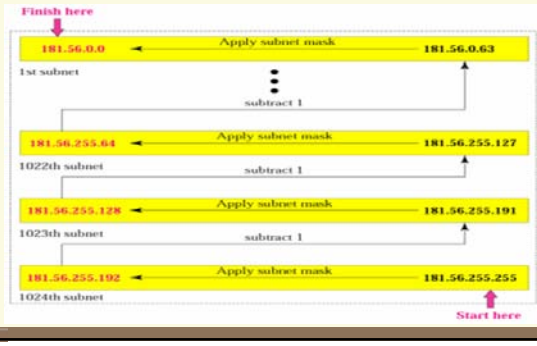
مثال: یک شرکت فضای آدرس ۱۸۱.۵۶.۰.۰(کلاس B) را دارد . این شرکت نیازمند۱۰۰۰ Subnet می باشد .این Subnet را طراحی کنید .

تعداد یکهای Mask پیش فرض ۱۶ می باشد ۱۰۰۰ توانی از ۲ نیست .اولین عدد توان ۱۰۲۴,۲ است بنابراین نیازمند ۱۰ یکدیگر در Subnet Mask هستیم. (۱۶=۱۰+۲۶)

تعداد صفرها نیز ۶=۲۶-۳۲ است.بنابراین Subnet Mask عبارتست از ۱۱۰۰۰۰۰۰ ۱۱۱۱۱۱۱۱ ۱۱۱۱۱۱۱۱ ۱۱۱۱۱۱۱۱ یا ۲۵۵.۲۵۵.۲۵۵.۱۹۲ تعداد Subnet ها ۱۰۲۴,هر Subnet=$۲^{۶}$ آدرس .

۵۴

زیر شبکه سازی



آدرس دهی بدون کلاس

هدف از آدرس‌دهی بد ون کلاس فراهم آوردن بلاکهای آدرس با طول متفاوت می‌باشد.

یک شبکه داخلی ممکن است تنها به ۲ آدرس نیاز داشته باشد؛ یک شرکت کوچک به ۱۶ آدرس و یک شرکت بزرگ به ۱۰۲٤ آدرس. در هر صورت تعداد آدرسهای بلاک باید توانی از ۲ باشد (2,4,8, ...). آدرس شروع بلاک باید بر تعداد آدرسها قابل تقسیم باشد. مثلا اگر بلاک ٤ آدرسه داشته باشیم، آدرس ابتدایی باید بر ٤ قابل تقسیم باشد. برای بلاک با کمتر از ۲۵٦ آدرس، تنها باید سمت راست‌ترین بایت آدرس چک شود و برای بلاکی با کمتر از ٦٥٥۳٦ آدرس ۲ بایت سمت راست چک می‌شود.

نماد /

A.B.C.D/n یک نماد برای نشان دادن تعداد یکهای Mask آدرس می باشند .نماد / را نماد CIDR[۲] نیز می نامند .

مثال: یک سازمان کوچک یک بلاک با آدرس شروع و طول پیشوندی ۲۰۵.۱٦.۳۷.۲٤/۲۹(در نماد /) رادارد .دامنه بلاک را تعیین کنید .

آدرس ابتدایی ۲۰۵.۱٦.۳۷.۲٤ است. برای پیدا کردن آدرس انتهایی ،ما باید ۲۹ بیت اول را حفظ کرده و ۳ بیت انتهایی را با یک تعویض کنیم

Beginning :11001111 00010000 00100101 00011000

Ending :11001111 00010000 00100101 00011111

۵۷

نماد /

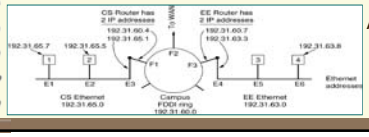
در هر بلاک تنها ۸ آدرس وجود دارد .دامنه آدرس برای این مثال ۸است . بنابراین می توان به شکل زیر نیز آدرس نهایی را محاصبه نمود :

24+7=31 → 205.16.37.31

۵۸

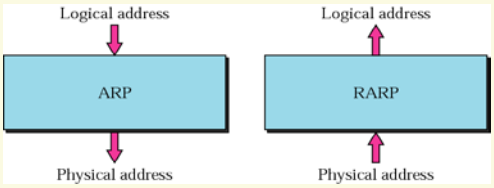
پروتکل Address Resolution Protocol : ARP

- 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

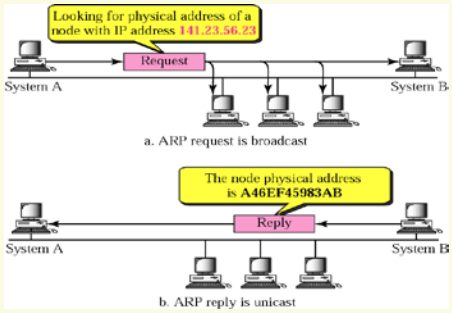


۵۹

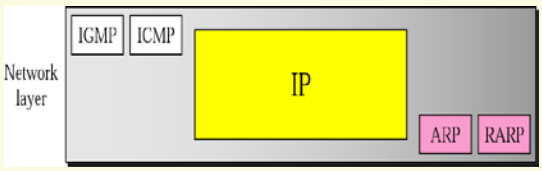
ARP and RARP



ARP operation



Position of ARP and RARP in TCP/IP protocol suite

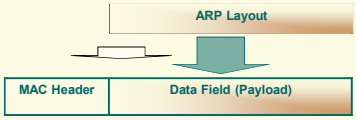


ARP packet

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

پروتکل ARP : Address Resolution Protocol

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

۶۳

ادامه پروتکل

ARP

protocol type: نوع پروتکلی که لایه دوم از آن استفاده می‌کند.

برای TCP/IP این شماره ۲۰۴۸ است .

Hardware Adress Length: طول آدرس فیزیکی(بر حسب بایت)

Porotocol Address Length: طول آدرسهای IP که در TCP/IP مقدار ٤ است.

Opration code (Opcode): ۱ برای ARP request و ۲ برای ARP reply

Source Hardware Address: آدرس فیزیکی مبدأ

Soursce IP Address: آدرس IP ماشین مبدأ

Destination Hardware Address: آدرس فیزیکی ماشین مقصد

Destination IP Address: آدرسIP ماشین مقصد

۶۵

ادامه پروتکل

ARP

برای بالابردن سرعت پروتکل ARP، وقتی برای یکبار آدرس فیزیکی متناظر با آدرس IP از یک ایستگاه بدست آمد، پروتکل ARP این دو آدرس را در جدولی درون حافظه اصلی که ARP Cache نامیده می‌شود ذخیره می‌کند تا اگر مجددا به این آدرس نیاز شد به سرعت در اختیار قرار بگیرد.

IF Index	Physical Address	IP Address	Type

IF Index: شماره پورت سخت‌افزاری کارت شبکه

Physical Address: آدرس سخت‌افزاری کارت شبکه

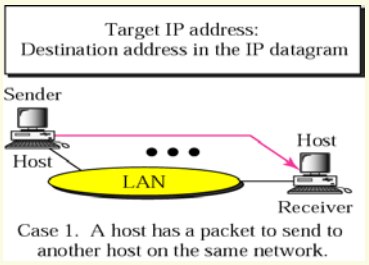
IP Address: آدرس IP متناظر با آدرس سخت‌افزاری

Type: مقدار ۱: یعنی این رکورد باید بطور متناوب به هنگام شوند.

٤: بدین معناست که این رکورد ثابت و بدون تغییر است.

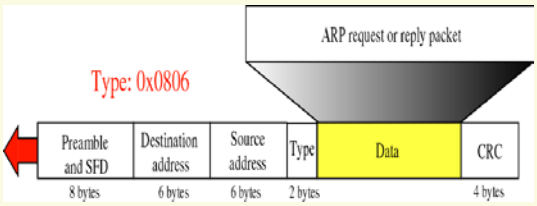
۶۶

Four cases using ARP

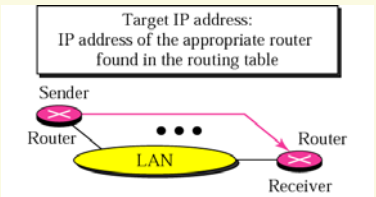


Case 1. A host has a packet to send to another host on the same network.

Encapsulation of ARP packet

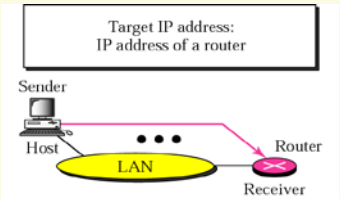


Four cases using ARP



Case 3. A router receives a packet to be sent to a host on another network.
It must first be delivered to the appropriate router.

Four cases using ARP

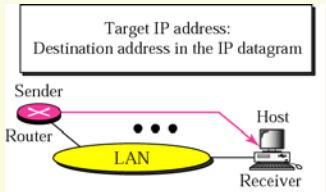


Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to a router.

An ARP request is broadcast;

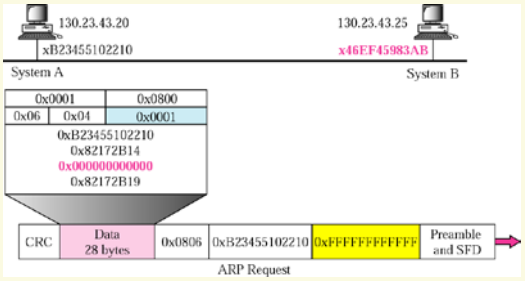
an ARP reply is unicast.

Four cases using ARP



Case 4. A router receives a packet to be sent to a host on the same network.

Example 1 (Request)



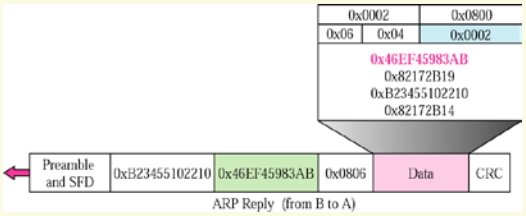
Example 1

A host with IP address 130.23.43.20 and physical address 0xB23455102210 has a packet to send to another host with IP address 130.23.43.25 and physical address 0xA46EF45983AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

Example 2

The ARP output module receives an IP datagram (from the IP layer) with the destination address 114.5.7.89. It checks the cache table and finds that an entry exists for this destination with the RESOLVED state (R in the table). It extracts the hardware address, which is 457342ACAE32, and sends the packet and the address to the data link layer for transmission. The cache table remains the same.

Example 1 (Reply)



Example 4

Fifteen seconds later, the ARP input module receives an ARP packet with target protocol (IP) address 188.11.8.71. The module checks the table and finds this address. It changes the state of the entry to RESOLVED and sets the time-out value to 900. The module then adds the target hardware address (E34573242ACA) to the entry. Now it accesses queue 18 and sends all the packets in this queue, one by one, to the data link layer.

Example 3

Twenty seconds later, the ARP output module receives an IP datagram (from the IP layer) with the destination address 116.1.7.22. It checks the cache table and does not find this destination in the table. The module adds an entry to the table with the state PENDING and the Attempt value 1. It creates a new queue for this destination and enqueues the packet. It then sends an ARP request to the data link layer for this destination.

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
- تمامی‌ایستگاههایی 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: بسته‌هایRARP, ARP از نوع فراگیر محلی Local Broadcast هستند و بالطبع توسط مسیریابها منتقل نمی‌شوند و فقط در محدوده شبکه محلی عمل می‌کنند.

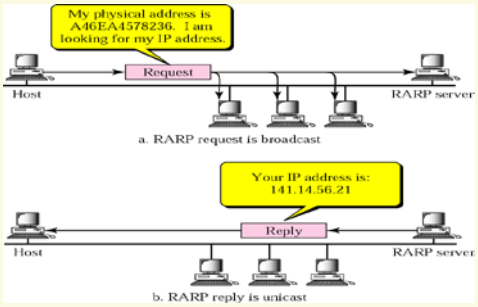
۸۰

Example 5

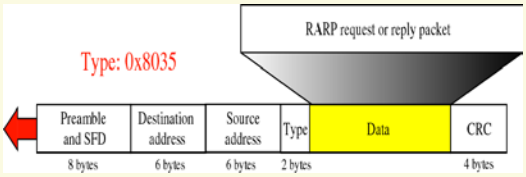
Twenty-five seconds later, the cache-control module updates every entry. The time-out values for the first three resolved entries are decremented by 60. The time-out value for the last resolved entry is decremented by 25. The state of the next-to-the last entry is changed to FREE because the time-out is zero. For each of the three entries, the value of the attempts field is incremented by one. After incrementing, the attempts value for one entry (the one with IP protocol address 201.11.56.7) is more than the maximum; the state is changed to FREE, the queue is deleted.

The RARP request packets are broadcast; the RARP reply packets are unicast.

RARP operation



Encapsulation of RARP packet



RARP packet

Hardware type		Protocol type
Hardware length	Protocol length	Operation (Request 3, Reply 4)
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP) (It is not filled for request)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For example, 4 bytes for IP) (It is not filled for request)		

Alternative Solutions to RARP

When a diskless computer is booted, it needs more information in addition to its IP address. It needs to know its subnet mask, the IP address of a router, and the IP address of a name server. RARP cannot provide this extra information. New protocols have been developed to provide this information. In Chapter 17 we discuss two protocols, BOOTP and DHCP, that can be used instead of RARP.

پروتکل BootP

•چون بسته های RARP از نوع محلی هستند از مسیریابها به خارج از شبکه منتقل نخواهد شد.

•بعضی ایستگاههای بدون دیسک پس از روشن شدن بایستی از طریق سرویس دهندهٔ شبکه بوت شوند لذا گاهی نیاز است که یک آدرسIP روی چند شبکه محلی جستجو شود که در این حالت RARP جوابگو نیست .

• داشتن آدرس فیزیکی ماشین مورد نظر و نیاز به پیداکردن آدرس IP ان در شبکه‌های محلی دیگر

• استفاده از بسته‌های UDP در این پروتکل

•علاوه بر IP درخواستی اطلاعات مربوط به بوتشدن ایستگاه هم ارسال خواهد شد.

۸۶

پروتکل DHCP

• DHCPمخفف عبارت Dynamic Host Configuration Protocol می باشد.

هدف سرویس فوق ، اختصاص نشانی های IP به صورت پویا در زمان اتصال کامپیوتر به شبکه است DHCPبر دو پروتکل قدیمی تر به نام های RARP و BOOTPبنا نهاده شده است. طرز کار سرویس دهنده DHCP به این صورت است که وقتی سیستم سرویس گیرنده راه اندازی می شود از سرویس دهنده DHCP آدرسی را تقاضا می کند و او هم یک آدرس از مخزن آدرس ها را به همراه سایر پارامترهای پیکربندی ایستای مورد نیاز سرویس گیرنده به او اختصاص می دهد

۸۷

پروتکل DHCP

سرویس دهنده DHCP علاوه بر اختصاص اطلاعات پایه نظیر یک آدرس IP و Subnet Mask، قادر به ارائه سایر اطلاعات مربوط به پیکربندی پروتکل TCP/IP برای سرویس گیرندگان نیز می باشد. آدرس دروازه اینترنت (Gateway) و سرویس دهنده DNS نمونه هایی در این زمینه هستند. سرویس دهنده DHCPمالکیت آدرس های IP را بر عهده داشته و سرویس گیرندگان اطلاعات فوق را اجاره و به صورت موقت و بر اساس یک بازه زمانی در اختیار خواهند داشت.

۸۸

پروتکل DHCP

• هنگامی که یک ماشین DHCP برای بدست آوردن آدرس IP یک پیغام DHCP DISCOVERرا منتشر میکند. در این پیام نام میزبان و MACارائه می کند.

• در مرحله بعد یک سرور DHCP که روی زیر شبکه قرار دارد توسط پیام DHCP OFFERآدرس IP پیشنهادی به همراه ماسک زیر شبکه و سایر پارامتر های لازم را ارائه می کند.

• مشتری پس از دریافت DHCP OFFER یک پیام DHCP REQUEST به DHCP شبکه می فرستند و پذیرش پیشنهاد ارائه شده را اعلام می کند.

• درنهایت سرور DHCPکه با پیشنهادش موافقت شده یک پیام تایید ACK برای مشتری می فرستد .

۸۹

سایر پیامها

• DHCP NACK: بدلیل تاخیر یا موارد دیگر درخواست را نمپذیرد و مشتری باید از ابتدا درخواست خود را تکرار نماید.

• DHCP DECLEAN: رد پیشنهادات ارائه شده توسط سرویس دهنده.

• DHCP INFORM: مشتری جهت آگاهی از پارامتر ها بجز ip استفاده میکند.

• DHCP RELEASE: مشتری جهت اعلام خروج از شبکه و هدم نیاز به پارامترهای ثبت شده ارسال می کند

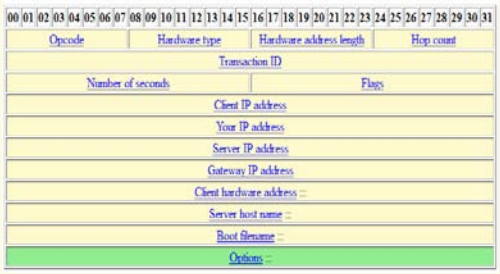
۹۰

فیلد های هدر

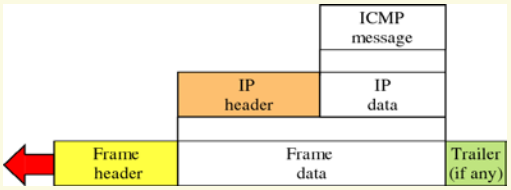
- OPCODE: ۱ بسته تقاضا ۲ بسته پاسخ
- HARDWARE TYPE: ۱ اترنت ۳۳ بیسیم ٦ شبکه های سازگار با 802.X
- ADDRESS LENGTH: طول MAC (٦بایت).
- HOP COUNT: مشتری جهت اعلام خروج از شبکه و هدم نیاز به پارامترهای ثبت
- TRANSACTION ID: ۱ بسته تقاضا ۲ بسته پاسخ
- SECOND: زمان سپری شده برای برسی اولویت
- FLAGS: ۱ یعنی نود هنوز پیکر بندی نشده و باید اطلاعات را BROADCAST کند

...

هدر dhcp

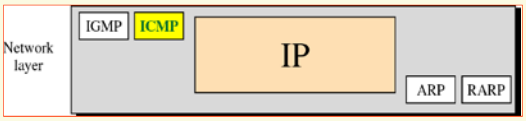


Encapsulation of ICMP packet



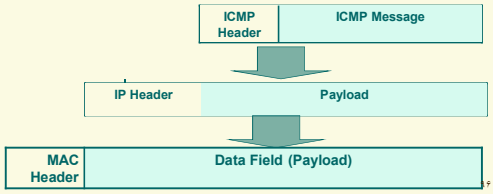
Internet Control Message Protocol (ICMP)

Position of ICMP in the network layer

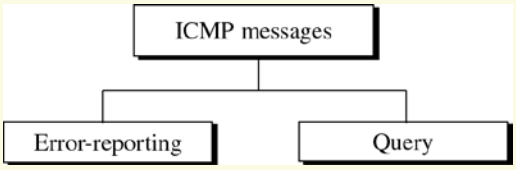


پروتکل Internet Control Message Protocol :ICMP

- 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



ICMP messages

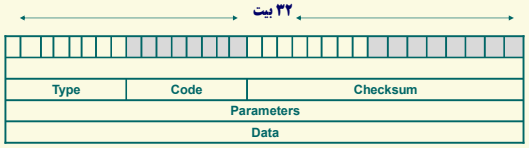


قالب پیام ICMP

فیلد Type: مشخص کننده نوع پیام

فیلد Code: مشخص کننده کد زیرنوع

فیلد Checksum: جهت سنجش اعتبار و درستی بسته ICMP

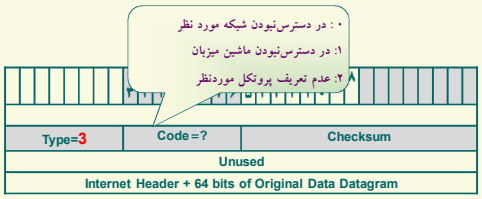


۹۷

انواع پیامهای ICMP

۱) پیام Destination Unreachable

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

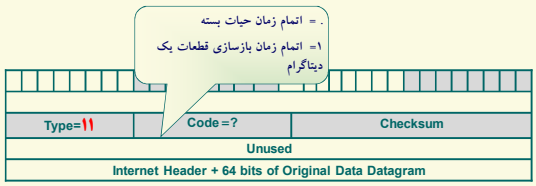


۹۸

انواع پیامهای ICMP

۲) پیام Time Exceeded

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

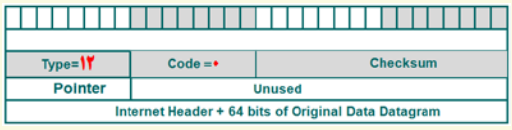


۹۹

انواع پیامهای ICMP

۳) پیام ParAameter Problem

نشان‌دهنده وجود مقدار نامعتبر در یکی از فیلدهای سرآیند بسته IP

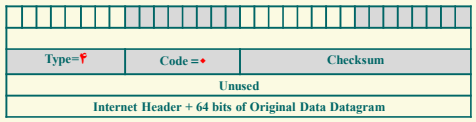


۱۰۰

انواع پیامهای ICMP

٤) پیام Source Quench

تقاضای کاهش نرخ تولید و ارسال بسته‌های IP از ماشین میزبان



۱۰۱

انواع پیامهای ICMP

۵) پیام Redirect

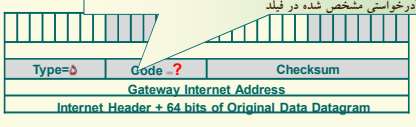
وجود اشکال در مسیریابی

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 درخواستی مشخص شده در فیلدType of service



۱۰۲

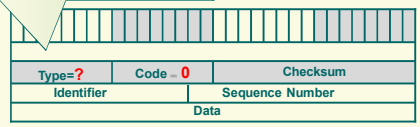
انواع پیامهای ICMP

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

8 : برای مشخص کردن پیام Echo Request
0 : برای مشخص کردن پیام Echo Reply



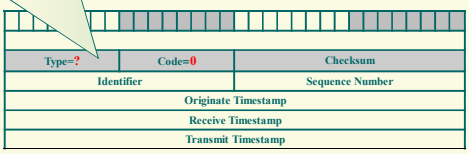
۱۰۳

انواع پیامهای ICMP

۷) پیامهای Timestamp Reply و Timestamp Request

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

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



۱۰۴

Important points about ICMP error messages:

1.No ICMP error message for a datagram carrying an ICMP error message.

2.No ICMP error message for a fragmented datagram that is not the first fragment.

3.No ICMP error message for a datagram having a multicast address.

4.No ICMP error message for a datagram with a special address such as 127.0.0.0 or 0.0.0.0.